Flexxible®

Documentation

FXXOne

Document generated on: 11/9/2025

This file was downloaded from https://docs.fxxone.com//en, FXXOne v25.7. For updated information, please visit https://docs.fxxone.com//en.

Contents

- Introduction 19
  - Documentation in PDF 20
- FlexxAgent 21
  - Features 21
  - Functionality 22
  - Data retention 25
- FlexxAgent / Supported Systems 27
- FlexxAgent / Supported Systems / Windows 28
  - Consumption 28
    - FlexxAgent Process (system) 29
    - FlexxAgent Analyzer Process (user) 29
  - Supported versions 29
  - Software Requirements 30
    - Considerations for Windows versions in EOL 30
    - Limitations 30
  - Download 31
  - Unattended Deployment 31
    - Installation 37
    - Uninstall 37
    - Reinstallation 37
  - Uninstallation Protection 38
    - Considerations 38
    - Configuration at Product Level 38
    - Configuration at Reporting Groups Level 38
    - Ways to uninstall FlexxAgent with protection enabled 40
  - Known Issues 41
  - Supported Parameters 43
  - Proxy Configuration 44
    - Proxy configuration through command line 44
    - Configuration through registry keys 45
    - Manual Update 46
  - Logs 47
    - Installation and update logs 47

Copyright © 2024 Flexxible. Todos los derechos reservados.

        - FlexxAgent Analyzer logs 47
        - FlexxAgent service logs 47
    - Information obtained from the device 49
        - General information 49
        - Extended Info 50
        - Information in tabs 52
- FlexxAgent / Supported Systems / Linux 60
    - Supported versions 61
    - Requirements 61
    - Limitations 62
    - Proxy Configuration 62
    - Download and installation 62
        - Installation Scripts 62
        - Installation steps 63
        - Installation script parameters 63
        - Examples 64
    - Offline installation 64
        - Offline installation steps 64
    - Uninstall 65
        - Uninstallation script parameters 66
        - Examples 66
    - Update 66
    - Logs 67
    - Information obtained from the device 67
        - General information 68
        - Extended Info 69
        - Information in tabs 70
- FlexxAgent / Supported Systems / macOS 72
    - Supported versions 72
    - Limitations 72
    - Proxy Configuration 73
    - Download and installation 73
        - Installation Scripts 73
        - Installation steps 74
        - Installation script parameters 74

Copyright © 2024 Flexxible. Todos los derechos reservados.

        - Examples 74
    - Offline installation 75
        - Offline installation steps 75
    - Uninstall 76
        - Uninstallation script parameters 76
        - Examples 76
    - Update 77
    - Information obtained from the device 77
        - General information 78
        - Extended Info 78
        - Information in tabs 79
- FlexxAgent / Supported Systems / ChromeOS 81
    - Requirements 81
    - Supported versions 81
    - Limitations 81
    - Download and installation 81
        - Installation 82
    - Update 85
    - Information obtained from the device 85
        - General information 86
        - Extended Info 87
        - Information in tabs 87
- FlexxAgent / Supported Systems / Android 90
    - Requirements 90
    - Supported versions 90
    - Limitations 90
    - Settings 90
    - Distribution 91
    - Download and installation 91
    - Update 95
    - Information obtained from the device 95
        - General information 96
        - Extended Info 97
        - Information in tabs 97
- FlexxAgent / Network and Security 100

Copyright © 2024 Flexxible. Todos los derechos reservados.

- Required URLs and Ports 100
- Security 102
  - Antivirus exclusions 102
  - Deep SSL Inspection 103
  - PowerShell process restriction 103
- Wake on LAN (WoL) 103
  - Configure Wake on LAN (WoL) in Windows 104
- Remote assistance through a proxy 105
- vPro 105
  - Requirements for vPro operation via a proxy 105

- FlexxAgent / Wake on LAN (WoL) 106
  - Requirements 106
  - Set up WoL in Windows 106
  - Available actions 107
    - Power on devices on demand from Workspaces 107
    - Schedule power on using Workspace Groups 107
    - Schedule power on after applying updates 107
- FlexxAgent / FlexxAgent Guides 111
- FlexxAgent / Guides / Validate FlexxAgent connectivity 112
  - Creating a scheduled task 112
  - Validation of results 118
- FlexxAgent / Guides / Install FlexxAgent by configuring a proxy server 120
  - Example 120
  - Explanation of the options 121
    - proxyPersistConfig 121
- FlexxAgent / Guides / Set up a proxy server through group policies (GPO) 123
- FlexxAgent / Guides / Deploy FlexxAgent via group policy (GPO) 129
  - Deploying 129
  - Verification 132
- FlexxAgent / Guides / Deploy FlexxAgent with Microsoft Intune 135
- FlexxAgent / Guides / Deploy FlexxAgent for Android with Microsoft Intune 135
- Analyzer 149
  - Included tools 149
  - Web Interface 150
    - List Views 150

Copyright © 2024 Flexxible. Todos los derechos reservados.

        - Detail Views 151
        - Search options 151
        - Column filter 151
        - Page navigation 153
- Analyzer / App Catalog & Inventory 154
- Analyzer / Diagnosis 157
    - Web Interface 157
    - Timeframe selection 158
    - Resource consumption charts 159
    - Performance Counters 160
        - CPU 160
        - RAM 160
        - GPU 160
        - Network Latency 160
        - Disk Usage 161
    - Applications and Processes Tables 161
- Analyzer / Carbon footprint analysis 162
    - Web Interface 162
        - Overview 162
        - Printed copies 163
        - Energy 164
- Analyzer / User experience 167
    - Basic concepts 167
        - Workspace Reliability Index (WRI) 167
        - User surveys 170
    - Web Interface 171
        - Global view 171
        - Individual view 172
- Analyzer / Workspaces in Analyzer 174
    - Workspace detail 175
    - Workspace analysis 177
        - Displays 177
        - Installed Apps 178
        - Running Apps 178
        - Issues in the last 30 days 178

Copyright © 2024 Flexxible. Todos los derechos reservados.

- Usage history 178
- Analyzer / App Groups 179
  - Group Types 179
  - Users consuming applications in the selected group 180
  - Creating a New Application Group 180
- Analyzer / App Versions 181
  - Graphical view 181
  - Table view 181
- Analyzer / Polls 183
  - Poll Settings 183
    - List view 183
    - Detail view 183
  - Poll Execution 185
- Analyzer / Users in Analyzer 186
  - List view 186
  - Detail view 186
    - User data in the detail view 187
- Analyzer / User Groups 189
  - List view 189
  - Detail view 189
- Portal 191
  - Sidebar menu 191
    - Menu collapse 192
  - Organization selector 192
  - User Settings 193
    - Operations List 193
    - My logins 193
    - Settings 193
  - Navigation bar 194
    - Considerations about the navigation bar 195
  - Tables 195
    - Top bar 195
    - Content 197
    - Bottom bar 198
- Portal / Access and authentication 199

Copyright © 2024 Flexxible. Todos los derechos reservados.

- Authentication with a Microsoft Entra ID or Google account 199
  - Enterprise Application Consent and Permissions in Entra ID 199
- Authentication with email and password 199
  - Login process 202
- Access to email and password authentication 203
  - Enable access for a new user 203
  - Enable access for a batch of users 203
  - Enable access from the user table 203
  - Reset the password from the user table 205
- Authentication security settings 206
- User-level authentication security settings 207
  - Two-factor authentication 207
  - Password 211
- Authentication security settings at the organization level 212
  - Enable or disable the email and password authentication option at the organization level 212
  - User table 212
  - User authentication detail 213
- Portal / Analyzer in Portal 213
- Portal / Analyzer / Installed apps 215
  - Installed Apps Details 216
    - Overview 217
    - Versions 217
    - Workspaces 217
    - Installation history 217
    - Report history 217
- Portal / Analyzer / Licenses 217
  - Types of licenses 221
  - Create a License 221
  - License list 221
  - License detail view 223
    - Details 223
    - Installed apps 223
    - Usage history 224
    - Running Processes 225

Copyright © 2024 Flexxible. Todos los derechos reservados.

- Portal / Analyzer / SAM 226
- Portal / Monitor in Portal 227
- Portal / Monitor / Active alerts 229
  - Alert detail view 230
- Portal / Monitor / Alert Configuration 231
  - Create a new alert setting 232
    - Alert Severity 233
    - Alert categories 234
  - Detail view 234
    - Edit alert settings 235
  - Sidebar menu 235
    - Overview 236
    - Active alerts 236
    - Microservices 236
    - Send history 236
- Portal / Operations 237
- Portal / Flows 238
  - Overview 240
    - Overview 241
    - Notification 241
    - Target 242
  - Flow 242
    - Flow conditions 243
    - Action's 244
  - Flow Management 248
    - Enable/Disable Flow 248
    - Edit - Overview, Notification, and Target 248
    - Edit - Flow 249
    - Delete 251
- Portal / Reports 252
  - Considerations about the reports 253
  - Report inventory 253
    - Office 365, Chrome and Adobe Workspaces Inventory 253
    - Office 365 Versions List 253
    - Workspaces Inventory 253

Copyright © 2024 Flexxible. Todos los derechos reservados.

- Generate a report 253
- Share a report 257
  - Share the last report 258
  - Delete a recipient 258
  - Share a specific report 260
- Portal / Tenants 260
  - Types of organizations 262
    - Partner-type organizations 262
    - Client-type organizations 262
    - Suborganizations 262
  - List of tenants 262
    - Tenant interface 263
- Portal / Tenants / Activation 264
- Portal / Workspaces in Portal 265
  - Device detail view 267
    - Overview 267
    - Installed apps 268
    - Active alerts 269
    - Operations 270
    - Sessions 271
    - Windows services 271
    - Disks 271
    - Reporting groups history 272
    - Plug and Play (PnP) events 272
    - Plug and Play (PnP) errors 273
    - Boot history 273
- Portal / Workspaces / Workspace groups 273
  - Static workspace group 275
  - Dynamic workspace group 275
  - Entra ID Workspace group 275
  - Group management 276
    - Workspace Group Details 276
    - Workspaces 276
    - History 276
    - Location 276

Copyright © 2024 Flexxible. Todos los derechos reservados.

        - Schedule 276
        - Sync 276
    - Create groups 280
        - Create a static workspace group from the Portal 281
        - Create a static workspace group from Workspaces 281
        - Create a dynamic workspace group 283
        - Create a Workspace group Enter ID 283
    - Group editing 284
        - Edit a dynamic workspace group 285
        - Delete a workspace group 285
- Portal / Microservices 286
    - Main characteristics of microservices in Portal 287
        - Access to a centralized catalog 288
        - Creation of customized microservices 288
        - Execution scope configuration 288
    - Ways to consume microservices 288
        - On-demand execution from Workspaces 289
        - Scheduled execution through Flows 289
        - Scheduled execution through Alert Settings 290
        - End-user execution 291
- Portal / Microservices / Enabled 291
    - Microservice detail 295
        - Overview 295
        - Code 295
        - Targets 295
        - Settings 295
        - Alert Configuration 295
        - License 298
        - Enabled Tenants 298
- Portal / Microservices / Microservices Marketplace 298
    - Microservice detail 301
        - Overview 301
        - Code 301
        - Targets 301
        - Settings 301

Copyright © 2024 Flexxible. Todos los derechos reservados.

        - Alert Configuration 301
        - License 304
        - Enabled Tenants 304
- Portal / Microservices / Designer 304
    - Microservice creation 307
        - Phase 1 307
        - Phase 2 - License 307
        - Phase 3 - README 308
        - Phase 4 - Script 308
        - Code 310
        - Steps to enable a Microservice 310
- Portal / Microservices / Create with AI 311
    - Create new microservice 312
    - My requests 312
        - Delete a request 317
    - Created Microservices 318
    - Enable a Microservice 319
    - Enable a microservice for the end user 321
- Portal / Microservices / Audit Log 323
- Portal / Patch 324
    - Patching management features 325
    - Patching management considerations in Portal 325
        - FlexxAgent behavior in patch management 325
- Portal / Patch / Summary 326
- Portal / Patch / Reporting groups in patch management 327
    - Total devices per reporting group 329
- Portal / Patch / Targets 329
    - Create a new target 331
    - Target details 331
        - Details 332
        - Schedule 332
    - Update process 332
- Portal / Patch / Microsoft patches 334
- Portal / Patch / Microsoft patch policies 334
    - Create a new update policy 334

Copyright © 2024 Flexxible. Todos los derechos reservados.

- Details 336
- Microsoft patches 337
  - Approve or reject a Microsoft update 337
- Automatic Approvals 338
  - Create an automatic approval rule 339
- Unlisted updates 339
  - Approve or reject an unlisted update 341
- Unlisted automated approvals 342
  - Create an automatic approval rule for unlisted updates 342

- Portal / Settings 343
- Portal / Settings / Organization 346
  - General 347
  - Branding 347
  - Microservices Configuration 347
  - Authentication 347
    - User table 347
    - User authentication detail 352
  - Products 352
    - View details 353
    - FlexxAgent Configuration 354
  - Modules 354
    - Create module 356
- Portal / Settings / Roles 357
  - Create a new role 359
- Roles table 359
  - Roles Subtable 360
- Detail view 360
  - Details 361
  - Permissions 361
    - All tenants 361
    - Tenant 361
    - Portal Permissions 361
    - Workspaces permissions 362
    - Analyzer permissions 362
    - All reporting groups 363

Copyright © 2024 Flexxible. Todos los derechos reservados.

        - Reporting Groups 363
    - Users 363
- Portal / Settings / Roles / Roles included by default 363
- Portal / Settings / Roles / Access levels 364
    - Levels of access by modules 367
        - Portal 367
        - Workspaces 368
        - Analyzer 368
- Portal / Settings / Users 368
    - Create users 380
    - Create a batch of users 380
        - Export users 381
        - Delete users 381
        - Email login actions 382
    - Additional options 382
- Portal / Settings / Integrations 383
    - Integration with Entra ID 384
        - Enable integration with Entra ID 384
    - Integration with Intel vPro® Enterprise 384
        - Requirements 385
        - Enable integration with Intel vPro® Enterprise 385
    - CrowdStrike integration 387
        - Enable integration with CrowdStrike 390
- Portal / Settings / Reporting Groups 391
    - Reporting groups creation 392
        - Fishing pattern 392
    - Reporting groups list 393
        - Auto update of FlexxAgent 394
        - View details 394
        - FlexxAgent configuration (Remote Assistance) 394
- Portal / Settings / FlexxAgent Versions 398
    - Version settings 400
        - Steps for configuration: 400
        - Management from Workspaces 400
- Portal / Settings / Directives 402

Copyright © 2024 Flexxible. Todos los derechos reservados.

- New Directive 404
- Portal / Portal Guides 404
- Portal / Guides / Create and manage workspace groups 406
  - Static workspace groups 407
    - Create a static workspace group from the Portal 407
    - Create a static workspace group from Workspaces 407
  - Dynamic workspace groups 408
    - Create a dynamic workspace group 409
  - Workspaces Enter ID groups 409
    - Create a Workspace group Enter ID 410
  - Manage a workspace group from Portal 410
  - Manage a workspace group from Workspaces 411
- Portal / Guides / Run microservices on a scheduled basis 413
  - Schedule a microservice execution 415
- Portal / Guides / Configure patch policies 415
  - Microsoft patch policy 419
    - Create a new Microsoft patch policy 422
    - Approve or reject a Microsoft update 422
    - Automatic Approvals 422
    - Create an automatic approval rule 423
- Portal / Guides / Enable microservices for the end user 423
  - How to enable a microservice for the end-user 425
    - Rename the microservices folder 425
- Portal / Guides / Set up integration with CrowdStrike 428
  - API Configuration in CrowdStrike 430
  - Configuration in Portal 430
    - View from Workspaces 433
- Portal / Guides / Configure integration with Entra ID 435
  - Requirements for integration 437
  - Configuration in Microsoft Azure 437
    - Create an application registration 437
    - Create a client secret 437
    - Configure permissions for the application registration 437
    - Permissions in the Azure subscription 437
  - Configuration in Portal 437

Copyright © 2024 Flexxible. Todos los derechos reservados.

- Portal / Guides / Set up Entra ID integration with Monitor 446
  - Configuration in Microsoft Azure 448
    - Create an application registration 448
    - Create a client secret 448
    - API permissions configuration 448
    - Create application roles 448
    - Review the manifest.xml file 448
  - Requirements 448
- Portal / Guides / Execution of a microservice after user login 460
  - Flow Configuration 462
  - Daily Recurrence Control 462
- Portal / Billing 463
  - View from a partner-type organization 465
    - Overview 465
    - Tenants consumption details 465
  - View from a client-type organization 465
    - Overview 468
  - FlexxAgent consumption 468
    - Steps to remove a device from a reporting group 469
- Workspaces 470
  - Interface and Access Segmentation 470
    - Level 1 471
    - Level 2 471
    - List Views 471
    - Filtering Options 472
  - Detail Views 472
- Workspaces / Level 1 475
- Workspaces / Level 1 / UX Panel 476
  - Organization filtering 477
  - Date filtering 477
  - Widgets 478
    - Default widgets 478
- Workspaces / Level 1 / Workspaces View 478
  - Filtering 483
    - Header filtering options 483

Copyright © 2024 Flexxible. Todos los derechos reservados.

        - Filtering Options 483
        - Filter management 484
    - Microservices execution 486
    - Available operations 487
    - Operations from the list view 487
        - Power and connection actions 488
        - Tags 488
        - FlexxAgent 488
        - Maintenance (drain mode) 489
        - Refresh device info 489
        - Force compliance check 489
        - Force update custom fields 489
        - Remote Administration 489
        - Remote Assistance 490
        - Device type 490
        - Notifications 490
        - Change the report group 491
- Workspaces / Level 1 / Workspaces / Detail view 491
    - Available actions 492
        - Microservices execution 492
        - Operations 492
    - Information obtained from the device 492
- Workspaces / Level 1 / Workspaces / Remote Assistance 494
    - Features 496
    - Privacy 496
    - Types of remote assistance 496
    - Interactive remote assistance 497
    - Unattended remote assistance 497
    - Dynamic remote assistance 497
    - Requirements to perform remote assistance 497
    - Settings 500
    - Activation 500
        - Activation file download 501
    - Processes 503
    - Behavior of remote assistance through proxy 505

Copyright © 2024 Flexxible. Todos los derechos reservados.

- Flexxible Tools 505
- Workspaces / Level 1 / Sessions 505
  - Available operations 508
    - Session management 509
    - Remote Assistance 509
    - Notifications 509
- Workspaces / Level 1 / Sessions / Detail view 509
  - Available actions 511
    - Microservices execution 511
    - Operations 511
  - General 511
  - Tabs 512
    - Connections 513
    - Performance 513
    - Login information 513
    - Notifications 513
    - Group Policy (GPO) 513
- Workspaces / Level 1 / Connection Logs 513
- Workspaces / Level 1 / Job 516
  - List view 517
    - Top options 517
    - Jobs list 517
  - Detail view 518
    - Statuses 518
    - Available information 518
    - Logs 519
    - Workspaces 519
  - Job subscription 519
- Workspaces / Level 2 520
- Workspaces / Level 2 / Event Logs 521
  - Detail view 522
    - Event log information on a device 525
  - Additional event settings 525
- Workspaces / Level 2 / Locations 525
  - List view 527

Copyright © 2024 Flexxible. Todos los derechos reservados.

- Detail view 527
- Workspaces / Level 2 / Networks 527
  - List view 529
  - Detail view 529
- Workspaces / Level 2 / Notifications 529
  - Close notifications 531
  - Types of notifications 531
    - Sending pop-up messages 531
    - Notifications 531
    - Sending notifications 531
- Workspaces / Level 2 / Reporting groups from Workspaces 534
  - List view 536
    - Download FlexxAgent 536
    - Configuration file download for Linux and macOS 537
  - Detail view 537
    - Devices 538
    - Devices history 538
    - Users 539
    - FlexxAgent Versions 539
- Workspaces / Level 2 / Servers 539
  - List view 540
    - Available operations 540
  - Detail view 540
    - General 541
    - Extended 541
    - Tabs 542
- Workspaces / Level 2 / Wireless networks 543
  - List view 547
  - Detail view 547
- Workspaces / Workspace Guides 547
- Workspaces / Guides / Provide remote assistance to a user 549
- Workspaces / Guides / Change Automatic Restart Sign-On (ARSO) settings 550
  - Deactivate ARSO settings on a device 554

Copyright © 2024 Flexxible. Todos los derechos reservados.

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 includes many features, such as secure remote assistance, detailed diagnostic data collection, system status notifications, self-repair of known issues, and unattended application of support procedures.

FXXOne includes three modules:

- 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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

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.

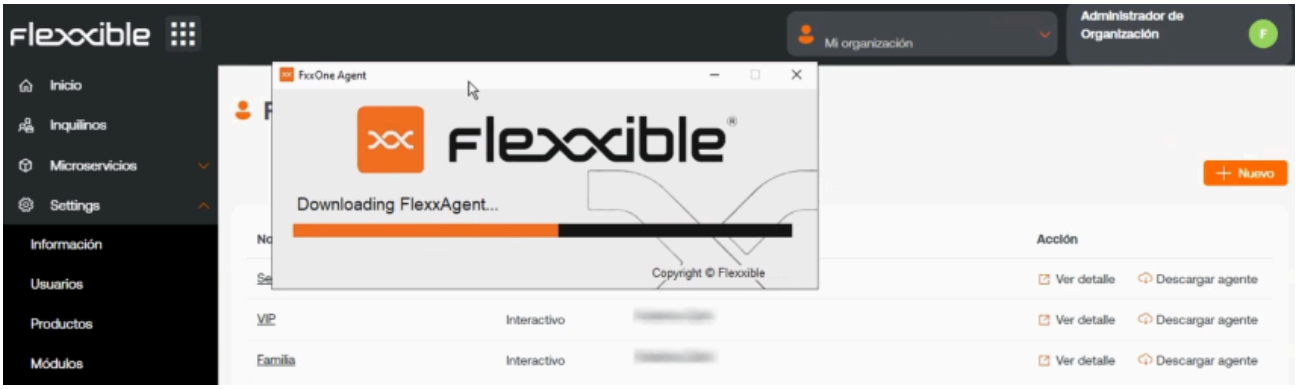
> **The downloaded file is an export of the content of this website for the selected version as of the version's publication date. It is recommended to periodically check for new versions on this page.**

Copyright © 2024 Flexxible. Todos los derechos reservados.

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).

Copyright © 2024 Flexxible. Todos los derechos reservados.

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	✅	✅	✅	✅	✅

Copyright © 2024 Flexxible. Todos los derechos reservados.

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

Copyright © 2024 Flexxible. Todos los derechos reservados.

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

Copyright © 2024 Flexxible. Todos los derechos reservados.

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

Copyright © 2024 Flexxible. Todos los derechos reservados.

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
Job	Log of actions performed in the environment	90 days
Notifications	Log of historical notifications generated in the environment	3 months

Copyright © 2024 Flexxible. Todos los derechos reservados.

FlexxAgent / Supported Systems

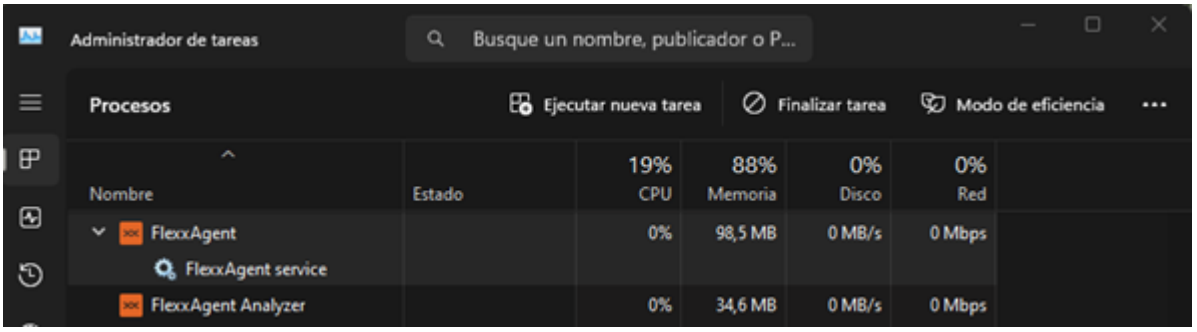
The agent is available in the support cycle for the following operating systems.

- Microsoft Windows
- Linux
- macOS
- ChromeOS
- Android

Copyright © 2024 Flexxible. Todos los derechos reservados.

FlexxAgent / Supported Systems / Windows

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



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

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

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

Consumption

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

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

Copyright © 2024 Flexxible. Todos los derechos reservados.

FlexxAgent Process (system)

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

FlexxAgent Analyzer Process (user)

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

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

Supported versions

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

Microsoft operating systems with full support and compatibility are:

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

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

Copyright © 2024 Flexxible. Todos los derechos reservados.

Software Requirements

FlexxAgent also requires certain software components:

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

Considerations for Windows versions in EOL

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

Limitations

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

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

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

Windows 7 and 2008

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

Copyright © 2024 Flexxible. Todos los derechos reservados.

- The update KB4474419: `SHA-2 code signing support update for Windows Server 2008 R2, Windows 7, and Windows Server 2008: September 23, 2019` must be installed.
- The update KB3140245: `Update to enable TLS 1.1 and TLS 1.2 as default secure protocols in WinHTTP in Windows` must be installed, and follow the instructions in the `How to enable TLS 1.1 and TLS 1.2 as default secure protocols in WinHTTP in Windows` section of the Microsoft support page.
- Requires at least .NET Framework 4.6, but Flexxible recommends installing `.NET Framework 4.8`.
- PowerShell 2.0 with Windows 7 is not compatible with the required TLS 1.2 version to install FlexxAgent. `Windows Management Framework 5.1` is required to be installed, which installs PowerShell 5.1.

Windows 8 and 2012

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

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

Download

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

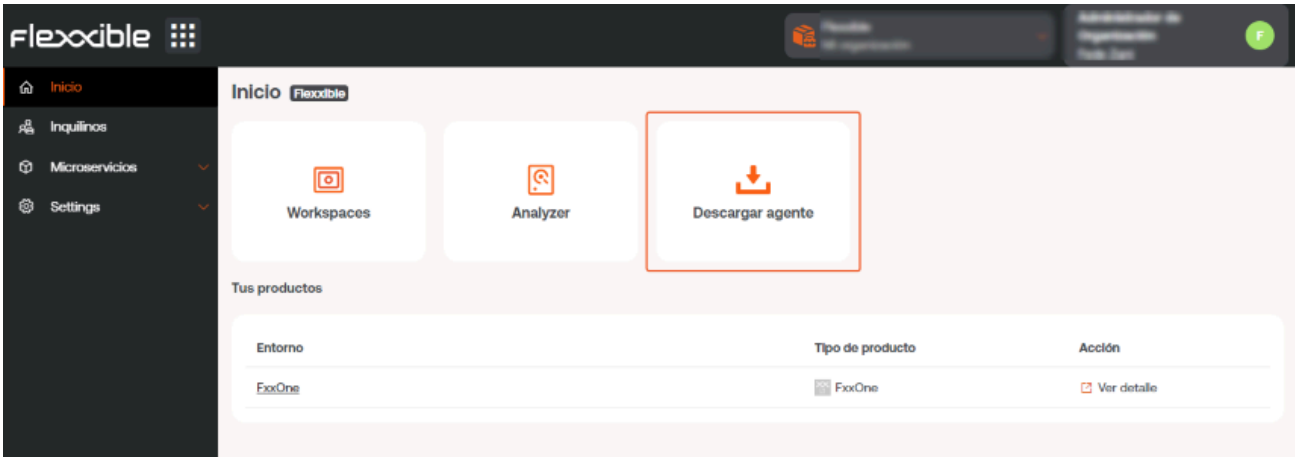
INSTALLATION BINARY DOWNLOAD WITH GRAPHICAL INTERFACE

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

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.

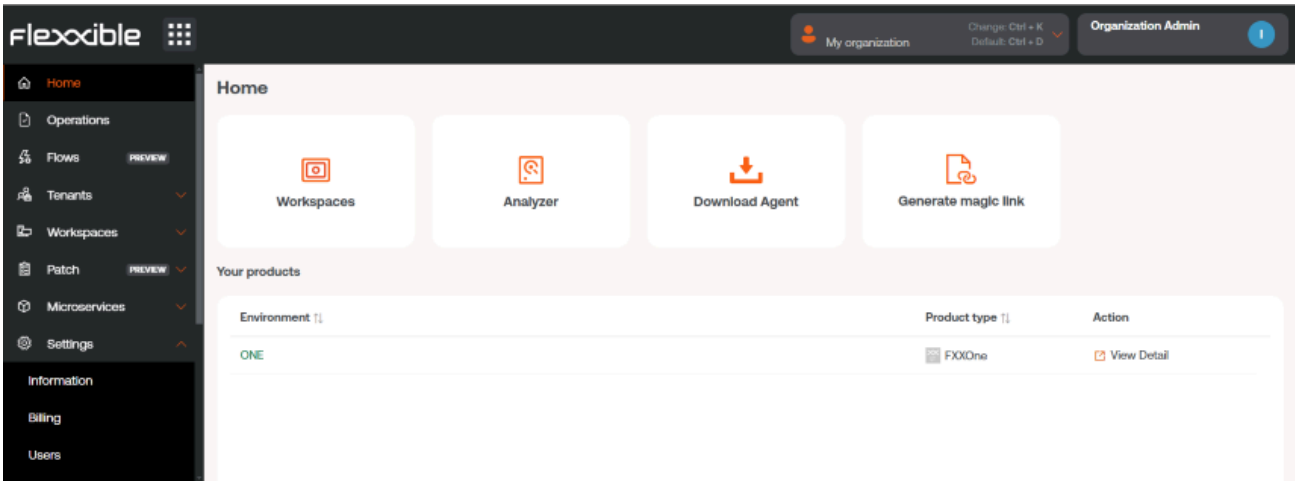
BUTTON TO GENERATE A MAGIC LINK

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.

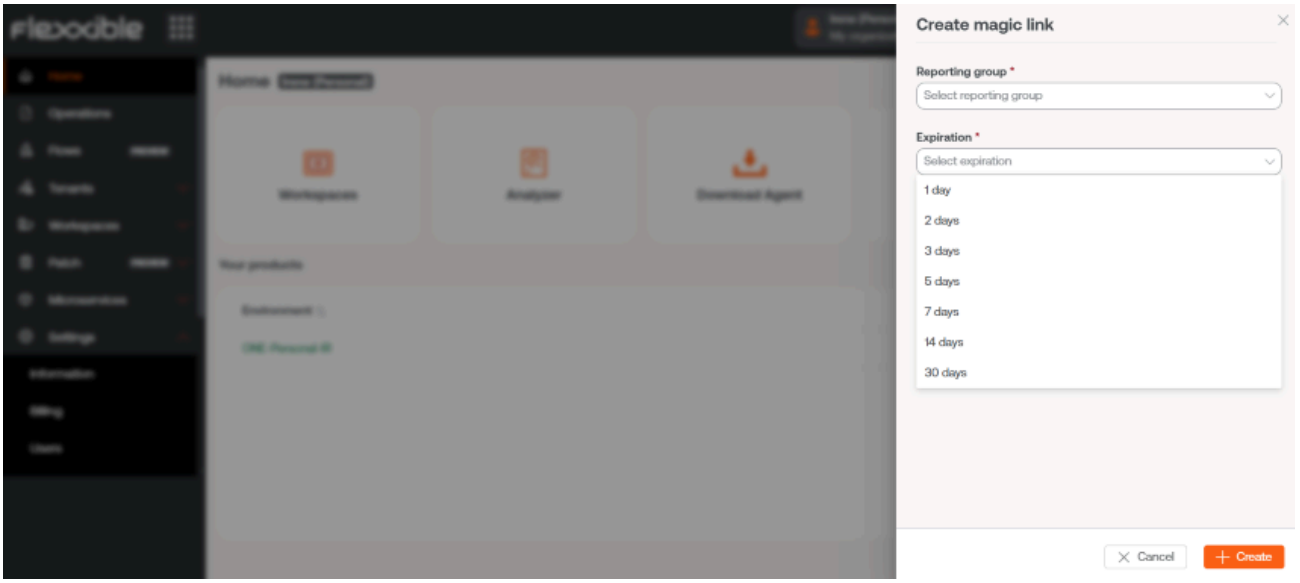
Create magic link

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

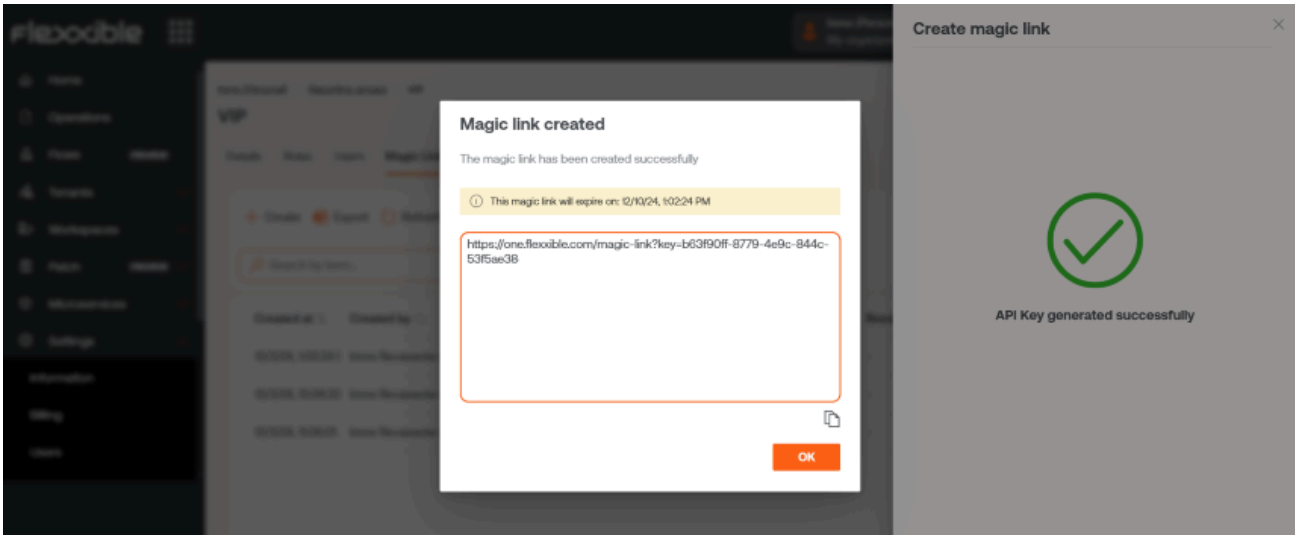


Clicking the button opens a form where you should specify which reporting group the link will be assigned to and for how long it will be active.

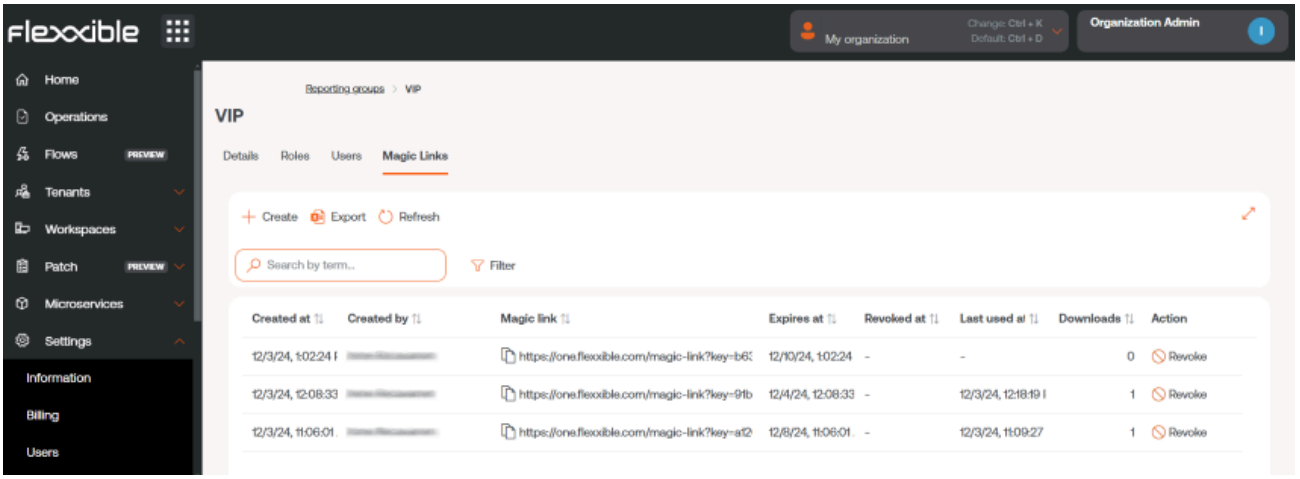


Next, a window will indicate that the link has been created. And it will allow you to copy it directly to share it.

Copyright © 2024 Flexxible. Todos los derechos reservados.



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

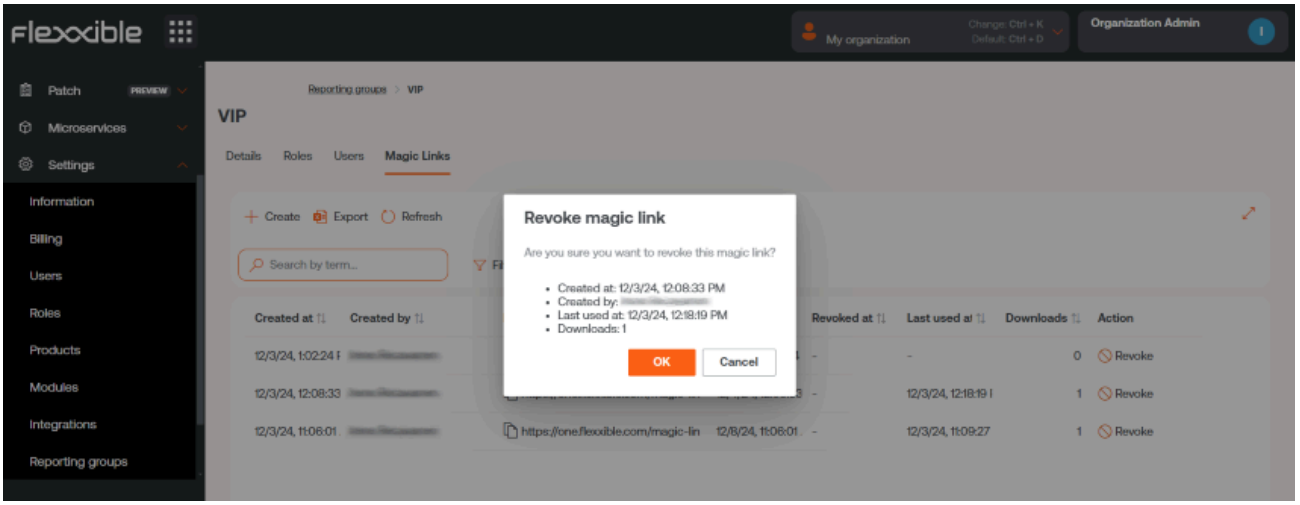
To use the link just copy and paste it into the browser's address bar. At that moment, FlexxAgent will show the following screen, indicating that it has been downloaded on the device.

Copyright © 2024 Flexxible. Todos los derechos reservados.

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."

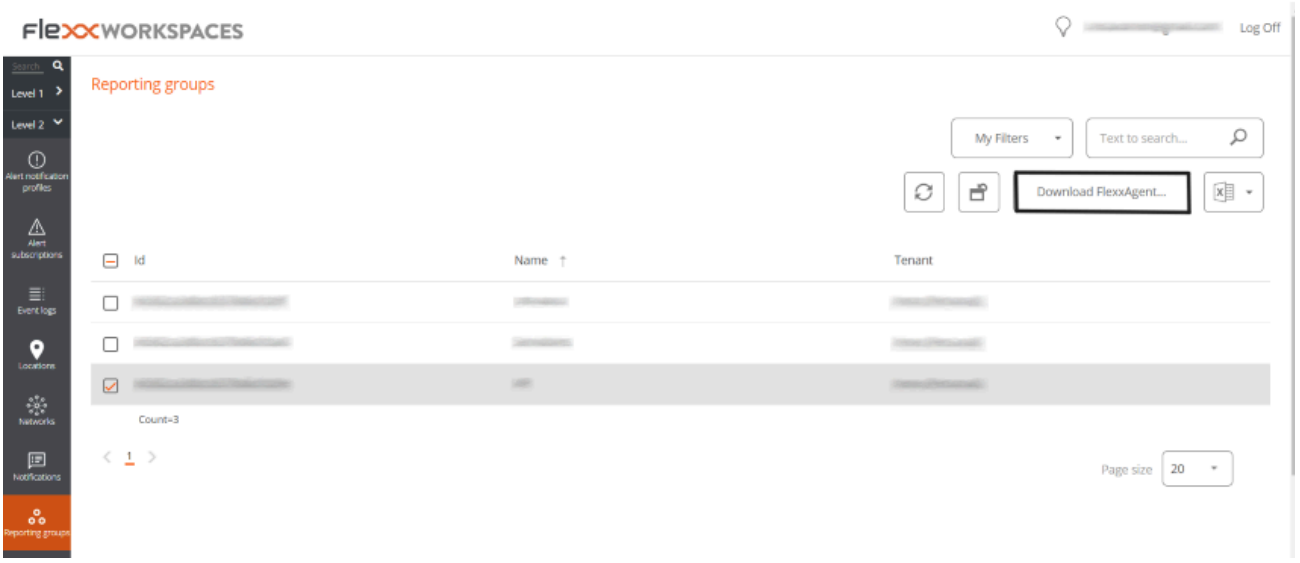
It is not possible to use a `Magic link` that has been revoked or has expired again.

INSTALLATION BINARY DOWNLOAD WITHOUT GRAPHICAL INTERFACE

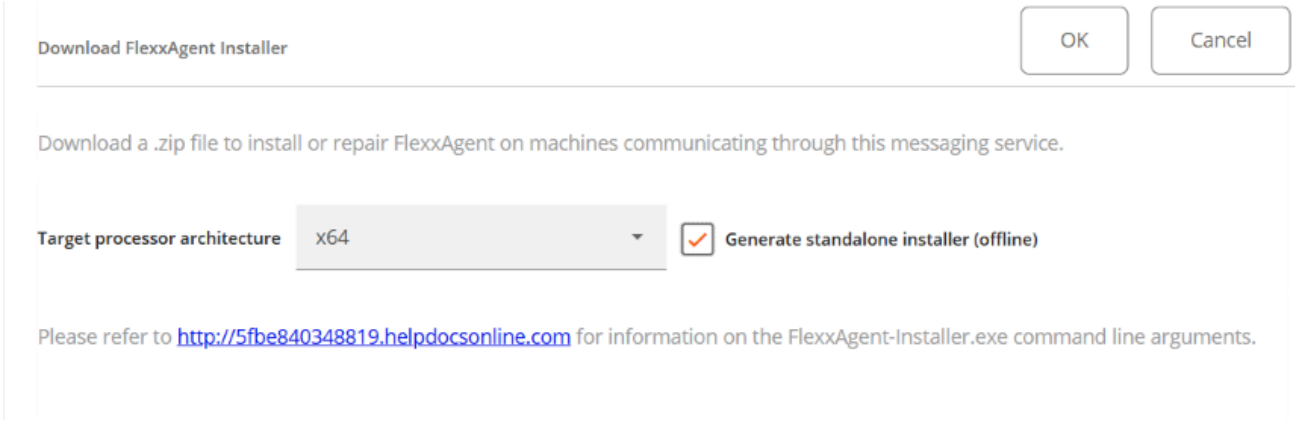
Copyright © 2024 Flexxible. Todos los derechos reservados.

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

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



A window will open to download the FlexxAgent installer.



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

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

Copyright © 2024 Flexxible. Todos los derechos reservados.

Unattended Deployment

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

Installation

The unattended installation of FlexxAgent is done via PowerShell.

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

Uninstall

To uninstall FlexxAgent unattended:

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

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

Files

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

Folders

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

Reinstallation

Copyright © 2024 Flexxible. Todos los derechos reservados.

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

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

For example:

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

Uninstallation Protection

This feature allows protecting the uninstallation process of FlexxAgent to prevent a user from uninstalling it from devices. Configuration can be performed at the Product level and at the Reporting Group level.

Considerations

- Only an *Organization Administrator* user can configure it.
- Version 25.4.2 of FlexxAgent must be installed.
- By default, the feature is disabled.

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

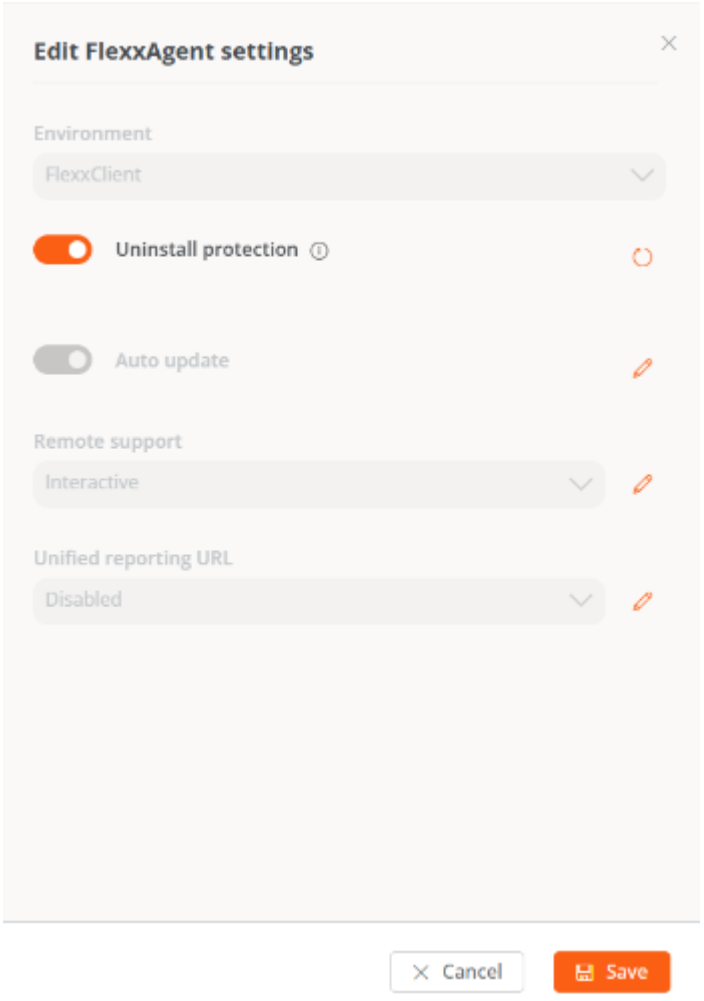
The feature can be executed on one or several reporting groups.

Copyright © 2024 Flexxible. Todos los derechos reservados.

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

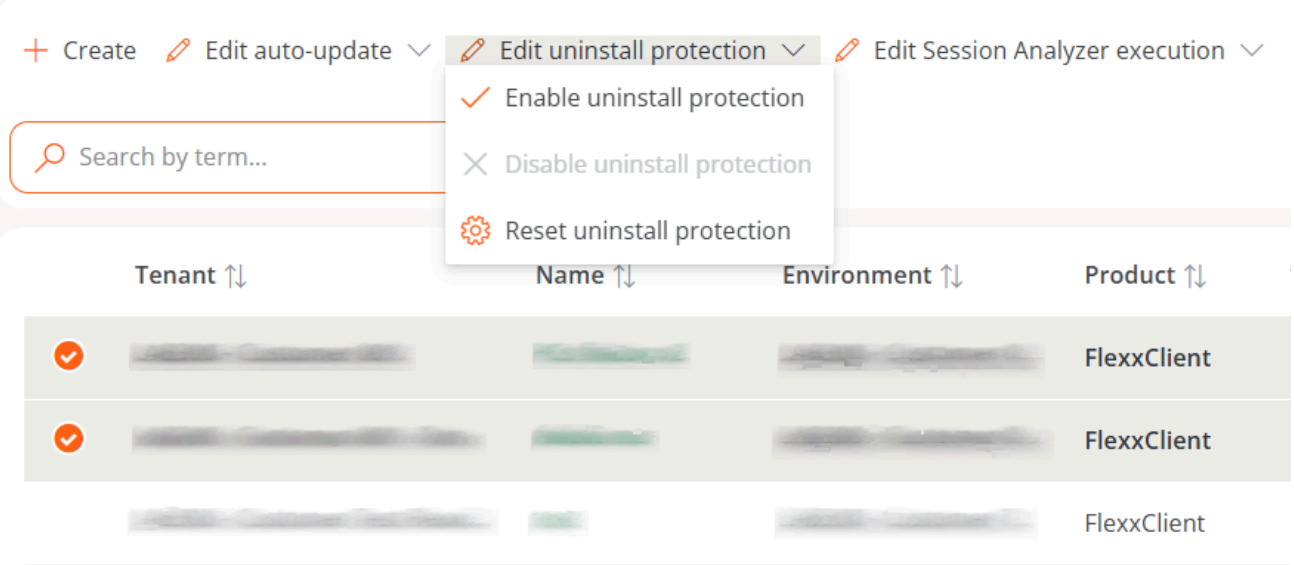


Enable protection for multiple reporting groups

Copyright © 2024 Flexxible. Todos los derechos reservados.

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.

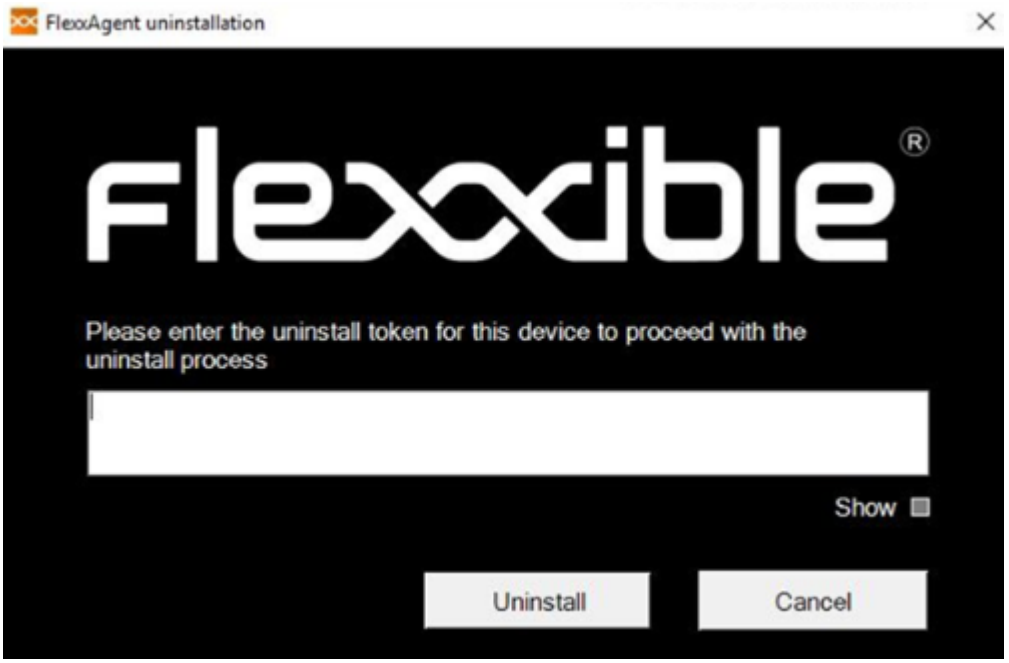
Ways to uninstall FlexxAgent with protection enabled

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

Copyright © 2024 Flexxible. Todos los derechos reservados.

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 uninstallation tasks of FlexxAgent on devices.

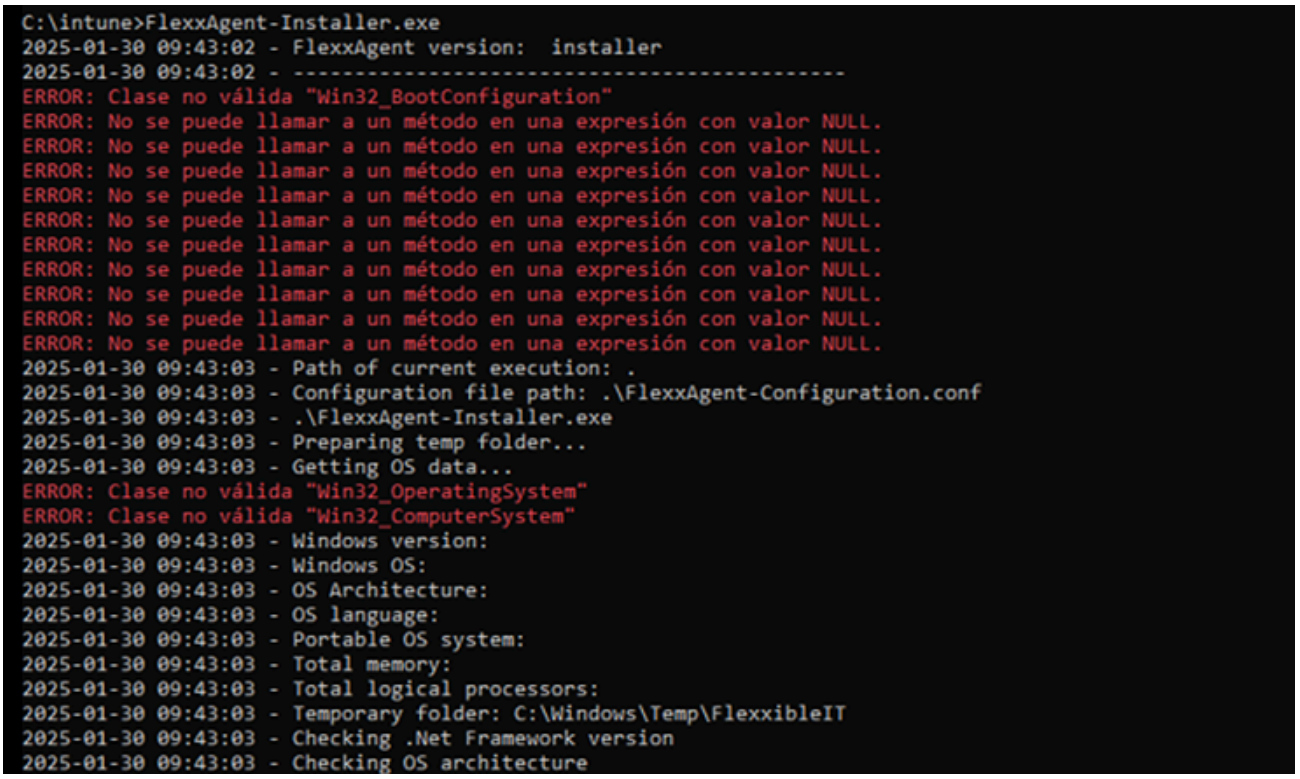
Known Issues

FlexxAgent installation

Issue 1 - Windows Management Instrumentation (WMI)

Copyright © 2024 Flexxible. Todos los derechos reservados.

During the installation and/or reinstallation of FlexxAgent, if the computer encounters issues generated by the Windows Management Instrumentation (WMI) service, the process might 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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

Solution

Exclude the following files from the device:

`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 FlexxAgent from being reinstalled.

Solution

Run the following command as administrator in the CMD window:

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

Then, restart the device.

Supported Parameters

Parameter	Type	Caption	
proxyAbsoluteUri	[string]	Proxy URL and port.	
proxyUser	[string]	User for authenticated proxy.	
proxyPass	[string]	Password for authenticated proxy.	
proxyPersistConfig	[switch]	If specified, the configuration is persisted in the registry.	

Copyright © 2024 Flexxible. Todos los derechos reservados.

Parameter	Type	Caption	
configFilePath	[string]	Alternative directory for the FlexxAgent-Configuration.conf file.	
DebugMode	[switch]	When specified, creates a text file in the same folder with the script execution transcription.	
RepairAgent	[bool]	Removes the preexisting configuration of FlexxAgent when it is reinstalled on a device.	
Help	[switch]	Lists the supported parameters, with type and description.	

Proxy Configuration

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

Proxy configuration through command line

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

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

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

Copyright © 2024 Flexxible. Todos los derechos reservados.

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

Configuration through registry keys

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

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

Registry keys related to the proxy configuration:

- Key Proxy_URL
- Key Proxy_User
- Key Proxy_Pwd

Key Proxy_URL

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

Key Proxy_User

- Key path: `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Flexxible\FlexxAgent\Communications`
- Key Name: Proxy_User
- Key type: REG_SZ

Copyright © 2024 Flexxible. Todos los derechos reservados.

- Supported values: the username to authenticate to the proxy; for example 'Administrator'. It can be bypassed for unauthenticated proxies.

Key Proxy_Pwd

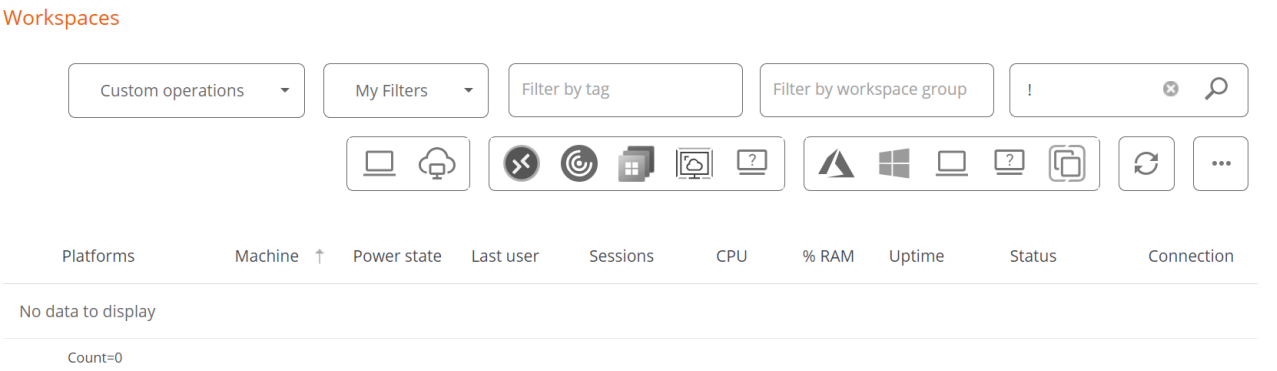
- Key path: `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Flexxible\FlexxAgent\Communications`
- Key Name: Proxy_Pwd
- Key type: REG_SZ
- Supported values: The password to authenticate to the proxy. It can be bypassed for unauthenticated proxies. The value of the Proxy_Pwd key can be set in plain text (not recommended)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

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

Manual Update

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

Copyright © 2024 Flexxible. Todos los derechos reservados.



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

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

Logs

FlexxAgent can generate three types of logs:

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

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

Installation and update logs

Copyright © 2024 Flexxible. Todos los derechos reservados.

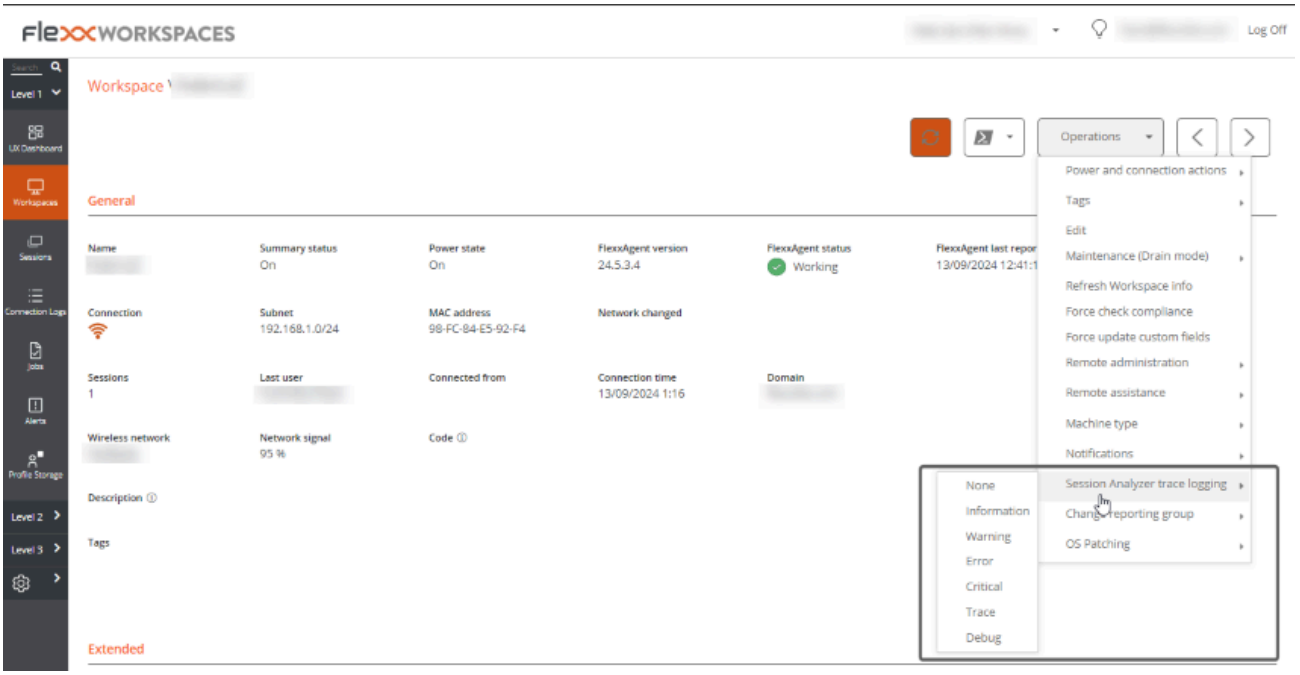
Inside the `%LOCALAPPDATA%\Flexxible` folder, a text log is left containing information about the installation or update process, as well as dependency information and process details.

FlexxAgent Analyzer logs

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

Change log level for FlexxAgent Analyzer

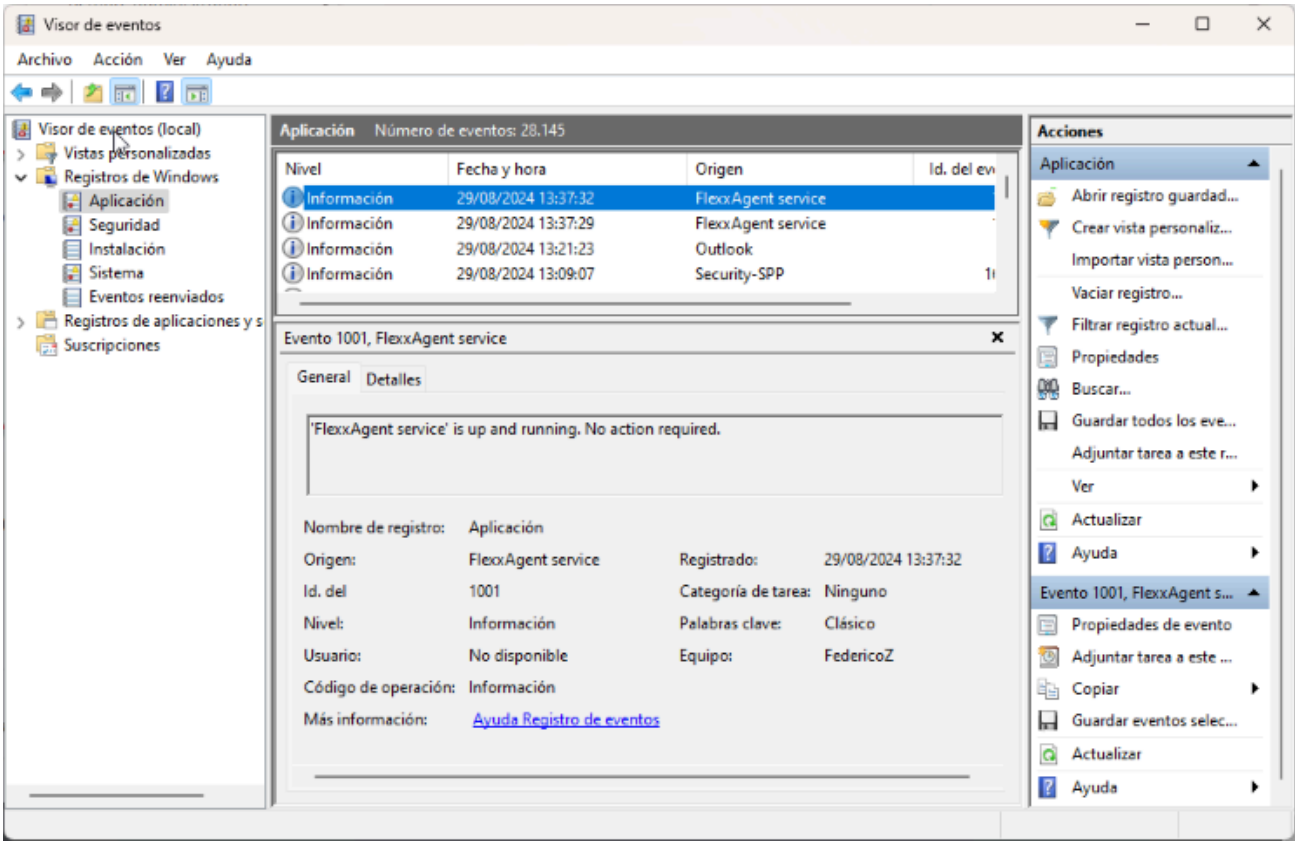
From Workspaces, it is possible to change the log level for one or more devices through the options available in the `Operations` button.



FlexxAgent service logs

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

Copyright © 2024 Flexxible. Todos los derechos reservados.



Information obtained from the device

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

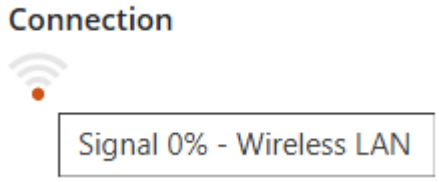
General information

- **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*.

Copyright © 2024 Flexxible. Todos los derechos reservados.

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

Copyright © 2024 Flexxible. Todos los derechos reservados.

- **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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

- **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

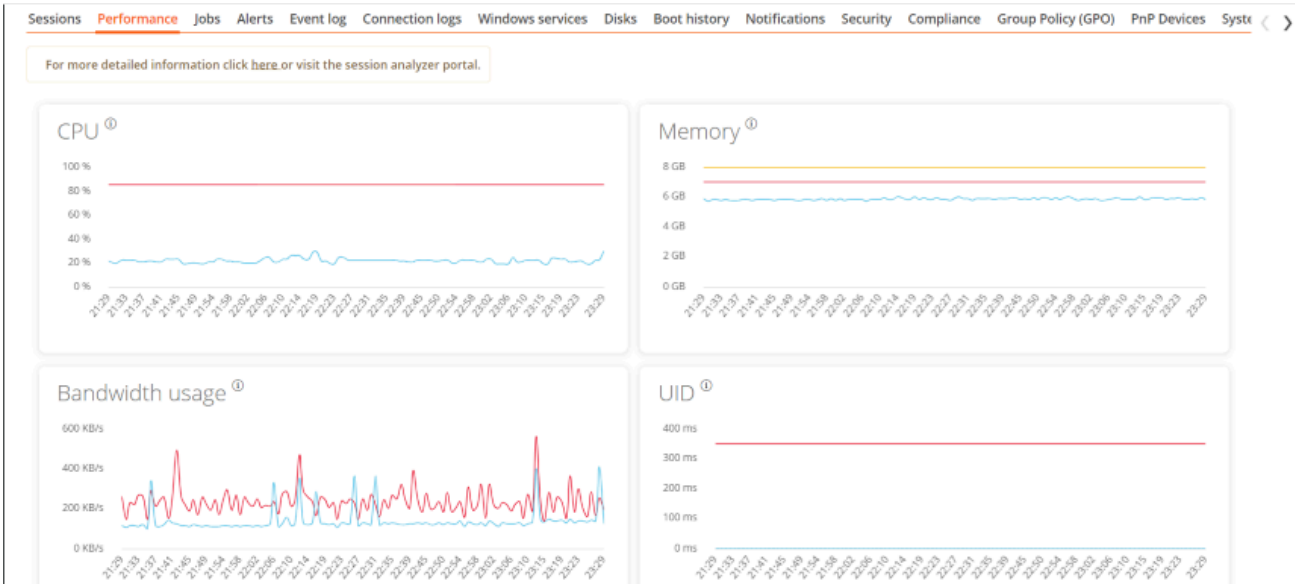
FlexxAgent groups information about the following aspects of the device:

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

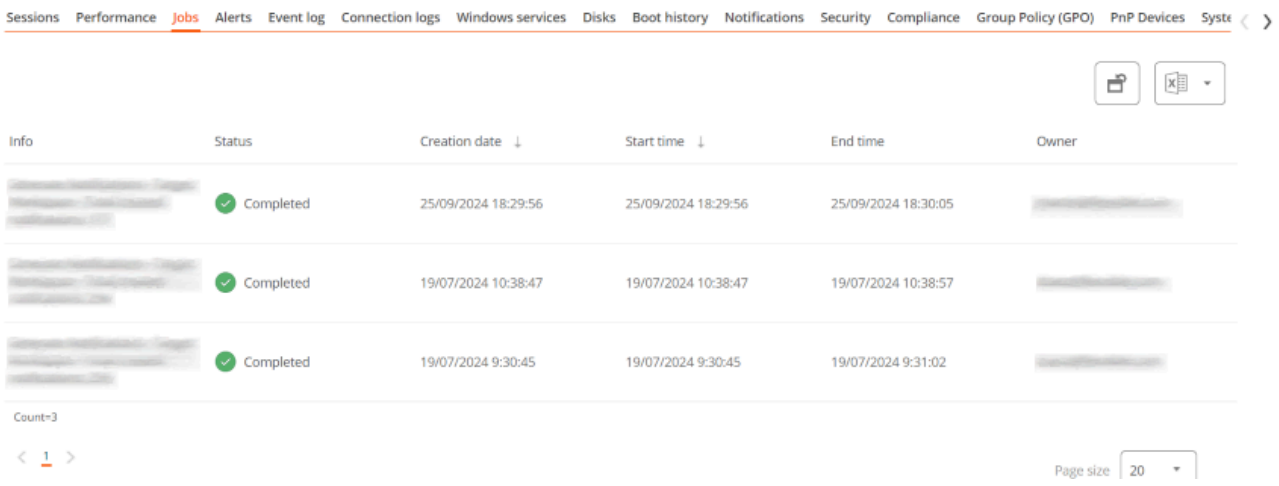
Copyright © 2024 Flexxible. Todos los derechos reservados.

- **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.

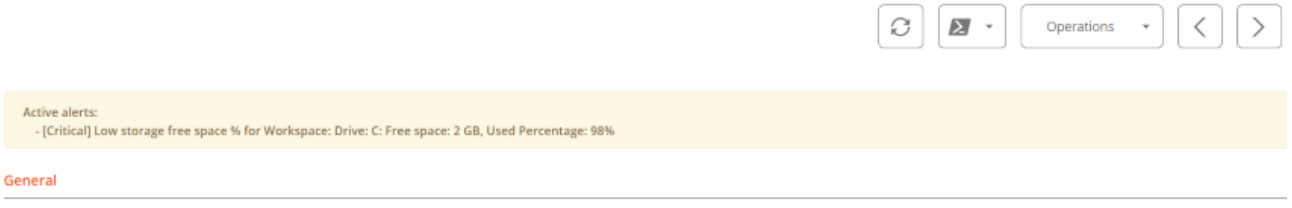
Job

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

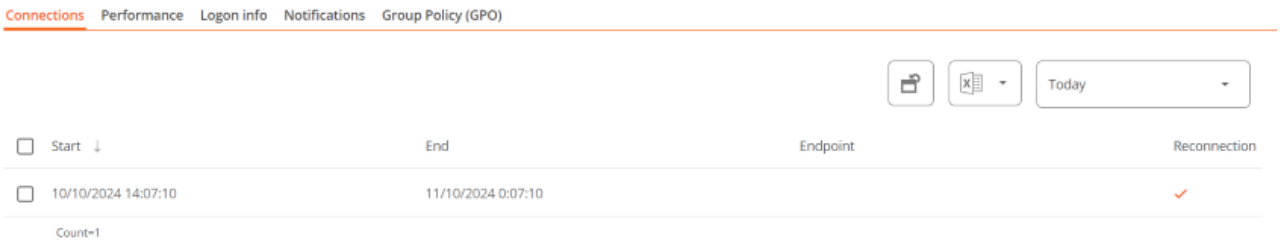
Copyright © 2024 Flexxible. Todos los derechos reservados.

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

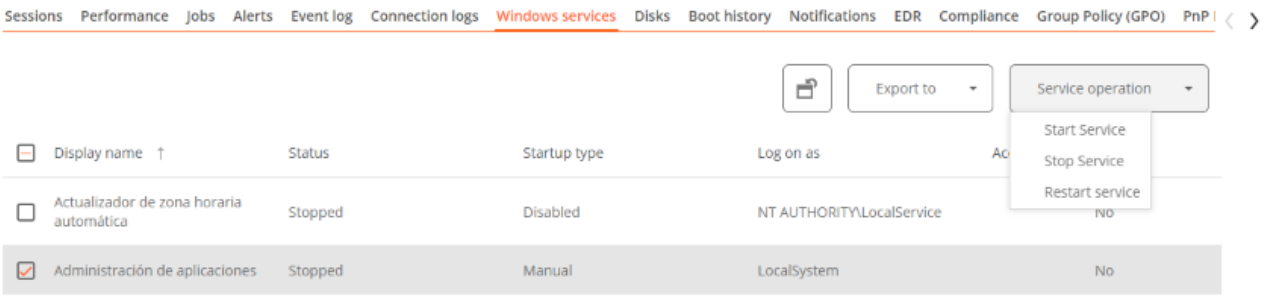
Presents a list of the connections established with the device, including each instance where a user logs in or reconnects a previously disconnected session.



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

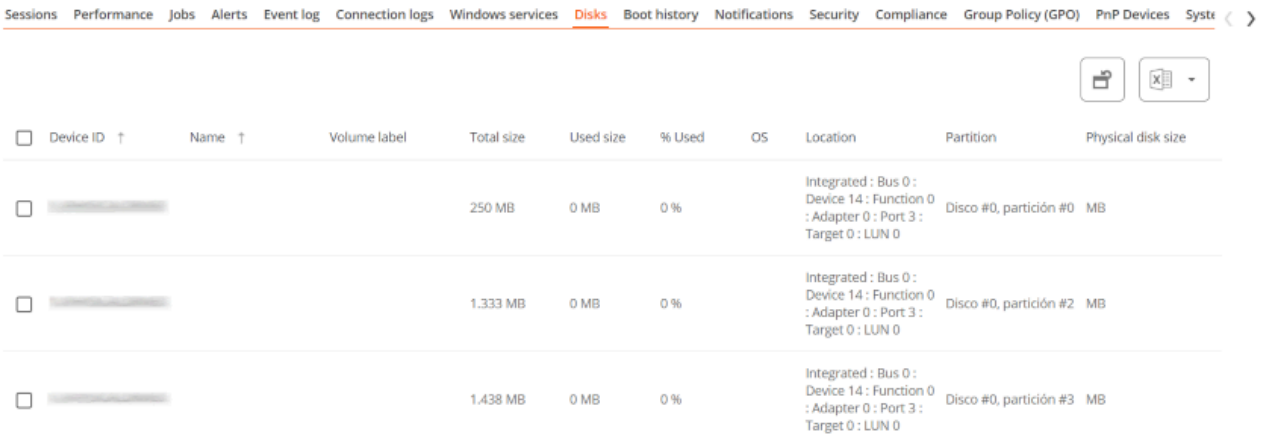
This option displays the status of services and performs start, restart, or stop operations on Windows services.



Disks

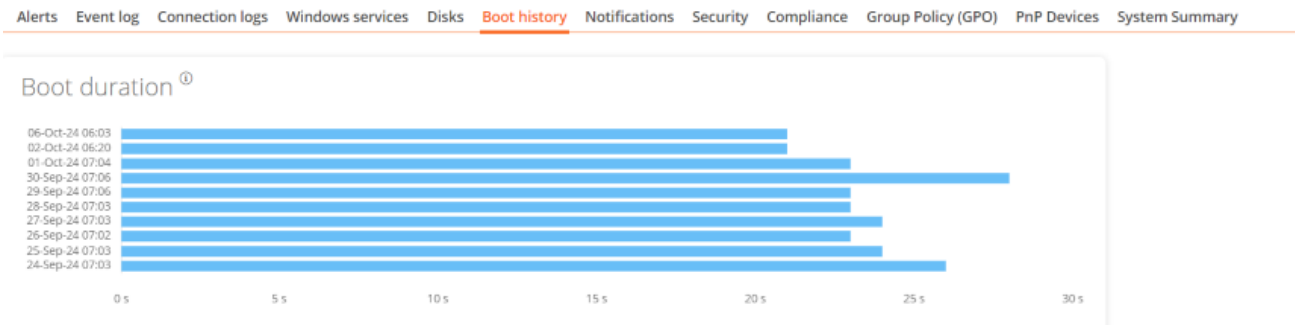
Displays a list of all partitions present on the disks identified in the system, as well as statistics of their capacity and occupancy levels.

Copyright © 2024 Flexxible. Todos los derechos reservados.



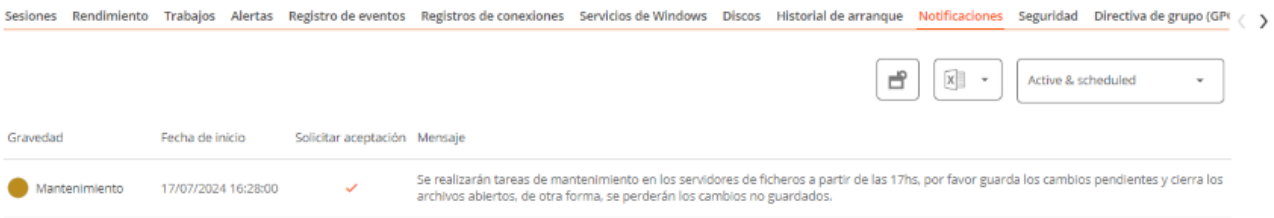
Boot history

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.

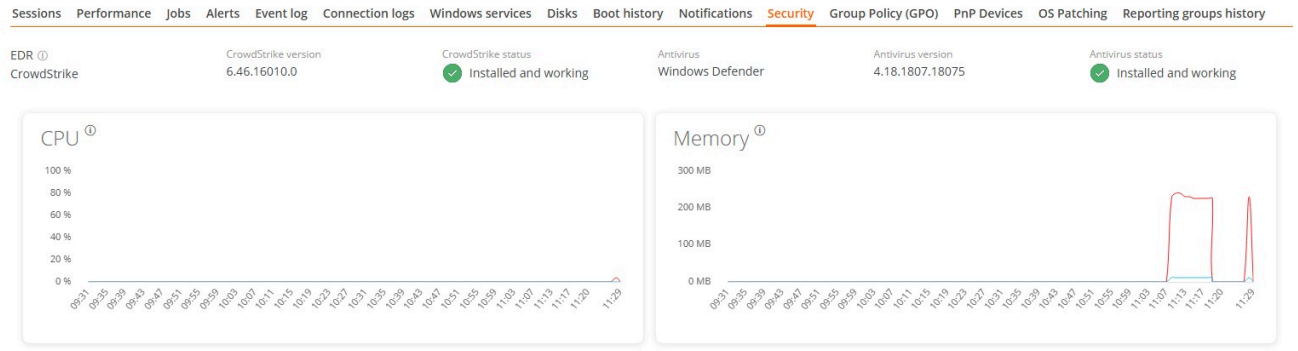


Security

From this section, you can 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

Copyright © 2024 Flexxible. Todos los derechos reservados.

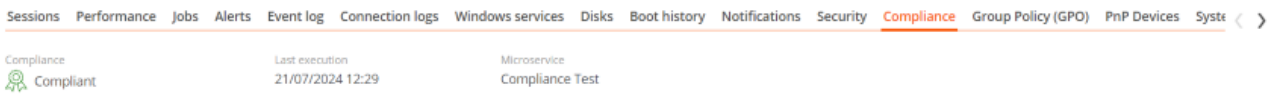
information will be shown if FlexxAgent detects CrowdStrike as Endpoint Detection and Response (EDR).



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

Compliance

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



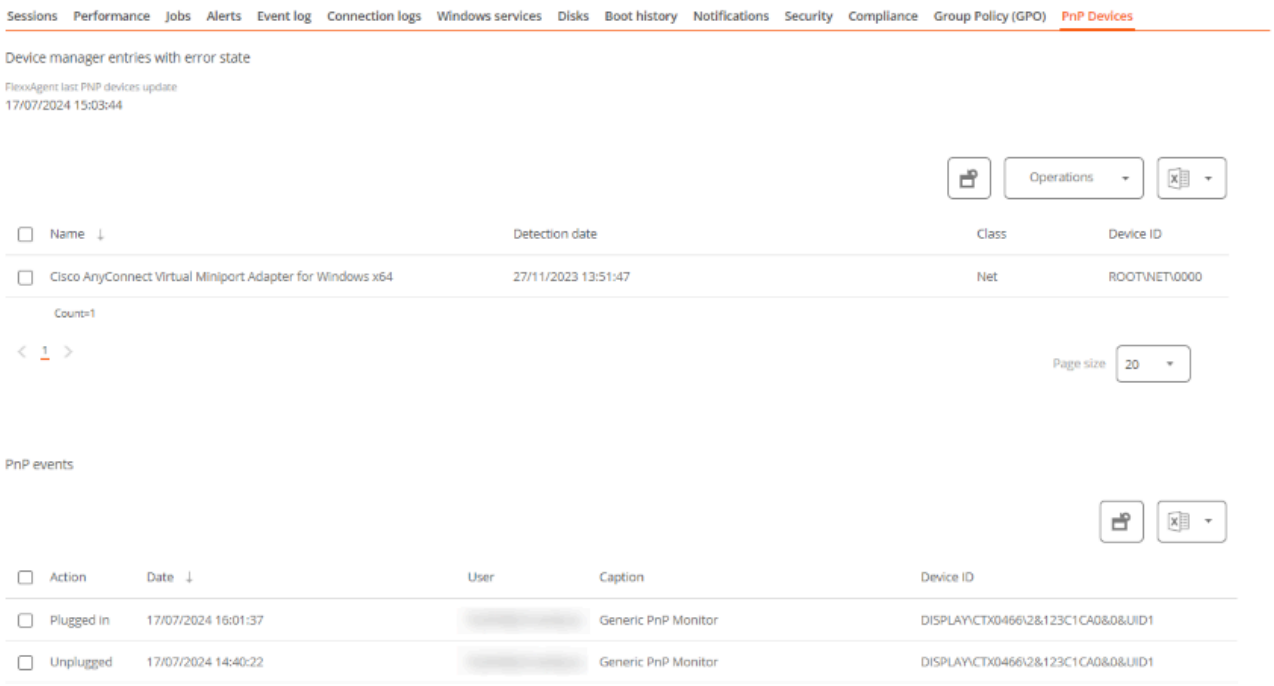
Group Policy (GPO)

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.



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"
SystemModel	Product name given by a manufacturer to a piece of equipment

Copyright © 2024 Flexxible. Todos los derechos reservados.

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

Copyright © 2024 Flexxible. Todos los derechos reservados.

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

Reporting groups history

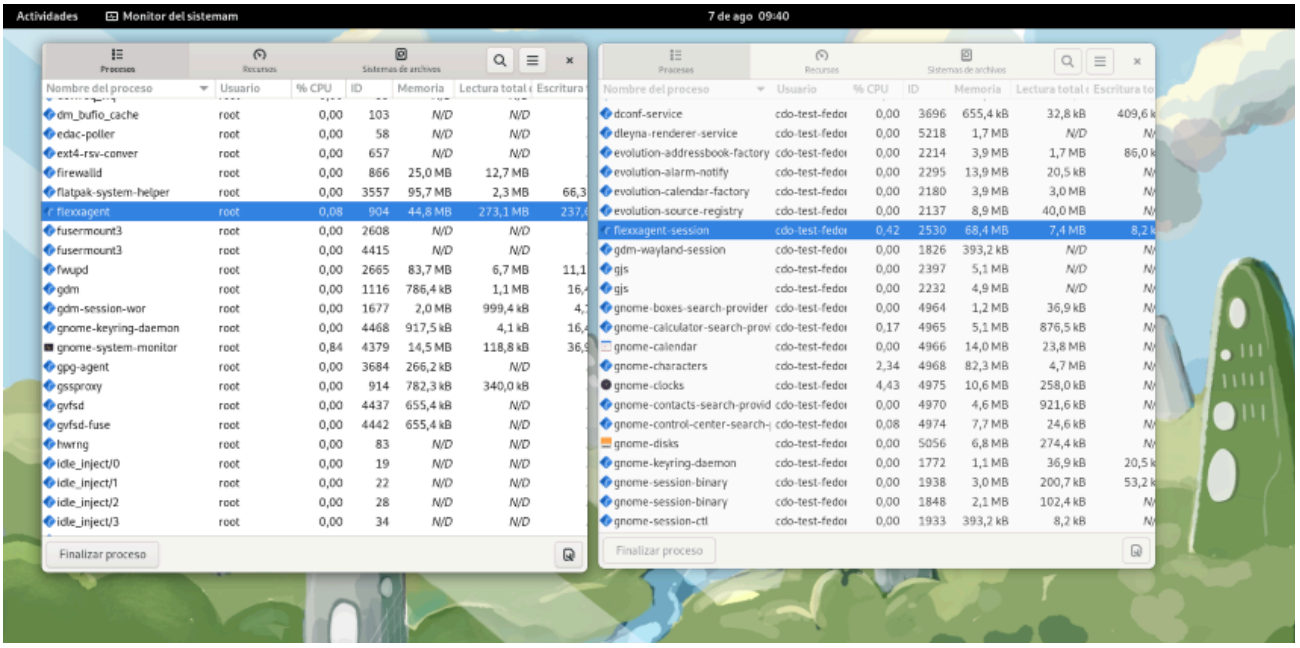
Allows you to see which reporting groups the device belongs to, the date of incorporation, and if it has been assigned to the group manually or automatically.

Copyright © 2024 Flexxible. Todos los derechos reservados.

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.

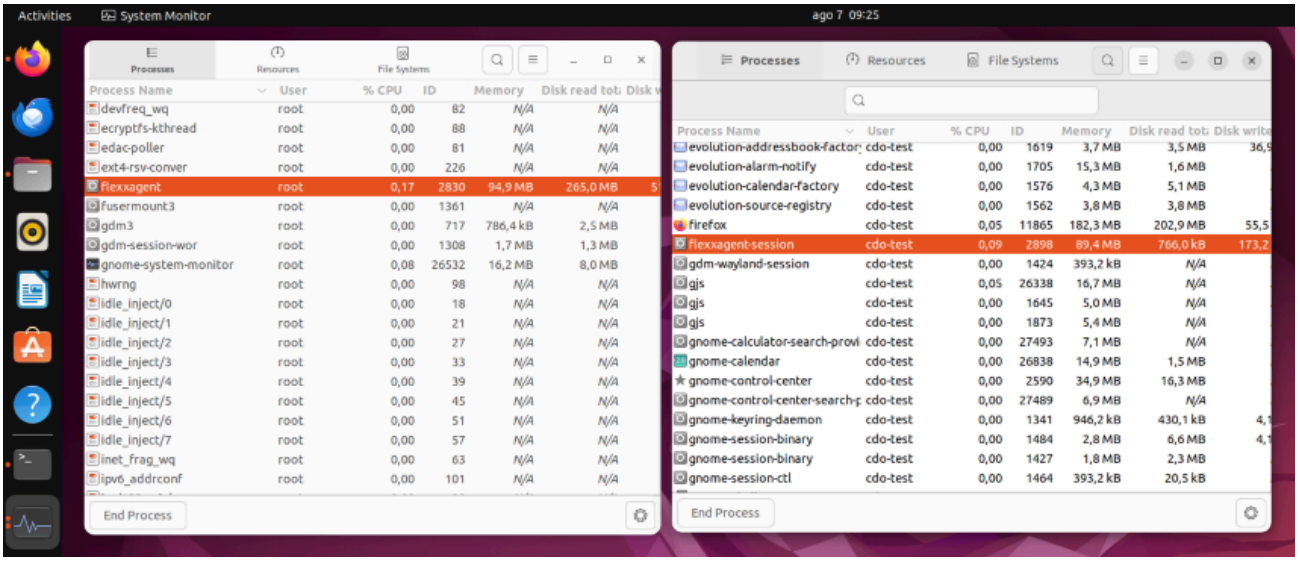
Linux support includes distributions like Fedora, Debian, and its derivative, Ubuntu. Both physical and virtual devices on VMware as a hypervisor and VDIs published with Citrix as a broker are supported.



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.

Copyright © 2024 Flexxible. Todos los derechos reservados.



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

Copyright © 2024 Flexxible. Todos los derechos reservados.

Limitations

Certain functionalities are not available for Linux, such as remote assistance, user microservices, or workflow execution, 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`

Copyright © 2024 Flexxible. Todos los derechos reservados.

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`.

Copyright © 2024 Flexxible. Todos los derechos reservados.

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`

Copyright © 2024 Flexxible. Todos los derechos reservados.

> Fedora: `flexxagent.rpm`

Offline installation steps

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

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

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

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

4. Clean the files used.

Uninstall

The uninstallation script can be downloaded from

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

Steps for uninstallation:

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

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

3. Run the script.

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

Copyright © 2024 Flexxible. Todos los derechos reservados.

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:

Copyright © 2024 Flexxible. Todos los derechos reservados.

- 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

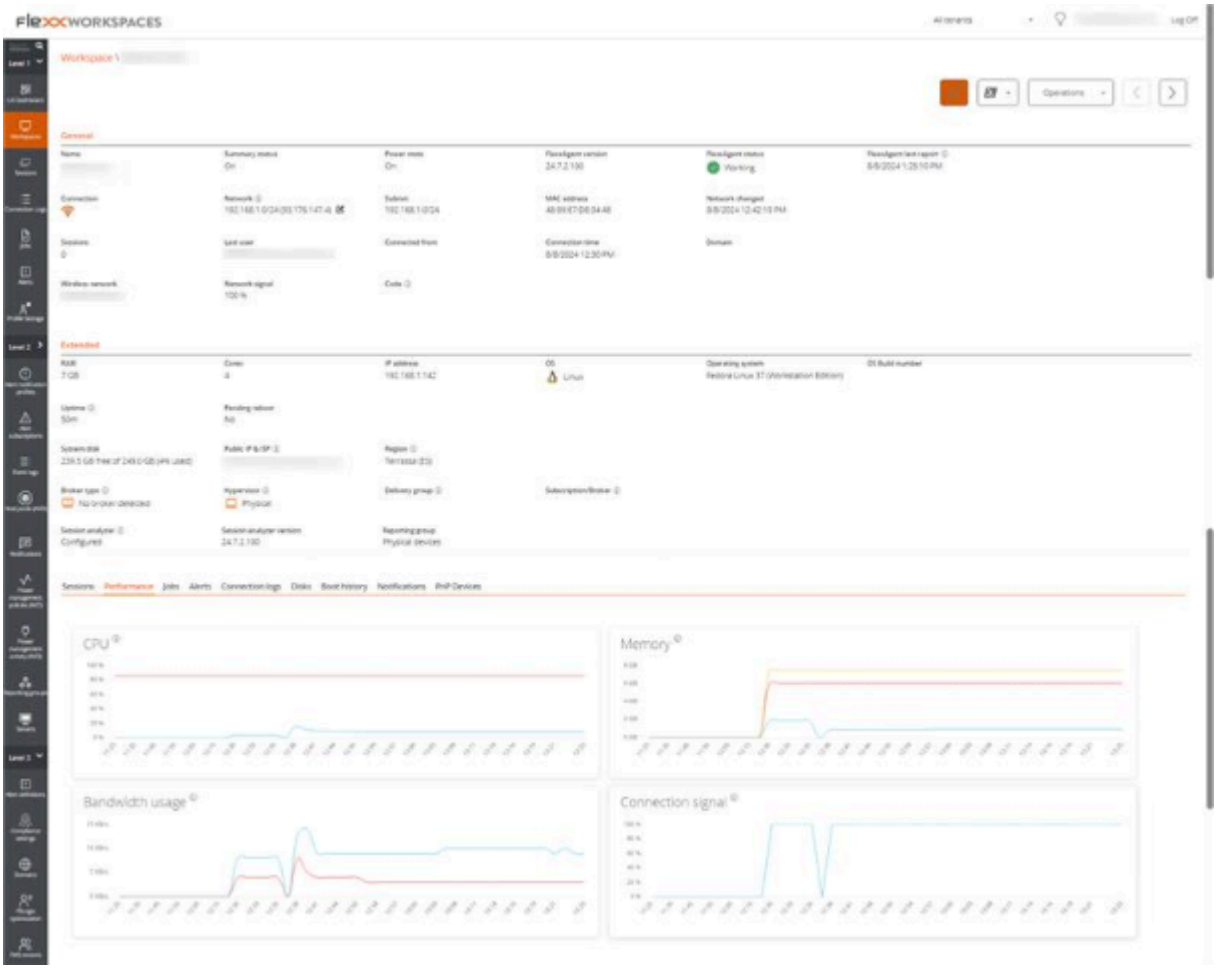
FlexxAgent can generate two types of logs:

- 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.

Copyright © 2024 Flexxible. Todos los derechos reservados.



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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

- **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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

- **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.

Job

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

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.

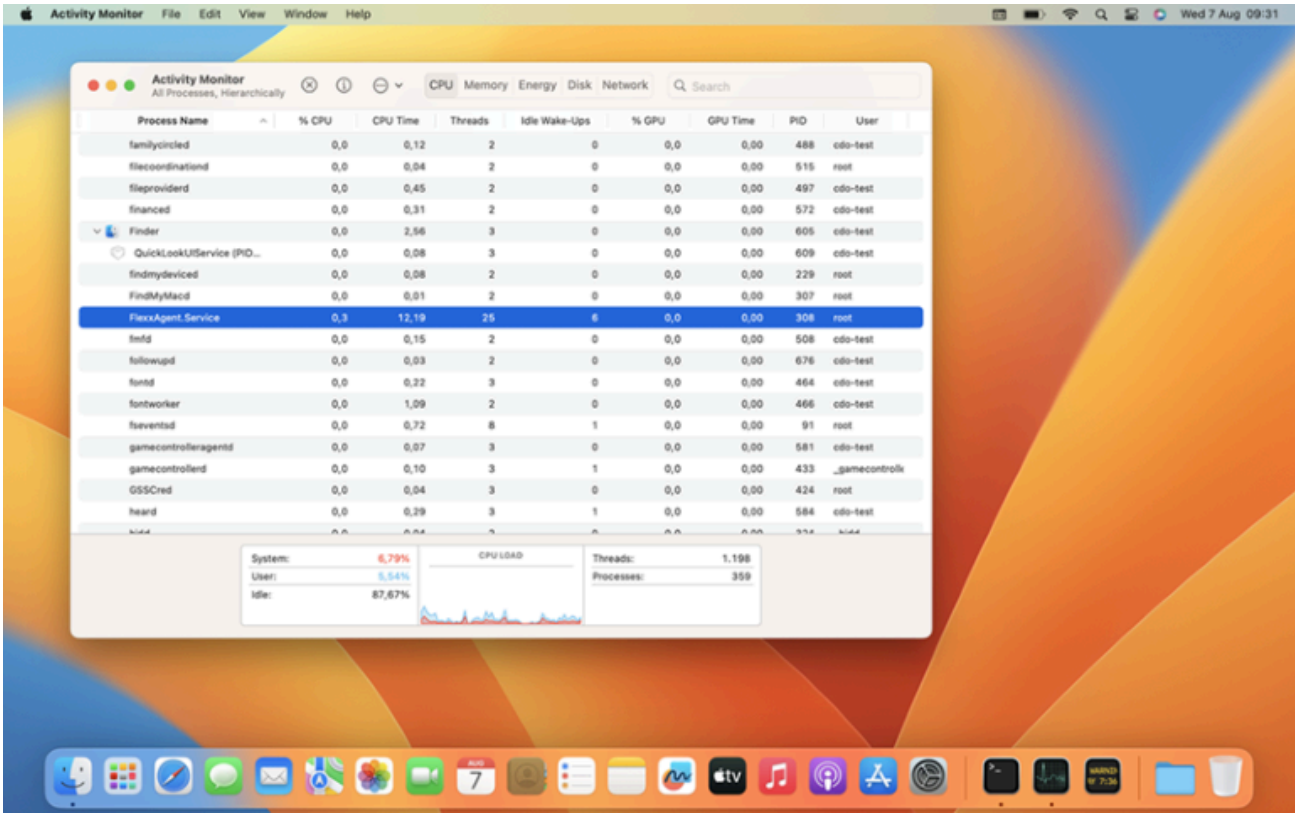
Reporting groups history

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

FlexxAgent / Supported Systems / macOS

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



Supported versions

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

Limitations

Certain features are not available for macOS, like remote assistance, on-demand microservices execution from Workspaces, user and flow microservices, and notifications.

Copyright © 2024 Flexxible. Todos los derechos reservados.

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

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:

Copyright © 2024 Flexxible. Todos los derechos reservados.

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

Install a specific version of FlexxAgent:

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

Access the help:

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

Offline installation

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

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

Offline installation steps

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

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

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

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

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

Copyright © 2024 Flexxible. Todos los derechos reservados.

> `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]`

Copyright © 2024 Flexxible. Todos los derechos reservados.

Access the help:

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

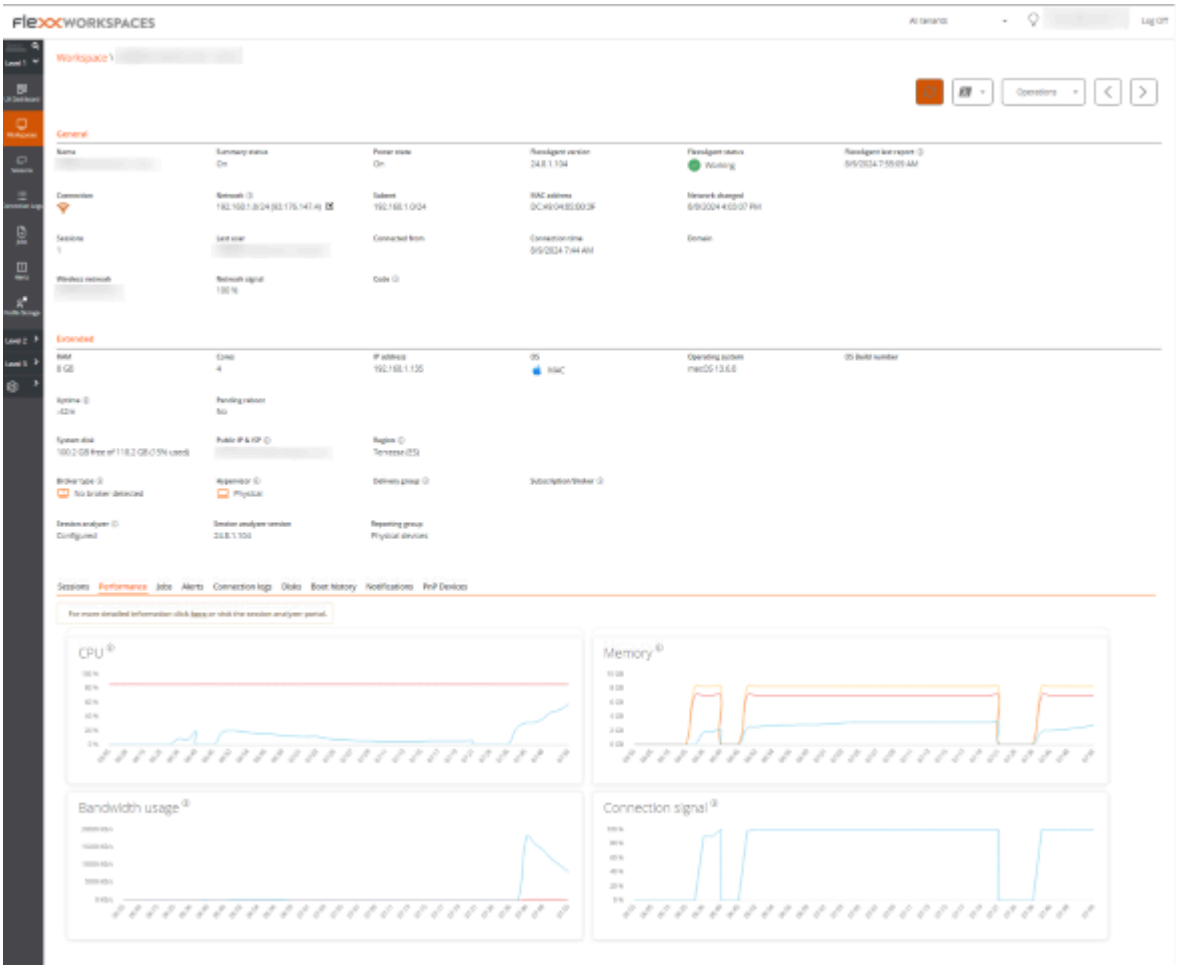
Update

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.



Copyright © 2024 Flexxible. Todos los derechos reservados.

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

Copyright © 2024 Flexxible. Todos los derechos reservados.

- **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.

Job

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

FlexxAgent / Supported Systems / ChromeOS

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

Requirements

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

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

Supported versions

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

Limitations

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

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

Download and installation

Copyright © 2024 Flexxible. Todos los derechos reservados.

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`.

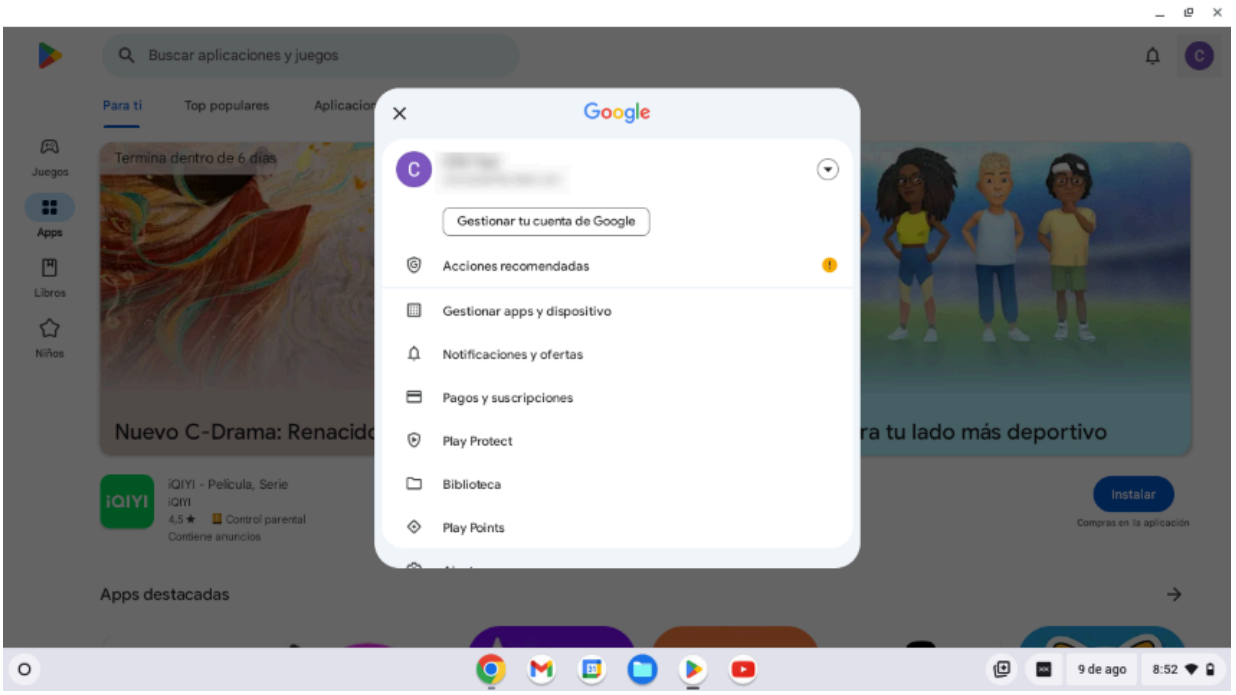
Please review the MDM documentation on how to deploy Google Play applications for managed users.

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

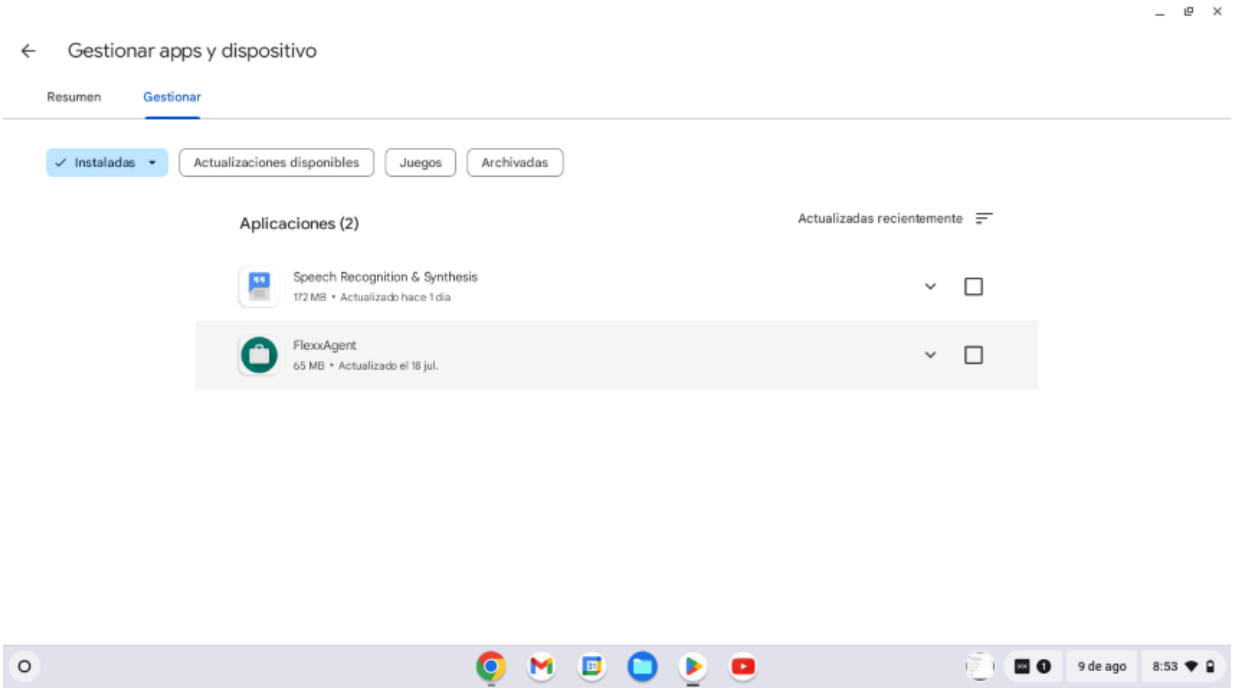
To ensure FlexxAgent configuration applies correctly, the app must be manually opened on each device at least once after installation. It is recommended to follow these steps:

Copyright © 2024 Flexxible. Todos los derechos reservados.

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

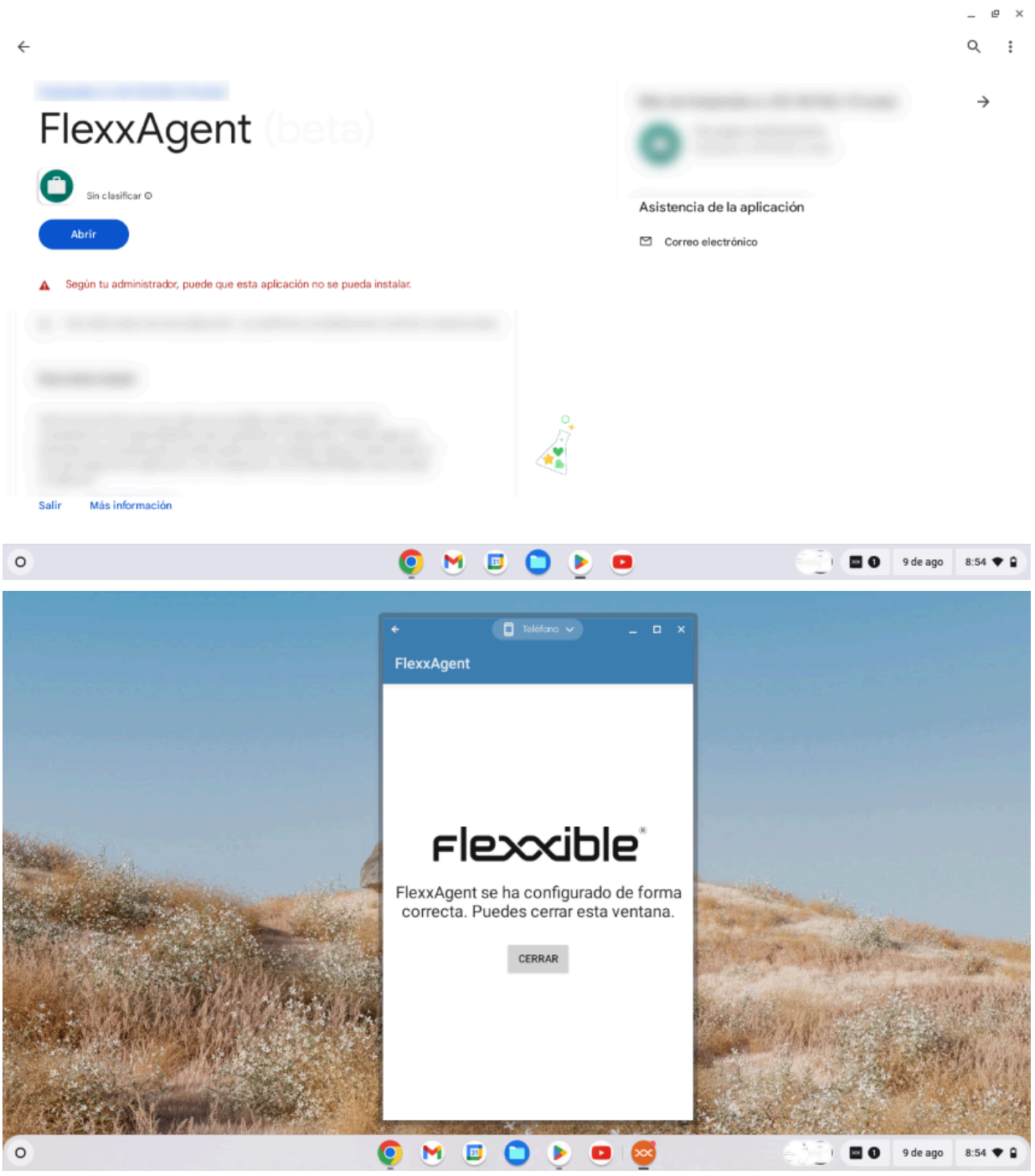


2. Go to the `Manage` tab and click on the FlexxAgent application.



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

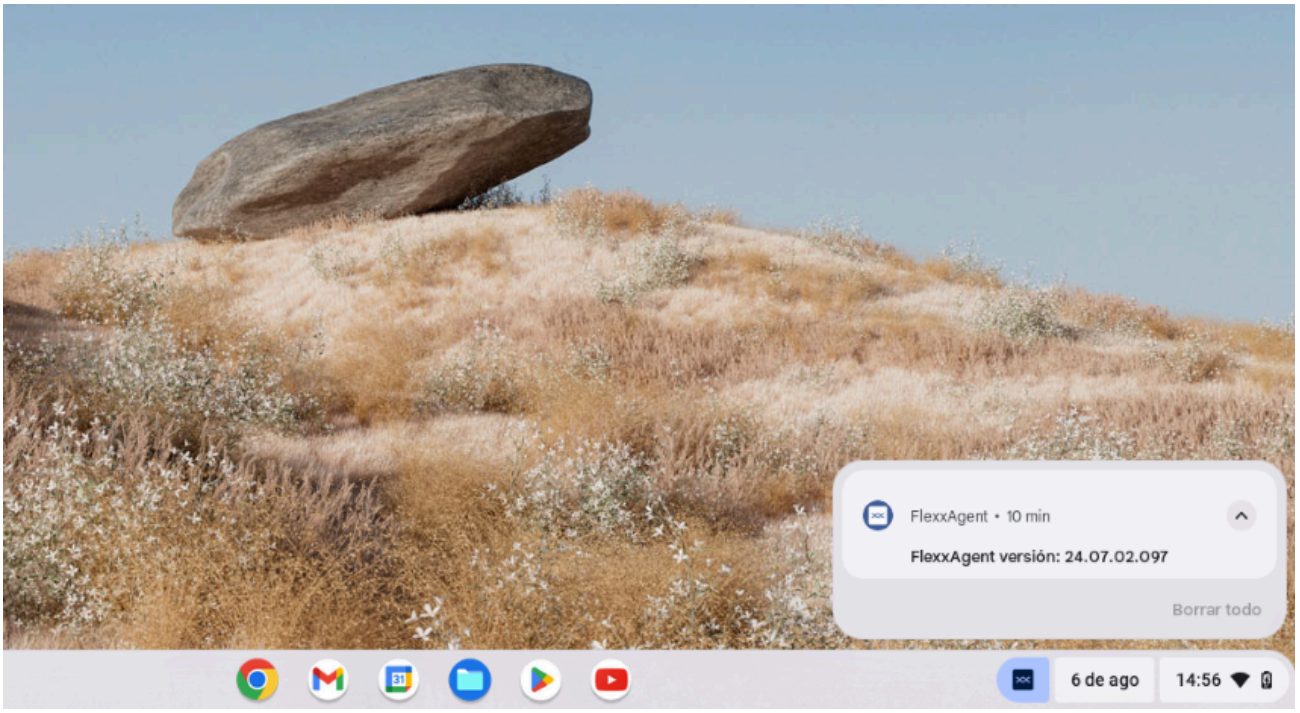
Copyright © 2024 Flexxible. Todos los derechos reservados.



4. Close the window.

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

Copyright © 2024 Flexxible. Todos los derechos reservados.



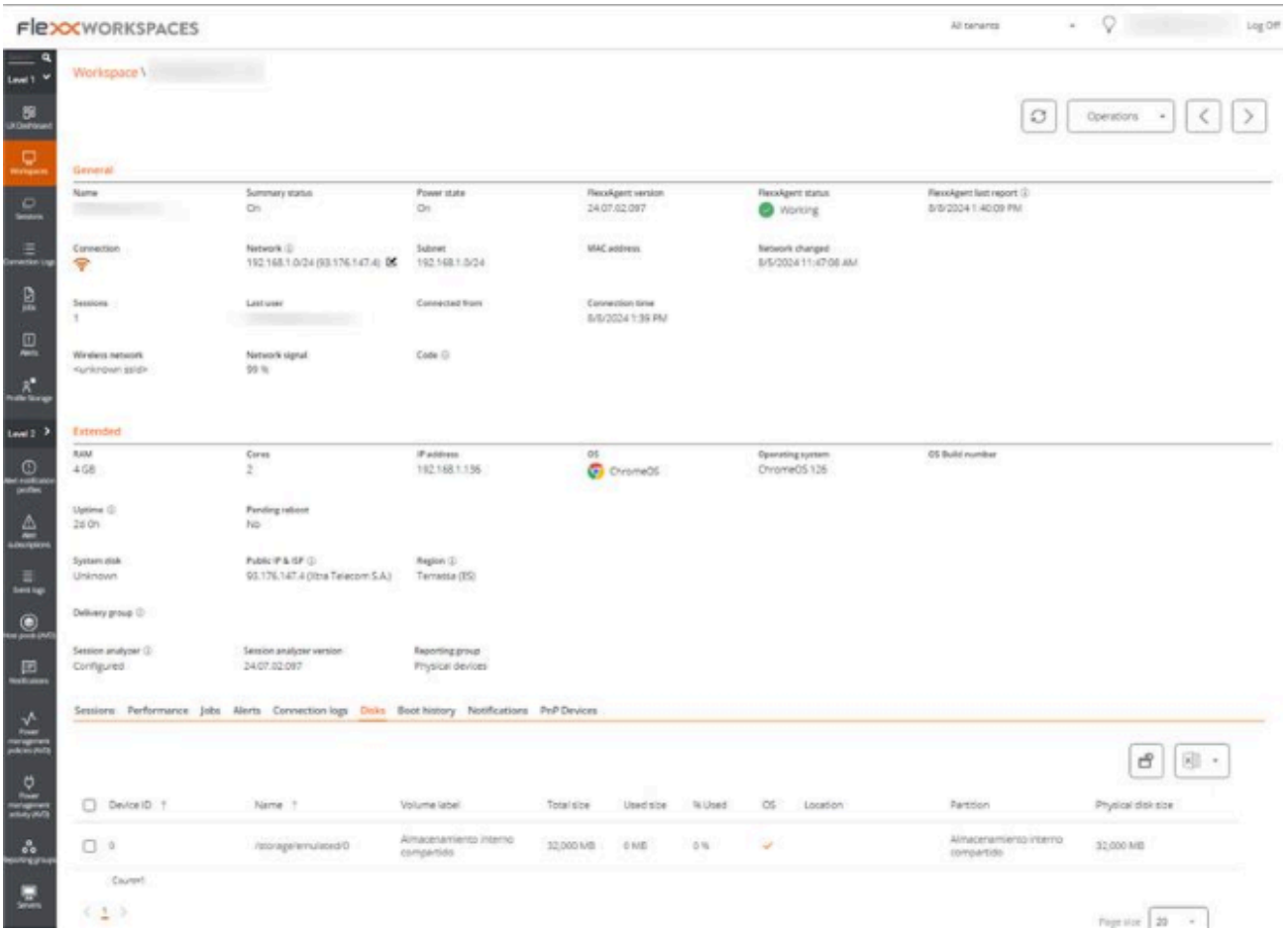
Update

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.



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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

- **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

Copyright © 2024 Flexxible. Todos los derechos reservados.

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.

Job

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

Copyright © 2024 Flexxible. Todos los derechos reservados.

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

FlexxAgent / Supported Systems / Android

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

Requirements

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

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

Supported versions

FlexxAgent runs on Android devices version 9.0 or later.

Limitations

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

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

Settings

Copyright © 2024 Flexxible. Todos los derechos reservados.

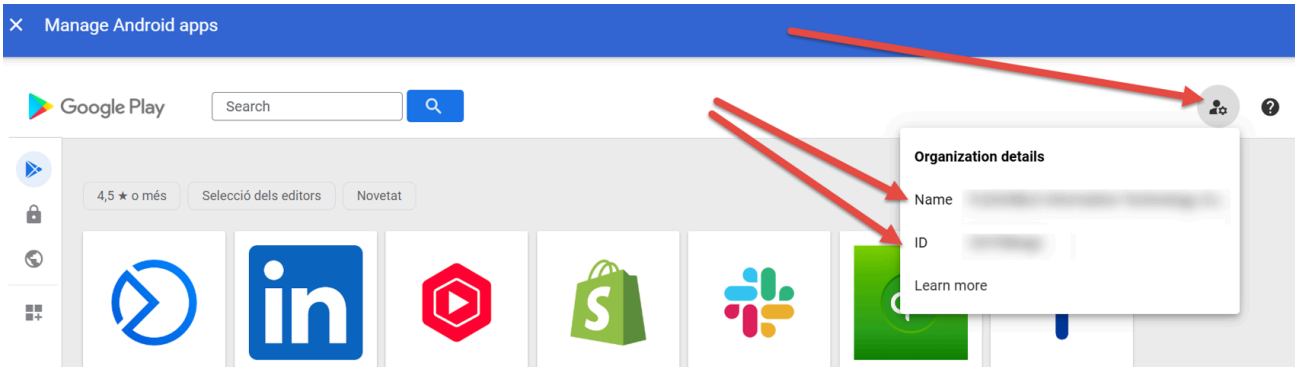
FlexxAgent configuration is managed through Managed Configurations to ensure correct operation.

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.



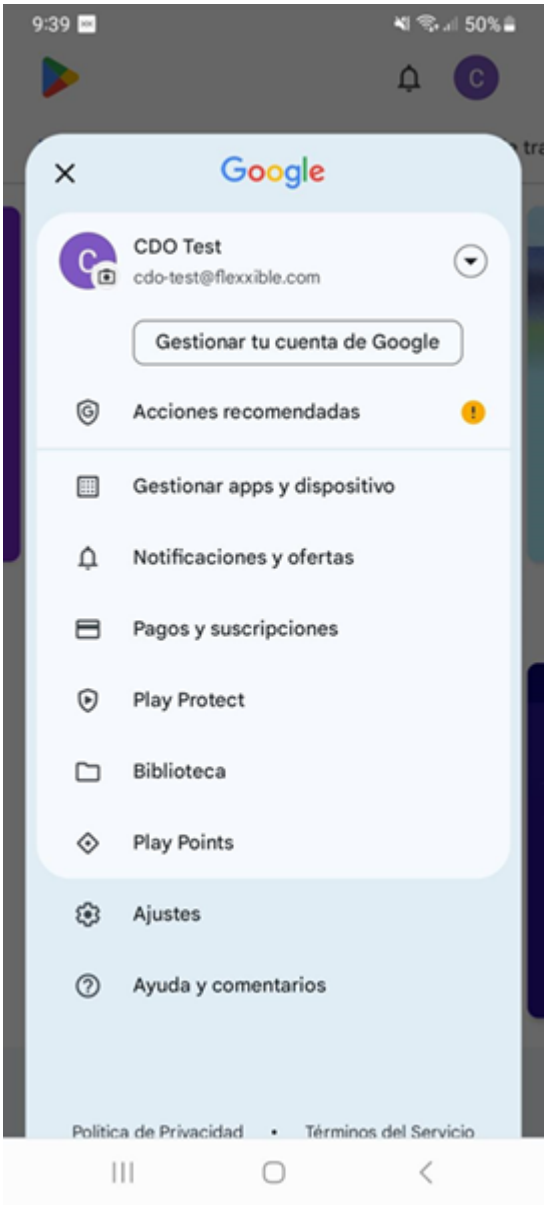
Download and installation

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:

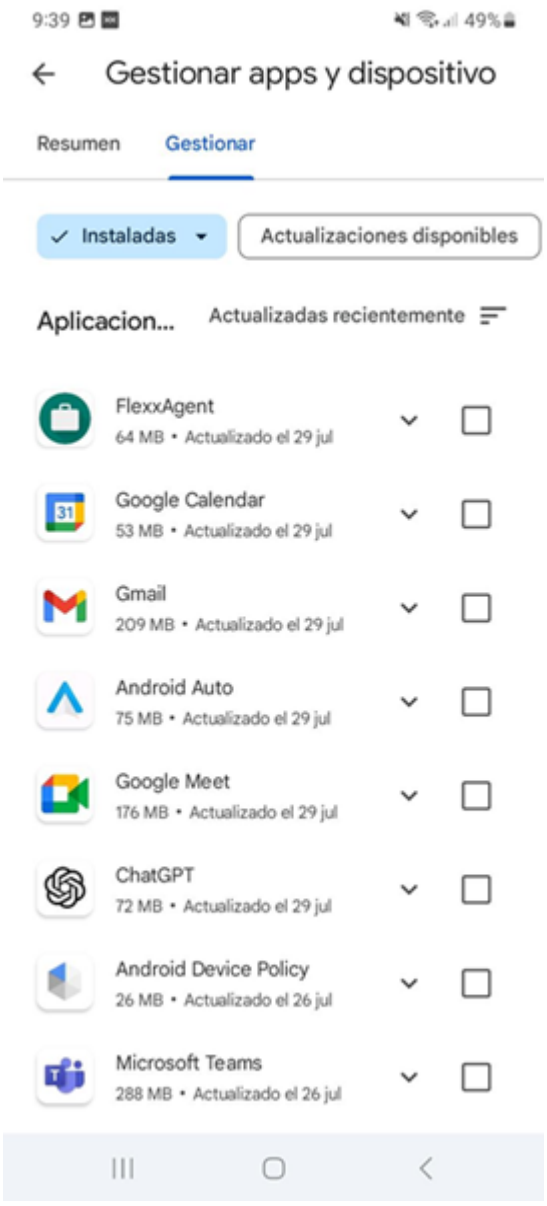
1. Go to Google Play and navigate to `Manage apps and devices`.

Copyright © 2024 Flexxible. Todos los derechos reservados.



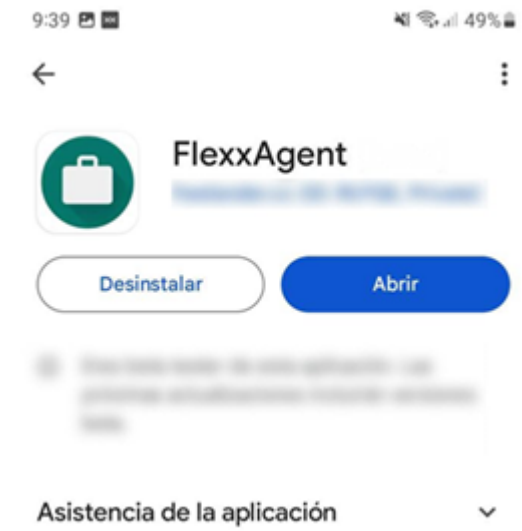
2. Go to the `Manage` tab and click on the FlexxAgent application.

Copyright © 2024 Flexxible. Todos los derechos reservados.



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

Copyright © 2024 Flexxible. Todos los derechos reservados.



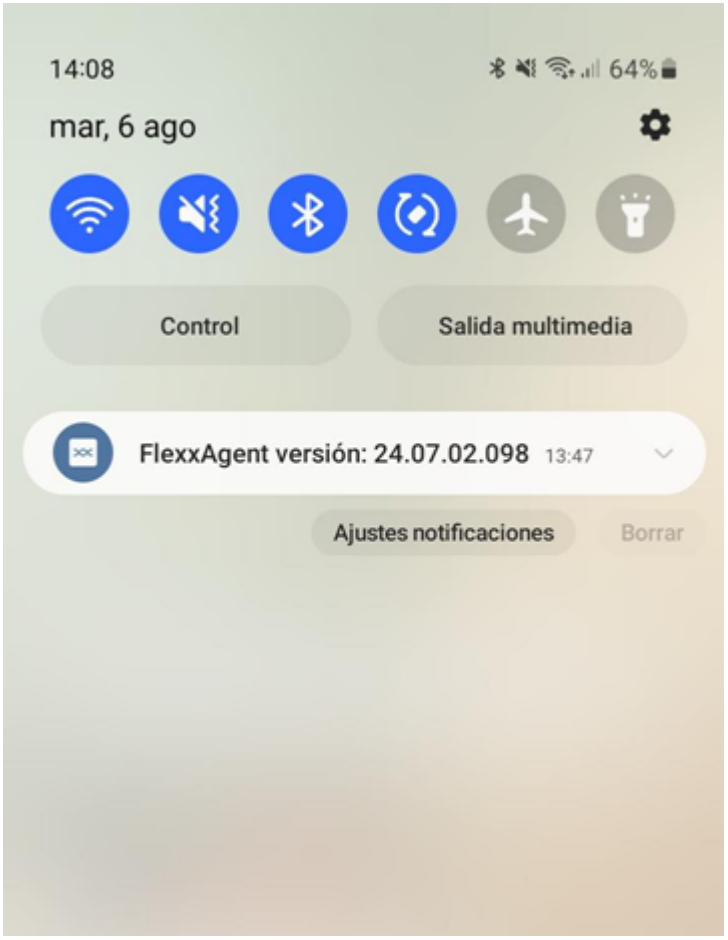
INFO

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

4. Close the window.

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



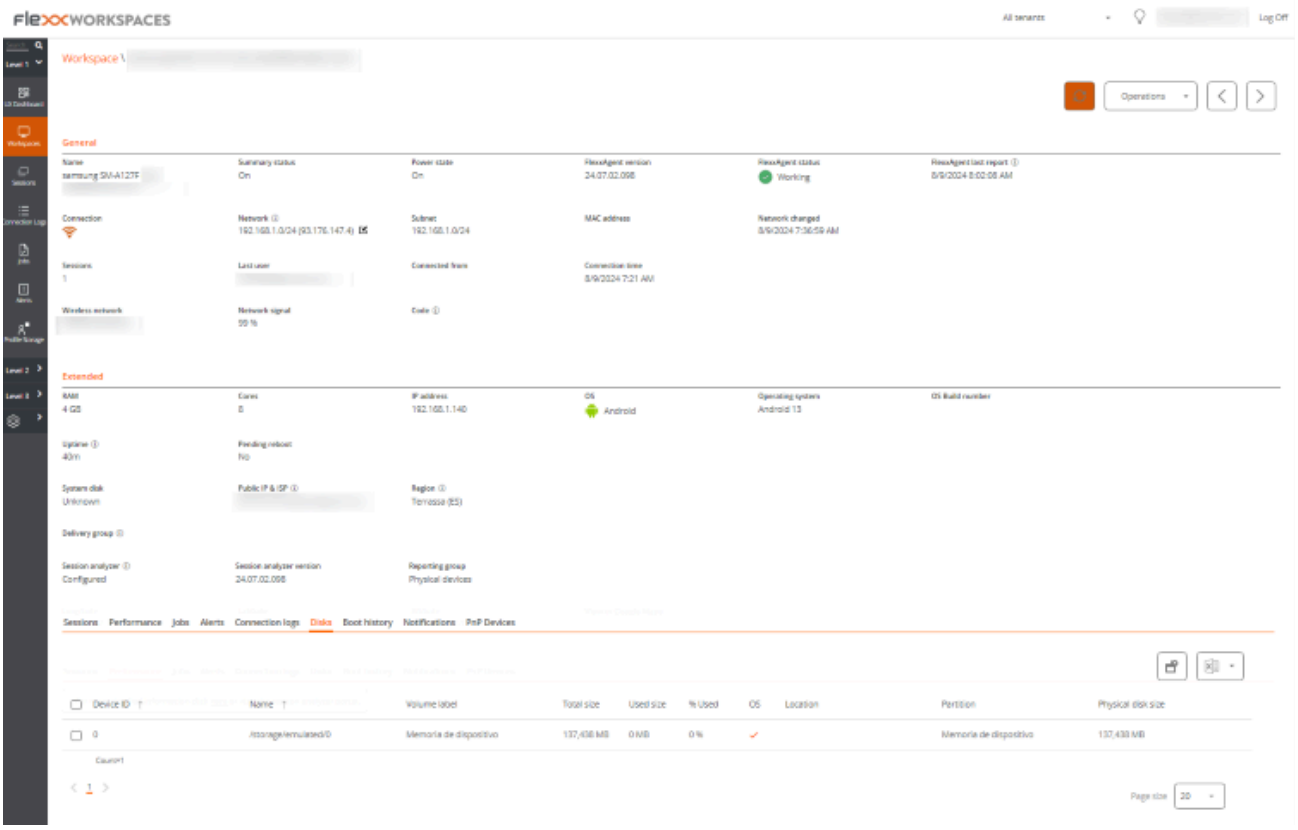
Update

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.



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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

- **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

Copyright © 2024 Flexxible. Todos los derechos reservados.

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.

Job

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

Copyright © 2024 Flexxible. Todos los derechos reservados.

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

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

Bandwidth usage

FlexxAgent process

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

FlexxAgent Analyzer process

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

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

Required URLs and Ports

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

Copyright © 2024 Flexxible. Todos los derechos reservados.

URL	Ambit	Port	Region
https://flxsbname***.servicebus.windows.net	Agent	443	West Europe
https://flxiothub***.azure-devices.net	Agent	443	West Europe
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 – 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

> *** unique identifier provided by Flexxible.

Copyright © 2024 Flexxible. Todos los derechos reservados.

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`

Copyright © 2024 Flexxible. Todos los derechos reservados.

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

Files

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

Deep SSL Inspection

Disable Deep SSL Inspection for the following URLs on devices that use it as a security solution to ensure optimal performance 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)

Copyright © 2024 Flexxible. Todos los derechos reservados.

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

Remote assistance through a proxy

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

If configured with a proxy that is not accessible at the time, remote assistance will launch with the “auto detect” option, using the end user's configured internet access settings.

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

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:

Copyright © 2024 Flexxible. Todos los derechos reservados.

`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

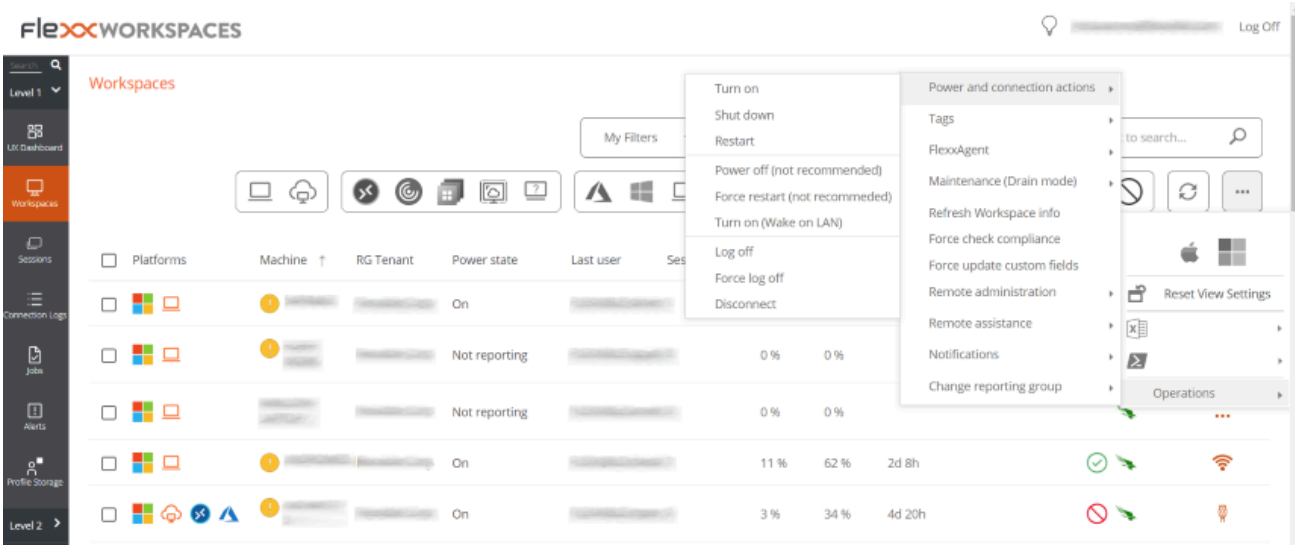
When the functionality has been correctly enabled and configured, the following actions will be available:

- 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)`.

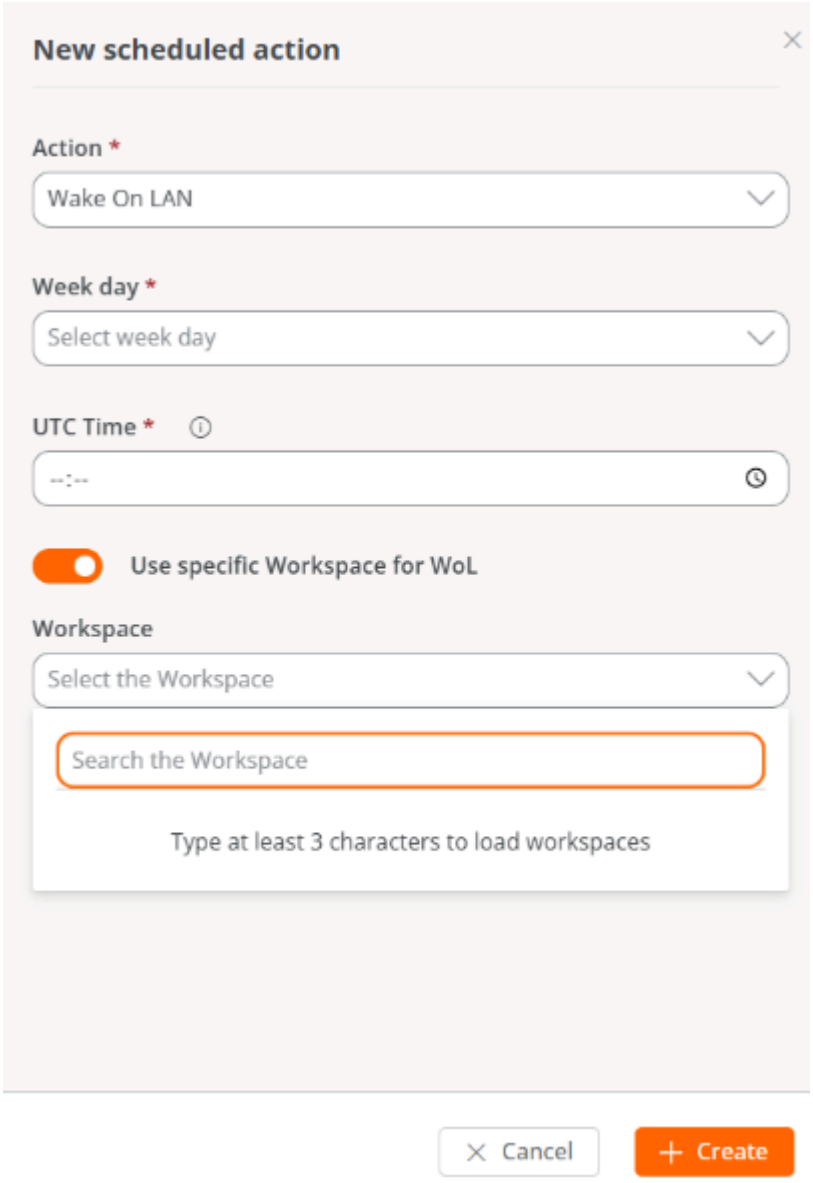
Copyright © 2024 Flexxible. Todos los derechos reservados.



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`.

Copyright © 2024 Flexxible. Todos los derechos reservados.



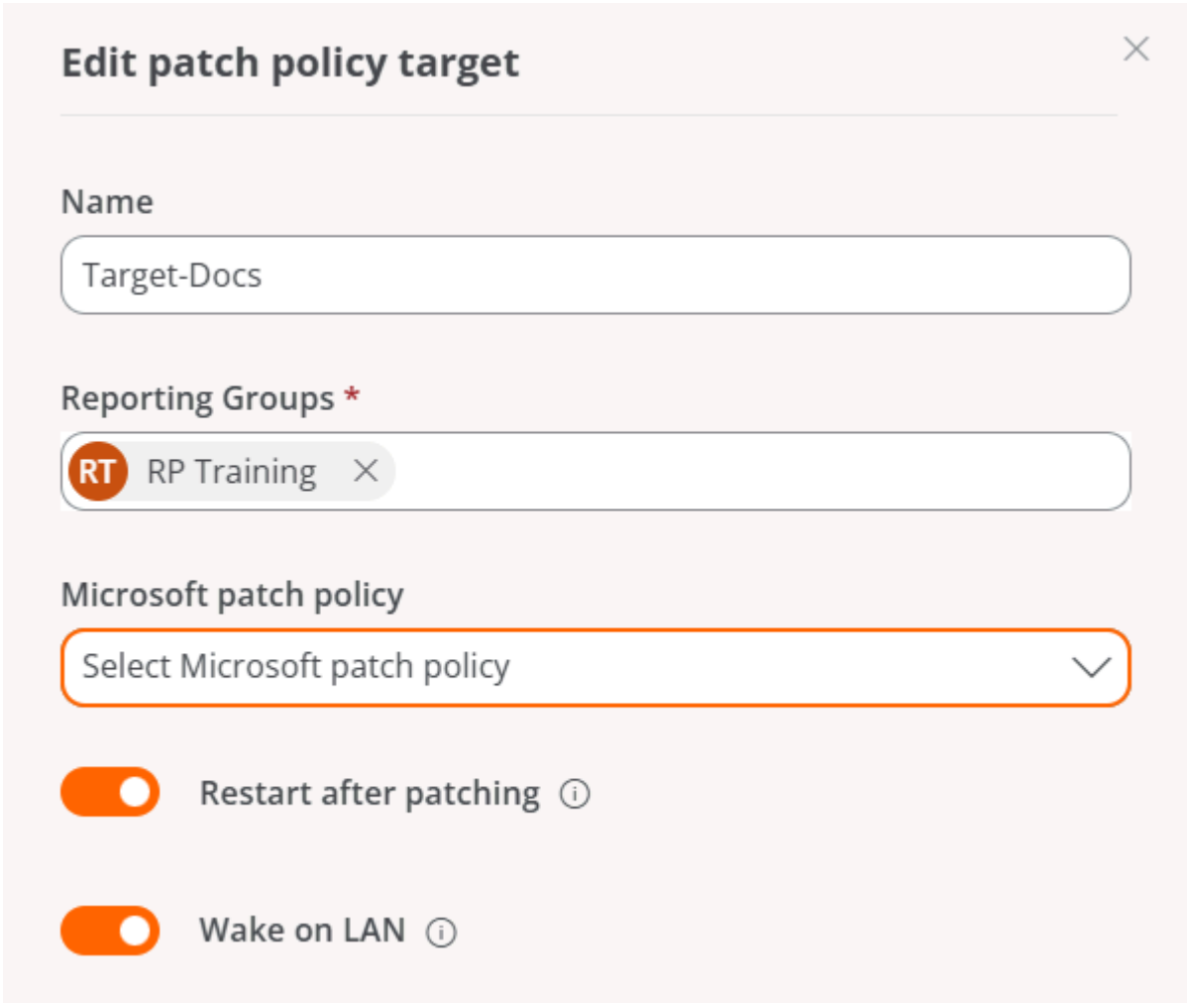
The data entered will be reflected in the table, along with the email of the user who created and updated the schedule. From `View details` you can edit and delete the scheduled action.

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.

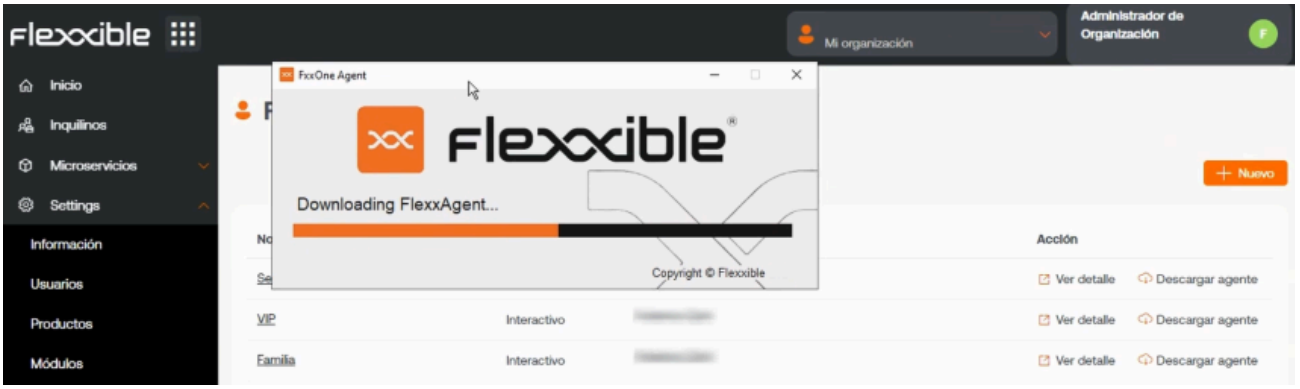
Copyright © 2024 Flexxible. Todos los derechos reservados.

5. Click on `Save`.



Copyright © 2024 Flexxible. Todos los derechos reservados.

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

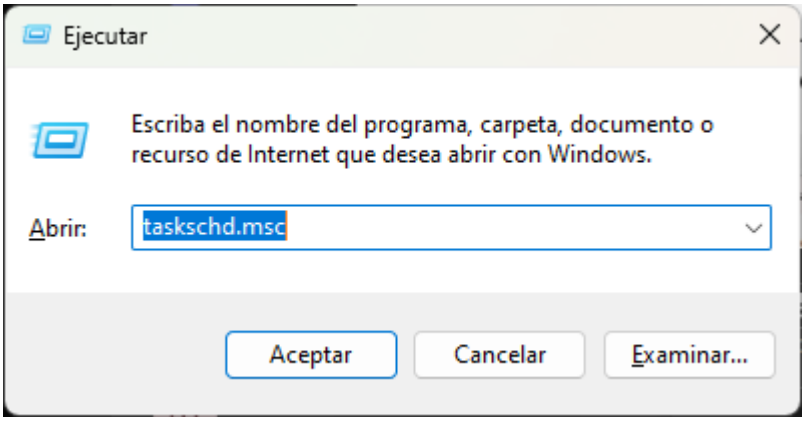
FlexxAgent / Guides / Validate FlexxAgent connectivity

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

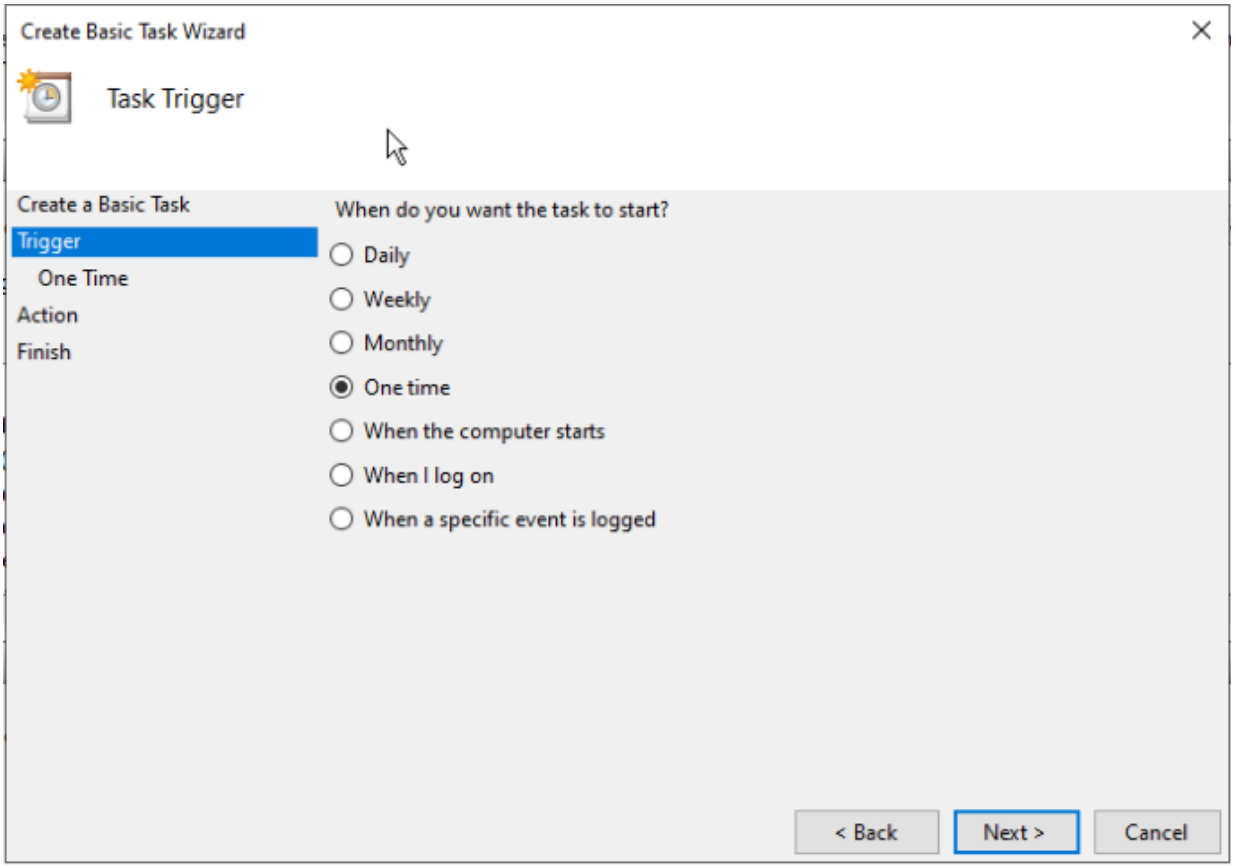
1. Access the `Run` menu (`Windows + R`) and type the command `taskschd.msc`. This opens the Windows task scheduler management console.



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`.

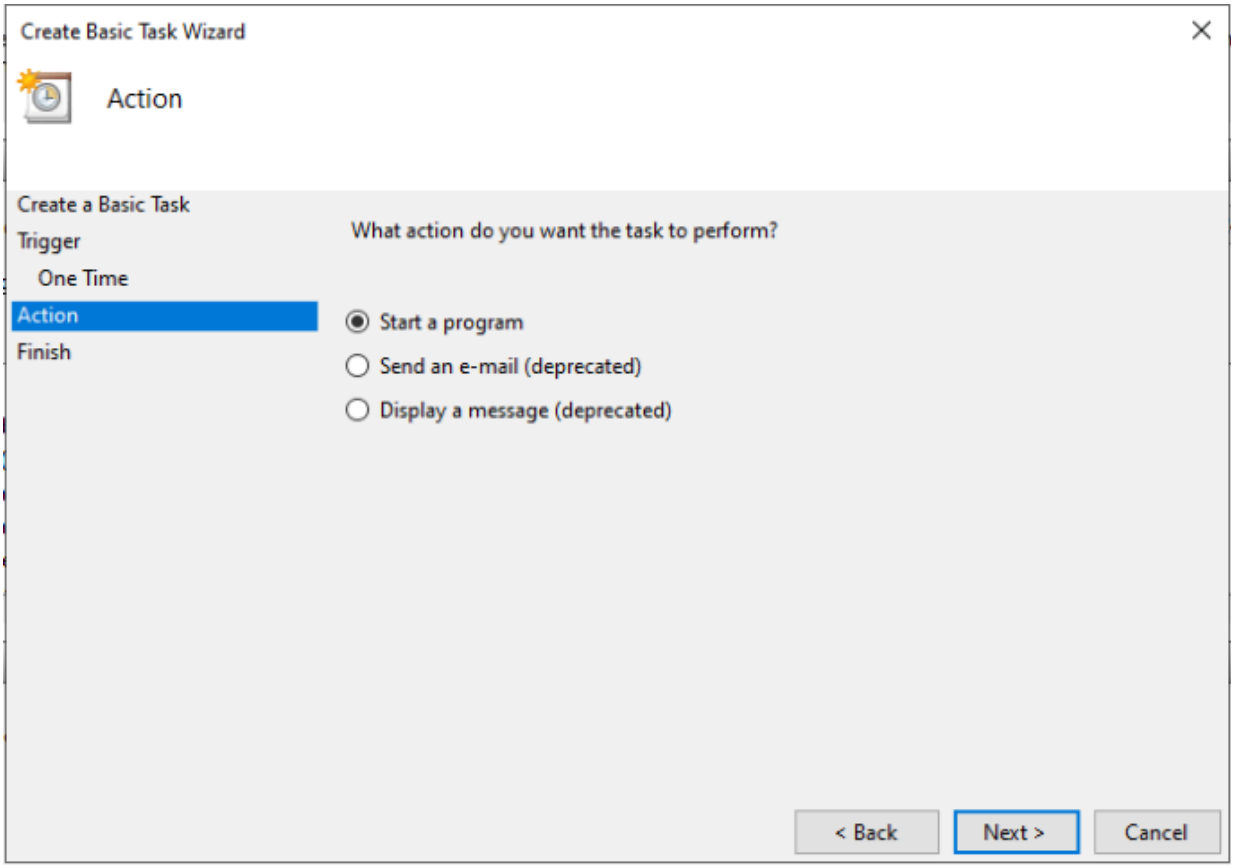
3. Next, select `One Time` and click `Next`. A date picker will appear, but it is not relevant because the task will be executed manually. Click `Next`.

Copyright © 2024 Flexxible. Todos los derechos reservados.



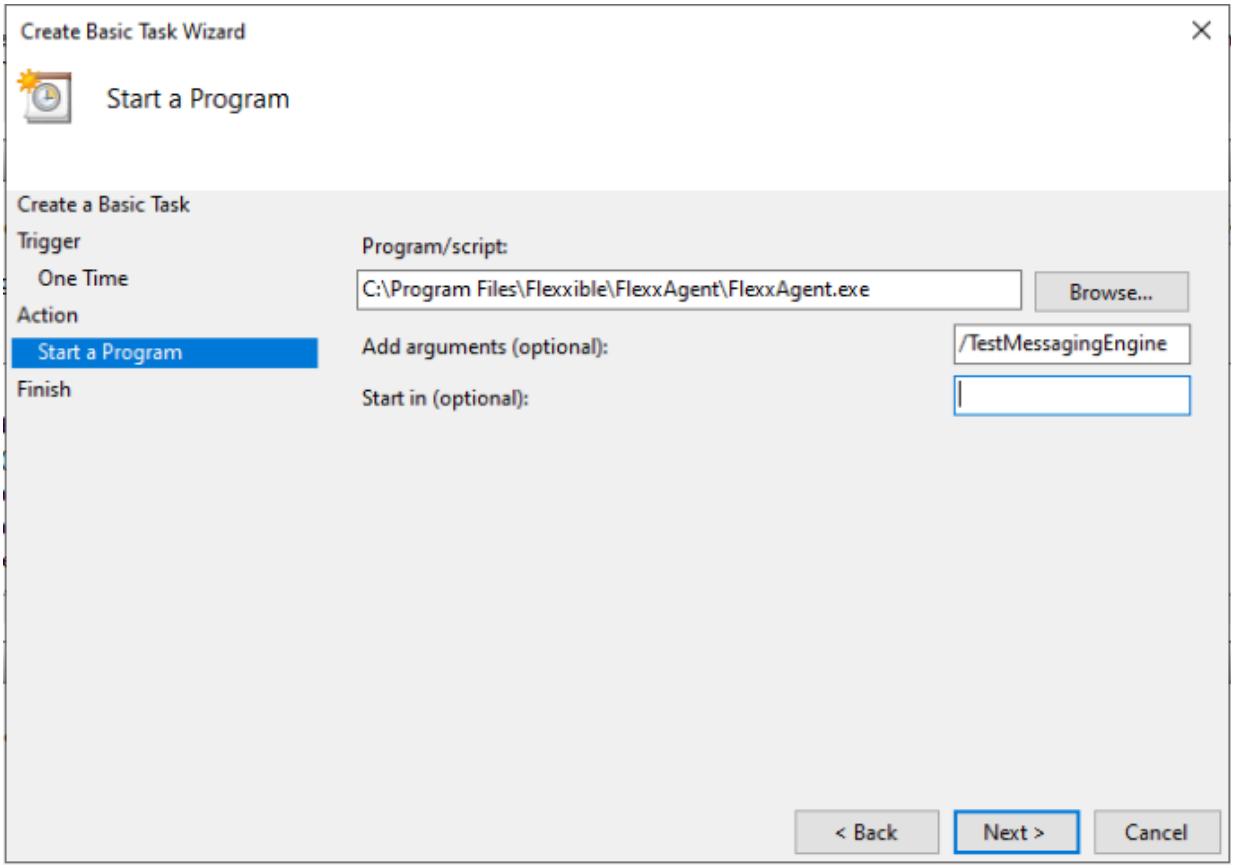
4. Select the `Start a program` action and click `Next`.

Copyright © 2024 Flexxible. Todos los derechos reservados.



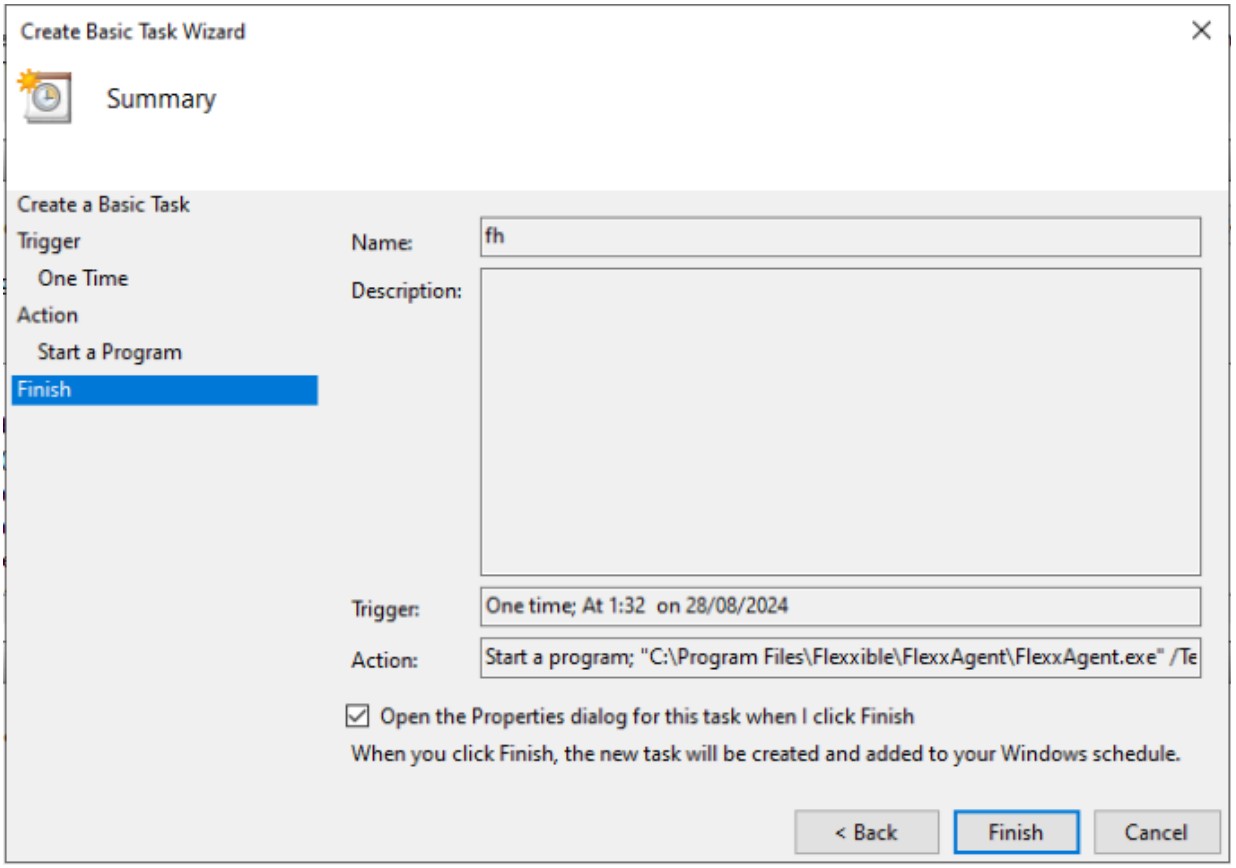
5. In the `Program/script` field, type or browse to the path `C:\Program Files\Flexxible\FlexxAgent\FlexxAgent.exe`. In `Additional Arguments`, type `/TestMessagingEngine`. Click `Next`.

Copyright © 2024 Flexxible. Todos los derechos reservados.



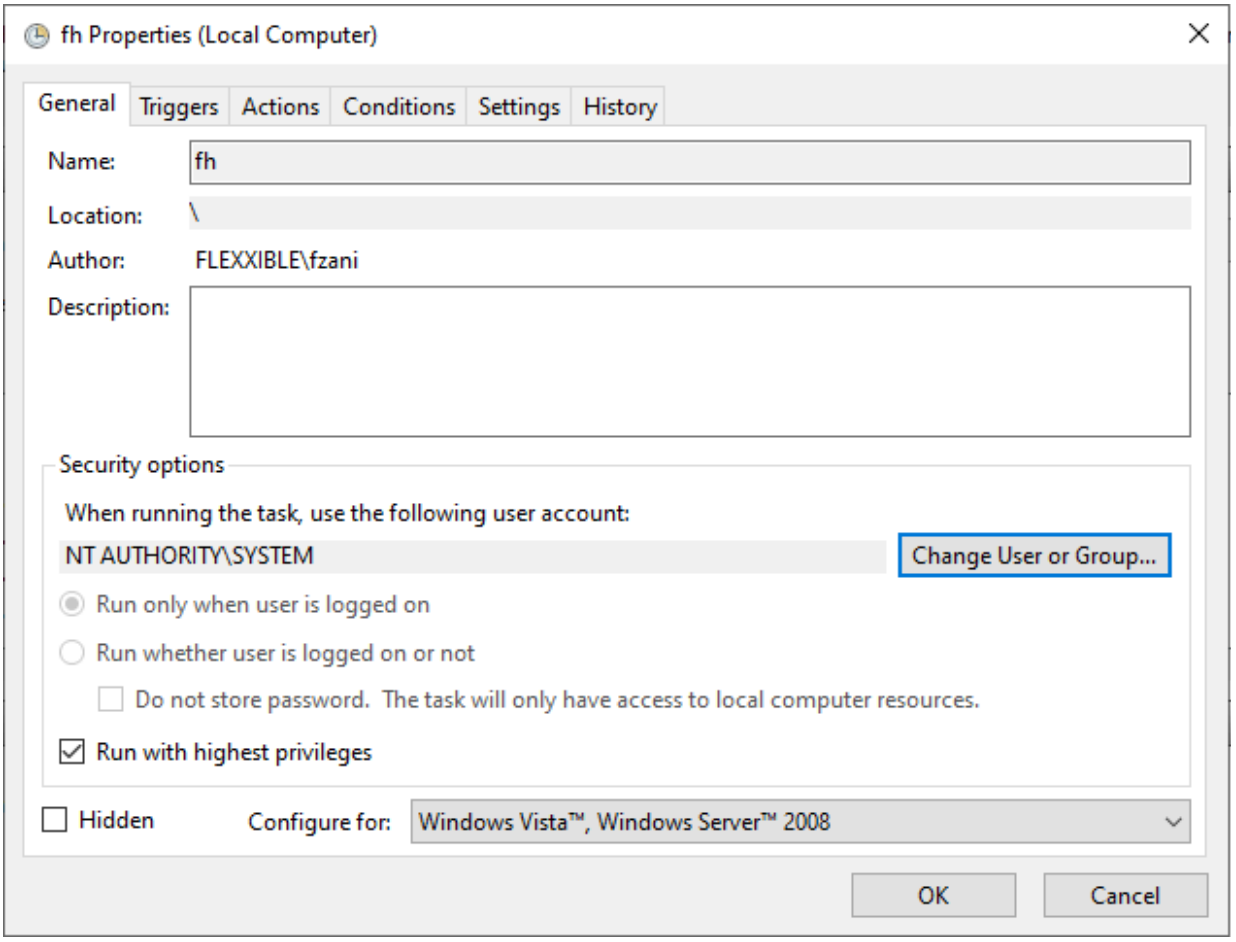
6. Select `Open the Properties dialog for this task when I click Finish` and click `Finish`. The task properties dialog will open.

Copyright © 2024 Flexxible. Todos los derechos reservados.



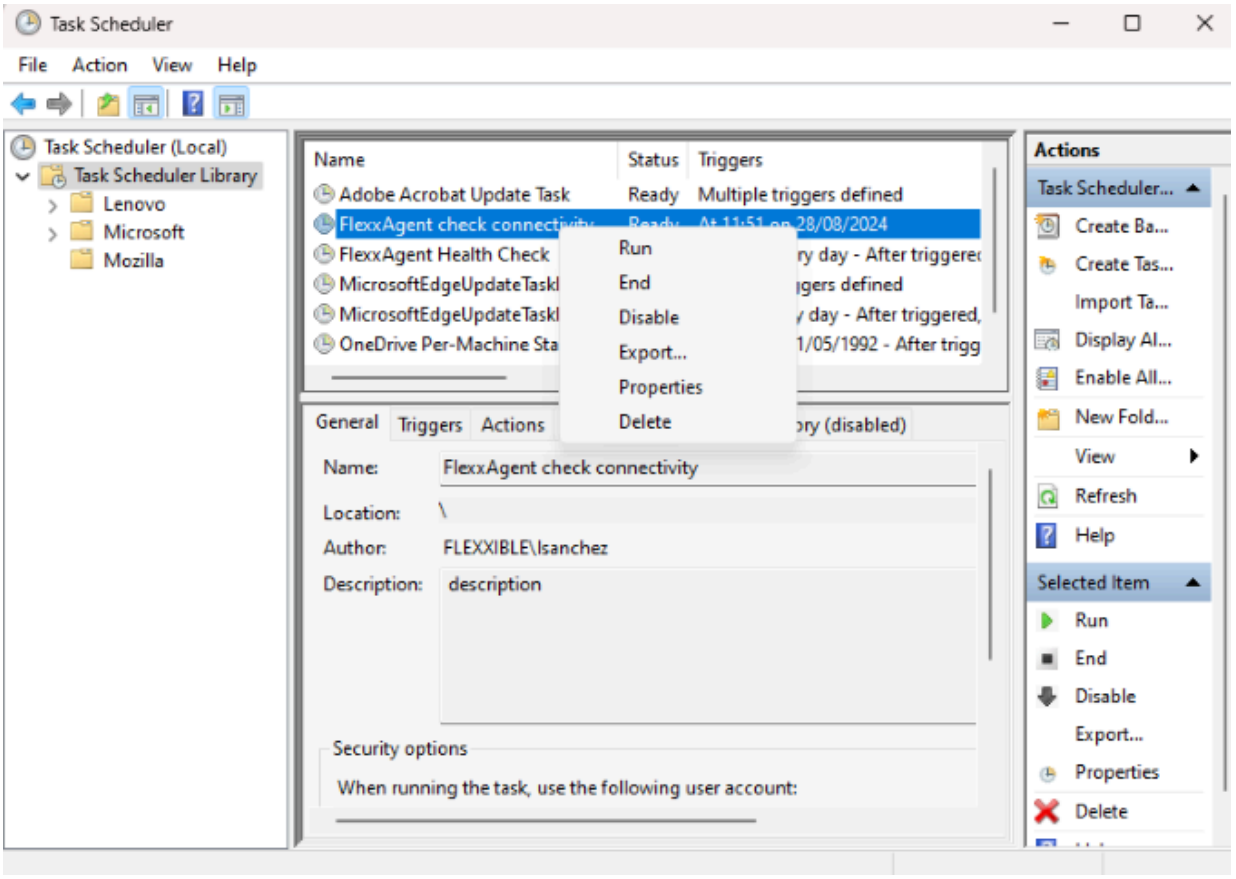
7. Click on `Change User or Group`. In the text box of the pop-up window, type `SYSTEM` and then click `Check Names`. This action will check that the `SYSTEM` group exists to run the task under its identity. Hacer clic en `Aceptar` (OK) para cerrar la ventana emergente. En la ventana de propiedades,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

Copyright © 2024 Flexxible. Todos los derechos reservados.



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.

Copyright © 2024 Flexxible. Todos los derechos reservados.



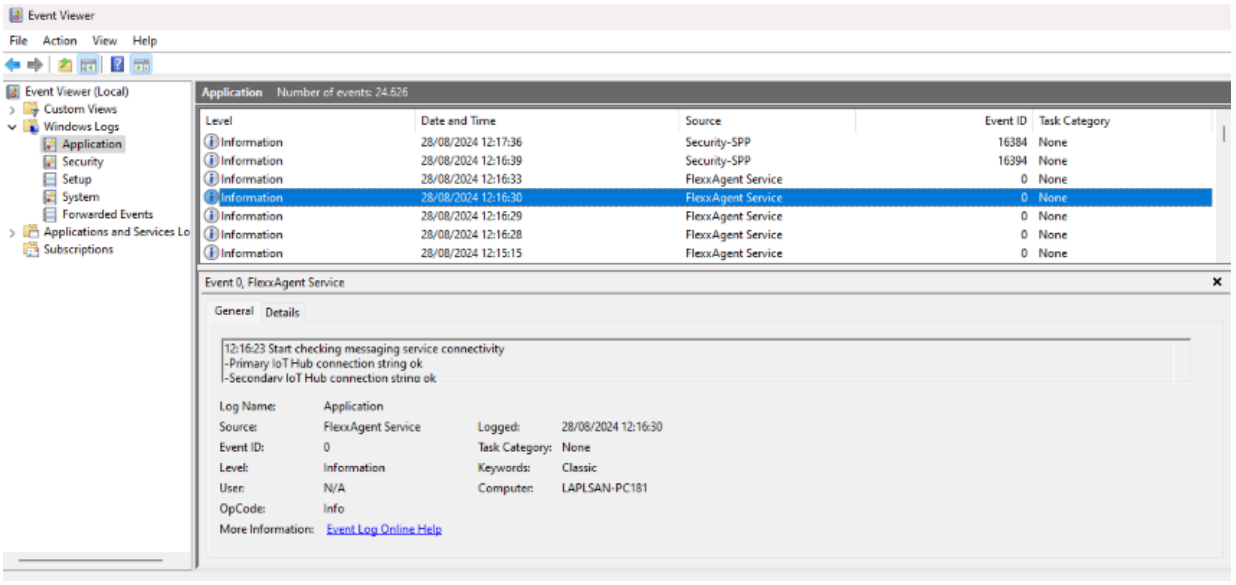
9. Select the `History` tab to see the progress of the task until you see the `Task completed` event. In case the history is disabled, it can be enabled with the `Enable history for all tasks` option in the right panel of the console.

Validation of results

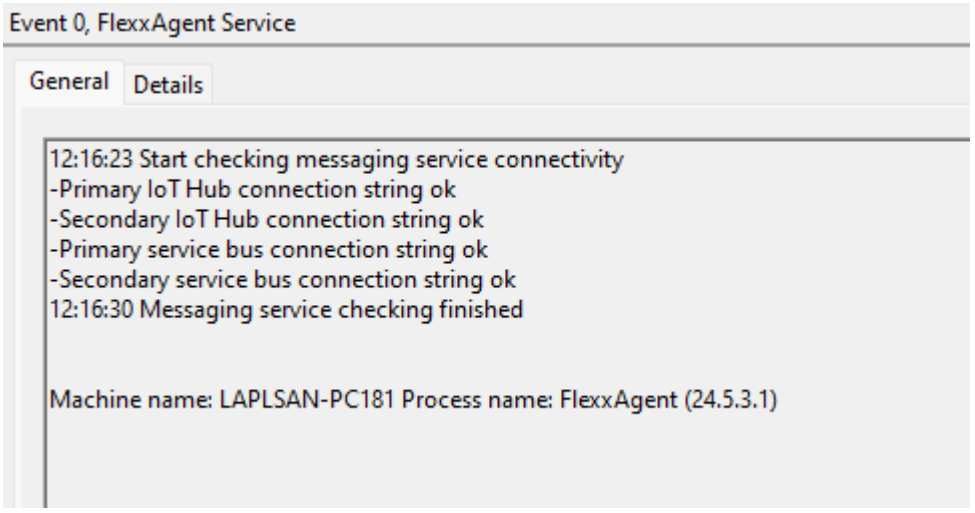
To review the FlexxAgent messaging engine information, access the `Event Viewer` and check for informational messages with the source service of `FlexxAgent Service`:

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`.

Copyright © 2024 Flexxible. Todos los derechos reservados.



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:



Copyright © 2024 Flexxible. Todos los derechos reservados.

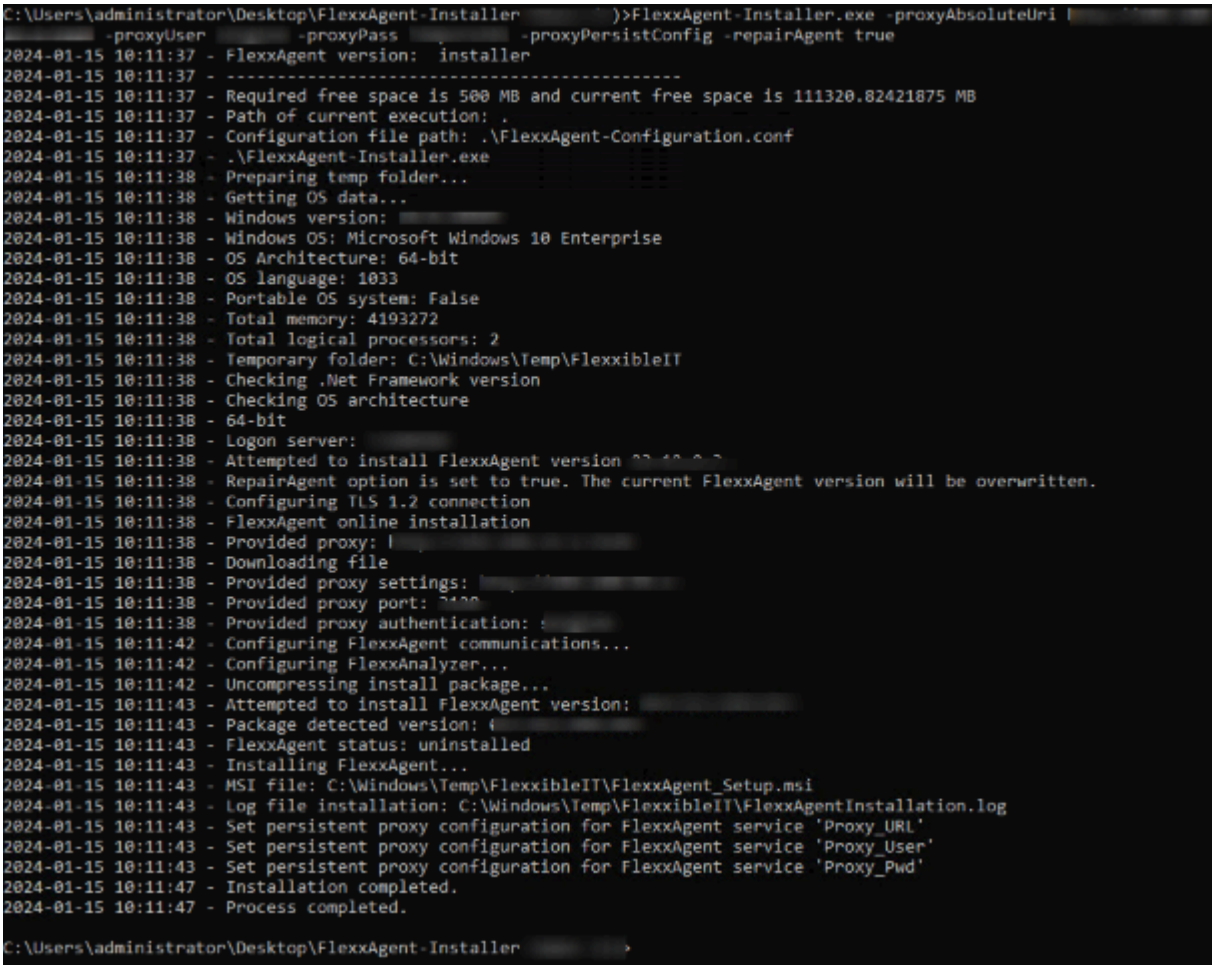
FlexxAgent / Guides / Install FlexxAgent by configuring a proxy server

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`



Copyright © 2024 Flexxible. Todos los derechos reservados.

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

Copyright © 2024 Flexxible. Todos los derechos reservados.

- 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

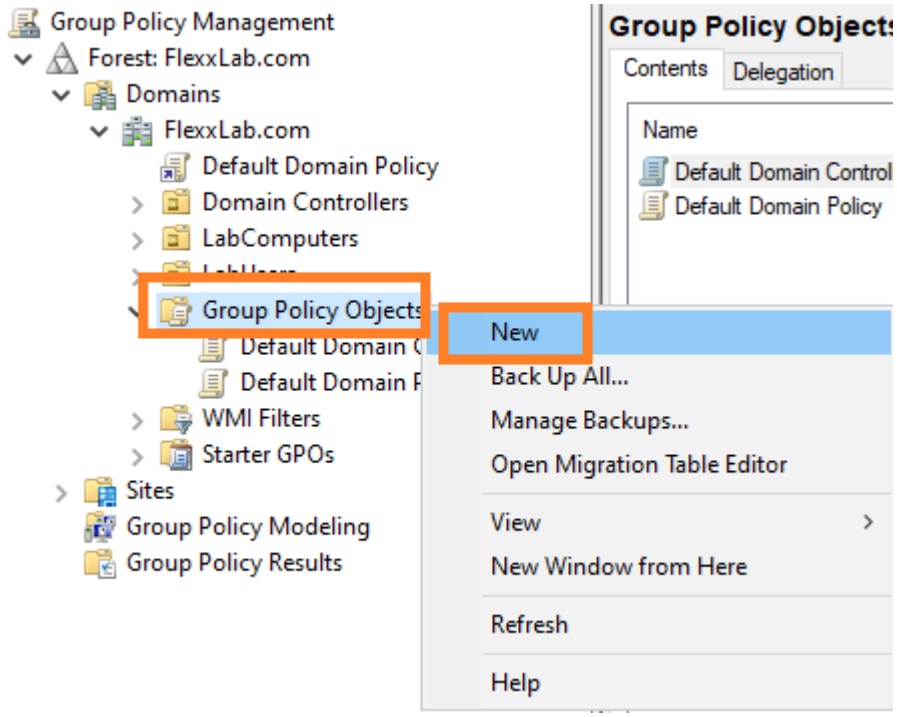
- Key path: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Flexxible\FlexxAgent\Communications
- Key Name: Proxy_Pwd
- Key type: REG_SZ
- Supported values: The password to authenticate to the proxy. It can be bypassed for unauthenticated proxies. The Proxy_Pwd key value can be set in plain text (not recommended)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

Copyright © 2024 Flexxible. Todos los derechos reservados.

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`.

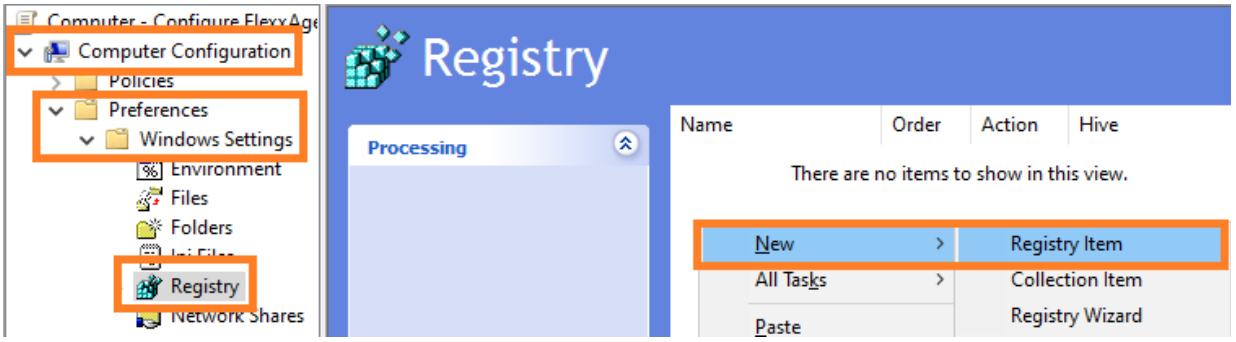


2. Give the new policy an appropriate name and click the `OK` button.

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`.

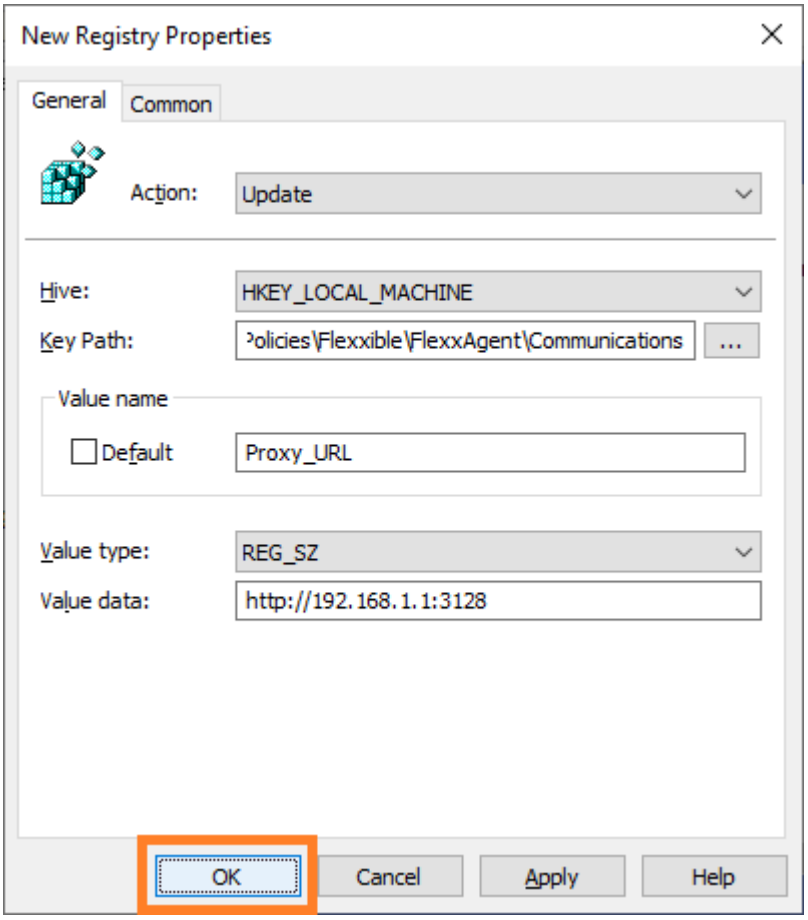
Copyright © 2024 Flexxible. Todos los derechos reservados.



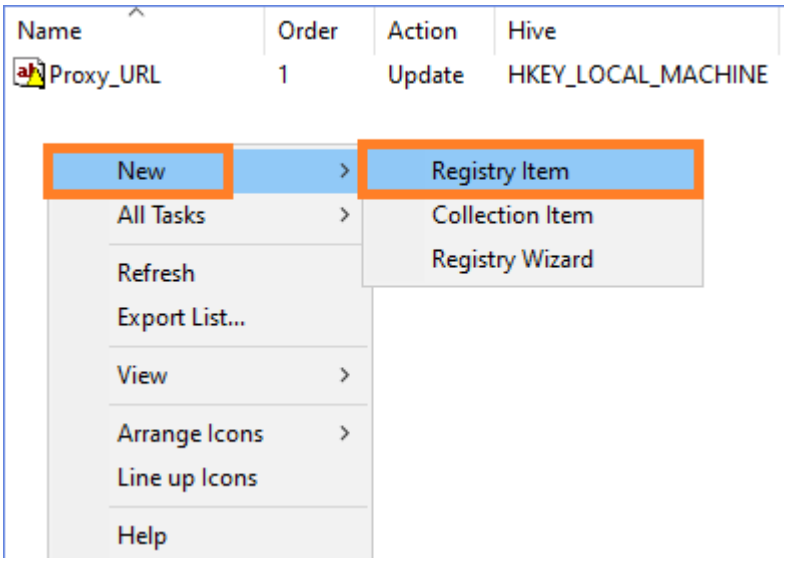
5. Add the following information and click `OK`.

   - 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`.

Copyright © 2024 Flexxible. Todos los derechos reservados.



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

Copyright © 2024 Flexxible. Todos los derechos reservados.

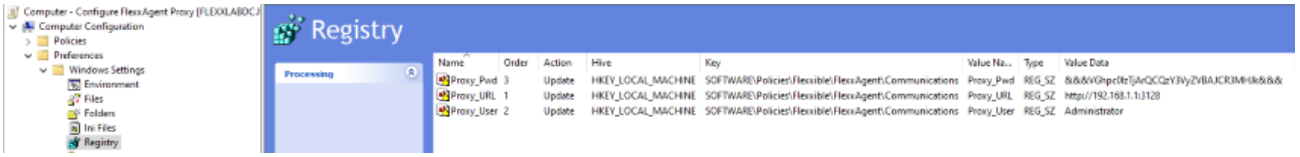
- Key path: `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Flexxible\FlexxAgent\Communications`
- Value Name: Proxy_User
- Value type: REG_SZ
- Value data: The username to authenticate on the proxy server. For example *Admin*.

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/.

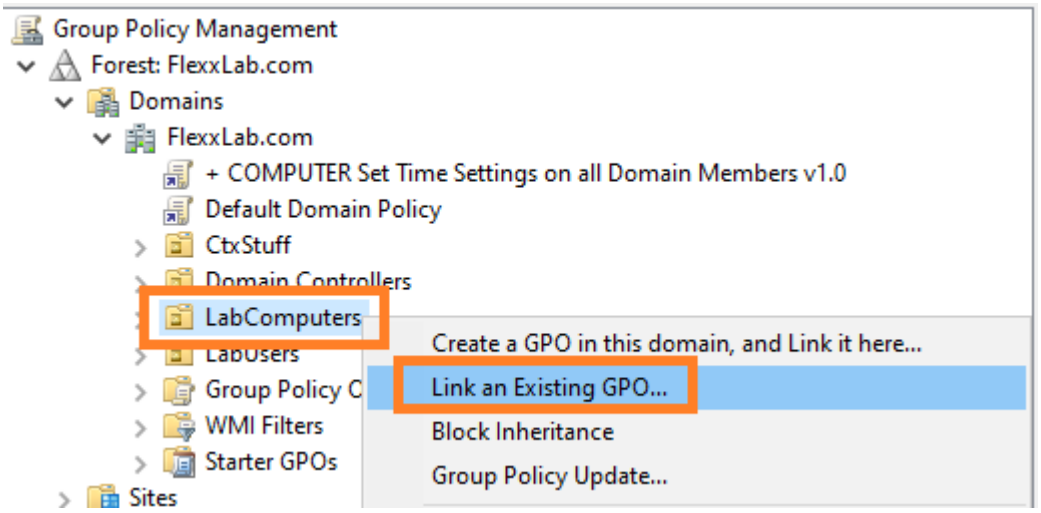
10. Three registry entries will have been created in the group policy.



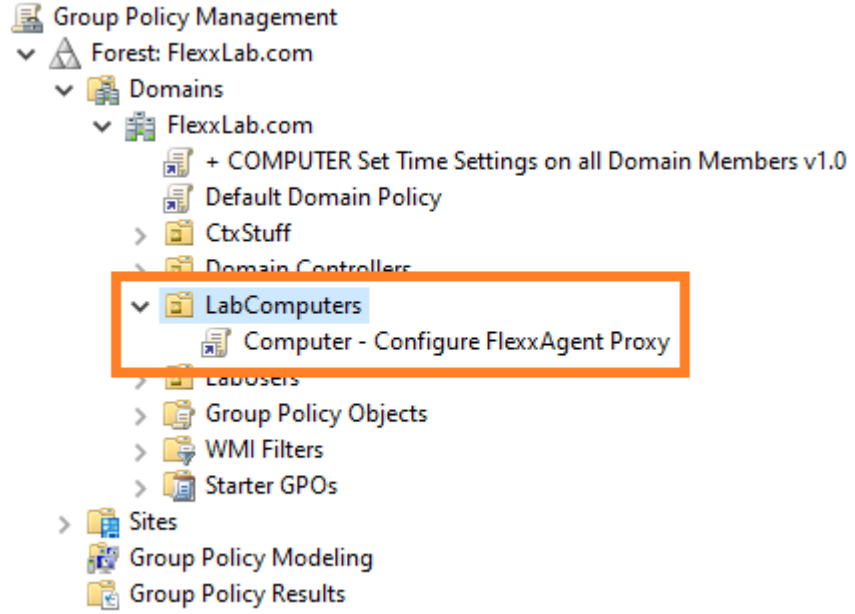
11. Close the editor.

Copyright © 2024 Flexxible. Todos los derechos reservados.

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`.

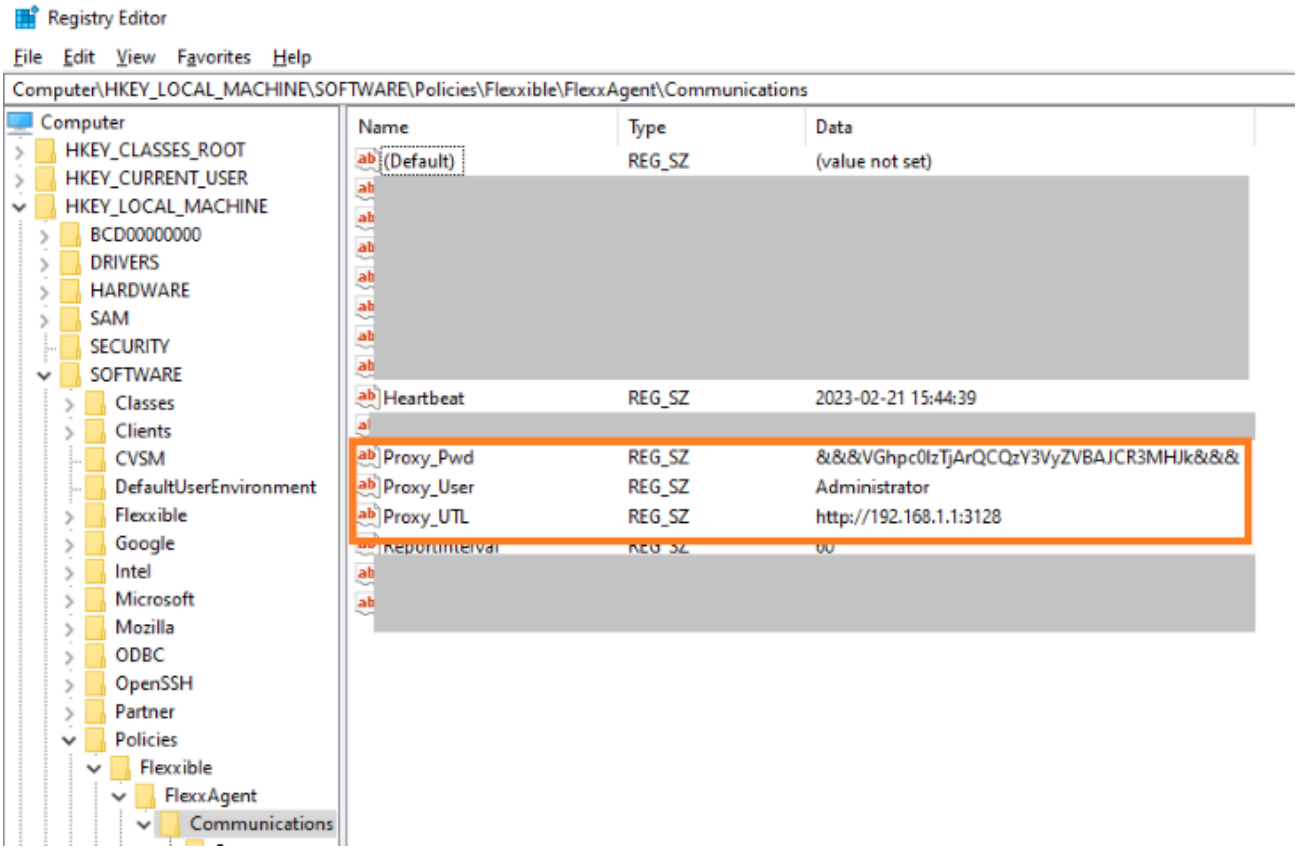


13. Select the previously created group policy.
14. The policy is linked to the devices selected in the domain controller.



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.

Copyright © 2024 Flexxible. Todos los derechos reservados.



Copyright © 2024 Flexxible. Todos los derechos reservados.

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:

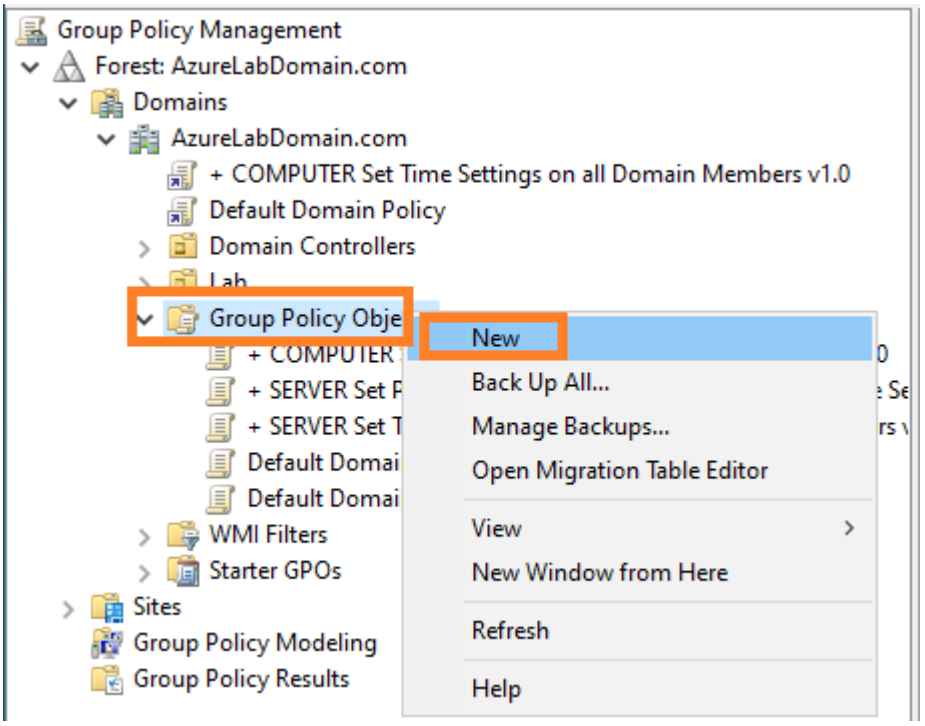
   Start-Process `Path to the file\FlexxAgent-Installer.exe`

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

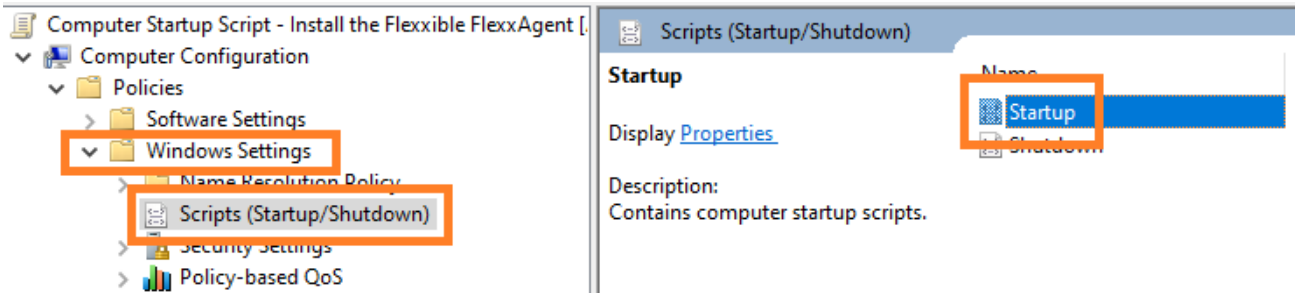
> Note: Make sure that, apart from the executable, the line includes the necessary installation parameters, such as the proxy, if needed.

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

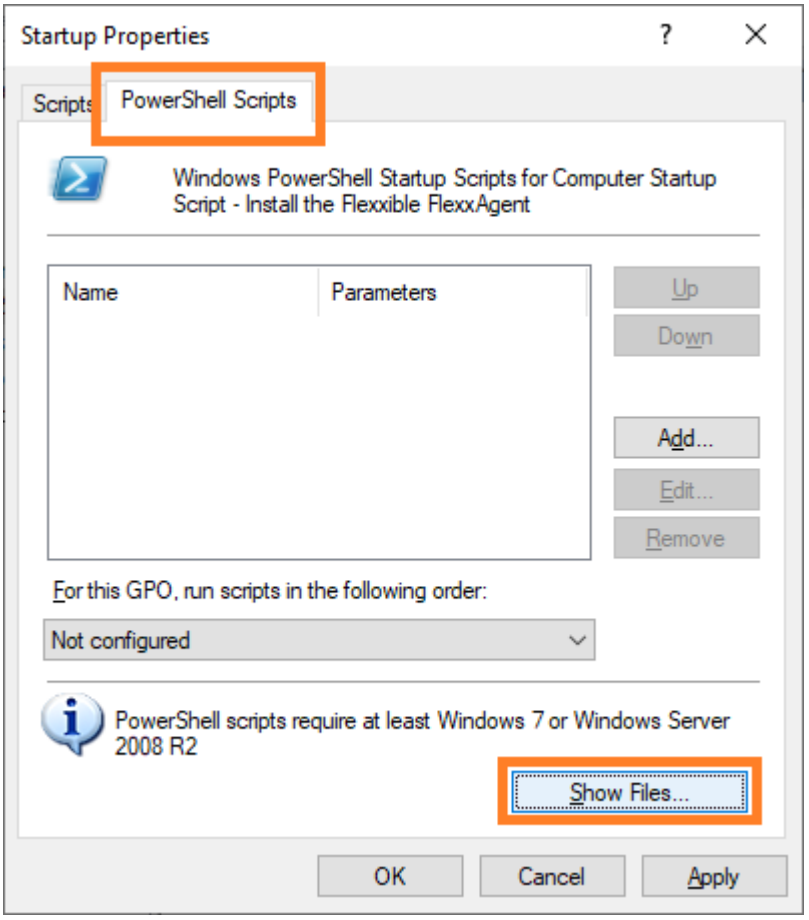


5. Give the new policy a name. Choose one that is meaningful.
6. Right-click on the group policy and select `Edit`.
7. Expand the tree `Computer Configuration` -> `Windows Settings` and select `Scripts (Startup/Shutdown)`

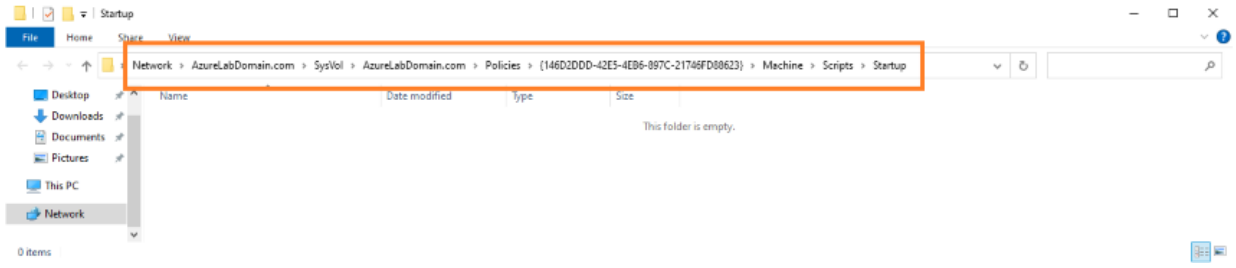


8. A dialog will appear in a new window. Select `PowerShell Scripts` in it. Next, click on the `Show Files...` button

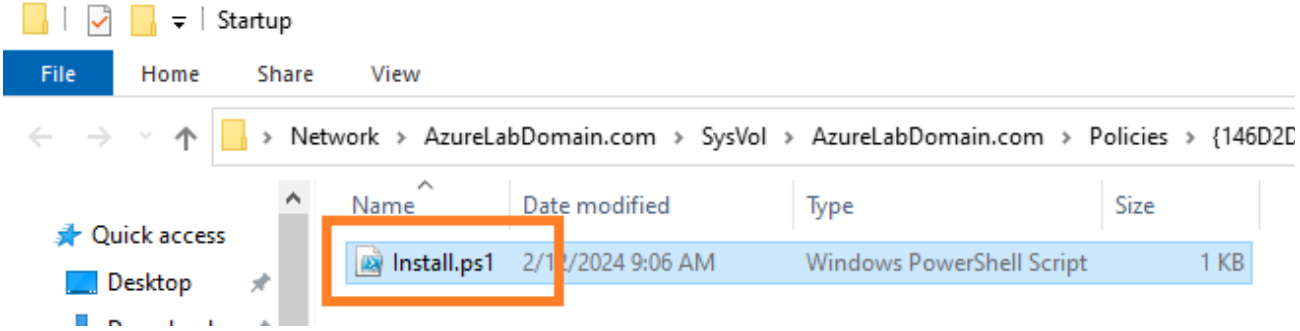
Copyright © 2024 Flexxible. Todos los derechos reservados.



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

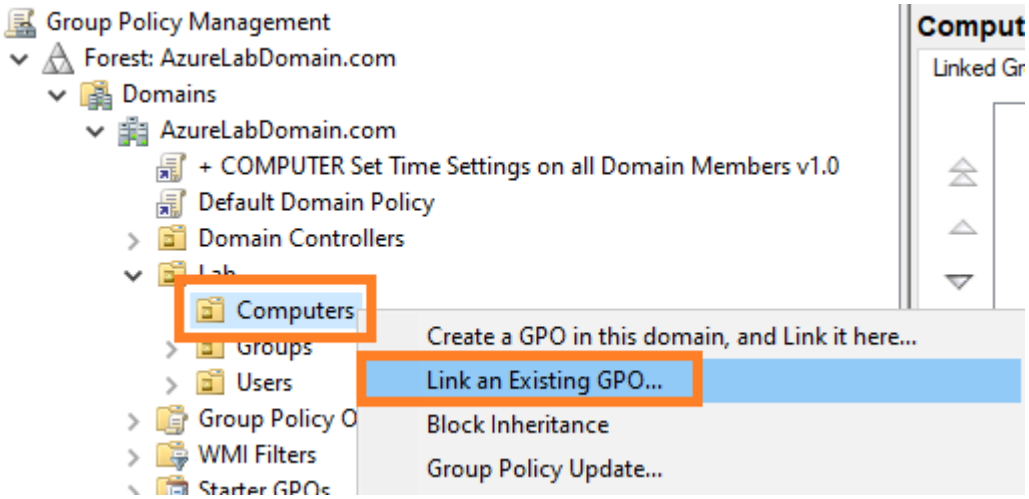


10. Copy the file `Install.ps1` that was created at the beginning and paste it into the network folder for storing Group Policy scripts.



Copyright © 2024 Flexxible. Todos los derechos reservados.

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`.



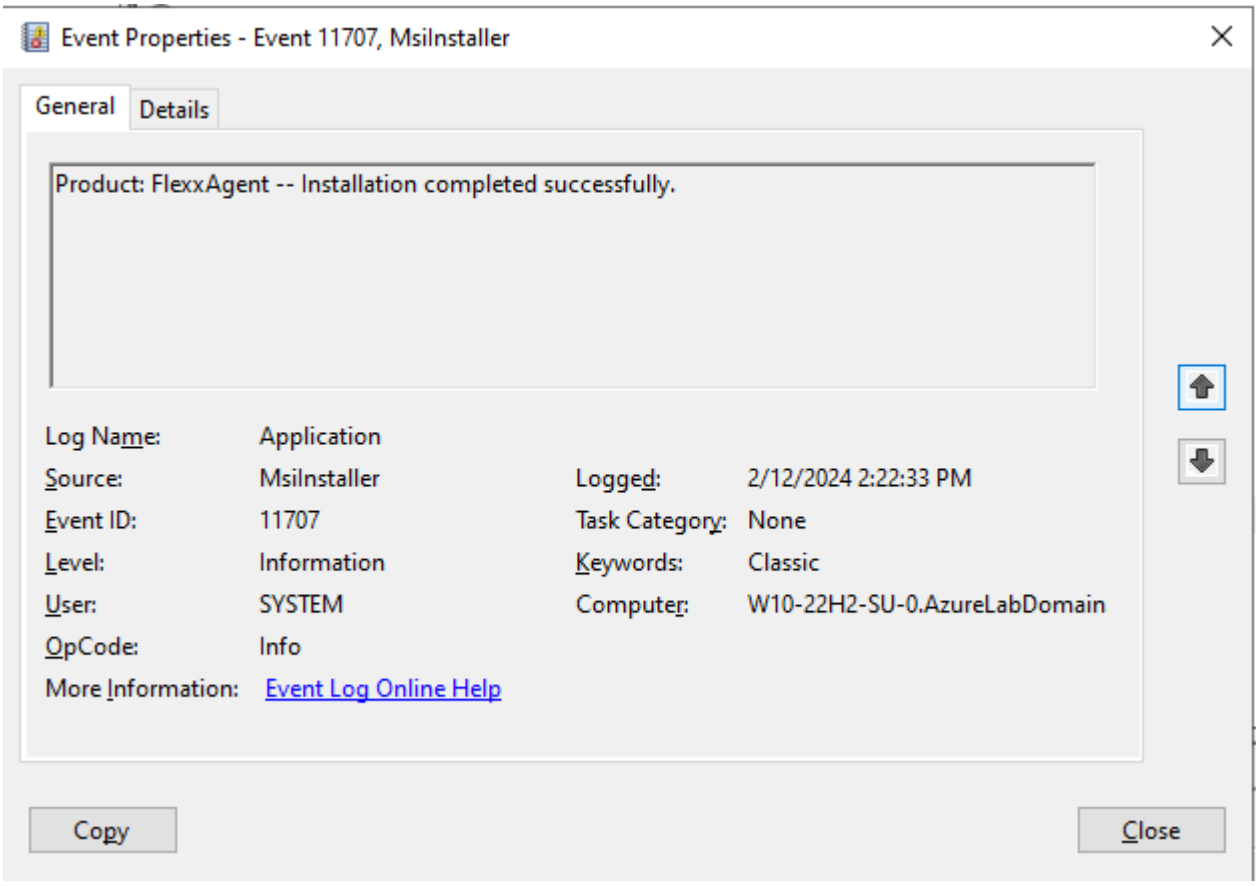
18. A selection dialog will appear where the previously created policy will be selected. Once selected, click `OK`.

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.

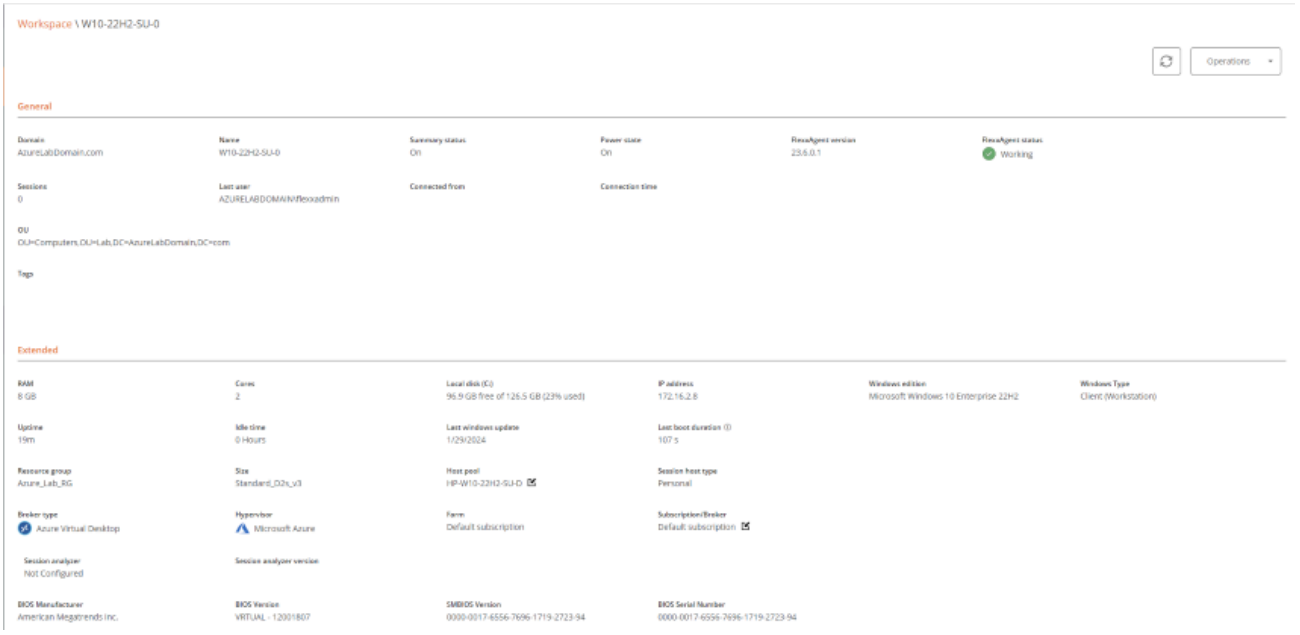
Copyright © 2024 Flexxible. Todos los derechos reservados.

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.

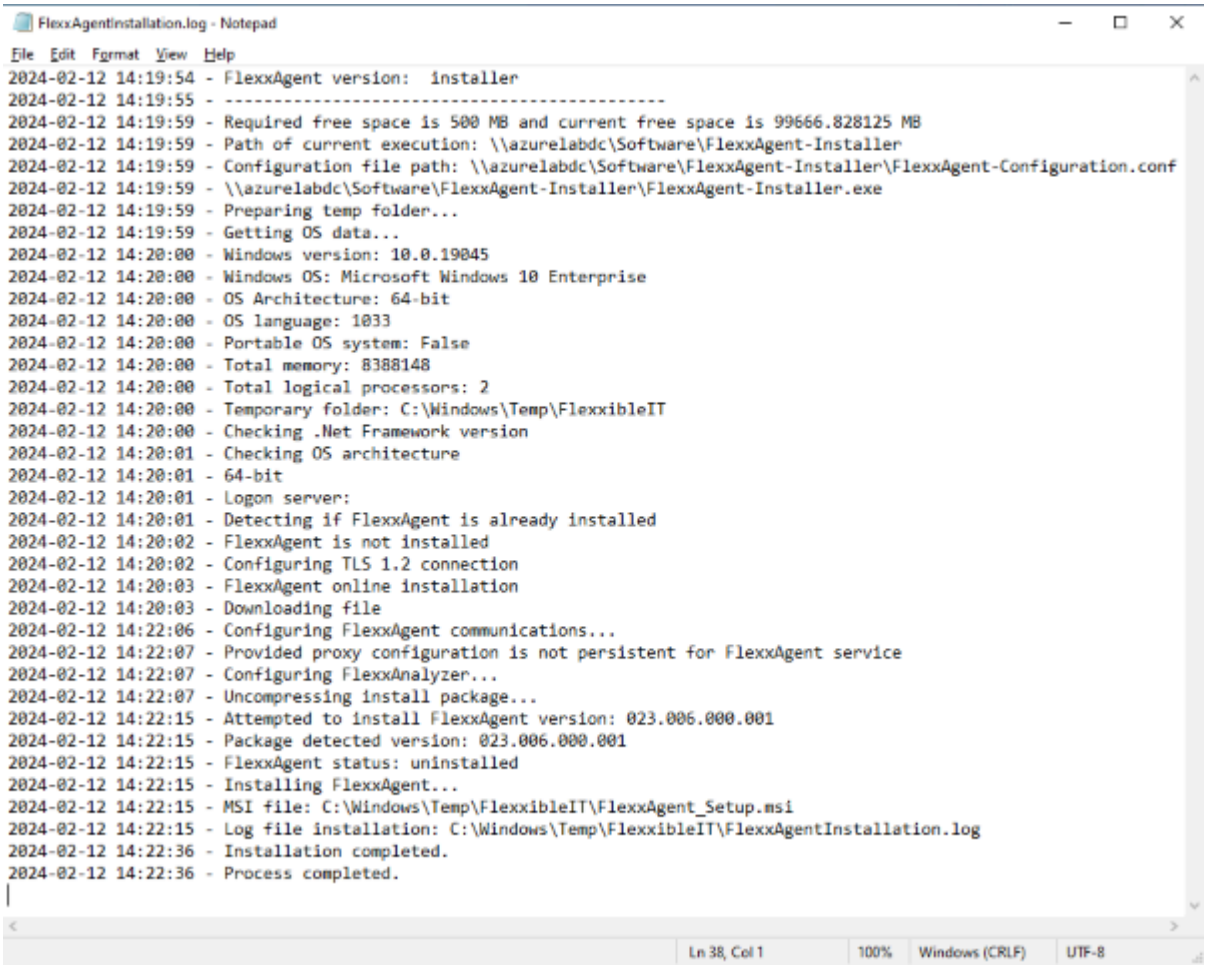


After a few minutes, you will see the new device registered in the Workspaces module and in the `Workspaces` view of the Portal.

Copyright © 2024 Flexxible. Todos los derechos reservados.



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



Copyright © 2024 Flexxible. Todos los derechos reservados.

FlexxAgent / Guides / Deploy FlexxAgent with Microsoft Intune

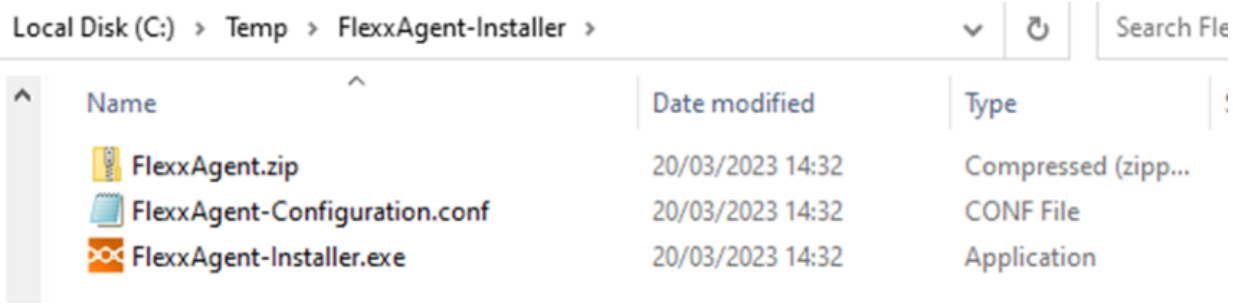
FlexxAgent can be deployed using Microsoft Intune. Before doing it, you need to check that you have the following requirements:

- 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:

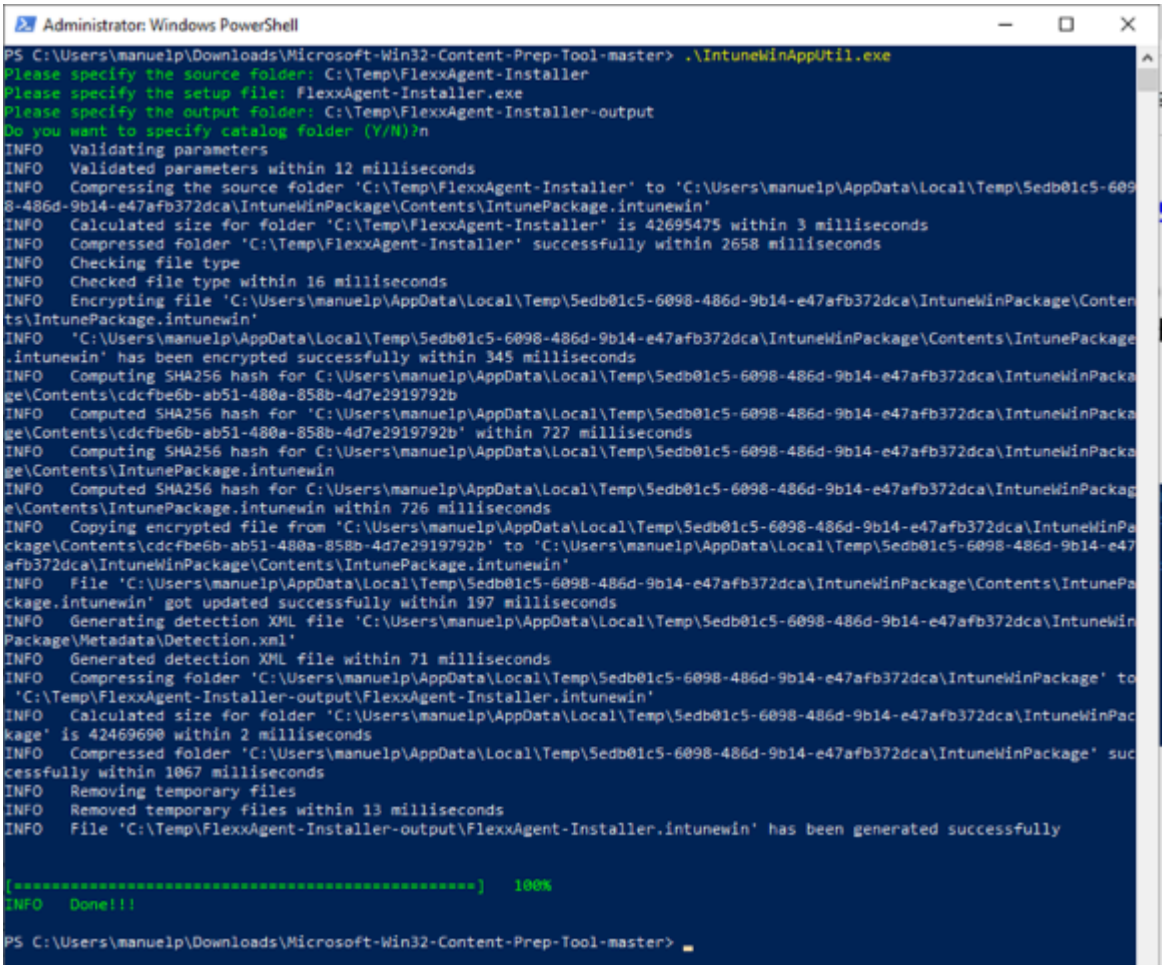


2. Download the `Microsoft Win32 Prep Tool`. For more information, see Prepare a Win32 app to be uploaded to Microsoft Intune.

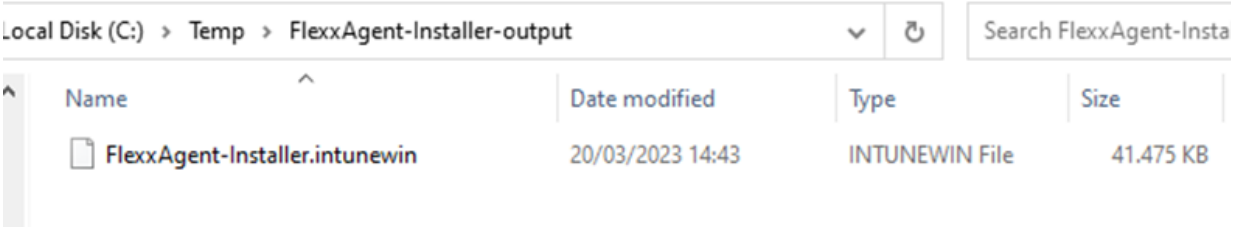
3. Create an empty folder; for example: `C:\Temp\FlexxAgent-Installer-output`.

Copyright © 2024 Flexxible. Todos los derechos reservados.

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.



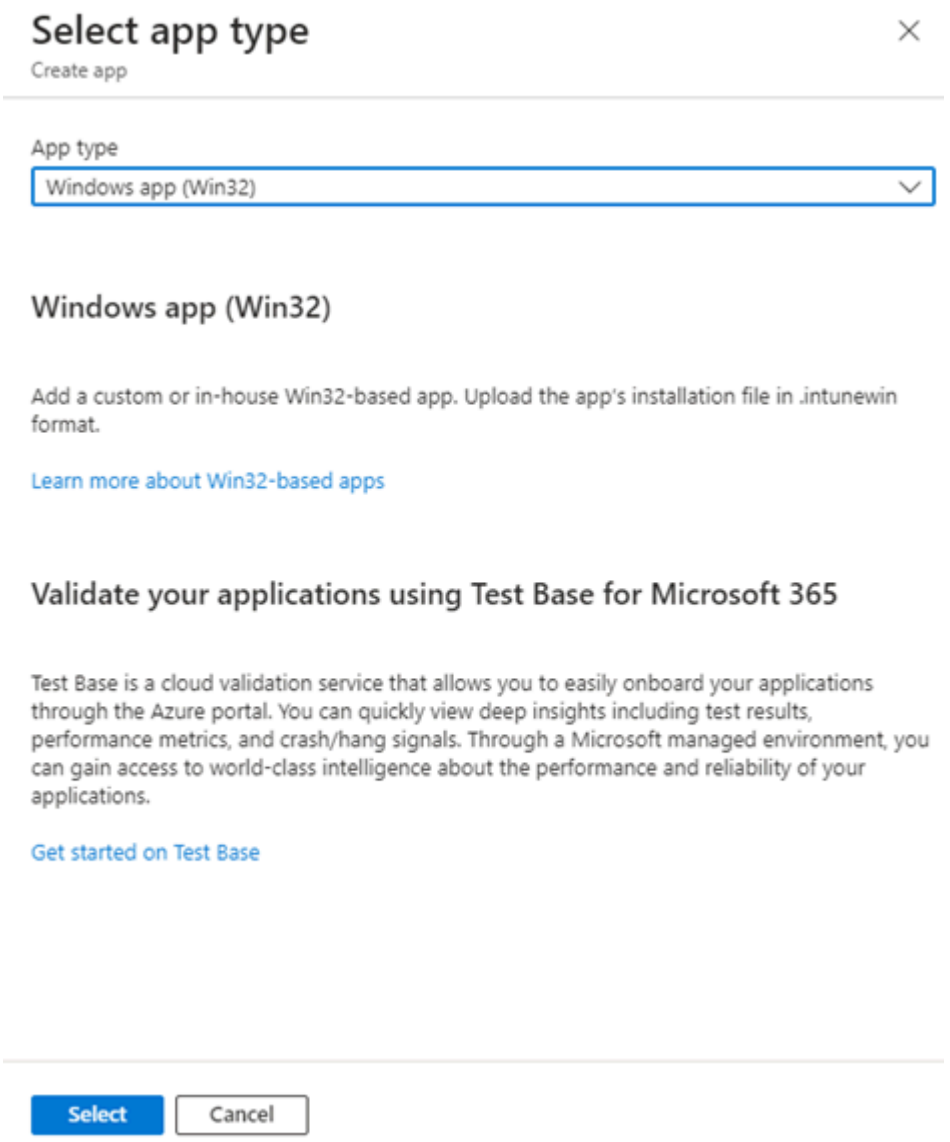
6. The created package is used to deploy an application within Intune.

7. Go to the Intune admin center.

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

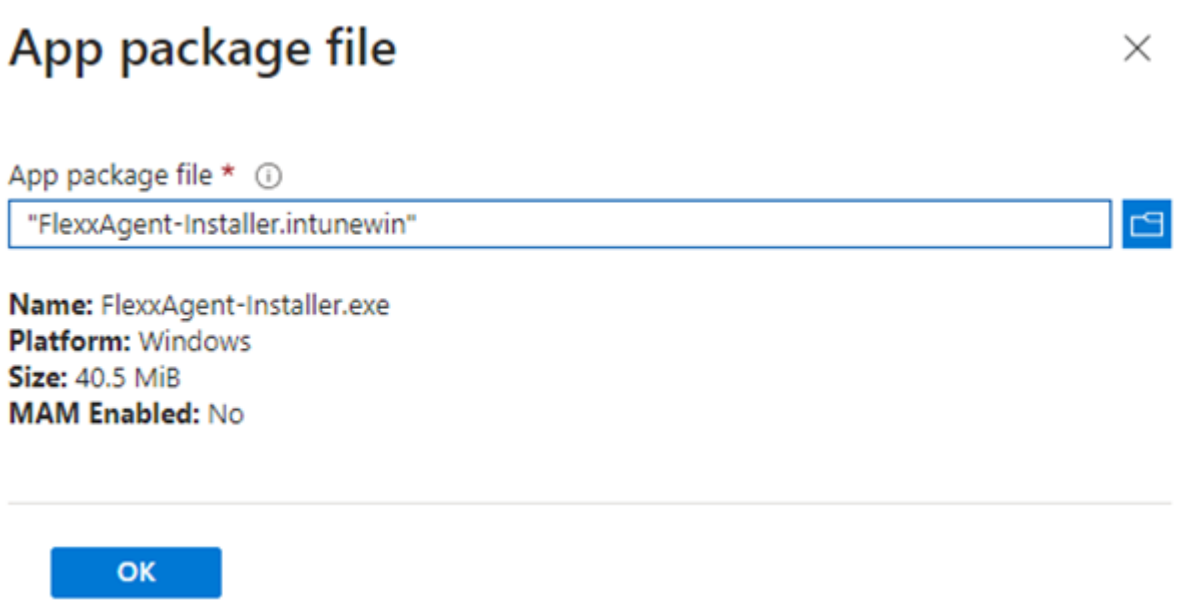
Copyright © 2024 Flexxible. Todos los derechos reservados.

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).

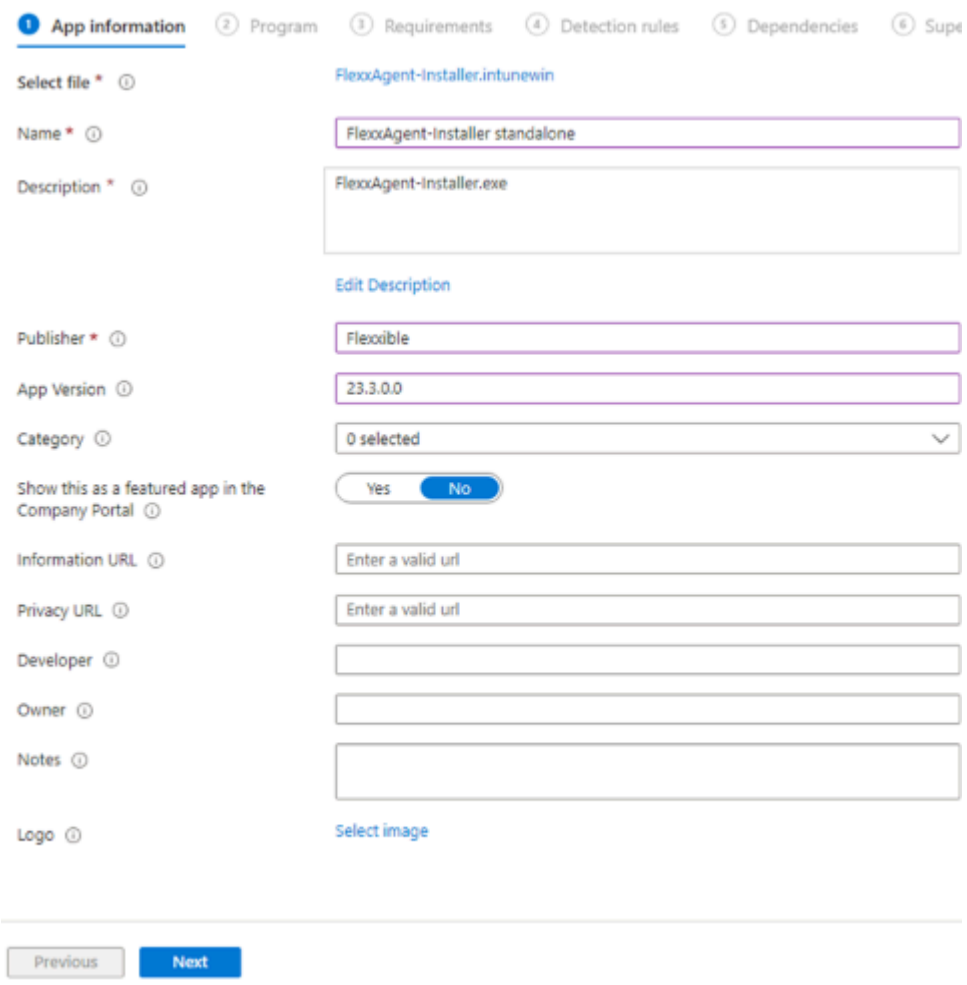
Copyright © 2024 Flexxible. Todos los derechos reservados.



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.

Copyright © 2024 Flexxible. Todos los derechos reservados.



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

    - Install command: `FlexxAgent-Installer.exe`

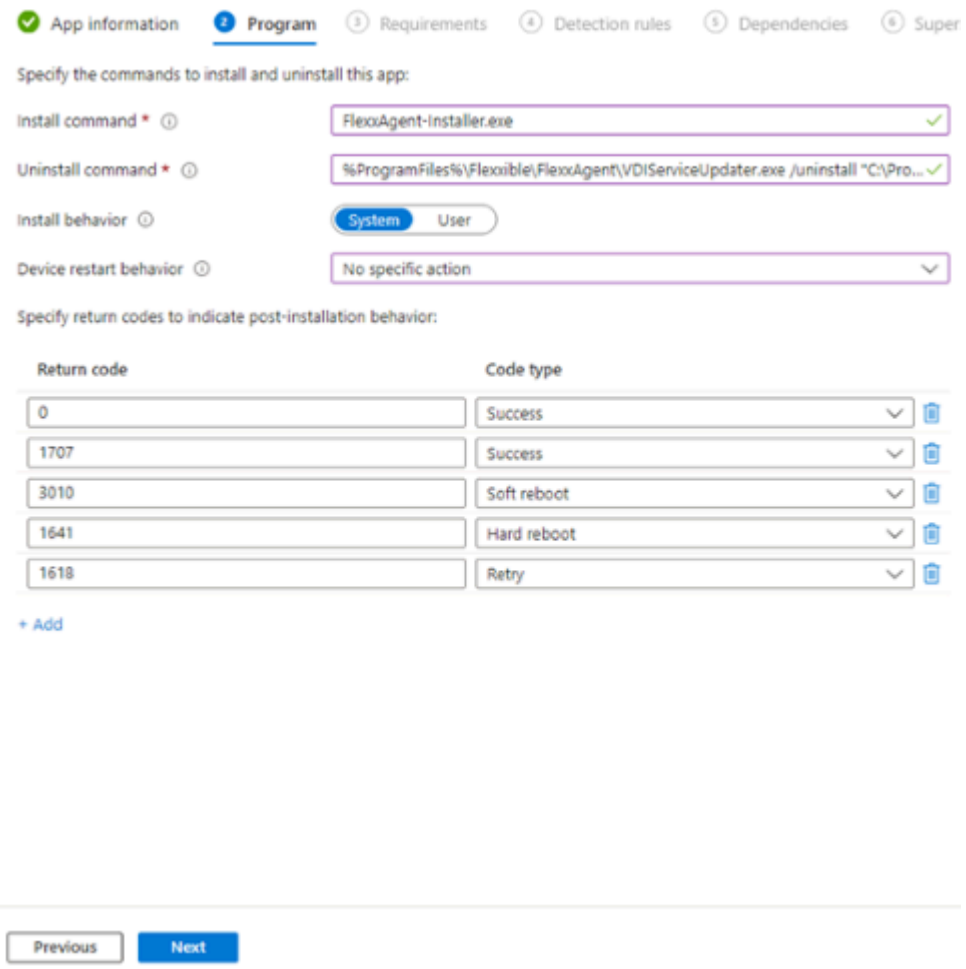
> Note: If necessary, proxy values could be entered in this command.

    - 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

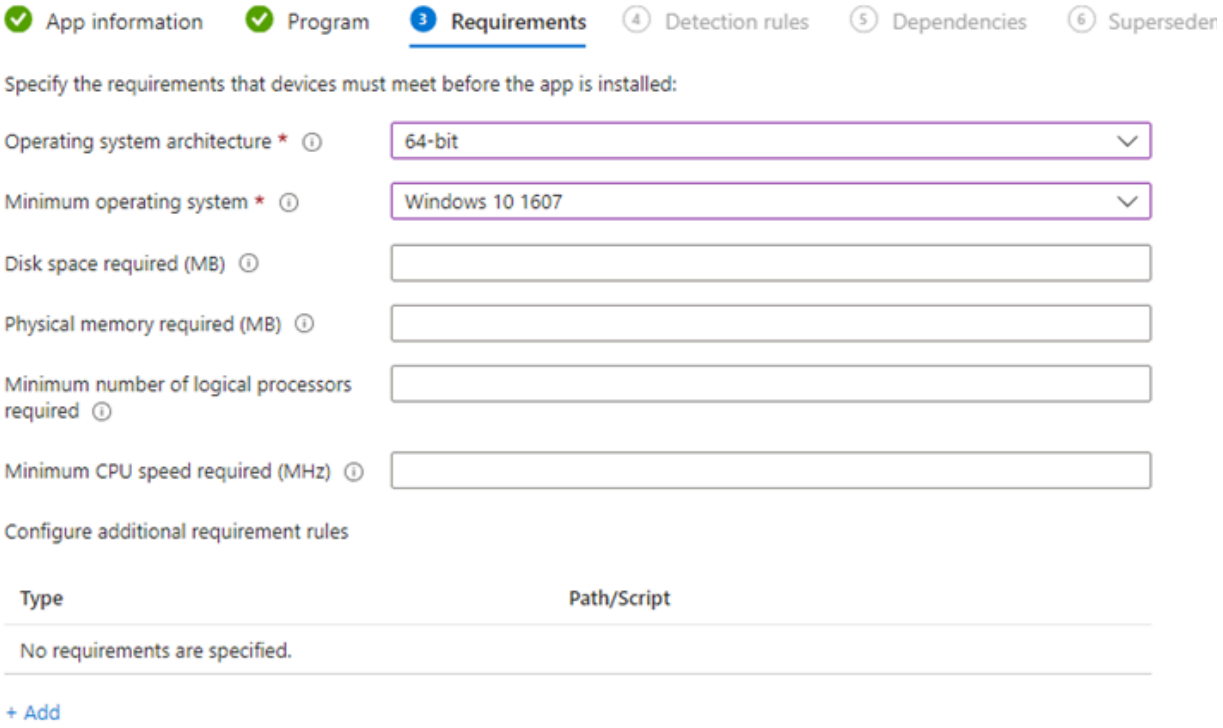
Copyright © 2024 Flexxible. Todos los derechos reservados.



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`.

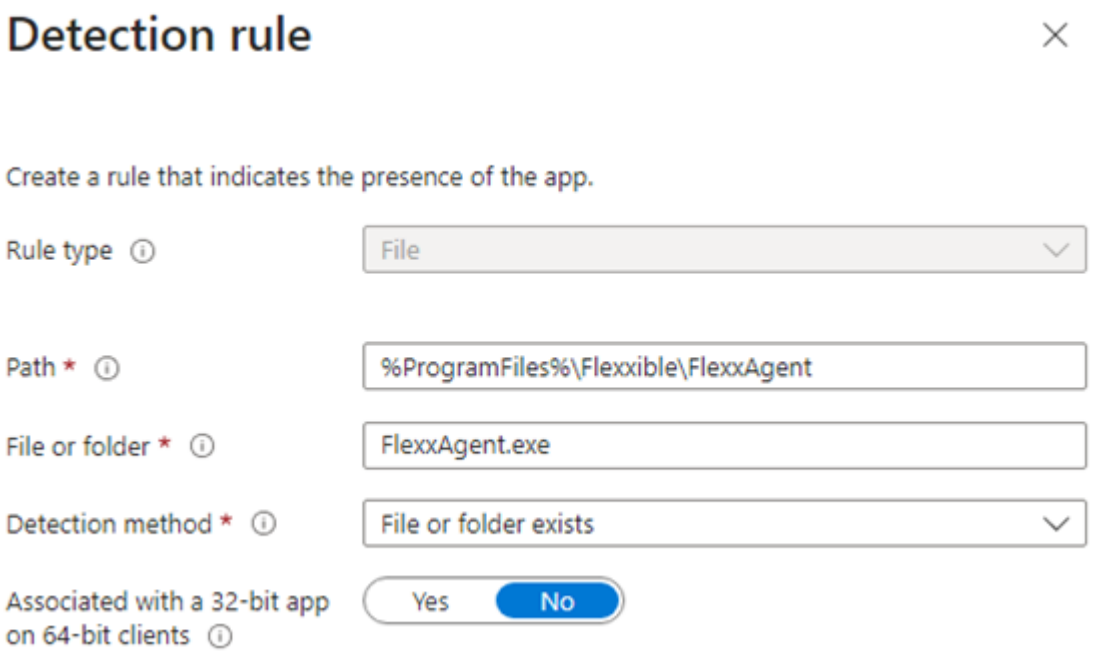
Copyright © 2024 Flexxible. Todos los derechos reservados.



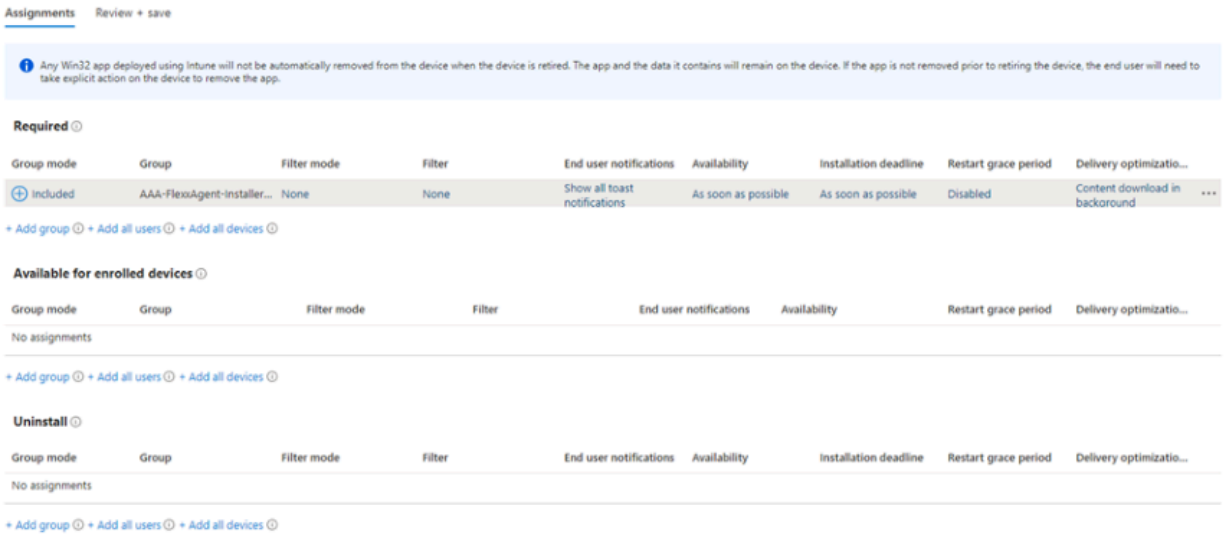
14. On the `Detection Rules` tab, select `Manually configure detection rules` and click on the link `+Add`. In the rule you are going to create, fill in the following fields:

    - 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

Copyright © 2024 Flexxible. Todos los derechos reservados.

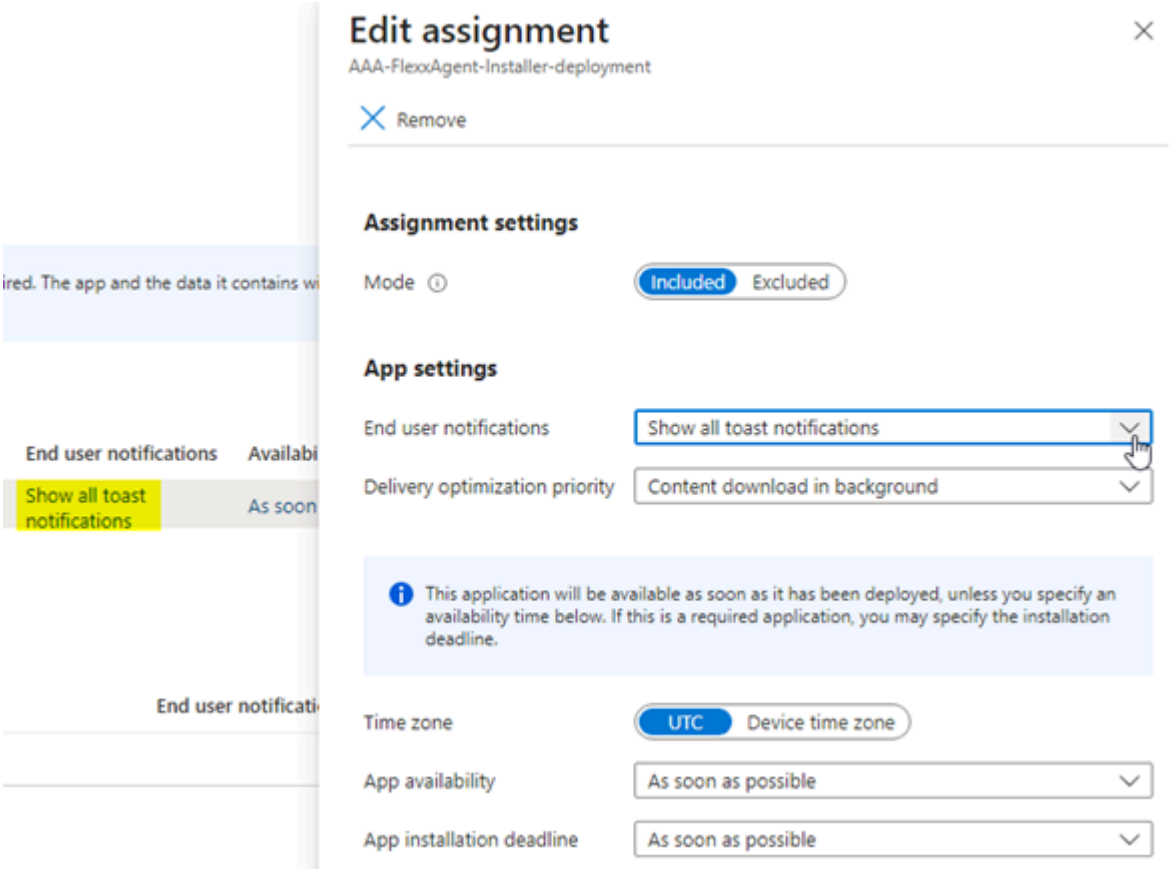


15. On the `Assignments` tab, create an Azure Entra ID security group containing the devices on which this package is to be installed.



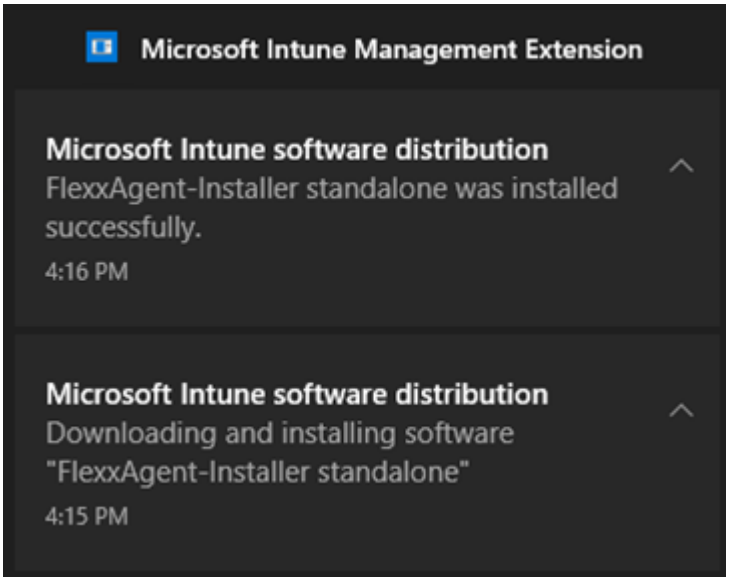
16. At this point, make sure to select the appropriate notification for the end user.

Copyright © 2024 Flexxible. Todos los derechos reservados.



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.



Copyright © 2024 Flexxible. Todos los derechos reservados.

FlexxAgent / Guides / Deploy FlexxAgent for Android with Microsoft Intune

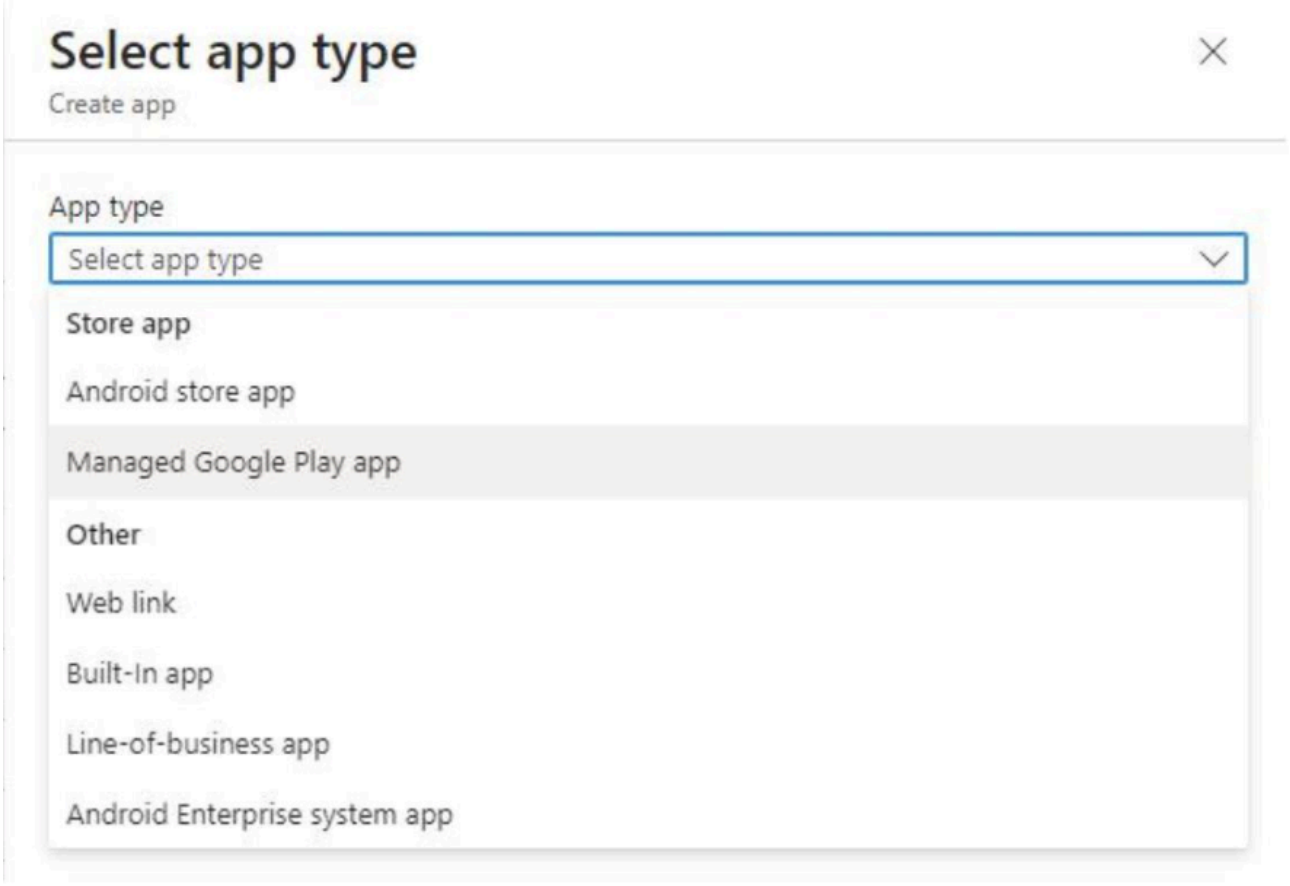
To deploy FlexxAgent on Android devices with Microsoft Intune, the latter must have an active connection with Android Enterprise. The linkage should be established by following this procedure.

Activate app visibility in Google Play

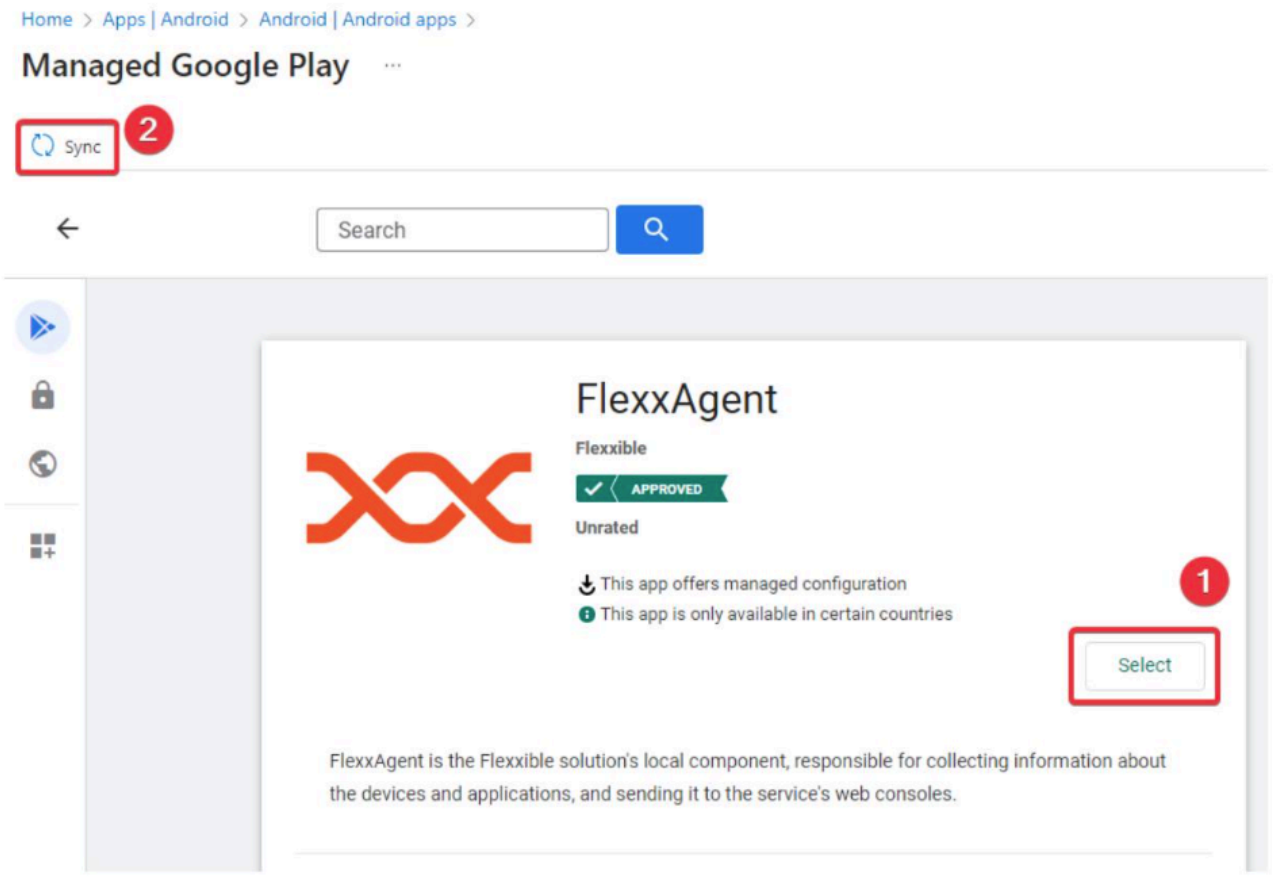
Flexxible will provide access to FlexxAgent in the Managed Google Play console, along with the necessary configuration data. For this, the client must provide Flexxible with the *Name* and *ID* of their Managed Google Play.

App configuration in Microsoft Intune

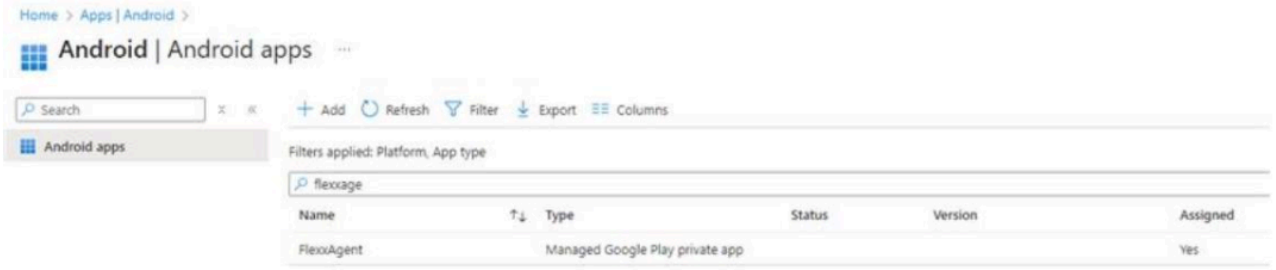
1. Select the app and sync it:



Copyright © 2024 Flexxible. Todos los derechos reservados.

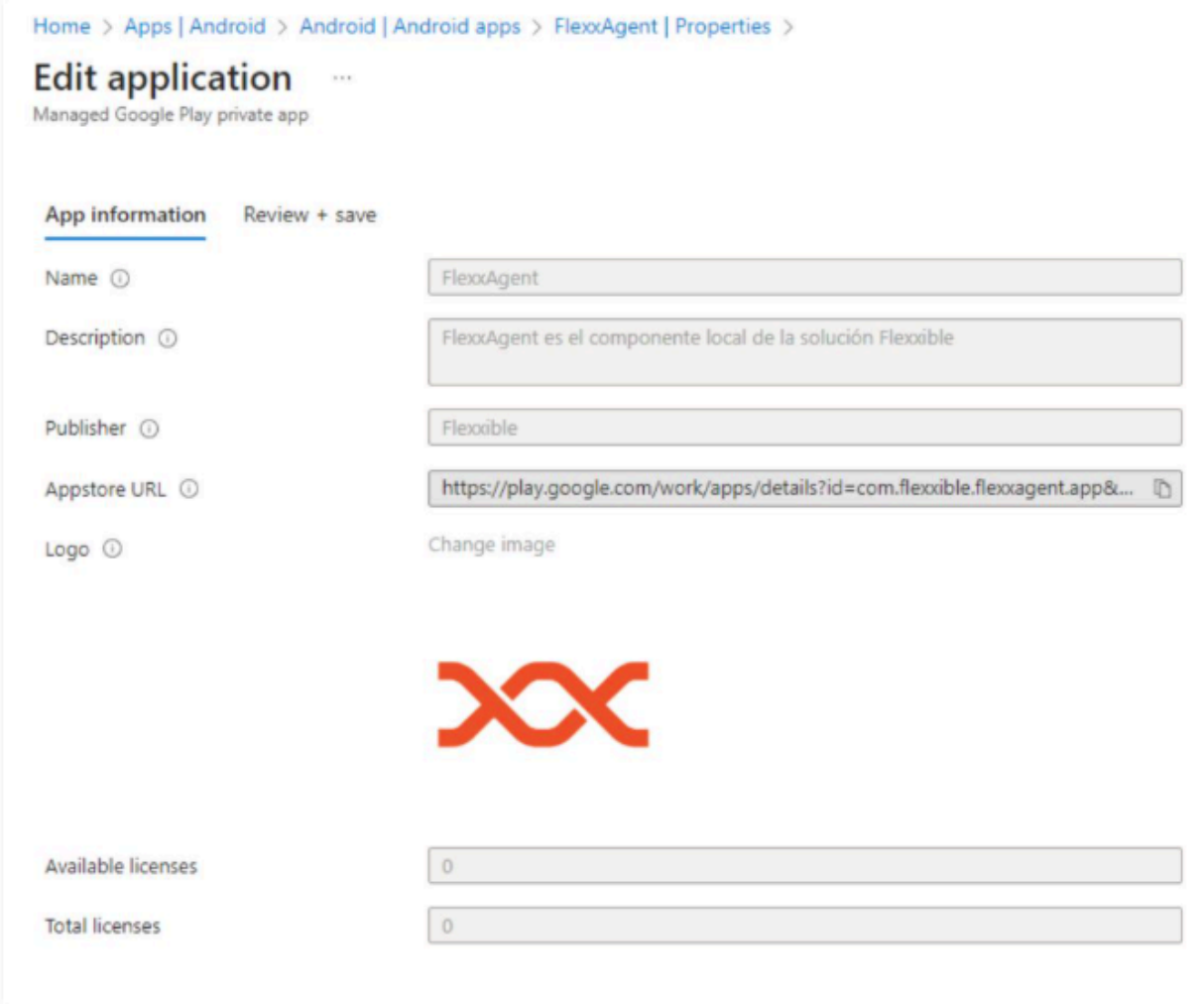


2. FlexxAgent will appear in the app list:



3. Configure the app:

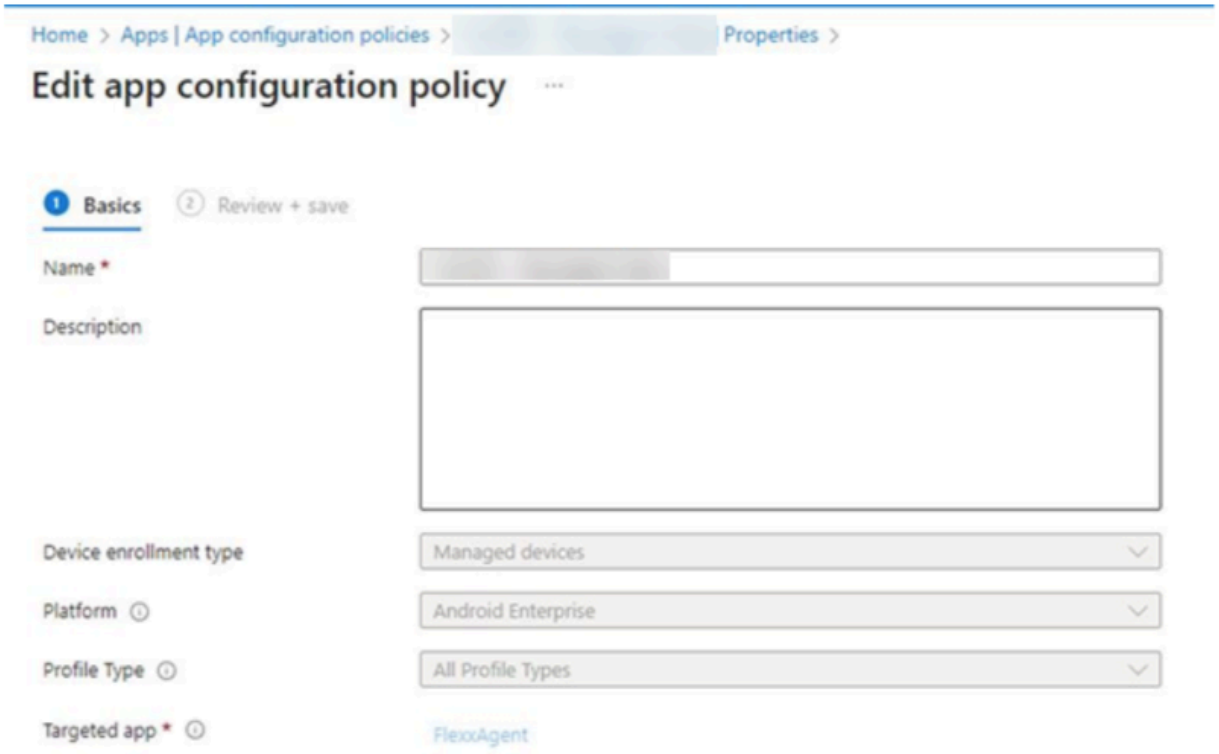
Copyright © 2024 Flexxible. Todos los derechos reservados.



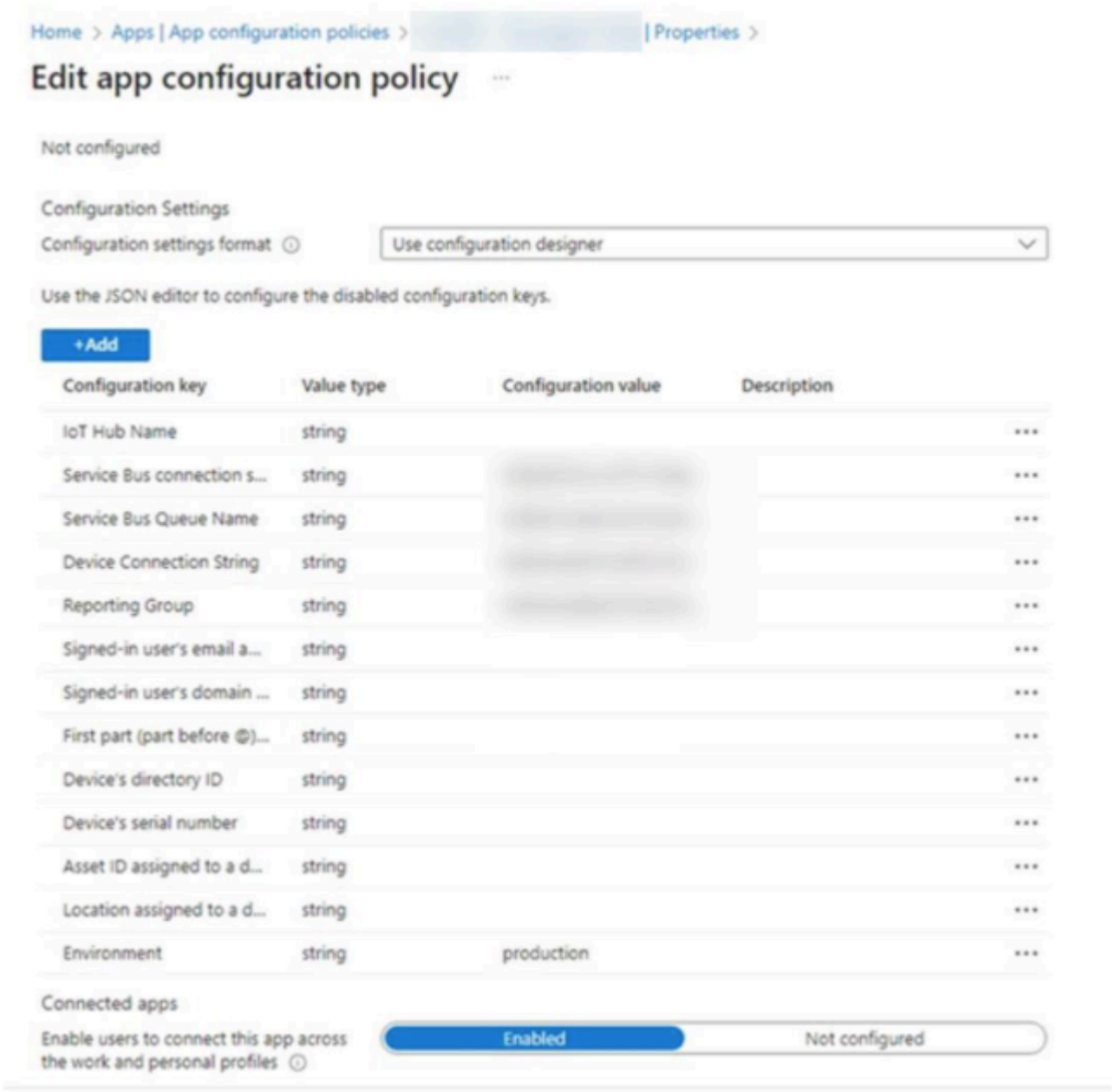
Configuration policy management

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

Copyright © 2024 Flexxible. Todos los derechos reservados.



Copyright © 2024 Flexxible. Todos los derechos reservados.



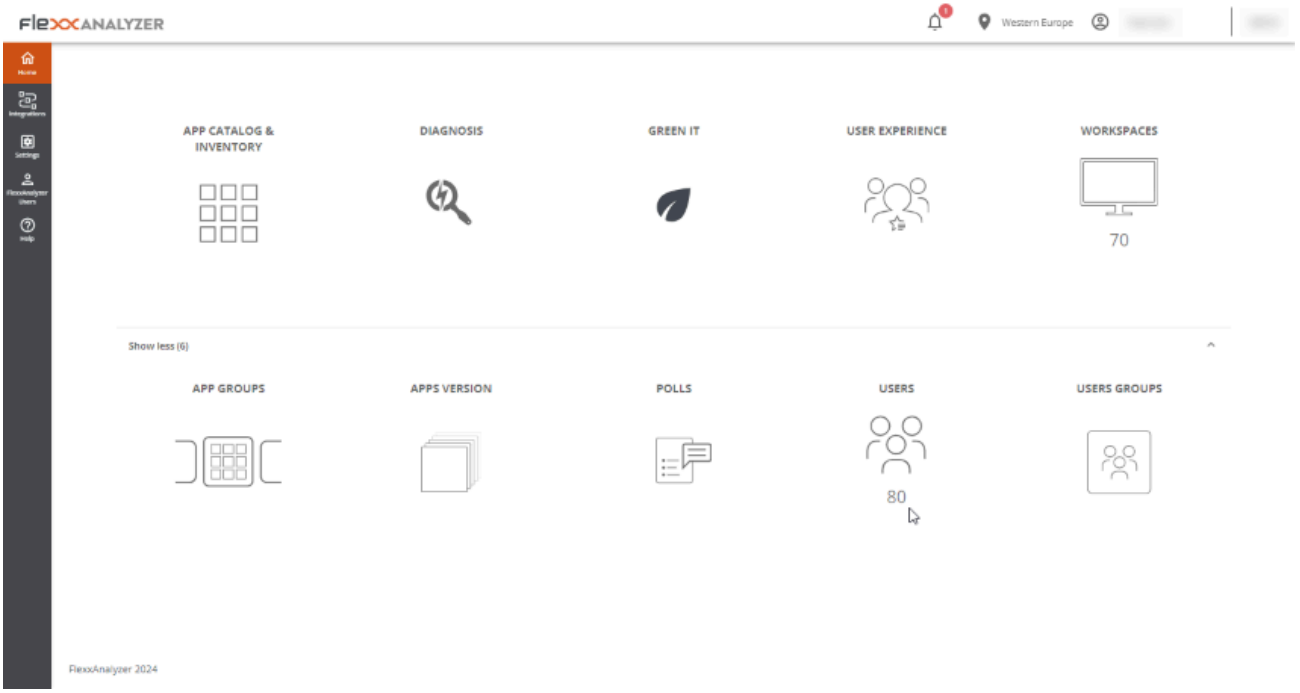
INFO

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

Copyright © 2024 Flexxible. Todos los derechos reservados.

Analyzer

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



Included tools

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

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

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

Tools included in Analyzer:

- **App Catalog & Inventory.** Offers an inventory of applications and their versions within the organization.

Copyright © 2024 Flexxible. Todos los derechos reservados.

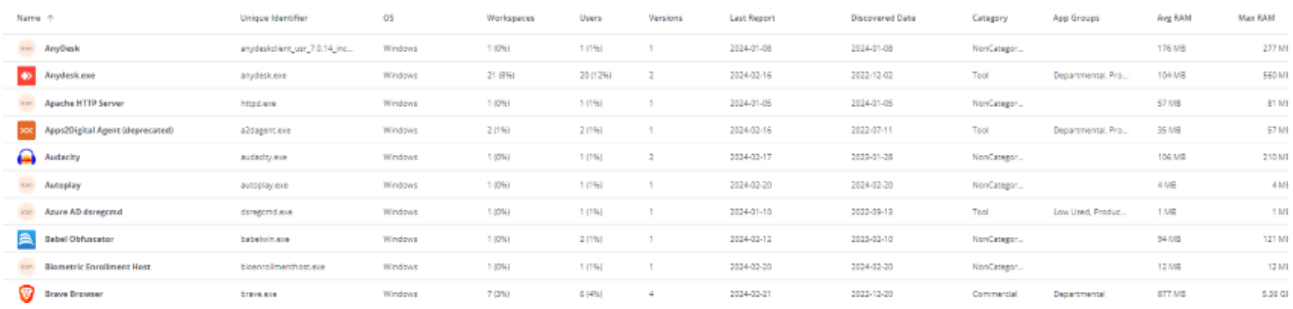
- **Diagnosis.** Enables a diagnostic view and allows you to see the details of resource and application usage by devices in configurable time slots.
- **Green IT.** Allows evaluating the carbon footprint generated by printing and the electrical consumption of devices and their peripherals.
- **User 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.

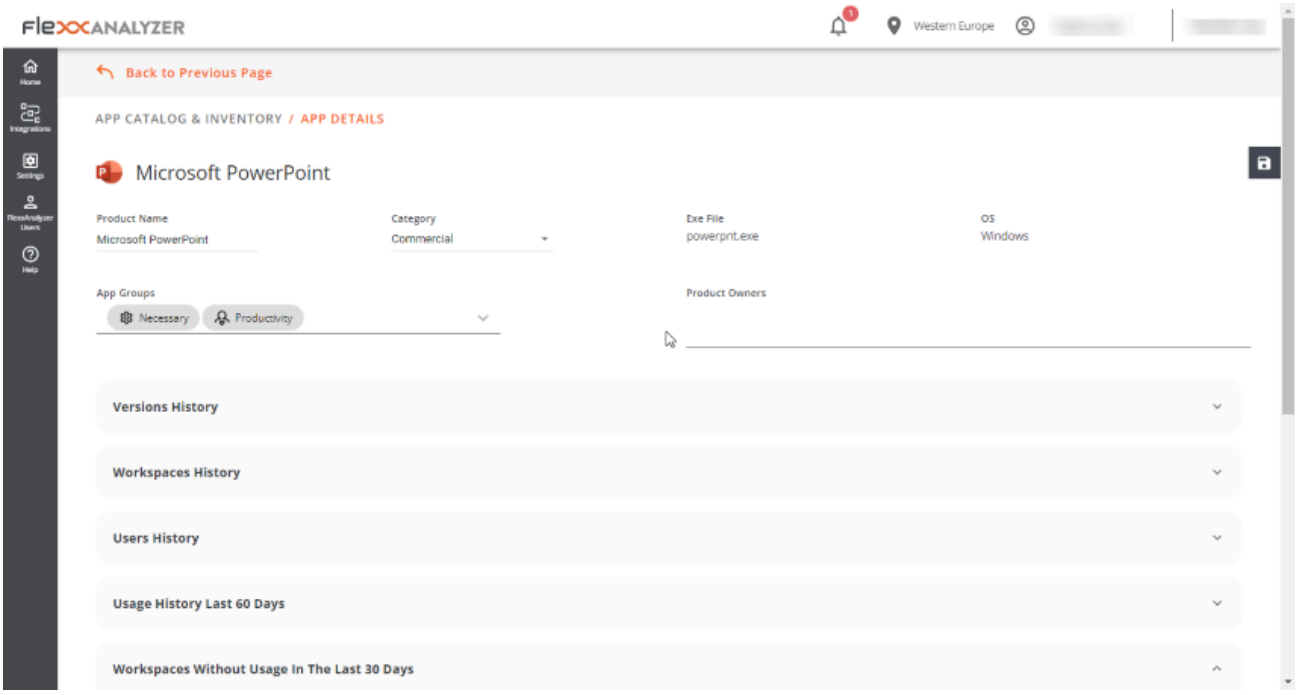
Results will appear in a list format, where you can make use of filters or navigate between different result pages.



Copyright © 2024 Flexxible. Todos los derechos reservados.

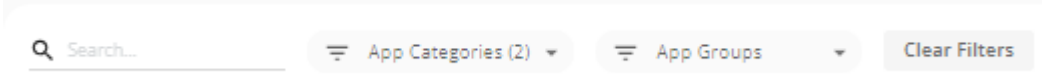
Detail Views

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

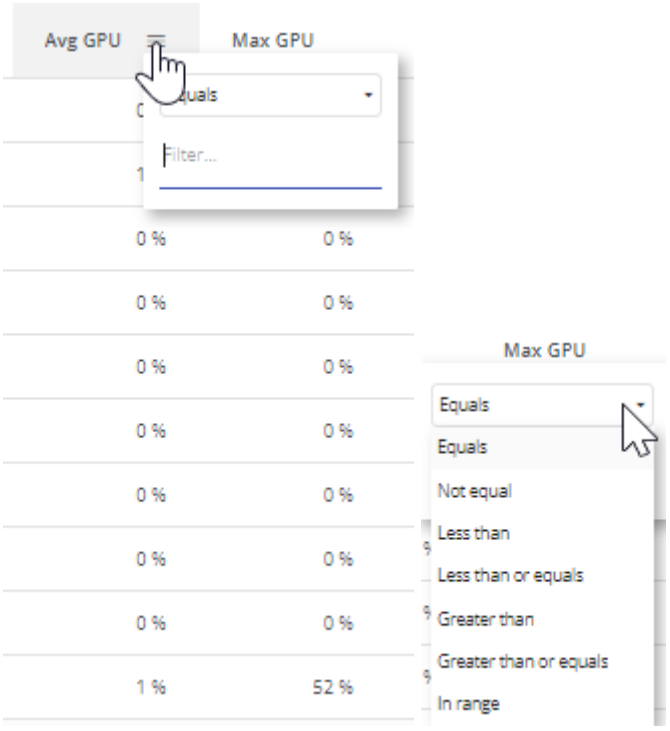
From any of the list views, you can access search options that allow locating a record within all results offered in the list.



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.

Copyright © 2024 Flexxible. Todos los derechos reservados.



Logical operators that can be operated with:

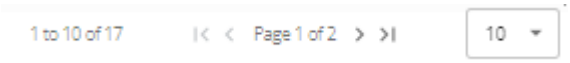
Condition	Caption
Equal to	The condition for filtering results must be equal to the value stated.
Not equal to	The condition for filtering results must be different from the value stated.
Greater than	The condition for filtering results must be greater than the value stated.
Less than	The condition for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

Copyright © 2024 Flexxible. Todos los derechos reservados.

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

Page navigation

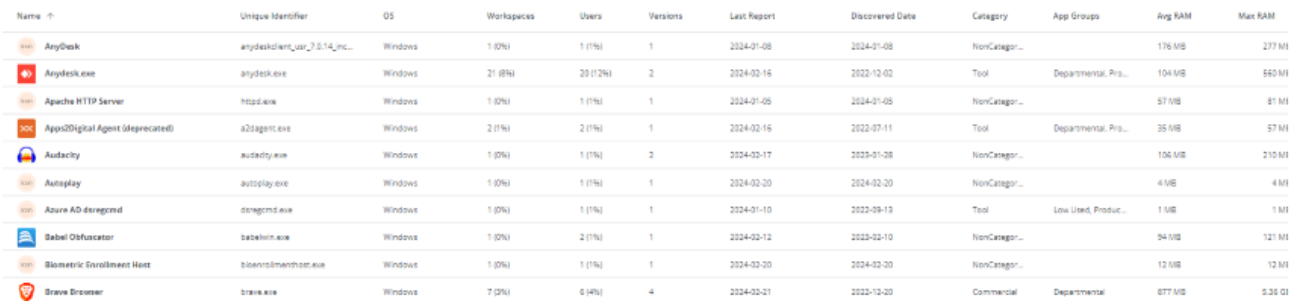
At the bottom of any list view is the page navigator. It's useful for navigating between pages of results.



Copyright © 2024 Flexxible. Todos los derechos reservados.

Analyzer / App Catalog & Inventory

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



List view

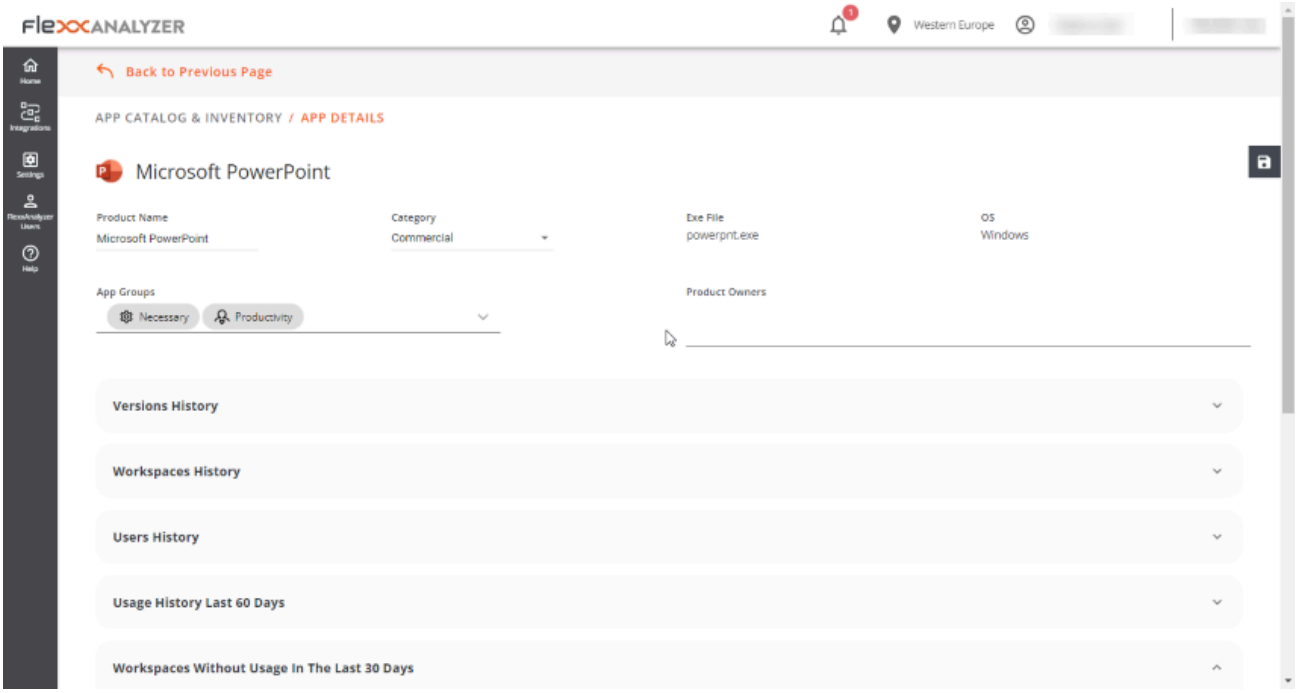
In the list view you can see the following information:

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

Detail view

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

Copyright © 2024 Flexxible. Todos los derechos reservados.



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

Copyright © 2024 Flexxible. Todos los derechos reservados.

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

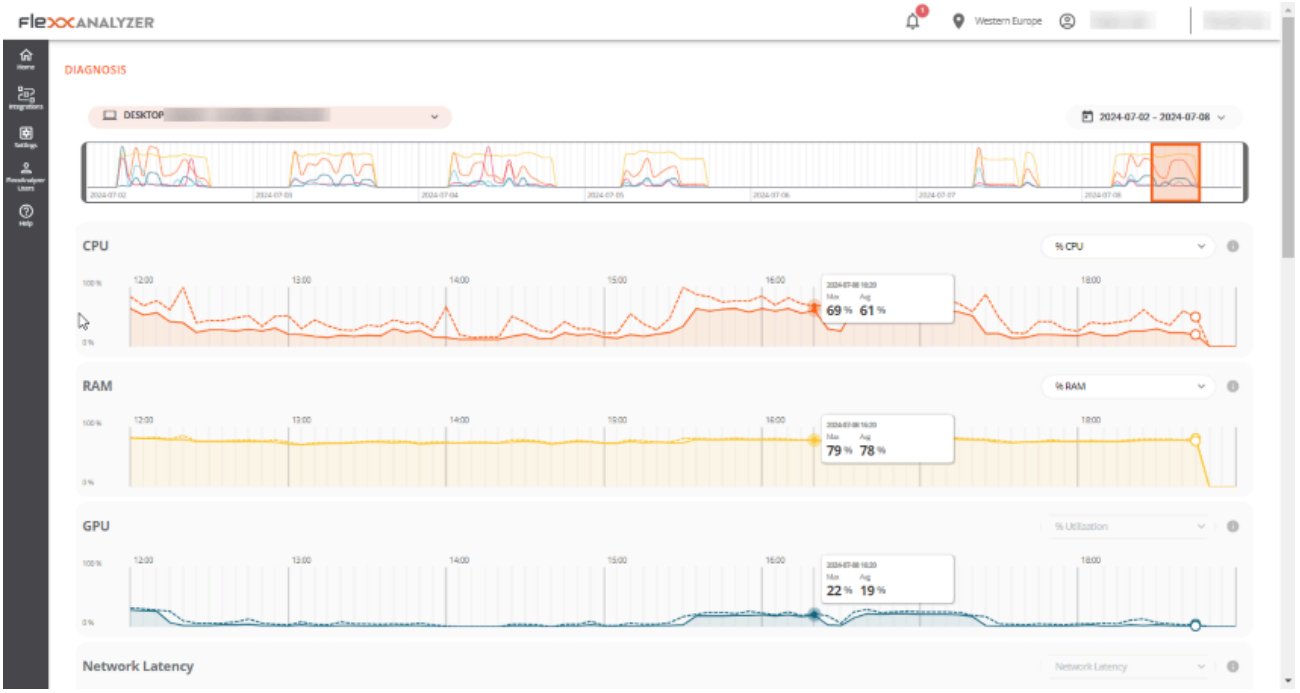
This list shows the devices that have the application installed but have had no usage in the last 30 days, which helps identify opportunities for license optimization. Includes:

- Device Name
- Installation date
- Last detection report

Copyright © 2024 Flexxible. Todos los derechos reservados.

Analyzer / Diagnosis

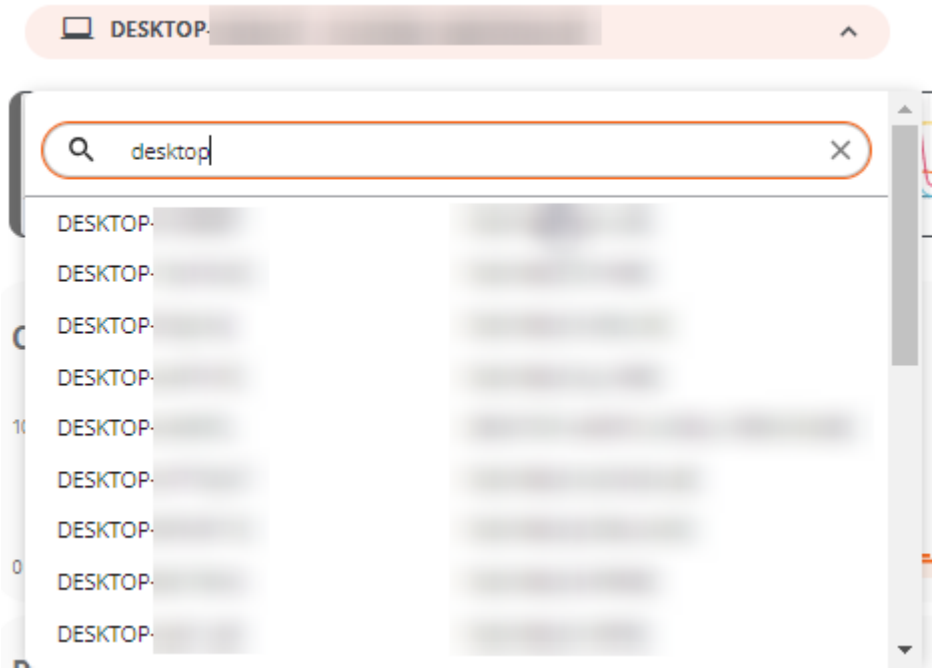
From the `Diagnosis` option, you can perform a detailed analysis of a device's resource consumption, as well as the applications and processes used in the user's session.



Web Interface

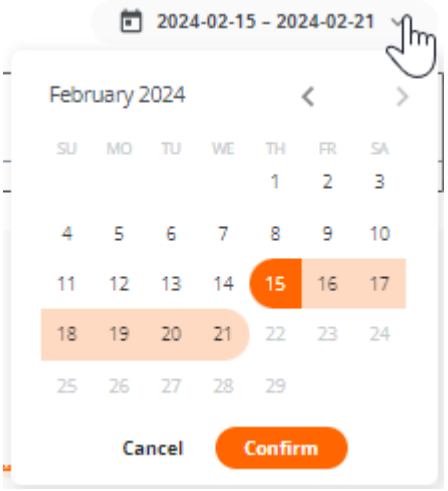
From the `Diagnosis` dropdown menu, you can search for a device and the user session you want to analyze. If you start typing a username, the dropdown menu will filter to show only devices that match that name.

Copyright © 2024 Flexxible. Todos los derechos reservados.



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

Copyright © 2024 Flexxible. Todos los derechos reservados.

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

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

Copyright © 2024 Flexxible. Todos los derechos reservados.

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

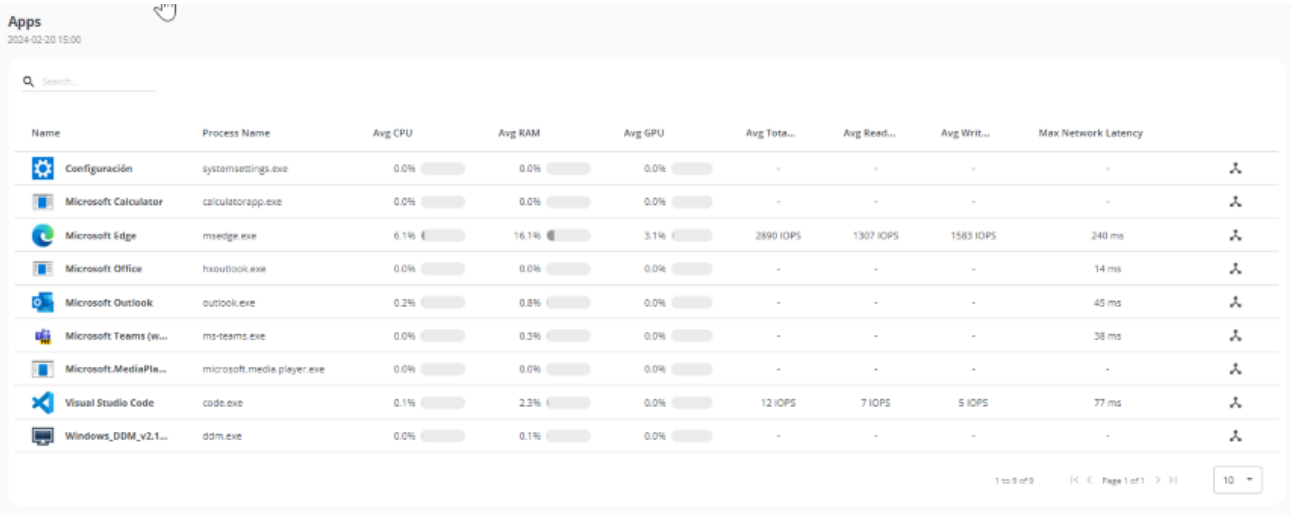
Disk Usage

- **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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

Analyzer / Carbon footprint analysis

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

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

Web Interface

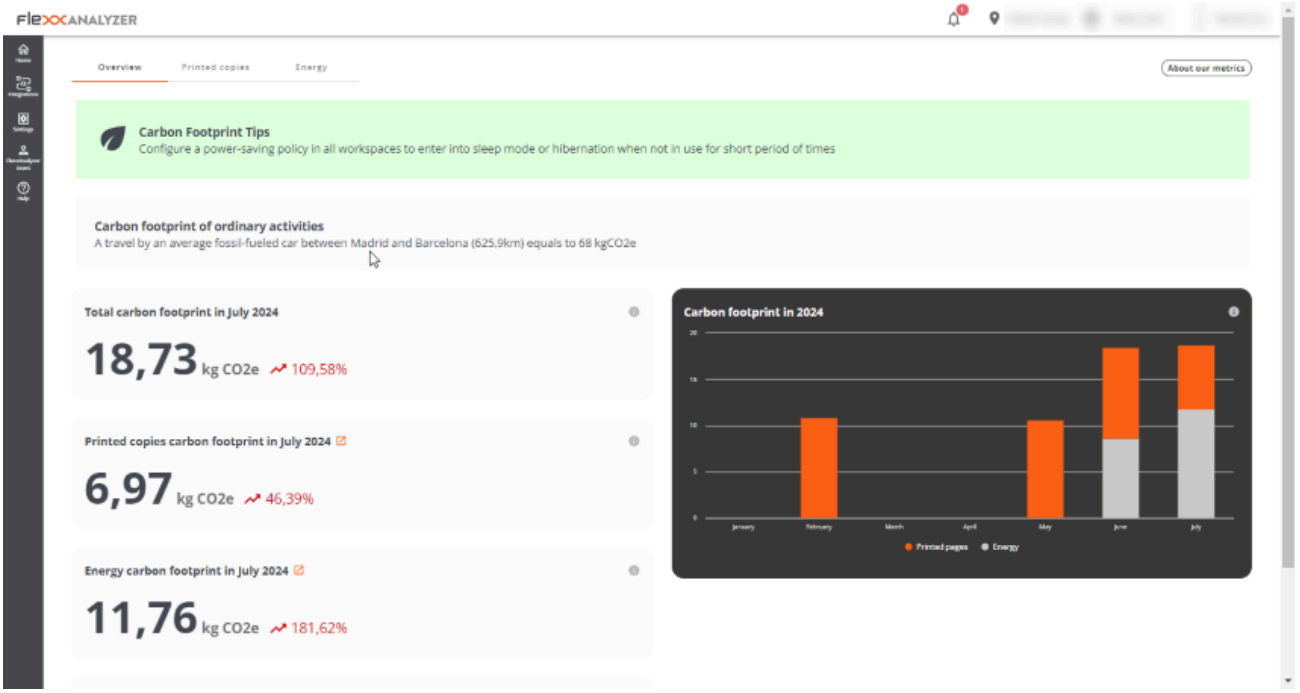
This dashboard view is divided into three tabs:

- **Overview.** 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

Copyright © 2024 Flexxible. Todos los derechos reservados.



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

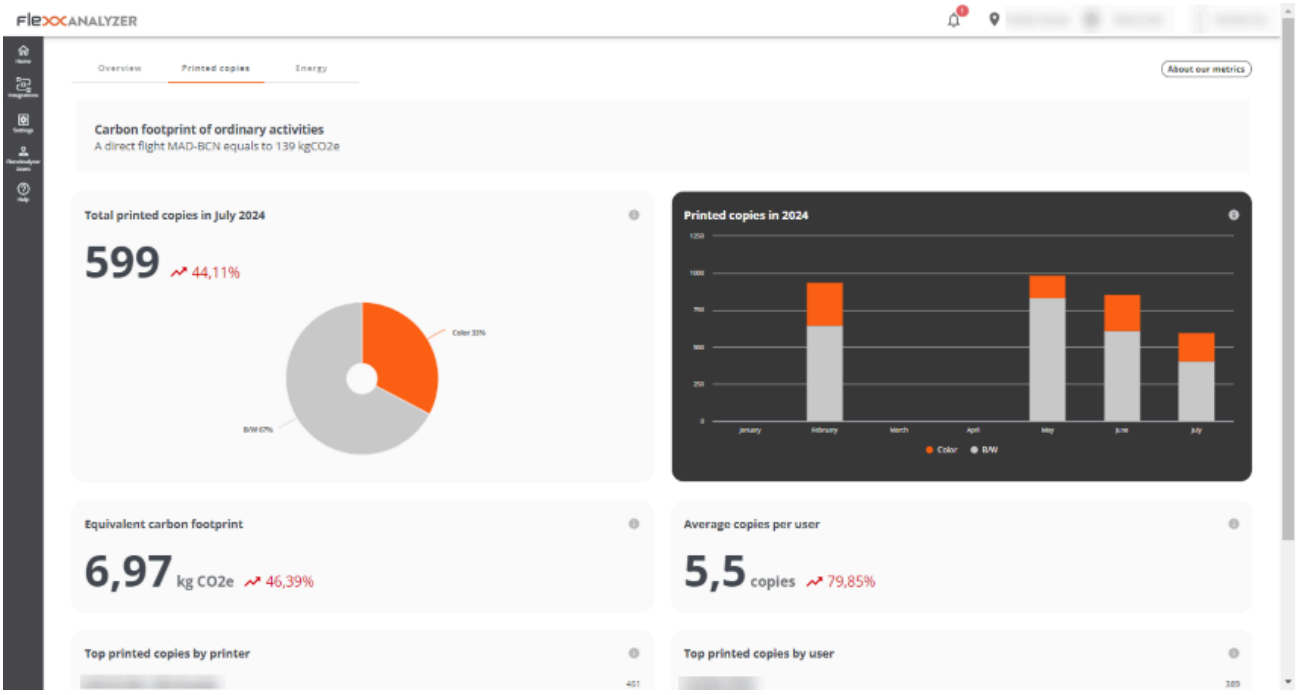
The adoption of Green IT practices for the management and optimization of resource usage in the field of printing involves taking measures that lead to a reduction in paper and energy consumption, as well as the carbon footprint associated with printing devices.

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:

Copyright © 2024 Flexxible. Todos los derechos reservados.

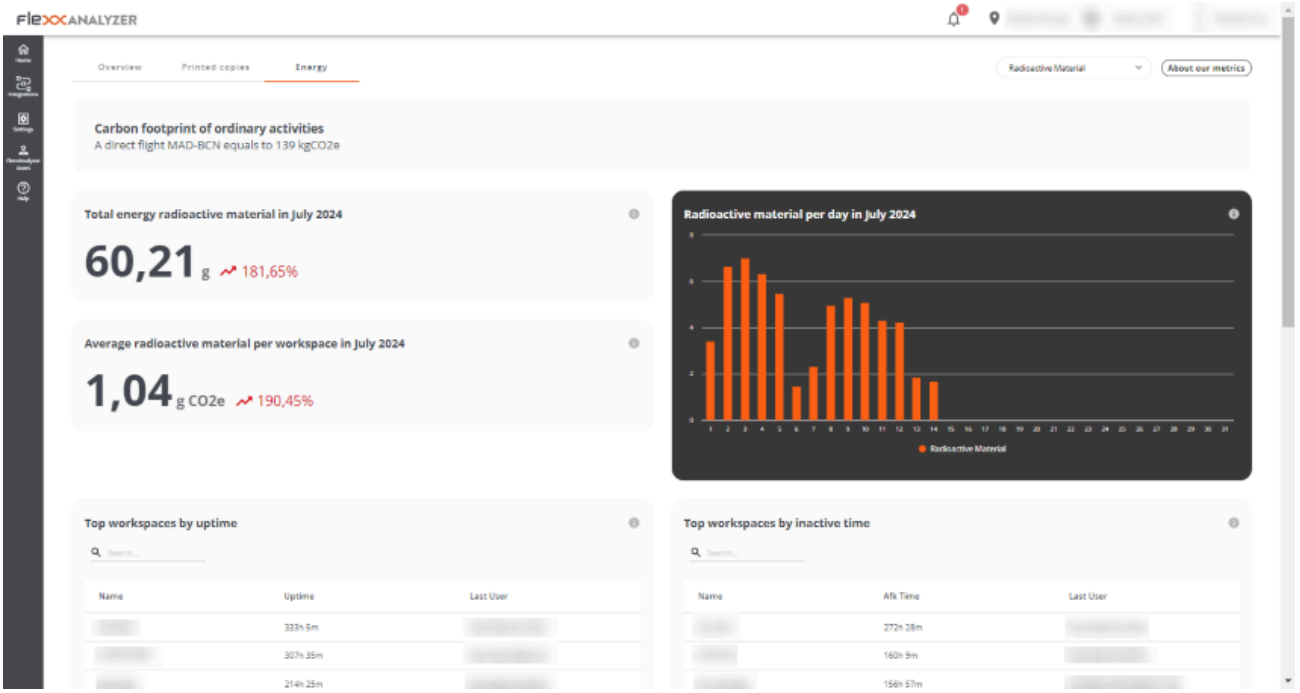
- 10 g of CO2e per A4 black and white copy
- 15 g of CO2e per A4 color copy



- **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

Copyright © 2024 Flexxible. Todos los derechos reservados.



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.

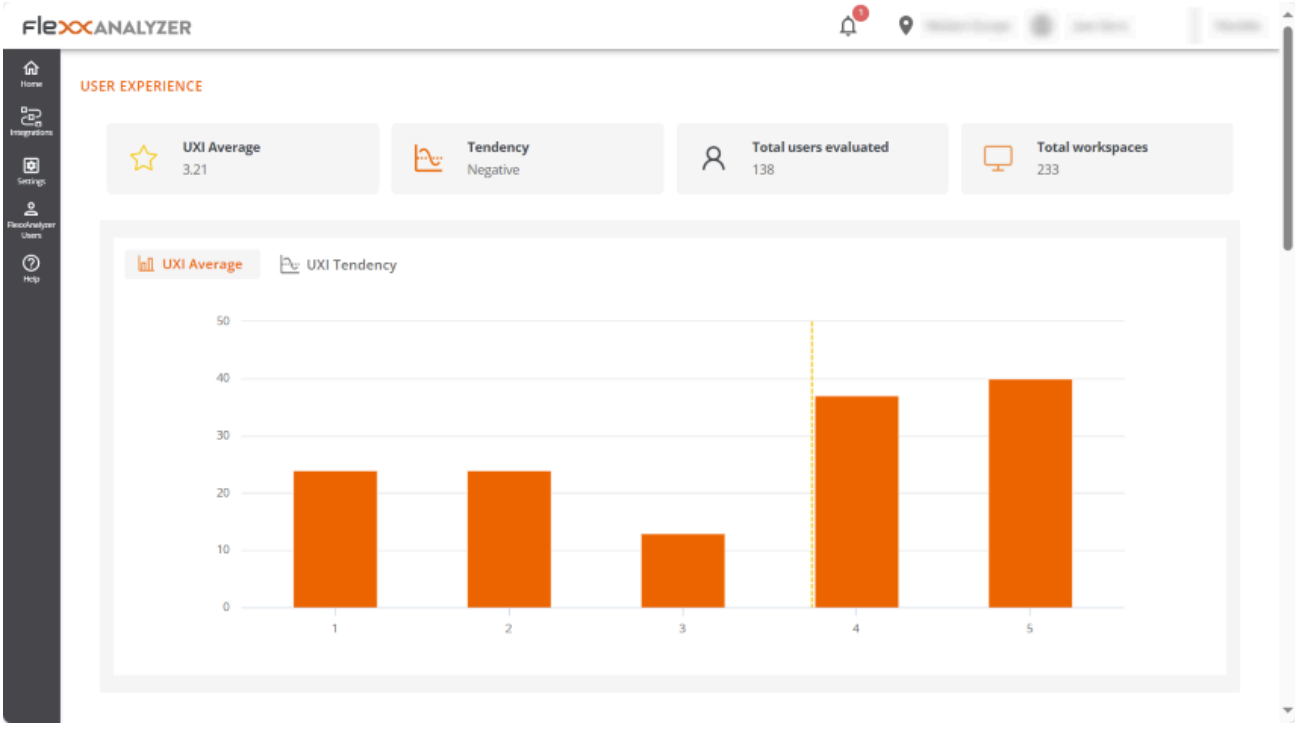
Copyright © 2024 Flexxible. Todos los derechos reservados.

- **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).

Copyright © 2024 Flexxible. Todos los derechos reservados.

Analyzer / User experience

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



Basic concepts

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

- Workspace Reliability Index (WRI)
- User sentiment

Workspace Reliability Index (WRI)

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

Copyright © 2024 Flexxible. Todos los derechos reservados.

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	

Copyright © 2024 Flexxible. Todos los derechos reservados.

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	

Copyright © 2024 Flexxible. Todos los derechos reservados.

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

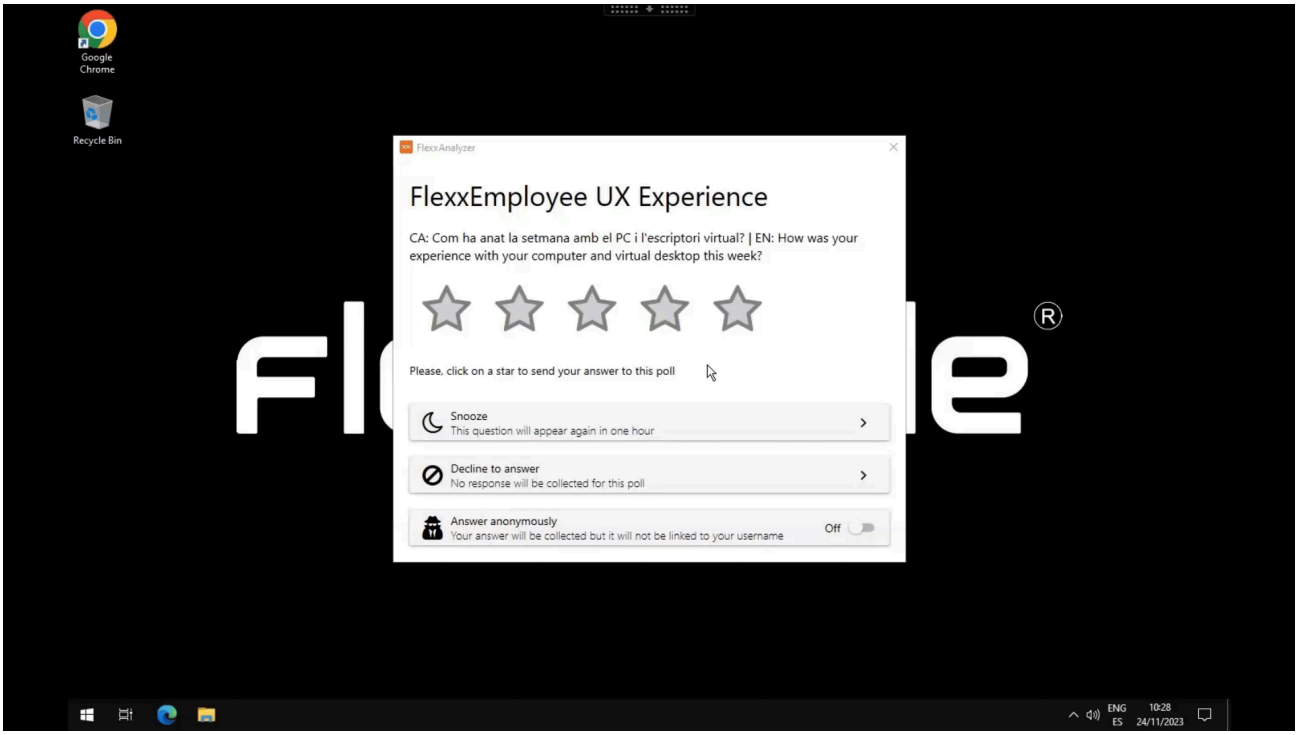
Where each severity deducts the following score from the initial 5-star rating.

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.



Web Interface

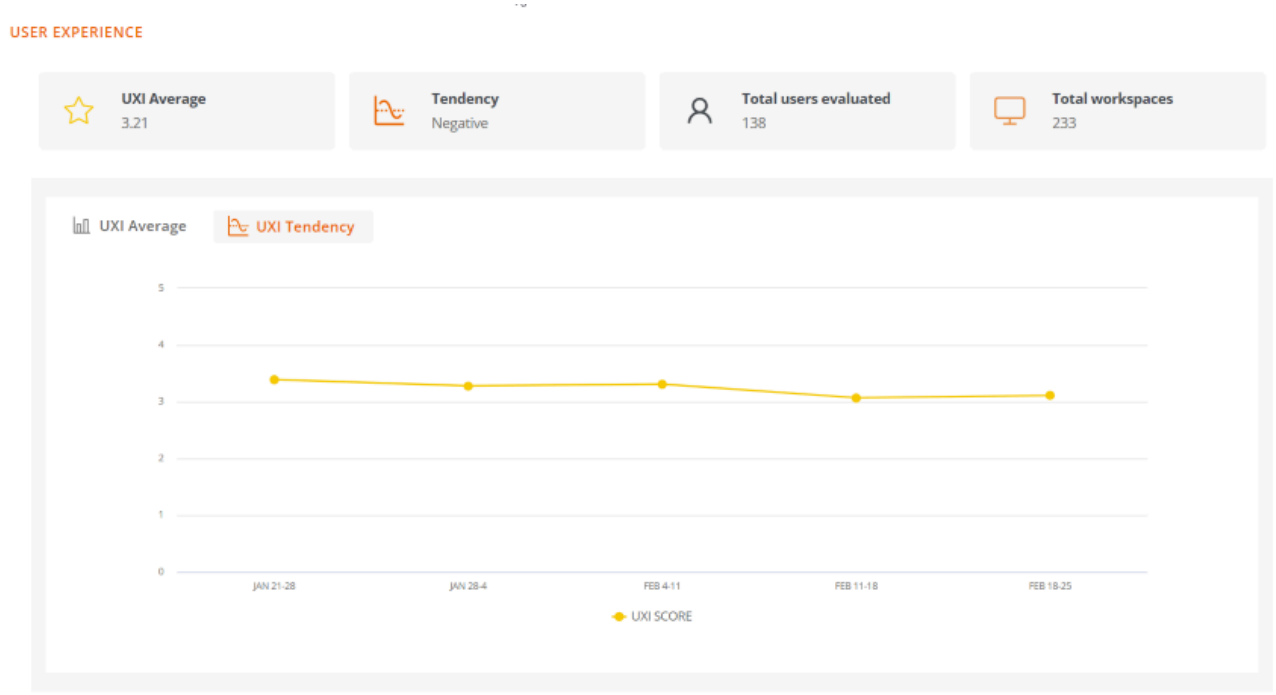
The dashboard view of the 'User Experience' section consists of the average information of all devices and users in the organization; it is calculated daily.

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.



Two charts are also included:

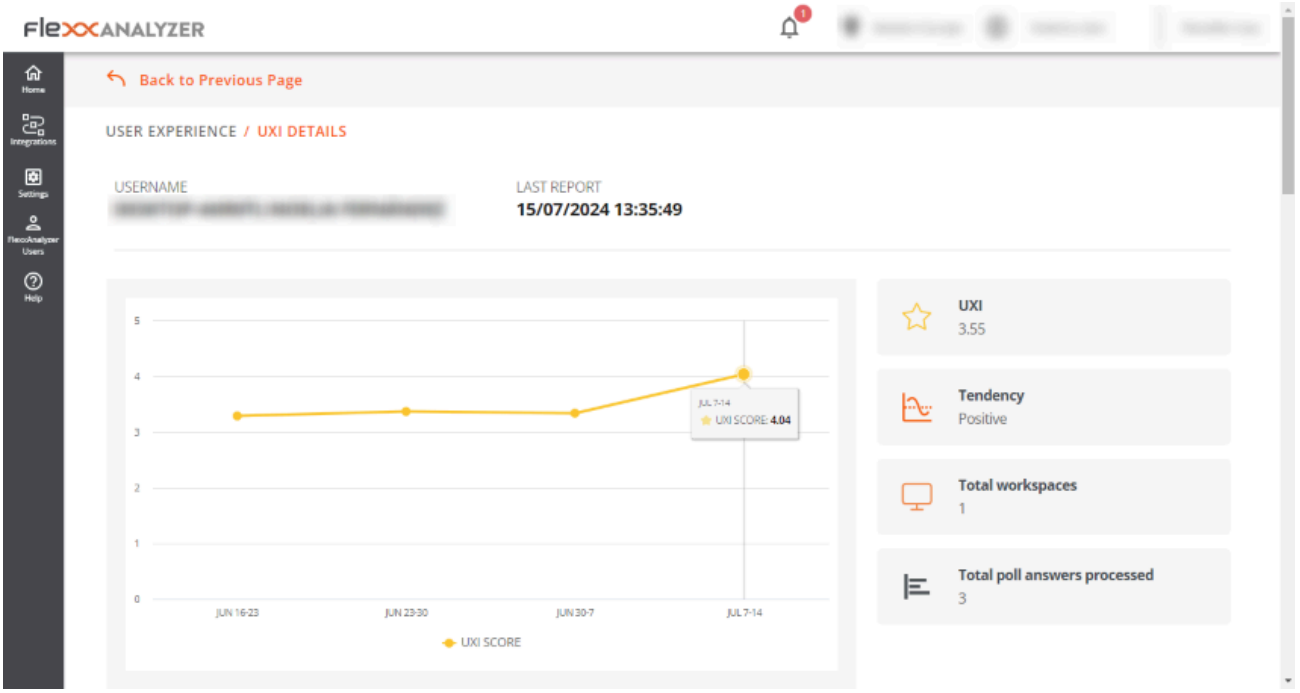
- **UXI Average.** Shows the distribution of users by UXI level, along with the organizational average.
- **UXI Tendency.** Shows the temporal evolution of the UXI for the last month.

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:

Copyright © 2024 Flexxible. Todos los derechos reservados.



- **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.

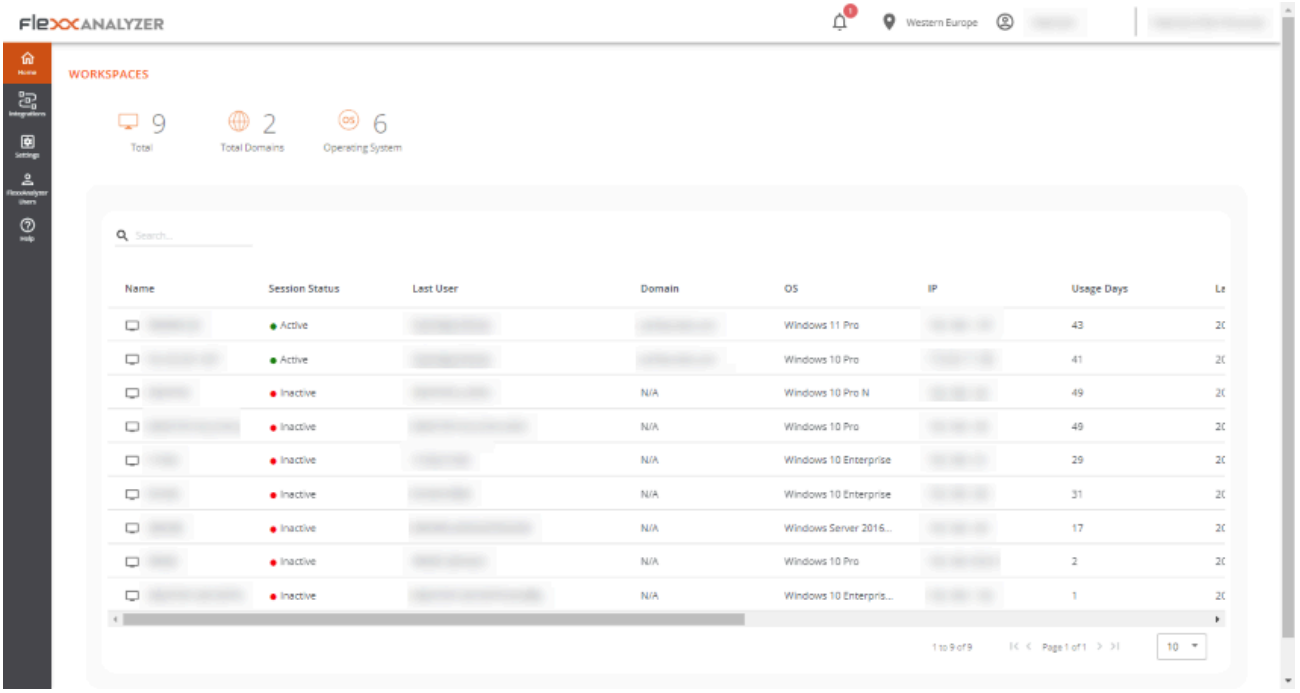
At the bottom of the screen, detailed information is included in a table format.

- **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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

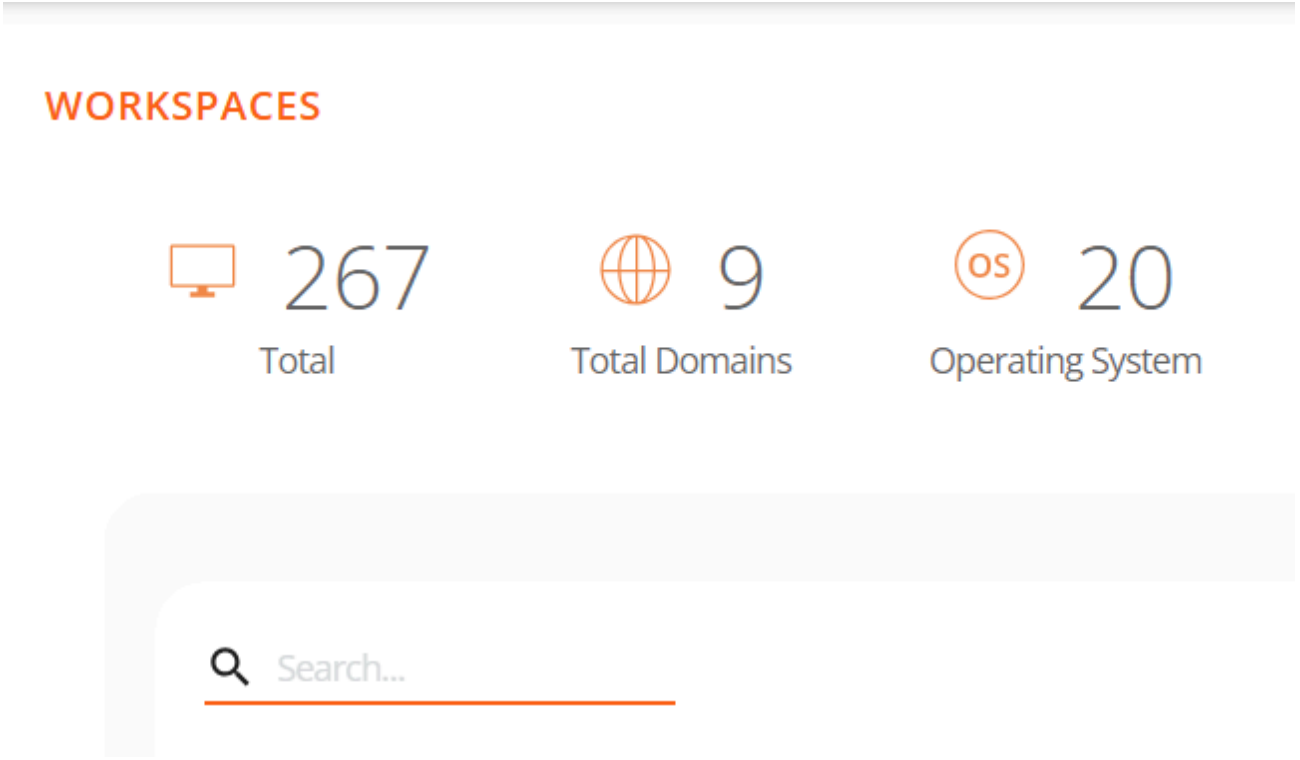
Analyzer / Workspaces in Analyzer

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



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

Copyright © 2024 Flexxible. Todos los derechos reservados.



Workspace detail

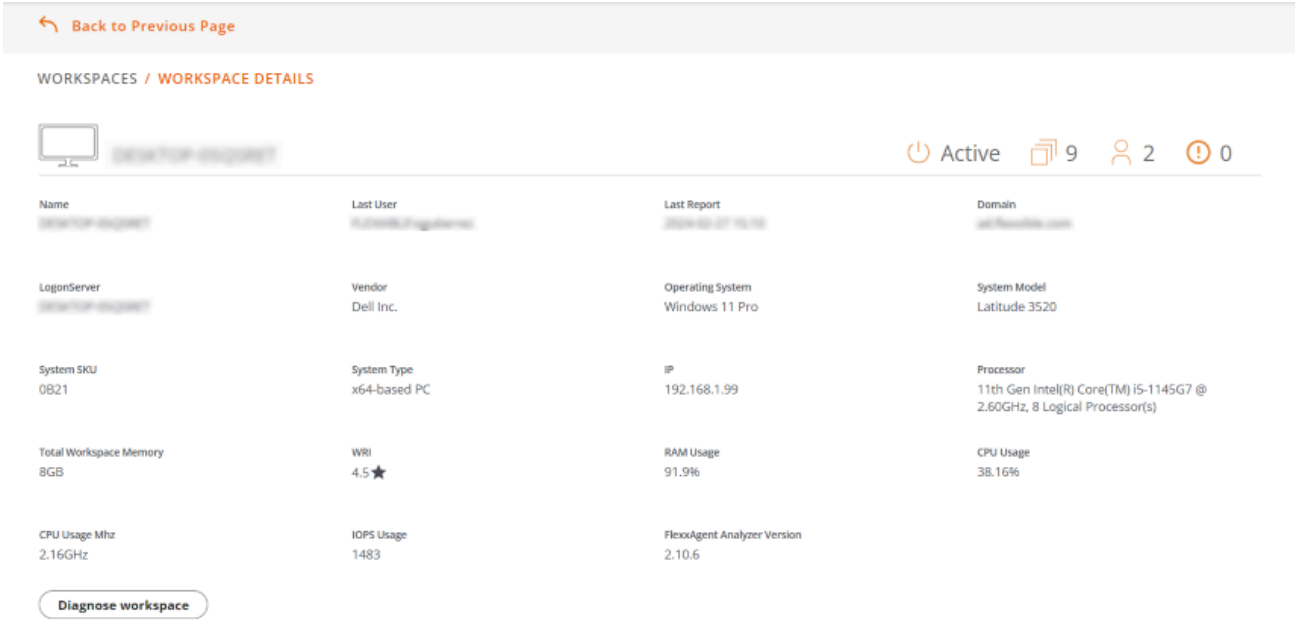
To access more precise data of a device, you must click on it in the table. Next, the user will see the following information:

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

Copyright © 2024 Flexxible. Todos los derechos reservados.

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

Copyright © 2024 Flexxible. Todos los derechos reservados.



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

Workspace analysis

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

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

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

Displays

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

Copyright © 2024 Flexxible. Todos los derechos reservados.

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.

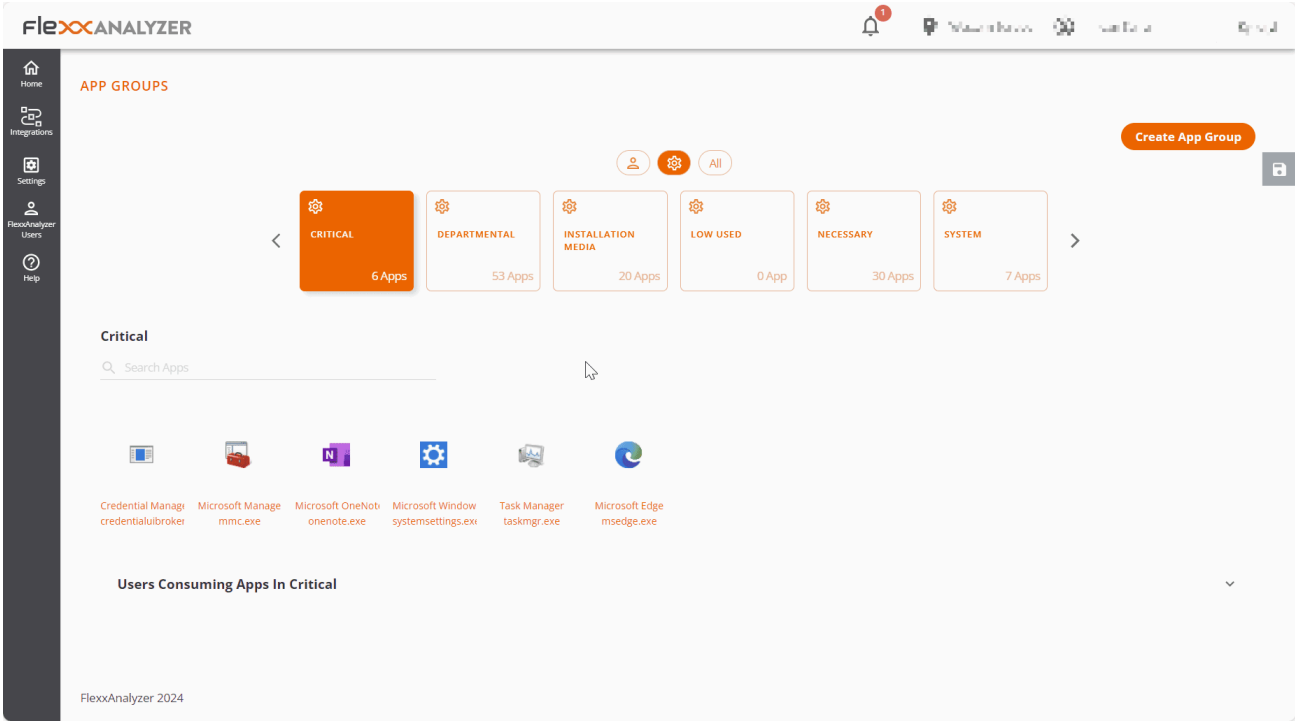
Usage history

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

Copyright © 2024 Flexxible. Todos los derechos reservados.

Analyzer / App Groups

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



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

Group Types

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

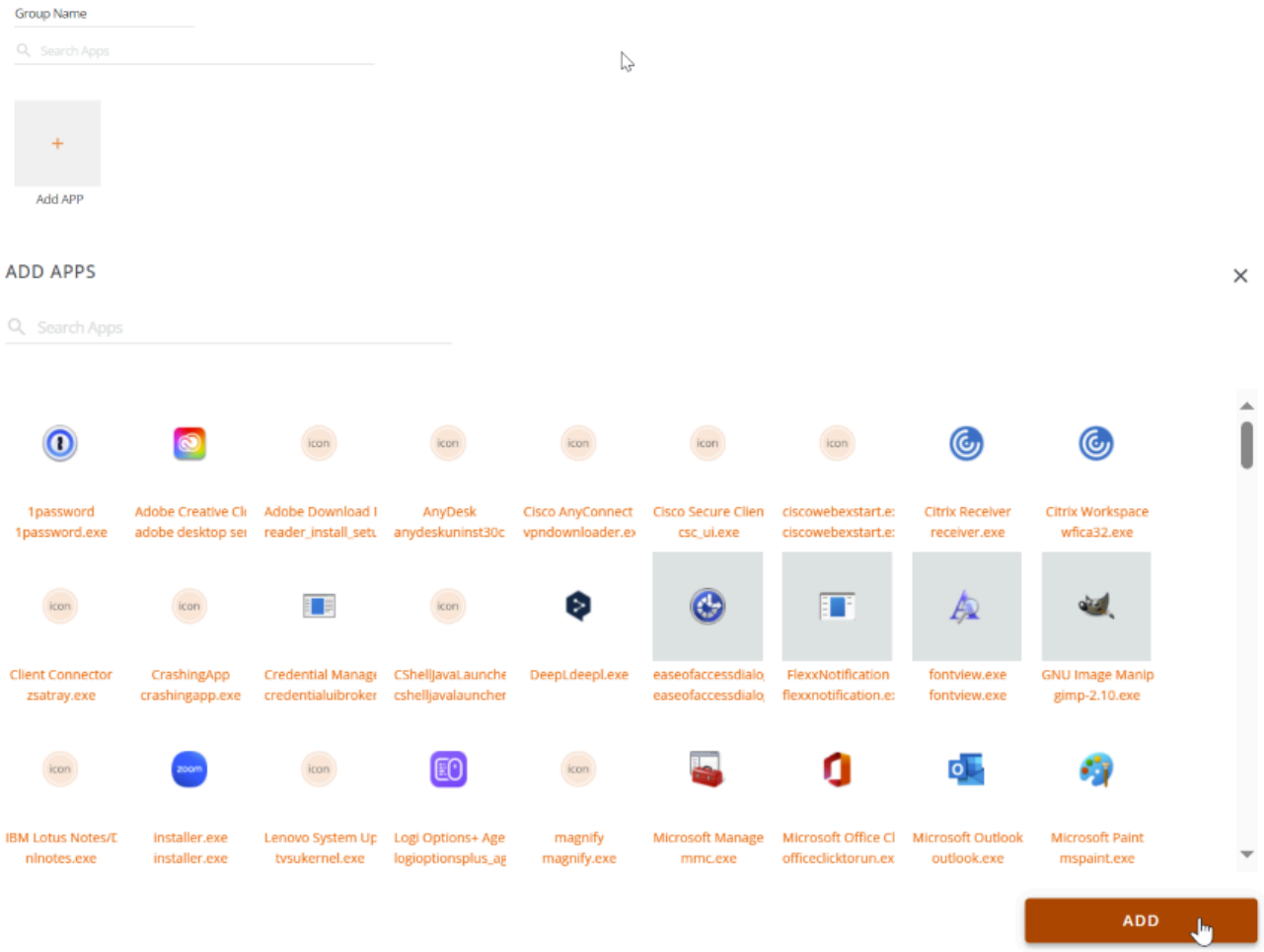
Copyright © 2024 Flexxible. Todos los derechos reservados.

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.

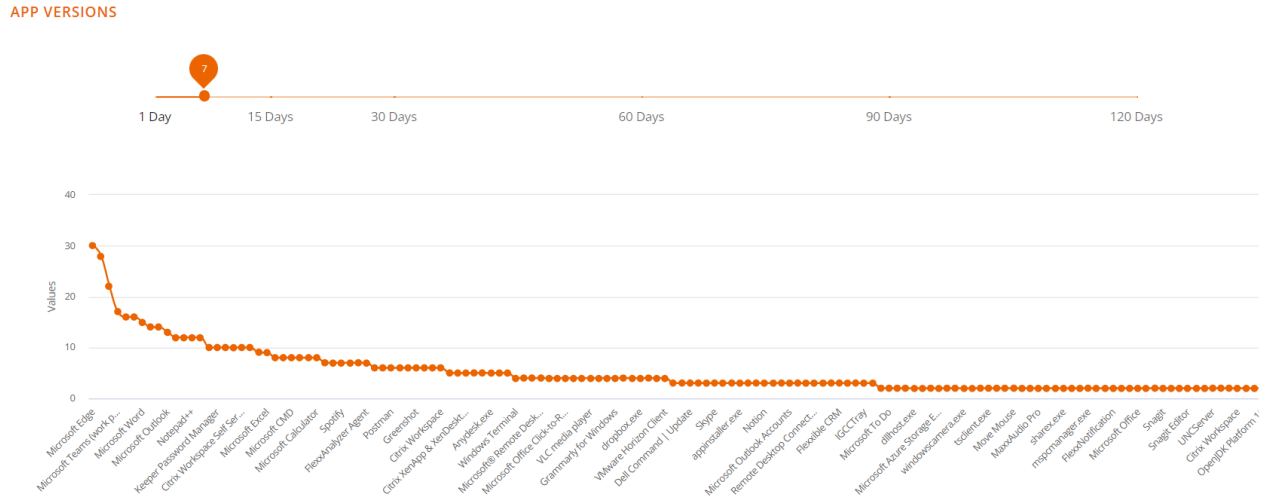
Copyright © 2024 Flexxible. Todos los derechos reservados.

Analyzer / App Versions

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

Graphical view

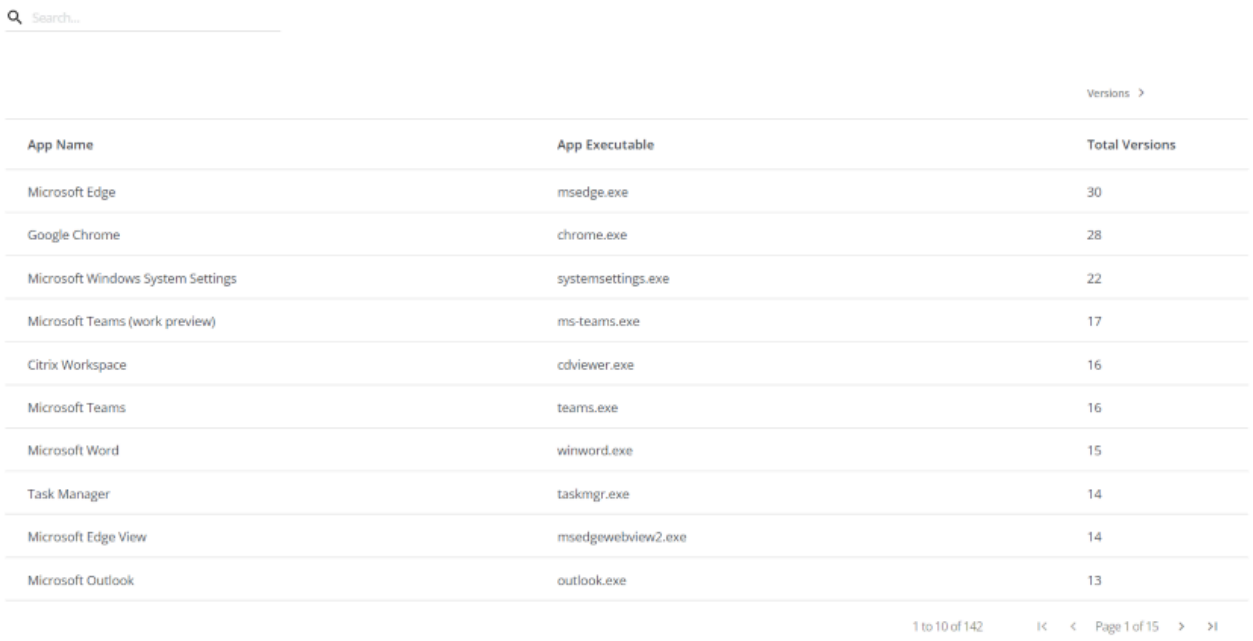
In the upper area of the `Apps Version` option, you can see a selector for the number of days you want to evaluate. By moving it, you can see the different versions of the registered applications, depending on the number of days selected.



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

Table view

Copyright © 2024 Flexxible. Todos los derechos reservados.



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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

Analyzer / Polls

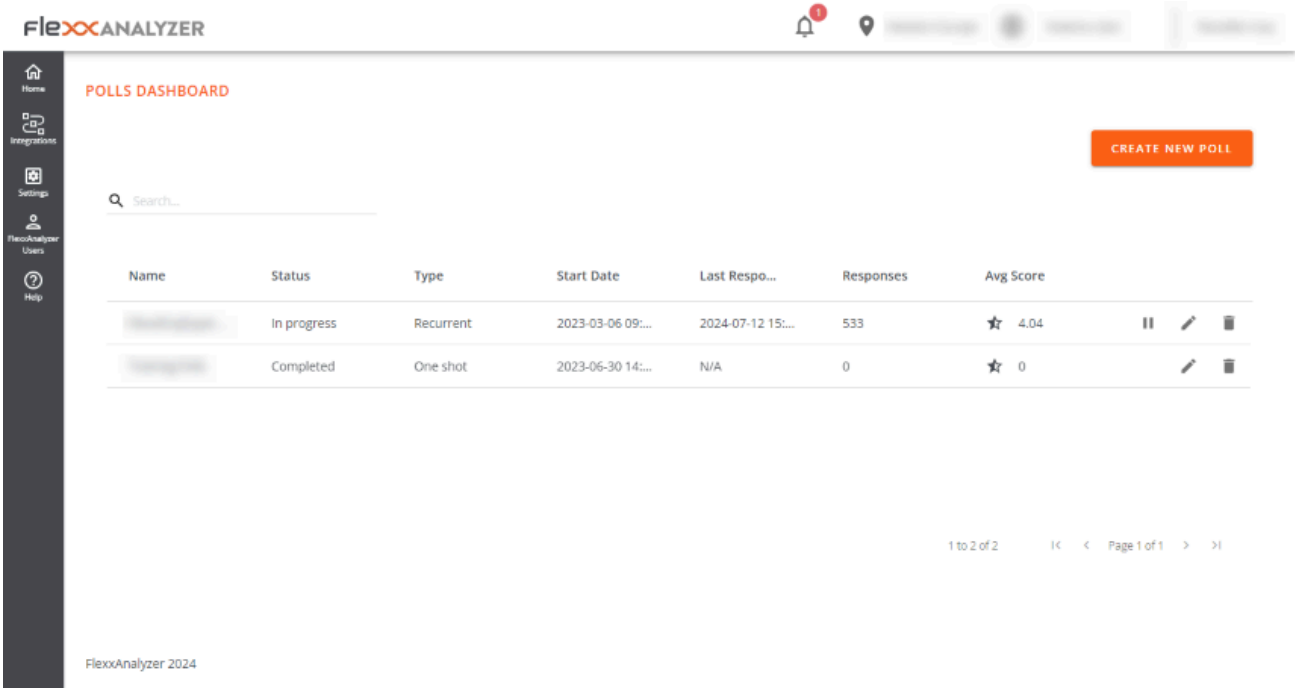
Polls allow us to get the user's sentiment or perception regarding very simple questions, trying to simplify the response mechanisms as much as possible to maximize the user response rate.

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

Poll Settings

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

List view

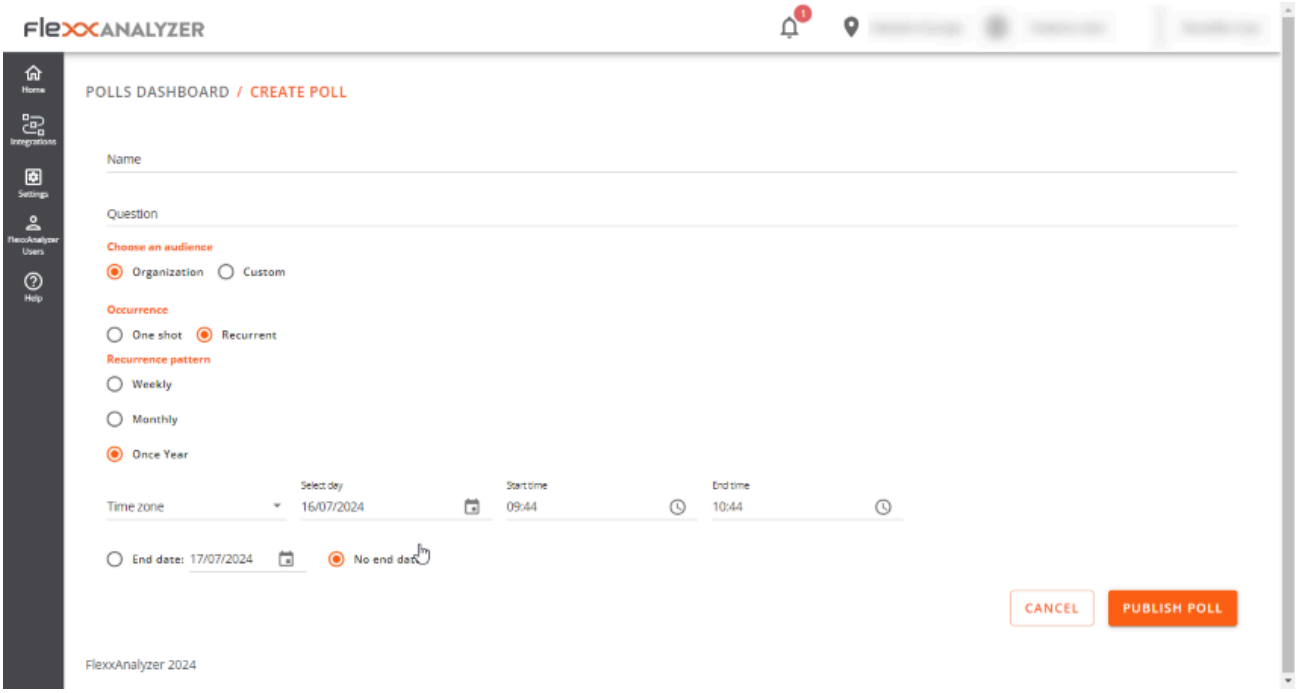


By accessing the section, you can see a list of the configured surveys, if any, as well as a preview of their configuration.

Detail view

Copyright © 2024 Flexxible. Todos los derechos reservados.

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

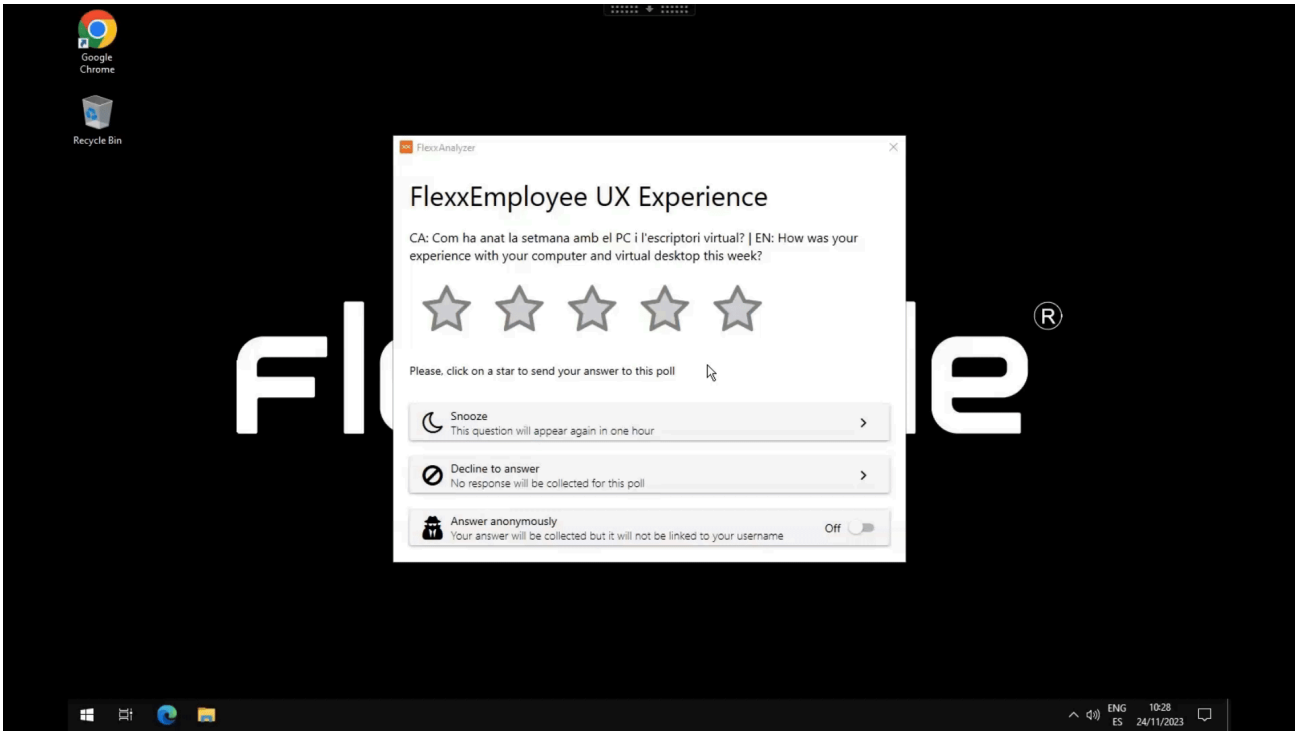
Occurrence

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).

Copyright © 2024 Flexxible. Todos los derechos reservados.

Analyzer / Users in Analyzer

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

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

List view

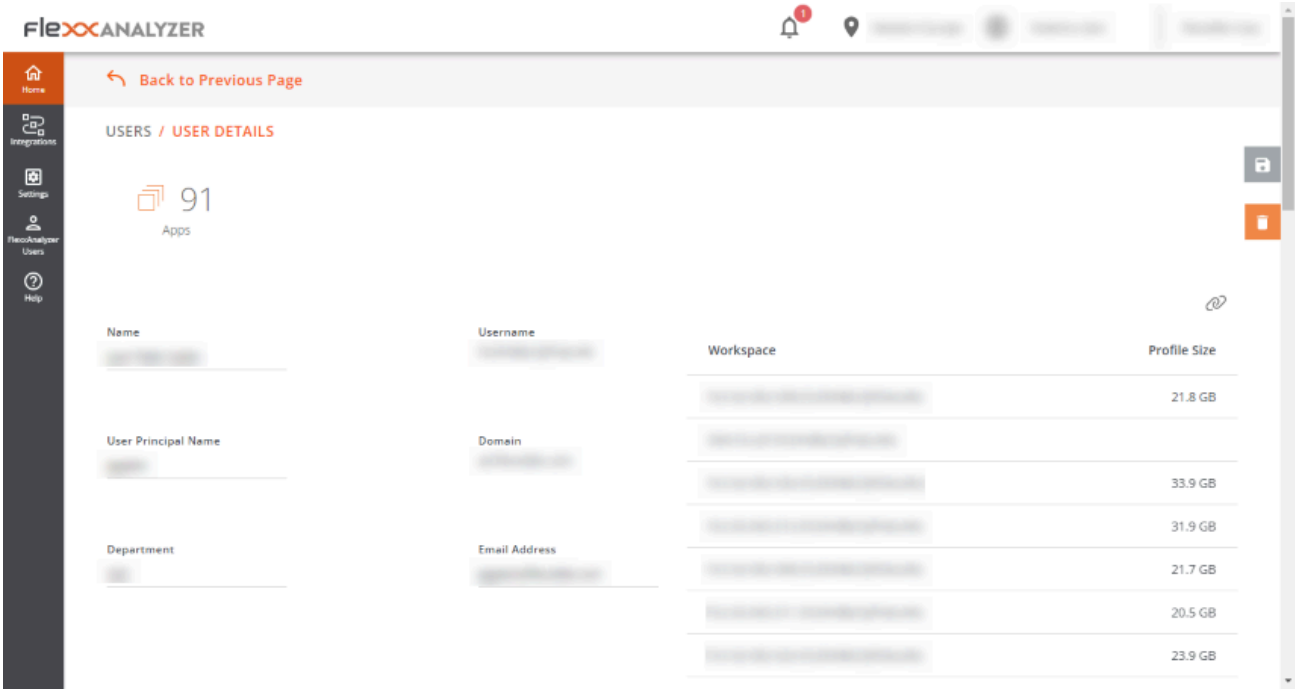
This view allows you to see condensed information about the total number of users and domains, as well as data about all users:

- **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:

Copyright © 2024 Flexxible. Todos los derechos reservados.



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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

`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.

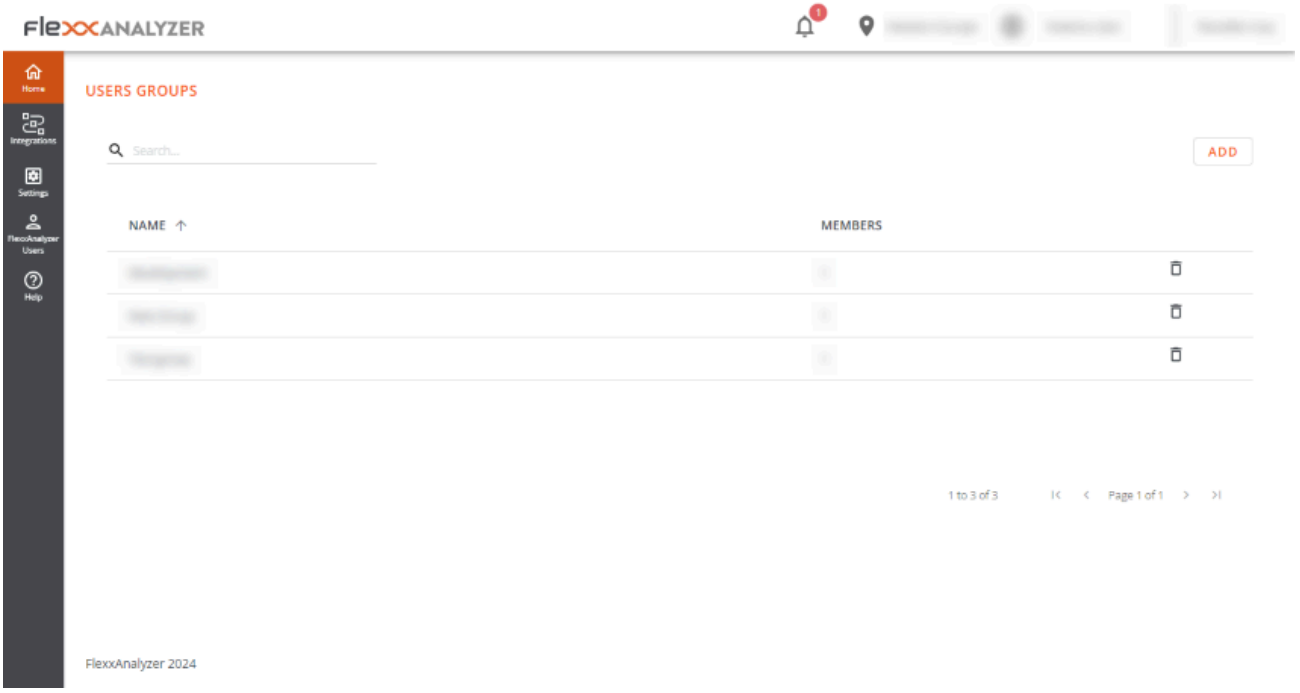
Copyright © 2024 Flexxible. Todos los derechos reservados.

Analyzer / User Groups

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

List view

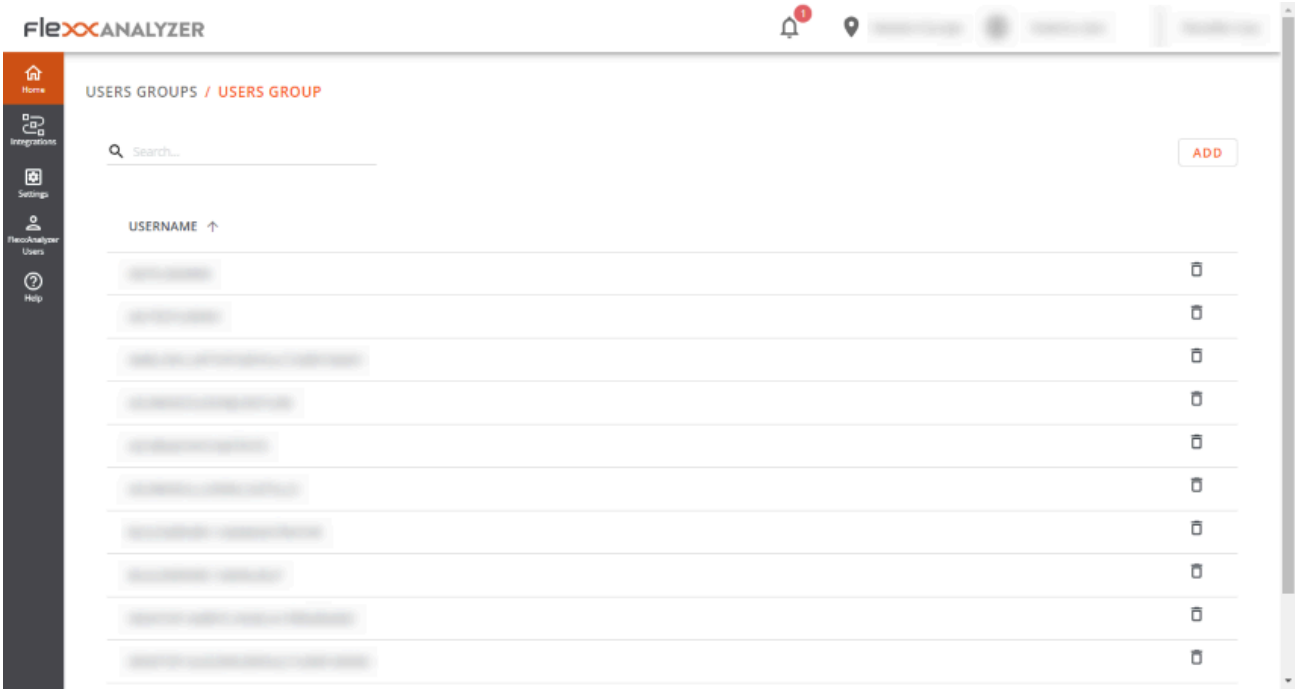
The list view presents the information of all existing groups and the button at the top right of the screen allows you to create new groups.



Detail view

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

Copyright © 2024 Flexxible. Todos los derechos reservados.



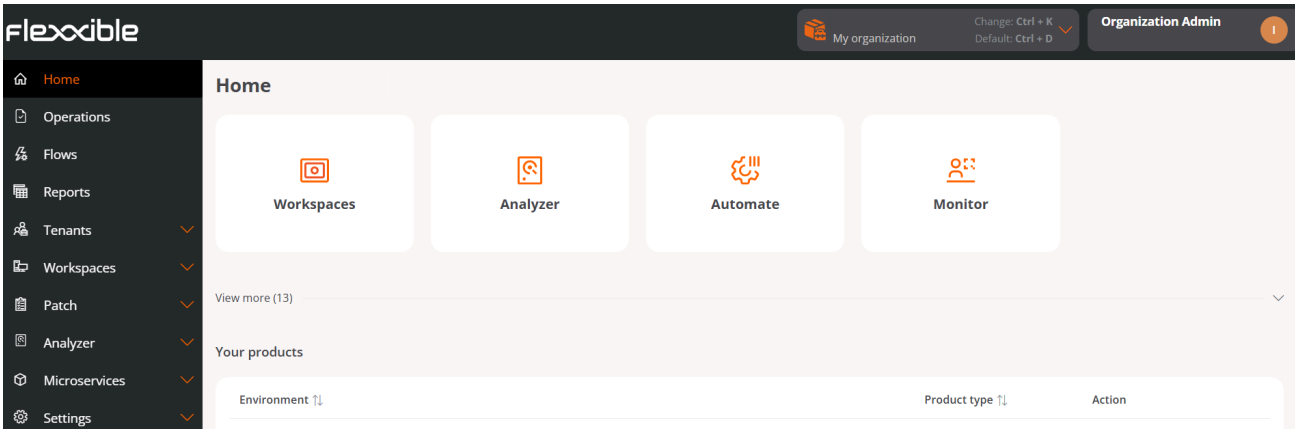
Copyright © 2024 Flexxible. Todos los derechos reservados.

Portal

Portal is the central space of the platform, from where you access the available modules of Flexxible products. 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 consult license consumption data by environment, manage reporting groups, and activate functionalities 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:

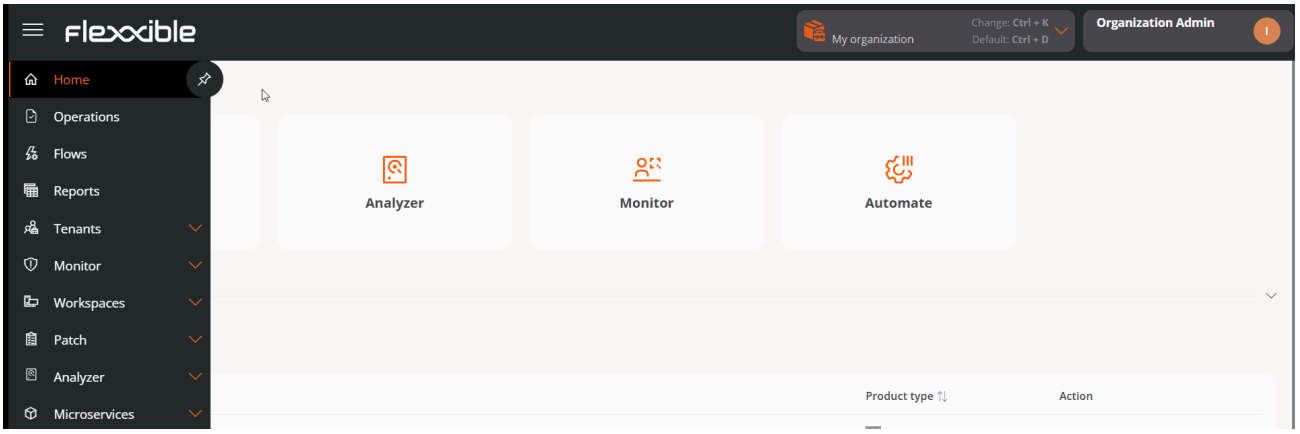
- Home
- Operations
- Flows
- Reports
- Tenants
- Monitor

Copyright © 2024 Flexxible. Todos los derechos reservados.

- 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.

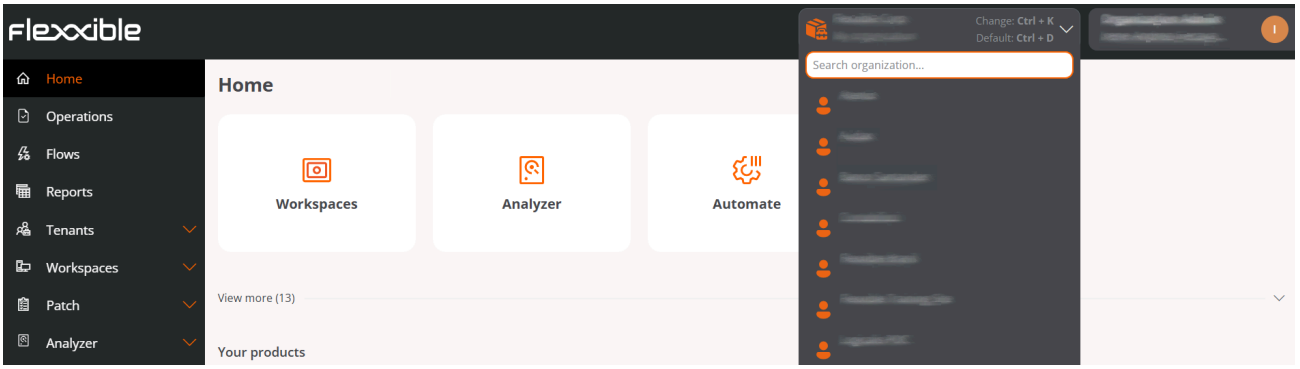


Organization selector

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).

Copyright © 2024 Flexxible. Todos los derechos reservados.



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

Copyright © 2024 Flexxible. Todos los derechos reservados.

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

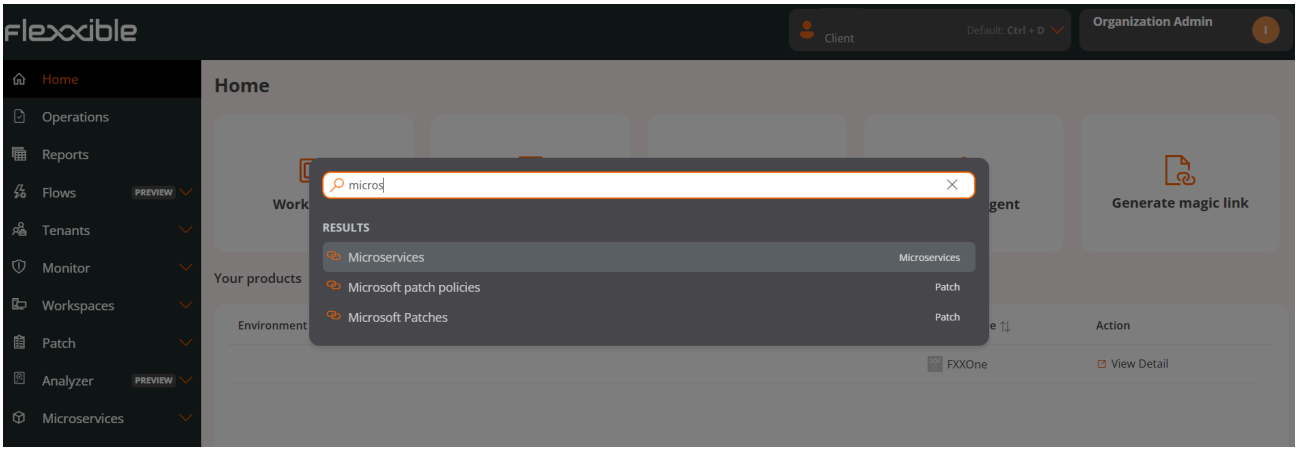
From this section, you can manage the security levels for user authentication by email and password. For more information, please refer to the Access and Authentication documentation.

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

Copyright © 2024 Flexxible. Todos los derechos reservados.

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`.

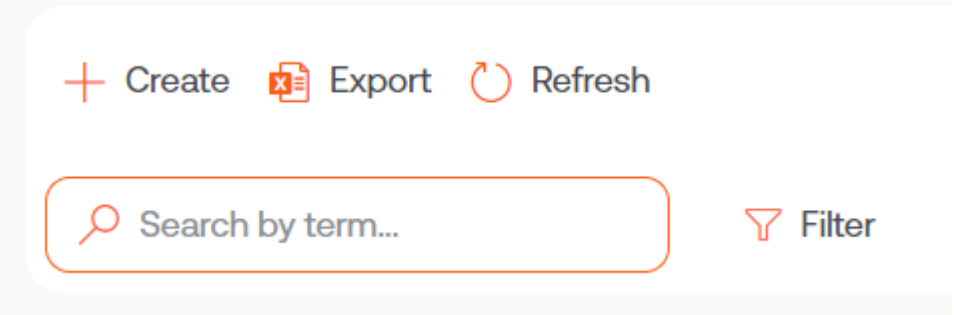
Tables

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

Copyright © 2024 Flexxible. Todos los derechos reservados.

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.

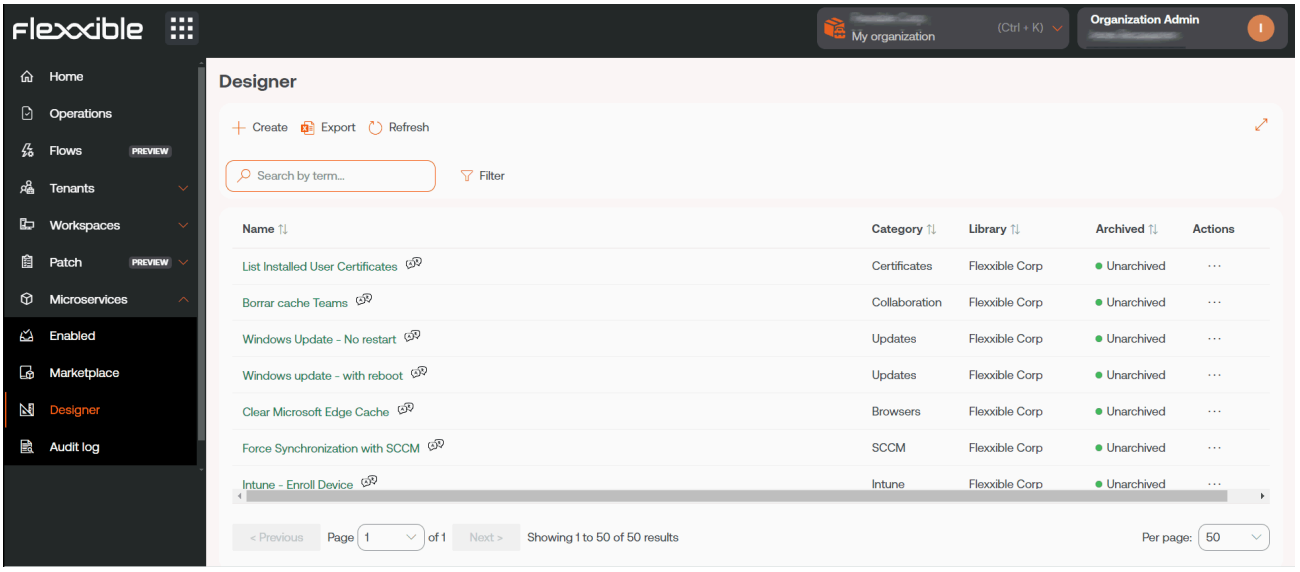
Filter

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

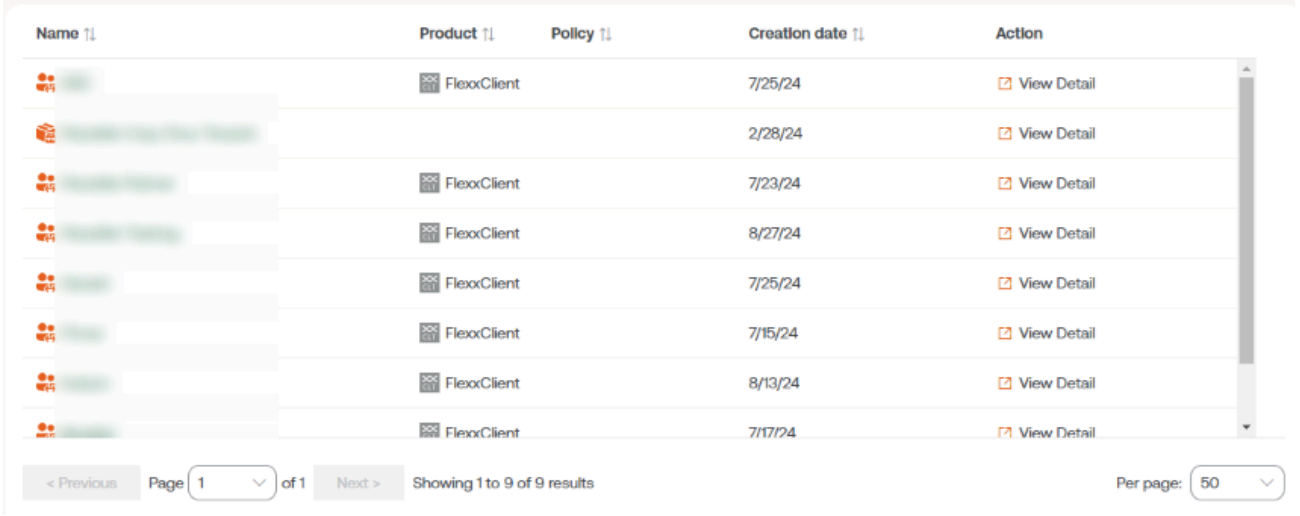
Copyright © 2024 Flexxible. Todos los derechos reservados.

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.



Copyright © 2024 Flexxible. Todos los derechos reservados.

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

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 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.

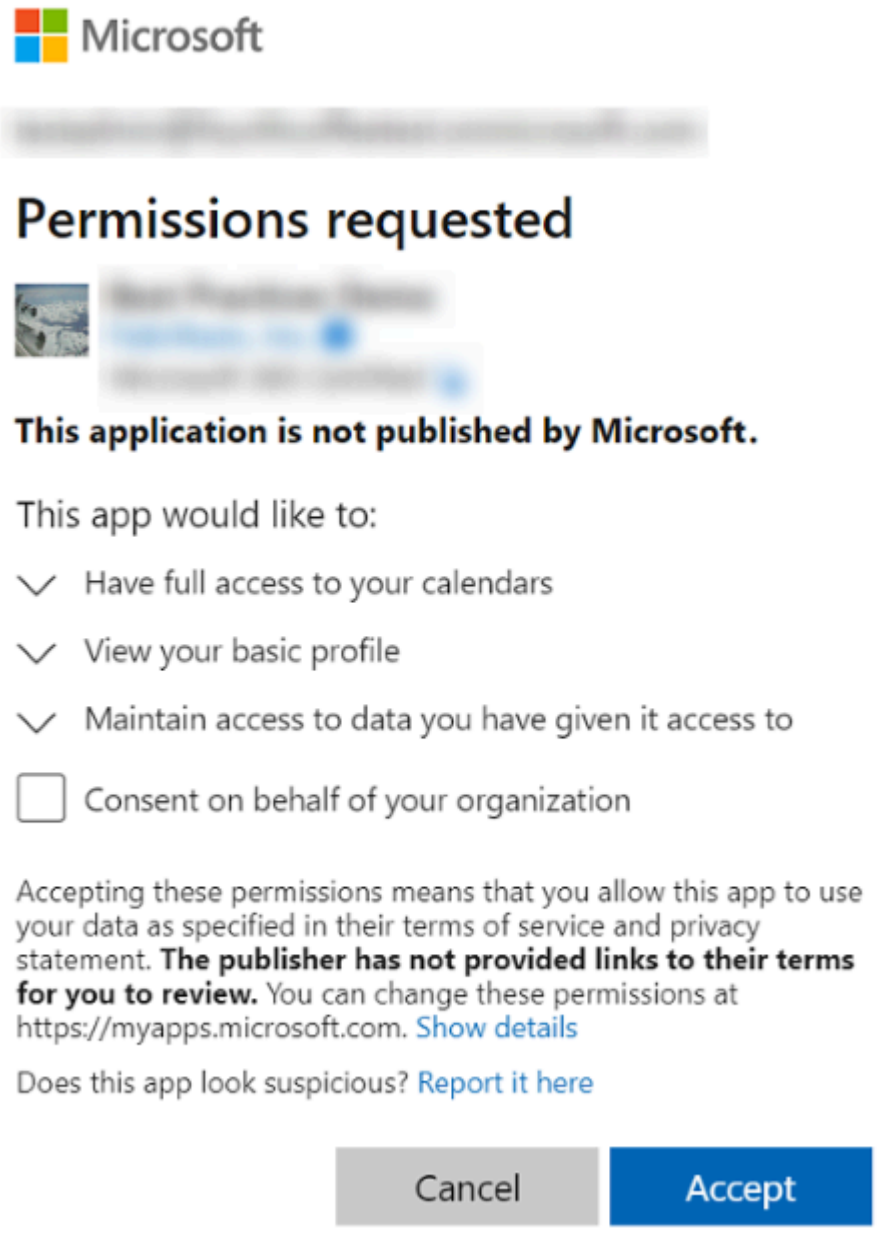
Enterprise Application Consent and Permissions in Entra ID

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

Copyright © 2024 Flexxible. Todos los derechos reservados.

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

Copyright © 2024 Flexxible. Todos los derechos reservados.

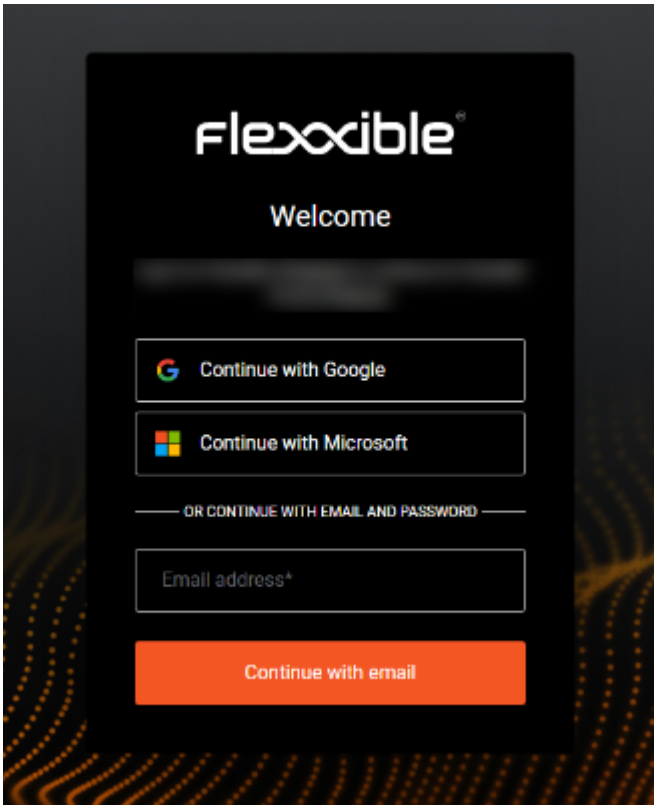
Permission	Caption
email	View users' email addresses
offline_access	Maintain access to data that has been granted access
openid	Log In
profile	View basic user profile
User.Read	Log in and read users' profiles

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.



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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

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:

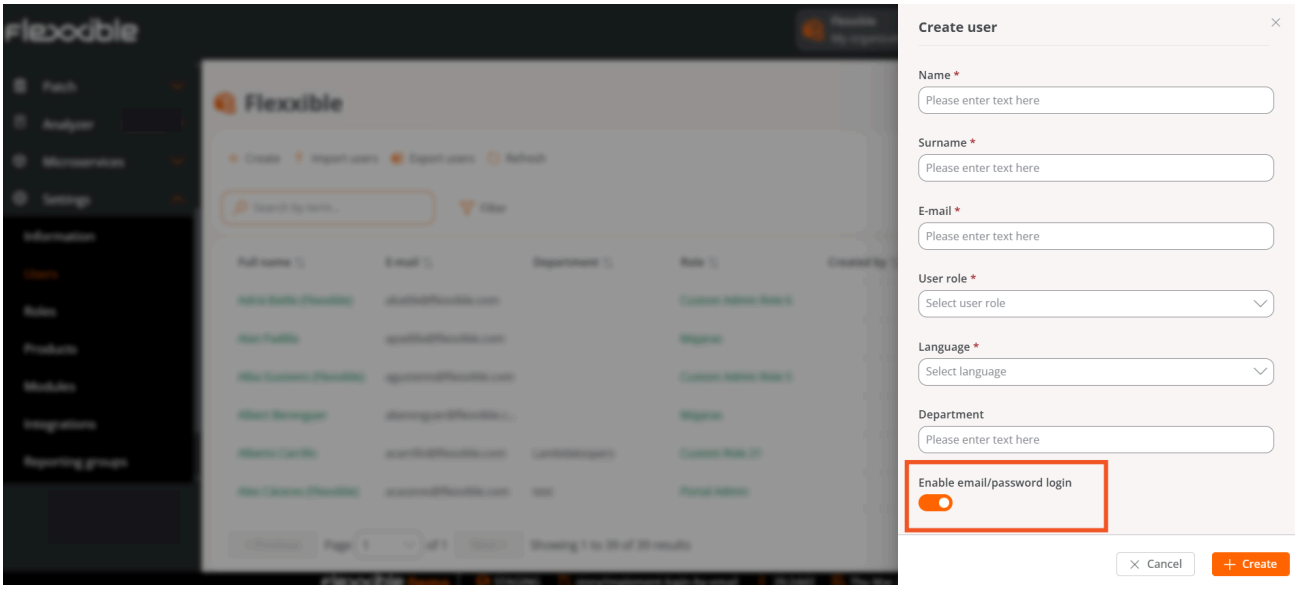
- Enable access for a new user
- Enable access for a batch of users
- Enable access from the user table

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.



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).

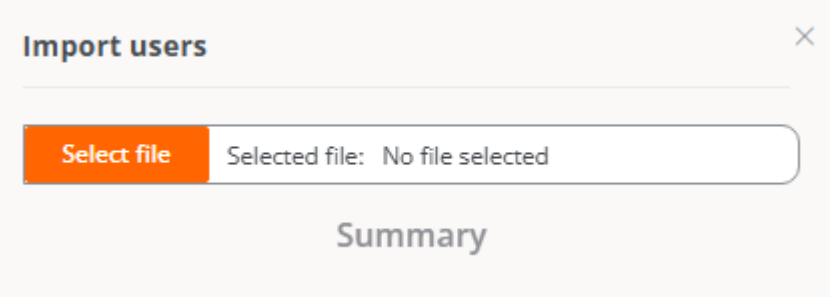
Action	Name	Surname	Email	Department	Role	Language	Email login enabled
Add/Update					Portal Admin	en	Y
Add/Update					Custom Admin Role 2	en	N
Add/Update					Portal Admin	en	Y
Add/Update					Custom Admin Role 4	en	N
Add/Update					Custom Admin Role 5	es	N
Add/Update					Majaras	en	N
Add/Update					Custom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

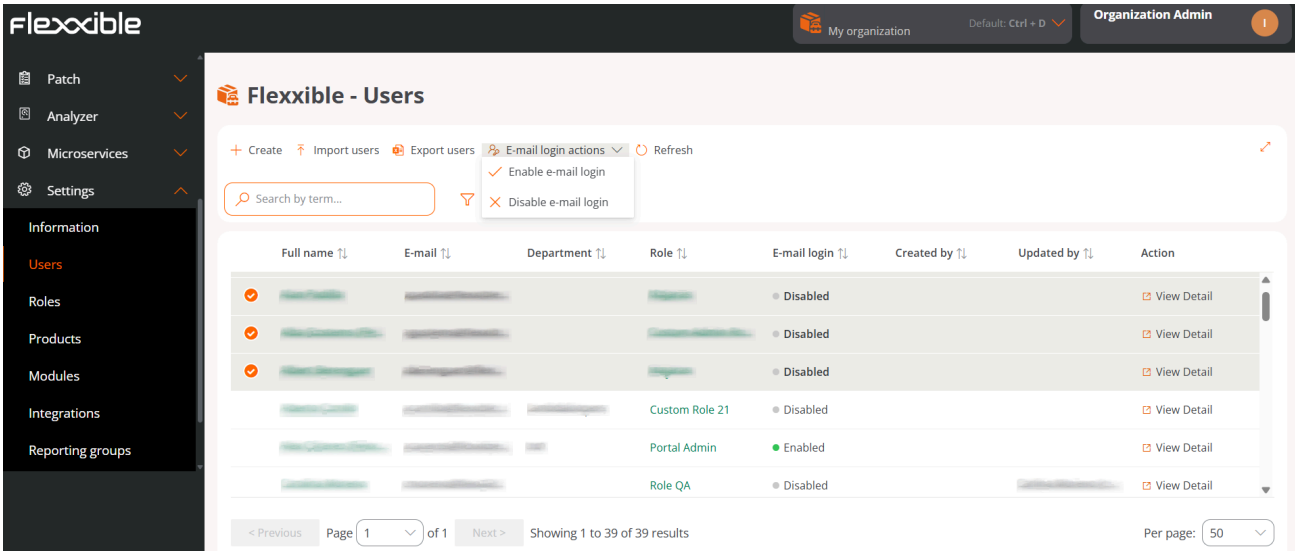
Copyright © 2024 Flexxible. Todos los derechos reservados.



5. Click on `Import`.

Enable access from the user table

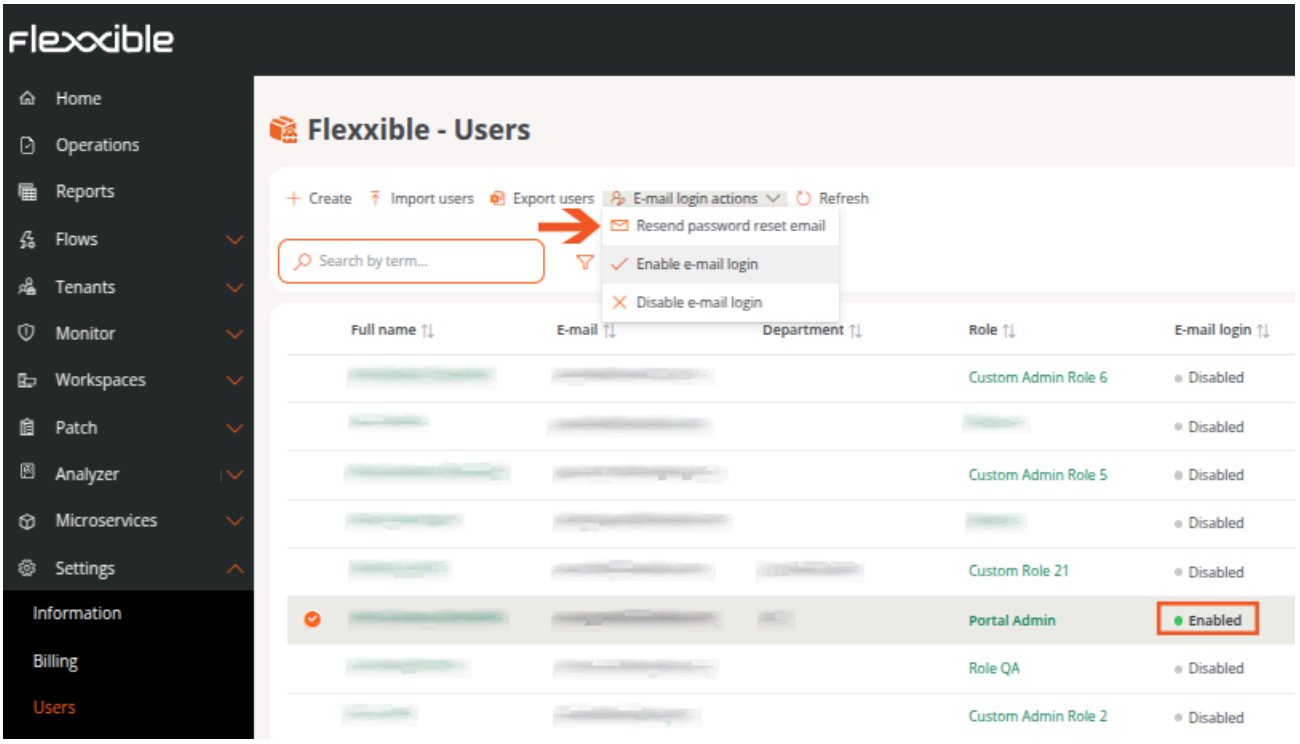
1. Go to `Portal` -> `Settings` -> `Users`.
2. Select the users you want to enable access for.
3. In the top menu, click on `Email login actions` -> `Enable email login` or `Disable email login`, as needed.

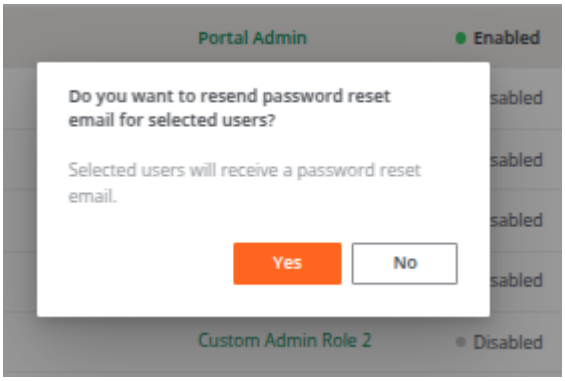


Reset the password from the user table

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`.

Copyright © 2024 Flexxible. Todos los derechos reservados.





INFO

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

Authentication security settings

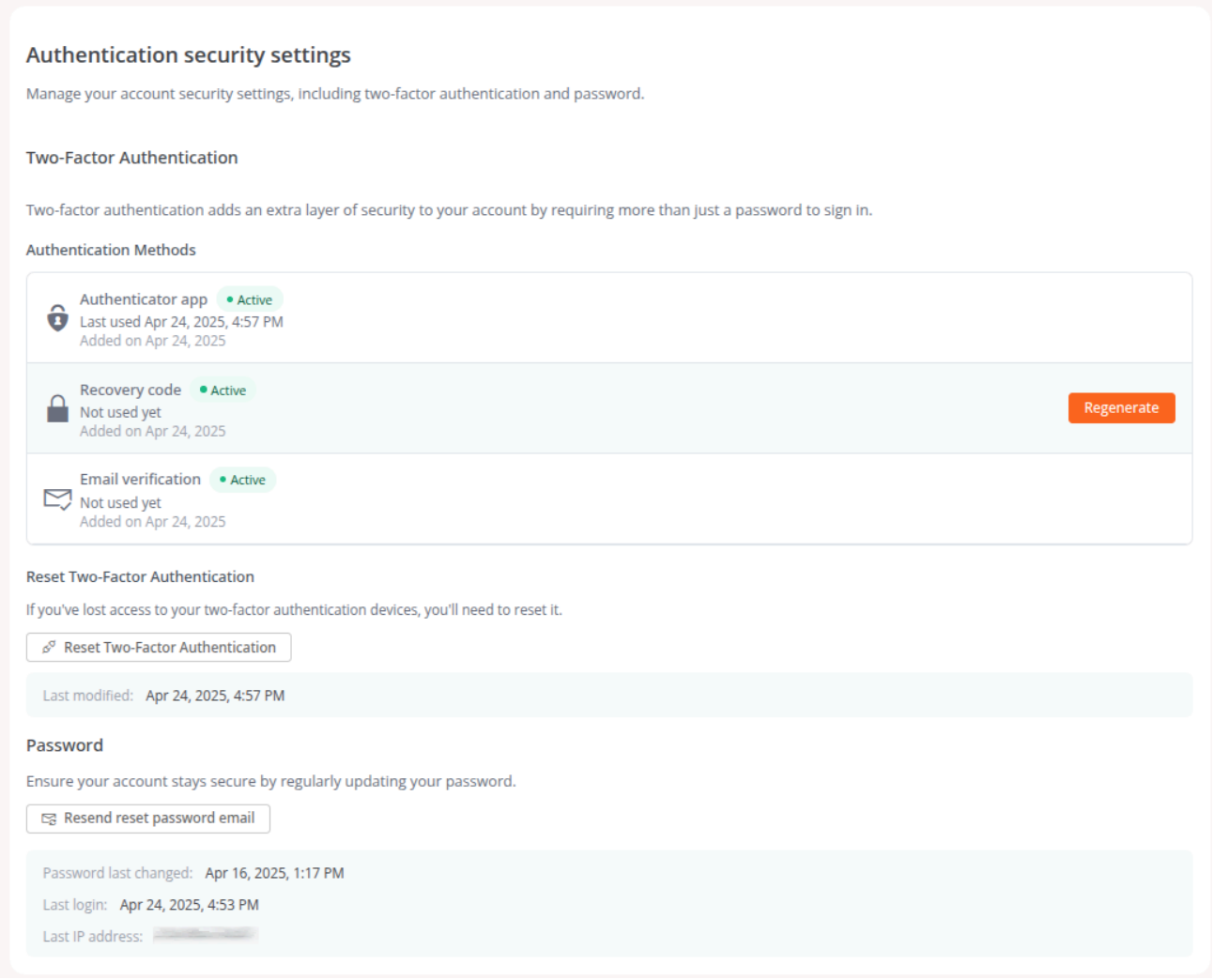
Flexxible allows managing security levels for email and password authentication, both at user and organization level.

Copyright © 2024 Flexxible. Todos los derechos reservados.

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

Copyright © 2024 Flexxible. Todos los derechos reservados.

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

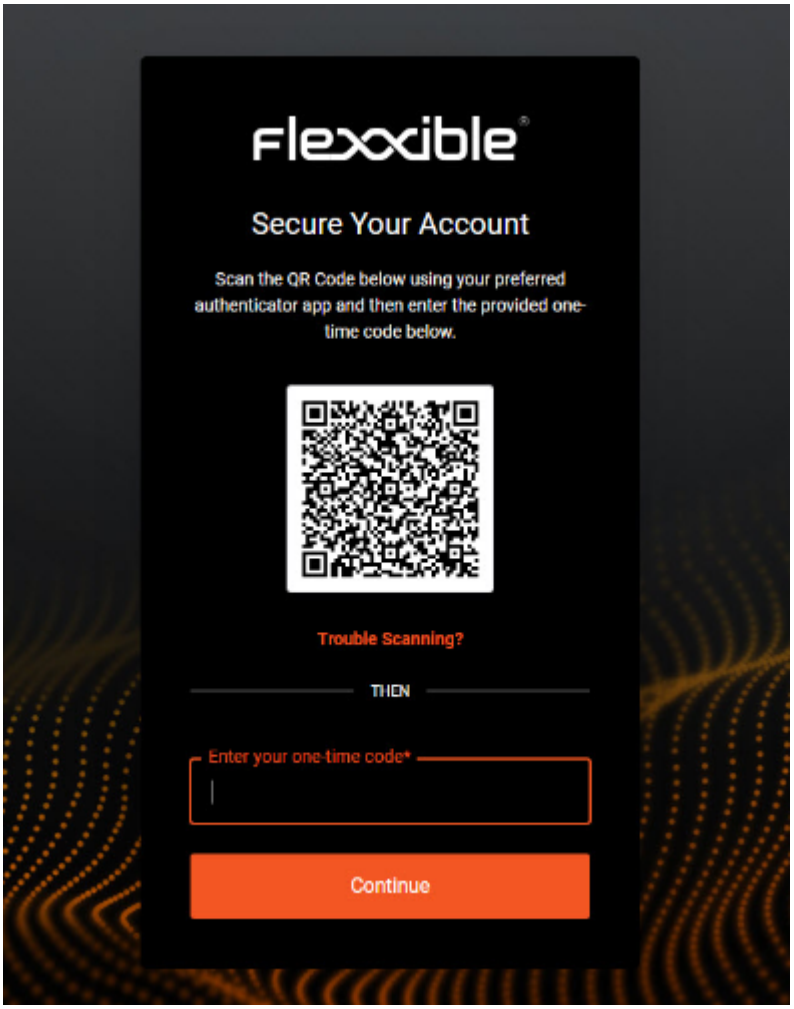
- Authentication app
- Recovery code
- Email verification

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.

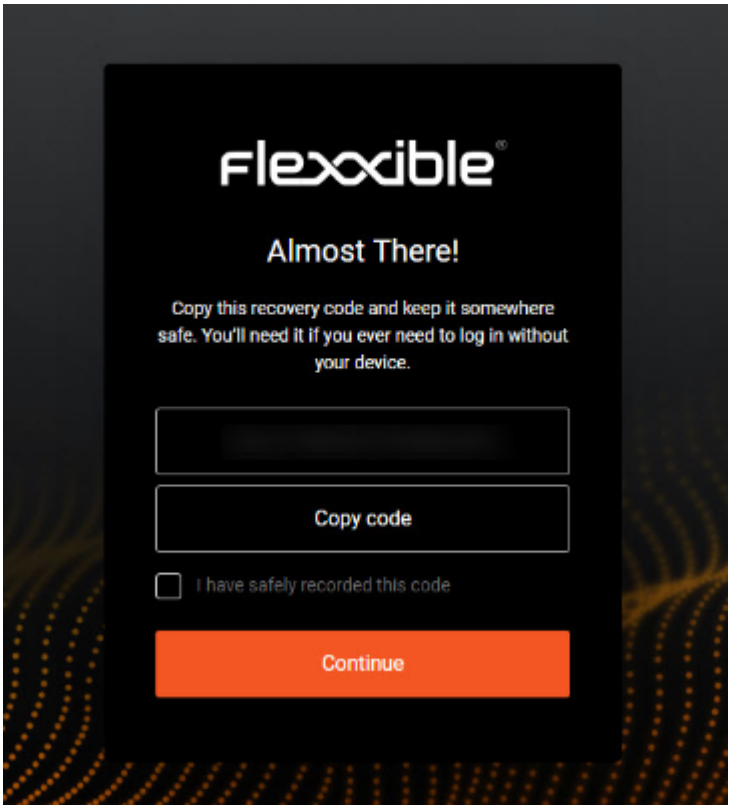
To add this method, the user must click on `Enable` in the authentication security settings panel. A modal window will display a QR code. When scanned, the user must enter the six-digit verification code provided by the authentication app in the designated field.

Copyright © 2024 Flexxible. Todos los derechos reservados.



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.

Copyright © 2024 Flexxible. Todos los derechos reservados.



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

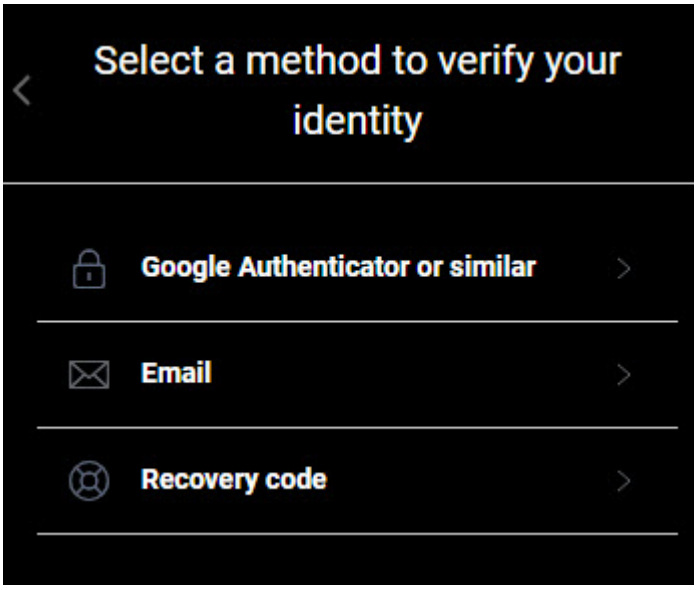
When the use of the authentication app is enabled, Flexxible generates a recovery code for the user to save and use when they don't have access to the device where the

Copyright © 2024 Flexxible. Todos los derechos reservados.

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

Copyright © 2024 Flexxible. Todos los derechos reservados.

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 via email and password for users of the organization and its suborganizations. The functionality can only be enabled or disabled from the main organization if suborganizations are available.

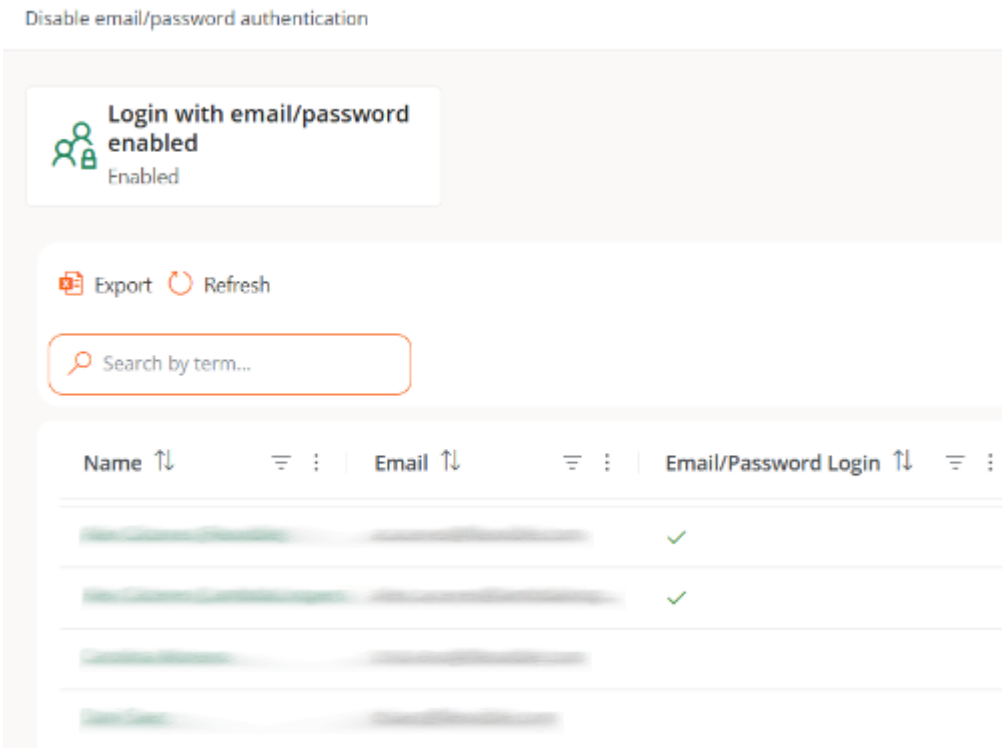
To do this, from the Portal, you must go to `Settings` -> `Organization`. And in the left side menu, you must click on the `Authentication` tab.

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.



User table

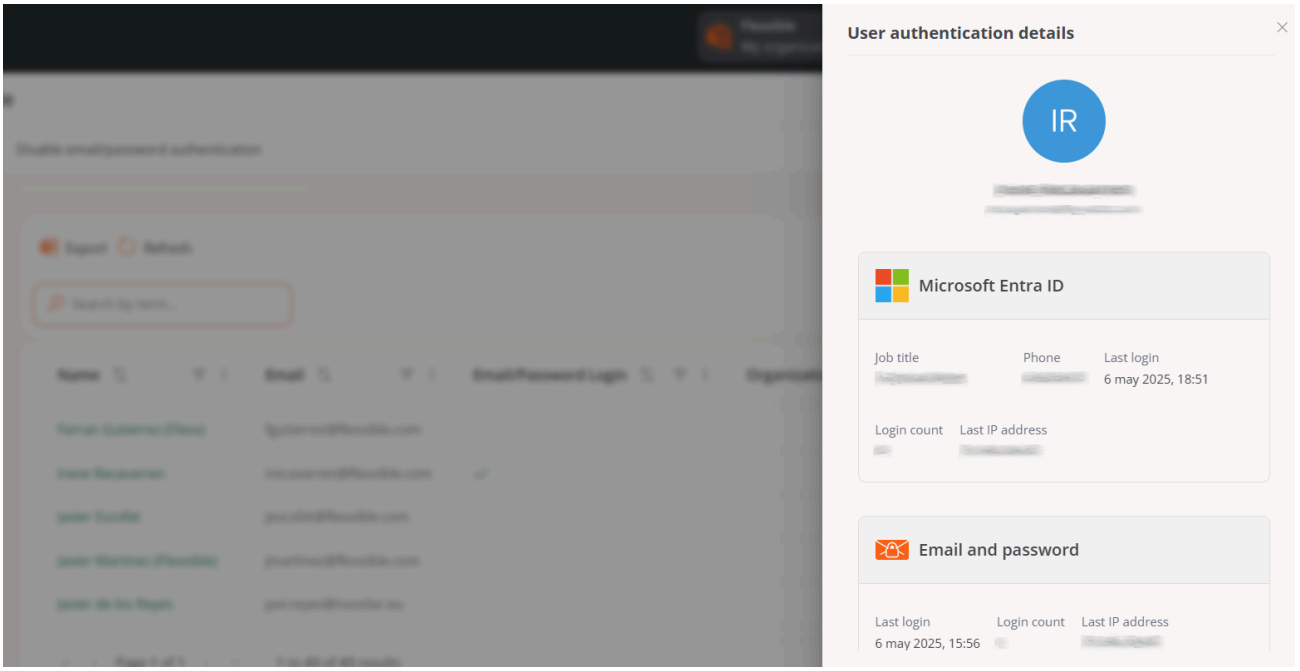
The user table in the `Authentication` tab shows the list of organization members. At a glance, you can see which members have the option to log in via email and password enabled.

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.

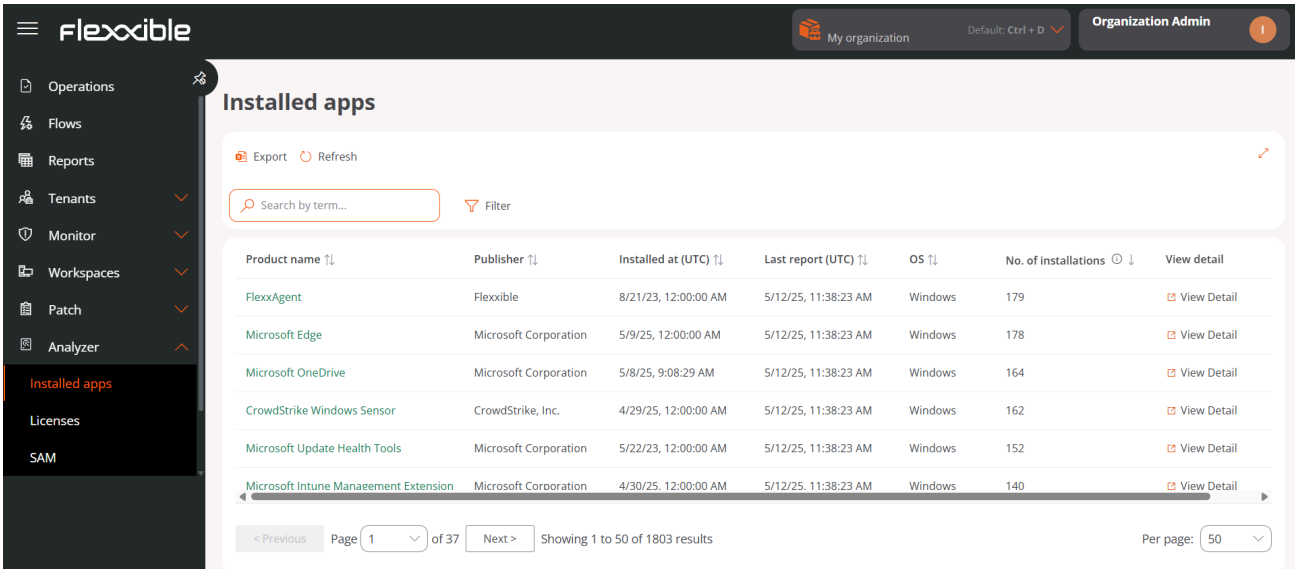
Copyright © 2024 Flexxible. Todos los derechos reservados.



Copyright © 2024 Flexxible. Todos los derechos reservados.

Portal / Analyzer in Portal

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

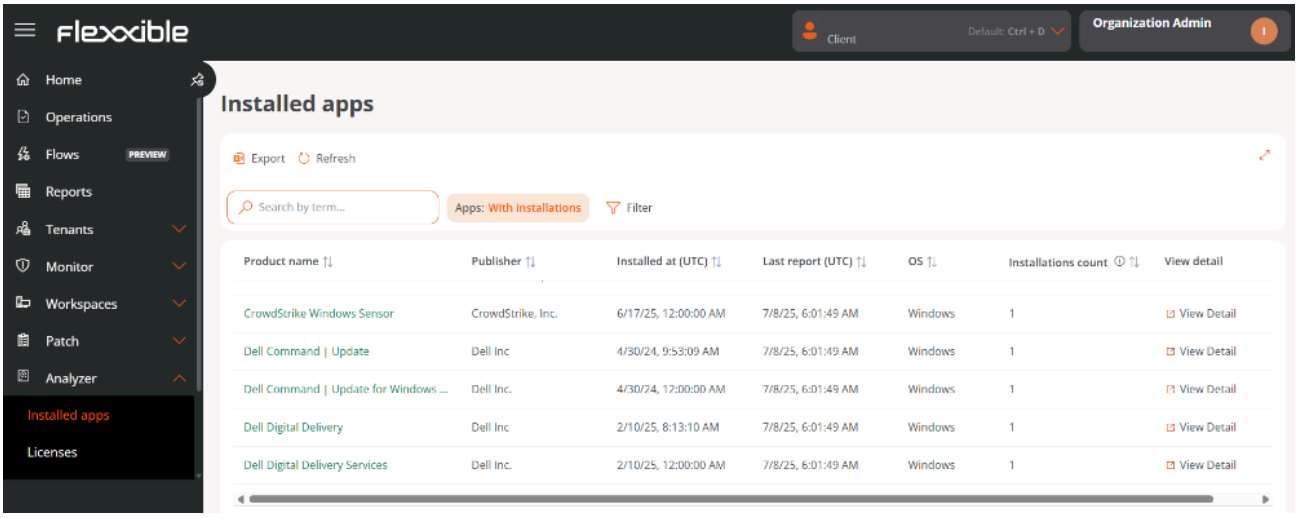


This information can also be accessed from the Workspaces section of the Analyzer module.

Copyright © 2024 Flexxible. Todos los derechos reservados.

Portal / Analyzer / Installed apps

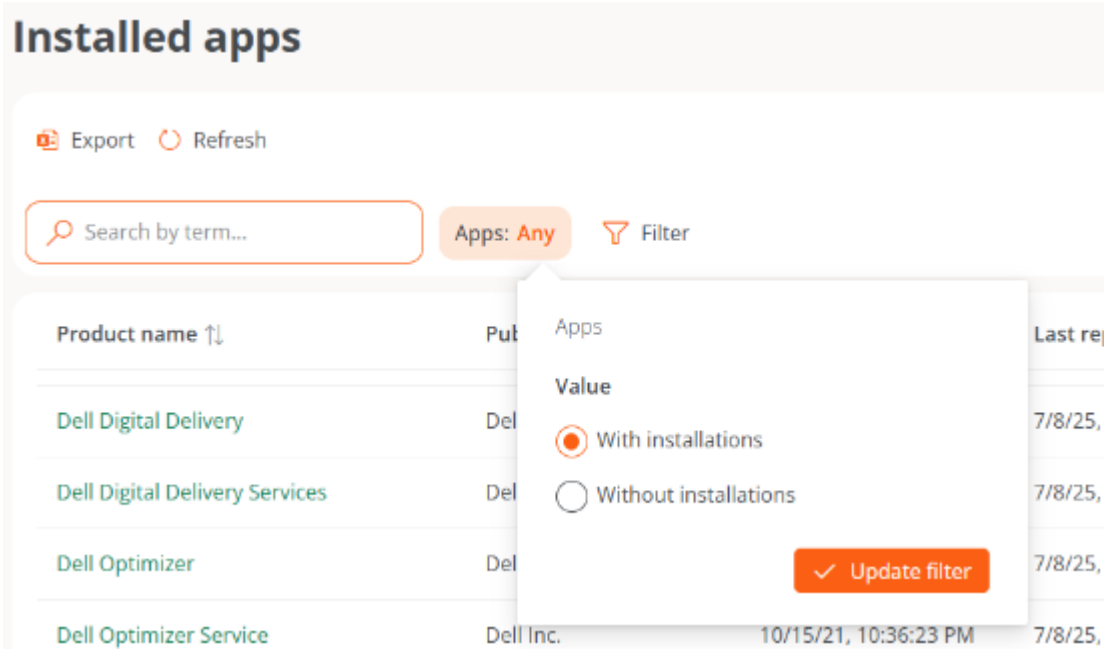
This section shows all the installed applications that FlexxAgent has found on the organization's devices.



The table offers the following data:

- **Product name.** Name of the installed application.
- **Publisher.** Company that developed the application.
- **Installed at (UTC).** Date and time when the application was first reported on a device, in Coordinated Universal Time standard.
- **Last report (UTC).** Date and time of the last application report on a device, in Coordinated Universal Time standard.
- **OS.** Operating system of the devices where the application is installed.
- **Number of installations.** Number of application installations on the organization's devices.
- **See details.** Opens the application's detailed view.

Copyright © 2024 Flexxible. Todos los derechos reservados.



The *Apps* filter, located at the top of the table, allows listing applications based on their installation status (*With installations* or *Without installations*).

> **INFO**
>
> The number of installations per installed application is calculated every two hours.

Installed Apps Details

From the overview, click on the application name or the `View details` option. Next, five tabs will be displayed:

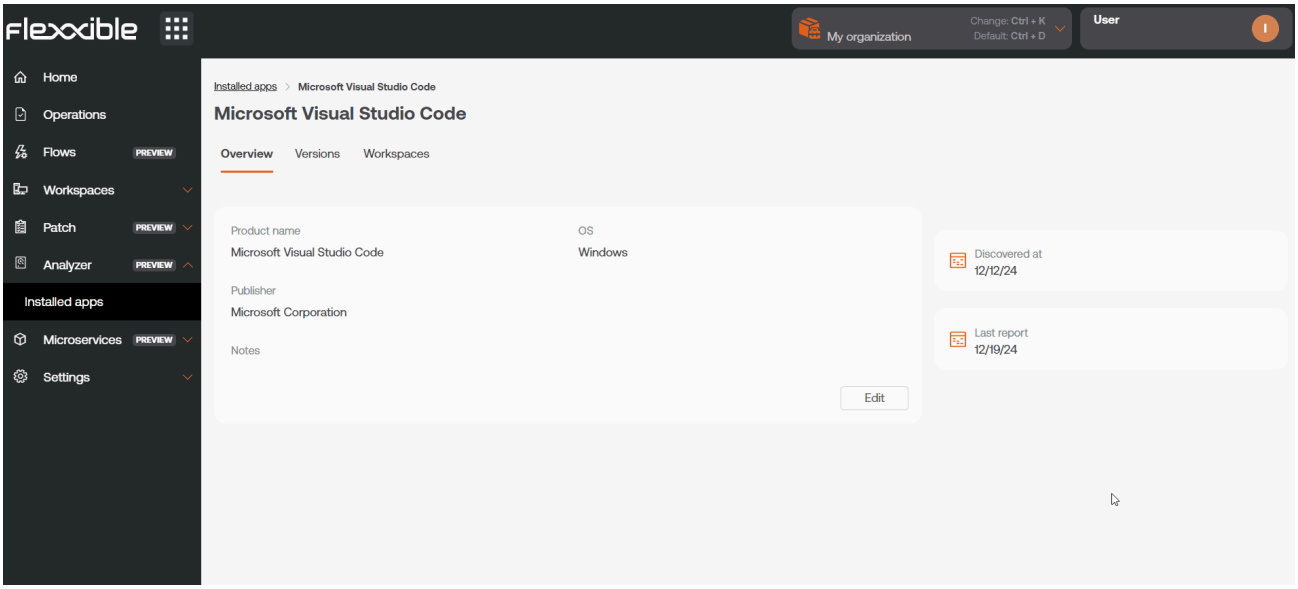
- Overview
- Versions
- Workspaces
- Installation history
- Report history

Copyright © 2024 Flexxible. Todos los derechos reservados.

> **INFO**
>
> Installed applications are reported at each FlexxAgent startup; from that moment, the information is updated every 12 hours, as long as there is a user session started.

Overview

Shows the same information as in the list view, plus the `Edit` button, which opens a modal window with a form to enter a free-text note.



Versions

The columns of this table show the following information:

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

Clicking on the version number will redirect the user to a detail view of the application version, to see which devices have it installed and the date of its last report.

Copyright © 2024 Flexxible. Todos los derechos reservados.

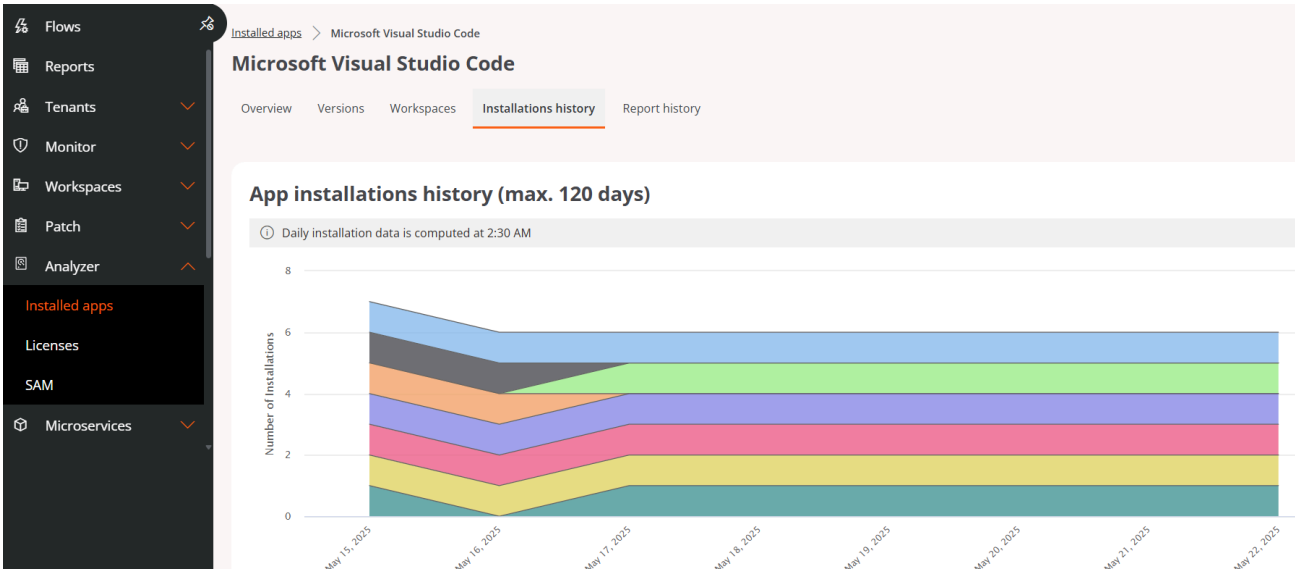
Workspaces

Details the following information:

- **Name.** Name of the device where the application being queried is installed.
- **Version.** Version number of the application installed on the device.
- **Installation location.** Path where the application's executable (binary) is located.
- **Last report (UTC).** Date of the last report of the application on the device, in Coordinated Universal Time standard.
- **Installed at (UTC).** Date of the first report of the application on the device, in Coordinated Universal Time standard.
- **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.



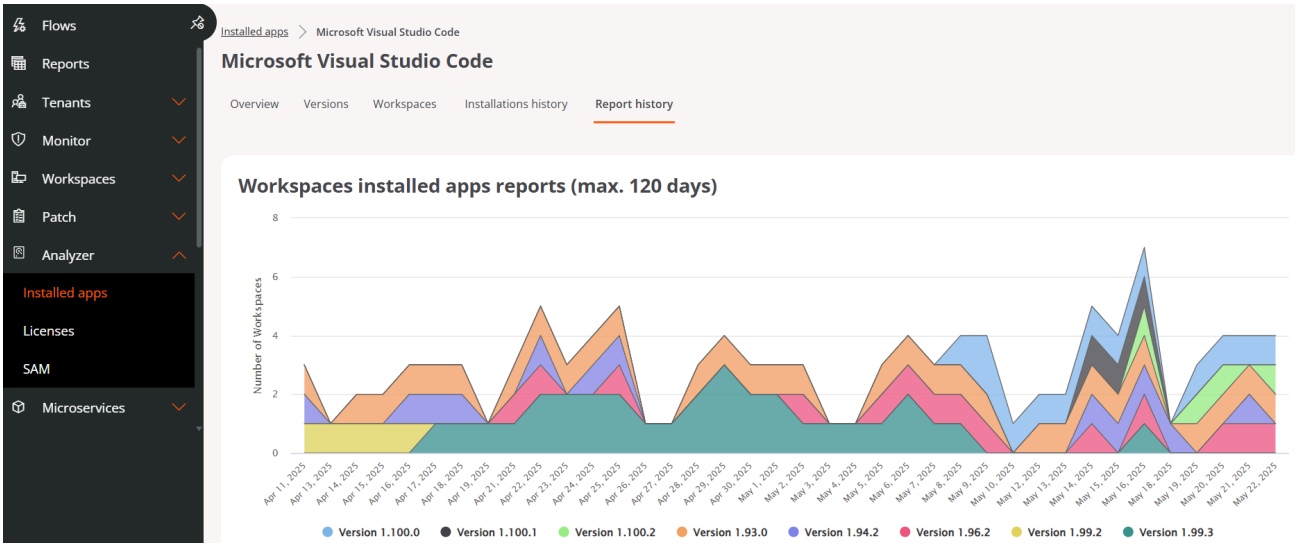
Hovering the cursor over the graph at a specific date will display a tooltip that indicates how many installations were present at that time for each of the application's versions.

Copyright © 2024 Flexxible. Todos los derechos reservados.

> **INFO**
>
> The installation history is updated once a day at 02:30 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 the cursor over the graph at a specific date will display a tooltip that indicates how many devices have reported a specific version number at that time. The version numbers are indicated below the graph as a legend.

Copyright © 2024 Flexxible. Todos los derechos reservados.

Portal / Analyzer / Licenses

This section shows information about all the software licenses acquired by an organization. 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 of licenses

There are three types:

- **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.

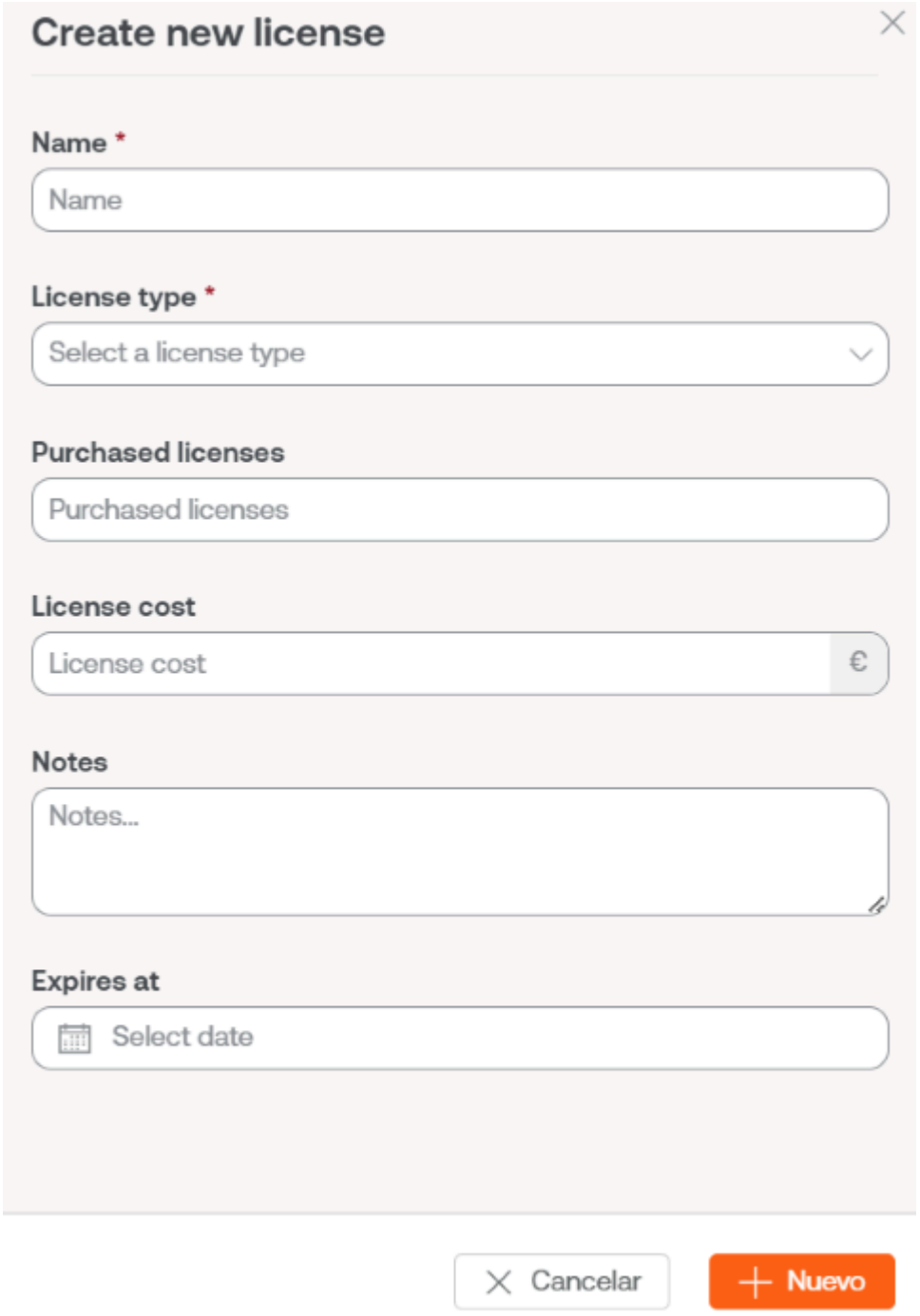
The configured license type will determine how its use is measured.

> **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:

Copyright © 2024 Flexxible. Todos los derechos reservados.

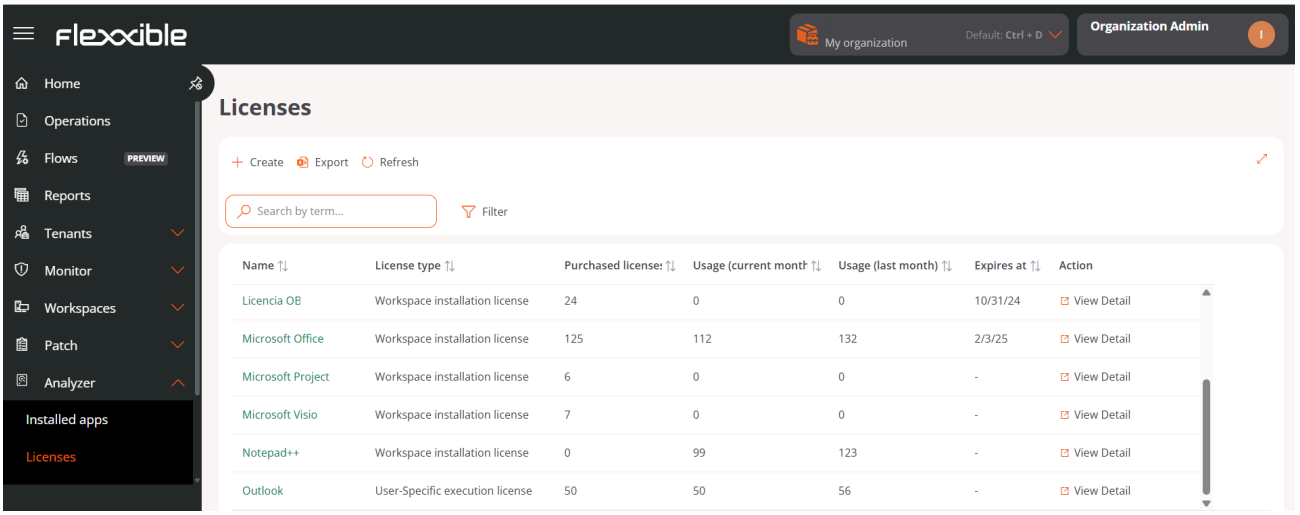


- **Name.** Name of the license the device has.
- **License type.** Option to choose the type of license.
- **Licenses purchased.** Number of licenses acquired.
- **License cost.** Monthly cost of the license, in euros.
- **Notes.**: Additional notes about the license.
- **Expires on.** Expiration date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

Copyright © 2024 Flexxible. Todos los derechos reservados.

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

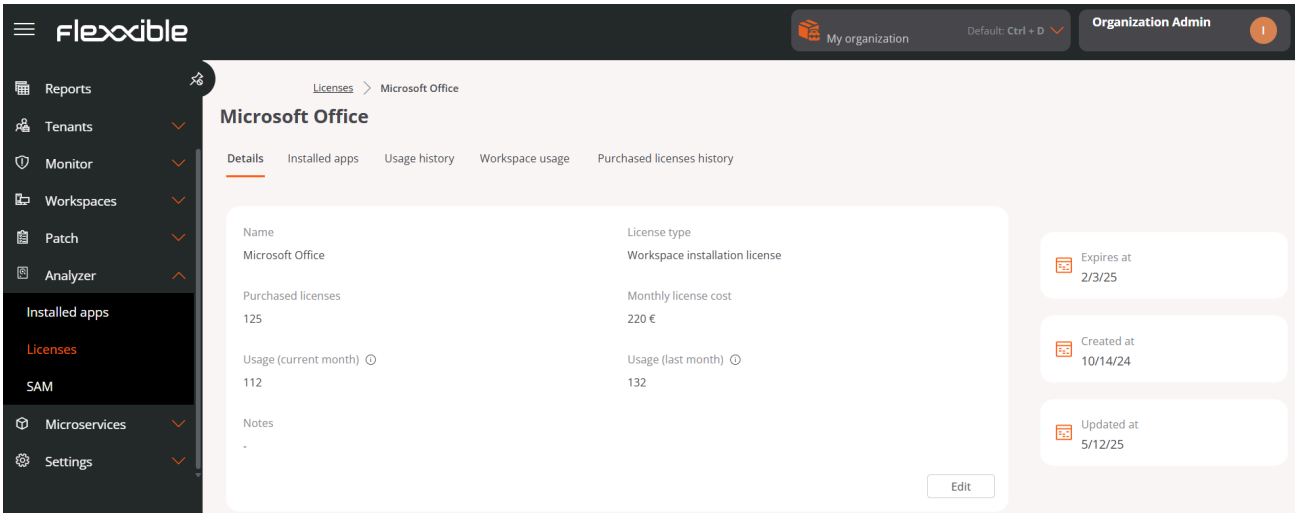
Copyright © 2024 Flexxible. Todos los derechos reservados.

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.

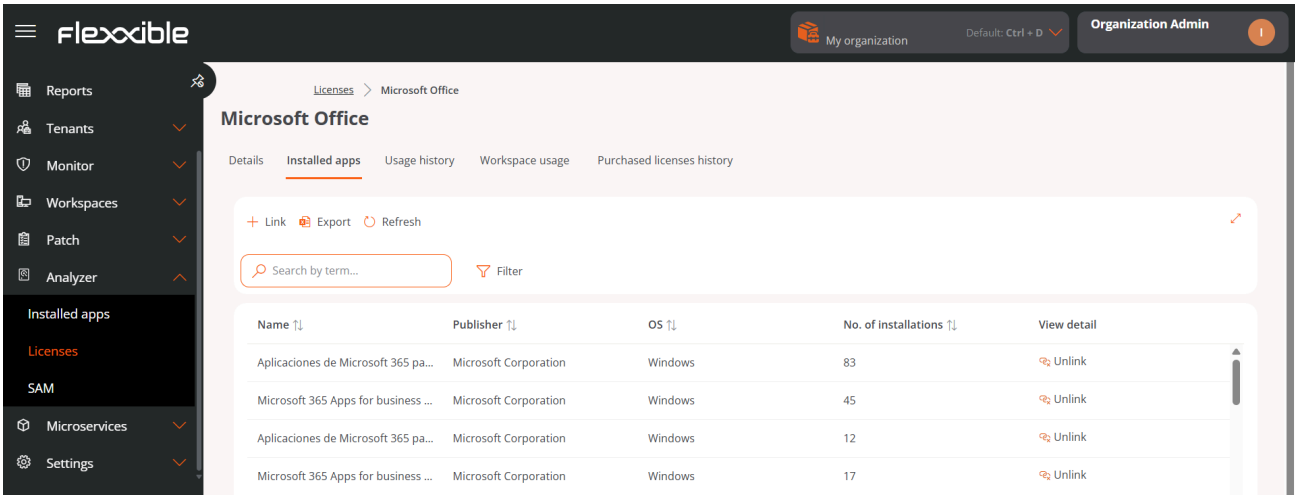


The `Edit` button opens a form to update information. The user also has the option to add free notes with data they consider relevant.

Installed apps

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

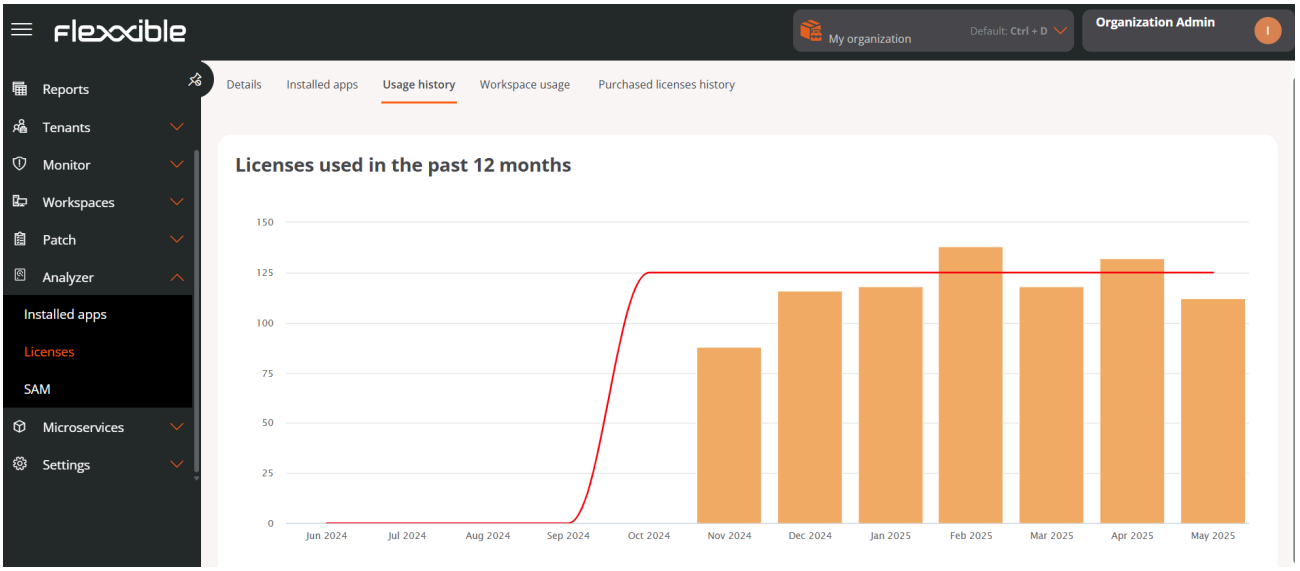
Copyright © 2024 Flexxible. Todos los derechos reservados.



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.

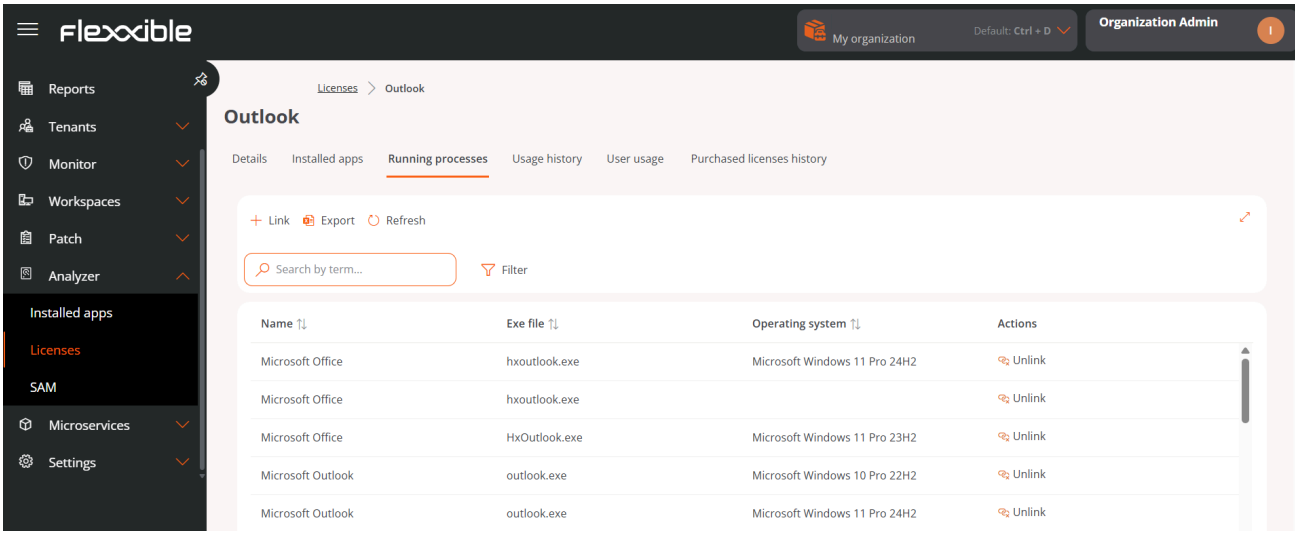
Usage history



Copyright © 2024 Flexxible. Todos los derechos reservados.

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

Running Processes



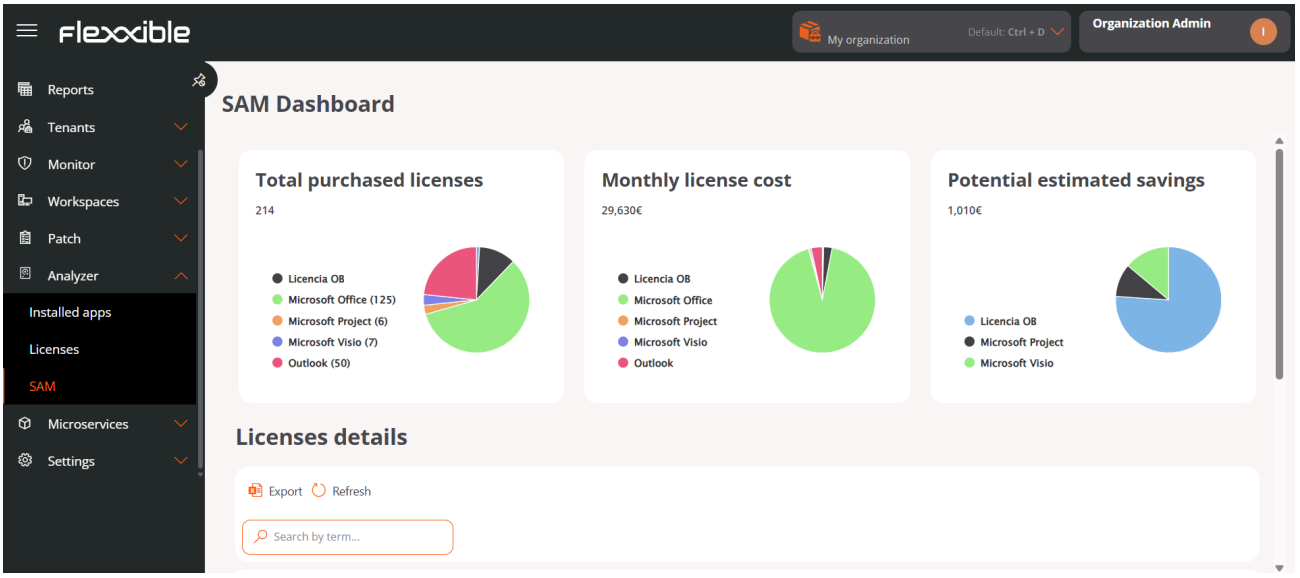
Reports on the running applications linked to this license. Those in which being in execution requires accounting for a license as *In use*. The table shows the following data:

- **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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

Portal / Analyzer / SAM

Allows measuring the organization's license usage when these have been correctly created and configured.



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:

Copyright © 2024 Flexxible. Todos los derechos reservados.

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

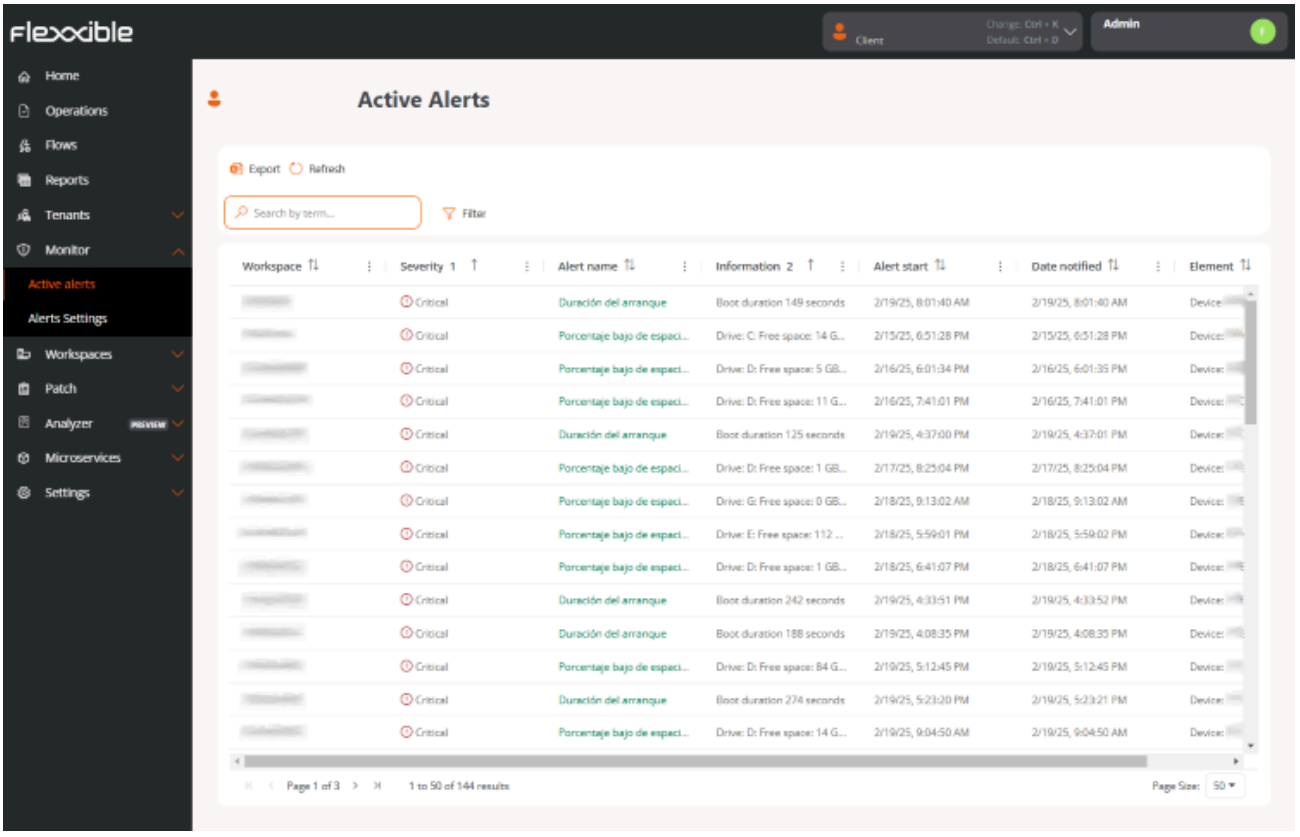
Clicking on the name of any license accesses graphs that indicate:

- 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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

Portal / Monitor in Portal

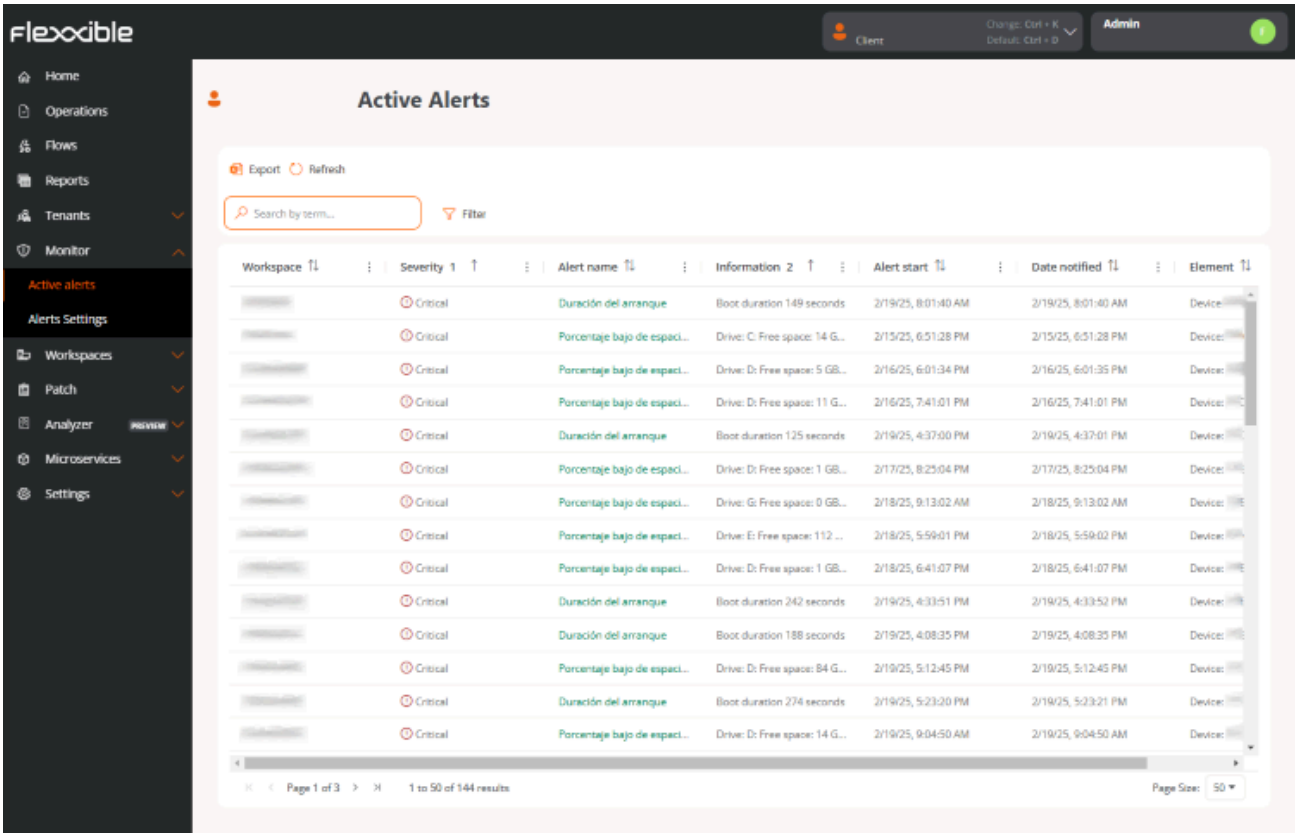
Monitor is the alerts and monitoring section of Portal. It consists of two sections: *Active alerts* and *Alert settings*. It provides real-time information on relevant events that could affect the device's operation and allows predefined alerts to be configured to meet each organization's specific needs.



Copyright © 2024 Flexxible. Todos los derechos reservados.

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. This section allows you to check the list of 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.

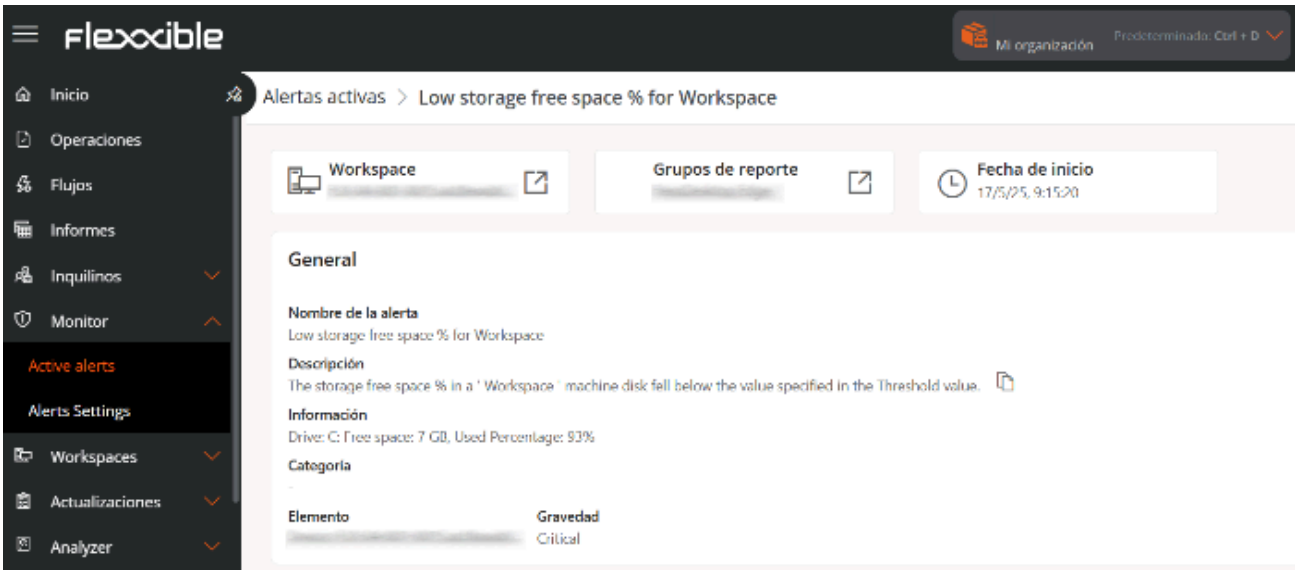
Copyright © 2024 Flexxible. Todos los derechos reservados.

- **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

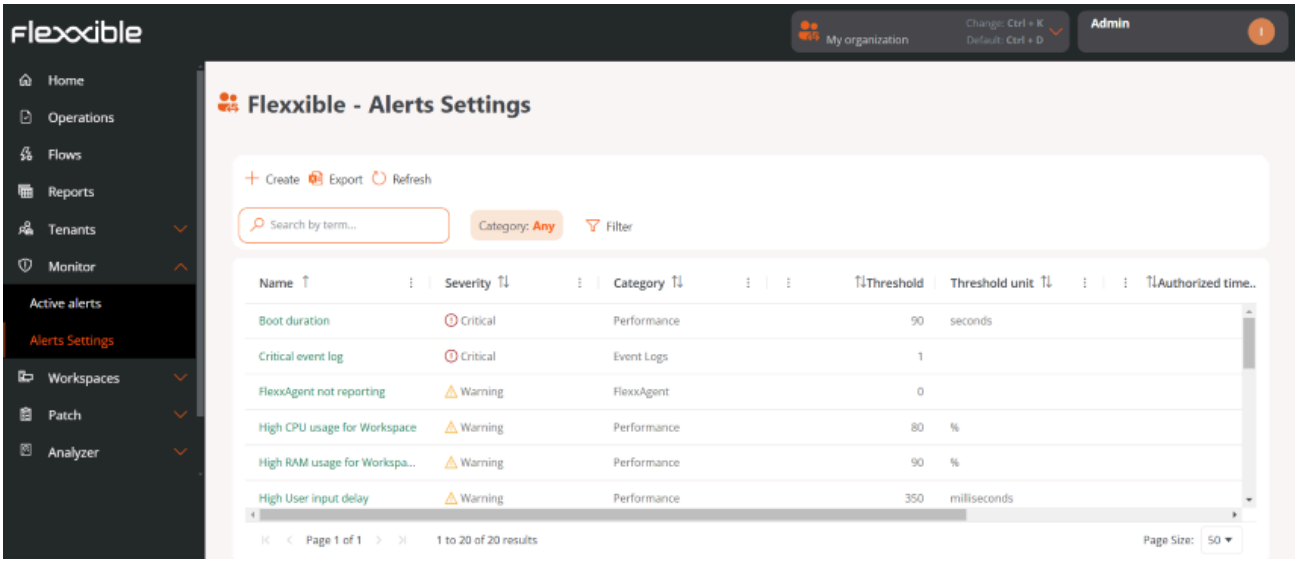
To view specific information, click on the alert name in the table. From this view, you can also access the details of the device where the alert occurs and its report group.



Copyright © 2024 Flexxible. Todos los derechos reservados.

Portal / Monitor / Alert Configuration

This section allows you to check 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.



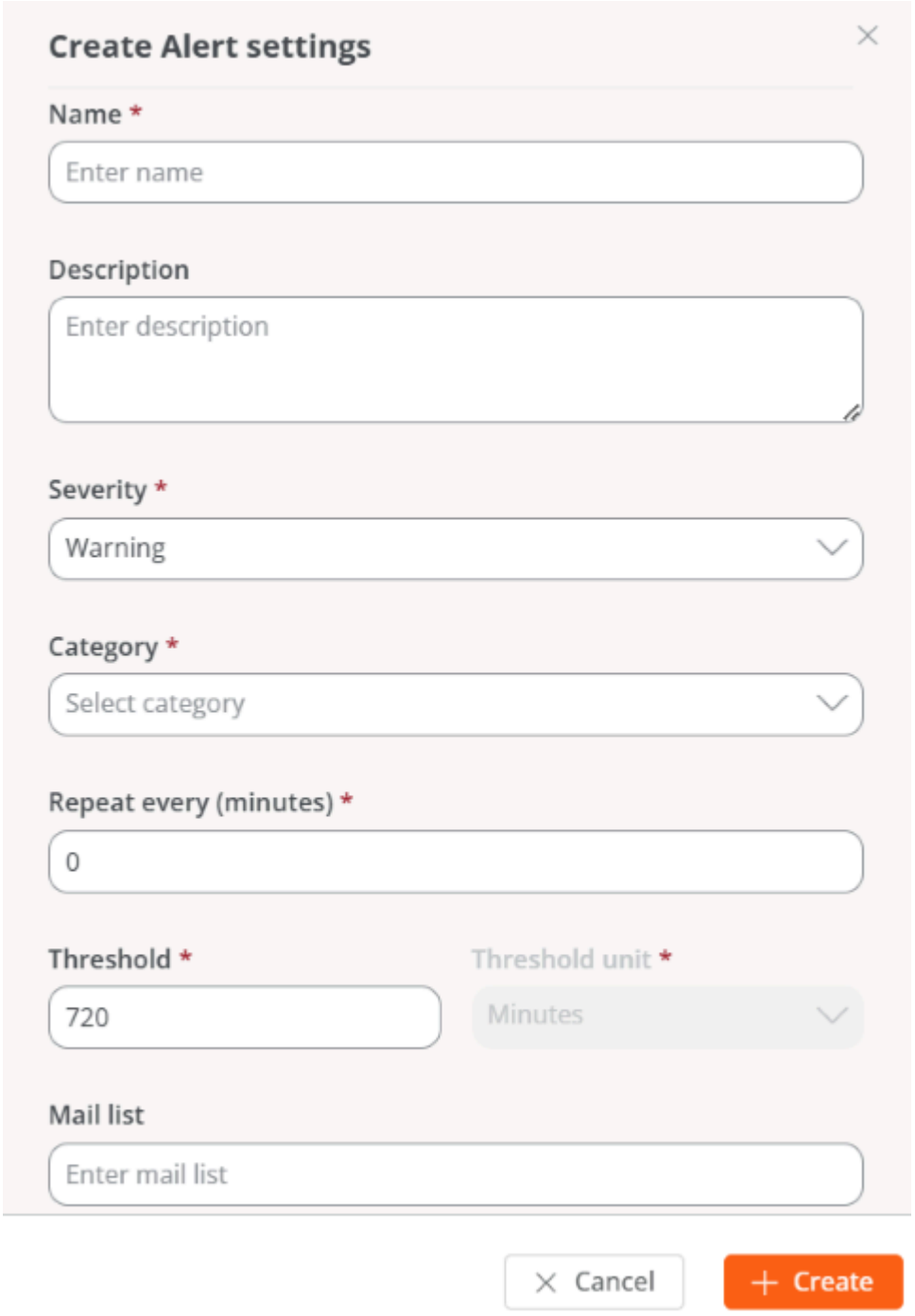
The list view displays a table with the alerts that could be activated on the device. The fields contain the following information:

- **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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

- **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:

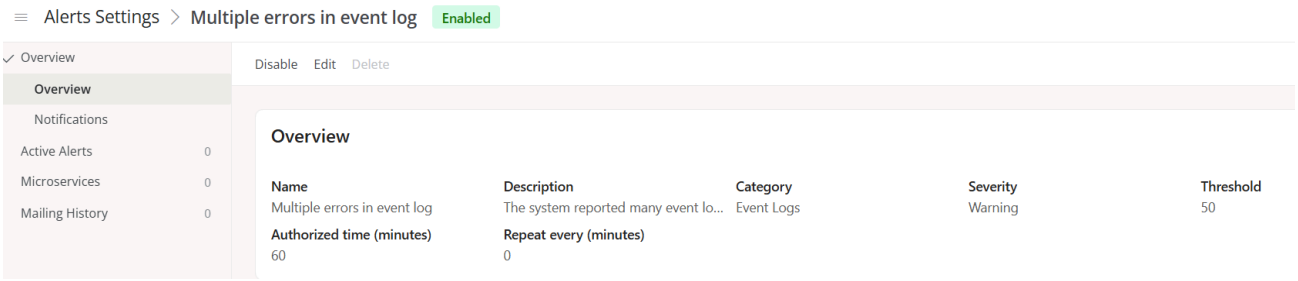
- Connectivity

Copyright © 2024 Flexxible. Todos los derechos reservados.

- 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:

Copyright © 2024 Flexxible. Todos los derechos reservados.

- **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

Copyright © 2024 Flexxible. Todos los derechos reservados.

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.

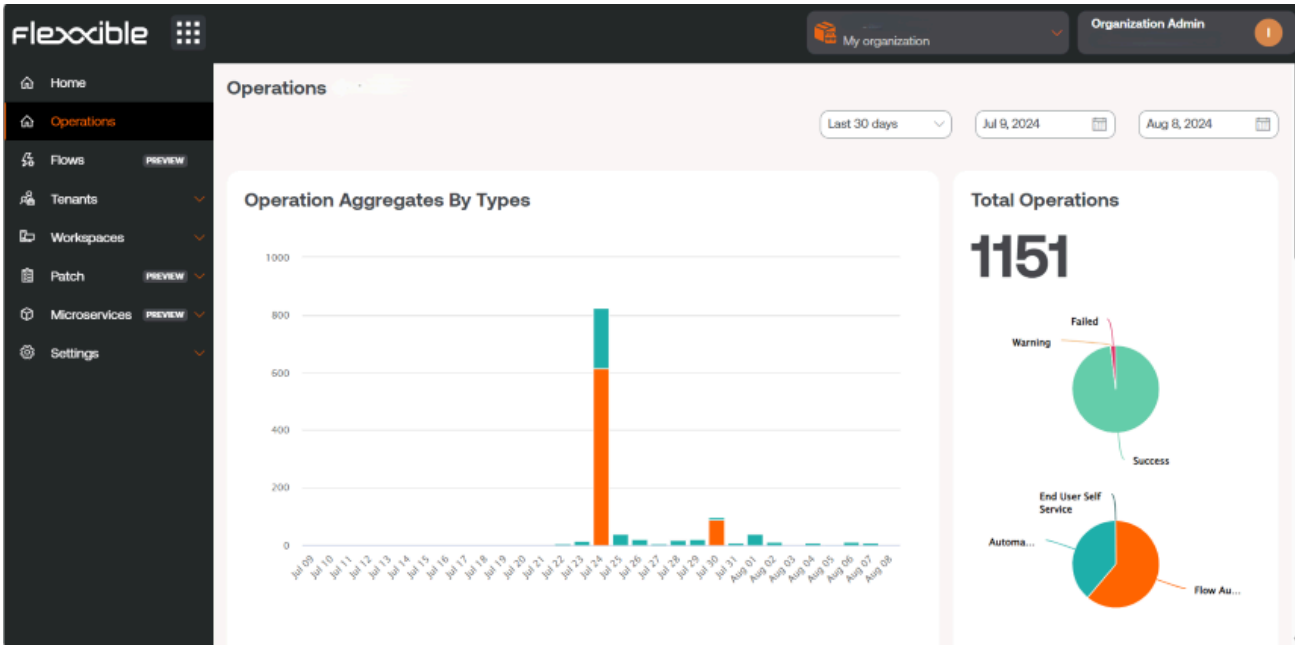
Copyright © 2024 Flexxible. Todos los derechos reservados.

Portal / Operations

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

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

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

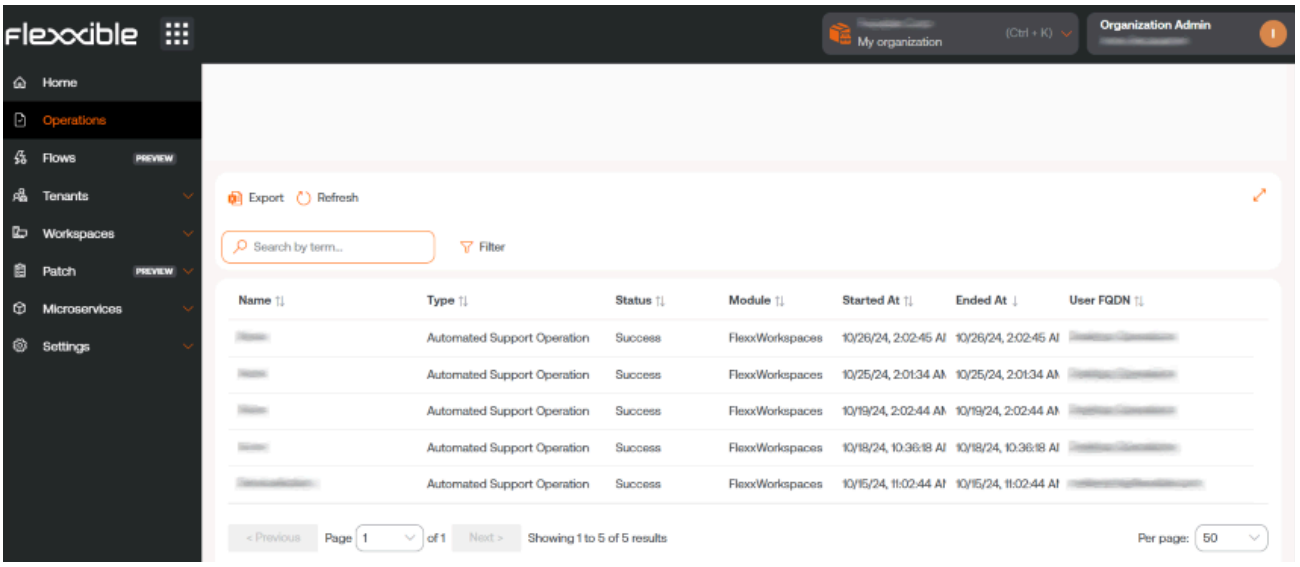


In this view, two types of graphs are generated, with results related to the date range set in the top menu.

- **Operations by type.** Shows the number of operations performed by type and day, following the selected date cycle.

Copyright © 2024 Flexxible. Todos los derechos reservados.

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



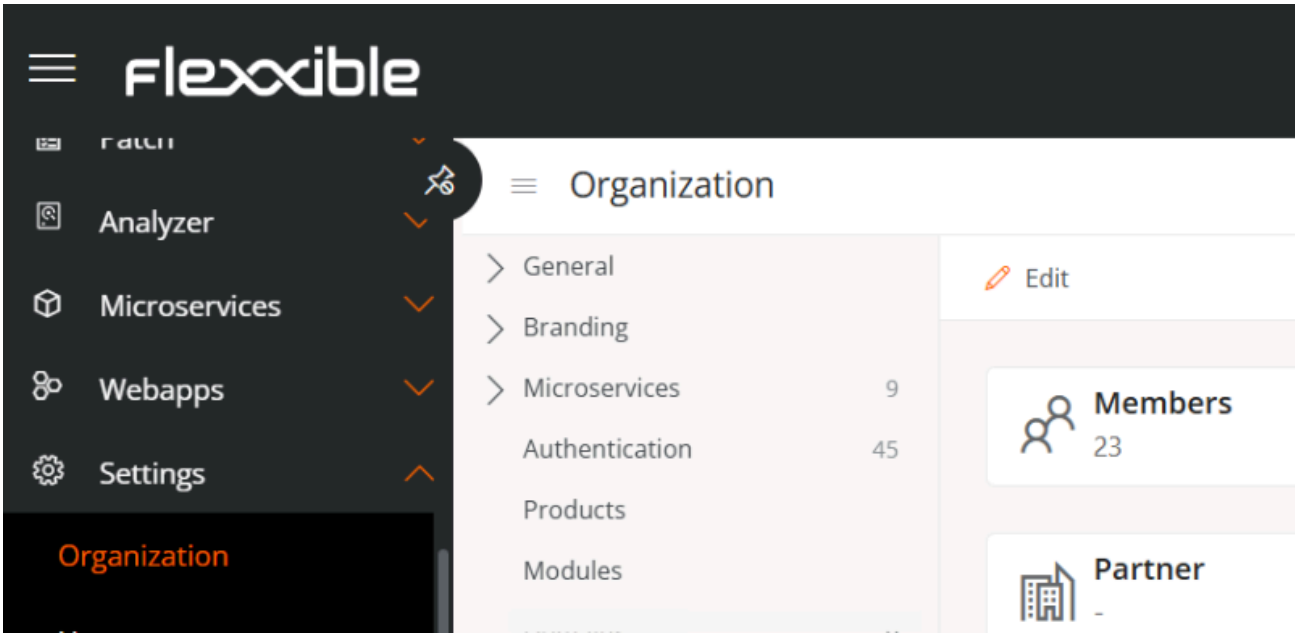
Operation List displays a table with details of the executed operations, specifying the type of operation, from which module they were carried out, and the start and end times. At the bottom of the view, there is a bar that allows you to navigate between pages, to see the details of all executions.

Copyright © 2024 Flexxible. Todos los derechos reservados.

Portal / 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.

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.



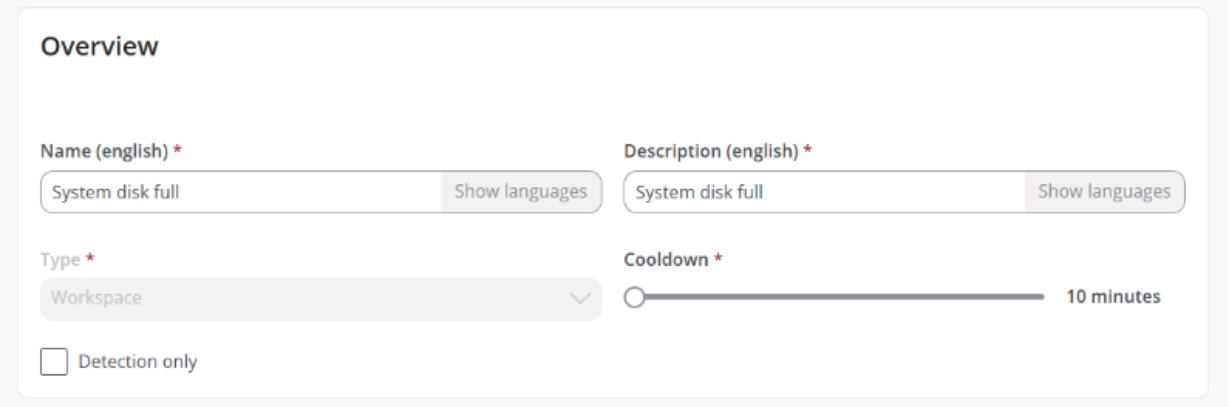
The list view presents the flows created in the organization, along with the following information:

- **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

Copyright © 2024 Flexxible. Todos los derechos reservados.

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 configuration parameter for the minimum cooldown time is set to 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

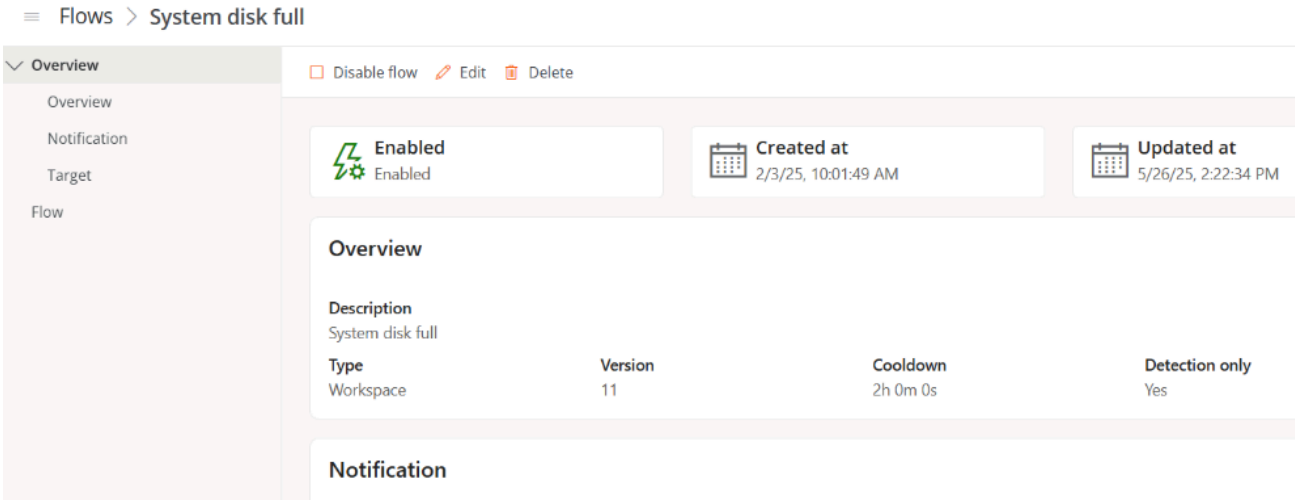
Copyright © 2024 Flexxible. Todos los derechos reservados.

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

Overview

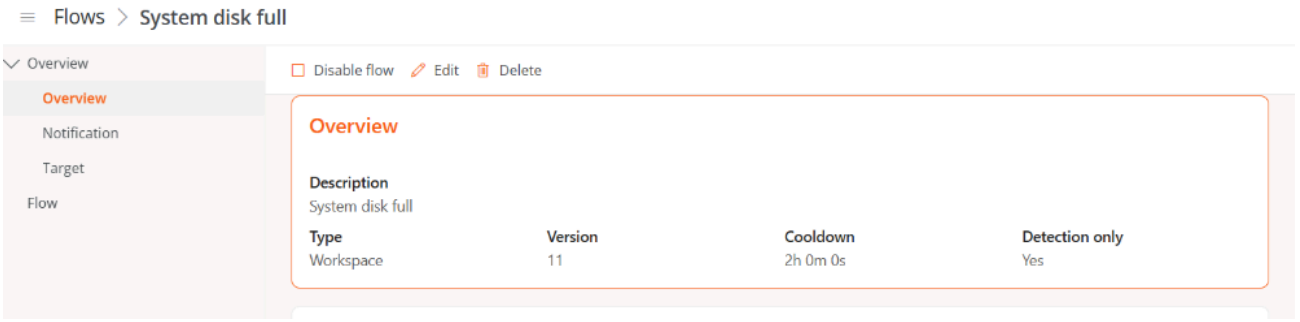
Stores the flow configuration data. It is divided into three tabs:

- Overview
- Notification
- Target



Overview

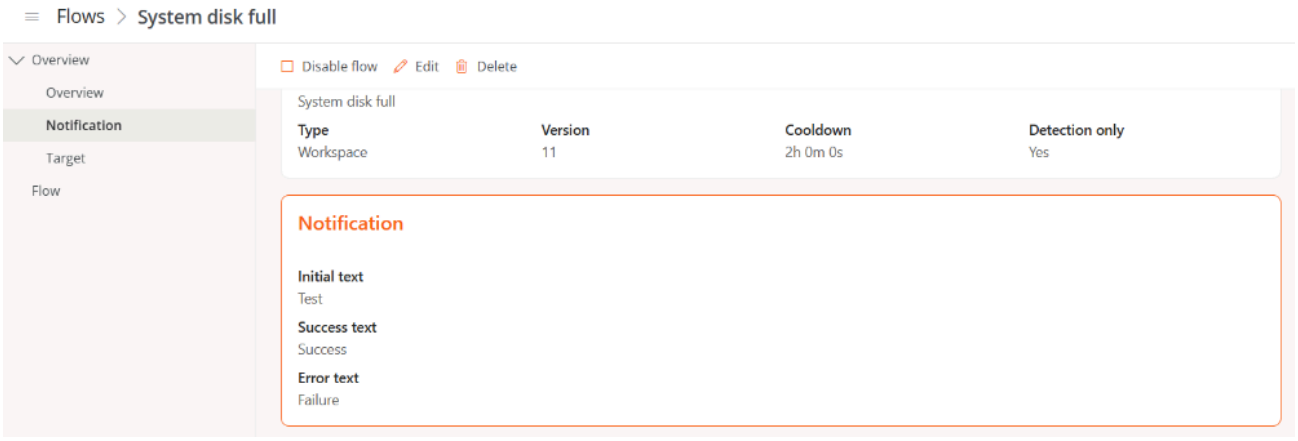
Provides general flow information: *Description*, *Type*, *Cooldown Time* and if it is set to *Detection Only*. It also reports on the *Version*, which increments by one each time the flow is edited.



Copyright © 2024 Flexxible. Todos los derechos reservados.

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.

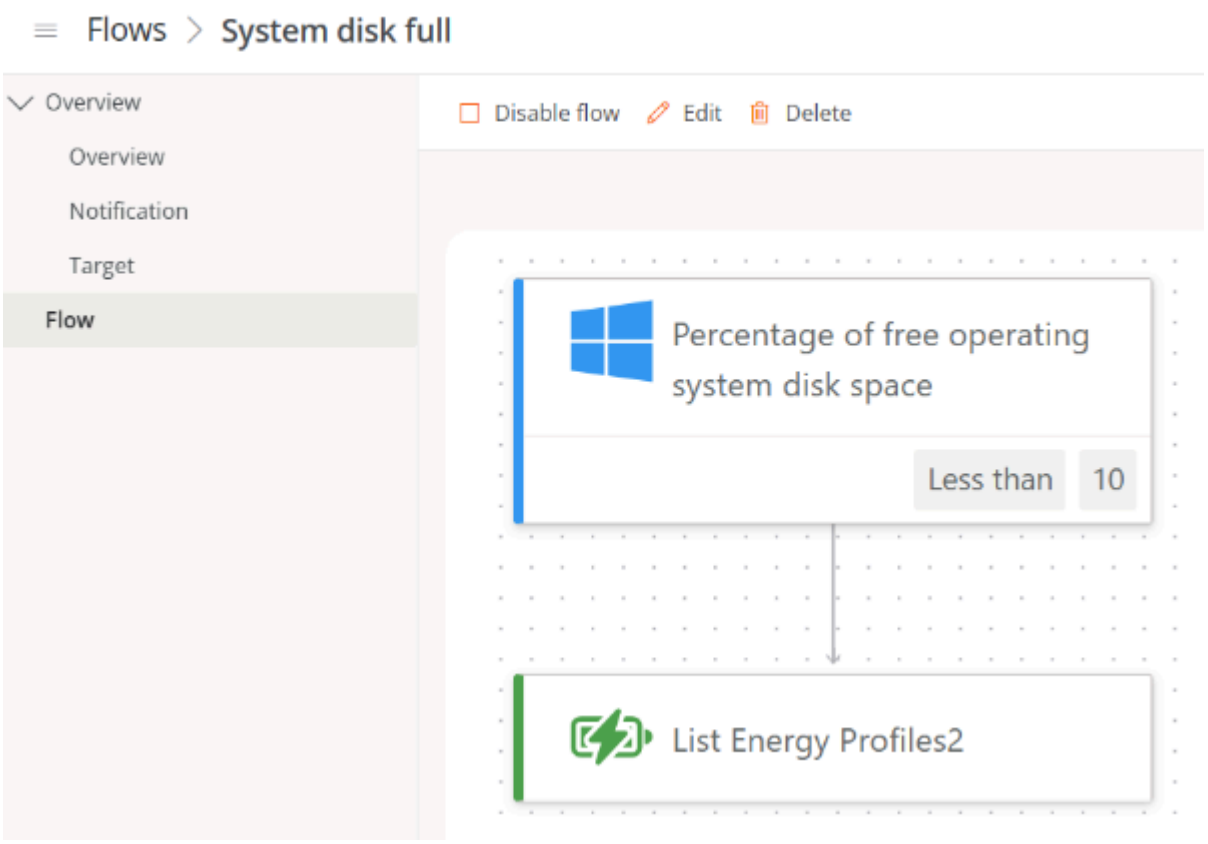
- **All workspaces.** All devices in the organization.
- **Workspaces.** Specific devices.
- **Workspace groups.** Specific workspace groups.
- **Report groups.** Specific report groups.

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

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>`

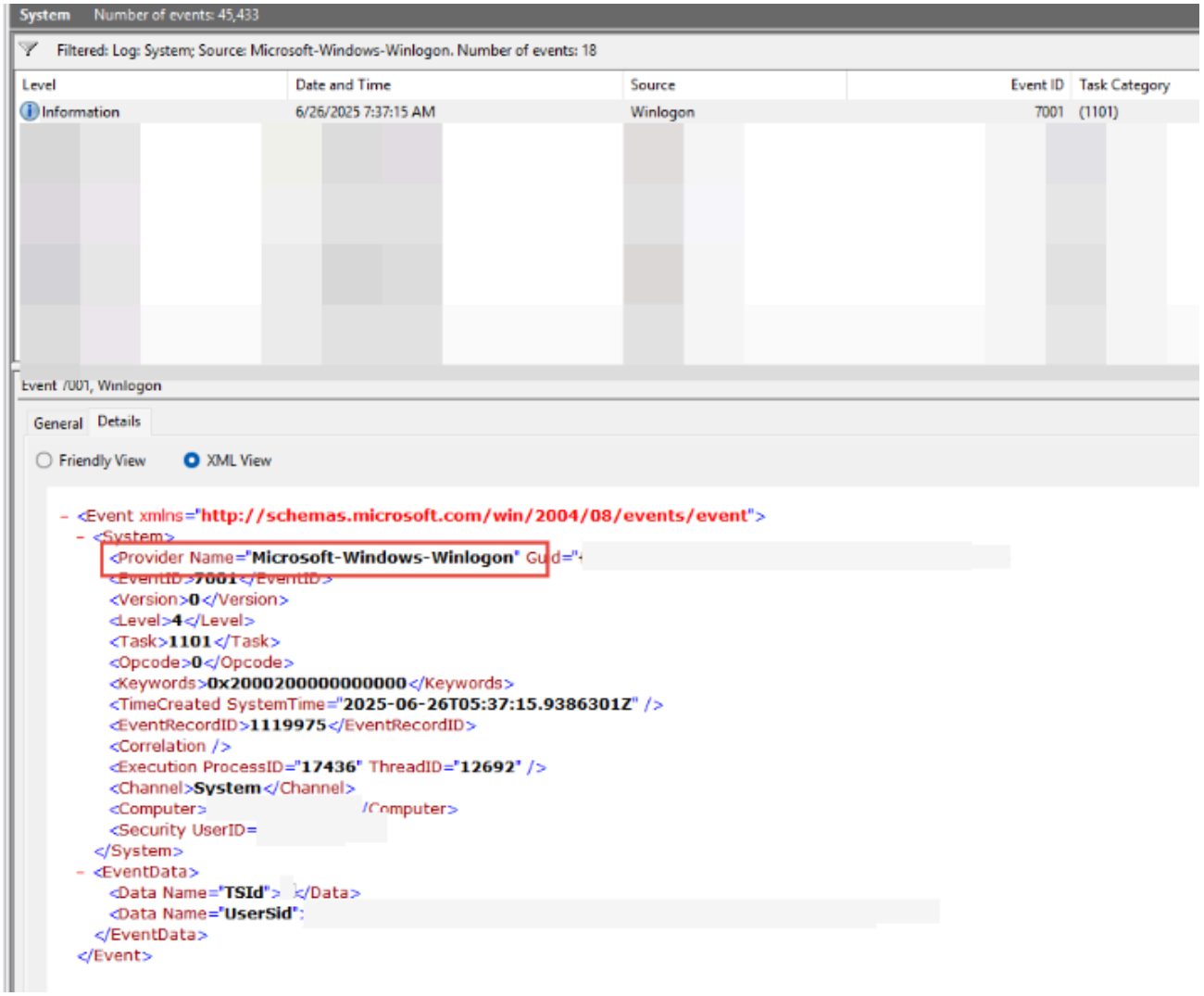
Copyright © 2024 Flexxible. Todos los derechos reservados.

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

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

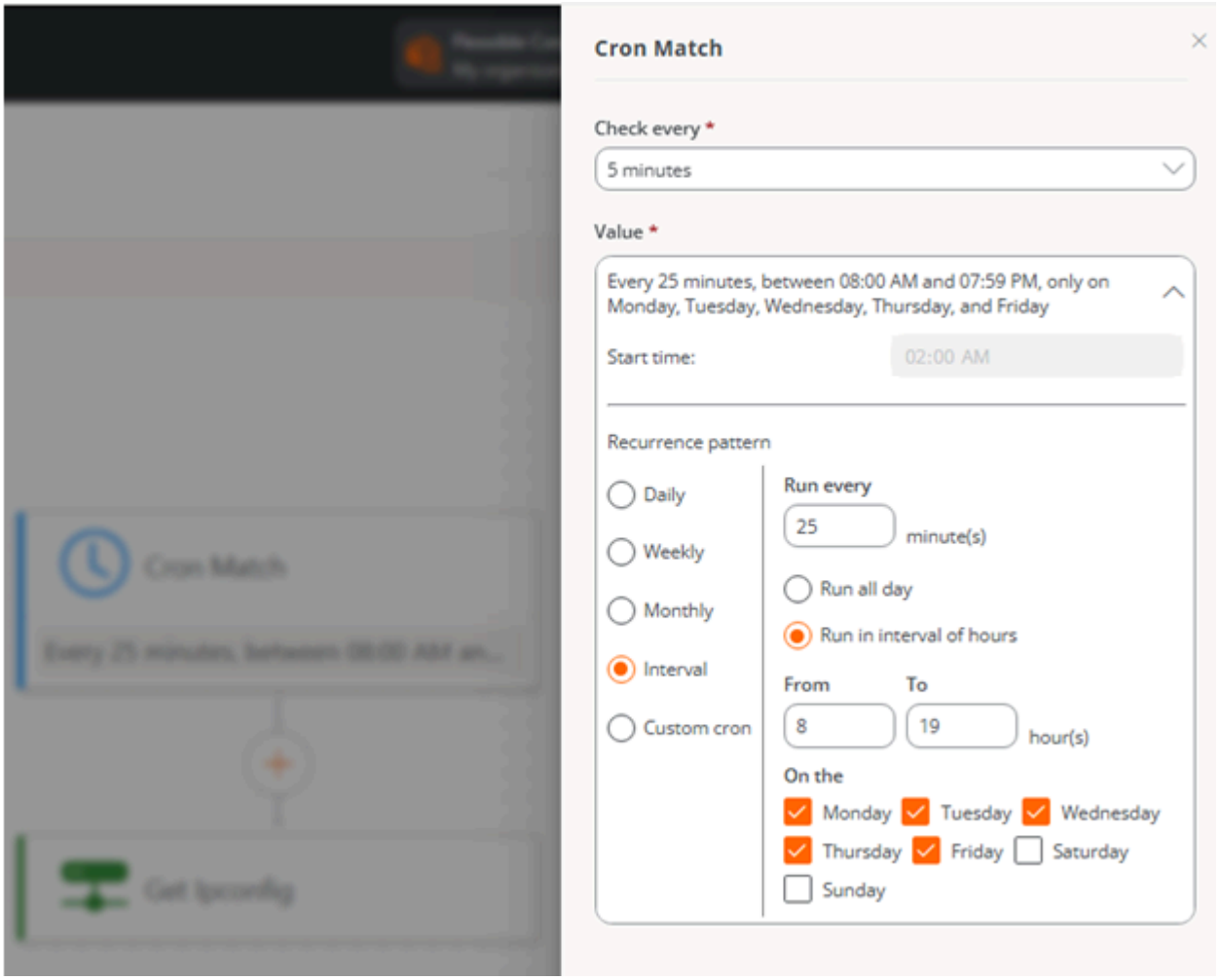
Checks if the current date and time match the schedule defined graphically in the *Value* field. If there is a match, the scheduled action will be executed.

- **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.

Copyright © 2024 Flexxible. Todos los derechos reservados.



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

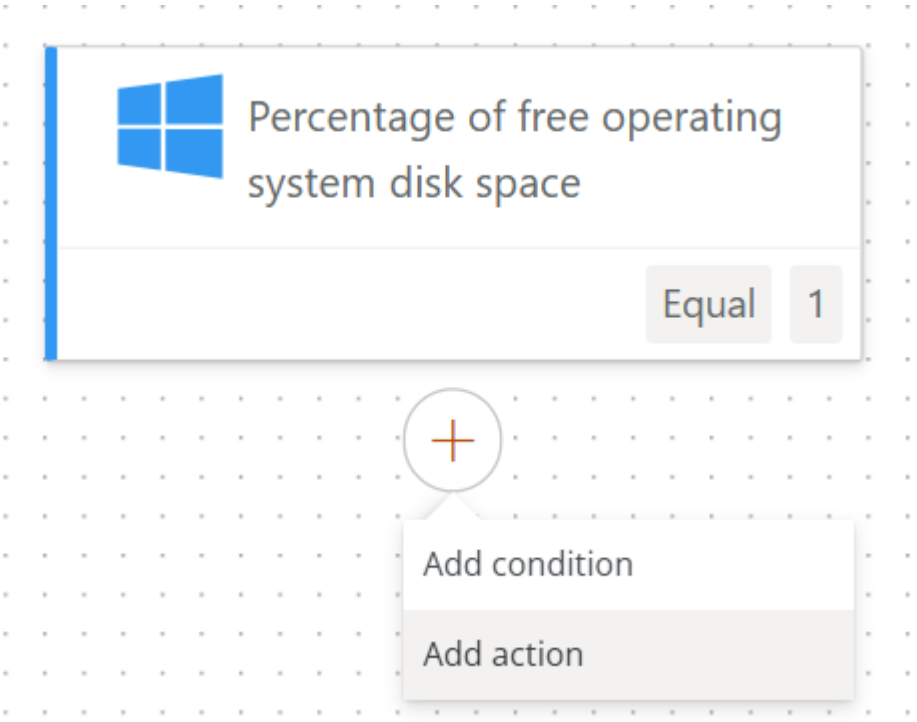
> **INFO**
>
> If you wish to implement custom flow conditions — such as evaluating uptime in days, checking the current status of services, or any other parameter that can be analyzed locally from the device — please consult with Flexxible.

Copyright © 2024 Flexxible. Todos los derechos reservados.

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

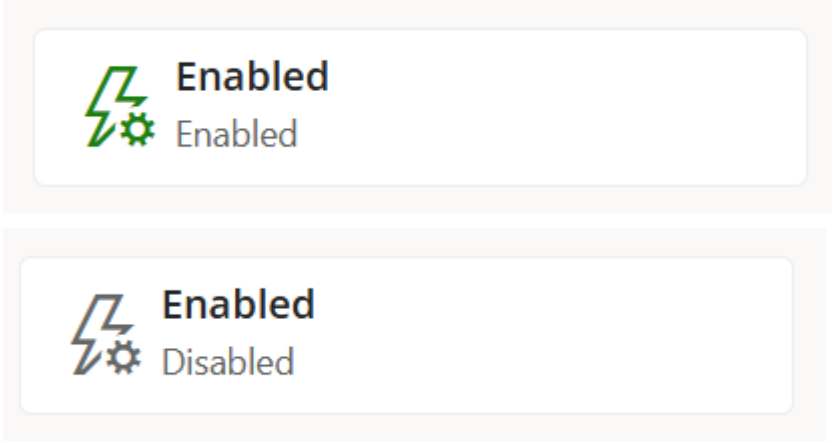
Once a flow is created, it can be managed through the following options:

- Enable/Disable Flow
- Edit
- Delete

Copyright © 2024 Flexxible. Todos los derechos reservados.

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.



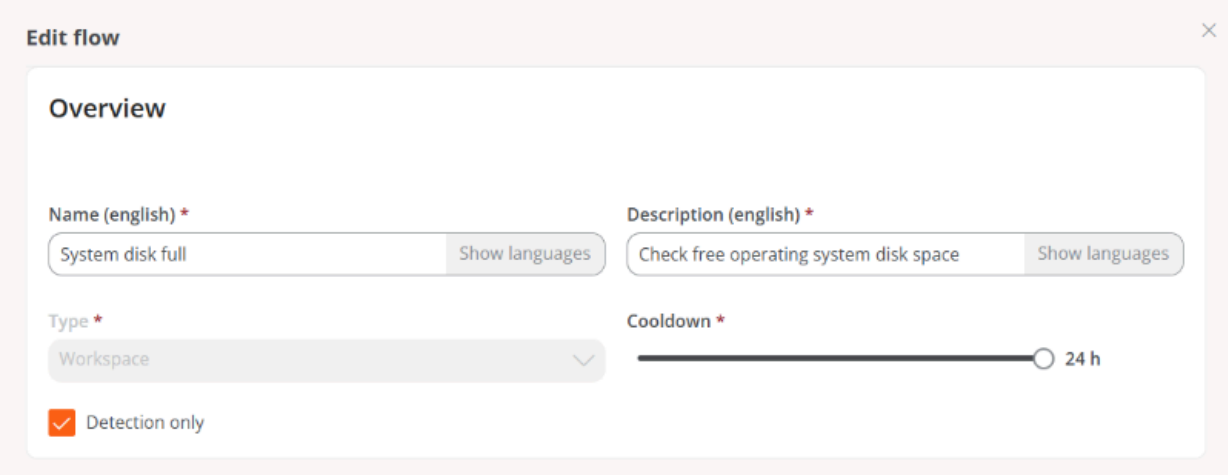
Edit - Overview, Notification, and Target

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

- Overview

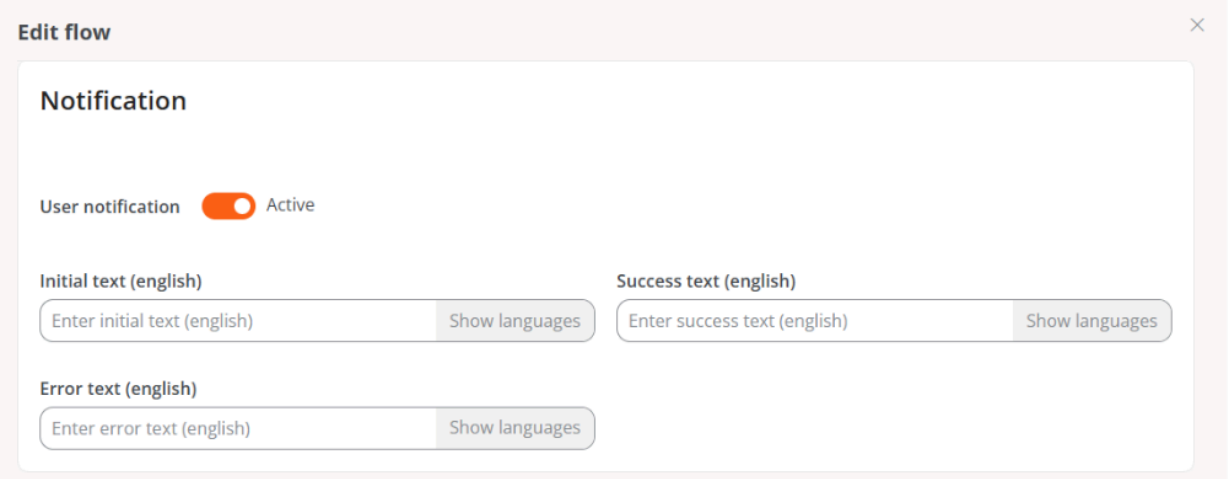
  Allows editing the name of the flow, its description, execution scope, reuse time, and the option to execute or not the microservice once the conditions are met. Each field is explained in the Overview section and in the guide Schedule microservices execution.

Copyright © 2024 Flexxible. Todos los derechos reservados.



- Notification

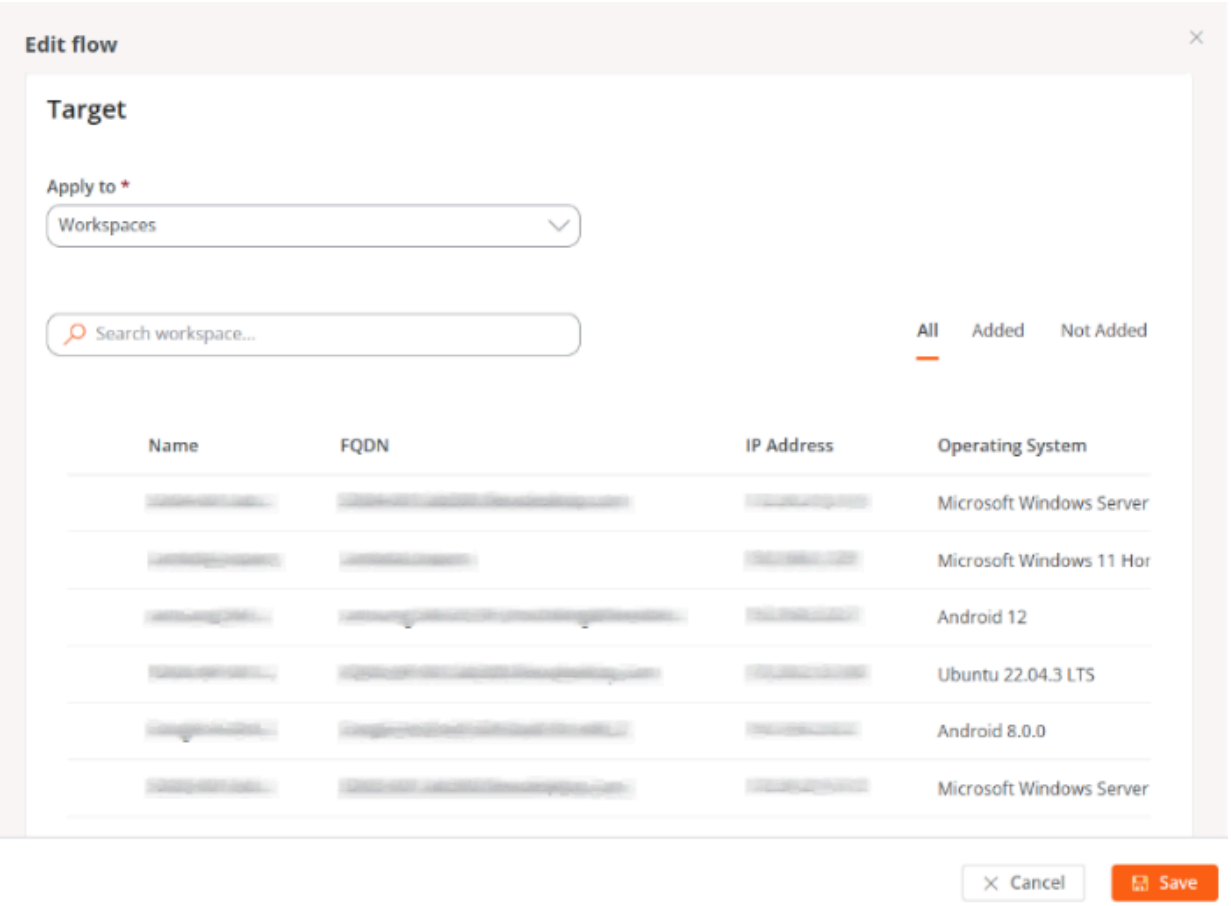
  Allows enabling or disabling sending notifications to users and editing their content. The available message types are explained in the Notification section and in the guide Schedule microservices execution.



- 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.

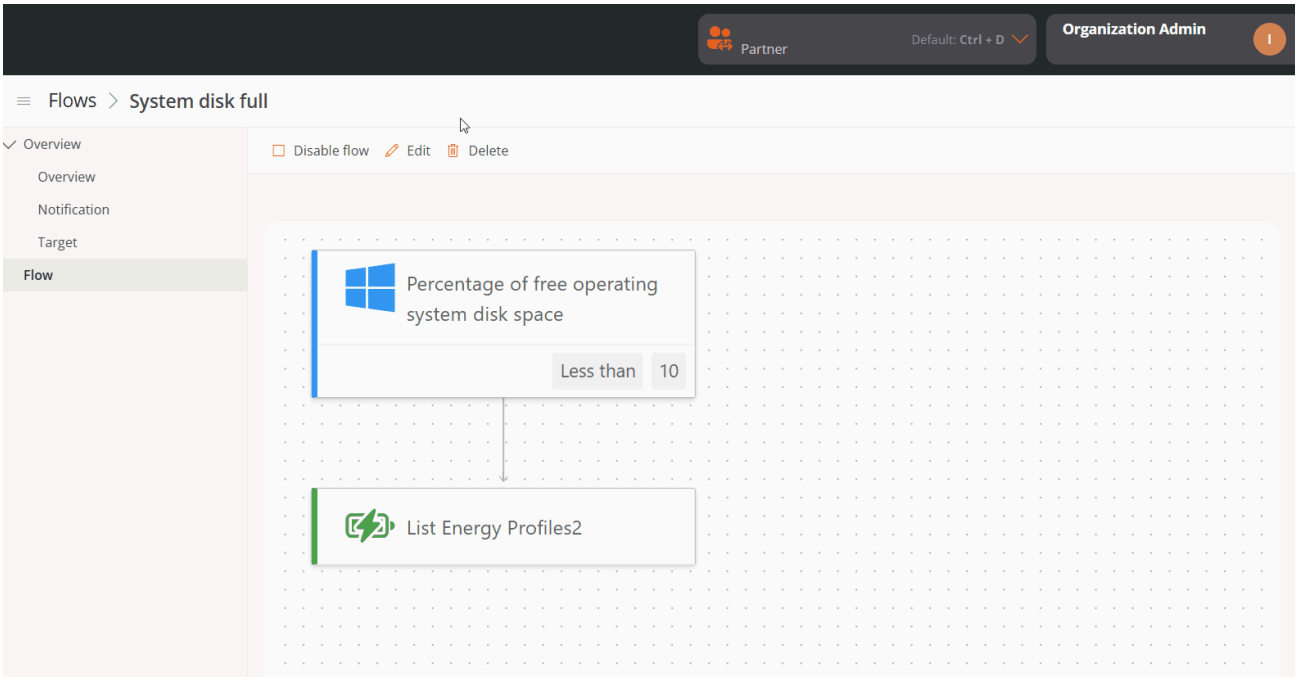
Copyright © 2024 Flexxible. Todos los derechos reservados.



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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

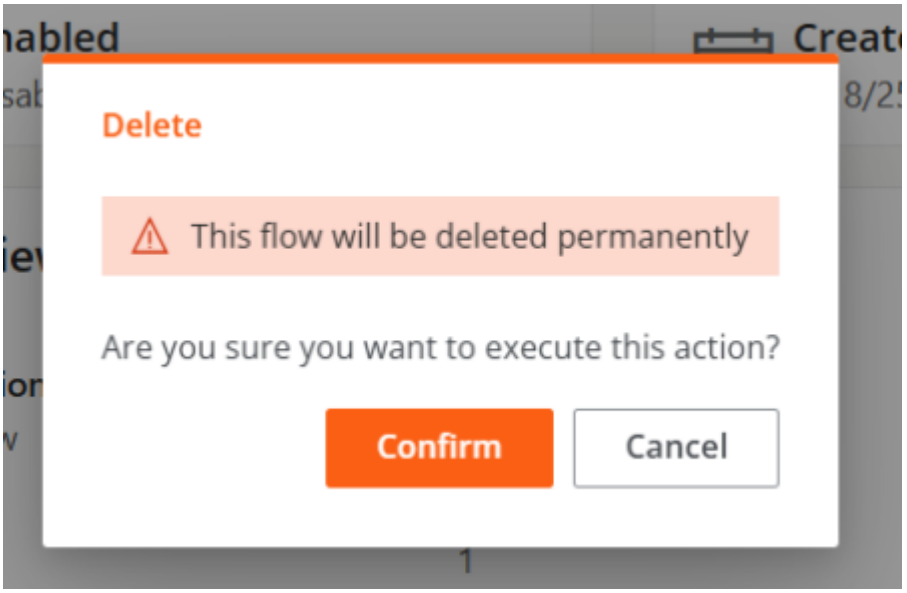


INFO

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

Delete

Allows permanent removal of the flow.



Copyright © 2024 Flexxible. Todos los derechos reservados.

Portal / Reports

The Reports system offered by Portal allows users with the *Organization Administrator* role to generate predefined reports, with relevant data from their organization's device fleet, for reviewing on-screen or sending via email.

Considerations about the reports

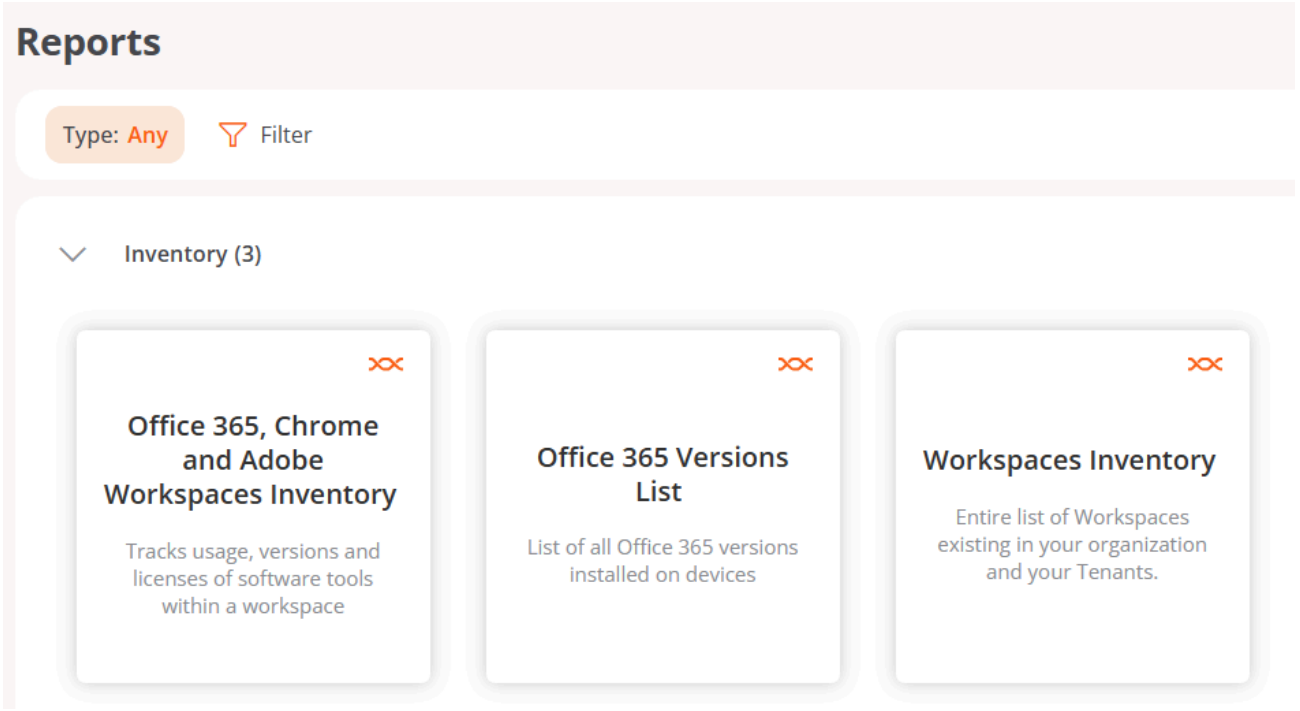
- They are automatically generated once a week.
- Historical reports will remain available in Portal for two months.
- It's possible to configure the automatic sending of reports, so that by specifying email addresses, the report is sent weekly.

Report inventory

Portal offers three types of predefined reports:

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

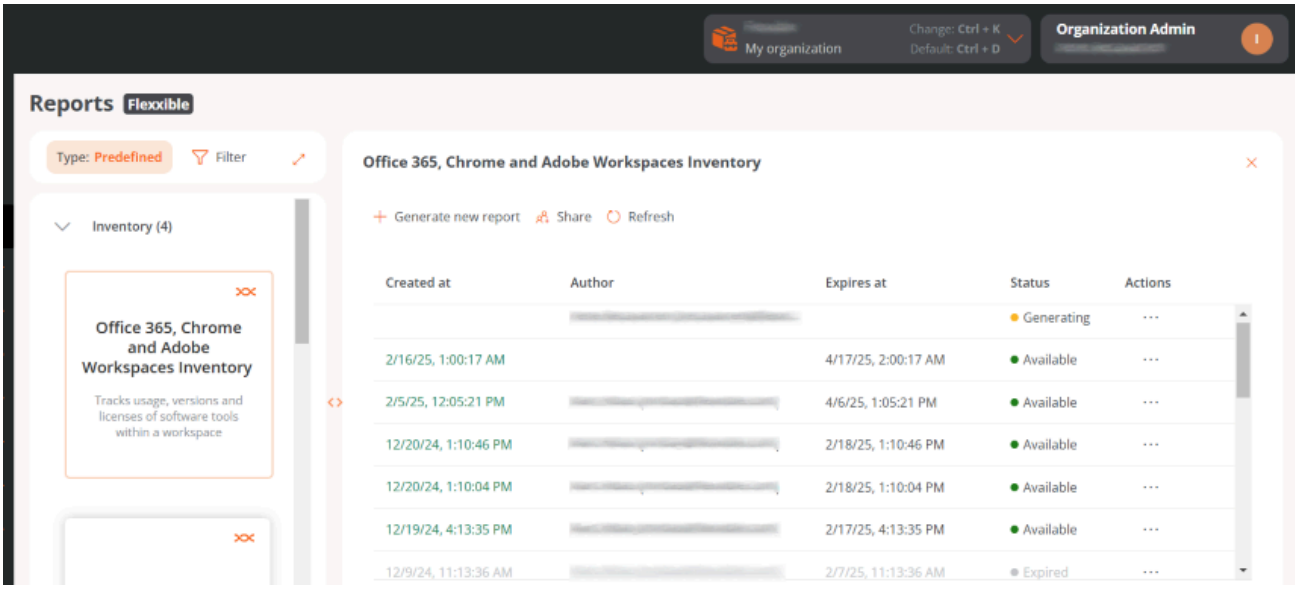
Copyright © 2024 Flexxible. Todos los derechos reservados.



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.

Copyright © 2024 Flexxible. Todos los derechos reservados.



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

Copyright © 2024 Flexxible. Todos los derechos reservados.

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

- **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

Copyright © 2024 Flexxible. Todos los derechos reservados.

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).

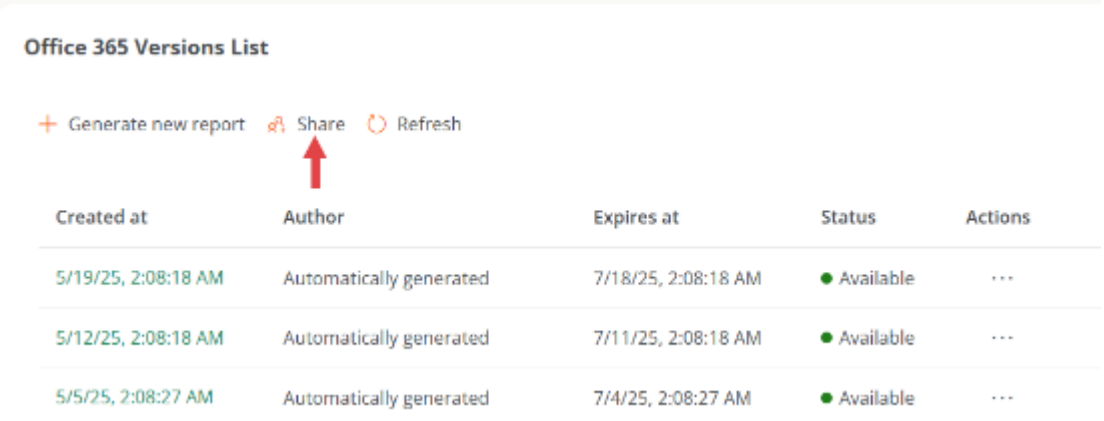
Reports can be shared with one or more recipients.

Share the last report

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

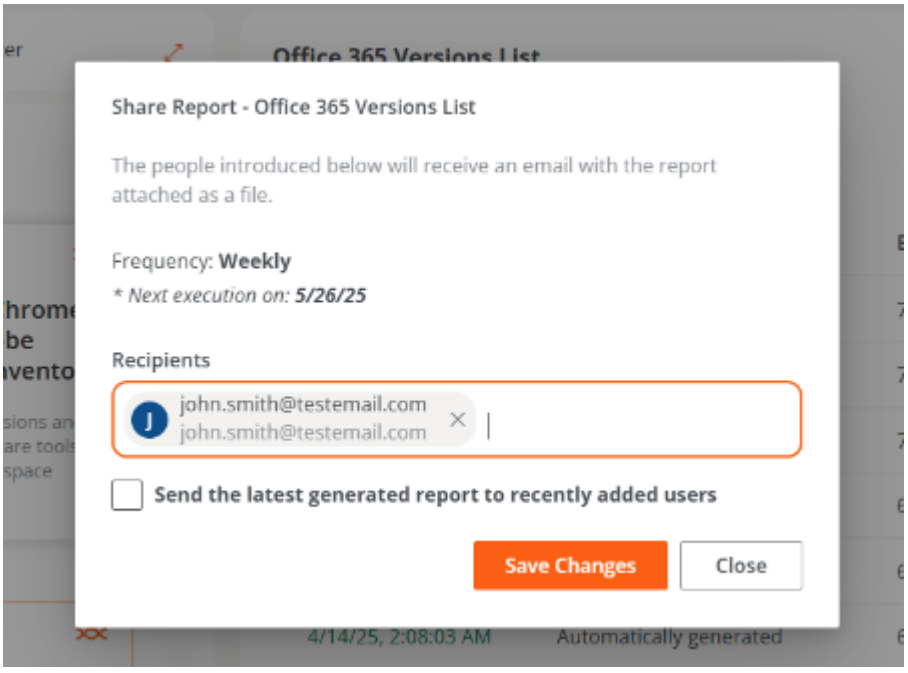
1. Go to `Portal` -> `Reports` and select a report type in the inventory.

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

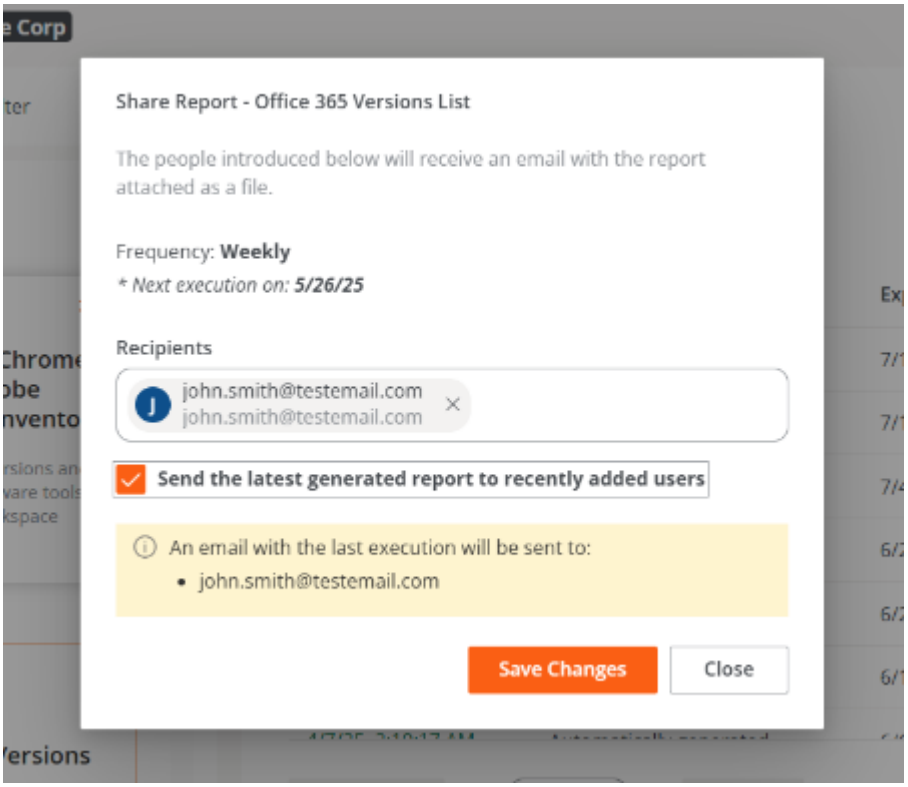


Copyright © 2024 Flexxible. Todos los derechos reservados.

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`.



Copyright © 2024 Flexxible. Todos los derechos reservados.

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

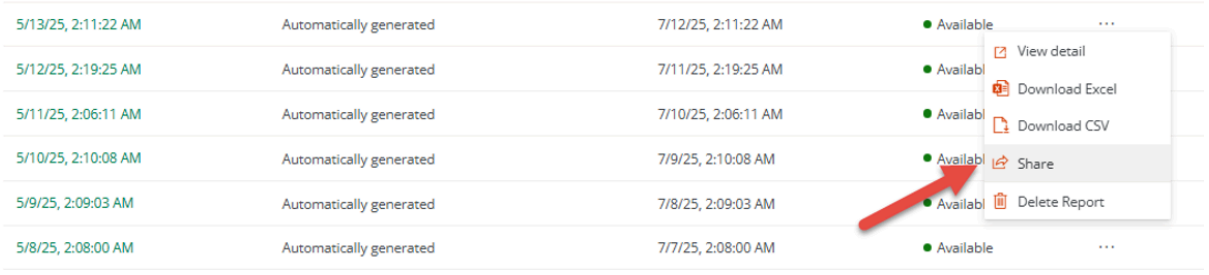
> **INFO**
>
> If email addresses are added and `Save changes` is clicked without selecting `Send the last generated report to newly added users`, the addresses will be saved correctly. This allows adding others later without losing the previous ones.

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`

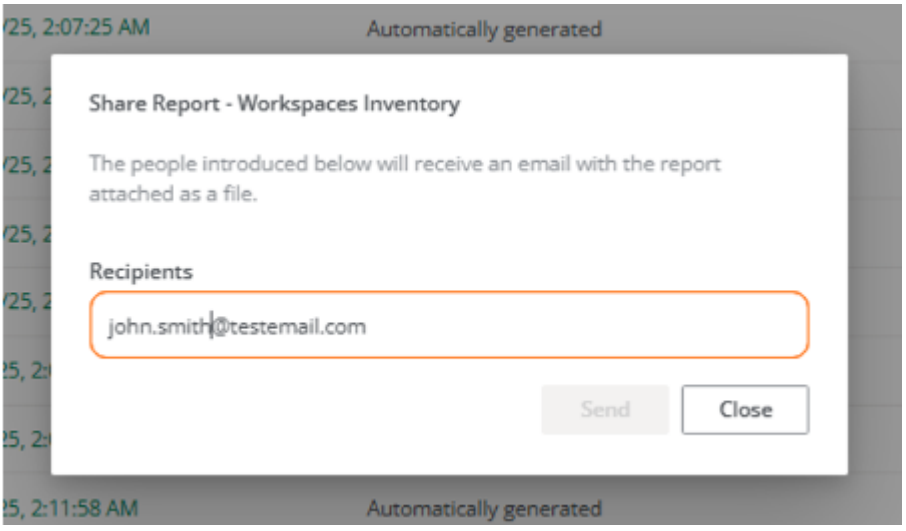
Share a specific report

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`.

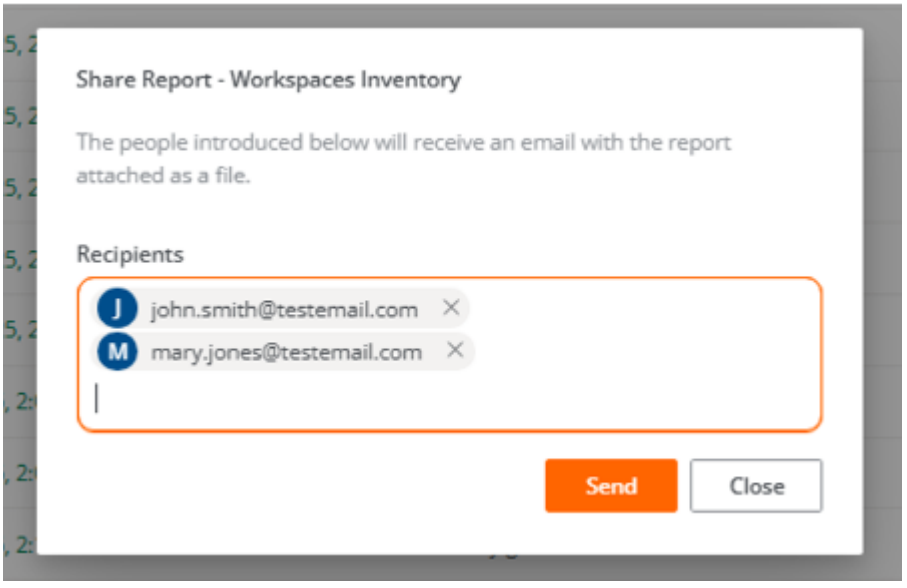


3. Enter the email addresses.

Copyright © 2024 Flexxible. Todos los derechos reservados.



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



5. Click `Send`.

Copyright © 2024 Flexxible. Todos los derechos reservados.

Portal / Tenants

Through `Tenants`, organizations operating under the managed service provider (MSP) model have the ability to establish subsidiary entities that they can support whenever needed.

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

Types of organizations

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

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

Partner-type organizations

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

Client-type organizations

- They have the option, if they wish, to segment their organization into multiple suborganizations to facilitate delegated administration.
- They can always see their entire 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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

- 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.

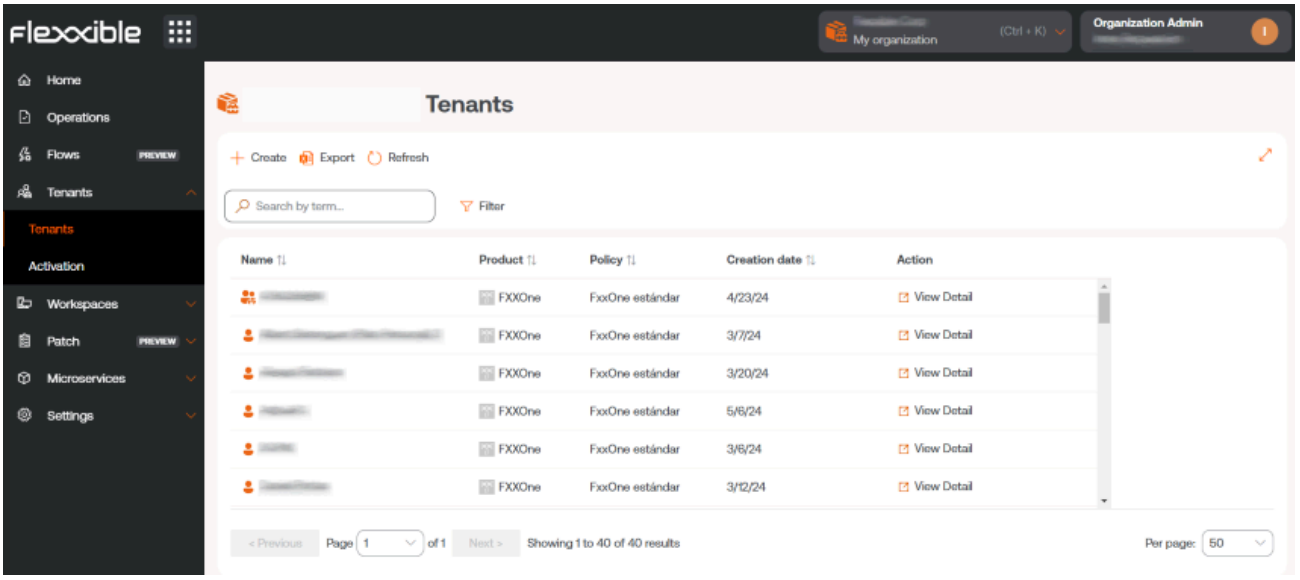
> **INFO**
>
> Client-type organizations can create suborganizations at a lower level. Suborganizations cannot be created from another suborganization.

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.



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*.

Copyright © 2024 Flexxible. Todos los derechos reservados.

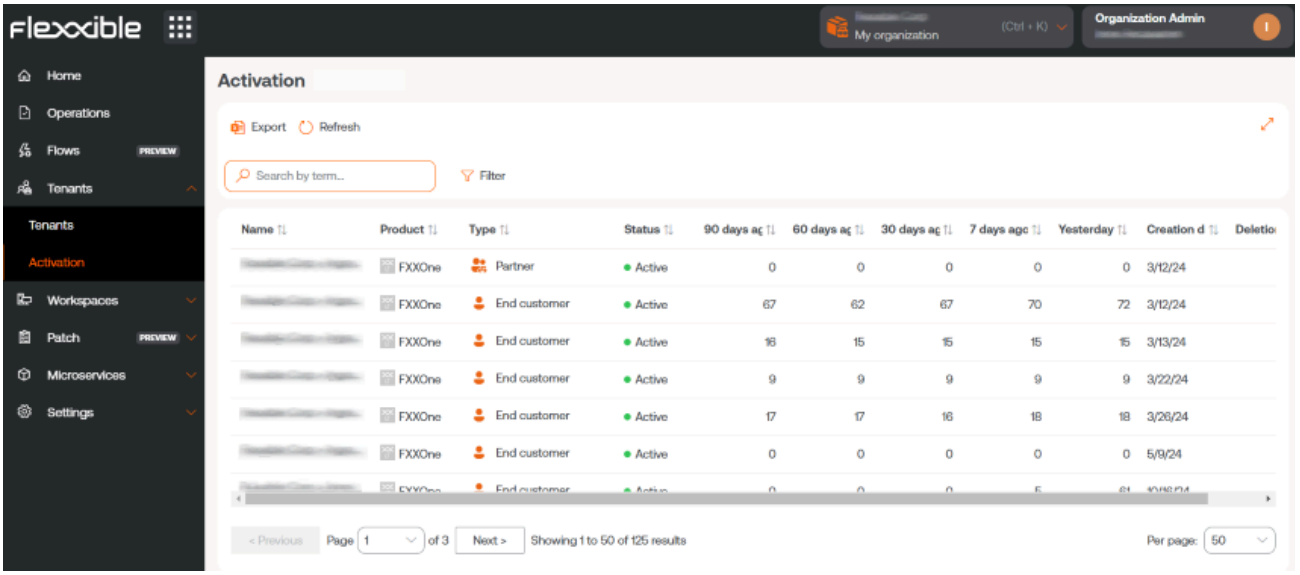
Portal / Tenants / Activation

`Activation` allows Managed Service Providers (MSP) to evaluate the evolution of FlexxAgent installations or deployment 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.

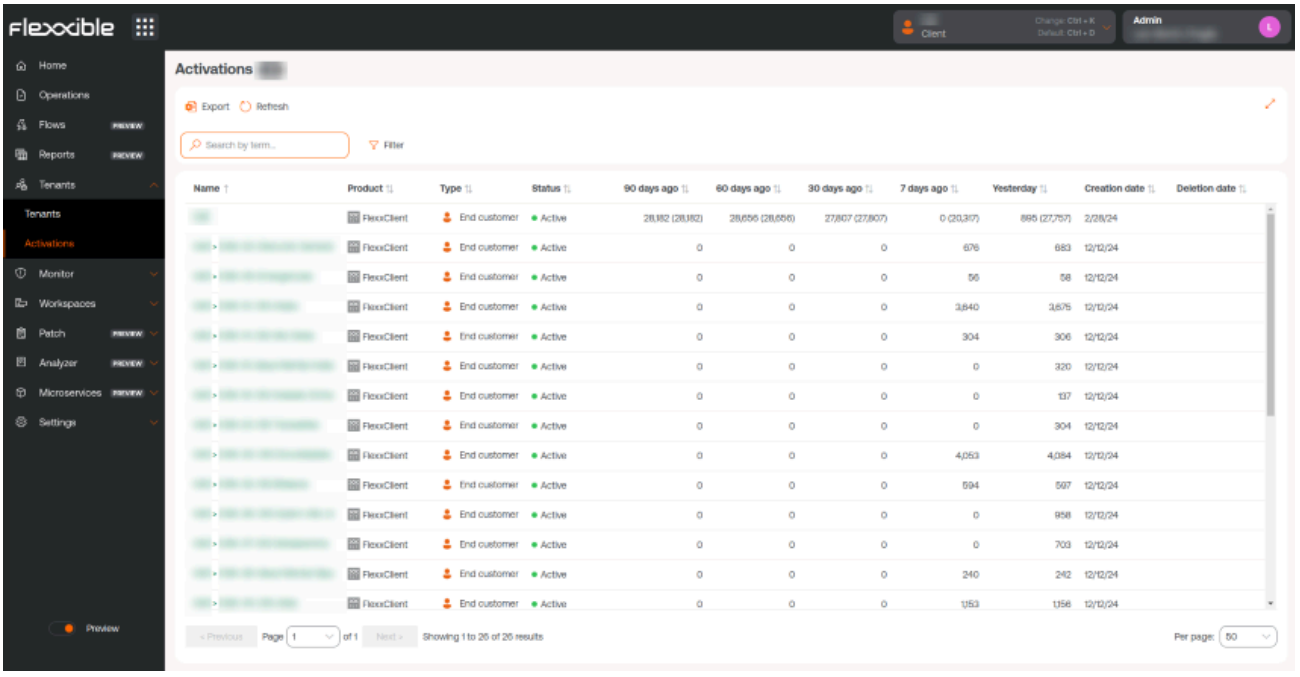
The time indicators offered by the table are *90 days ago*, *60 days ago*, *30 days ago*, *7 days ago* and *Yesterday*. Each field specifies the number (units) of active agents at that particular moment.



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

Copyright © 2024 Flexxible. Todos los derechos reservados.

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

Portal / Workspaces in Portal

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

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

- **Name.** Device Name.
- **Status.** Current status of the device (*Online* or *Offline*).
- **IP Address.** IP Address of the device.
- **Operating System.** Operating System of the device.
- **CPU Cores.** Number of CPU cores that the device has.
- **RAM.** Amount of RAM that the device has, in megabytes (MB).
- **Type.** Type of device (*Physical* or *Virtual*).
- **Last User.** Name of the last user who used the device.
- **Intel vPro Enterprise.** Indicates if the device supports integration with Intel vPro.
  - *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*: The device supports Intel® AMT technology. For more information, please refer to the documentation on the Intel vPro Enterprise integration.

Device detail view

To access more specific data, click on the device's name in the table. Next, at the top of the view, you will see the current status: *Online* (green background) or *Offline* (gray background).

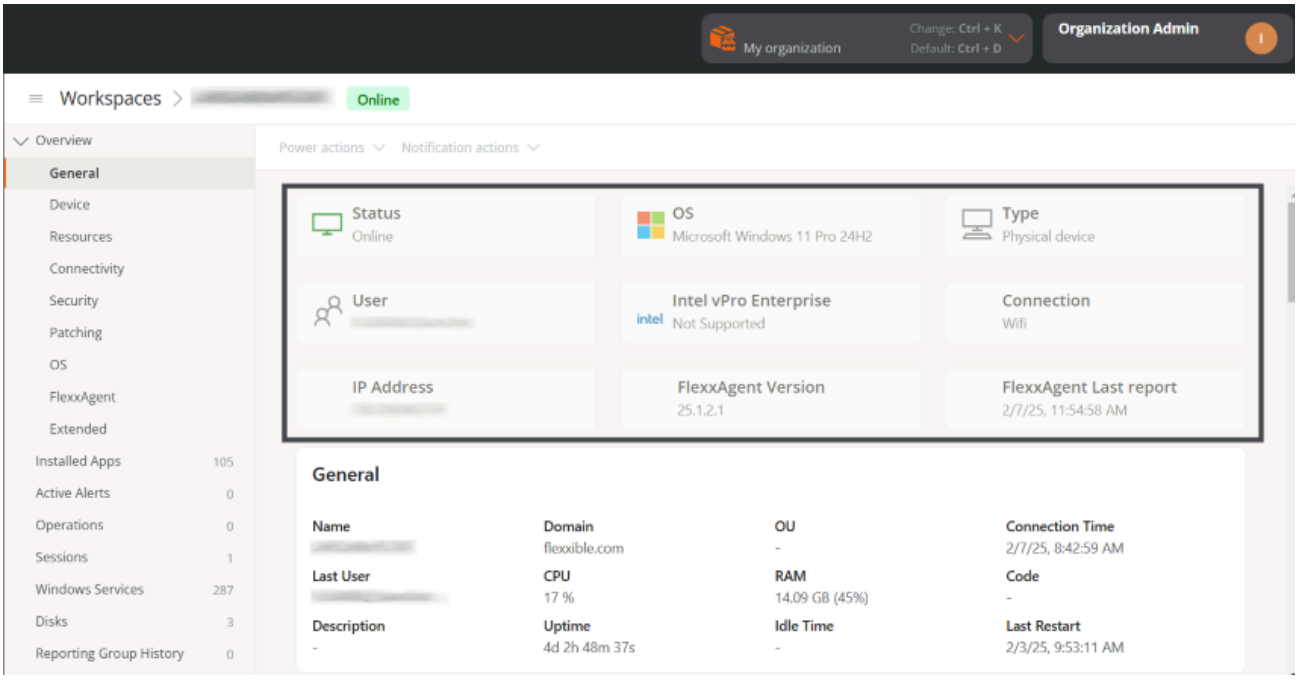
Copyright © 2024 Flexxible. Todos los derechos reservados.

The detail view includes the following tabs:

- Overview
- Installed applications
- Current active alerts
- Operations
- Sessions
- Windows Services
- Disks
- All reporting groups
- PnP Events
- PnP Errors
- Boot history

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*.



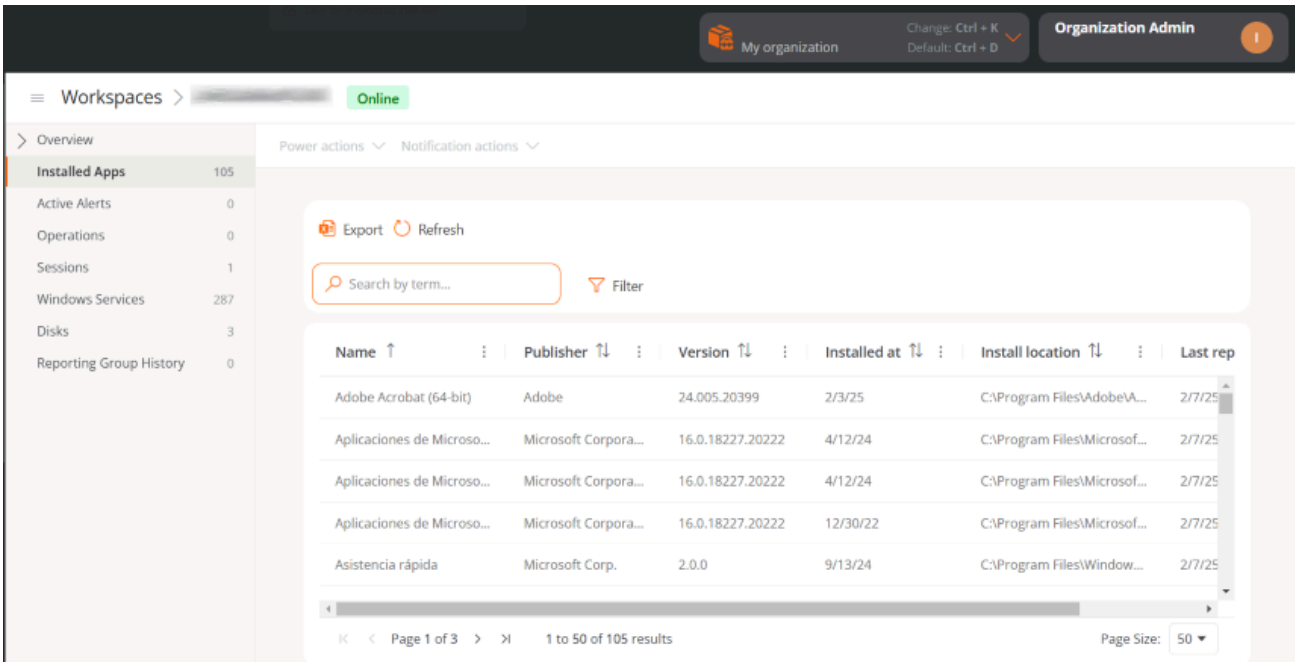
Copyright © 2024 Flexxible. Todos los derechos reservados.

At the bottom, ten sections provide detailed information:

1. **General.** Identification, use, and connection of the device.
2. **Device.** Hardware description of the device.
3. **Resources.** Space resources of the device that are in use.
4. **Connectivity.** Type of connectivity and addresses associated with the device.
5. **Security.** Security solution data for the device.
6. **Update.** Update status of the operating system and the target
7. **OS.** Type, version, and location of the operating system
8. **FlexxAgent.** General status of FlexxAgent on the device and information about its reporting group.
9. **Expanded.** Data about the motherboard and Basic Input Output System (BIOS) of the device.
10. **Virtualization.** Hypervisor, broker, and more data about the virtual device, if applicable.

Installed apps

This tab shows a table with the list of installed applications found by FlexxAgent on the device.



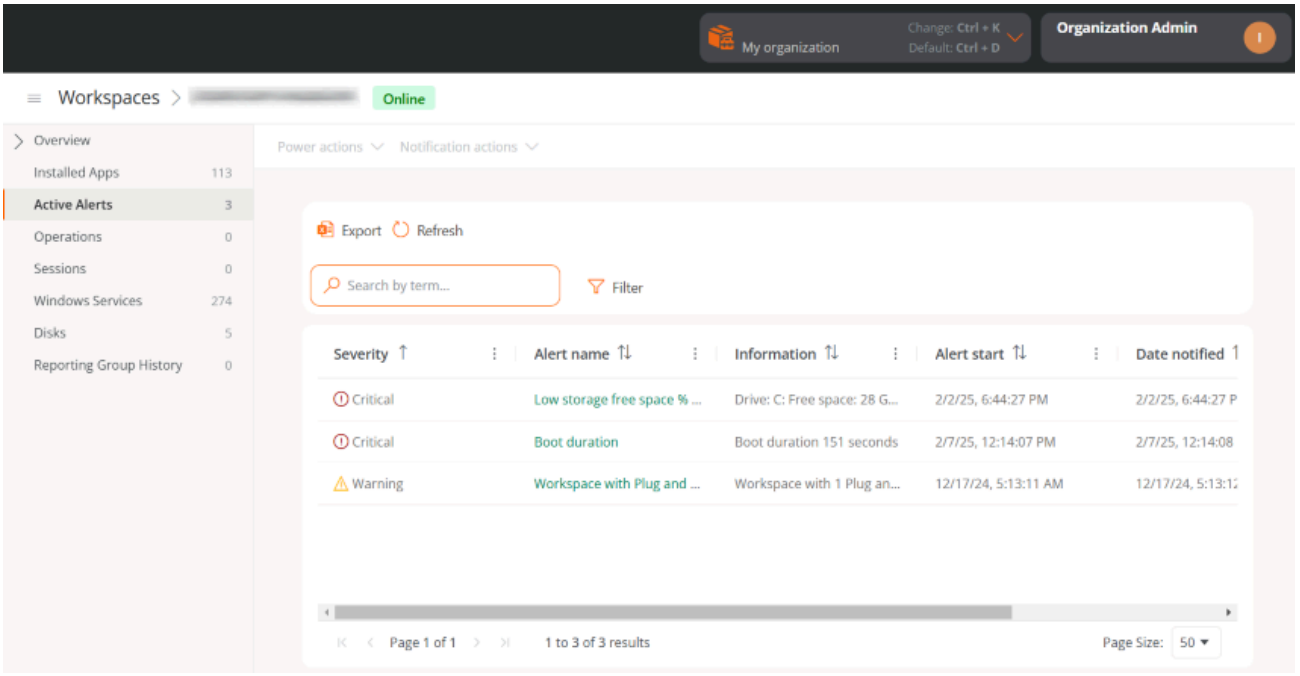
The information includes:

Copyright © 2024 Flexxible. Todos los derechos reservados.

- **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.

Active alerts

This section shows a table with the list of active alerts found on the device.



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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

Operations

This section shows a table with the list of operations recorded on the device. The information includes:

- **Operation Name.** Type of operation performed on the device.
- **Status.** Status of the operation (*Successful* or *Failed*).
- **Created On.** Date and time the operation was created.
- **Start Date.** Date and time the operation started.
- **End Date.** Date and time the operation ended.
- **Owner.** Email of the user who performed the operation.

Sessions

This section shows a table with the list of sessions recorded on the device. The information includes:

- **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

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

Copyright © 2024 Flexxible. Todos los derechos reservados.

- **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

This section shows a table with the list of partitions registered on the device. The information includes:

- **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.
- **OS Unit.**: Unit possession (*Yes* or *No*).
- **Location.**: Path to disk location.
- **Partition.**: Indicates the number of storage divisions the disk has.

Reporting groups history

This section shows a table with the list of reporting groups the device belongs or has belonged to. The information includes:

- **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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

Plug and Play (PnP) events

This section shows a table with the list of PnP events registered on the device. 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.

Plug and Play (PnP) errors

This section shows a table with the list of PnP errors registered on the device. 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.

Boot history

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

Copyright © 2024 Flexxible. Todos los derechos reservados.

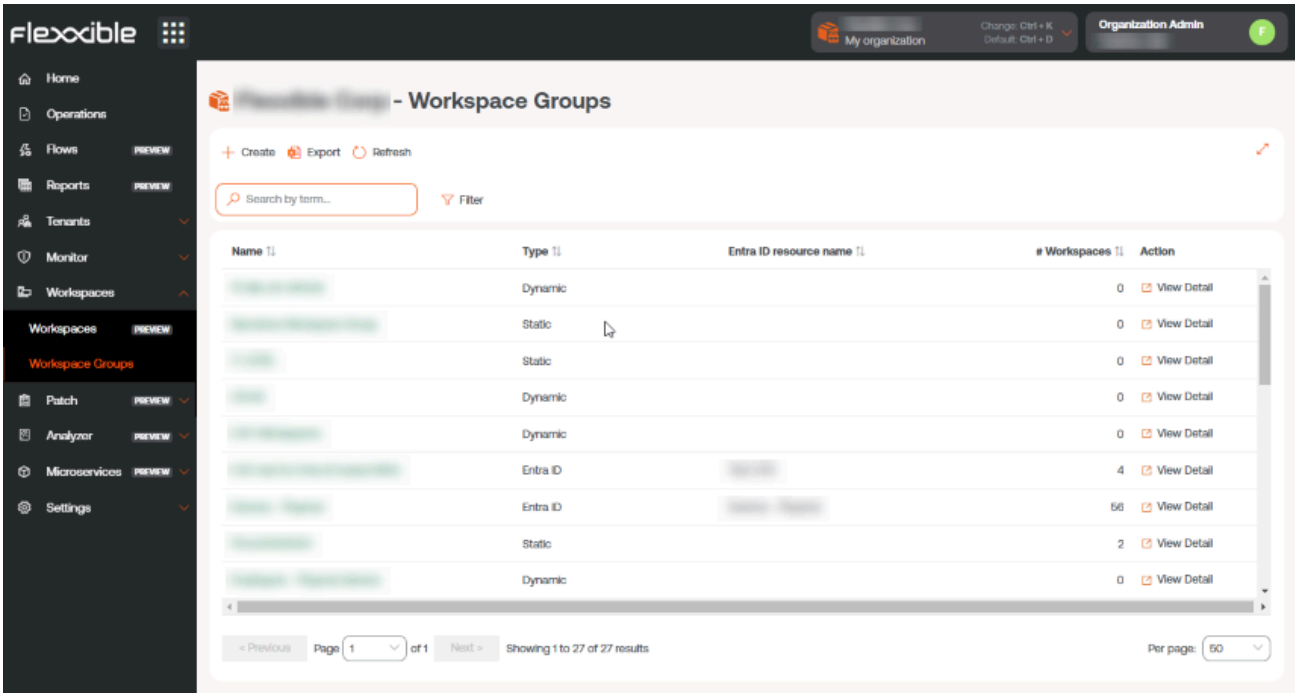
INFO

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

Copyright © 2024 Flexxible. Todos los derechos reservados.

Portal / Workspaces / Workspace groups

Workspace groups make device management easier for organizations by 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

Copyright © 2024 Flexxible. Todos los derechos reservados.

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

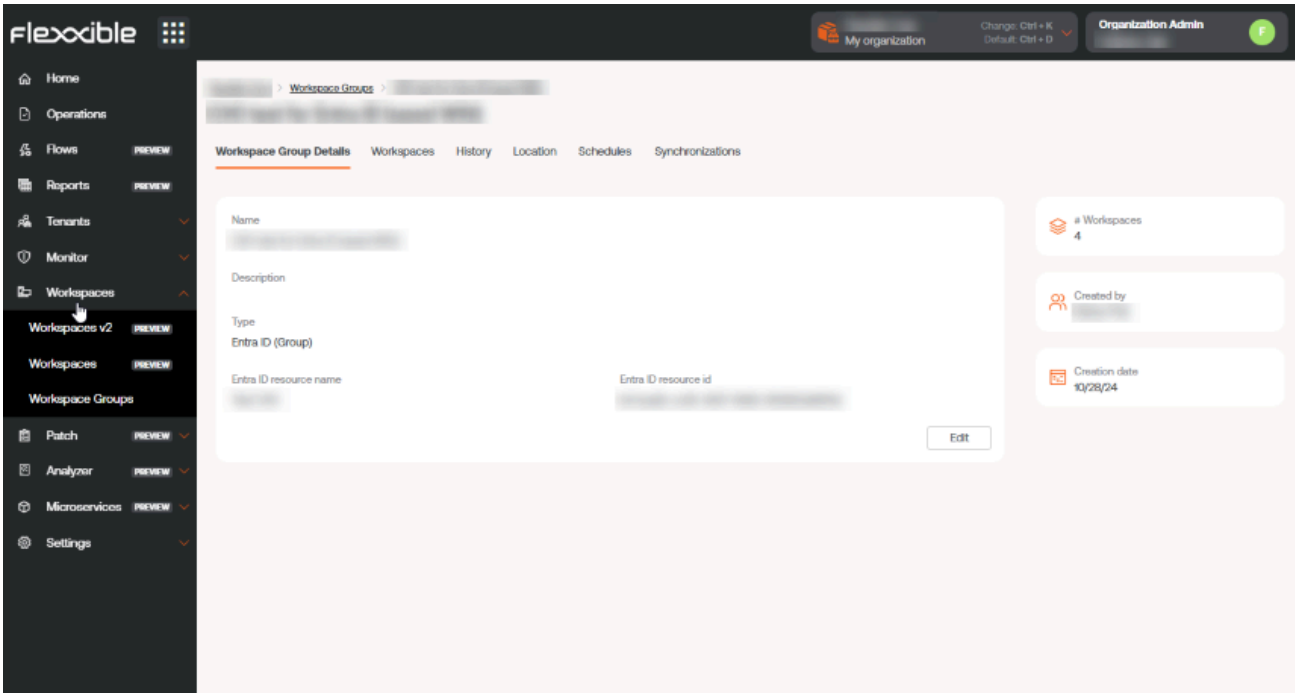
The list view of the Workspace groups section provides information on the name of the groups, their type, Entra ID feature, and the number of devices they contain. The `See Details` button shows the following tabs:

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

Workspace Group Details

Copyright © 2024 Flexxible. Todos los derechos reservados.

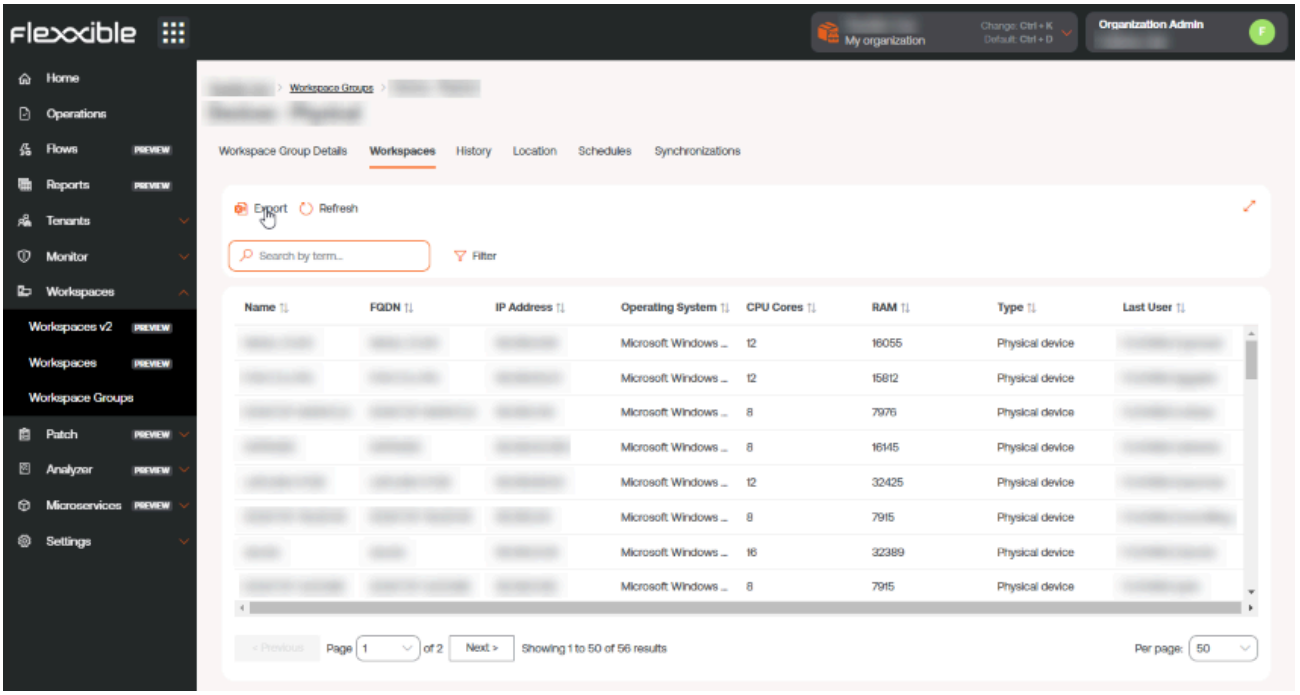
Shows the same data as the list view, as well as the group's creation date and the user who created it. The `Edit` button allows you to change the device name, add a description, or even delete it.



Workspaces

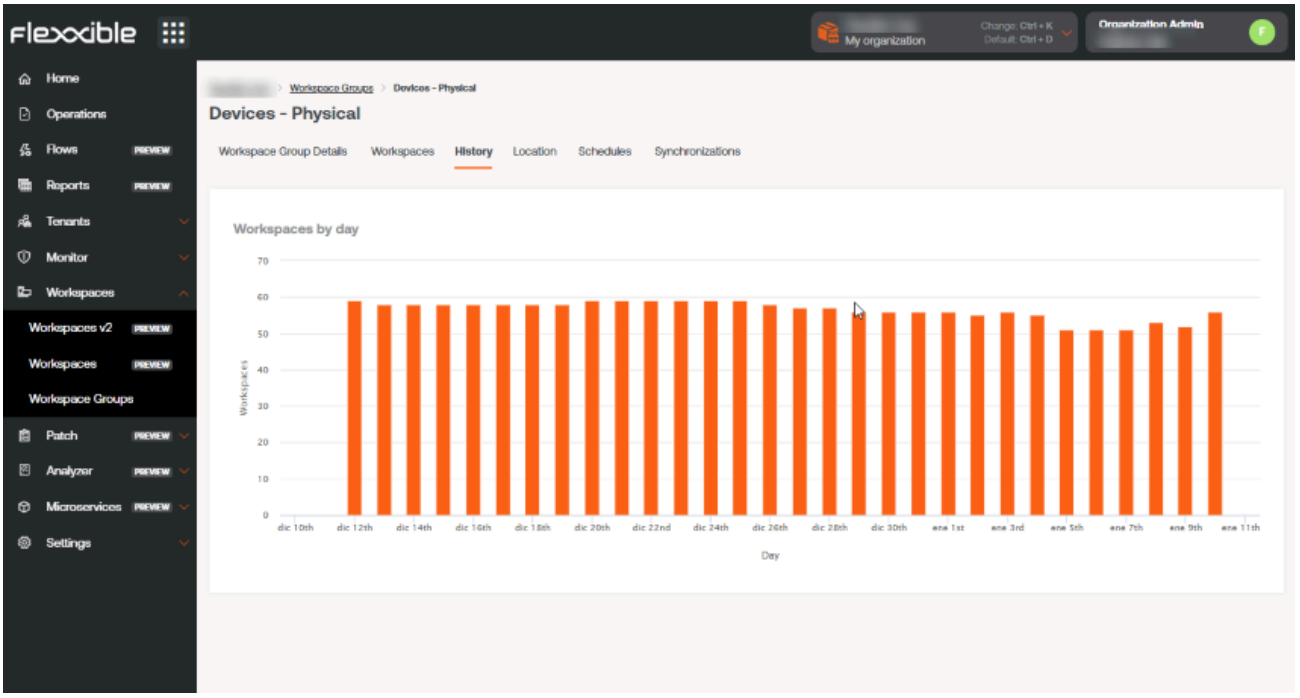
Displays a table with a list of the devices that make up that group. Provides information about the Fully Qualified Domain Name (FQDN) of the device, IP address, operating system, CPU cores, Random Access Memory (RAM), type (physical or virtual), and the last user. The options `Import Workspaces` and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

Copyright © 2024 Flexxible. Todos los derechos reservados.



History

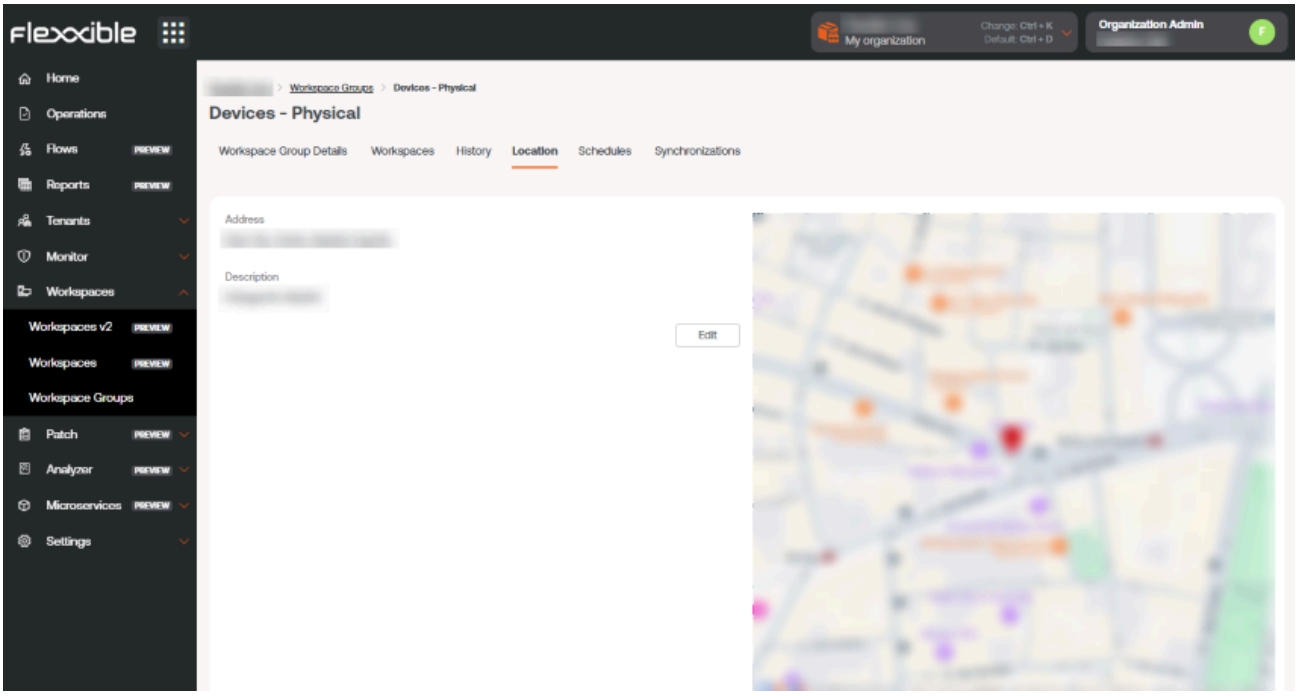
Displays a bar chart with the daily number of devices that have made up the group during the last month. You can zoom in on the chart for better reading by selecting the bars you want to enlarge with the mouse. Using `Reset zoom`, the information returns to its original state.



Copyright © 2024 Flexxible. Todos los derechos reservados.

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.

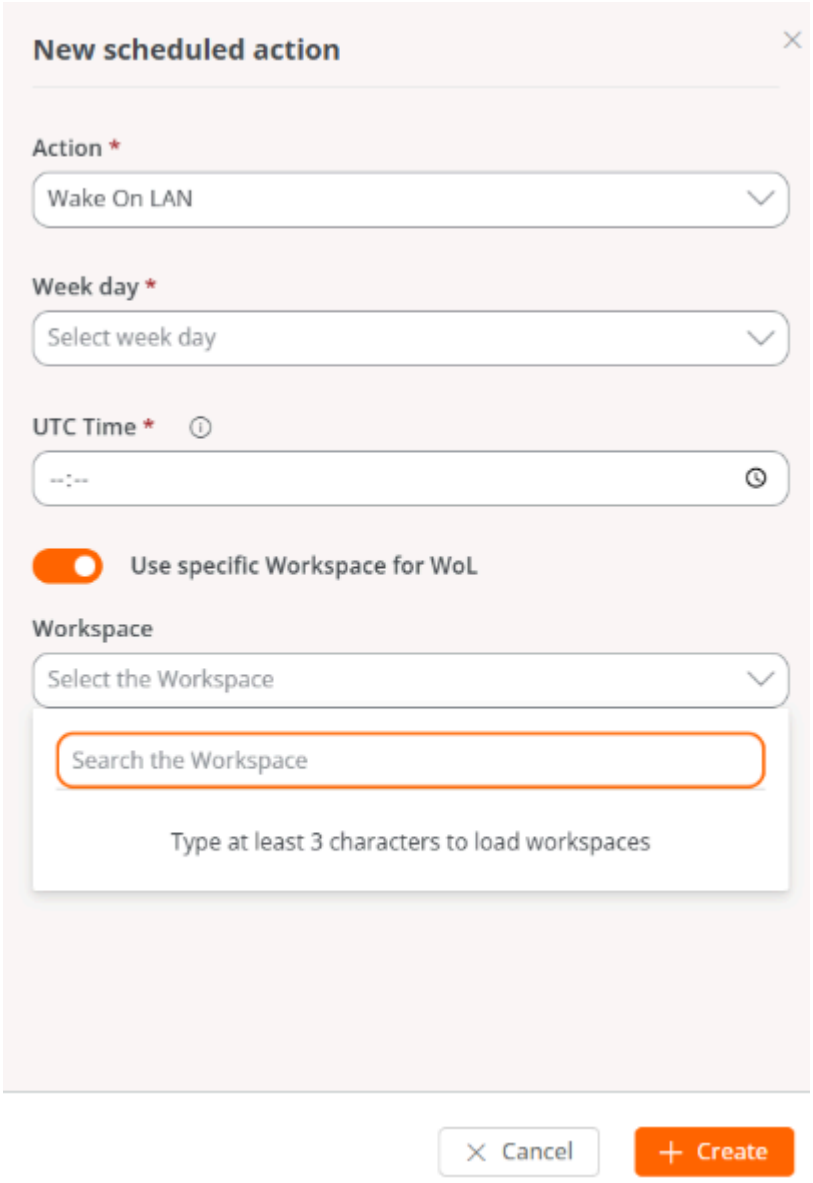


Schedule

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.



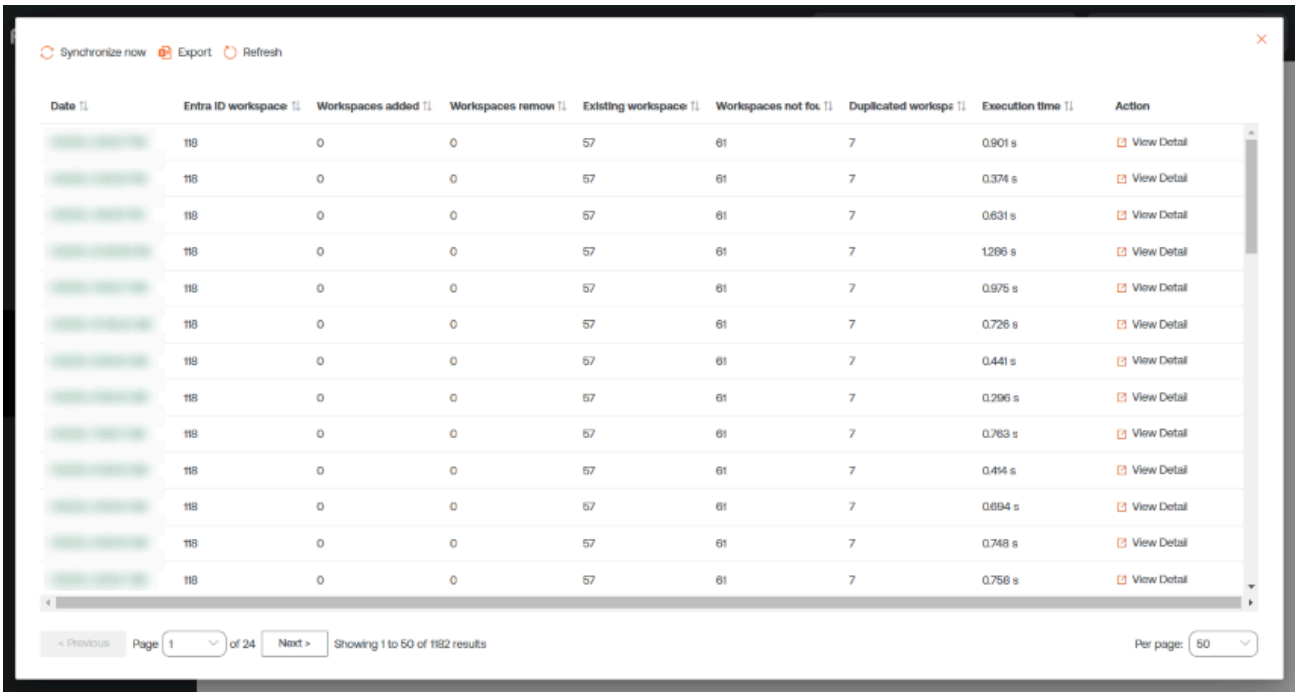
Sync

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

- **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.



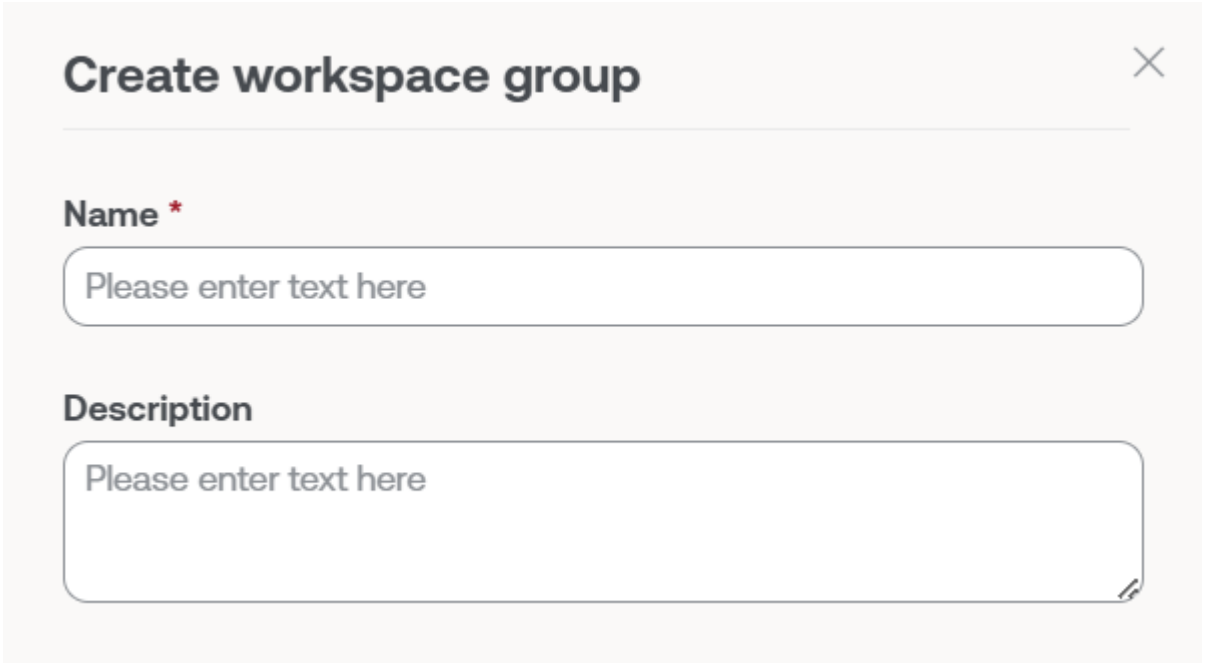
Create groups

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

Create a static workspace group from the Portal

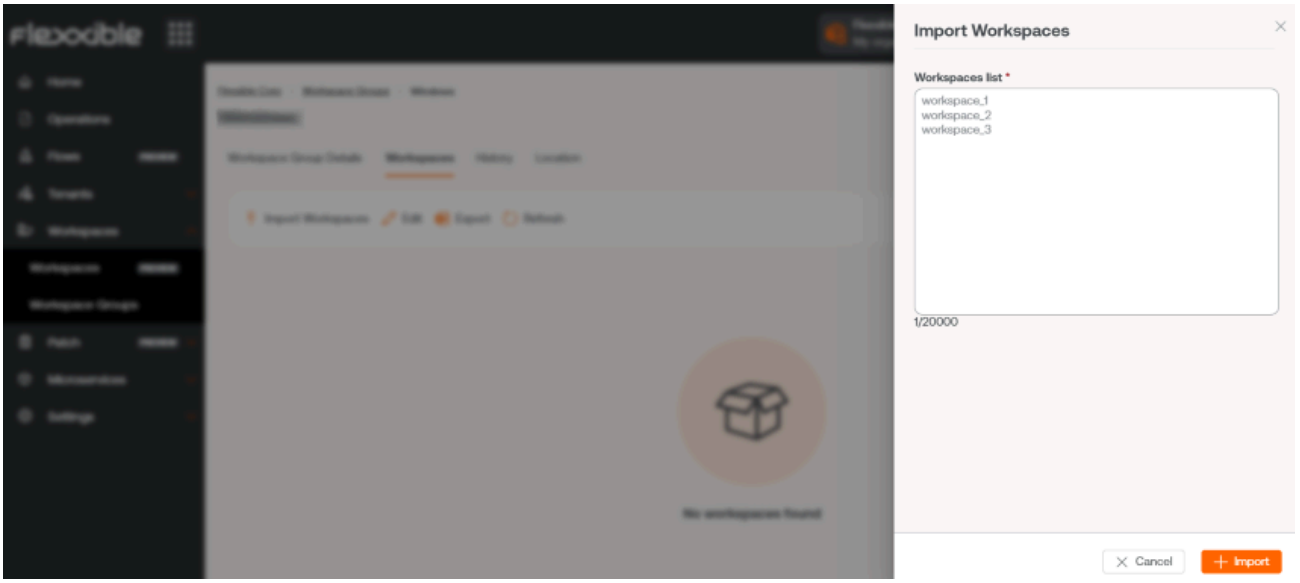
At the top of the list view in the Workspace groups section, click on `New`. A form will open where you will be asked to add a name and a description for the new group.

Copyright © 2024 Flexxible. Todos los derechos reservados.



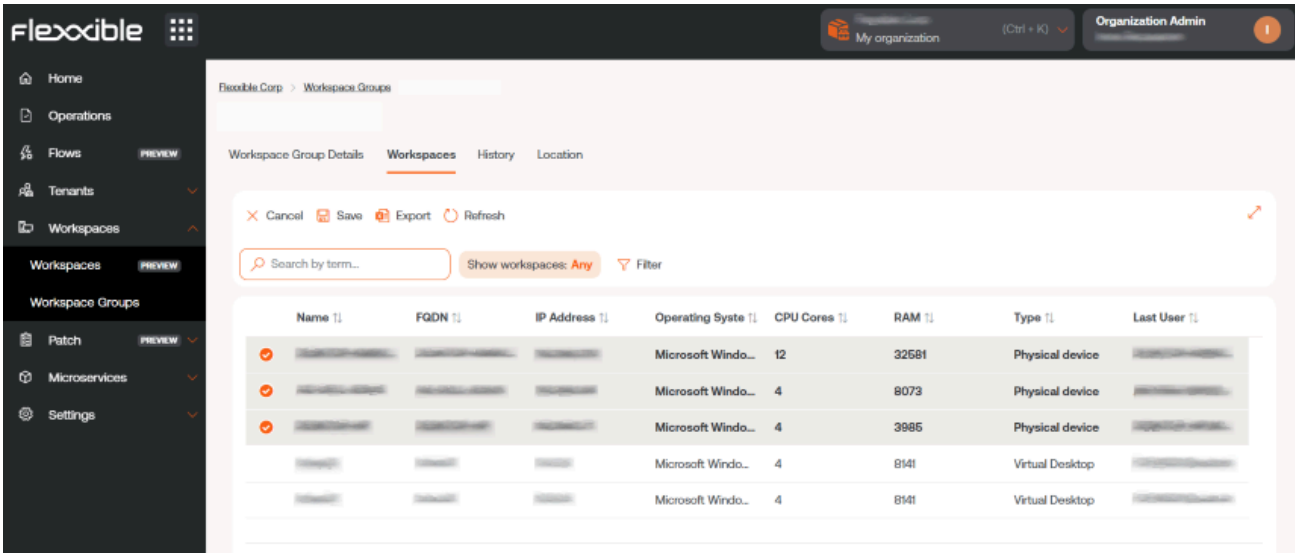
There are two ways to add devices to a static workspace group from Portal:

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.

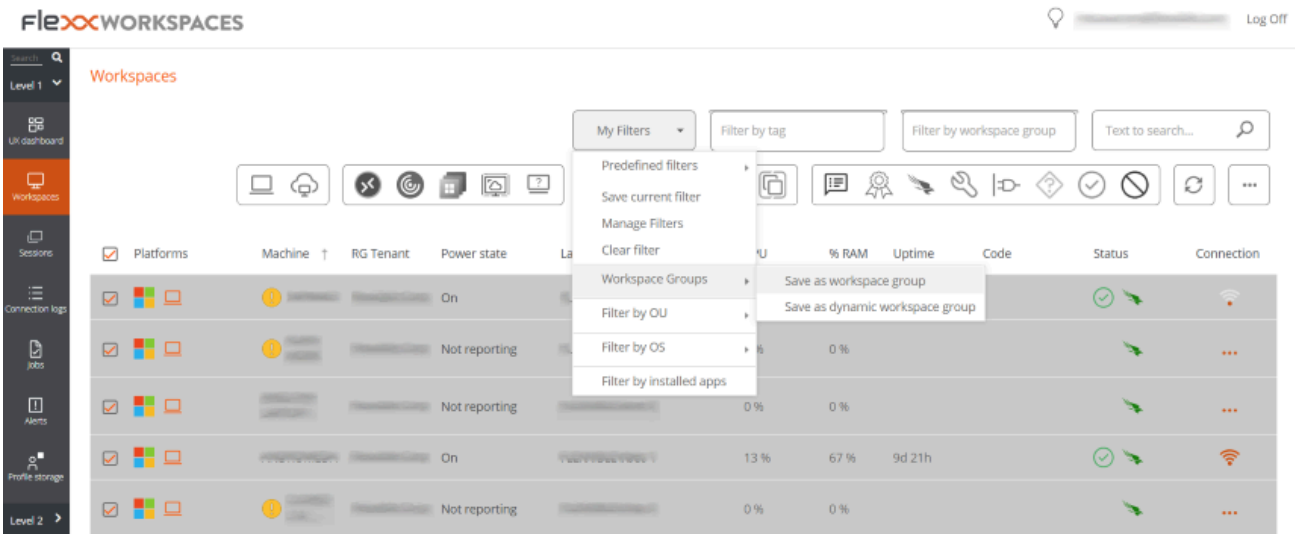
Copyright © 2024 Flexxible. Todos los derechos reservados.



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

Create a static workspace group from Workspaces

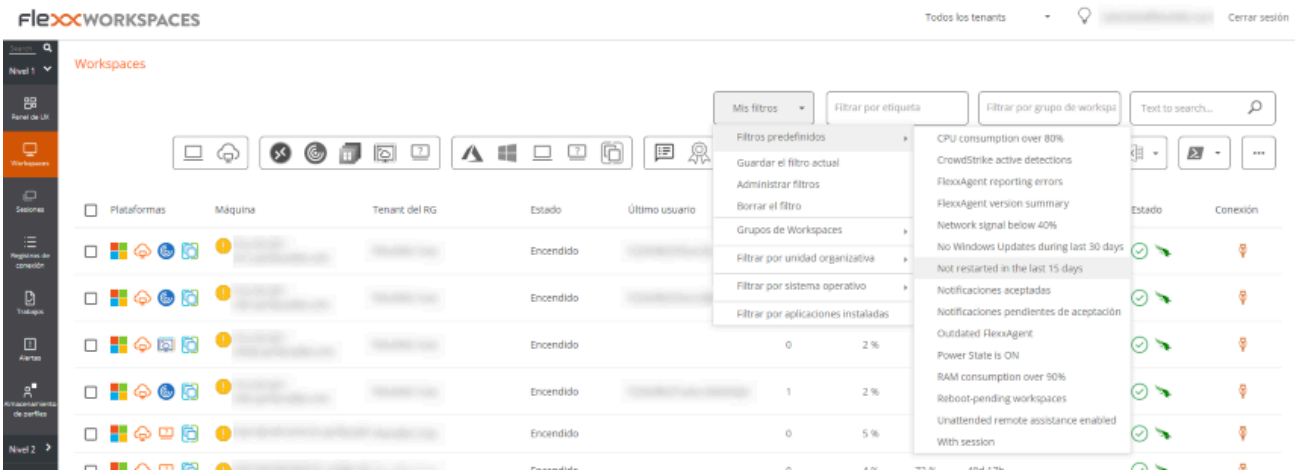
In the sidebar of the Workspaces module, navigate to the Workspaces section. Select the desired devices in the list view and save them in a new group by clicking on `My filters` -> `Workspace group` -> `Save as workspace group`.



Create a dynamic workspace group

Copyright © 2024 Flexxible. Todos los derechos reservados.

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.



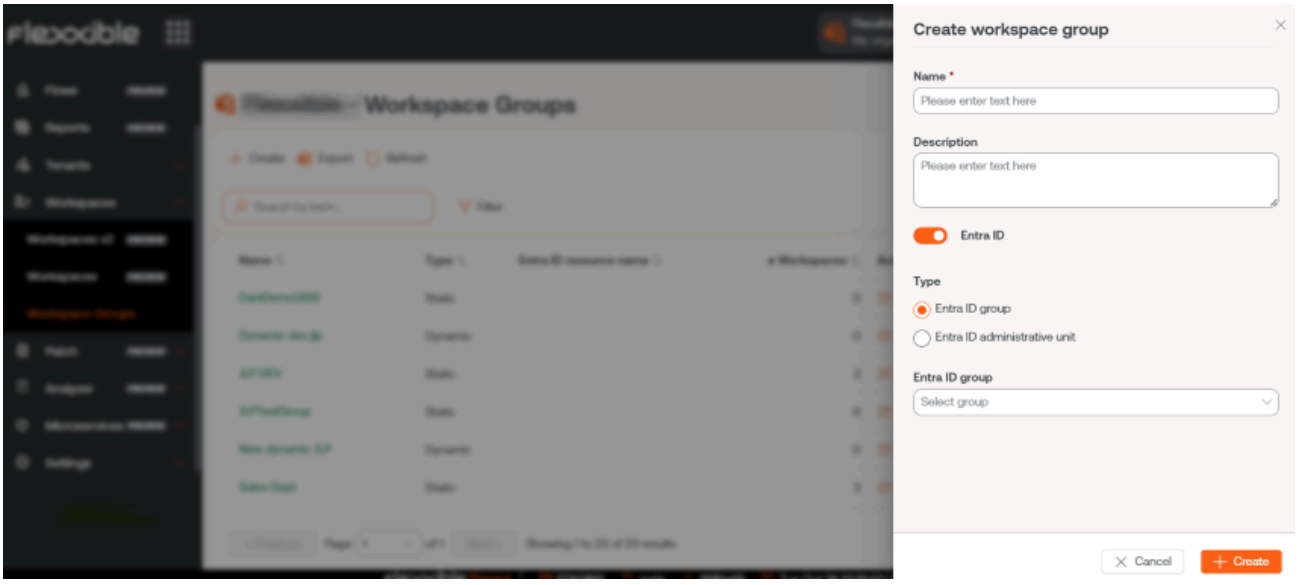
With the device list ready, go to `My filters` -> `Workspace group` -> `Save as dynamic workspace group`. Workspaces will not allow creating a group if the filters for the devices are not specified first.

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**.

Copyright © 2024 Flexxible. Todos los derechos reservados.



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

Copyright © 2024 Flexxible. Todos los derechos reservados.

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.

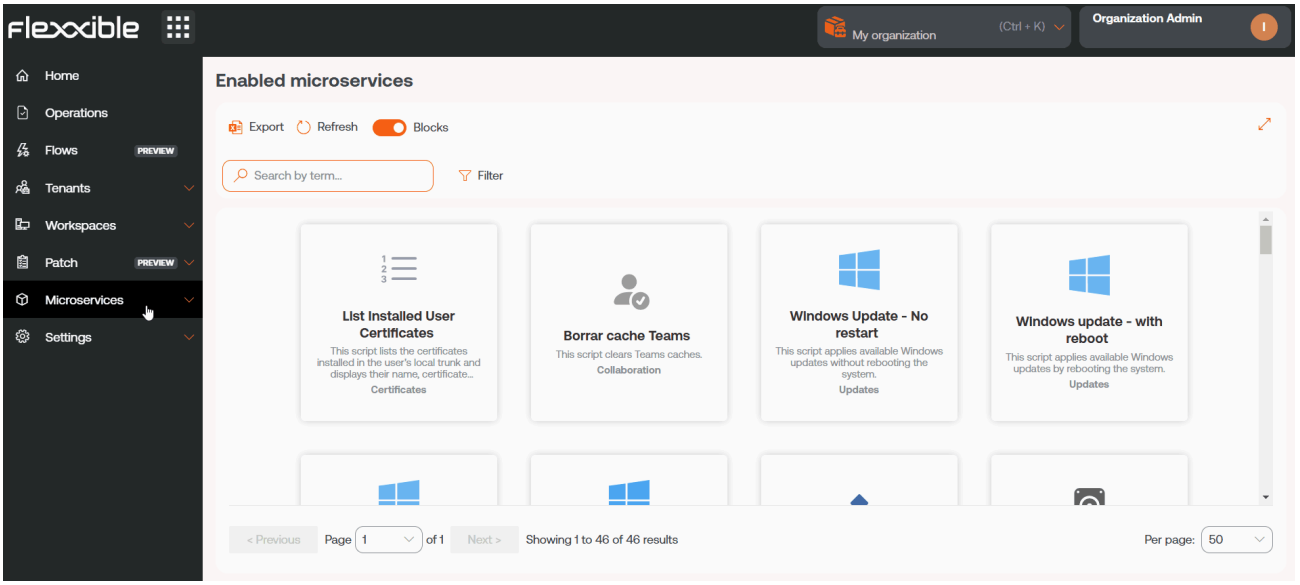
> **INFO**
>
> For more information on how to create or manage workspace groups, please refer to this guide.

Copyright © 2024 Flexxible. Todos los derechos reservados.

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.

The Microservices section allows you to create, enable, and publish 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.
- Audit log. Describe what the user microservices execution tracking consists of.

Copyright © 2024 Flexxible. Todos los derechos reservados.

Main characteristics of microservices in Portal

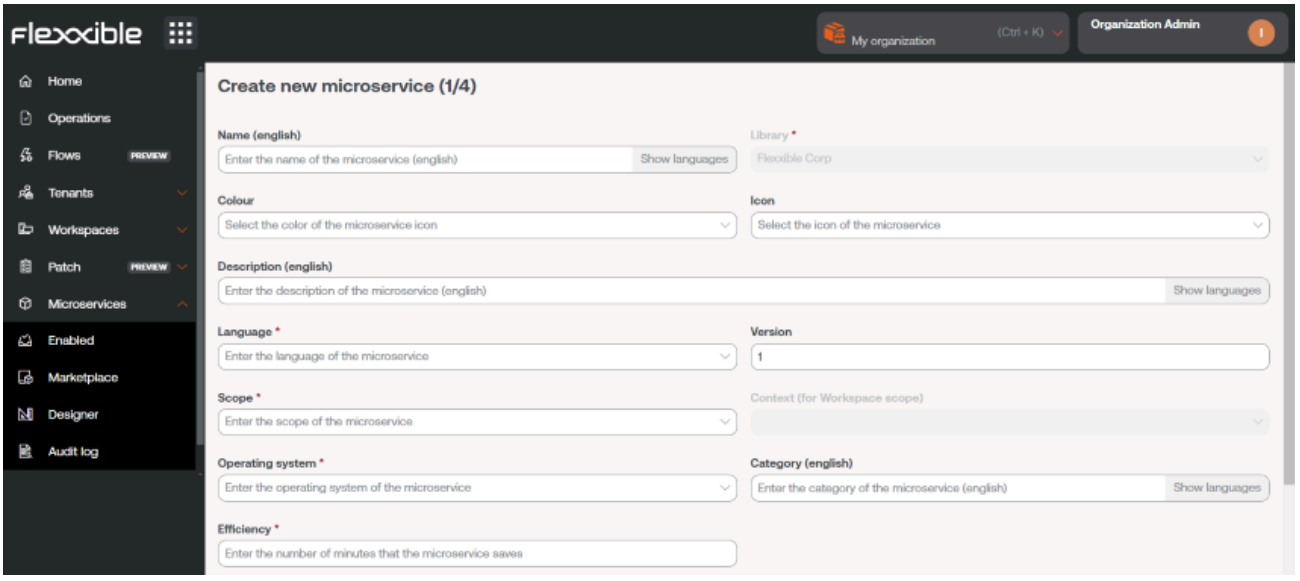
The Microservices section offers a number of key advantages. The most relevant ones are described below:

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

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.

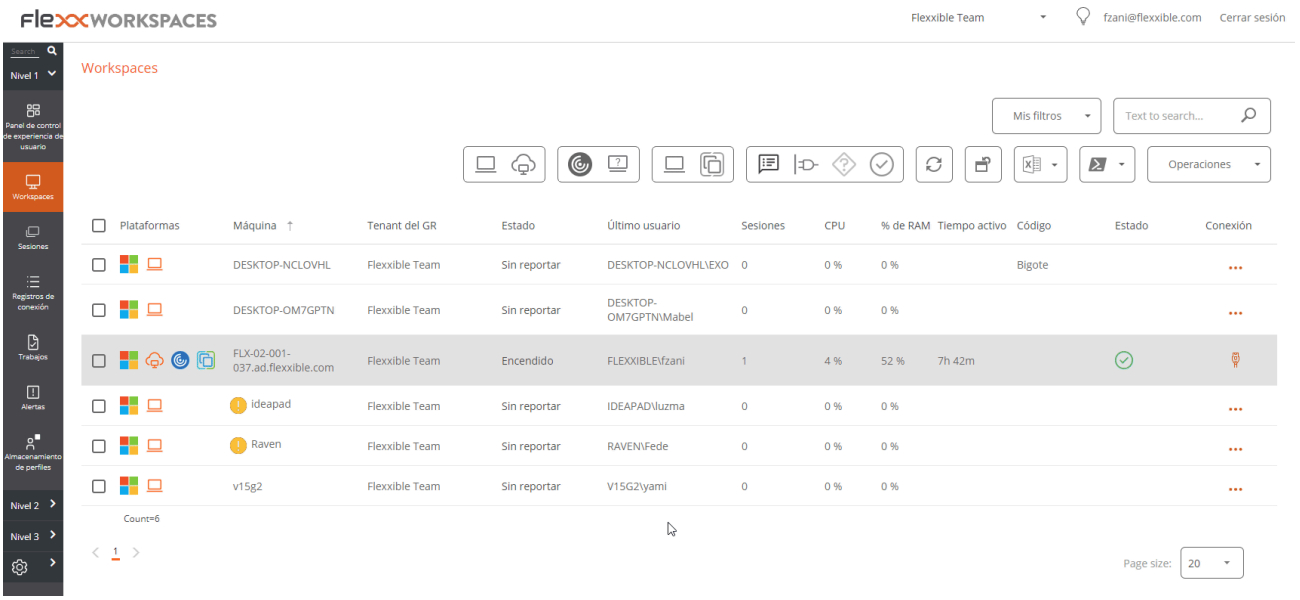
On-demand execution from Workspaces

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 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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

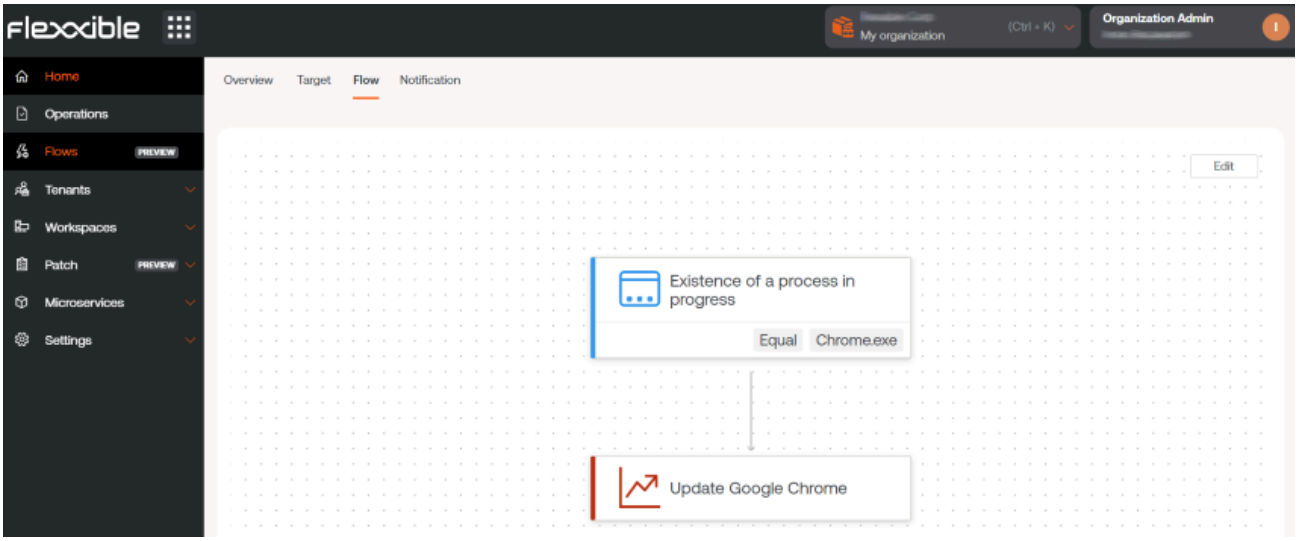


Management of the execution scope of the microservice and permissions can be done from the Designer section. It should be noted that the ability to execute certain microservices will depend on the user's role in the platform.

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.



Copyright © 2024 Flexxible. Todos los derechos reservados.

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`.

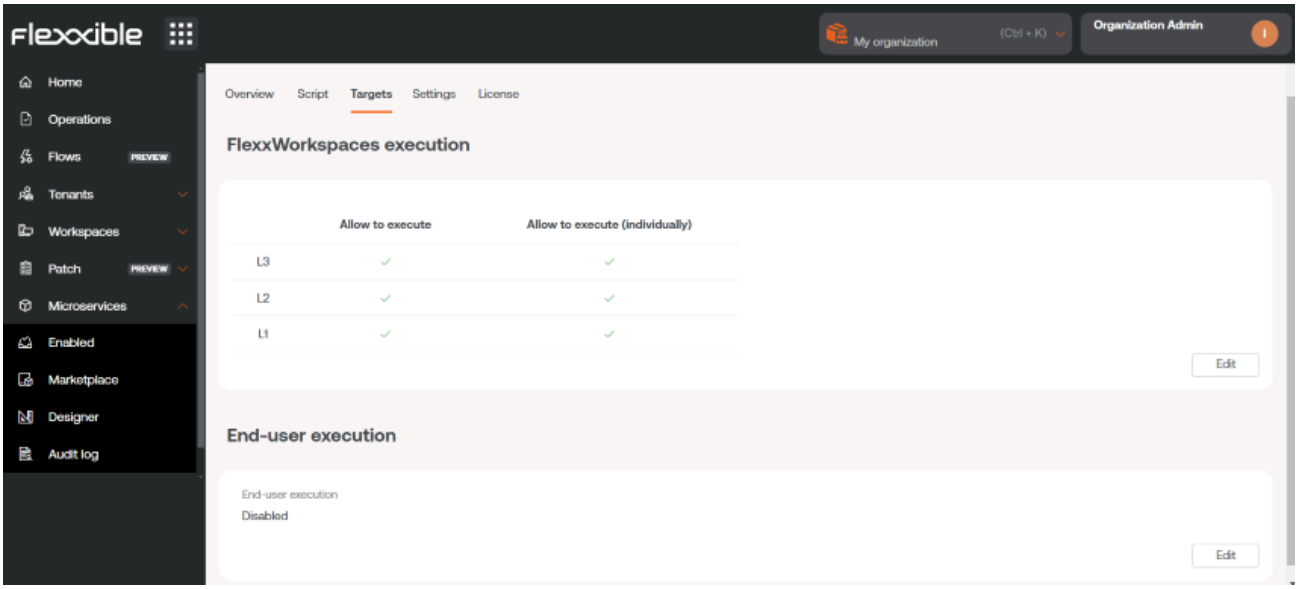
For more information on linking an alert to a microservice, please refer to the Alert Settings documentation.

End-user execution

When a microservice is created, it is not automatically enabled for execution by the end user. To be available, the following configuration needs to be completed:

1. Go to `Portal` -> `Enabled`.
2. Click on a microservice from the list.
3. In the `Targets` tab, go to the `End user execution` section.
4. Click `Edit` and activate the `End user execution` option.

Copyright © 2024 Flexxible. Todos los derechos reservados.



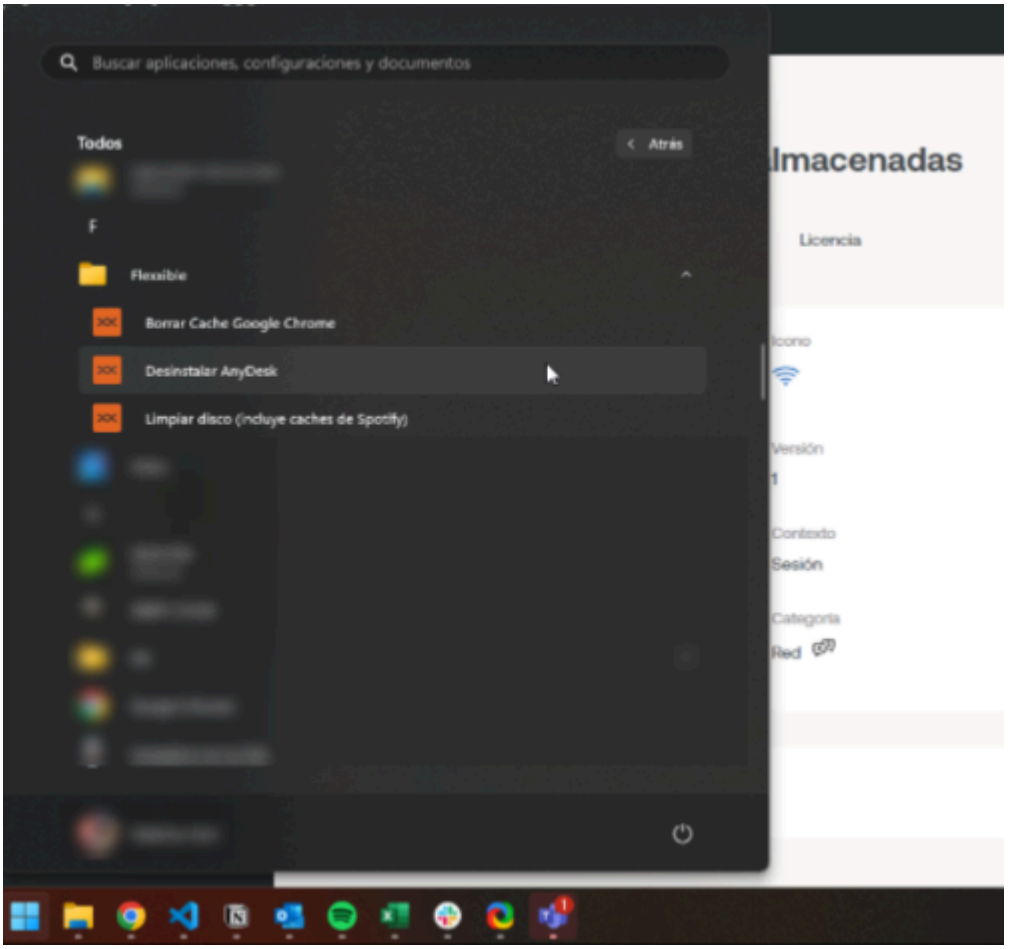
Rename the microservices folder

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`.

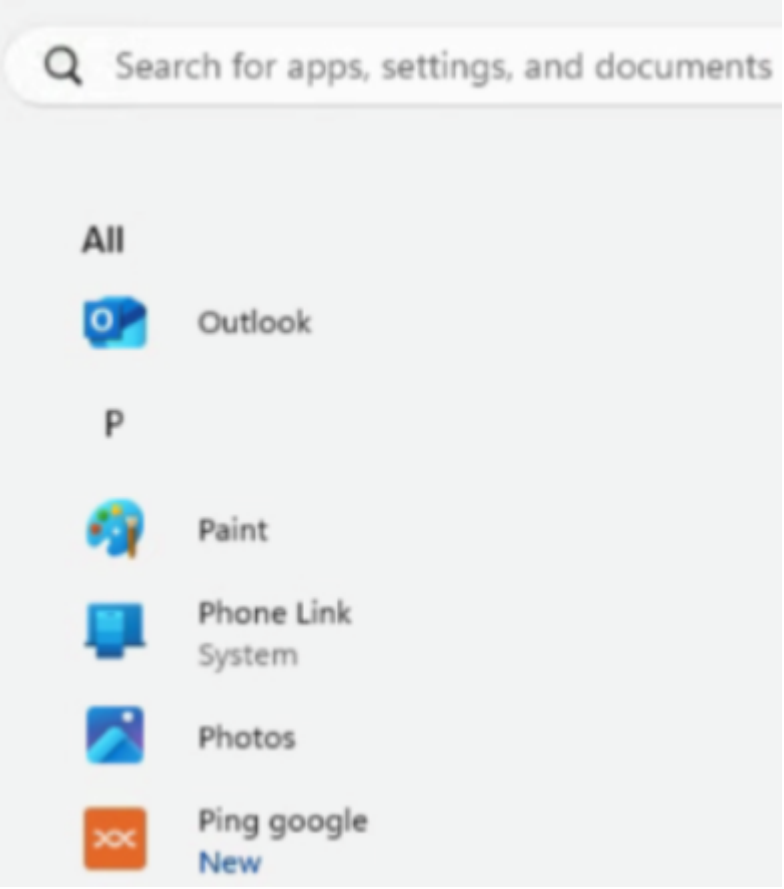
The chosen name must be between 3 and 50 characters, and can only contain letters, numbers, hyphens, and underscores.

Copyright © 2024 Flexxible. Todos los derechos reservados.



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.

Copyright © 2024 Flexxible. Todos los derechos reservados.



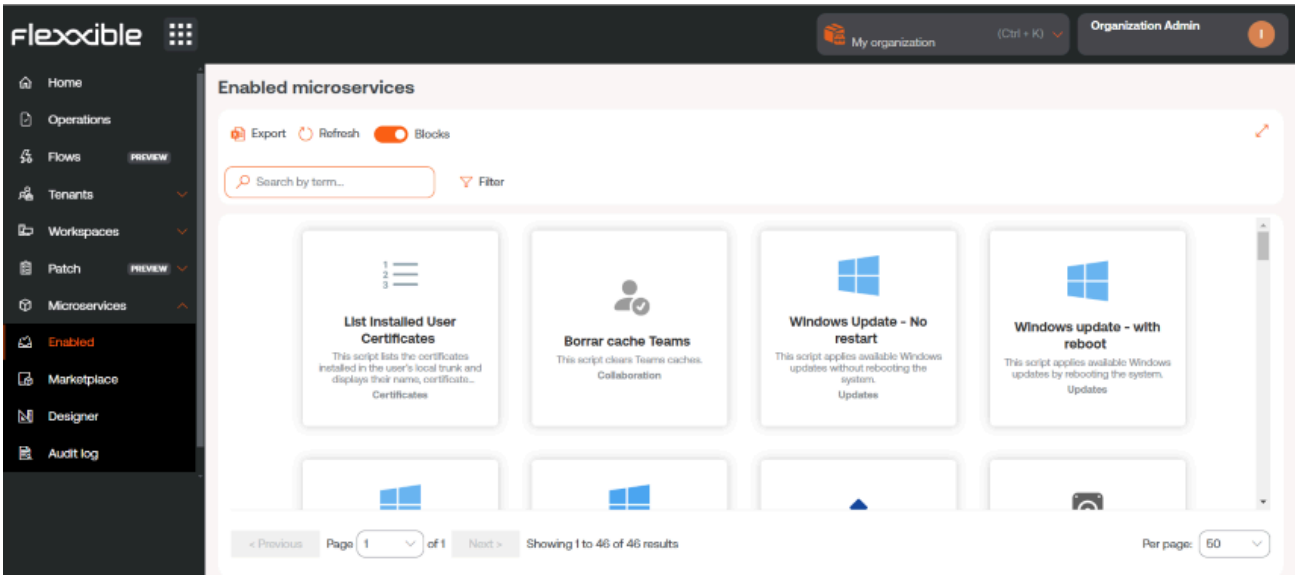
TIP

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

Copyright © 2024 Flexxible. Todos los derechos reservados.

Portal / Microservices / Enabled

The Enabled section, in Portal, displays 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

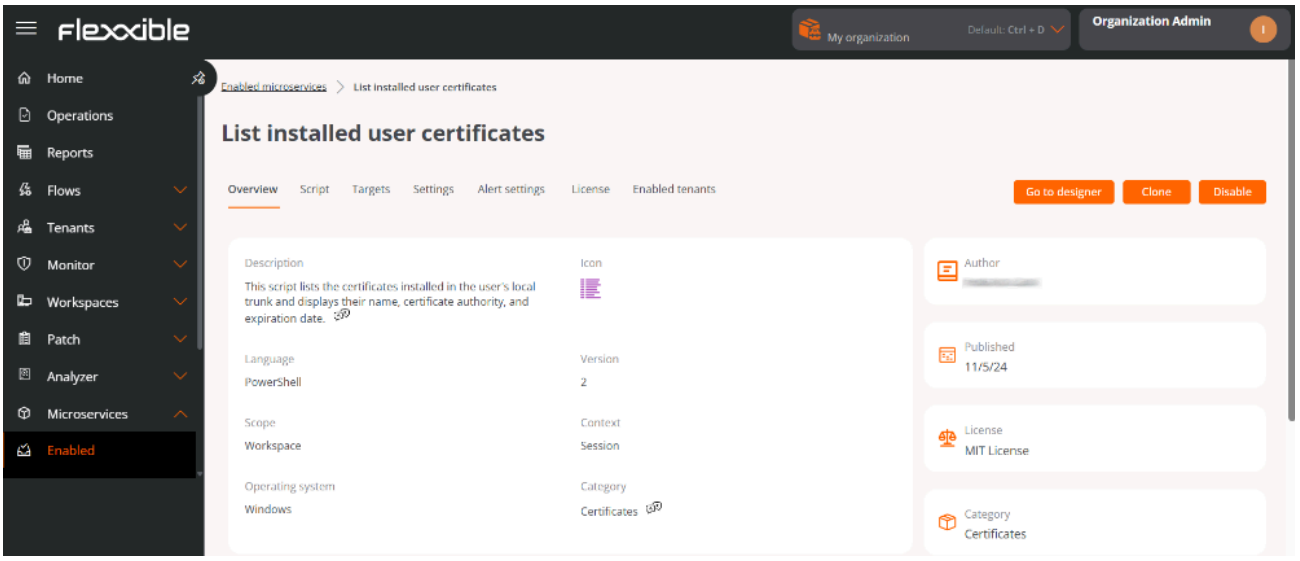
Clicking on a microservice in the table allows access to its detailed view, divided into seven tabs:

- Overview
- Code
- Targets
- Settings
- Alert configuration
- License
- Enabled tenants

Overview

Copyright © 2024 Flexxible. Todos los derechos reservados.

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

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 preloaded with the cloned microservice information, allowing you to create a new one from that configuration.

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

> **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.

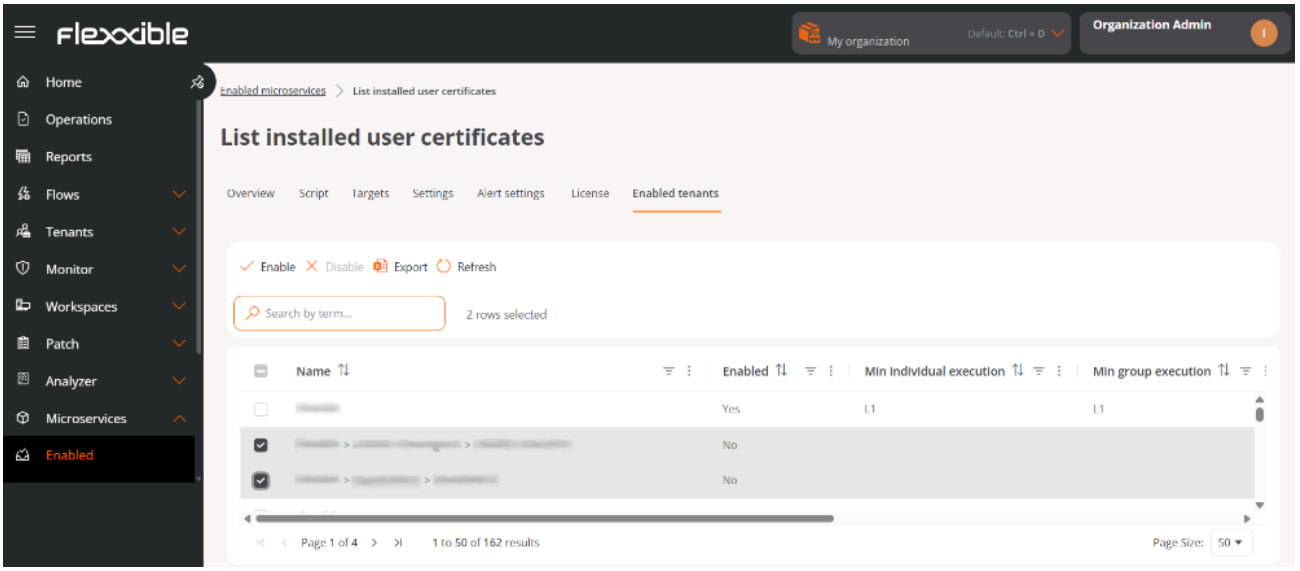
License

Shows the type of license configured for the microservice.

Enabled Tenants

Allows enabling/disabling the microservice in bulk for the selected tenants and suborganizations.

Copyright © 2024 Flexxible. Todos los derechos reservados.



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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

Steps to enable/disable a microservice for tenants

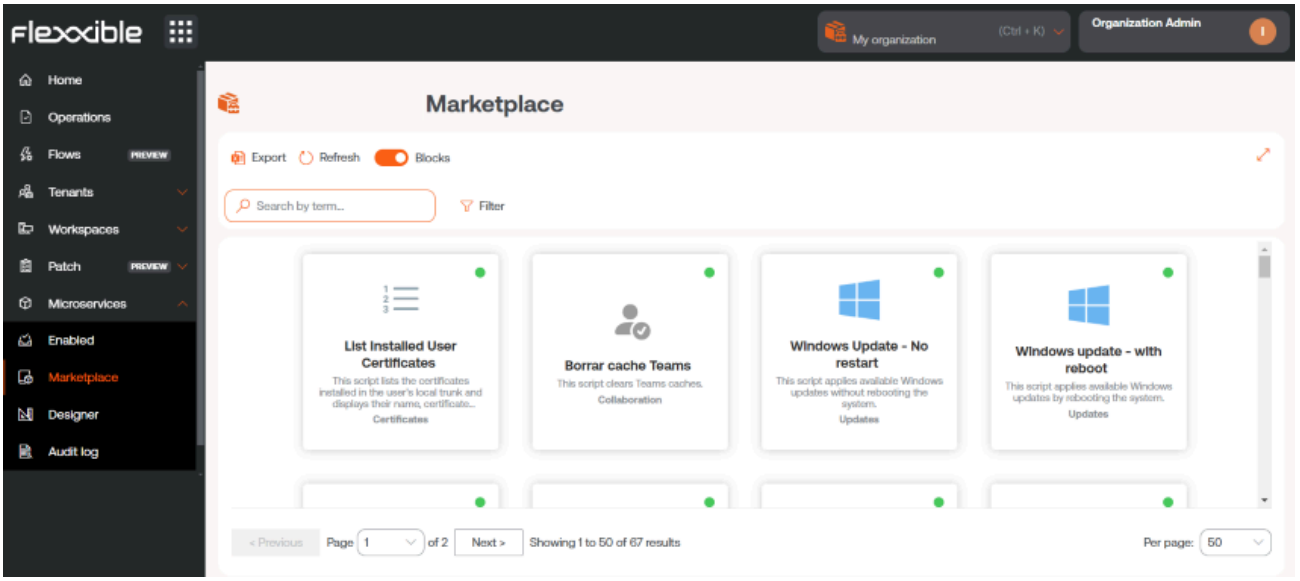
1. Go to `Portal` -> `Enabled`.
2. Go to the `Enabled Tenants` tab.
3. Select the desired tenants in the table.
4. Click `Enable` or `Disable`, as applicable.
5. Read the warning message.
6. Click on `Confirm`.

Copyright © 2024 Flexxible. Todos los derechos reservados.

Portal / Microservices / Microservices Marketplace

The Marketplace section offers a wide range of microservices that can be used without deep computer knowledge, as they are ready to be enabled and executed immediately.

The general view of Marketplace offers microservices in block or table format. In both cases, if the microservice shows a green dot it means it's enabled and can be run directly from the Workspaces module, if the dot is gray, it means it's not.



Microservice detail

Clicking on a microservice in the table allows access to its detailed view, divided into seven tabs:

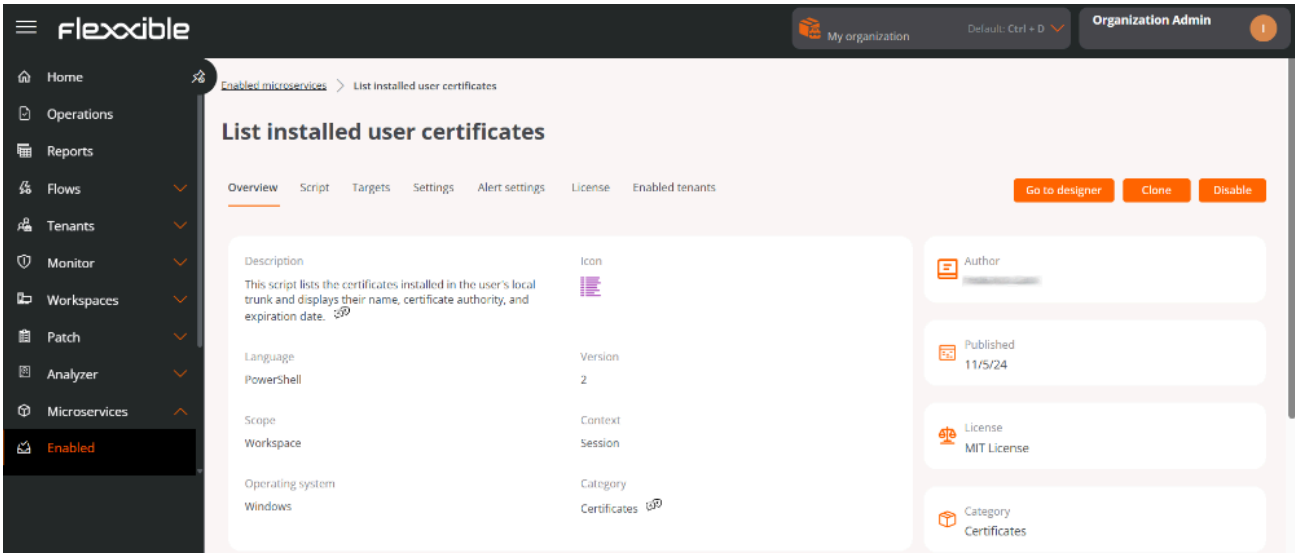
- Overview
- Code
- Targets
- Settings
- Alert configuration
- License

Copyright © 2024 Flexxible. Todos los derechos reservados.

- 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)*

Copyright © 2024 Flexxible. Todos los derechos reservados.

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.

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

Copyright © 2024 Flexxible. Todos los derechos reservados.

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.

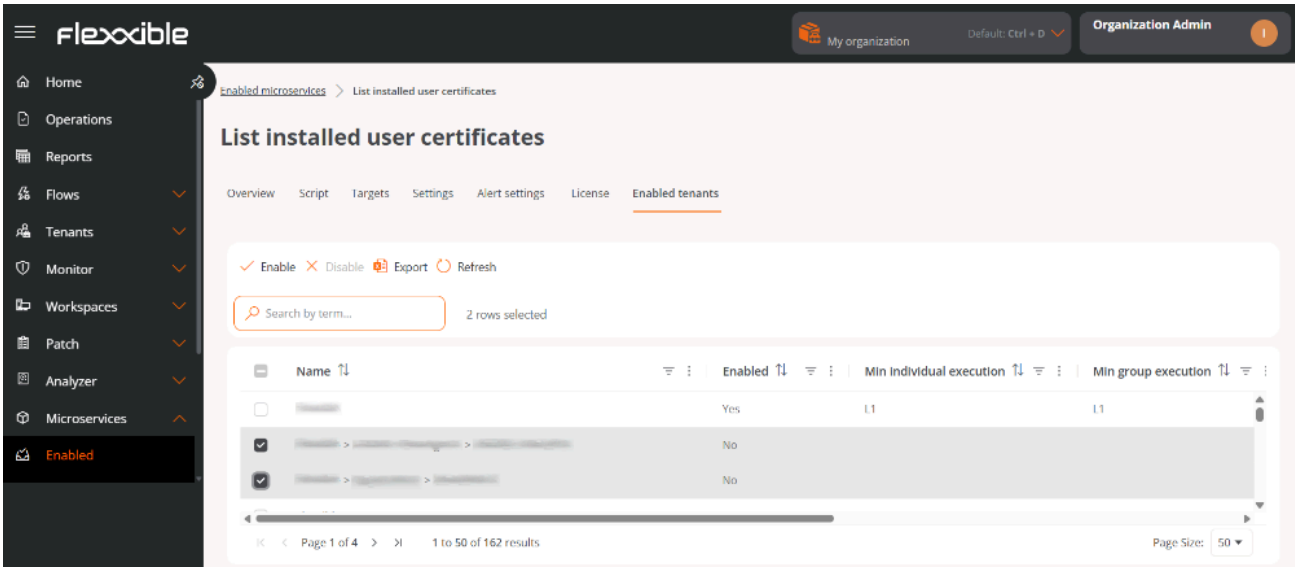
License

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.



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

Copyright © 2024 Flexxible. Todos los derechos reservados.

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`.

Copyright © 2024 Flexxible. Todos los derechos reservados.

Portal / Microservices / Designer

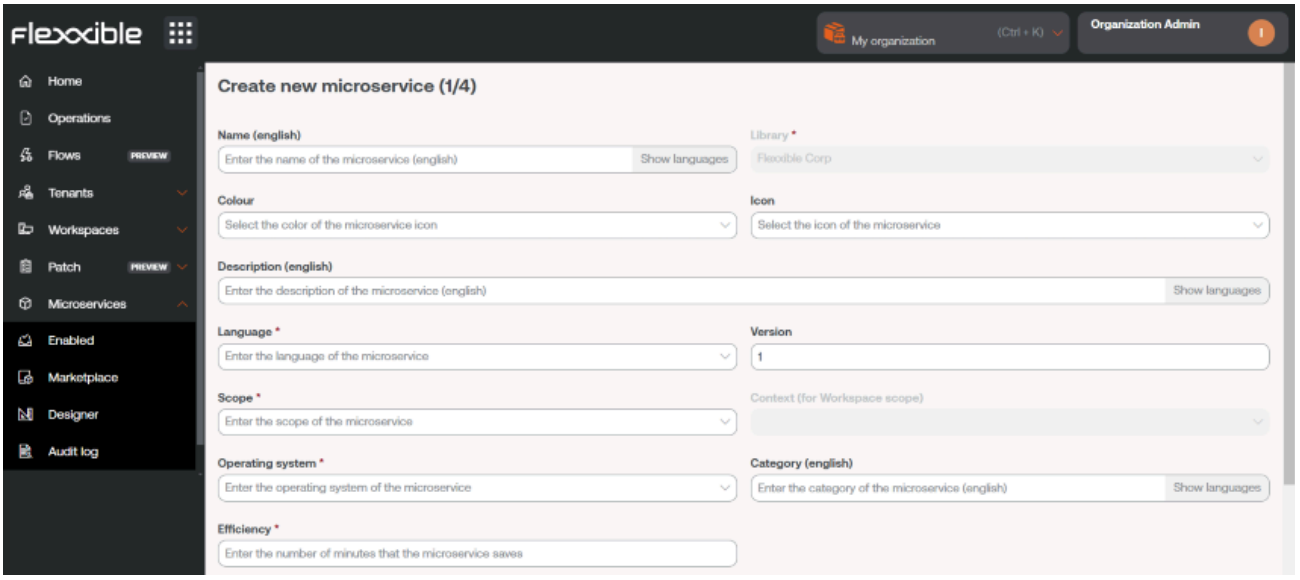
Through the Designer section, you can access all information about existing microservices, such as the author, script, execution dates, problem it solves, or license type; but most importantly, it allows you to create new microservices.

Microservice creation

Microservices are created in four phases:

Phase 1

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.** Icon color.
- **Icon.** Icon type.
- **Description.** Brief text explaining what the microservice does.
- **Language.** Programming language it is developed with.

Copyright © 2024 Flexxible. Todos los derechos reservados.

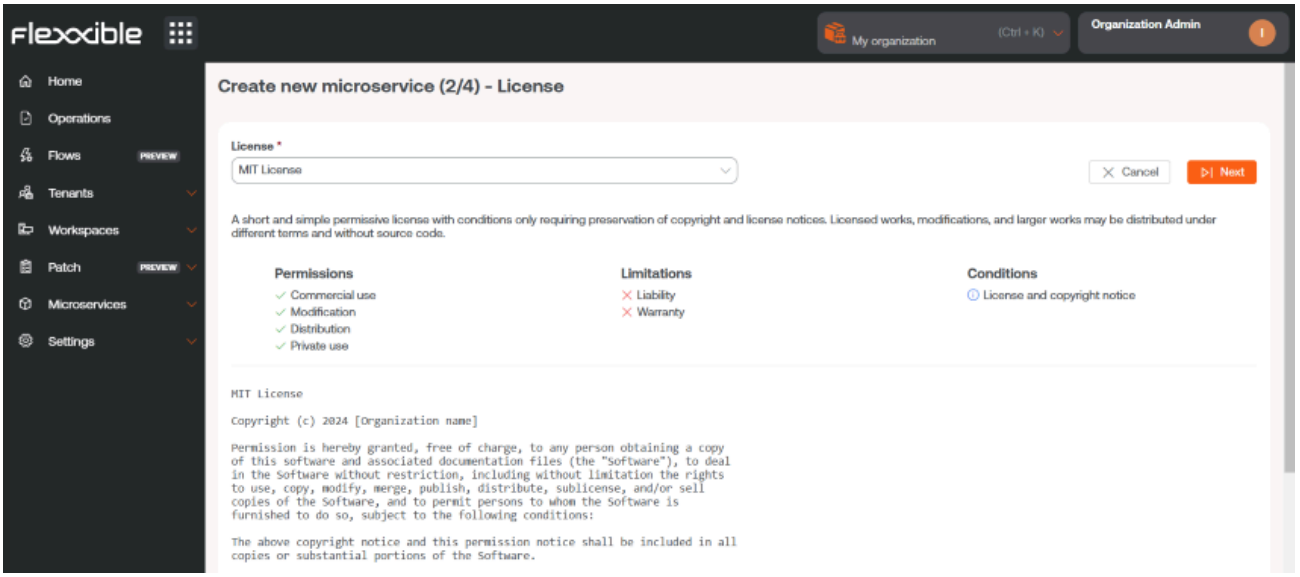
- **Version.** Microservice version number.
- **Scope.** Execution scope. You can select *Workspace* (context *System* or *Session*) or *Platform*.
- **Operating system.** Operating system it is designed for.
- **Categoría.** Directorio o grupo de microservicios accesibles desde Workspaces en el que se alojará.
- **Efficiency.** Amount of minutes the user saves with each execution.

4. 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

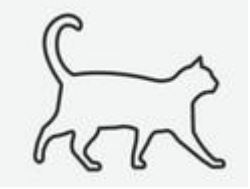
Copyright © 2024 Flexxible. Todos los derechos reservados.

1. Insert a description of the microservice in Markdown format.
2. Click `Next`.

Copyright © 2024 Flexxible. Todos los derechos reservados.

INFO

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 - Script

1. Enter the script.
2. Click `Next`.

The created microservice will appear in the main table of the section.

Code

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

Copyright © 2024 Flexxible. Todos los derechos reservados.

that reason, if you are creating a script in PowerShell you should keep a series of considerations in mind:

- 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.

Steps to enable a Microservice

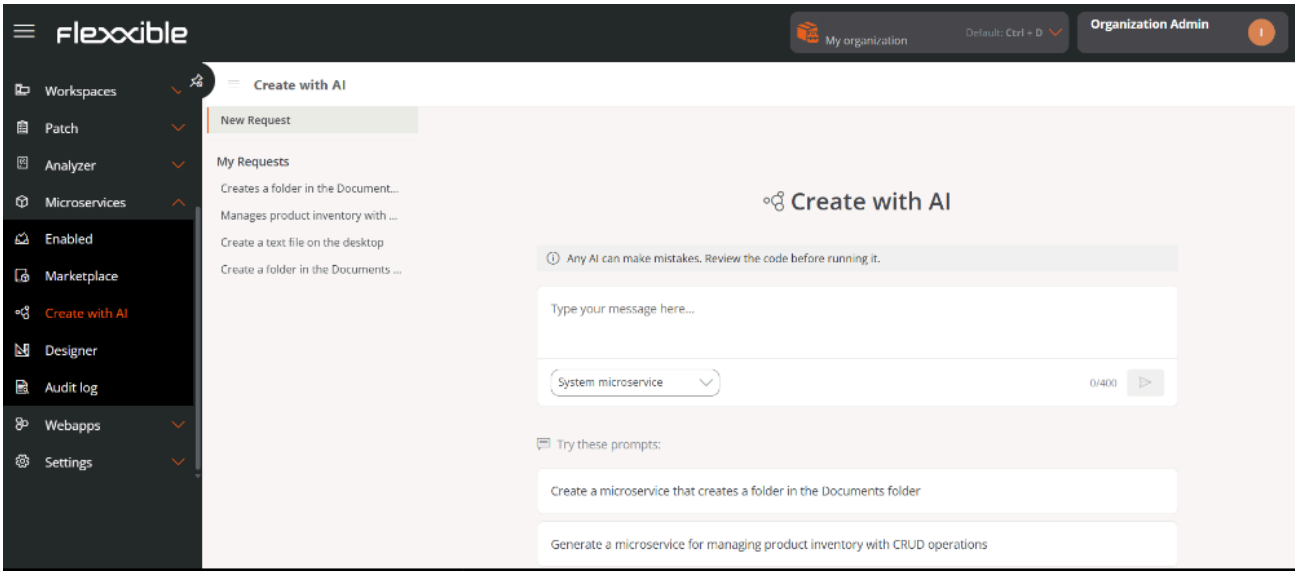
1. Access `Portal` -> `Designer`.
2. Find the microservice in the list and click on it.
3. Click the `Enable` button located at the top right of the screen.
4. The Microservice will appear with a green dot (signifying it is enabled) in the Marketplace section.

Copyright © 2024 Flexxible. Todos los derechos reservados.

Portal / Microservices / Create with AI

Microservices design using Artificial Intelligence (AI) allows for automatic generation from requests expressed in natural language. This functionality 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.



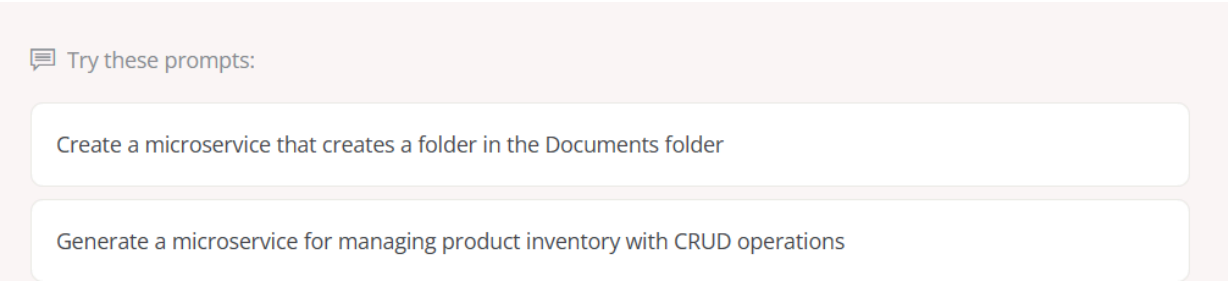
Create new microservice

The steps to create a microservice through AI are as follows:

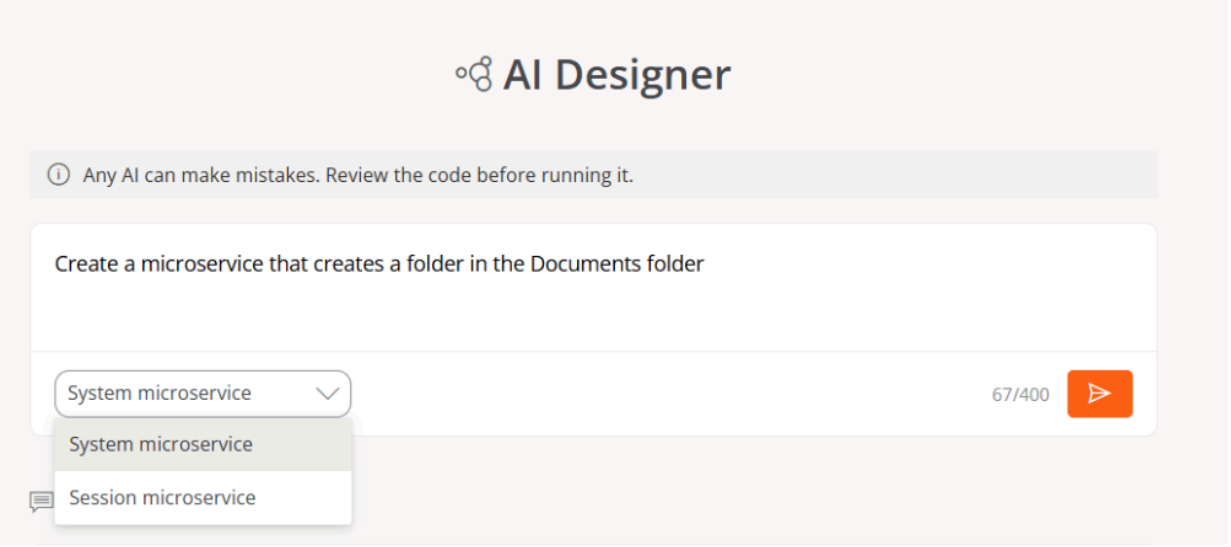
1. Access `Portal` -> `Microservices` -> `Create with AI`.

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.



3. In the dropdown, choose the scope of execution: *System Microservice* or *Session Microservice*.

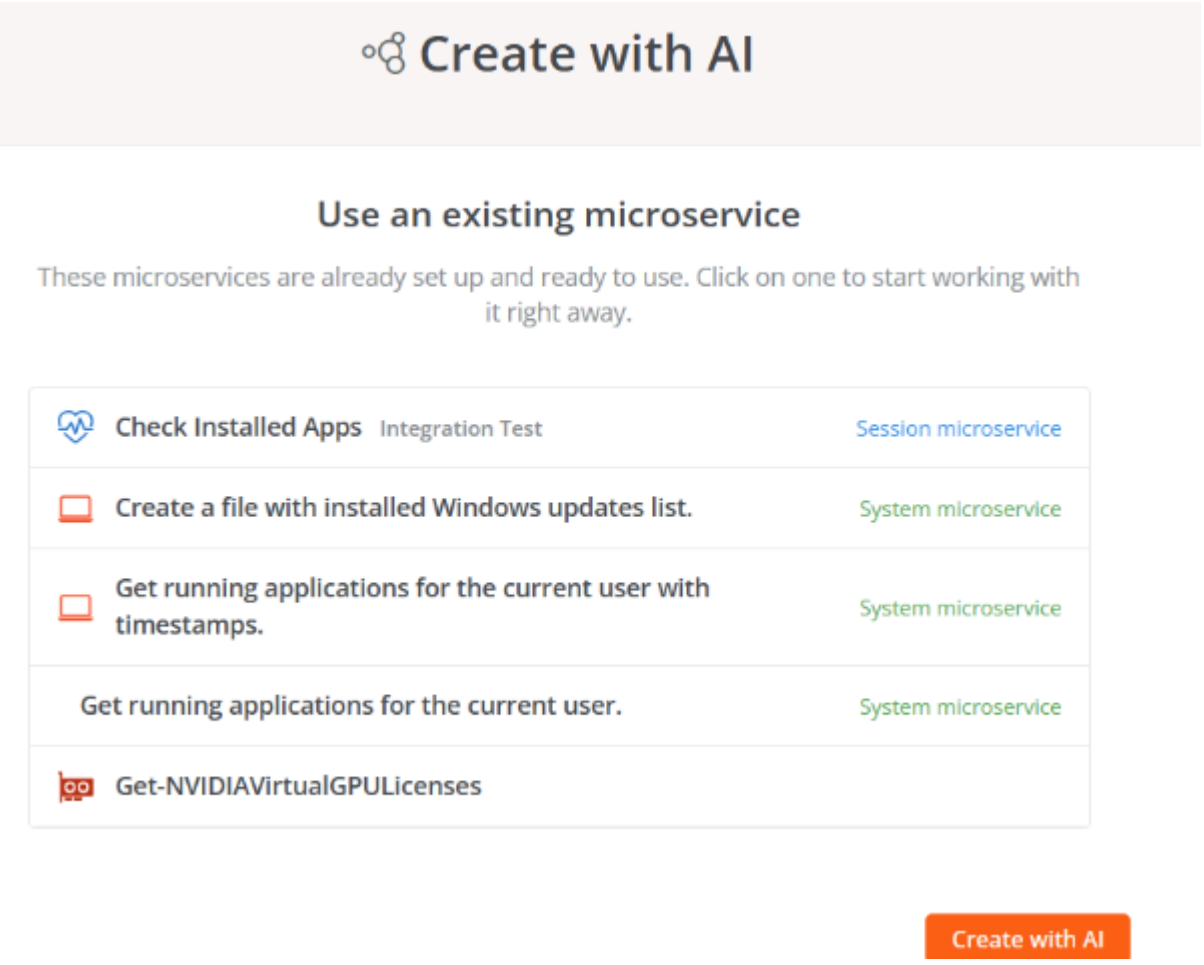


4. Click the arrow in the orange box to continue.

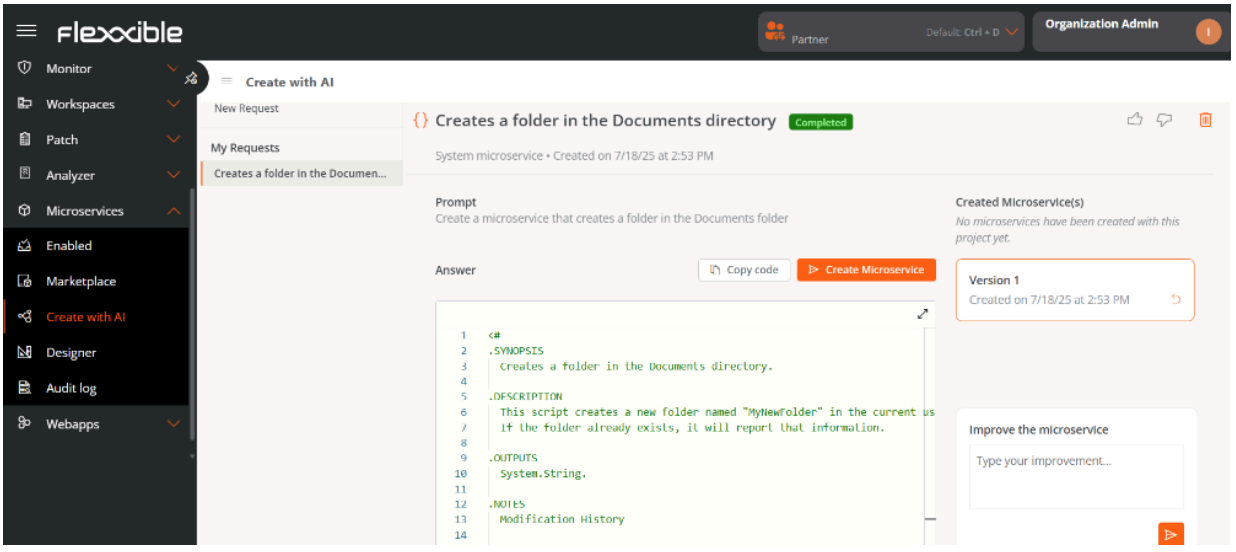
5. If similar microservices exist, they will be offered as available alternatives. The user can click on each one of them to analyze their use in relation to the desired goal. By doing so, they will be redirected to the Marketplace section.

   If, after reviewing the alternatives, the user decides they need to create a new microservice, they should click on `Create with AI`.

Copyright © 2024 Flexxible. Todos los derechos reservados.

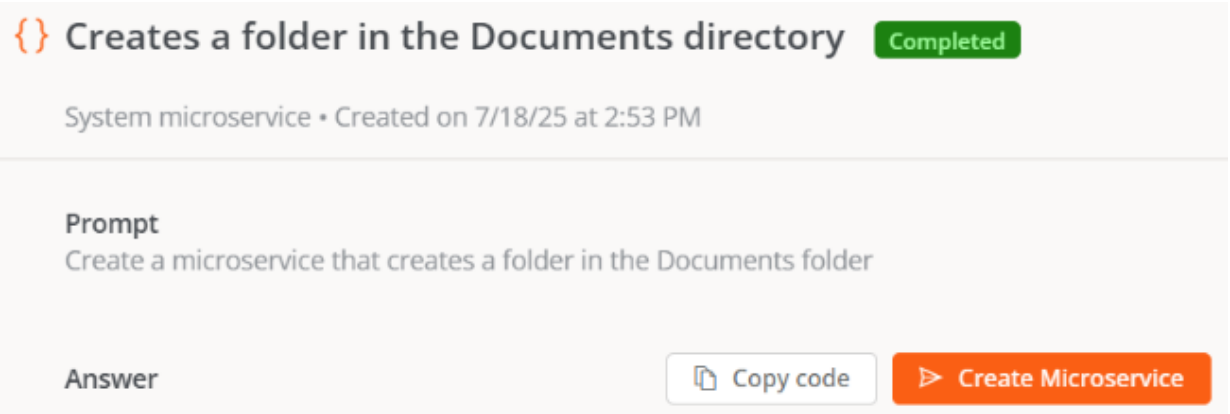


6. A few seconds later, the AI will design the microservice.



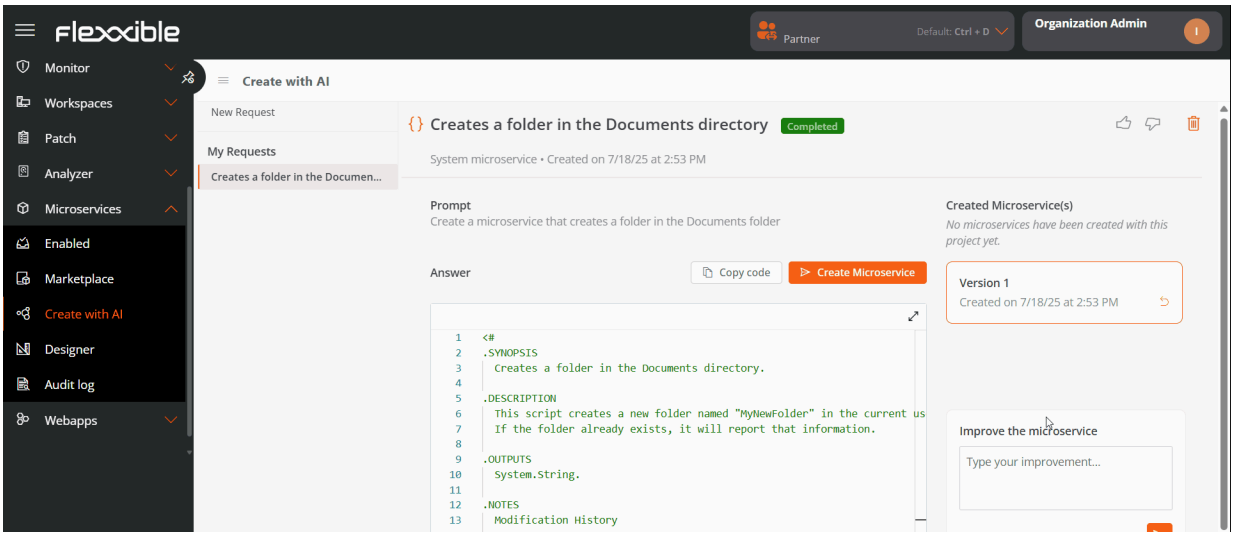
The `Copy Code` button allows you to copy the generated code to the clipboard, facilitating its use in testing if required.

Copyright © 2024 Flexxible. Todos los derechos reservados.



> **INFO**
>
> This feature only generates microservices in PowerShell.

7. Review the microservice code.



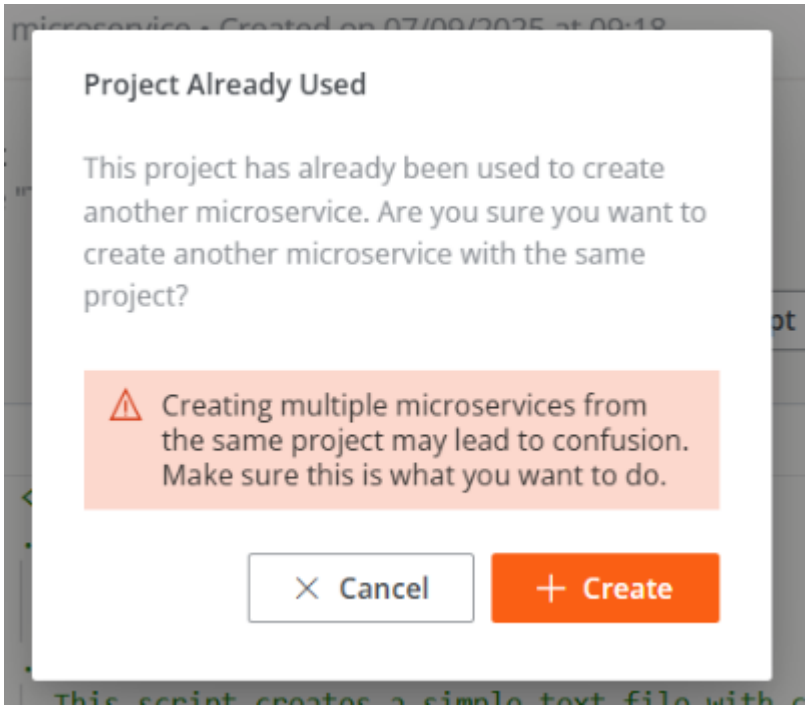
8. The `Improve the microservice` box, located at the bottom right of the screen, allows the user to add information to optimize the microservice. With each improvement, a new version of the code is generated, which can be seen in the Created Microservices column at the top.

9. Click on `Create microservice`.

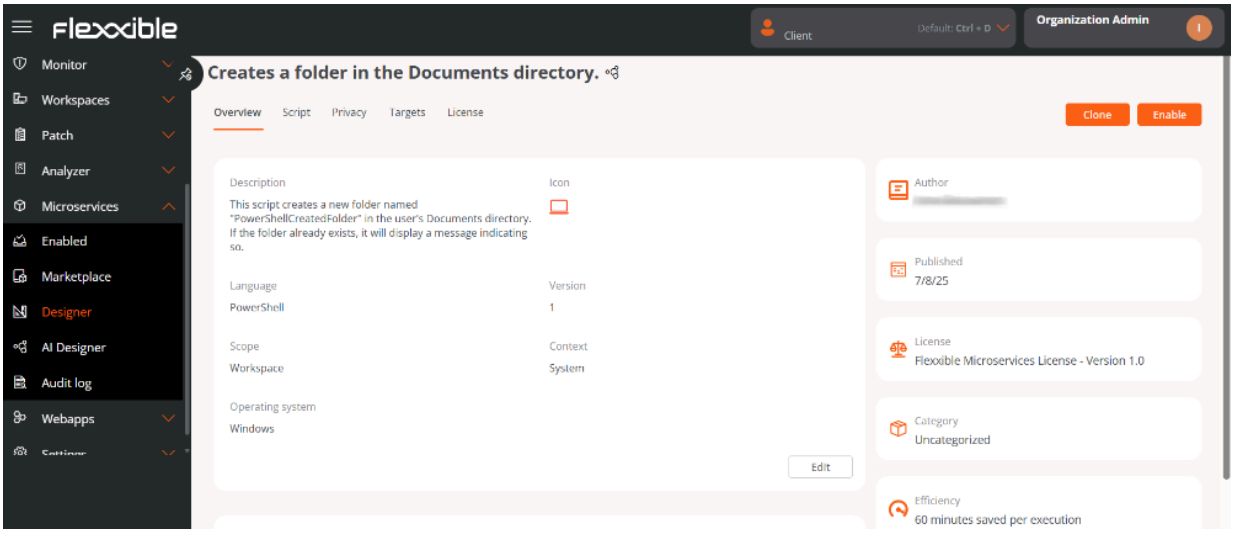
Copyright © 2024 Flexxible. Todos los derechos reservados.

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.



Copyright © 2024 Flexxible. Todos los derechos reservados.

11. Click on `Save`.

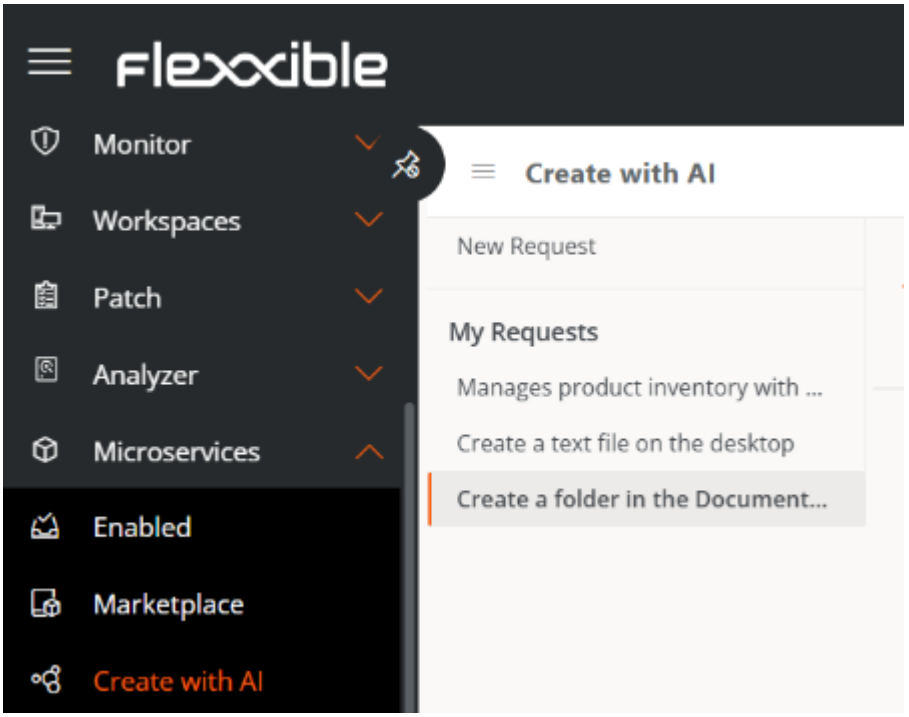
12. The microservice will appear in the list of the Designer and Marketplace sections.

> **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.

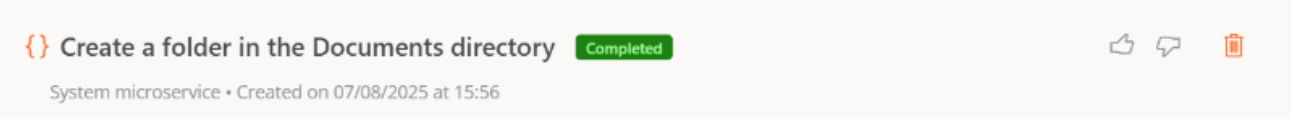
My requests

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.



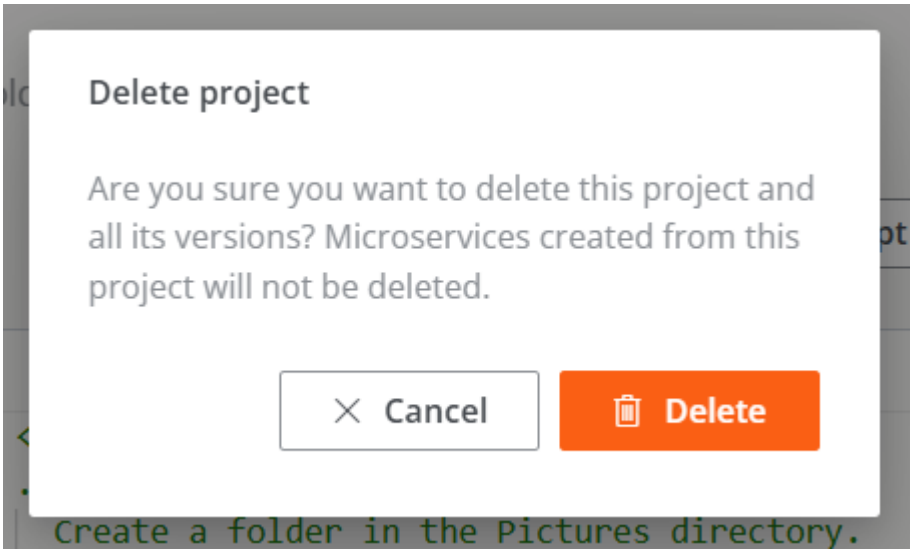
Copyright © 2024 Flexxible. Todos los derechos reservados.

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.

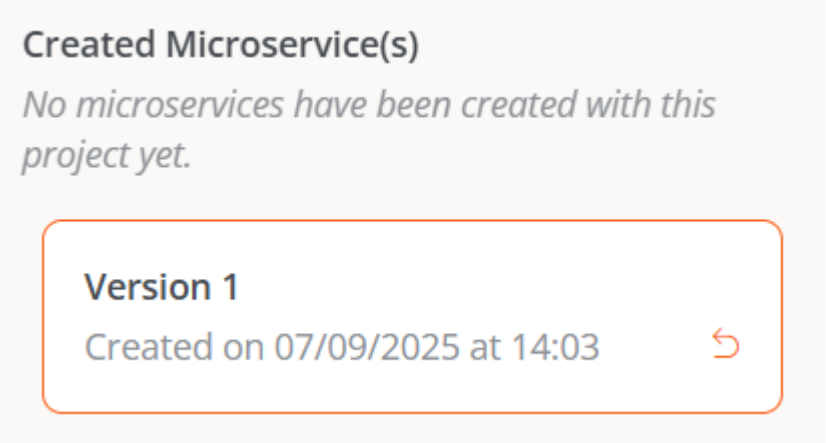
> **INFO**
>
> Deleting a request does not imply deleting the microservice created from it.

Copyright © 2024 Flexxible. Todos los derechos reservados.

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.

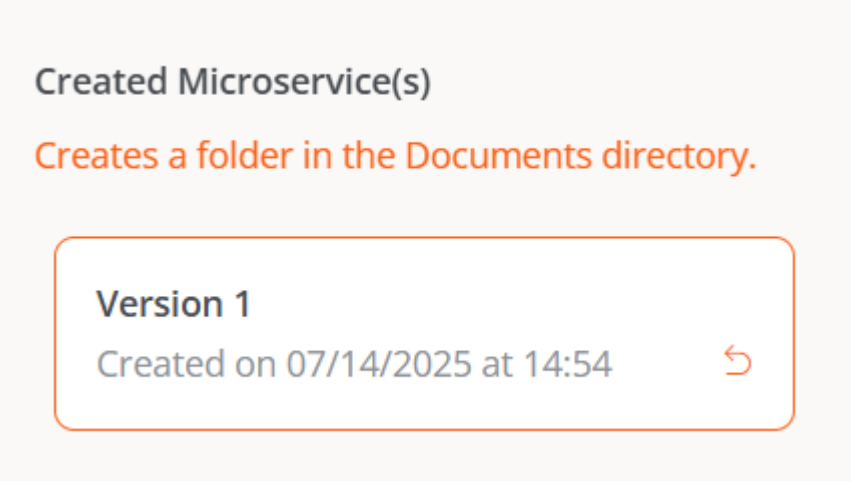
- When the AI designs the first version of a microservice, but it has not been created through the `Create microservice` button, the `Created Microservices` column shows a message like the one in the following image:



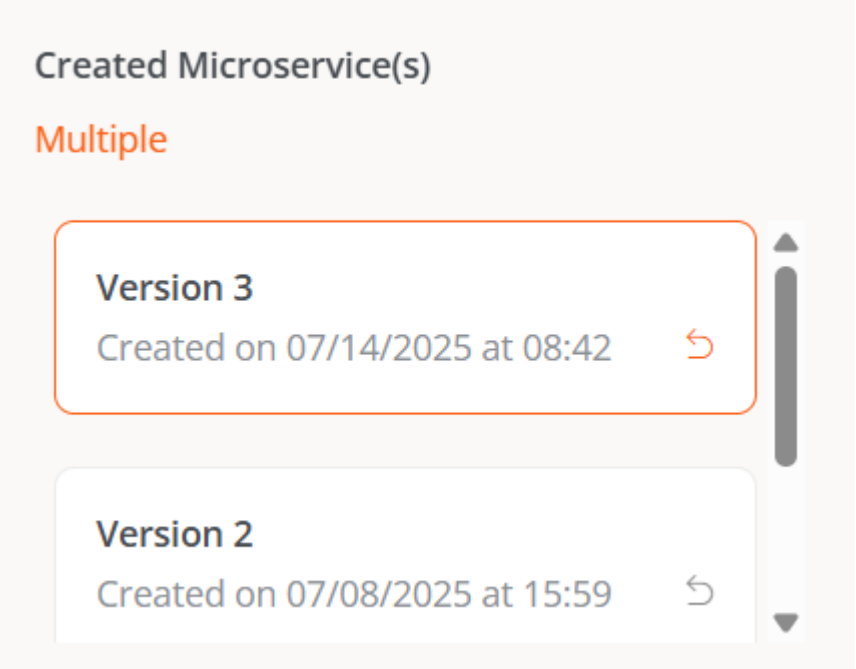
The orange arrow located in the box of each version allows loading the previous version's code.

- 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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

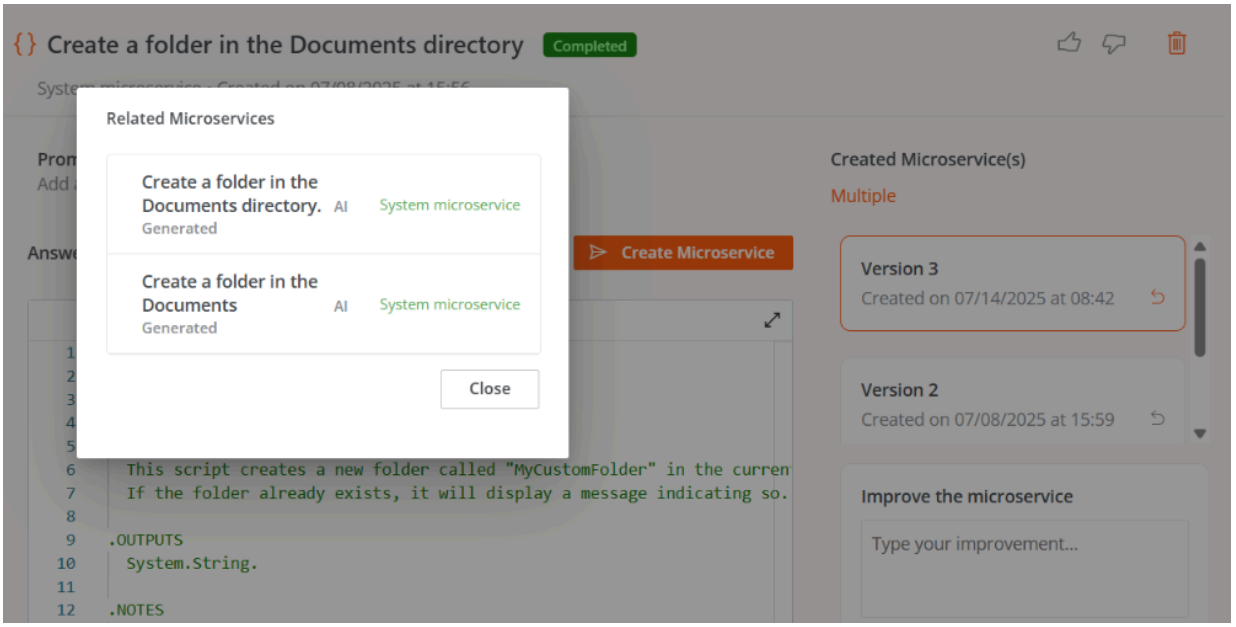


- When the AI designs and creates more than one version of a microservice, the `Created Microservices` column shows the word *Multiple*.



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.

Copyright © 2024 Flexxible. Todos los derechos reservados.



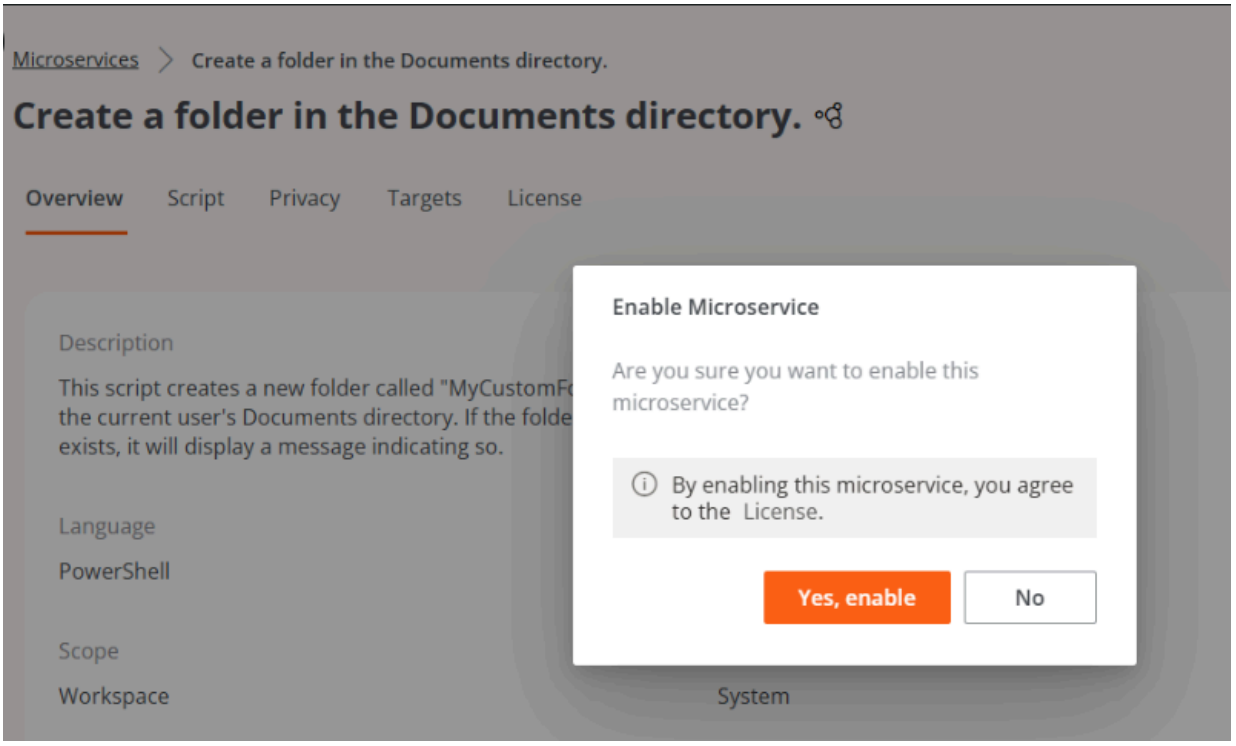
Enable a Microservice

The process to enable or disable an AI-generated microservice is the same as that used for manually creating microservices.

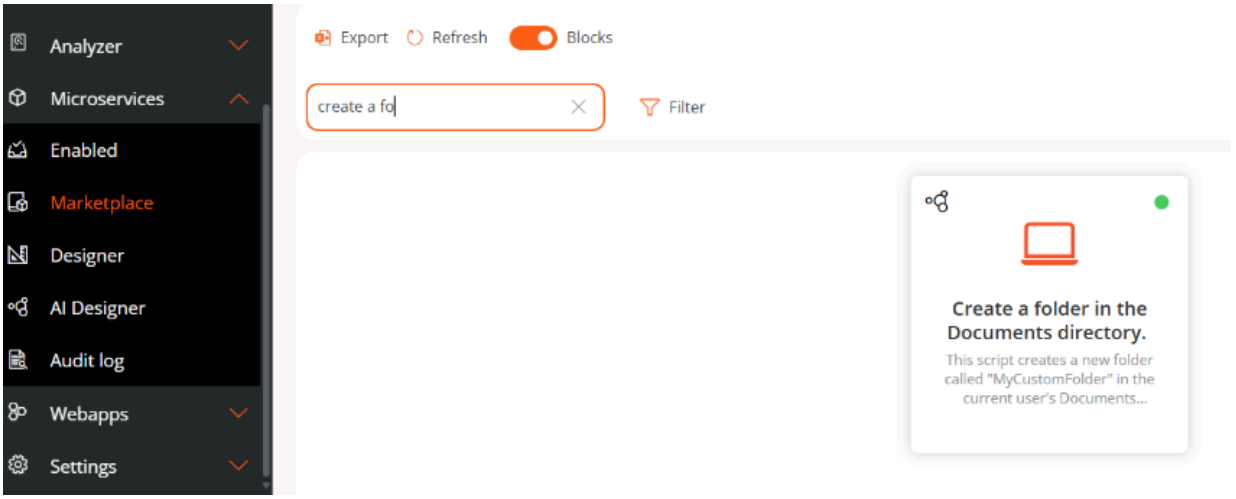
Steps to enable a microservice from Designer:

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.



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).

Copyright © 2024 Flexxible. Todos los derechos reservados.

> **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.

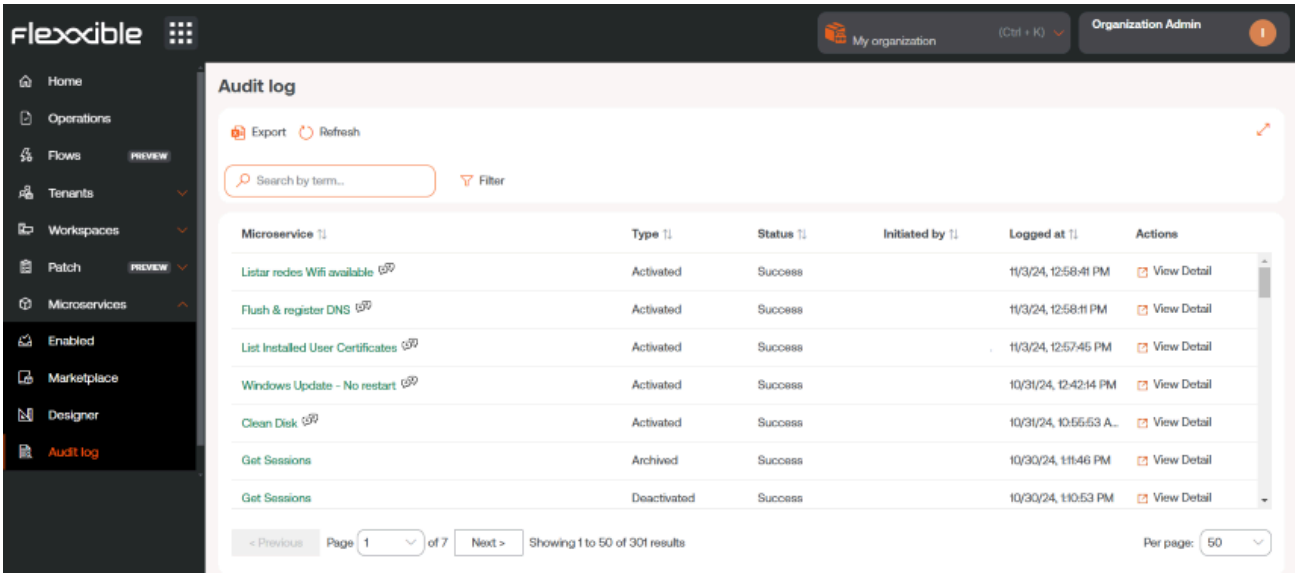
Please consult the guide Enable Microservices for End Users.

> **INFO**
>
> Flexxible recommends checking the `Privacy` and `Recipients` tabs in the Designer section before enabling a microservice to ensure they have the desired configuration.

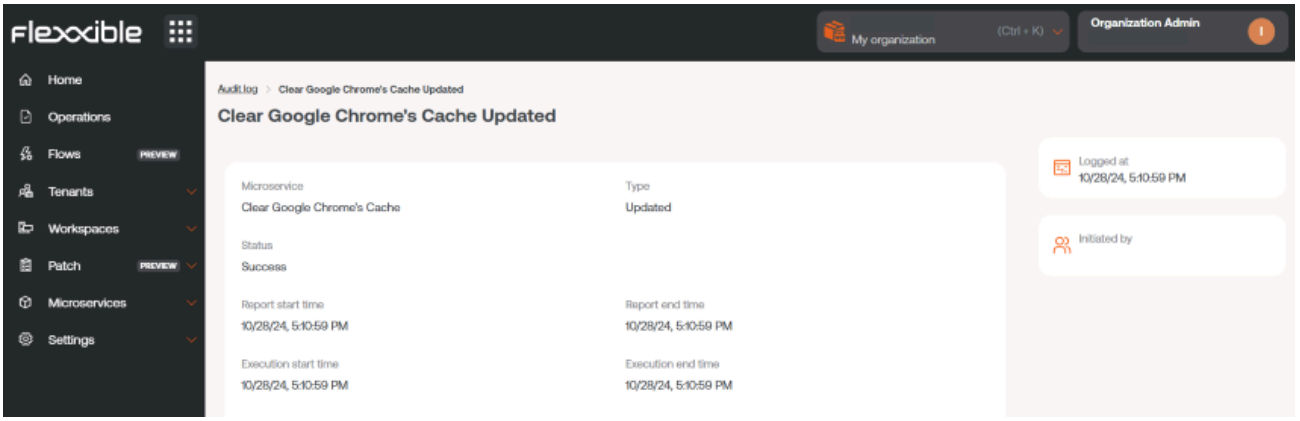
Copyright © 2024 Flexxible. Todos los derechos reservados.

Portal / Microservices / Audit Log

The audit log allows you to track microservice usage. From the overview, you can view the following information:



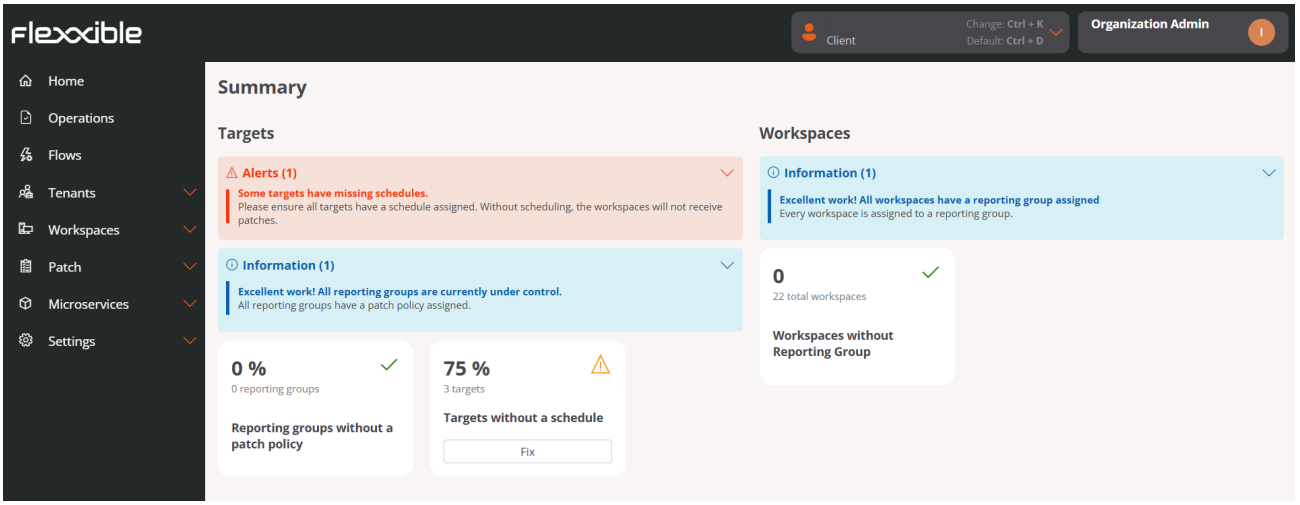
- **Microservice.** Name of the microservice.
- **Type.** It can be *Enabled*, *Disabled*, *Created*, *Updated*, or *Archived*.
- **Status.** Result of the microservice execution
- **Started by.** Email of the user who last executed it.
- **Registered on.** Date and time when it was created.
- **Actions.** Contains `View Details` to check more information about the microservice.



Copyright © 2024 Flexxible. Todos los derechos reservados.

Portal / Patch

Through `Updates`, a user will be able to manage how, which, and when updates will be applied on the devices of the report groups of their organization.



Patching management features

- They are essential to keep systems updated and secure because they significantly reduce the chance of a cyberattack.
- They solve known vulnerabilities, which minimizes the risk of security breaches that could compromise sensitive data and technological integrity.
- They ensure the stability and optimal performance of operating systems and applications.
- They fix errors, resulting in a smoother and more productive work environment. This translates to fewer interruptions and an overall increase in organizational efficiency.
- Many regulations require organizations to keep their systems updated to protect against threats; in this sense, patch management facilitates regulatory compliance and contributes to business continuity.

Patching management considerations in Portal

Copyright © 2024 Flexxible. Todos los derechos reservados.

- 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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

Portal / Patch / Summary

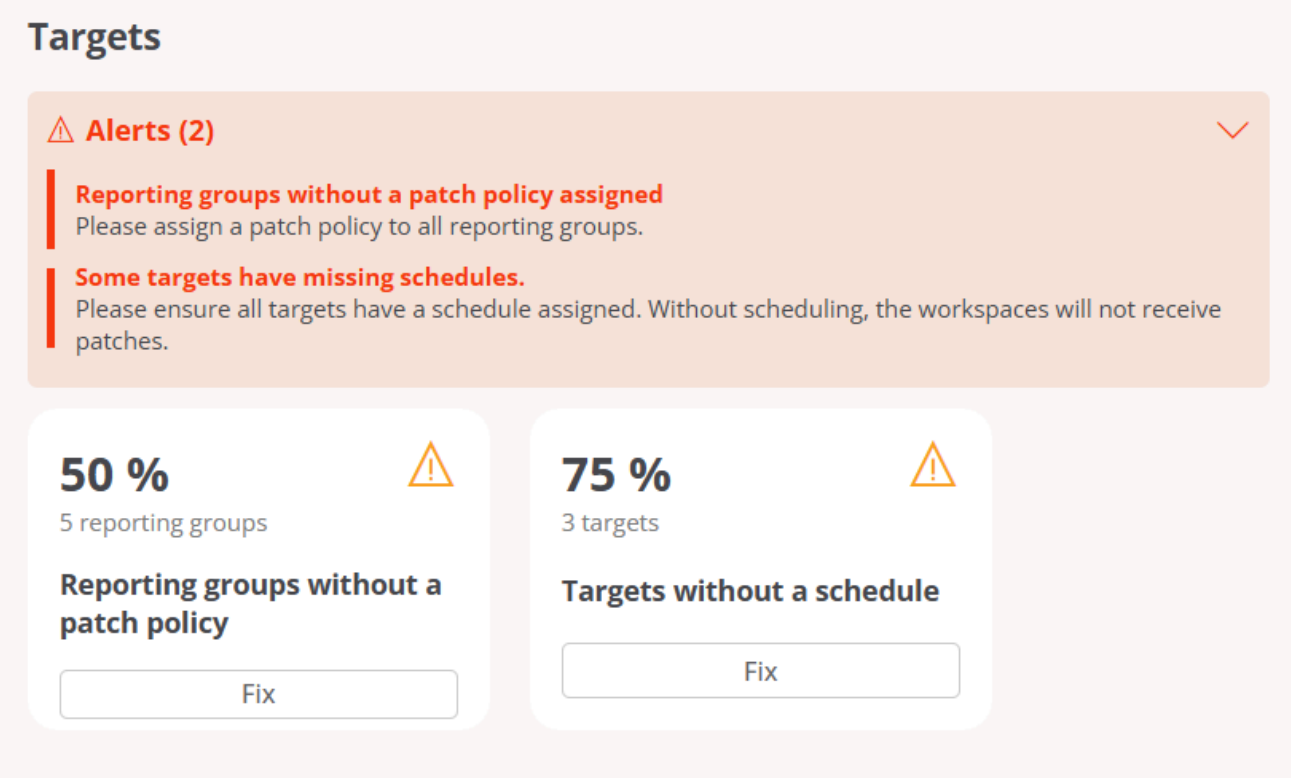
`Summary` shows a panel that describes the status of patch application on the organization's devices. From this view, you can get quantitative information about two aspects:

- 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.

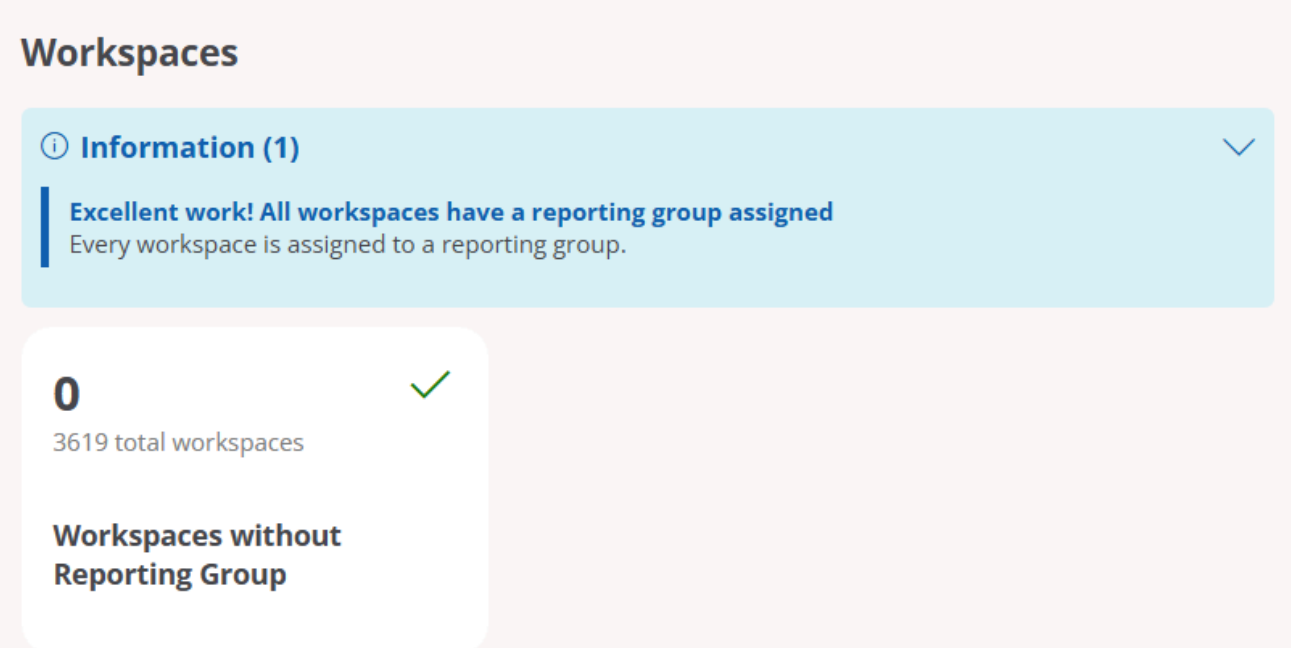
When it is detected that there are report groups without an associated patch policy or targets without a configured schedule, an alert warning is displayed (in orange); and when the cause of the warning is resolved, an informative alert is displayed (in blue).



Workspaces

Copyright © 2024 Flexxible. Todos los derechos reservados.

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).

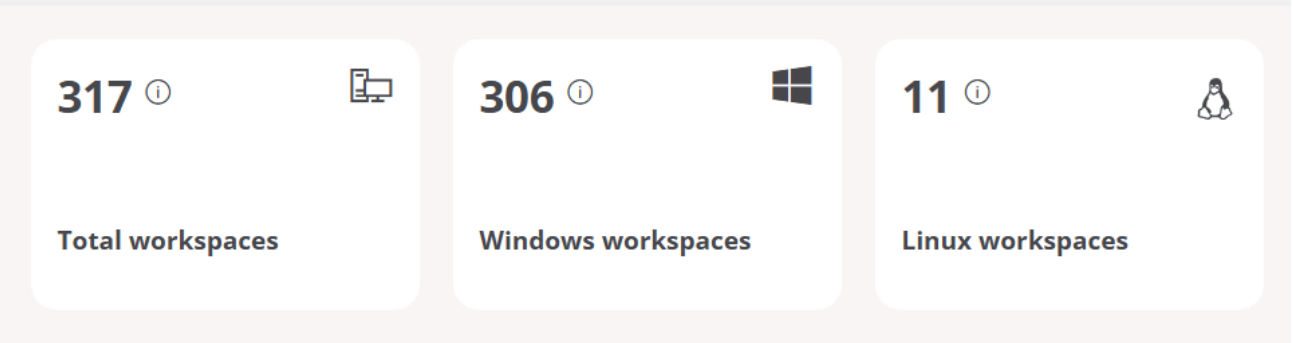


Copyright © 2024 Flexxible. Todos los derechos reservados.

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.



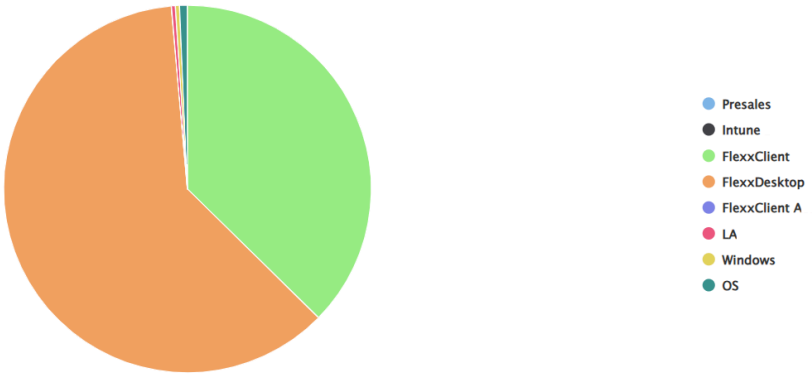
> **INFO**
>
> A reporting group can only have one target, but a target can be applied to more than one reporting group.

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

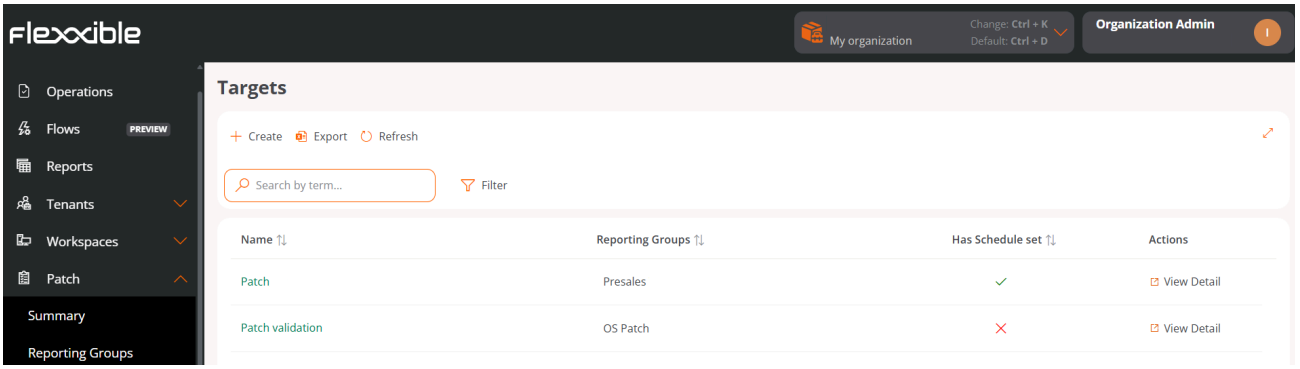
Total workspaces by reporting group ⓘ



Copyright © 2024 Flexxible. Todos los derechos reservados.

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

Copyright © 2024 Flexxible. Todos los derechos reservados.

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, the target's update policy can be configured regarding two scopes:

- Details
- Schedule

Details

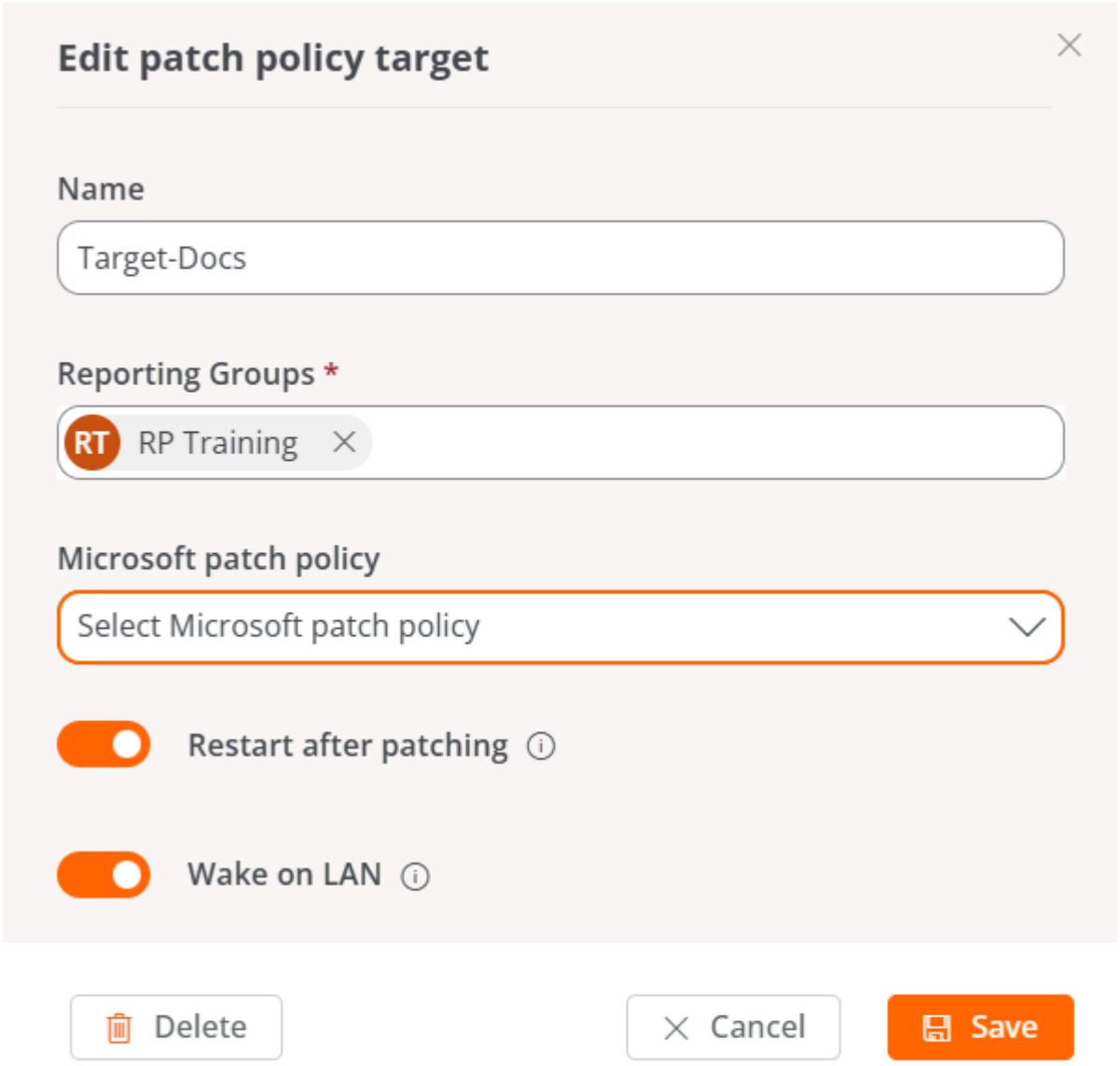
This tab shows the following information about the policy being consulted:

- **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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

The `Edit` button opens a modal window that allows configuring the aforementioned aspects.



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

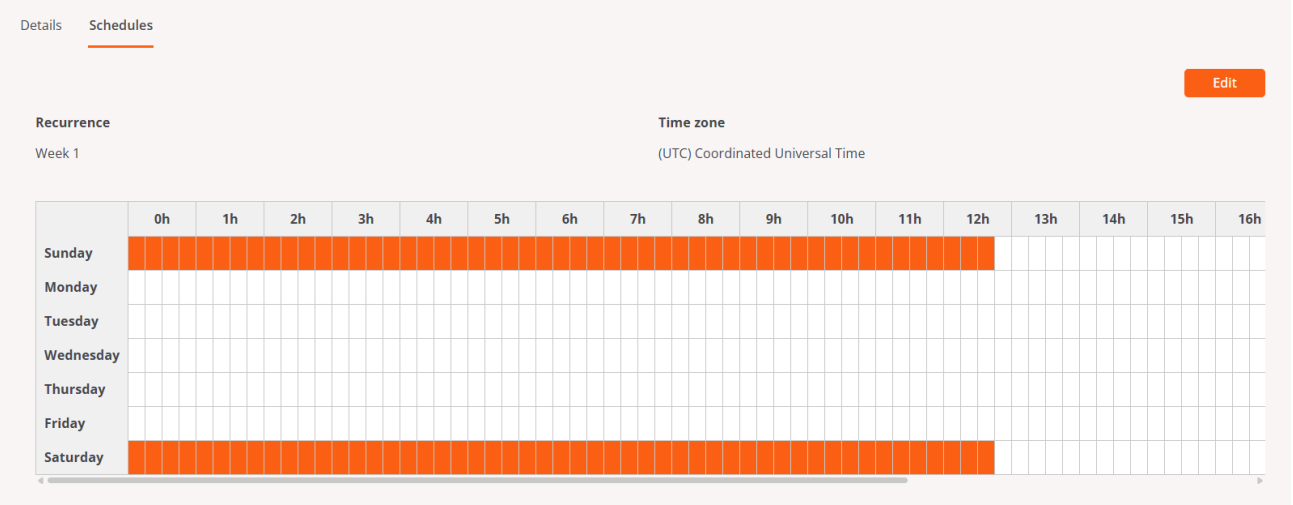
`Details` also provides information about the creation date of the update policy and the user who created it.

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

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.

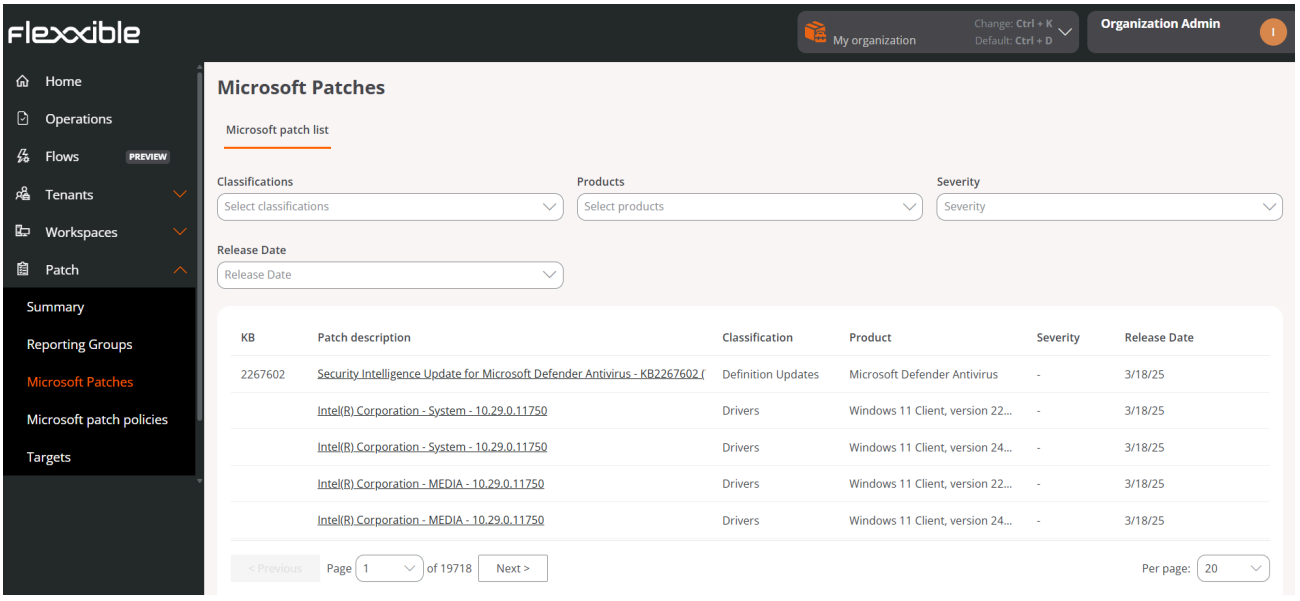
Update process

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

Copyright © 2024 Flexxible. Todos los derechos reservados.

Portal / Patch / Microsoft patches

This section allows you to check the available Microsoft update catalog. The table fields provide the following information:



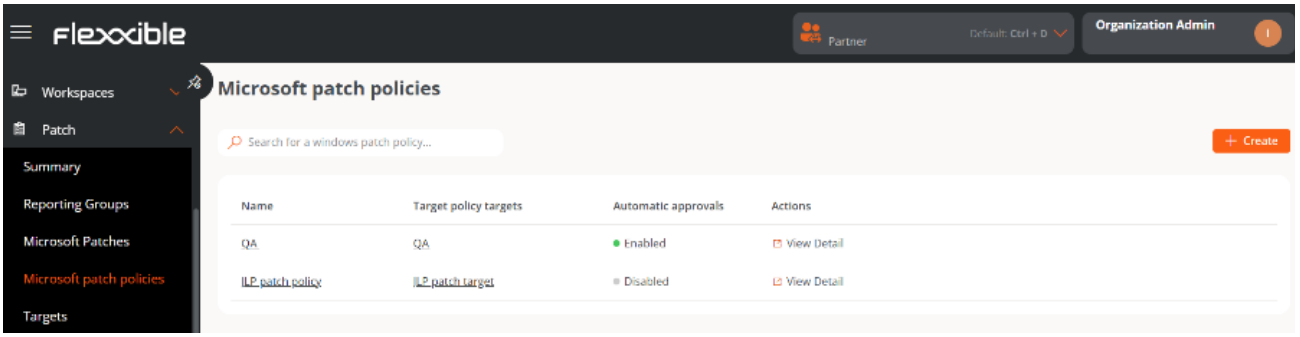
- **KB (Knowledge Base).** Unique identifier assigned to the Microsoft update package. Some drivers or firmware do not have an assigned KB.
- **Revision description.** Link that directs to detailed information about the Microsoft update.
- **Classification.** Category that corresponds to the update.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

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

Copyright © 2024 Flexxible. Todos los derechos reservados.

Portal / Patch / Microsoft patch policies

While Targets allows you to define when, how, and to whom updates are applied, from this section you can define what gets updated; that is, you can manage the approval or denial of the installation of one or more updates from the Microsoft catalog on an organization's devices.

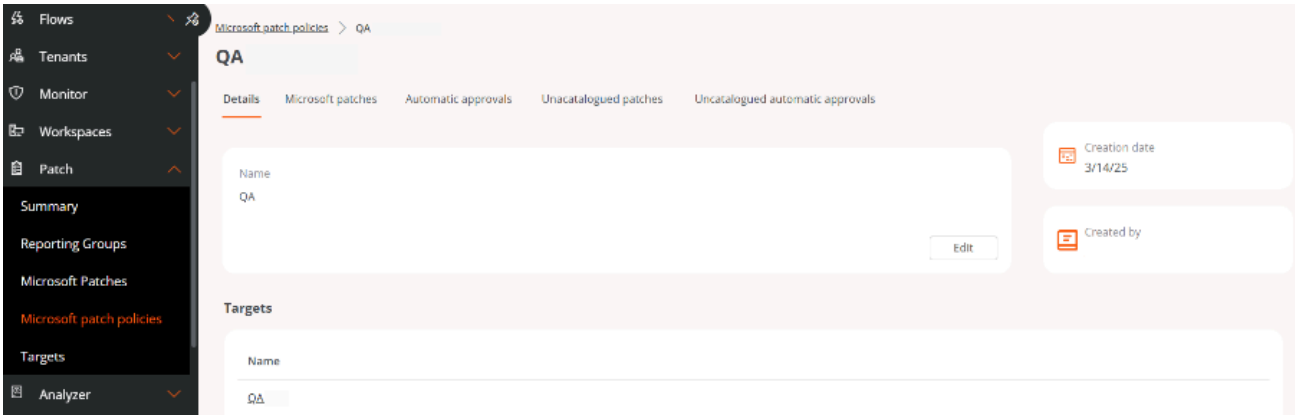


Create a new update policy

1. Access `Portal` -> `Updates` -> `Microsoft Update 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 newly created policy will appear in the table, in addition to the following fields:

- **Update policy targets.** Targets configured with a Microsoft update policy.
- **Automatic approvals.** Indicates if the automatic approvals setting is *Enabled* or *Disabled*.
- **Actions.** Contains the `View Details` button, to access five configuration scopes:

Copyright © 2024 Flexxible. Todos los derechos reservados.



- Details
- Microsoft patches
- Automatic approvals
- Non-cataloged Updates
- Non-cataloged Automatic Approvals

Details

Shows specific information about the policy being consulted:

- **Name.** Name of the policy.
- **Targets.** List of targets linked to the policy.
- **Creation Date.** Date when the policy was created.
- **Created by.** User who created the policy.

The `Edit` button opens a form to change the name of the policy or to delete it, if desired.

Microsoft patches

Shows a table with the list of Microsoft updates available for the linked target. The fields contain the following data:

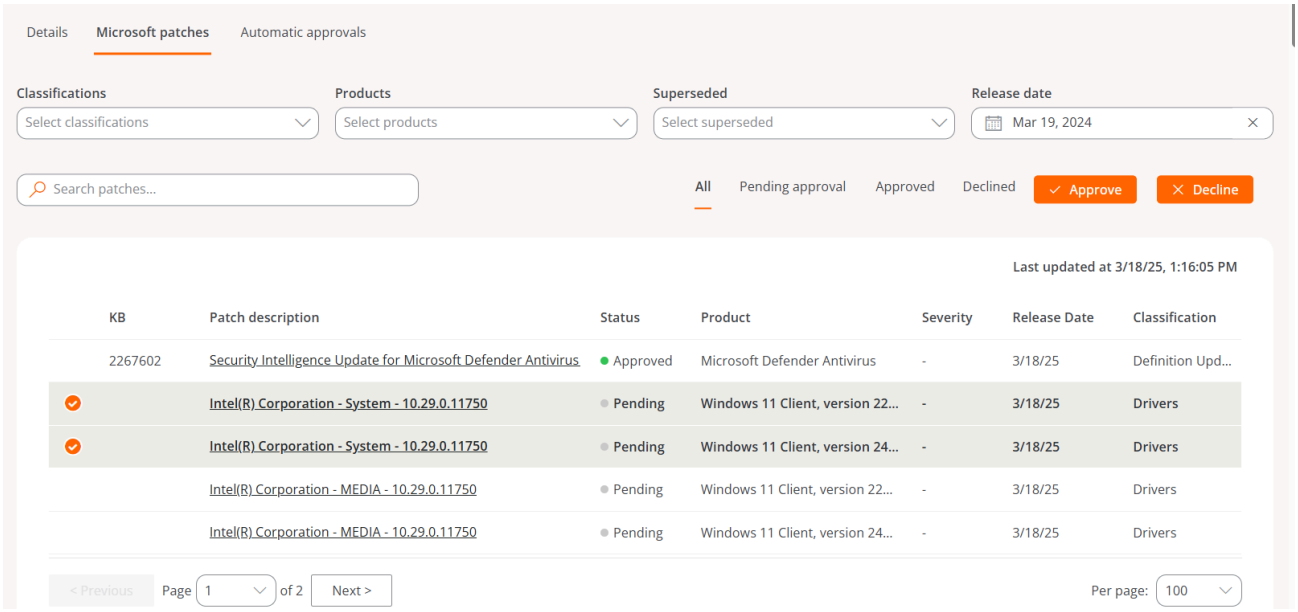
- **KB.** Unique identifier assigned to the Microsoft update package. Some drivers or firmware do not have an assigned KB.

Copyright © 2024 Flexxible. Todos los derechos reservados.

- **Revision description.** Link that directs to detailed information about the Microsoft update.
- **Status.** *Approved*, *Rejected*, or *Pending*.
- **Product.** Microsoft product to which the update applies.
- **Severity.** Level of urgency detected for executing the update.
- **Release Date.** Date from when the update is available.
- **Classification.** Category that corresponds to the update.
- **Last Update.** Date and time the list was last updated.

Above the table, there are several filtering options that allow listing the available updates according to *Classifications*, *Products*, *Superseded*, or *Release Date*.

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



Approve or reject a Microsoft update

To approve or reject an update, select one or more entries available in the table and choose the desired 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

Copyright © 2024 Flexxible. Todos los derechos reservados.

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 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

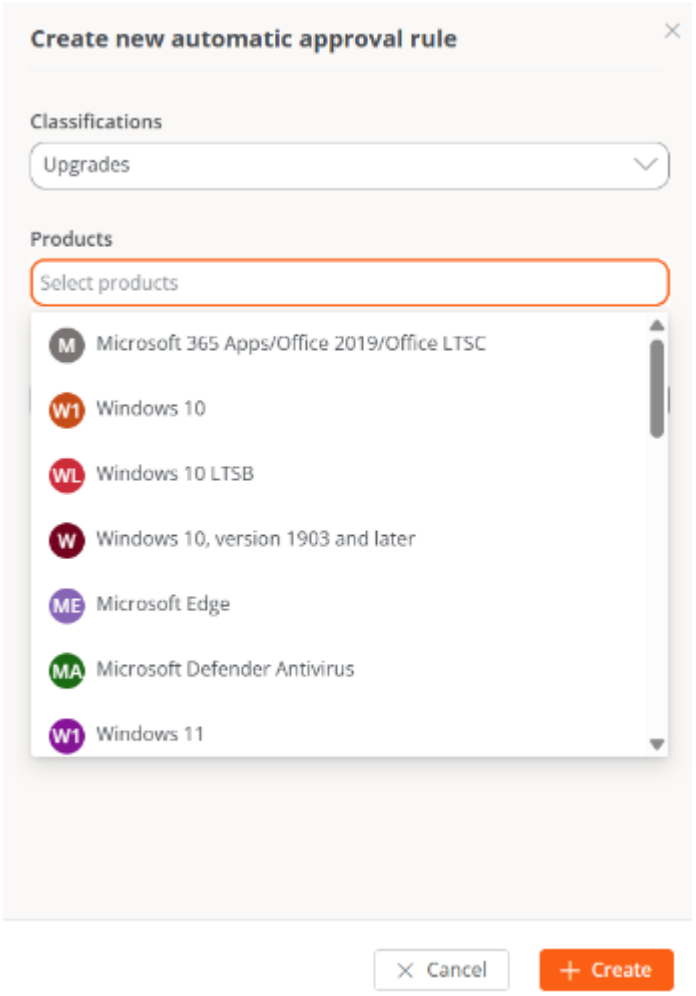
It is possible to configure automatic approval rules to apply updates, even more than one within the same update policy.

Create an automatic approval rule

1. Access `Portal` -> `Updates` -> `Microsoft Update 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.

Copyright © 2024 Flexxible. Todos los derechos reservados.



The fields of this section's table contain the following data:

- **Classification.** Category of the update. It can be *Updates*, *Critical Updates*, *Security Updates*, *Upgrades*, *Definition Updates*, *Drivers*, *Feature Packs*, and *Update Rollups*.
- **Products.** Name of the product to which the update applies.
- **Days after release.** Numeric value indicating how many days after the release date the update will be automatically approved.
- **Actions.** Contains the `View detail` button, which opens a form to edit the automatic approval rule.

Copyright © 2024 Flexxible. Todos los derechos reservados.

> 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.

Unlisted updates

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

Unlisted Updates correspond to these cases. These are pending updates that could be related to Microsoft features, but do not have an exact match with the entries in the Microsoft Updates list.

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

The fields of the table contain 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 that directs to detailed information about the Microsoft update.
- **Status.** *Approved*, *Rejected*, or *Pending*.
- **Product.** Microsoft product to which the update applies. In this type of updates, it is possible that the product is not informed since, at times, the data is not provided by the devices.
- **Severity.** Level of urgency detected for executing the update.
- **Release Date.** Date from when the update is available.
- **Classification.** Category that corresponds to the update.

Copyright © 2024 Flexxible. Todos los derechos reservados.

Above the table, there are several filtering options to list the available updates according to *Classifications*, *Products*, or *Date of arrival*.

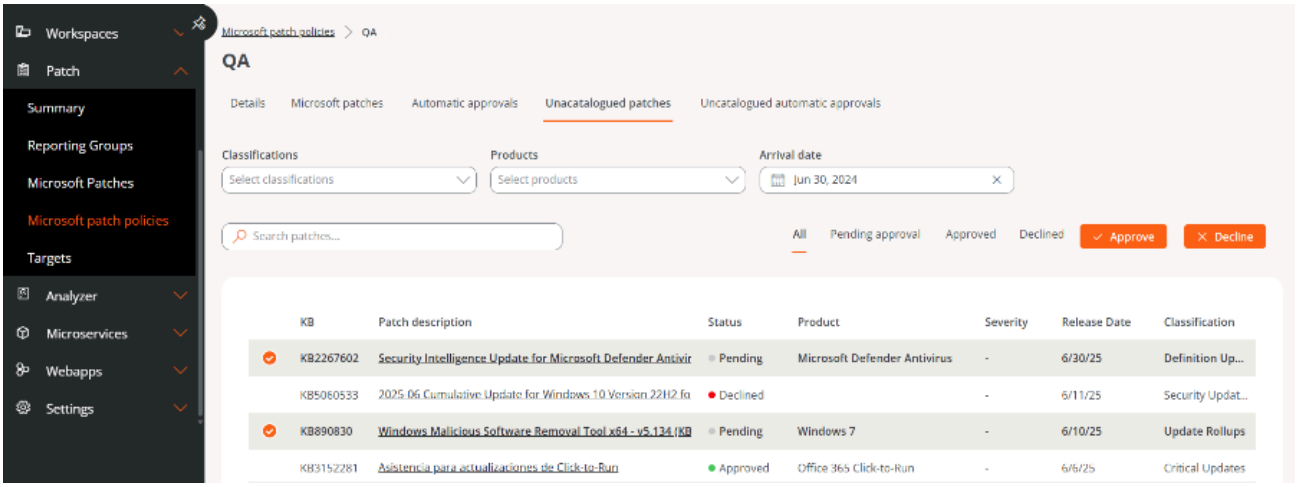
It is also possible to search by character strings or filter by their *Pending Approval*, *Approved*, or *Rejected* status.

Approve or reject an unlisted update

To approve or reject an unlisted update, select one or more entries available in the table and choose the desired 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.

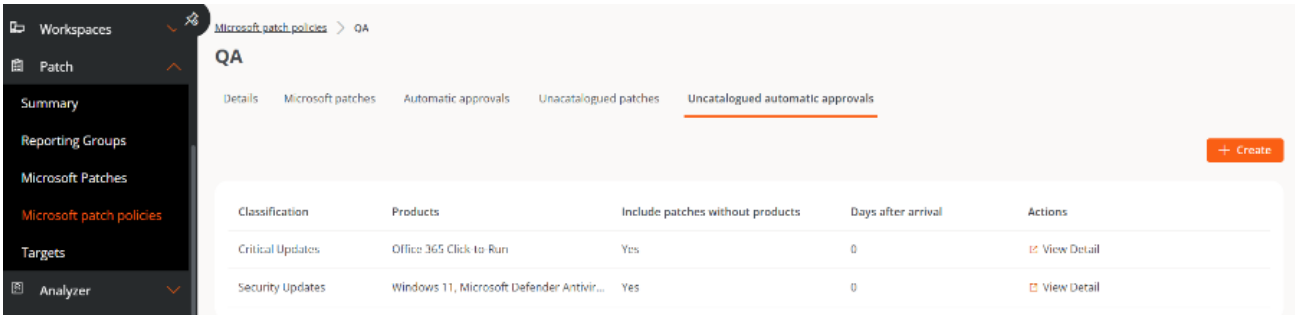
- Clicking `Reject` indicates that the update will attempt to uninstall during the next update process on devices that have it installed, in accordance with the target configuration. Not all updates can be uninstalled; the execution of this process depends on the update status of the device and other factors. The result of the process will be available in the corresponding update task.



Unlisted automated approvals

It's possible to set up automatic approval rules to apply unlisted updates.

Copyright © 2024 Flexxible. Todos los derechos reservados.

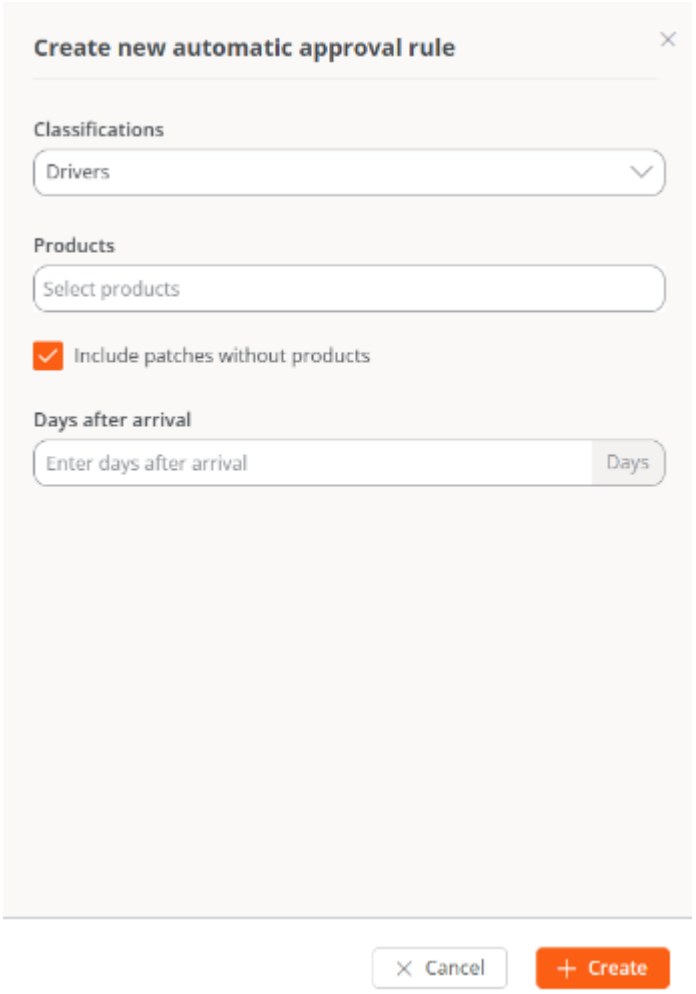


Create an automatic approval rule for unlisted updates

1. Access `Portal` -> `Updates` -> `Microsoft Update Policies`.
2. Click the name of the policy.
3. Go to the `Unlisted automated 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 *Updates Rollups*.
- **Products.** Products reported by the devices.
- **Include updates without products.** By checking this option, updates that don't have a product will be considered.
- **Days after arrival.** Specify how many days after the update arrives in the list it will be automatically approved.

Copyright © 2024 Flexxible. Todos los derechos reservados.



The fields of this section's table contain the following data:

- **Classification.** Category of the update. It can be *Updates*, *Critical Updates*, *Security updates*, *Upgrades*, *Definition updates*, *Drivers*, *Feature packs*, and *Updates Rollups*.
- **Products.** Reported product name.
- **Include updates without products.** Indicate whether the automatic approval rule includes updates without products.
- **Days after arrival.** Numeric value indicating how many days after the update arrives in the list it will be automatically approved.
- **Actions.** Contains the `View details` button, which opens a form to edit the automatic approval rule being viewed.

Copyright © 2024 Flexxible. Todos los derechos reservados.

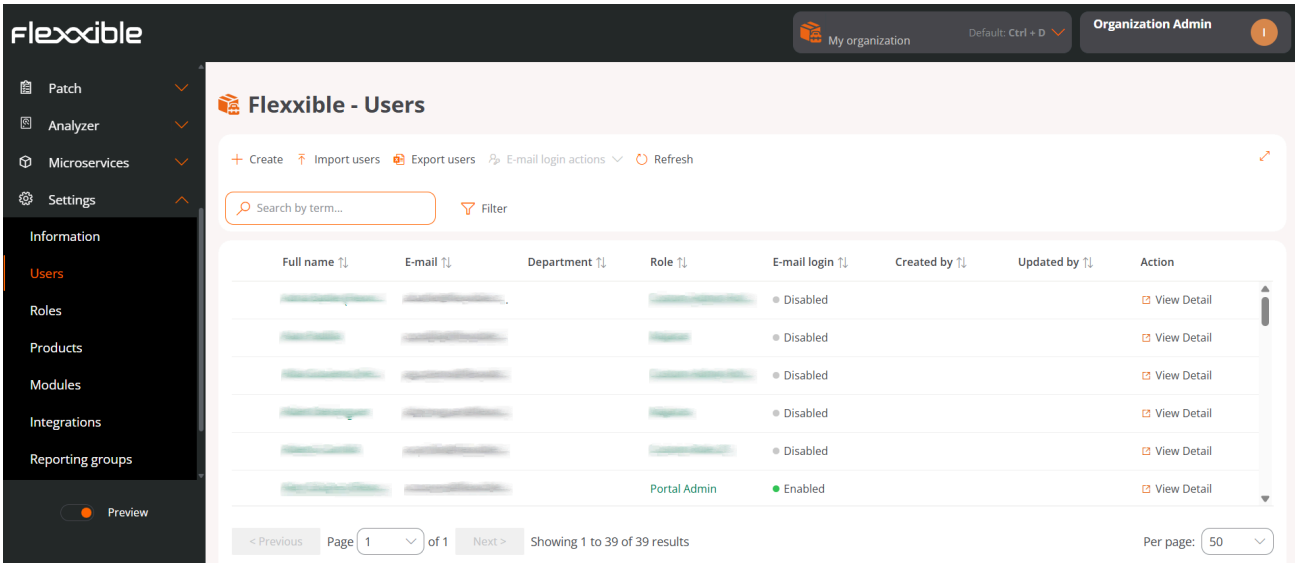
INFO

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

Copyright © 2024 Flexxible. Todos los derechos reservados.

Portal / Settings

The Configuration section in Portal provides specific management tools for the selected organization. Its subsections cover key aspects for service implementation, such as user creation, role assignment, remote assistance, reporting groups, among others.



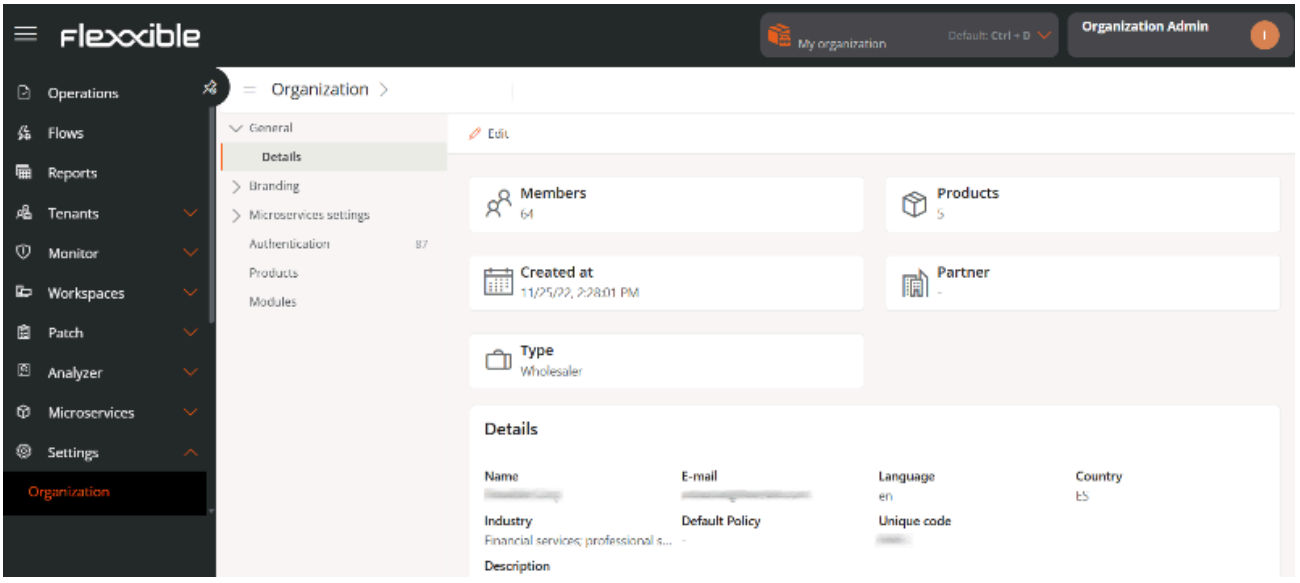
The Configuration section consists of the following subsections:

- Organization
- Users
- Roles
- Integrations
- Reporting Groups
- FlexxAgent Versions
- Policies

Copyright © 2024 Flexxible. Todos los derechos reservados.

Portal / Settings / Organization

The Organization section of Portal lets you manage the features that affect the organization's environment on a global level, from platform name assignment to remote assistance configuration.



Management can be done from the following sections:

- General
- Branding
- Microservices Configuration
- Authentication
- Products
- Modules

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

- **Language.** Configured language.
- **Country.** Country the organization belongs to.
- **Sector.** The sector it belongs to.
- **Description.** Description of the organization.

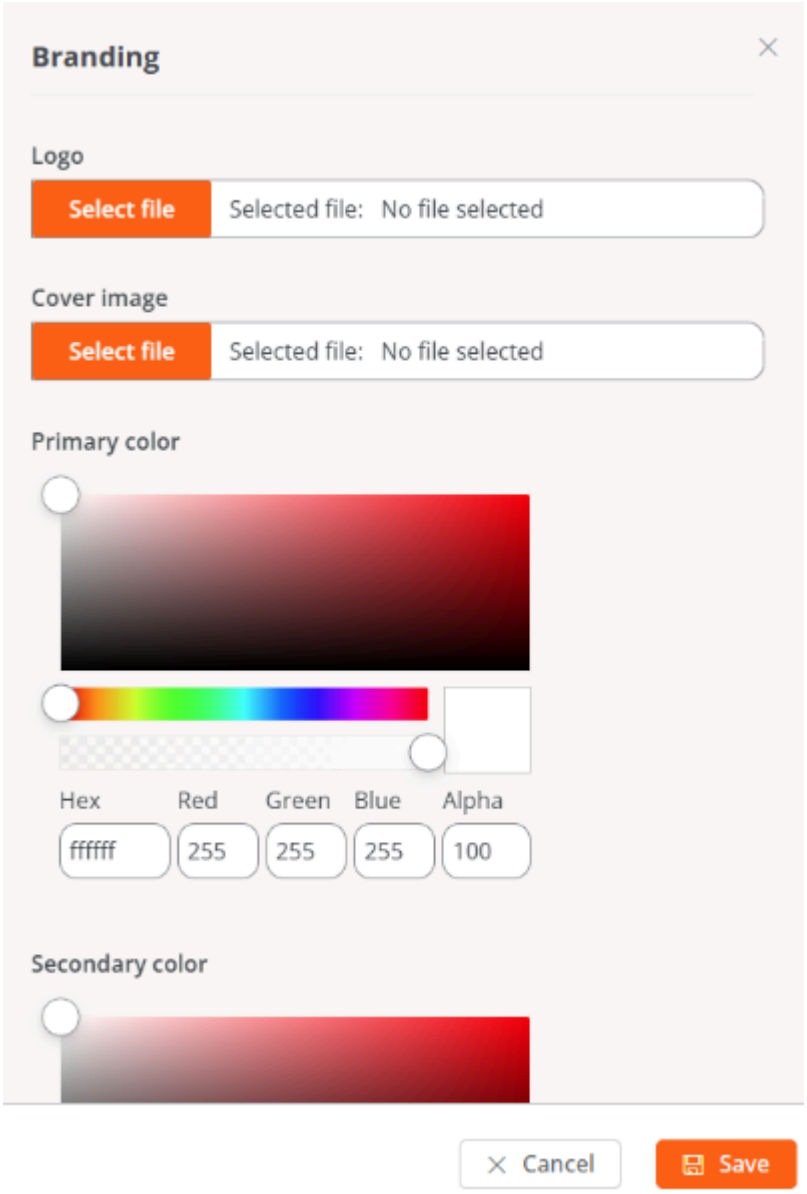
Additionally, from this section you can also access the following information:

- **Organization Members.** Number of members the organization has registered on the platform.
- **Products.** Number of Flexxible products the organization has contracted.
- **Created at.** Date when the organization was registered on the platform.
- **Partner.** For *client* type organizations, allows defining or modifying the *partner*.
- **Type.** Corresponding organization type.

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

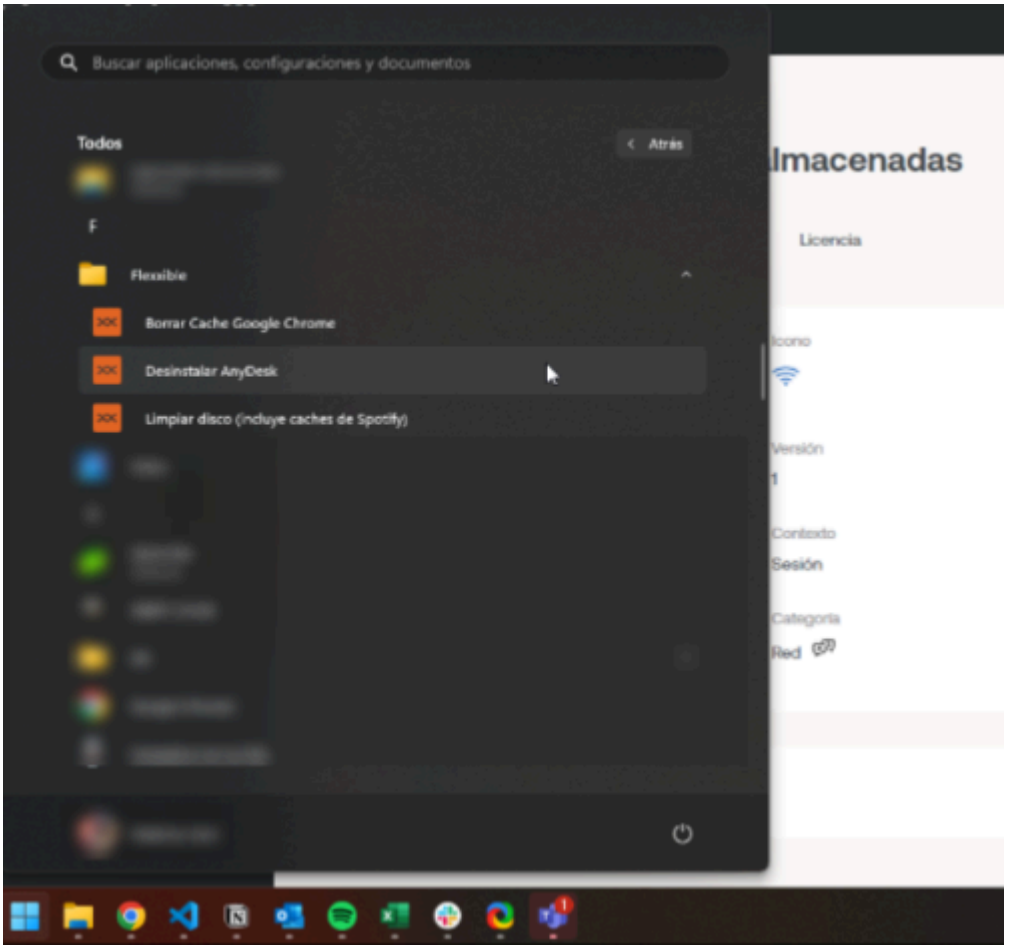


This section also indicates the date and time of the last update, as well as the name and email of the user who made it.

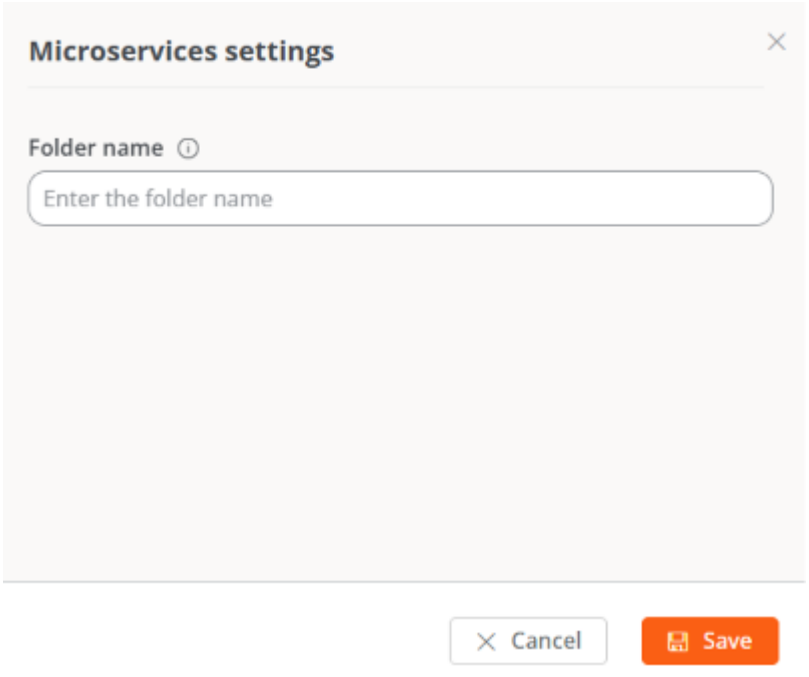
Microservices Configuration

When microservices are enabled for execution by the end user, they are automatically added to a device folder named Flexxible; however, this name can be modified via the `Edit microservices settings` button.

Copyright © 2024 Flexxible. Todos los derechos reservados.

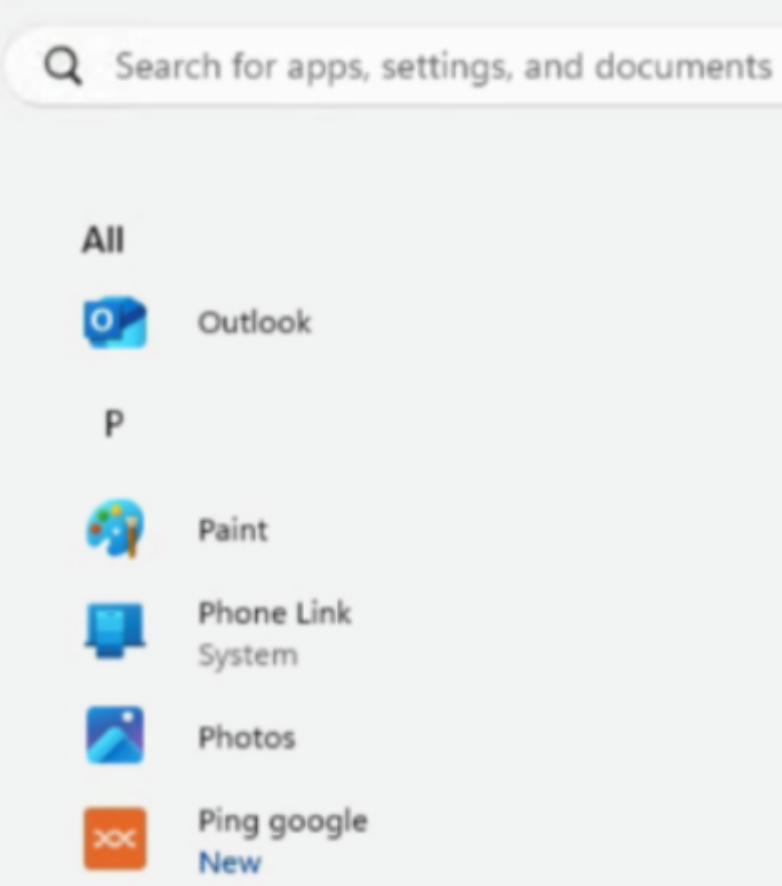


The chosen name must be between 3 and 50 characters, and can only contain letters, numbers, hyphens, and underscores.



Copyright © 2024 Flexxible. Todos los derechos reservados.

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.



Just like in the previous section, this one also indicates the date and time of the last time the information was updated, as well as the name and email of the user who did it.

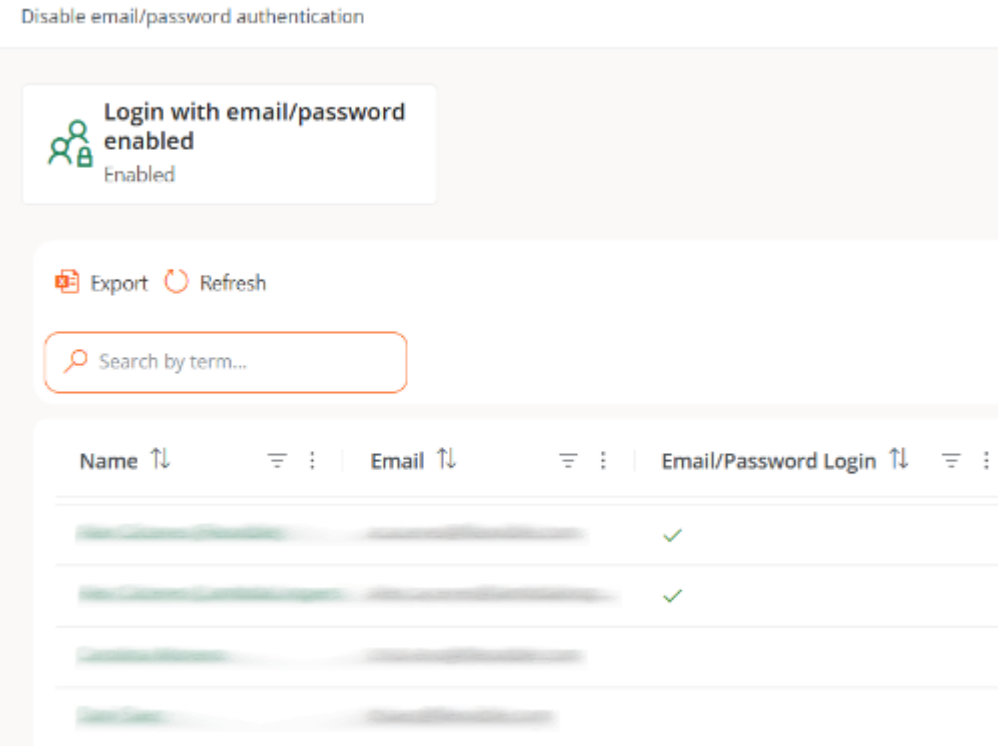
Authentication

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

> **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.

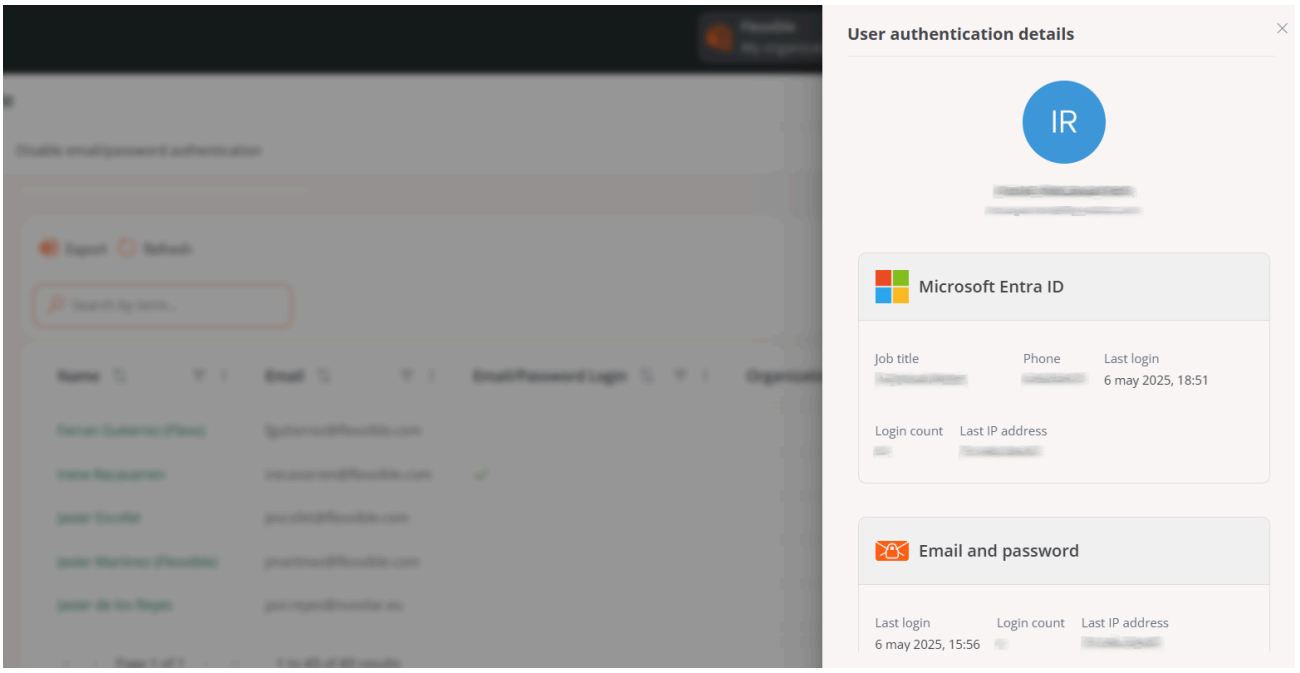
User authentication detail

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*.

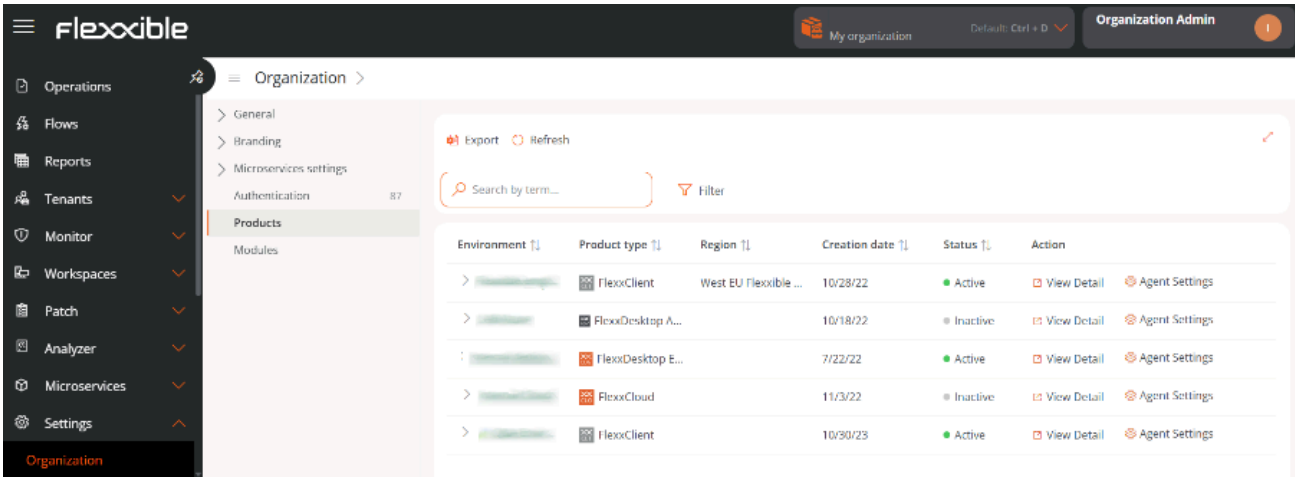
Copyright © 2024 Flexxible. Todos los derechos reservados.

- **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.



Copyright © 2024 Flexxible. Todos los derechos reservados.

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

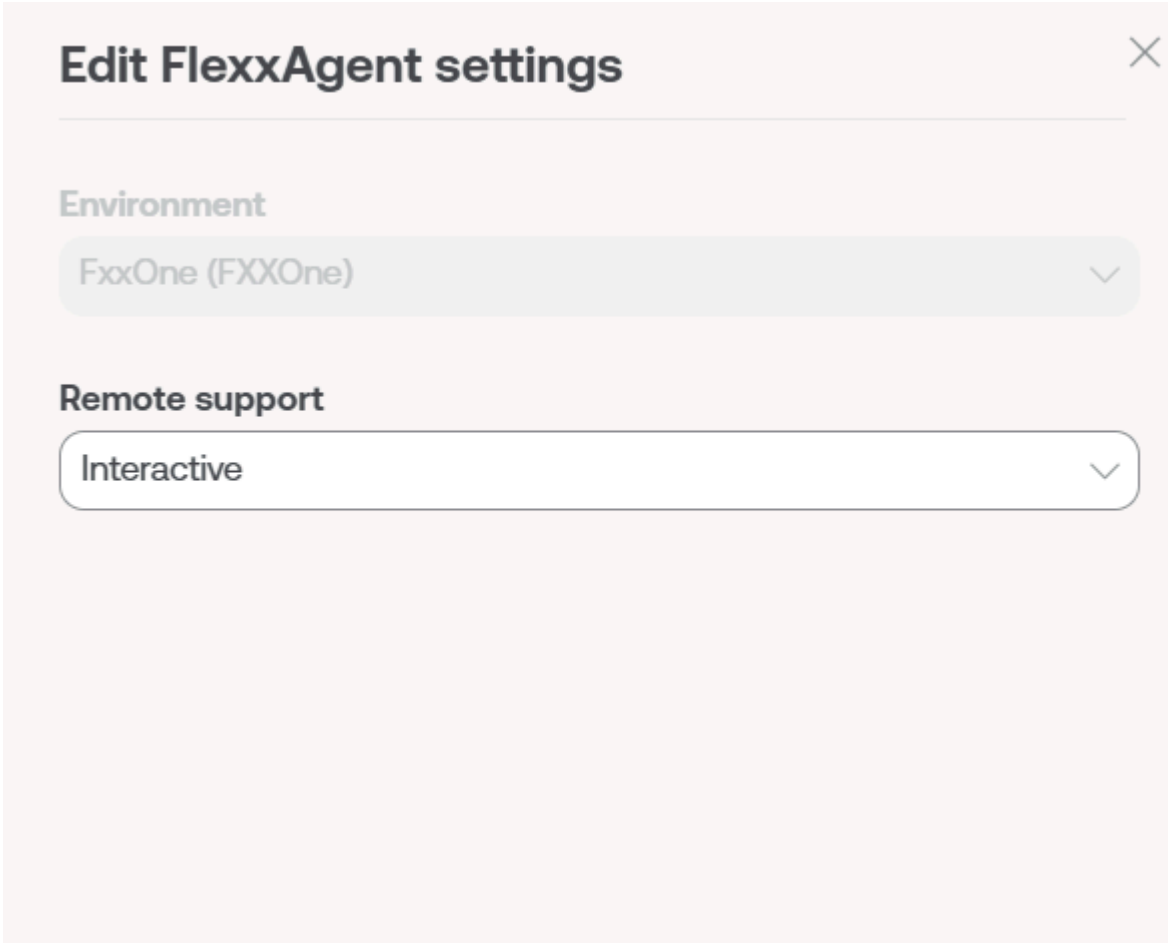
This form allows changes at the *Remote Assistance* and *Analyzer Proxy* levels.

FlexxAgent Settings - 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.

Copyright © 2024 Flexxible. Todos los derechos reservados.



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.

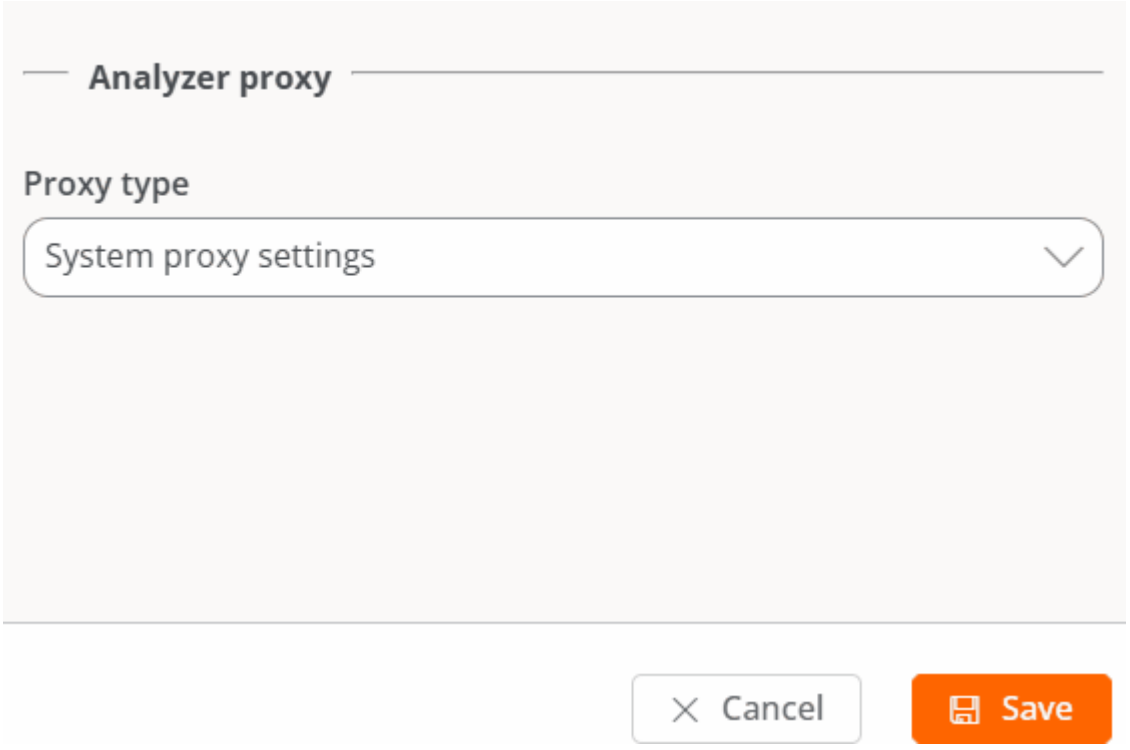
The proxy configuration of *FlexxAgent Analyzer* is not always the same as that of *FlexxAgent*, so according to the proxy operation in each environment, its settings will need to be set appropriately.

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

- 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.



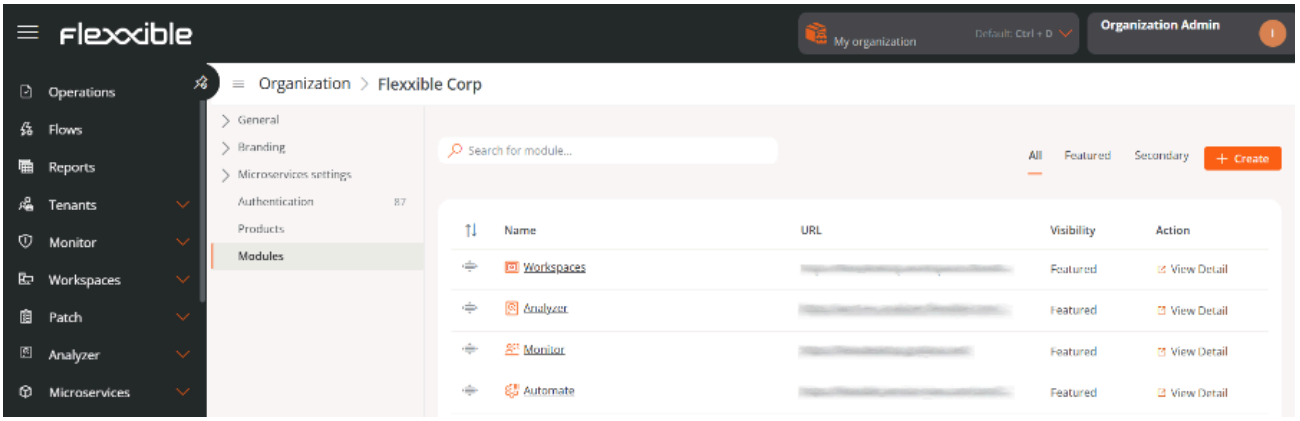
INFO

Some of the FlexxAgent configuration options 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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

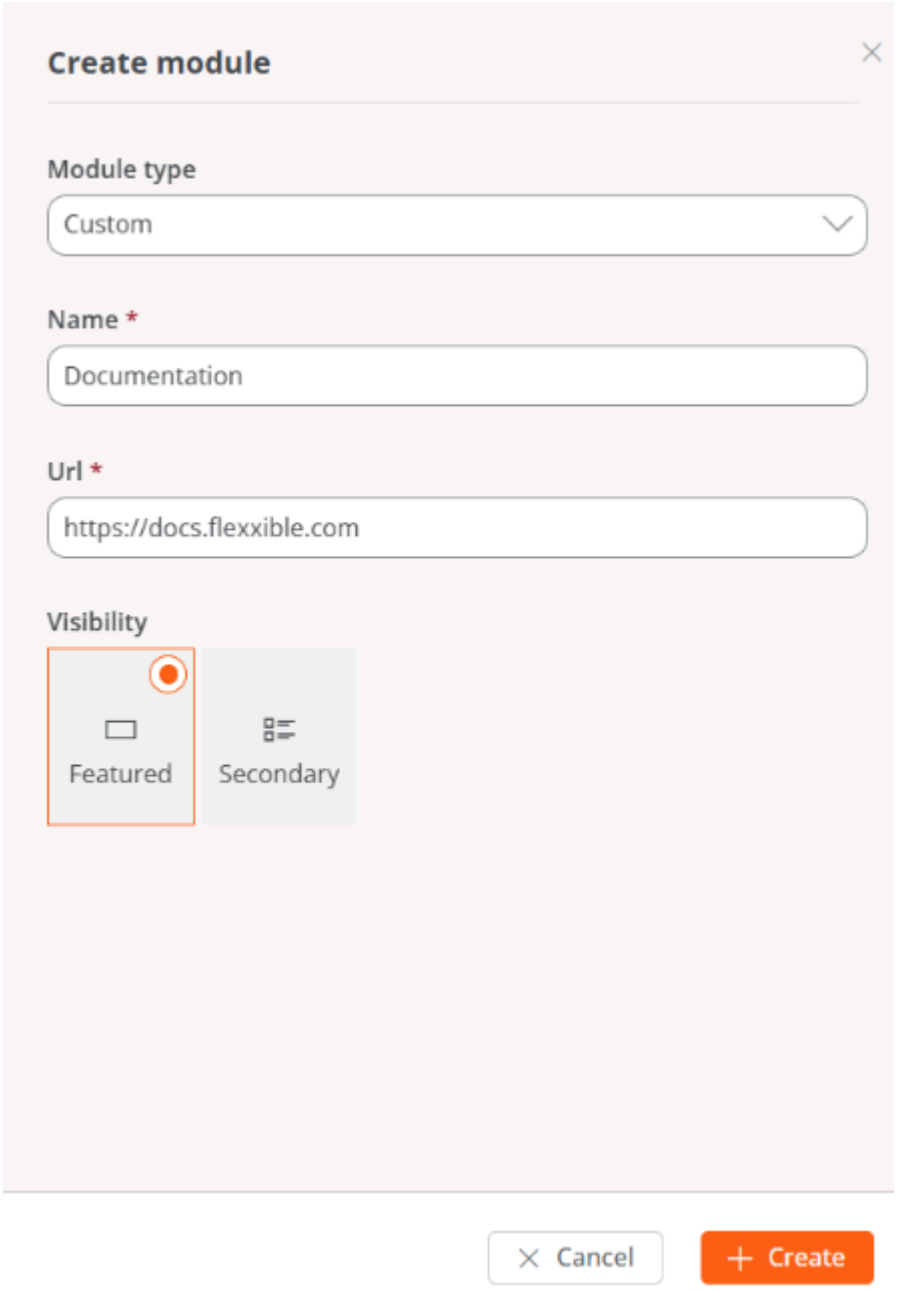


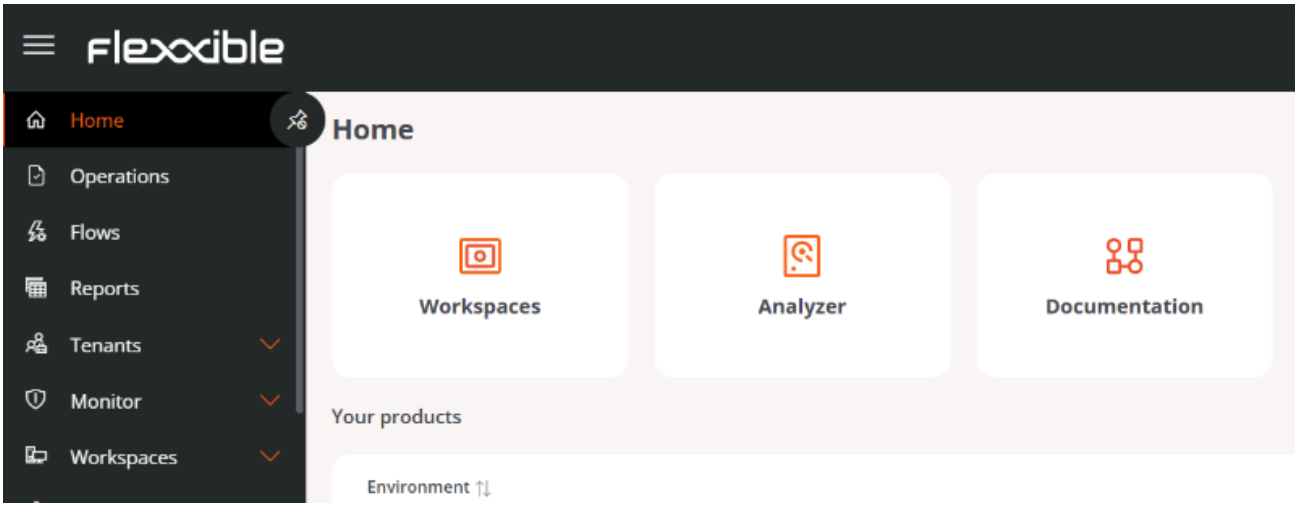
The table contains the module name, its corresponding URL, and its visibility level. From `See detail`, a label and URL can be assigned to the selected module, and you can define whether it is visible as *Featured* or *Secondary*. When it is featured, it appears among the main modules in the Home section 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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

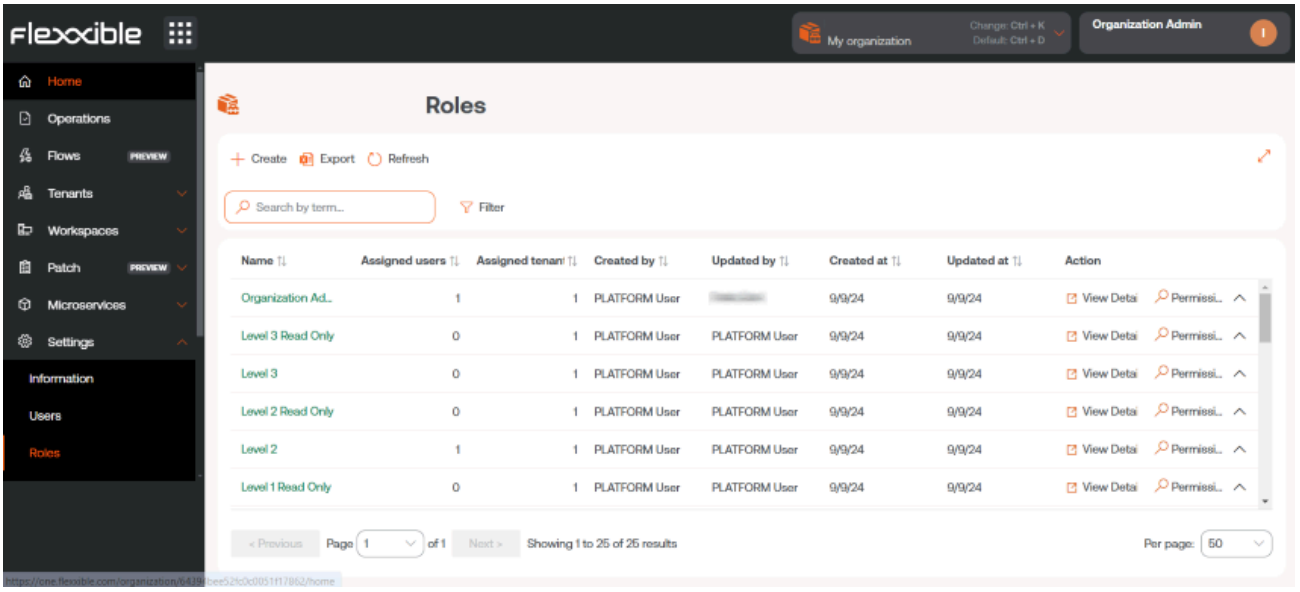




Copyright © 2024 Flexxible. Todos los derechos reservados.

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

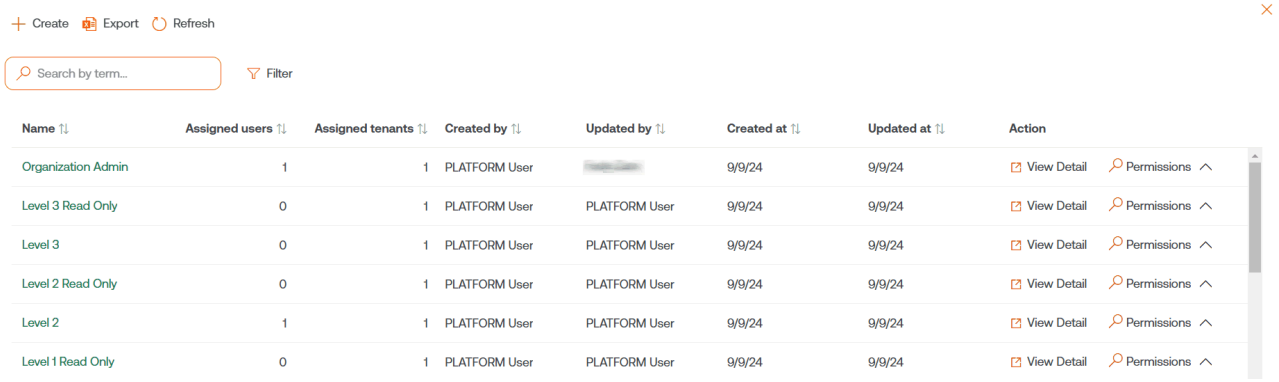
Roles table

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.** Date the role was created.
- **Updated on.** Date the role was updated.
- **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.



Copyright © 2024 Flexxible. Todos los derechos reservados.

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

Copyright © 2024 Flexxible. Todos los derechos reservados.

It allows you to apply the permissions to all the organizations you have access to. In service provider use cases, it allows you to centrally manage permissions and replicate changes to the client organizations you manage.

When role permissions mix permissions applied at the "All tenants" level and specific configurations for an organization, which may be different, the more specific permission wins. In this way, a default configuration can be made for all organizations and overwrite those that require modifications.

Tenant

Allows informing the organization to which permissions are being granted in the role being edited; the `All tenants` check allows configuring the role's permissions to apply to all organizations that can be accessed.

Portal Permissions

It allows you to select access level to Portal at different levels:

- No access
- User
- L1 Support Team
- L1 Support Team Read Only.
- L2 Support Team
- L2 Support Team Read Only
- L3 Engineering Team
- L3 Engineering Team Read Only
- Organization Admin
- Organization Admin Read Only

Details of the visibility and allowed operations at each level can be found in Additional Considerations

Workspaces permissions

Copyright © 2024 Flexxible. Todos los derechos reservados.

In `Workspaces`, there are four roles with different levels of access available:

- Level 1
- Level 1 read-only
- Level 2
- Level 2 read-only

Details of the visibility and allowed operations at each level can be found in Additional Considerations

Analyzer permissions

Gives the option to allow or deny access to Analyzer.

All reporting groups

It allows you to apply permissions to all reporting groups you have access to. In service provider use cases, it allows you to centrally manage permissions and replicate changes to the client organizations you manage.

Reporting Groups

It allows you to apply permissions to specified reporting groups; it can be more than one.

Users

This table allows you to see the users assigned to the role and provides the option to search.

Copyright © 2024 Flexxible. Todos los derechos reservados.

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

Copyright © 2024 Flexxible. Todos los derechos reservados.

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

Copyright © 2024 Flexxible. Todos los derechos reservados.

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

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.

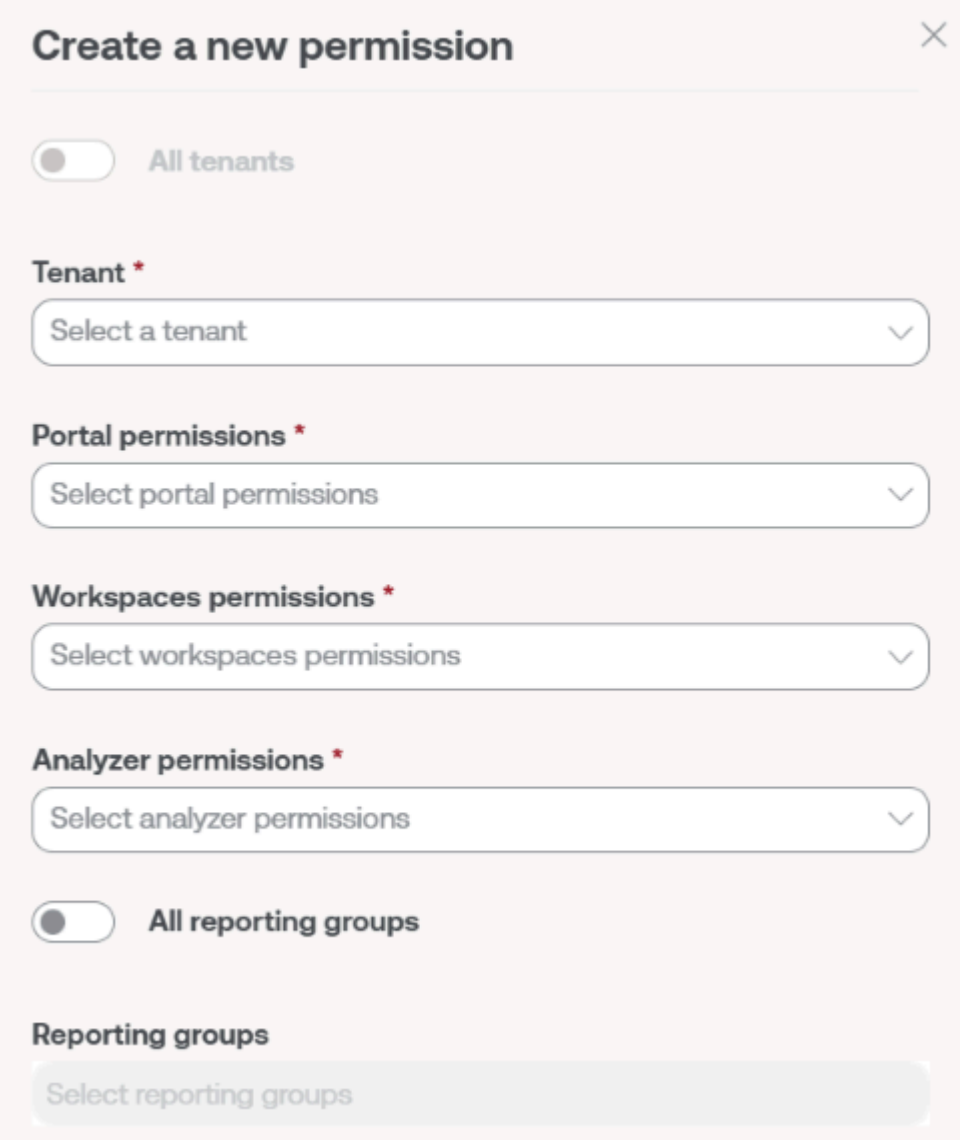
An organization is dependent when:

- 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

Copyright © 2024 Flexxible. Todos los derechos reservados.



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

Copyright © 2024 Flexxible. Todos los derechos reservados.

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	✅	❌	⭐⭐	❌	❌	❌	
		Refresh	✅	❌	⭐⭐	❌	❌	❌	
		Delete	✅	❌	⭐⭐	❌	❌	❌	
Reports	List	Read	✅	✅	❌	✅	✅	✅	
	Detail	Read	✅	✅	❌	✅	✅	✅	

Copyright © 2024 Flexxible. Todos los derechos reservados.

Section	Functionality	Action	1	2	3	4	5	6	
		Create	✅	❌	❌	❌	❌	❌	
		Delete	✅	❌	❌	❌	❌	❌	
	Settings	Refresh	✅	❌	❌	❌	❌	❌	
Tenants		Create	✅	❌	❌	❌	❌	❌	
		Read	✅	✅	❌	❌	❌	❌	
		Refresh	✅	❌	❌	❌	❌	❌	
		Delete	✅	❌	❌	❌	❌	❌	
	Activation	Read	✅	✅	❌	❌	❌	❌	
Monitor	Active alerts	Read	✅	✅	✅	✅	✅	✅	
	Alert Configuration	Create	✅	❌	❌	❌	❌	❌	
		Read	✅	✅	✅	❌	❌	❌	
		Refresh	✅	❌	❌	❌	❌	❌	
		Delete	✅	❌	❌	❌	❌	❌	
Workspaces		Read	✅	✅	⭐	✅	✅	✅	
		Refresh	✅	❌	✅	✅	❌	✅	
	Workspace Groups	Read	✅	✅	⭐	✅	✅	✅	

Copyright © 2024 Flexxible. Todos los derechos reservados.

Section	Functionality	Action	1	2	3	4	5	6	
		Create	✅	❌	❌	❌	❌	✅	
		Refresh	✅	❌	❌	❌	❌	✅	
		Delete	✅	❌	❌	❌	❌	✅	
Patch		Read	✅	✅	⭐	❌	❌	❌	
		Create	✅	❌	⭐⭐	❌	❌	❌	
		Refresh	✅	❌	⭐⭐	❌	❌	❌	
		Delete	✅	❌	⭐⭐	❌	❌	❌	
Analyzer	Installed apps	Read	✅	✅	✅	❌	❌	✅	
		Refresh	✅	❌	✅	❌	❌	✅	
	Licenses	Read	✅	✅	❌	❌	❌	✅	
		Create	✅	❌	❌	❌	❌	✅	
		Refresh	✅	❌	❌	❌	❌	✅	
		Delete	✅	❌	❌	❌	❌	✅	
	SAM	Read	✅	✅	❌	❌	❌	✅	
Microservices		Create	✅	❌	❌	❌	❌	✅	
		Read	✅	✅	✅	❌	❌	✅	

Copyright © 2024 Flexxible. Todos los derechos reservados.

Section	Functionality	Action	1	2	3	4	5	6	
		Refresh	✅	❌	❌	❌	❌	✅	
	Enabled	Read	✅	✅	✅	❌	❌	✅	
		Refresh	✅	❌	❌	❌	❌	✅	
Billing		Read	✅	✅	❌	❌	❌	❌	
		Refresh	✅	❌	❌	❌	❌	❌	
Product		Read	✅	✅	❌	❌	❌	❌	
	Report	Read	✅	✅	✅	❌	❌	❌	
	Environment	Read	✅	✅	✅	❌	❌	❌	
		Refresh	✅	❌	❌	❌	❌	❌	
	Baseline	Read	✅	✅	✅	❌	❌	❌	
	FlexxAgent Configuration	Read	✅	✅	❌	❌	❌	❌	
		Refresh	✅	❌	❌	❌	❌	❌	
Integrations		Create	✅	❌	❌	❌	❌	❌	
		Read	✅	✅	❌	❌	❌	❌	
		Refresh	✅	❌	❌	❌	❌	❌	
Modules		Create	✅	❌	❌	❌	❌	❌	

Copyright © 2024 Flexxible. Todos los derechos reservados.

Section	Functionality	Action	1	2	3	4	5	6	
		Read	✅	✅	❌	❌	❌	❌	
		Refresh	✅	❌	❌	❌	❌	❌	
Information		Read	✅	✅	✅	❌	❌	✅	
		Refresh	✅	❌	❌	❌	❌	❌	
Directives		Create	✅	❌	❌	❌	❌	❌	
		Read	✅	✅	✅	❌	❌	❌	
		Refresh	✅	❌	❌	❌	❌	❌	
		Delete	✅	❌	❌	❌	❌	❌	
Reporting Groups		Create	✅	❌	❌	❌	❌	❌	
		Read	✅	✅	❌	❌	❌	❌	
		Refresh	✅	❌	❌	❌	❌	❌	
		Delete	✅	❌	❌	❌	❌	❌	
	FlexxAgent Configuration	Read	✅	✅	❌	❌	❌	❌	
		Refresh	✅	❌	❌	❌	❌	❌	
	Automatic Update	Refresh	✅	❌	❌	❌	❌	❌	

Copyright © 2024 Flexxible. Todos los derechos reservados.

Section	Functionality	Action	1	2	3	4	5	6	
	FlexxAgent Versions	Read	✅	✅	❌	❌	❌	❌	
		Refresh	✅	❌	❌	❌	❌	❌	
	Magic link	Create	✅	❌	❌	❌	❌	❌	
		Read	✅	✅	❌	❌	❌	❌	
		Refresh	✅	❌	❌	❌	❌	❌	
Roles		Create	✅	❌	❌	❌	❌	❌	
		Read	✅	✅	❌	❌	❌	✅	
		Refresh	✅	❌	❌	❌	❌	❌	
		Delete	✅	❌	❌	❌	❌	❌	
Users		Create	✅	❌	❌	❌	❌	❌	
		Read	✅	✅	❌	❌	❌	✅	
		Refresh	✅	❌	❌	❌	❌	❌	
		Delete	✅	❌	❌	❌	❌	❌	

Copyright © 2024 Flexxible. Todos los derechos reservados.

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	✅	❌	💡	❌	❌	✅	❌	✅	❌	❌

Copyright © 2024 Flexxible. Todos los derechos reservados.

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

Copyright © 2024 Flexxible. Todos los derechos reservados.

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	✅	✅	✅	✅
Job	View	✅	✅	✅	✅
Job	Cancel	✅	❌	✅	❌
Alert	View	✅	✅	✅	✅
Alert	Off	✅	❌	✅	❌
Profile Storage	View	✅	✅	✅	✅
Profile Storage	Modify	✅	❌	✅	❌
Profile Storage	Delete	✅	❌	✅	❌
Alert notification profiles	View	❌	❌	✅	✅
Alert notification profiles	Modify	❌	❌	✅	❌
Alert notification profiles	Delete	❌	❌	✅	❌

Copyright © 2024 Flexxible. Todos los derechos reservados.

Functionality	Action	L1	L1 RO	L2	L2 RO
Alert Subscriptions	View	✗	✗	✓	✓
Alert Subscriptions	Modify	✗	✗	✓	✗
Alert Subscriptions	Delete	✗	✗	✓	✗
Event Logs	View	✗	✗	✓	✓
Event Logs	Modify	✗	✗	✓	✗
Event Logs	Delete	✗	✗	✓	✗
Locations	View	✗	✗	✓	✓
Locations	Create	✗	✗	✓	✗
Locations	Modify	✗	✗	✓	✗
Networks	View	✗	✗	✓	✓
Networks	Modify	✗	✗	✓	✗
Notifications	View	✗	✗	✓	✓
Notifications	Create	✗	✗	✓	✗
Notifications	Modify	✗	✗	✓	✗
Notifications	Delete	✗	✗	✓	✗
Reporting Groups	View	✗	✗	✓	✓
Servers	View	✗	✗	✓	✓

Copyright © 2024 Flexxible. Todos los derechos reservados.

Functionality	Action	L1	L1 RO	L2	L2 RO
Servers	Execute operations	❌	❌	✅	❌
Wireless networks	View	❌	❌	✅	✅
Wireless networks	Modify	❌	❌	✅	❌

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.

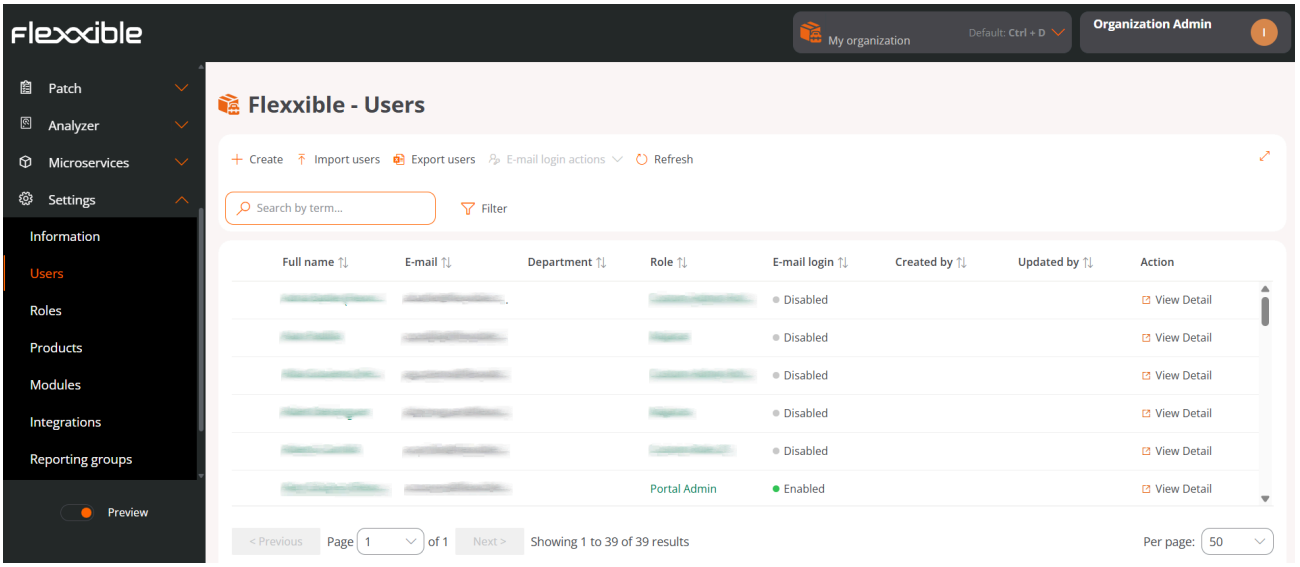
Copyright © 2024 Flexxible. Todos los derechos reservados.

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:

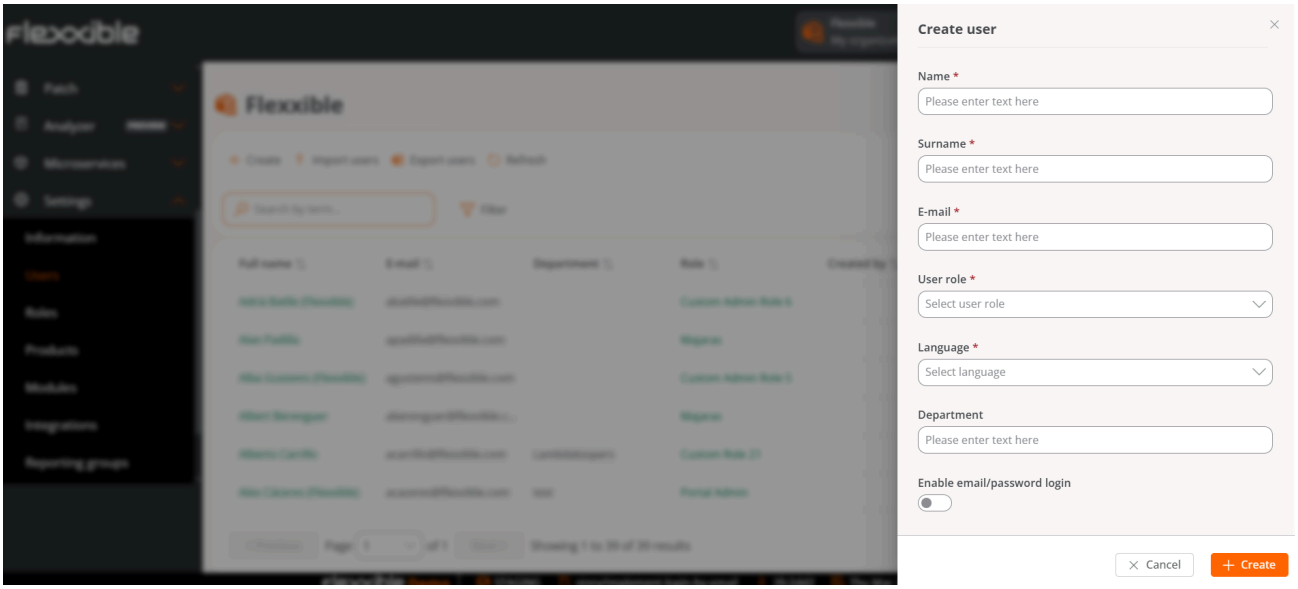
- **Full name.** User's first and last name.
- **Email address.** User's email address.
- **Department.** Department to which the user belongs within their organization.
- **Role.** Role type assigned to the user.
- **Email login.** Indicates if the user has *Enabled* or *Disabled* email and password 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

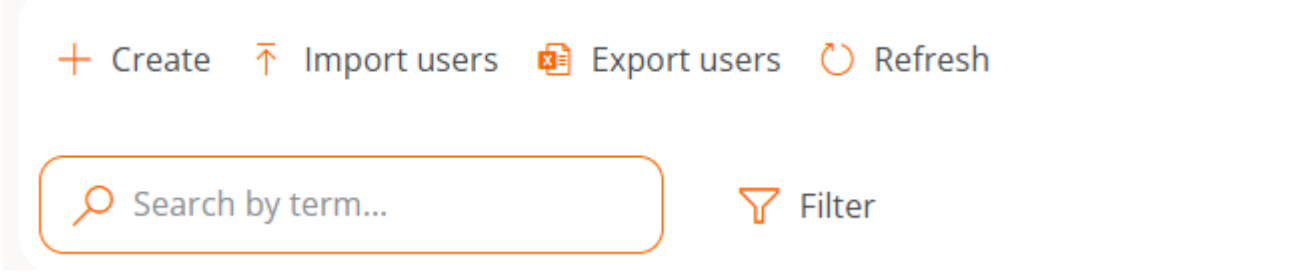
Copyright © 2024 Flexxible. Todos los derechos reservados.

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

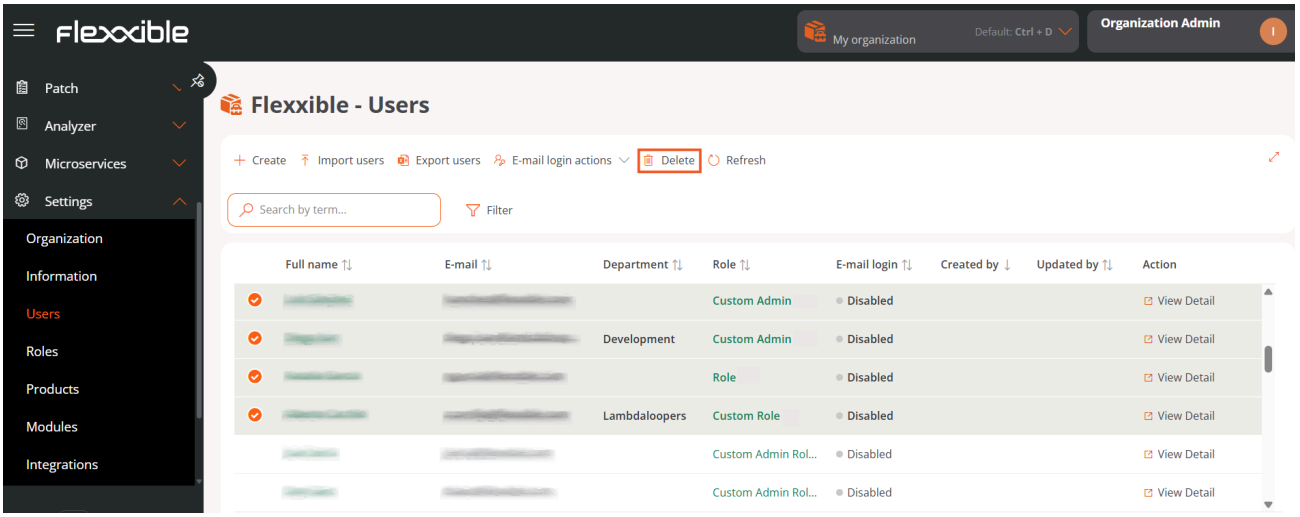
Delete users

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`.

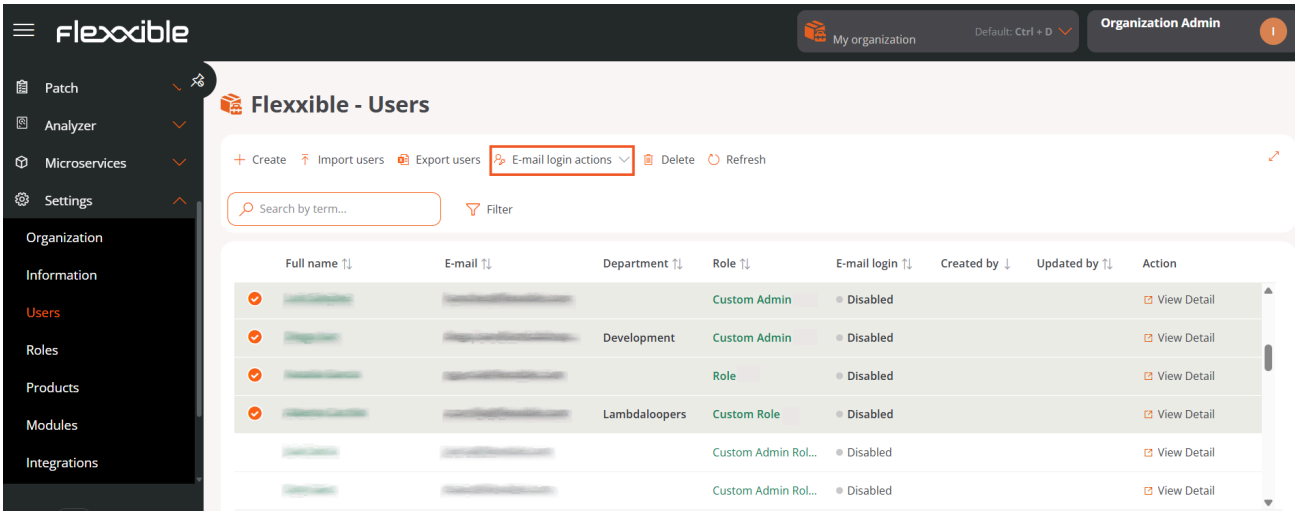


Email login actions

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.



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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

Portal / Settings / Integrations

From this section, it is possible to register the integration of Portal with services available to organizations on external platforms, to facilitate the management of tasks on devices, visualize unified information, or perform actions.

Integration with Entra ID

Portal's integration with Entra ID allows treating an organization's devices as another group in `Workspaces`; in this way, in addition to the dynamic and static `Workspaces Groups` that an organization could have, Entra ID Workspaces Groups would be generated.

The integration does not imply that those groups will exist in `Portal`, but at the moment when an action is desired on them in `Workspaces`, Portal will show the list of devices that comprise them to make a decision.

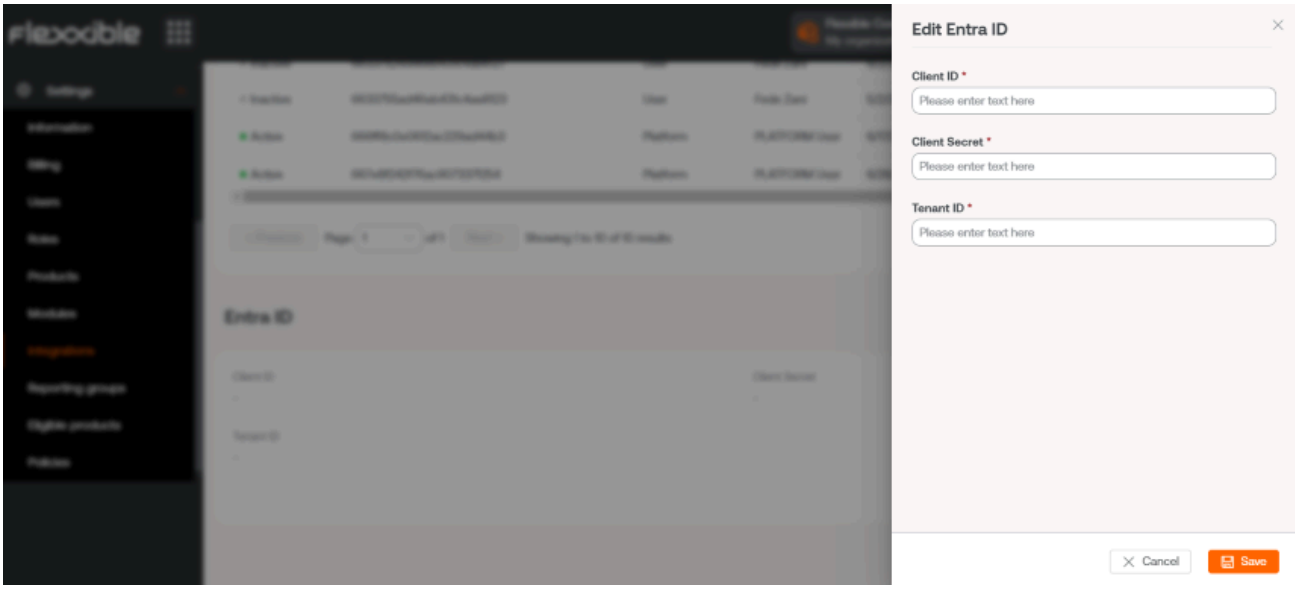
Enable integration with Entra ID

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.



> **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 of Flexxible Odin with Intel vPro® Enterprise will allow you to perform useful additional manageability operations on the physical Windows workspaces that provide support to Intel AMT® technology.

From the `Workspaces` view in `Portal`, you can check information about the hardware and status of devices, and additional operations including out-of-band actions will be made available.

Requirements

To benefit from the Intel vPro® Enterprise integration, devices must meet the following requirements:

Supported operating systems

Copyright © 2024 Flexxible. Todos los derechos reservados.

Devices must have Windows 10 and Windows 11, 64-bit, installed.

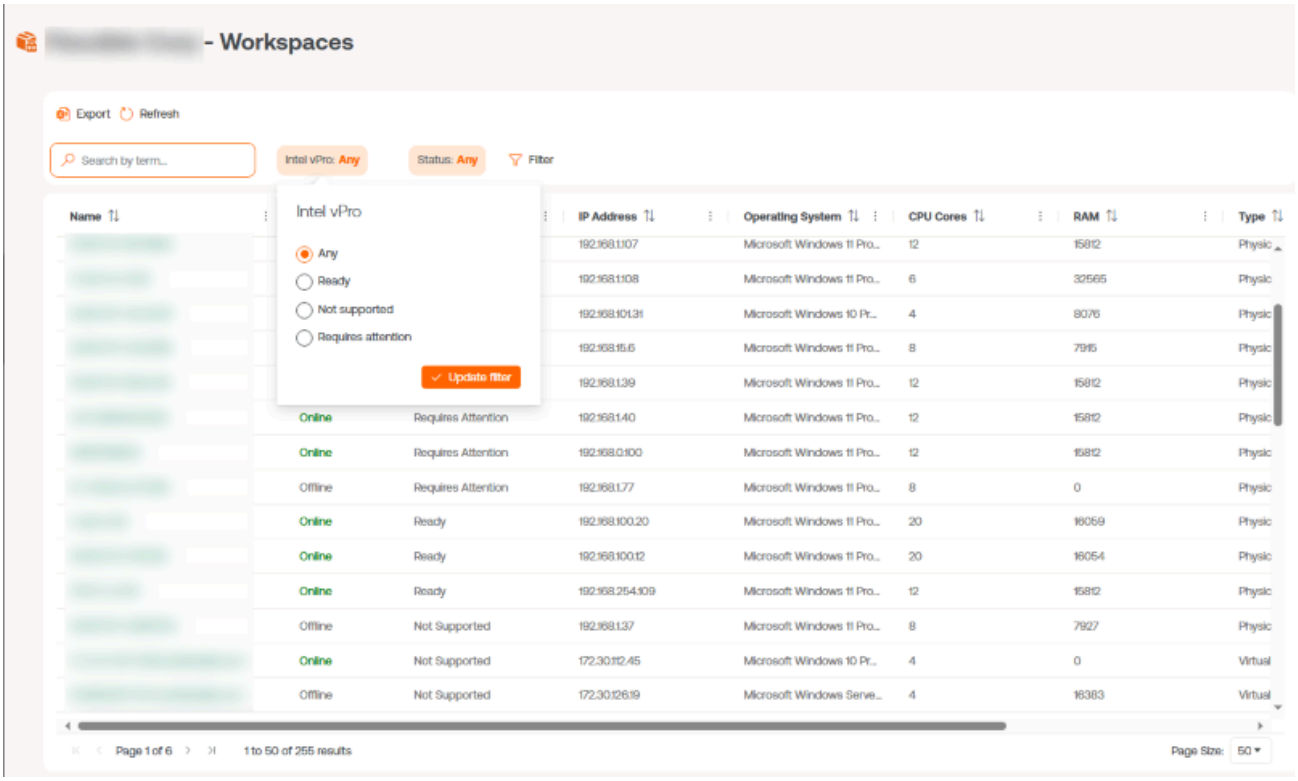
Compatibility with Intel® AMT

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.



Copyright © 2024 Flexxible. Todos los derechos reservados.

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:

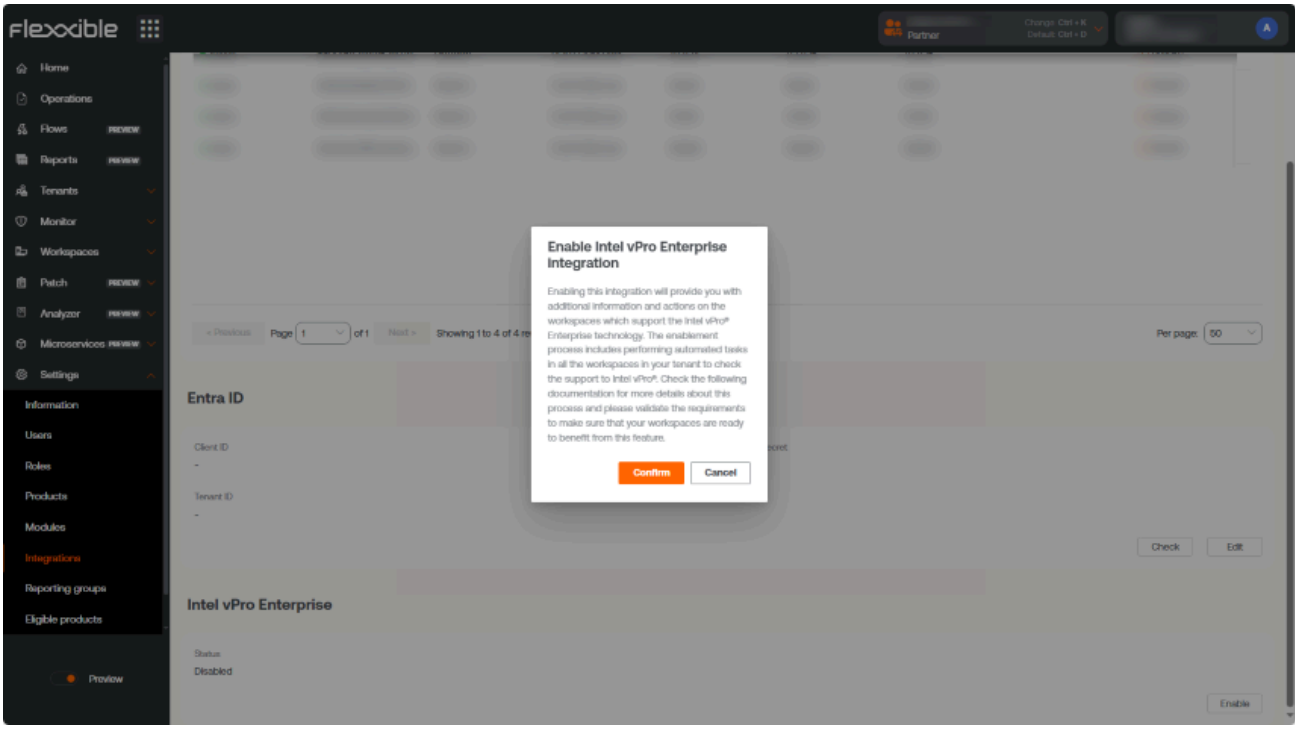
1. That the hostname of the Flexxible Intel EMA server, *iagent.flexxible.com*, can be resolved to an IP address from all devices planned to be included in the integration.
2. Make sure the server is accessible from the device through port 443.
3. That traffic between the device and the server is allowed by the proxy server, if applicable.

Enable integration with Intel vPro® Enterprise

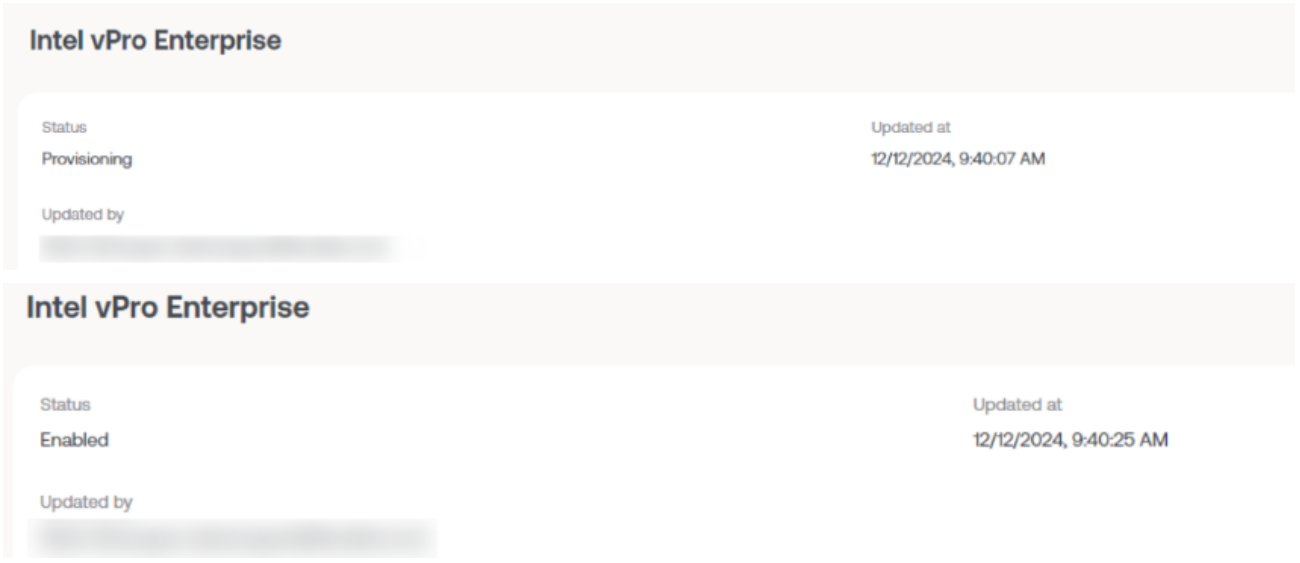
This action can only be performed by users with *Organization Administrator* permission in `Portal`.

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`.

Copyright © 2024 Flexxible. Todos los derechos reservados.



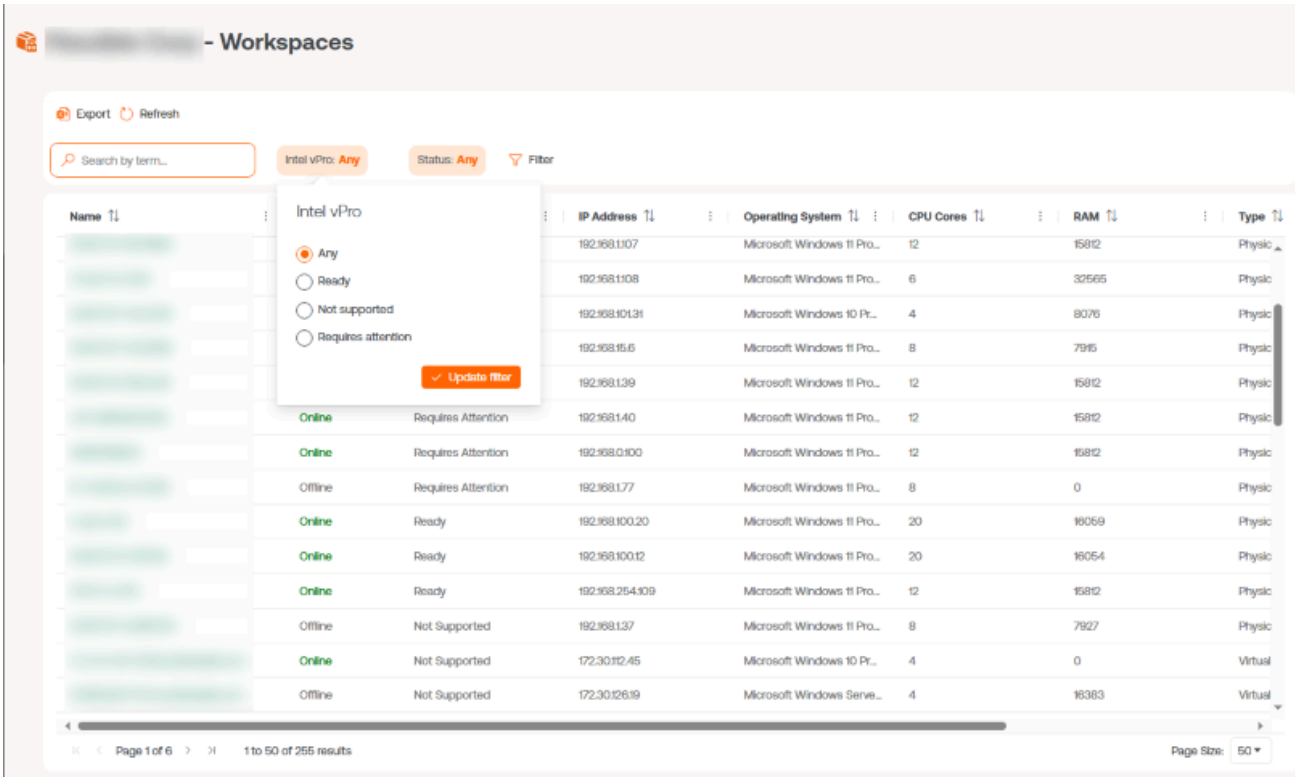
The integration process may take a few minutes to provision and configure the tenant. Once completed, the status will appear as "Enabled" along with related information.



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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

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.

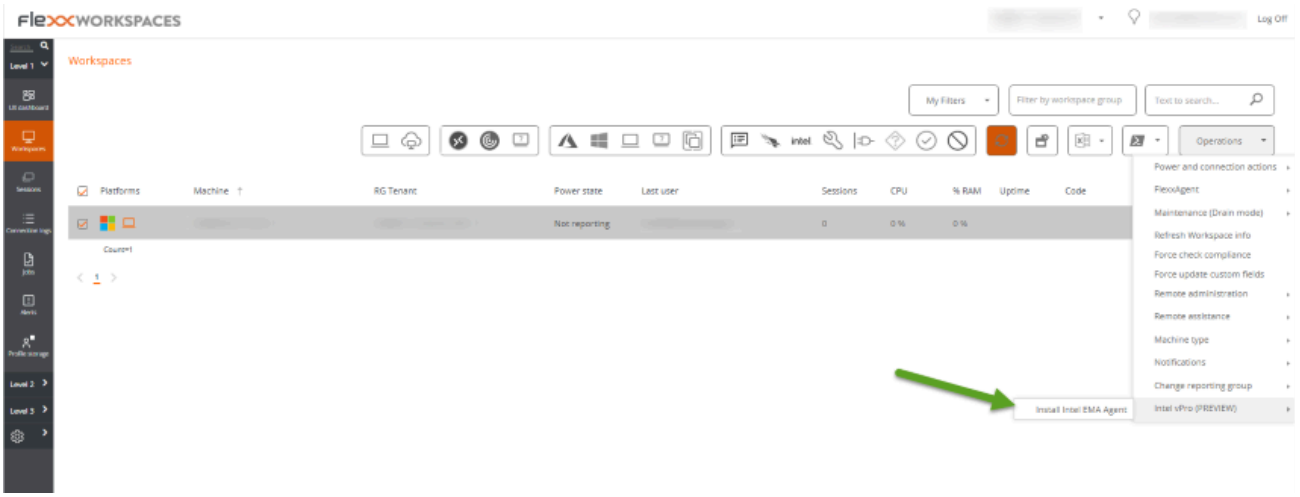


Install Intel EMA Agent on devices that indicate support for Intel® AMT (in the `Intel vPro Enterprise` column of Workspaces, they are labeled as `Requires attention`).

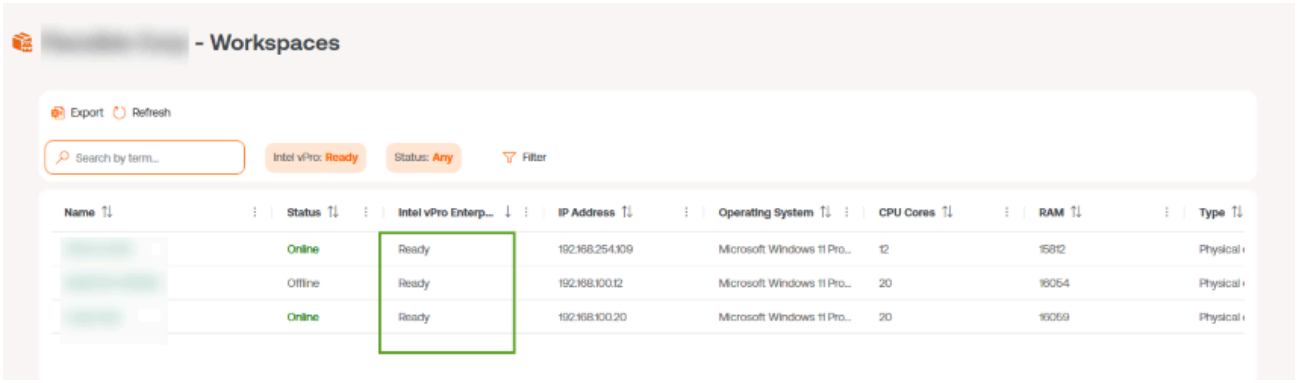
Install Intel EMA Agent

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.



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)

CrowdStrike integration

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

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*.

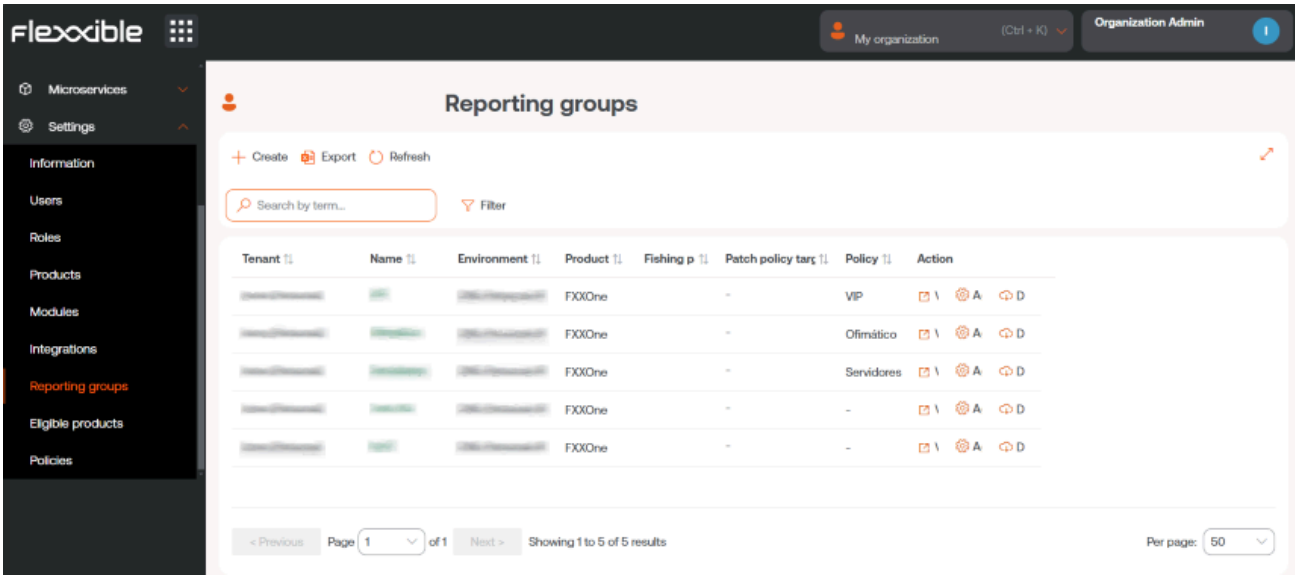
4. Click on `Save`.

> **TIP**
>
> For more information about this feature, please refer to the guide Set up integration with CrowdStrike.

Copyright © 2024 Flexxible. Todos los derechos reservados.

Portal / Settings / Reporting Groups

From `Reporting groups` you can create and preconfigure groups within the same organization using different criteria to meet the needs of departments, offices or user groups that make them up.



It's also possible to see which users and roles have access to the reporting group, as well as activate remote assistance features.

Reporting groups creation

To create a reporting group, press the `New` button and fill in the following fields:

- **Tenant.** This is a dropdown menu to select the tenant where the new reporting group will be created.
- **Name.** Name that the reporting group will have.
- **Environment.** Opens a dropdown to select the environment in which the reporting group will be.
- **Patch Policy Target.** Opens a dropdown to select which patch policy the reporting group will be subjected to.
- **Fishing Pattern.** This is an optional field. Allows indicating the regular expression (RegEx) that will be used to add devices to the reporting group. For example: `company`

Copyright © 2024 Flexxible. Todos los derechos reservados.

(includes all devices whose names contain the word "company") or `.*2023$` (includes devices whose names end in "2023").

Once the reporting group has been created, it will appear in the table of the list view.

The `Reload` button is very helpful if you want to refresh the list to ensure the reporting group has been created.

Fishing pattern

The fishing pattern allows automatically grouping in a reporting group the devices that share a regular expression (RegEx) in the name.

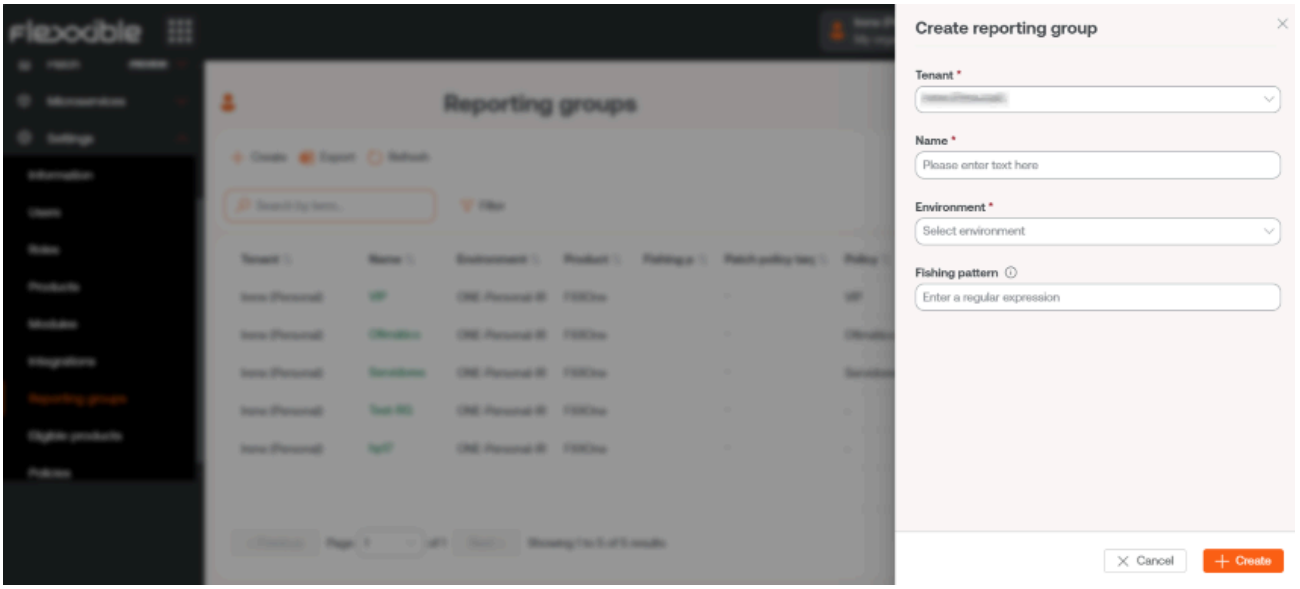
The devices that form the reporting group will be updated every hour. It is an automatic process that checks if there are new devices matching the configured RegEx. If there are, the devices will be moved to the corresponding reporting group.

> **INFO**
>
> The regular expression (RegEx) should have a maximum of 250 characters.

It's important to pay attention to all active RegEx to avoid conflicts between reporting groups, because it can happen that when creating a new one, its RegEx matches an existing one.

You can verify which reporting group a device belongs to from the Reporting Groups section, in the Workspaces module. And the history of a reporting group can be queried from the device detail view, in the same module.

Copyright © 2024 Flexxible. Todos los derechos reservados.



From `Reporting group history`, you can query the reporting groups a device has been through.

Reporting groups list

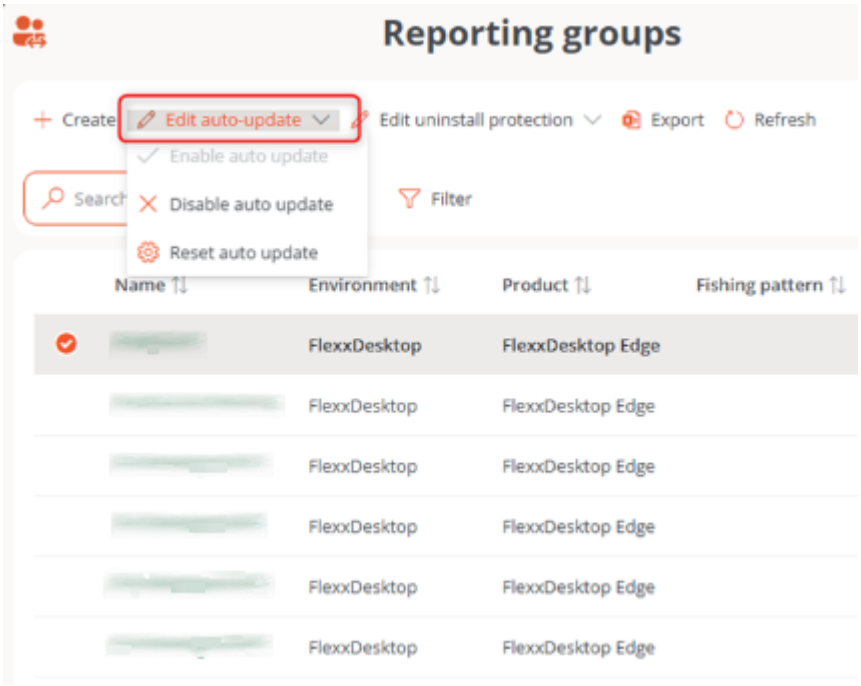
The list view shows a table whose fields match the data requested to create the reporting group. It also has the `Action` field, which allows access to `View details` and `Agent configuration`.

Auto update of FlexxAgent

From the `Edit auto update` button, located at the top of the table, you can *Enable*, *Disable*, or *Reset* the update of FlexxAgent on devices.

Regarding the FlexxAgent Version settings, the automatic update will always target the *Production* environment, not the *Early* one.

Copyright © 2024 Flexxible. Todos los derechos reservados.



View details

The detail view allows consulting three types of information about the selected reporting group:

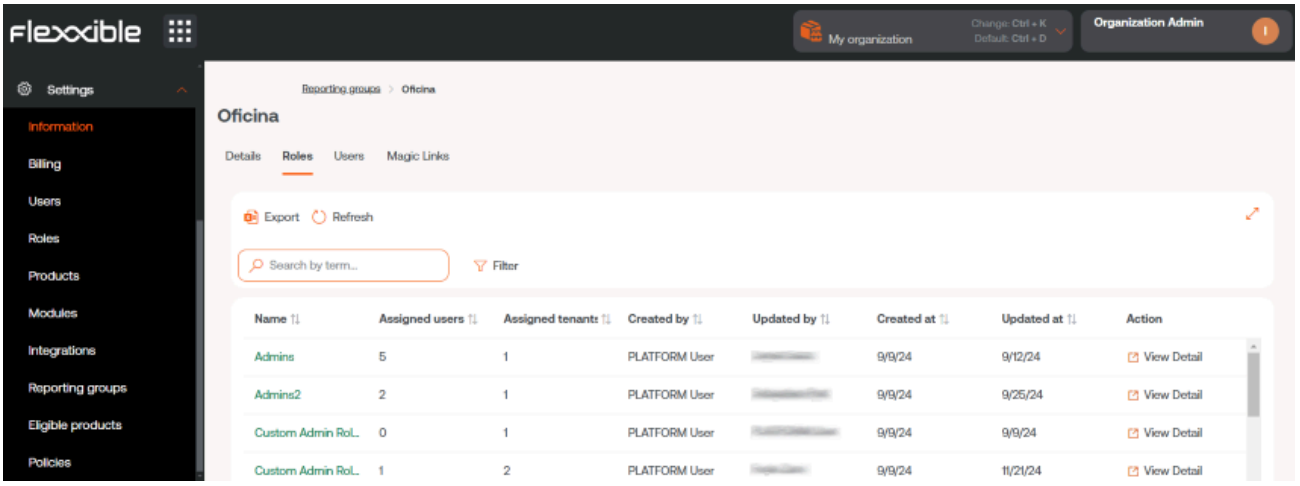
Details

This tab offers general information about the reporting group being consulted. The `Edit` button opens a form that allows you to change the initial characteristics of the group, such as the name or the patch directive destination.

Roles

This tab shows a table with the list of roles that can access the reporting group being consulted. In turn, this table also has the `Action` field -> `View details`, which allows you to consult more specific information about the roles: details, permissions and users.

Copyright © 2024 Flexxible. Todos los derechos reservados.



- **Details.** General information about the role. At the bottom right, the `Edit` button allows you to change the name of the role.
- **Permissions.** Through a table, it shows the permissions that role has in the Portal, Workspaces, and Analyzer modules.
- **Users.** Through a table, it shows a list of users assigned to that role.

> More information about roles, users and permissions in `Roles`.

Users

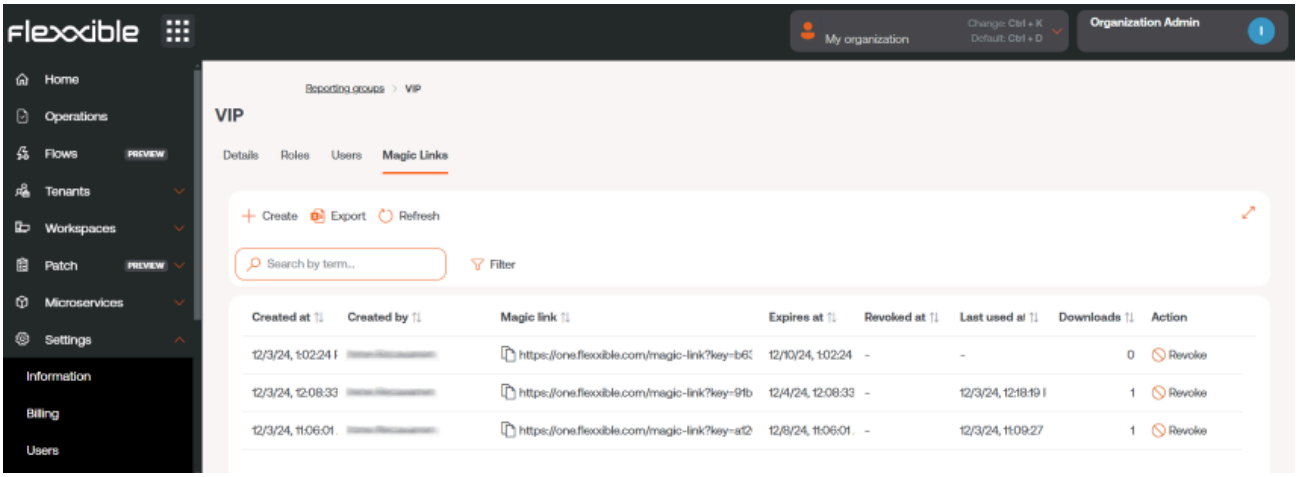
This tab shows the name and associated email of the users who make up the reporting group being consulted.

Magic link

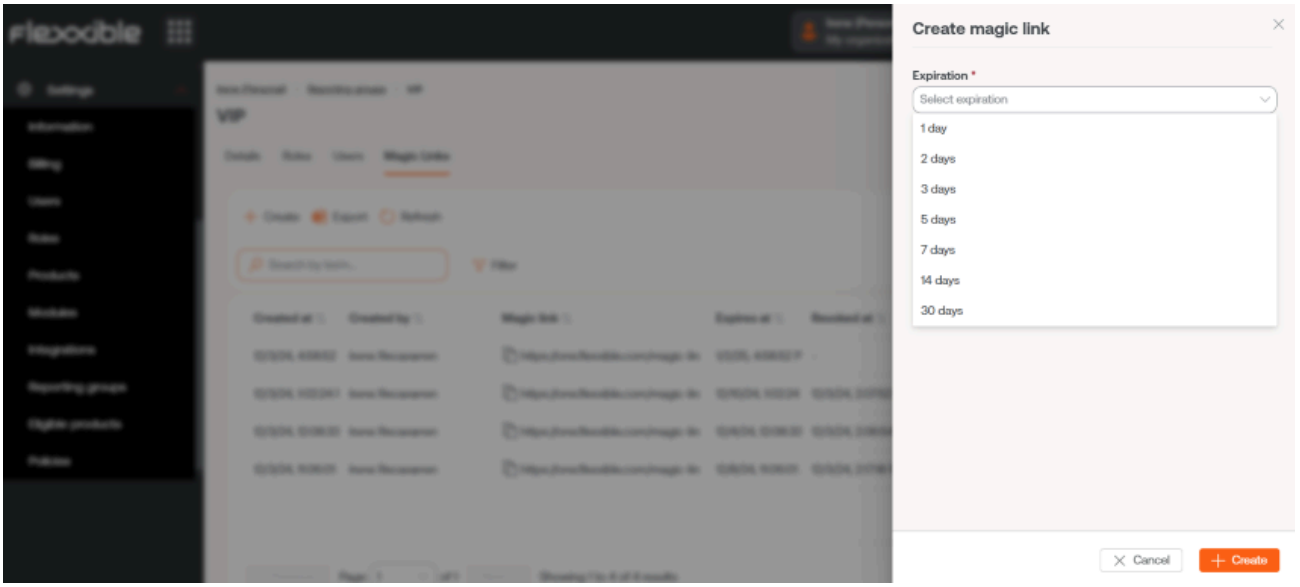
Users with the `Organization Administrator` role within a partner-type organization can generate and send `Magic links` to users so they can download FlexxAgent on their devices without being logged in.

This tab shows a table listing the magic links created in the reporting group being queried, both from the `Generate magic link` button on the Portal Home page and from this same tab.

Copyright © 2024 Flexxible. Todos los derechos reservados.



The `Create` button allows you to generate magic links in the reporting group to optimize access to downloading FlexxAgent on devices, by defining their expiry time in advance.



`Export` allows exporting the list in .xlsx format and `Refresh` updates the list of magic links displayed in the table.

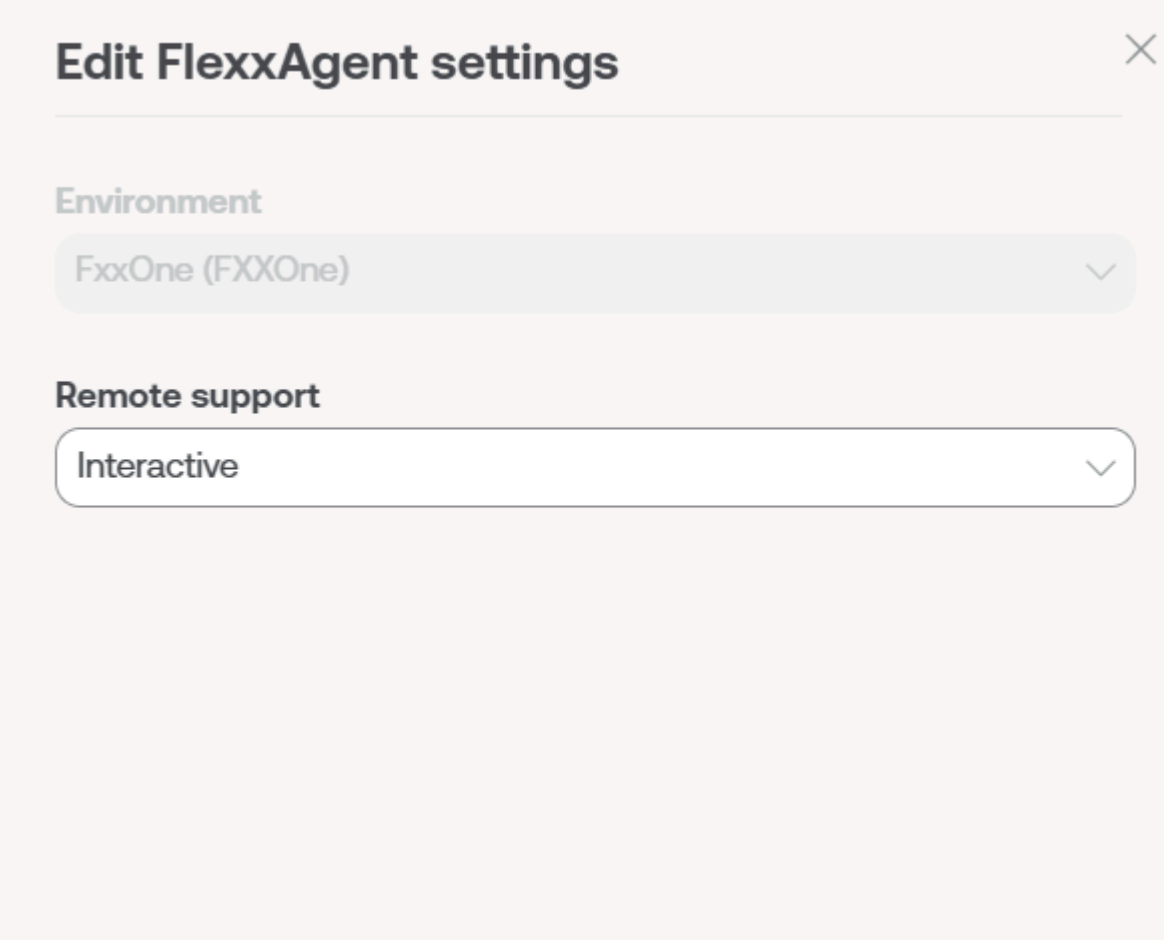
The table provides information about specific data of the created Magic link, such as the author, creation, and expiration dates; it also shows if it has been revoked and when. From here it is also possible to copy the generated magic link to share it and revoke it when deemed convenient.

> More information about `Magic links`

Copyright © 2024 Flexxible. Todos los derechos reservados.

FlexxAgent configuration (Remote Assistance)

From here, a user with the *Organization Administrator* access level in Portal can configure the type of remote support the report group will have: interactive, unattended, dynamic, or none.



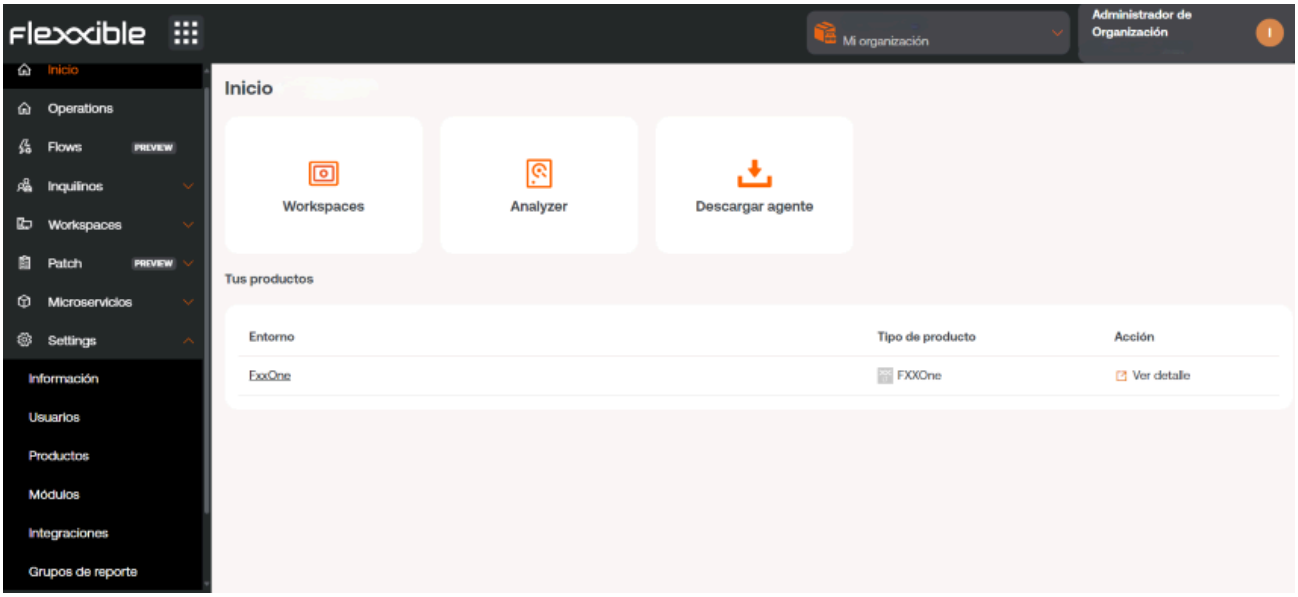
This configuration is set from Products. However, specific configurations can be made for report groups.

Download FlexxAgent

In FXXOne it is possible to download FlexxAgent from the reporting groups. Simply click on `Download agent` to perform this action and then follow the installation steps.

Copyright © 2024 Flexxible. Todos los derechos reservados.

This action can also be performed from the Portal home page.



> **INFO**
>
> Some of the FlexxAgent configuration options are not visible to users with the *Organization Administrator* role.

Copyright © 2024 Flexxible. Todos los derechos reservados.

Portal / Settings / FlexxAgent Versions

As FlexxAgent versions evolve and incorporate new functionalities, organizations need to control which version of FlexxAgent will be installed on their devices.

In this regard, the *FlexxAgent Versions* functionality allows users with the *Organization Administrators* role to choose the FlexxAgent version to be used in each of the report groups created in the organization's environment.

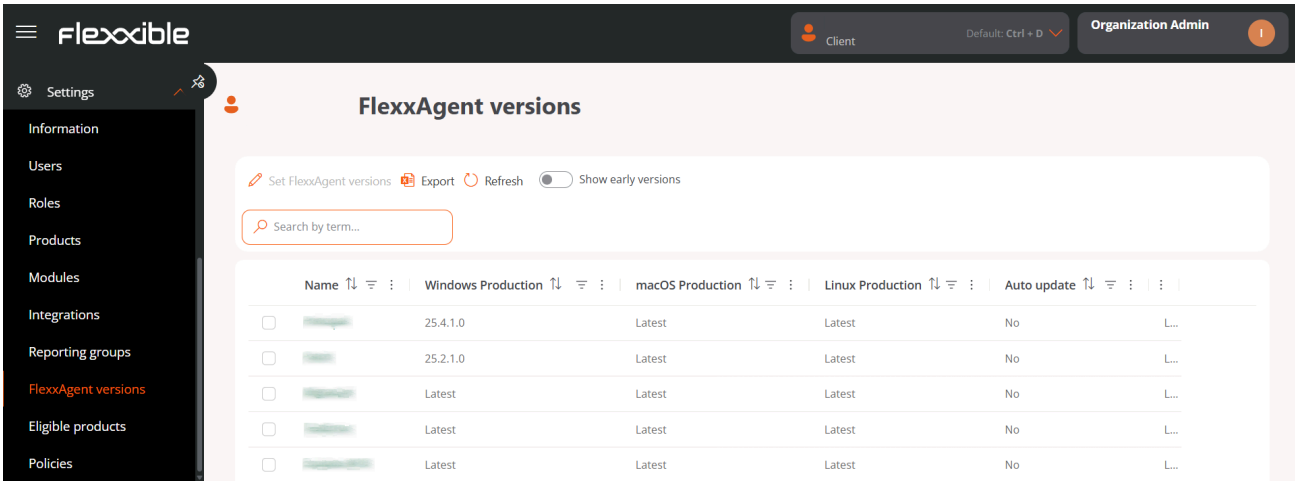
> **INFO**
>
> To access this feature, please consult with your contact at Flexxible.

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. Access `Portal` -> `Configuration` -> `FlexxAgent Versions`.



The table will display the list of reporting groups in the organization with the following information:

Copyright © 2024 Flexxible. Todos los derechos reservados.

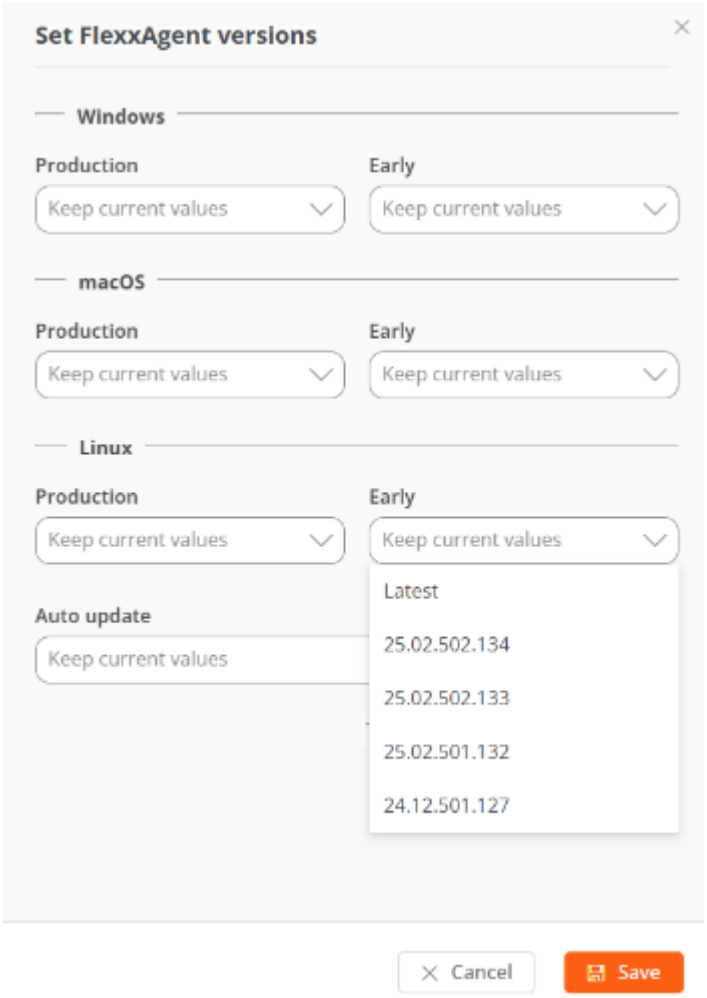
- **Name.** Name of the report group.
- **Windows Production.** Version number set for *Production* on Windows.
- **macOS Production.** Version number set for *Production* on macOS.
- **Linux Production.** Version number set for *Production* on Linux.
- **Automatic Update.** Defined from the report group 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.

Copyright © 2024 Flexxible. Todos los derechos reservados.



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.

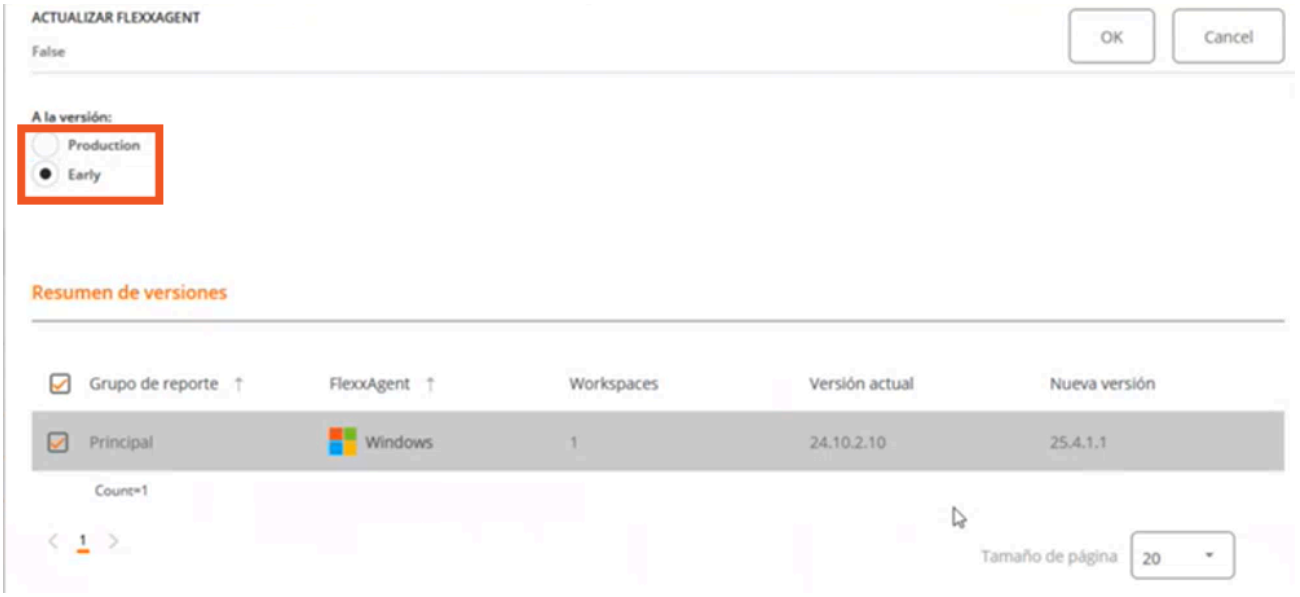
Management from Workspaces

Copyright © 2024 Flexxible. Todos los derechos reservados.

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*.



Copyright © 2024 Flexxible. Todos los derechos reservados.

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 general view of Directives in Portal, you can access a list and description of the created directives. 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.

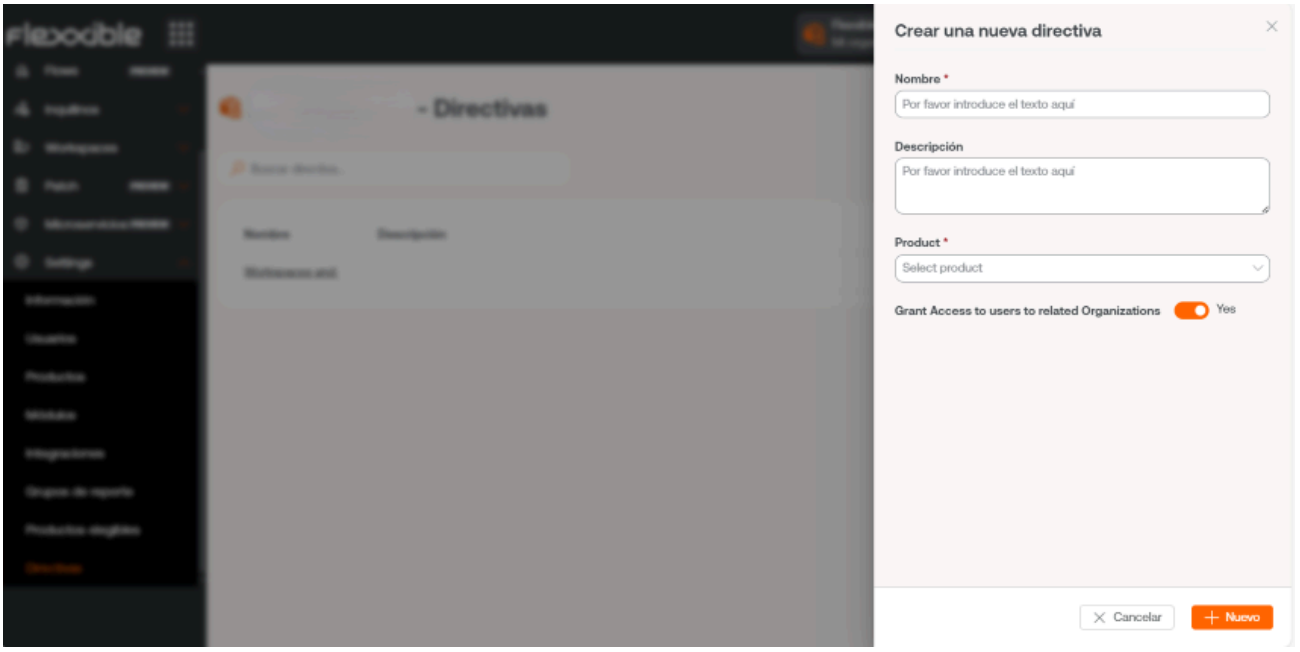
Each time a new organization is registered, the report groups that are defined in the directive will be created. At the same time, from the directive itself, it can be determined whether partner-type users will have access to manage an organization in Portal or not.

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.

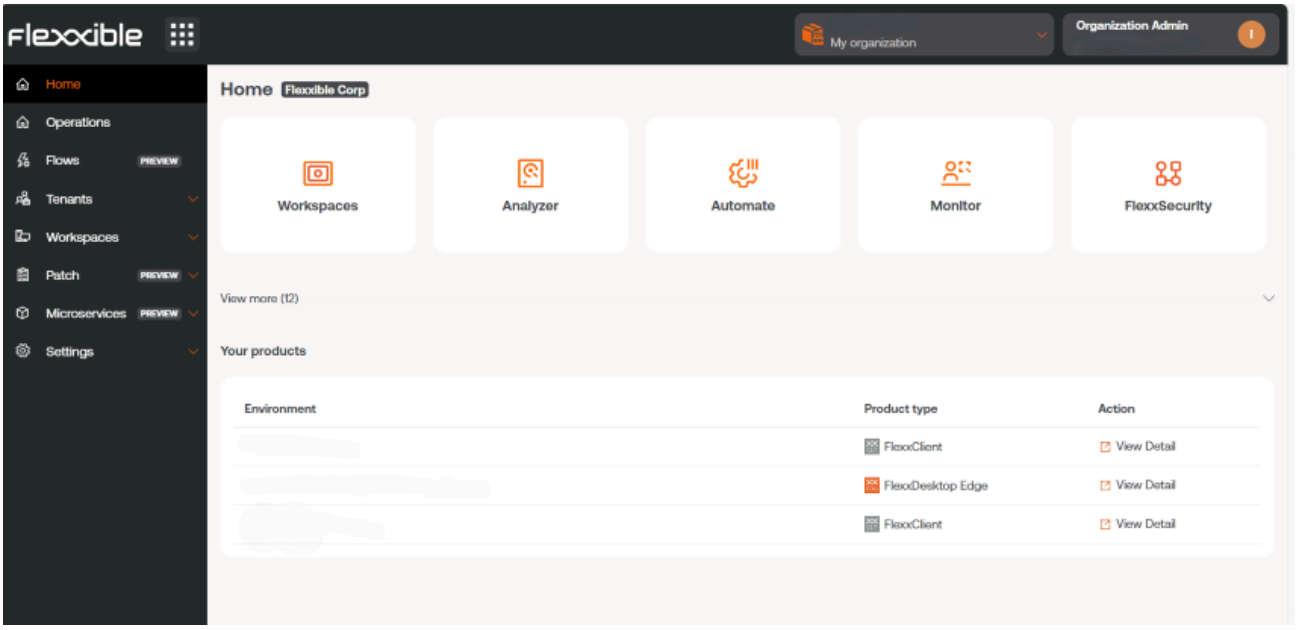
You can also assign a directive to an organization from Tenants.

Copyright © 2024 Flexxible. Todos los derechos reservados.



Copyright © 2024 Flexxible. Todos los derechos reservados.

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

Portal / Guides / Create and manage workspace groups

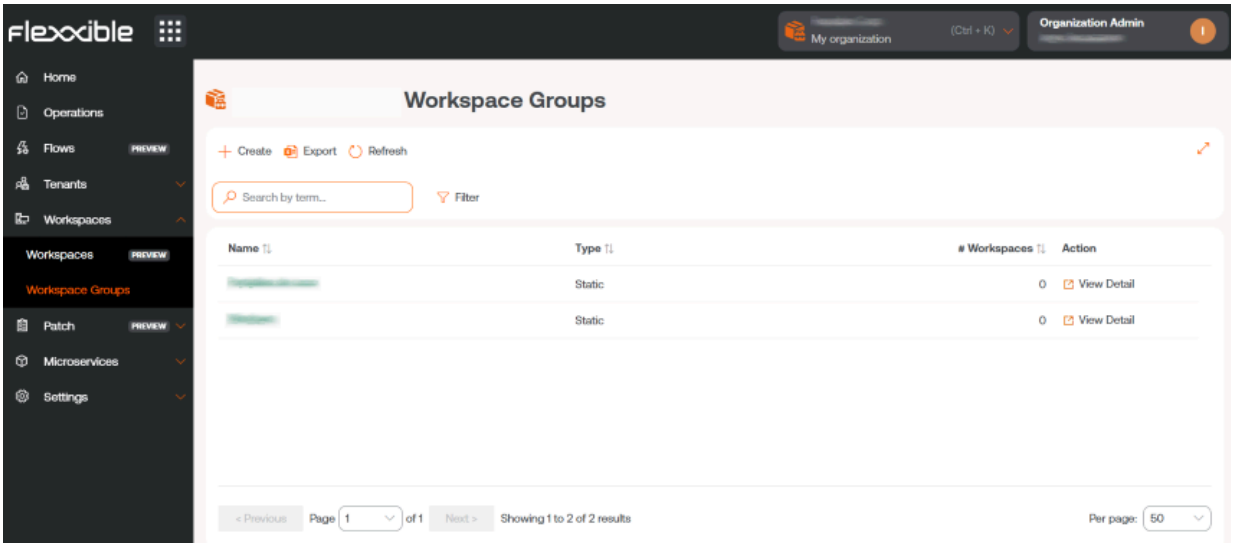
Workspace groups are logical groupings of a set of devices (or endpoints) that can be used when managing an organization. They can be static, dynamic, and Entra ID type.

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.

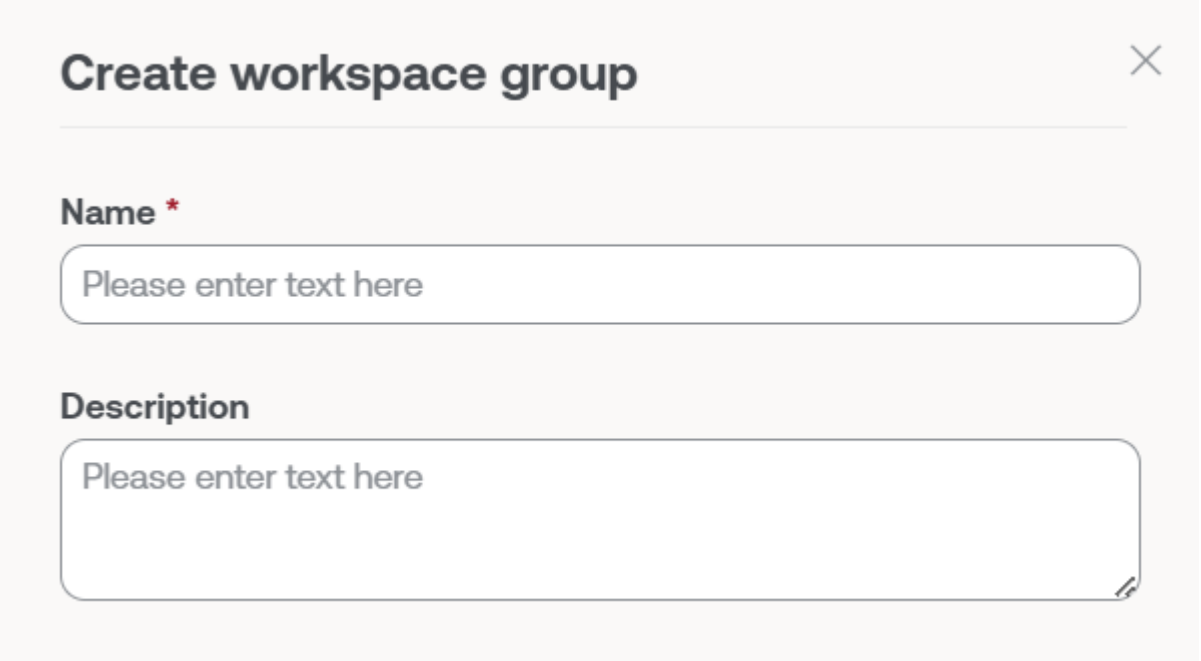
Create a static workspace group from the Portal

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).



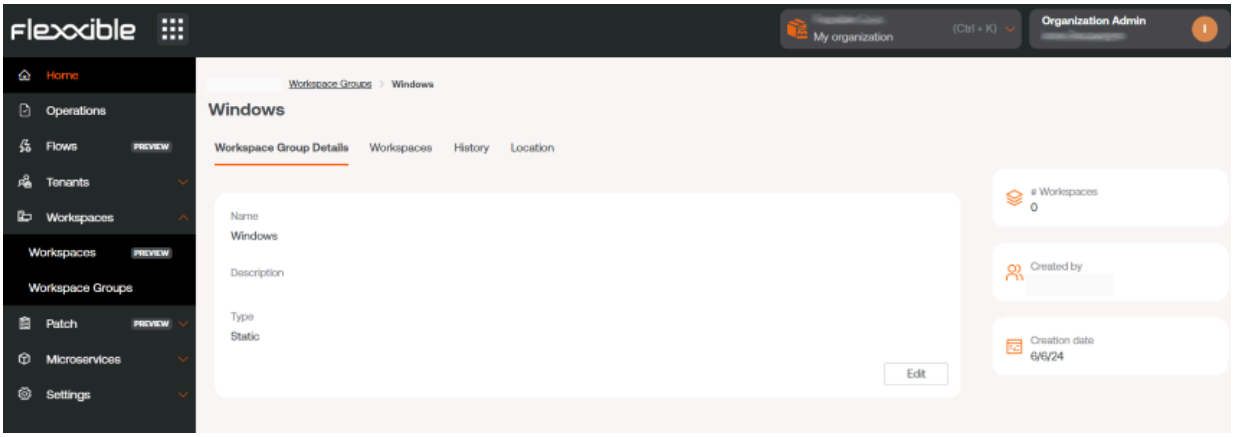
2. Click on the `+ New` button at the top of the list. A modal window will appear on the right side of the screen. Enter the group name and its description (optional). Click the `+ New` button at the bottom of the window.

Copyright © 2024 Flexxible. Todos los derechos reservados.



3. A confirmation message of the group's creation will appear. Close the window using the cross at the top right.

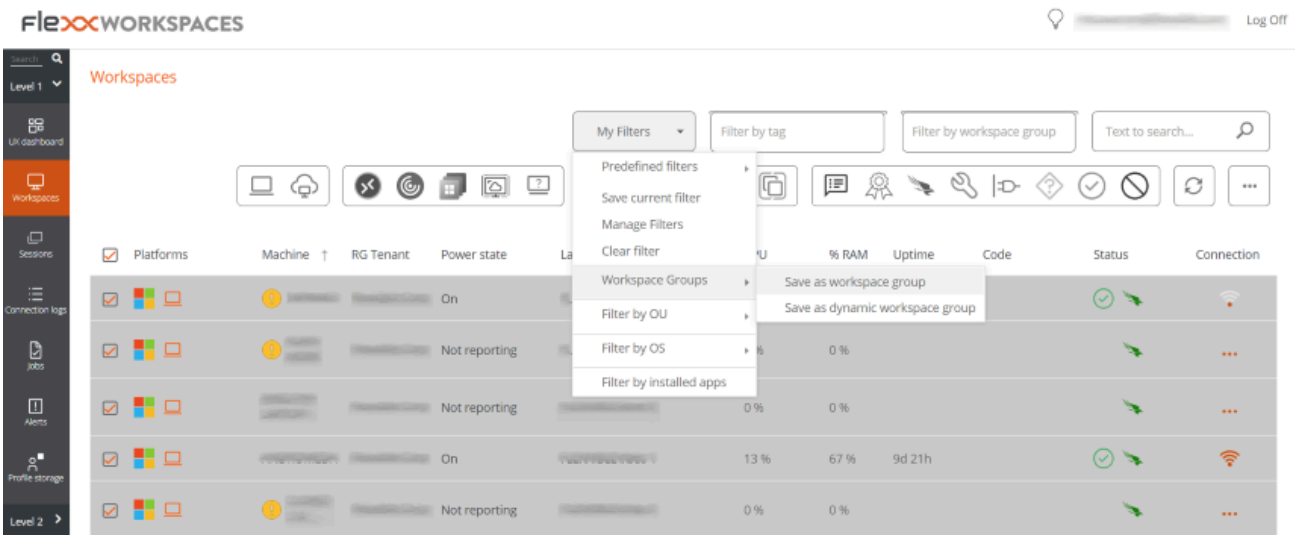
4. The new group will appear in the list of workspace groups. Click on its name to access the details.



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`.

Copyright © 2024 Flexxible. Todos los derechos reservados.



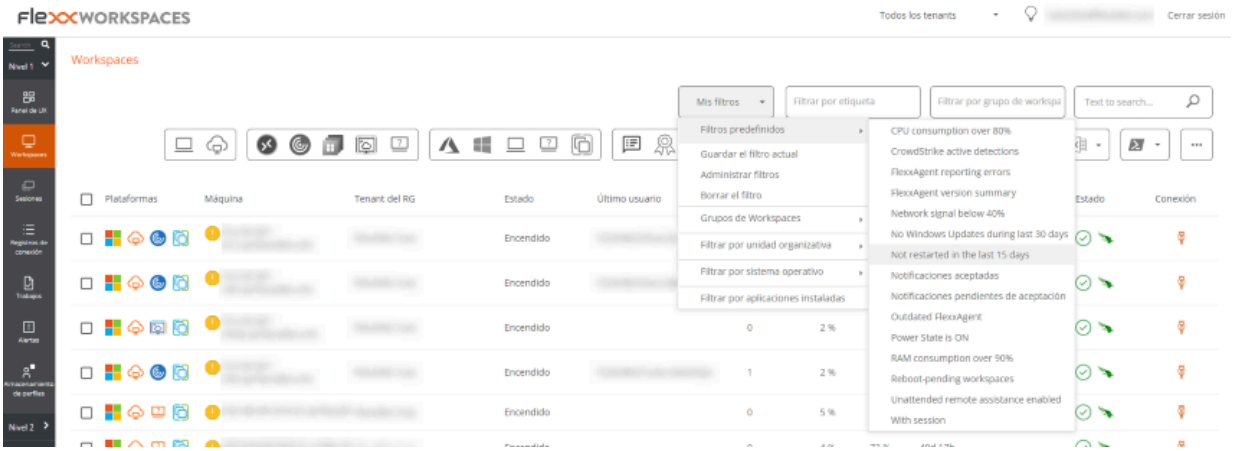
Dynamic workspace groups

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

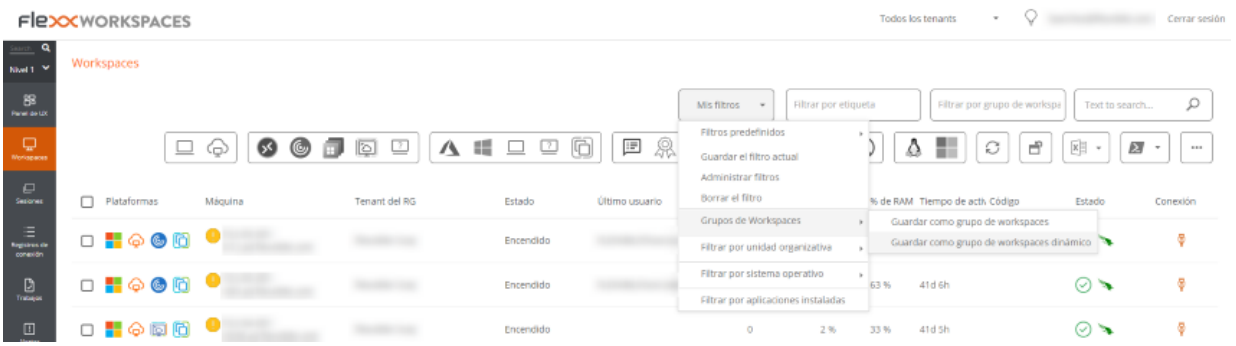
Dynamic groups are created from the `Workspaces` view, within the Workspaces module.

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.



Copyright © 2024 Flexxible. Todos los derechos reservados.

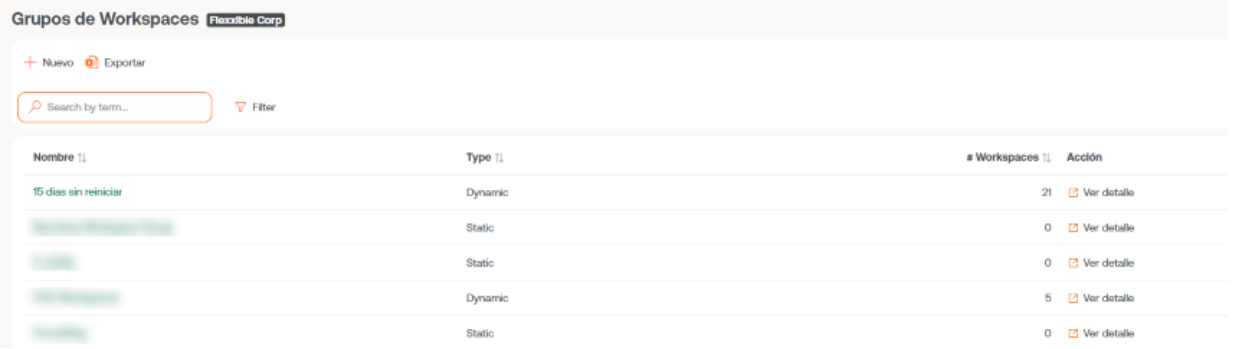
2. Once inside the filter results, use the `My Filters` -> `Workspace Groups` -> `Save as Dynamic Workspace Group` option.



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

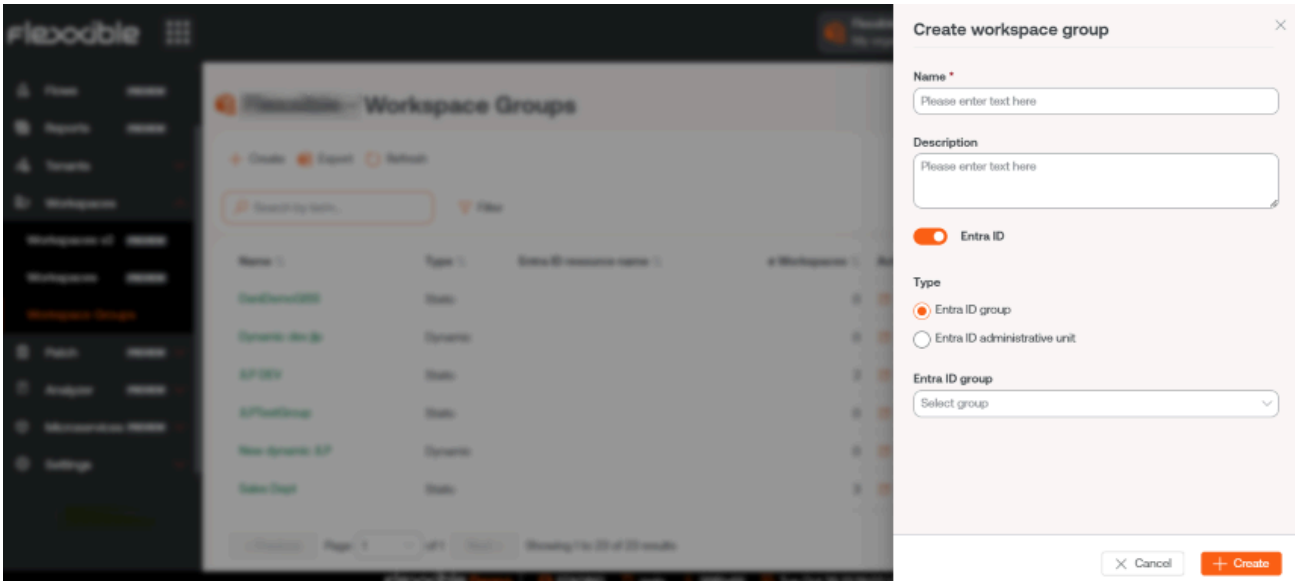
It is a group that can pull members from an existing group or organizational unit in the Entra ID domain in use. Creating this type of group requires at least one active integration with the Entra ID domain under `Settings` -> `Integrations` in Portal.

Create a Workspace group Enter ID

Entra ID groups are created from Portal.

Copyright © 2024 Flexxible. Todos los derechos reservados.

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

- **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.

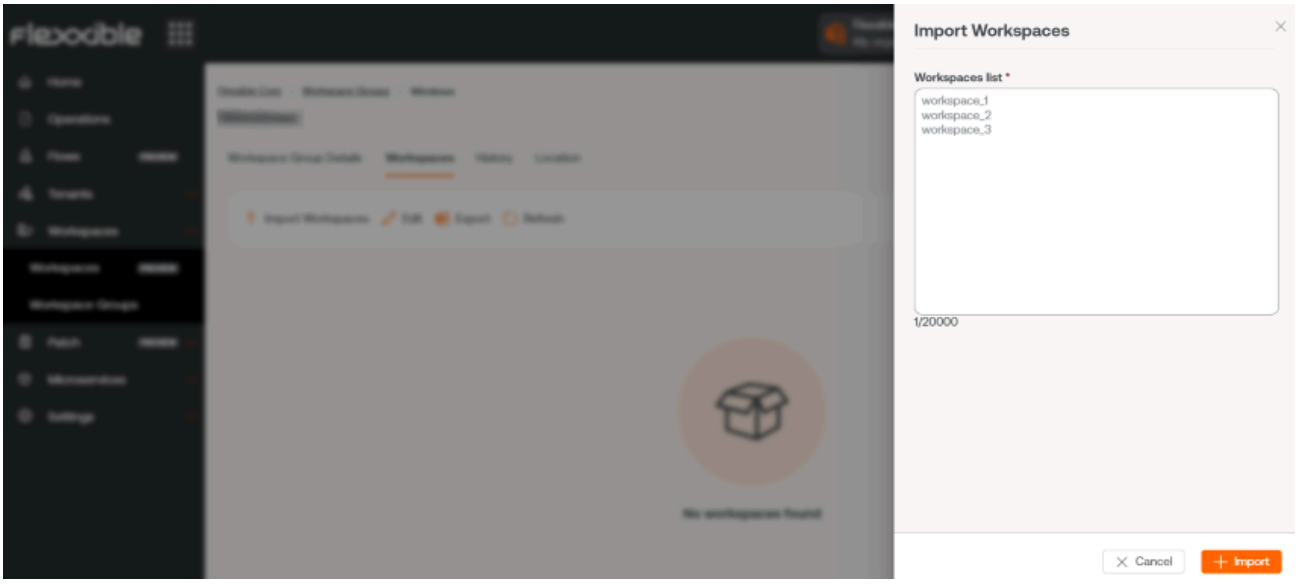
- **Synchronizations.** This tab is only visible when the group is of type Entra ID. Displays a table with details of the performed syncs.

Add devices to the static workspace group

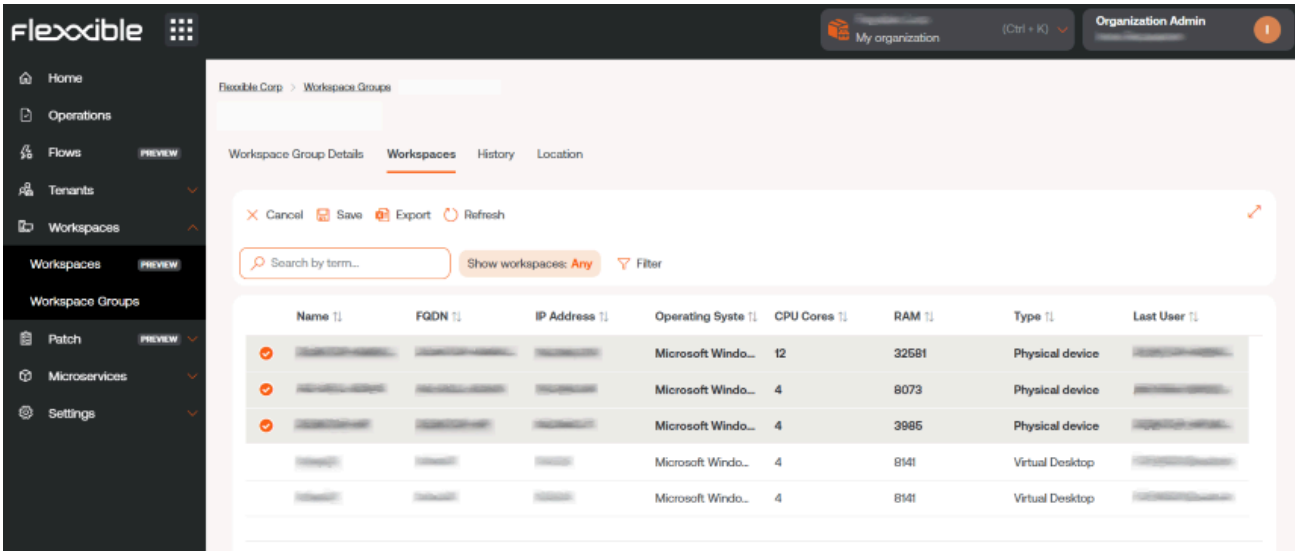
There are two ways to add devices to a static workspace group from Portal:

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.



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.

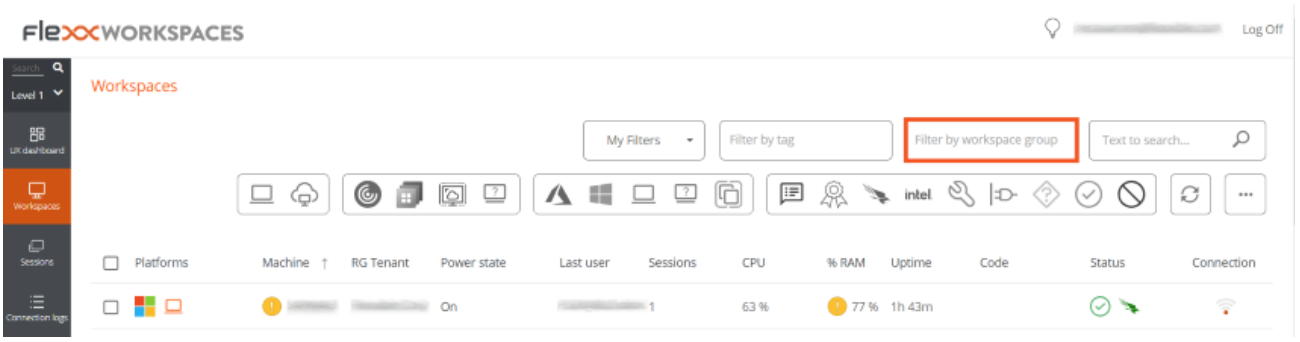


Manage a workspace group from Workspaces

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.



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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

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.

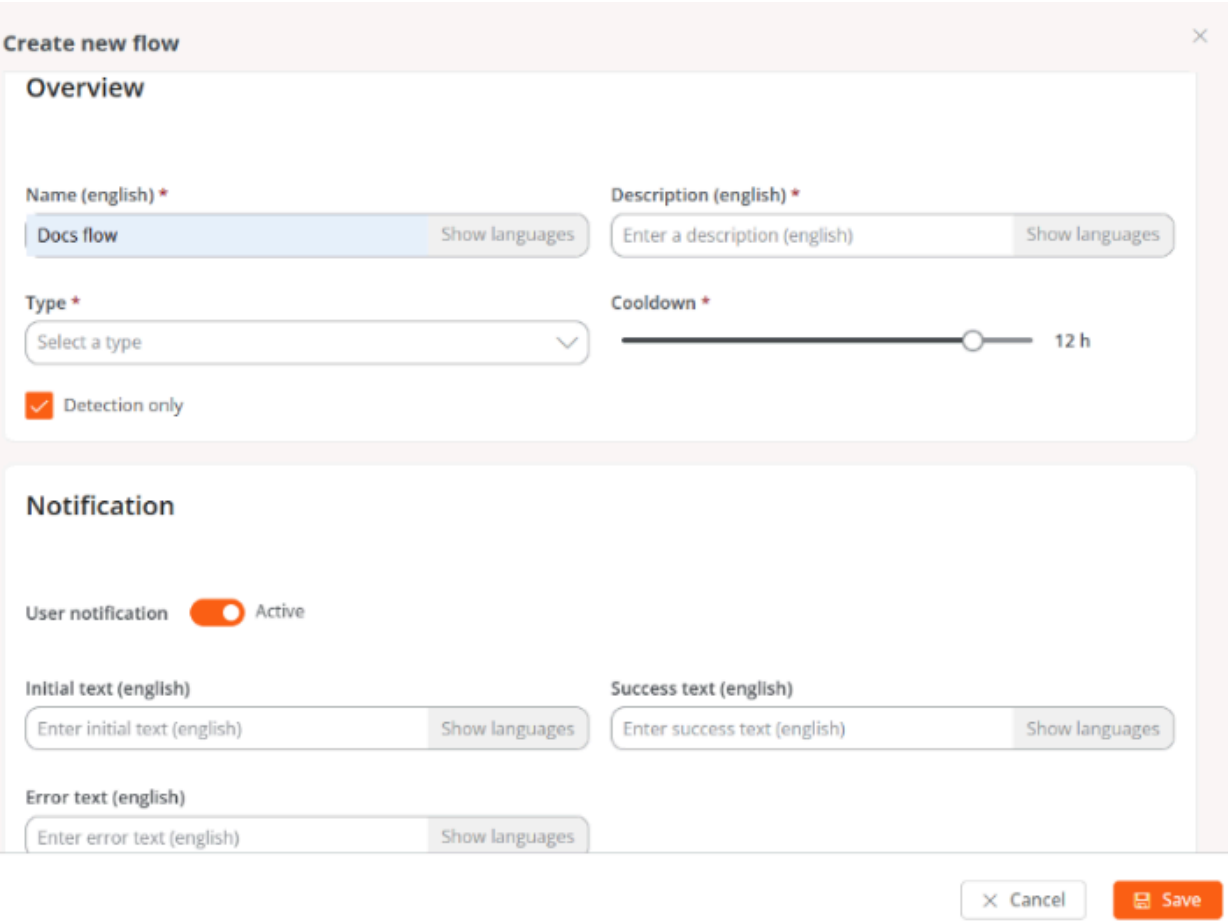
Schedule a microservice execution

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.



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

Copyright © 2024 Flexxible. Todos los derechos reservados.

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.

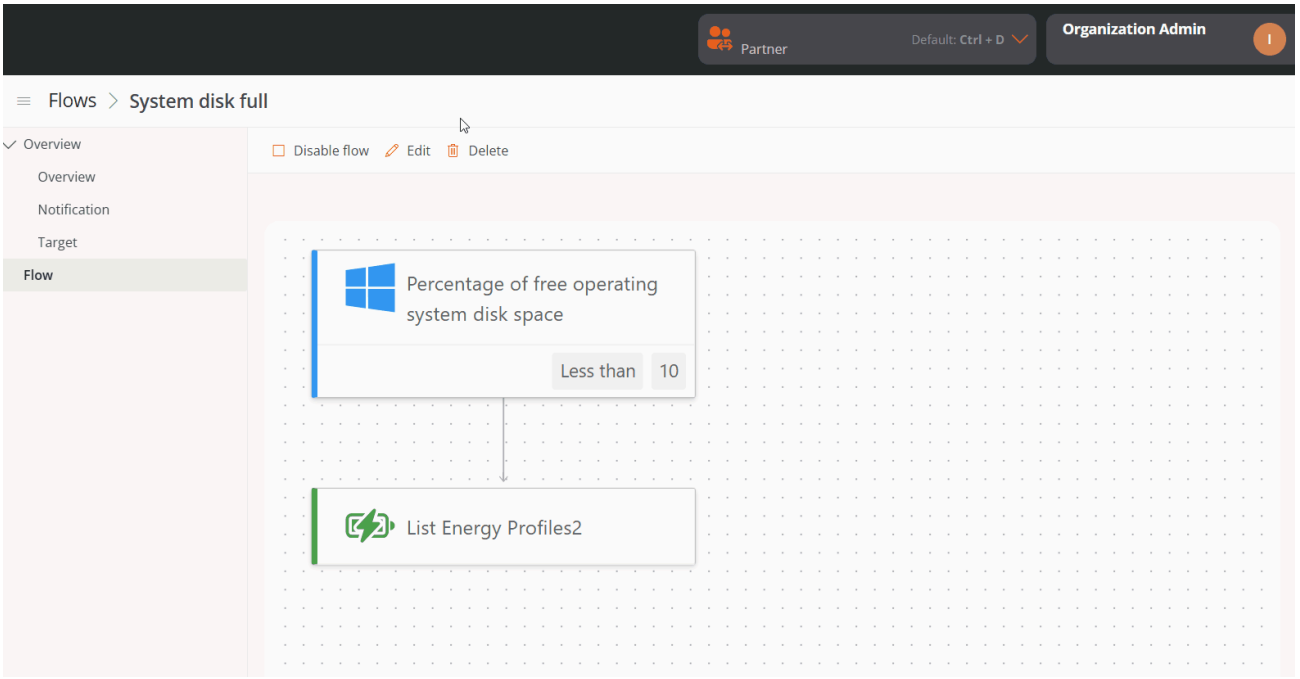
- **All workspaces.** Apply the flow to all devices in the organization.
- **Workspaces.** Apply the flow to the devices that the user chooses in the table.
- **Workspaces groups.** Apply the flow to the workspaces groups that the user chooses in the dropdown shown when selecting this option.
- **Reporting 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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

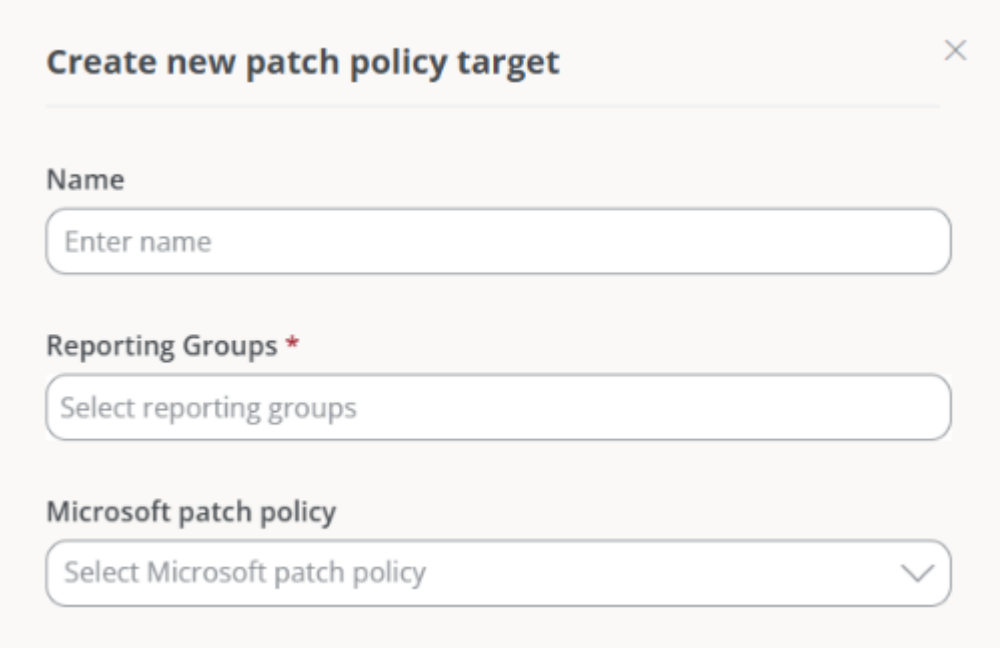
Portal / Guides / Configure patch policies

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:

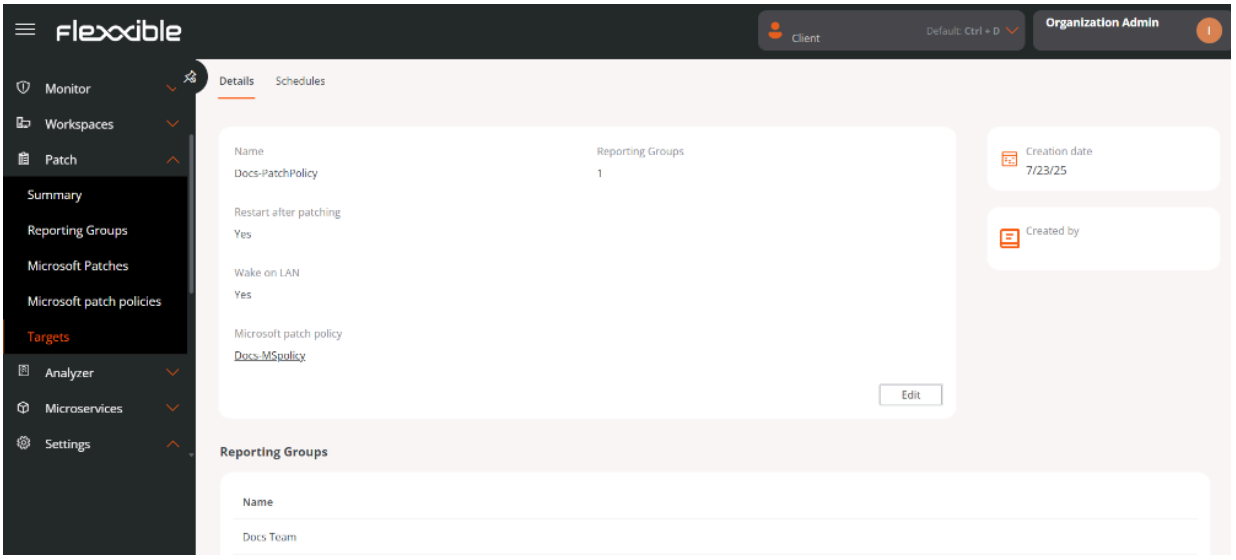
- **Name.** Name of the new patch policy.
- **Report Group.** Target device group for the new patch policy (can be more than one).
- **Microsoft Patch Policy.** Microsoft patch policy to which the new patch policy will be linked. This field is optional.



4. Click on `Save`.

5. The new patch policy information will appear on the screen.

Copyright © 2024 Flexxible. Todos los derechos reservados.



Edit a patch policy

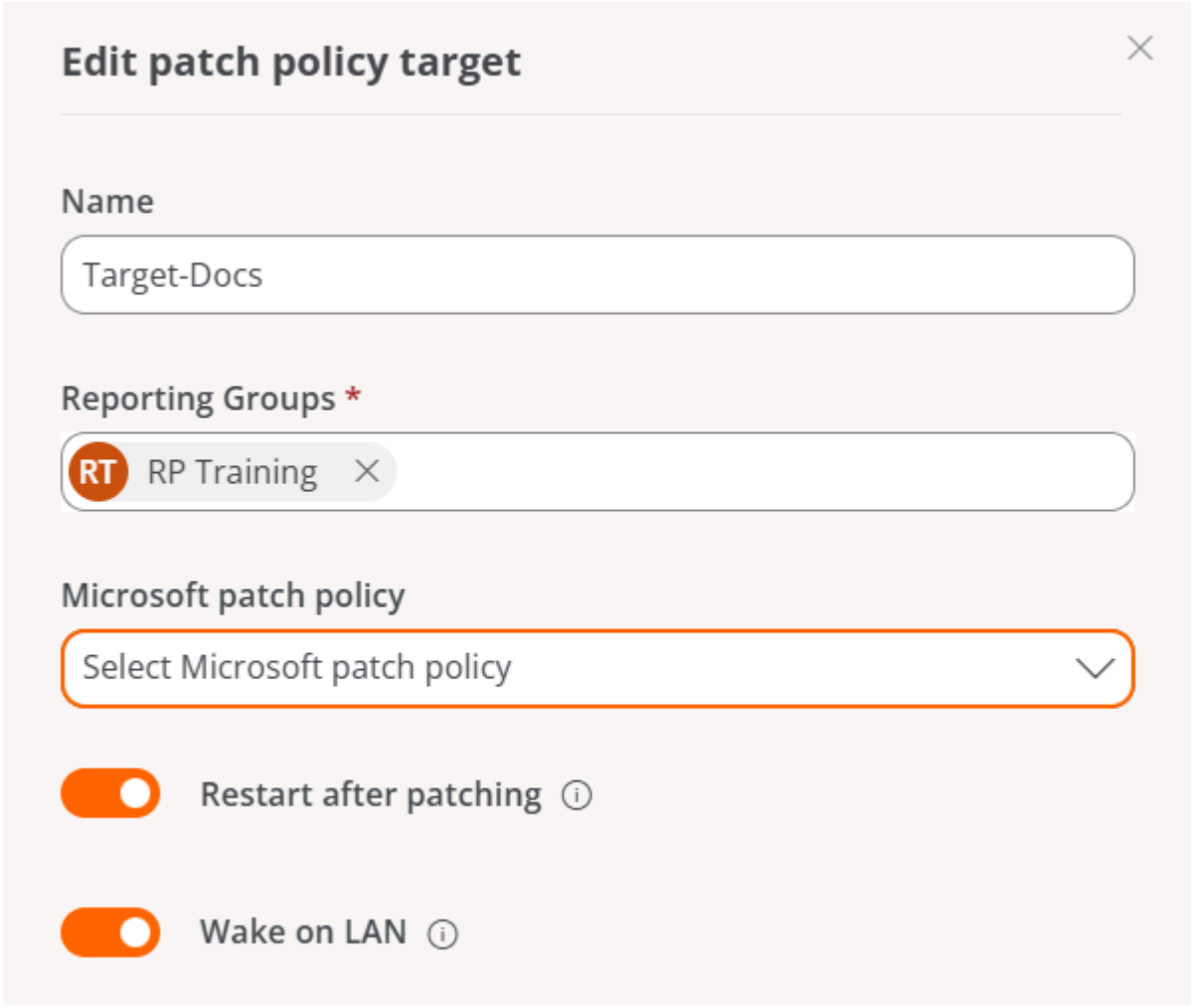
Once created, patch policies can be modified to define device behavior after updates, including options like automatic reboot or remote startup via Wake on LAN (WoL).

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.

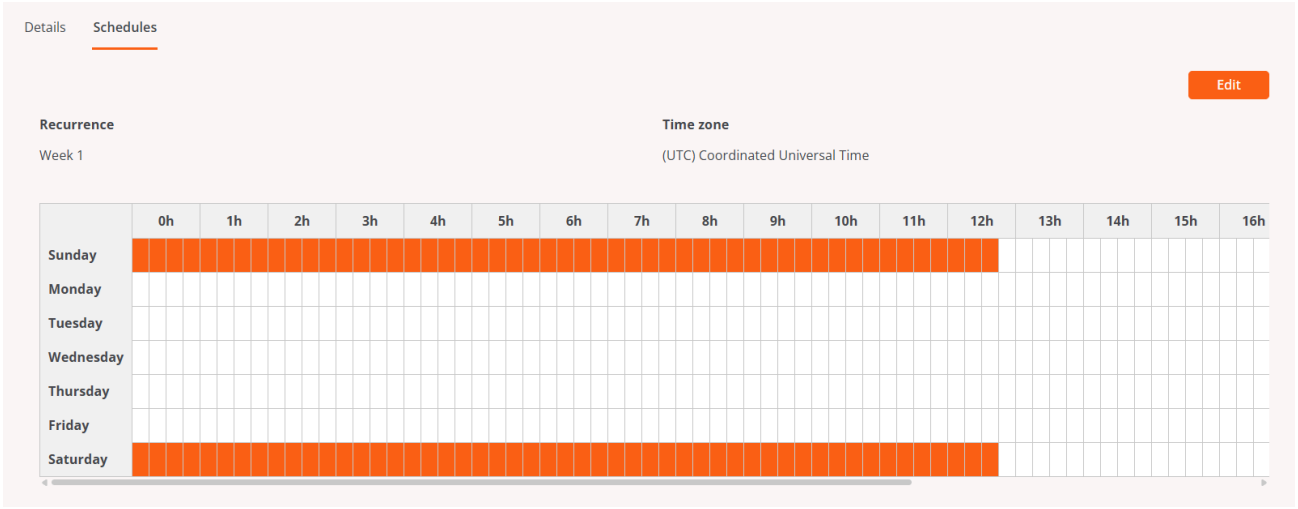
5. Click on `Save`.

Copyright © 2024 Flexxible. Todos los derechos reservados.



Schedule patches

The patch policy allows scheduling the day and time for applying patches on devices associated with a report group, facilitating controlled maintenance.



Copyright © 2024 Flexxible. Todos los derechos reservados.

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`.

Copyright © 2024 Flexxible. Todos los derechos reservados.

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*

Copyright © 2024 Flexxible. Todos los derechos reservados.

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.

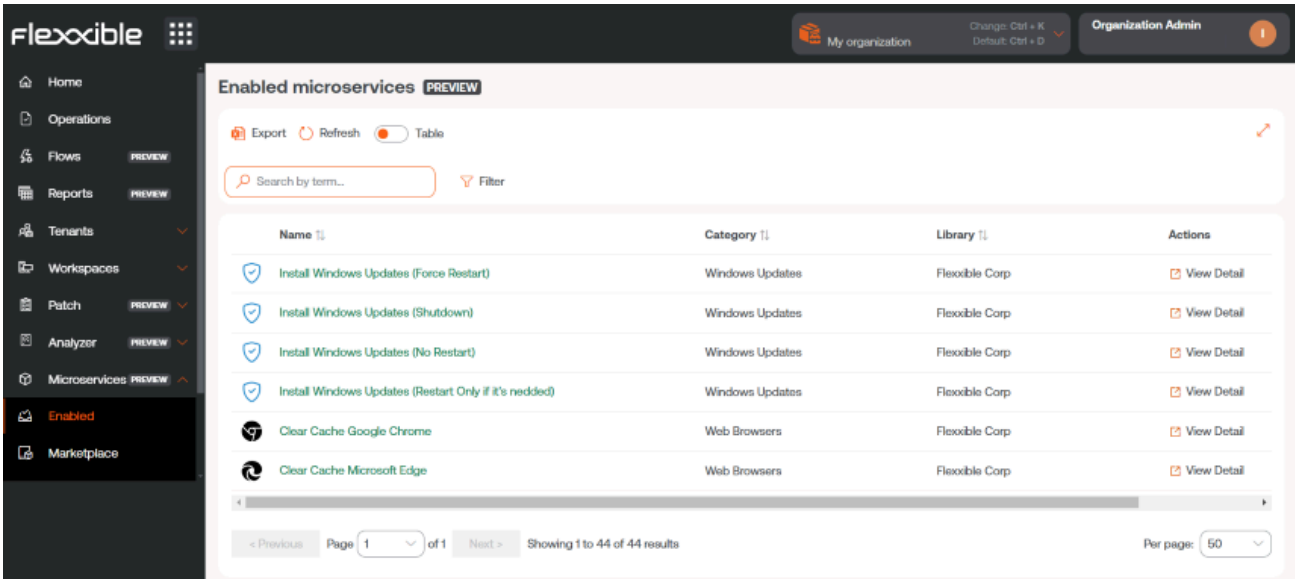
Copyright © 2024 Flexxible. Todos los derechos reservados.

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.

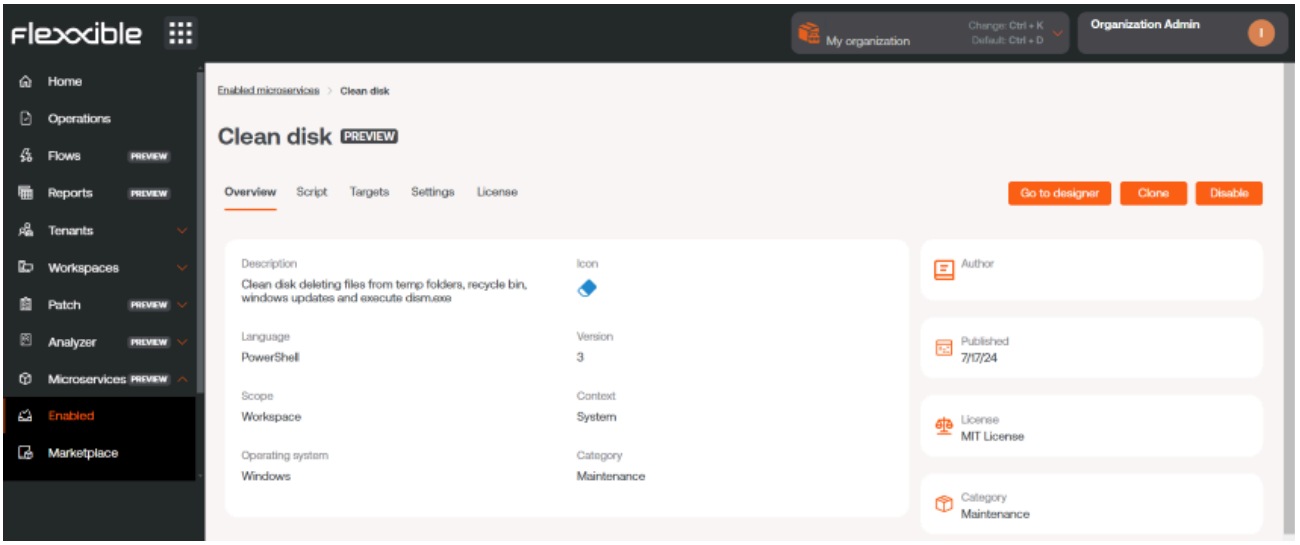
How to enable a microservice for the end-user

1. Access the `Microservices` -> `Enabled` menu within the Flexxible Portal (microservices can be organized either in blocks or lists).

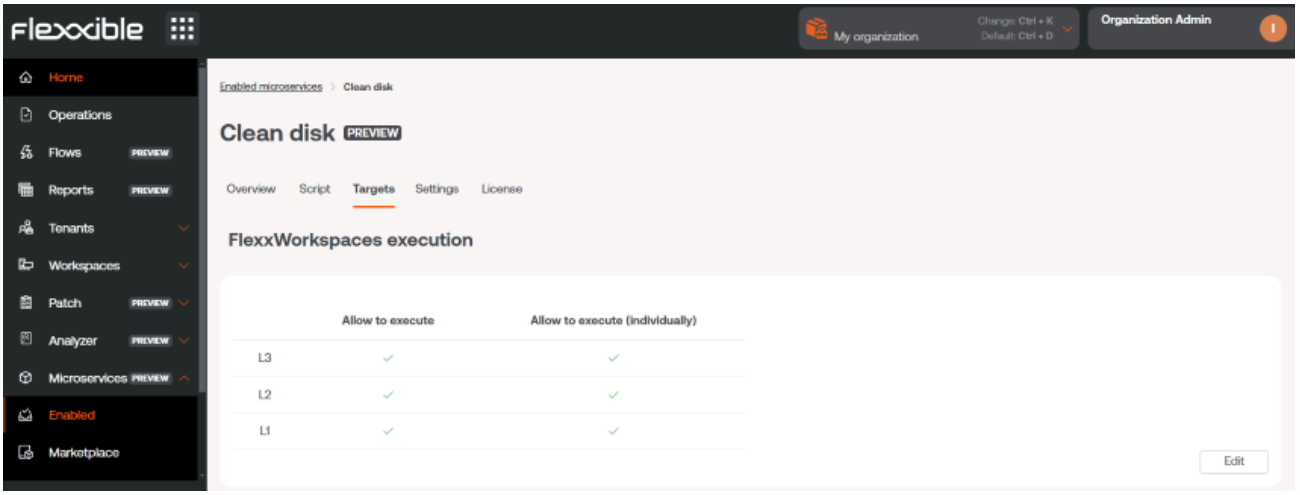


2. Select the microservice you want to enable by clicking on its name (if organized in blocks) or on the `See details` link (if organized in lists). Next, the microservice details will appear (in the example, “Clean Disk”).

Copyright © 2024 Flexxible. Todos los derechos reservados.

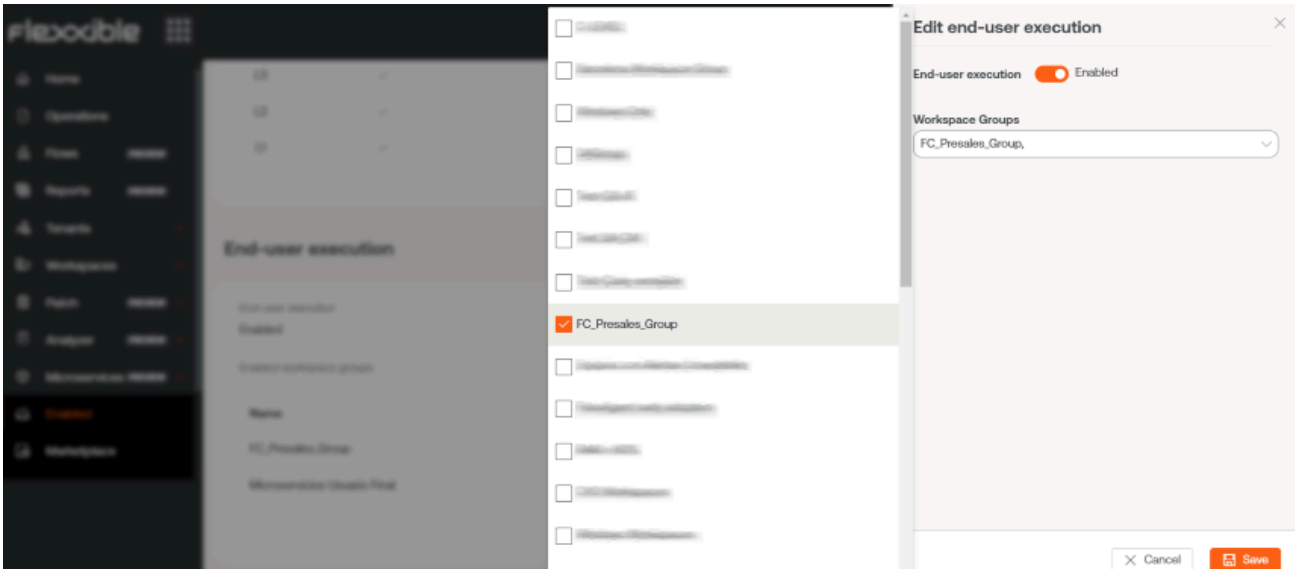


3. Select the `Targets` tab, which shows the execution permissions and recipients of this microservice.



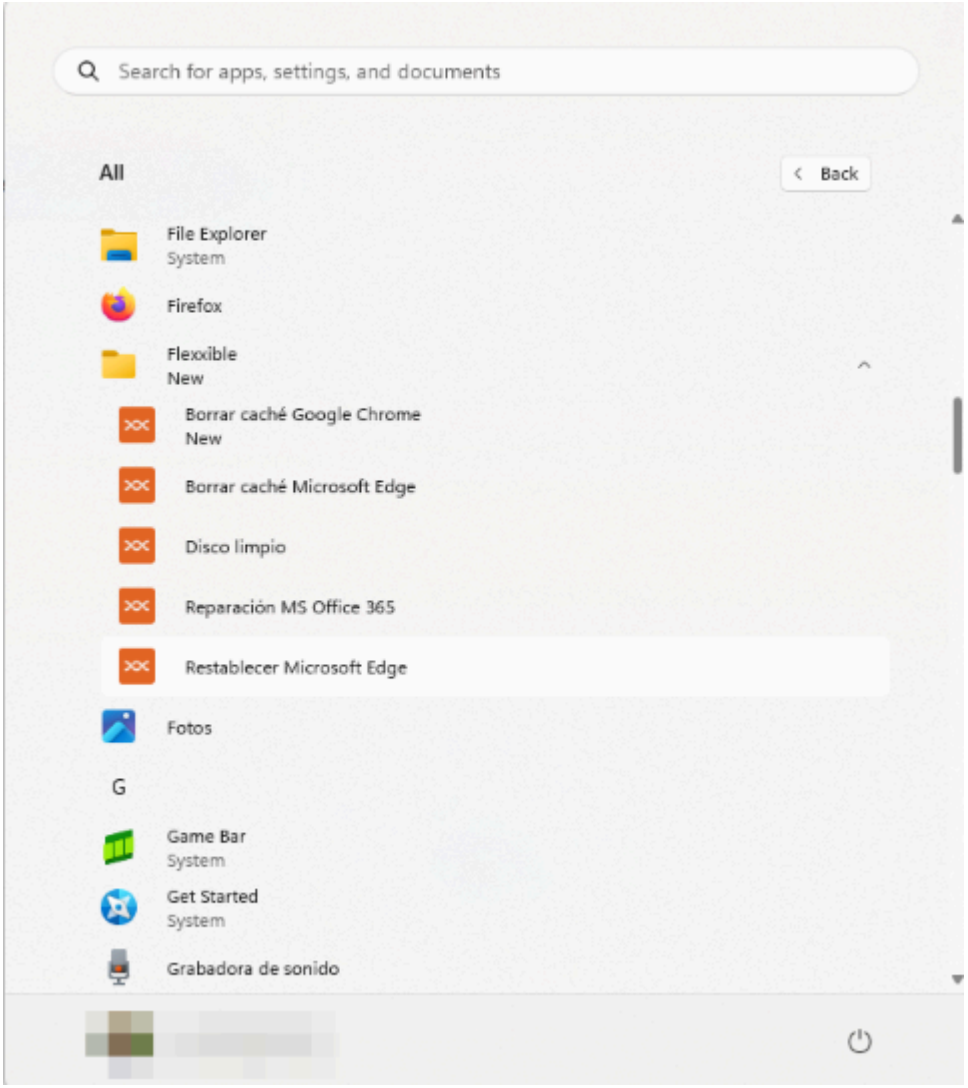
4. Click on the `Edit` button in the bottom right corner, within the `User Execution` section. A modal window with the configuration option will appear.

Copyright © 2024 Flexxible. Todos los derechos reservados.



5. In the panel, enable the execution of the microservice by the end user and select one or more `Workspace groups` where this option will be valid. Once selected, click `Save`.
6. In the next few minutes, the new microservice will appear as a new operating system option within the folder *Flexxible* in the start menu.

Copyright © 2024 Flexxible. Todos los derechos reservados.



Rename the microservices folder

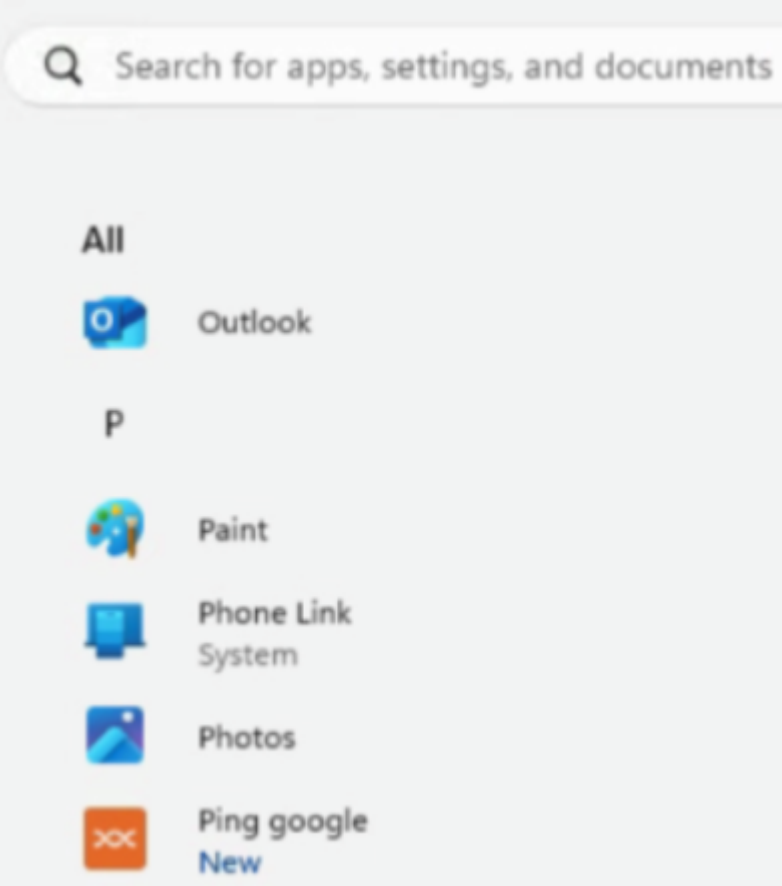
1. Go to `Portal` -> `Settings` -> `Organization`.
2. In the left side menu, select `Microservices` -> `Edit microservices settings`.
3. Rename the folder.
4. Click on `Save`.

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

Copyright © 2024 Flexxible. Todos los derechos reservados.

microservice icon will be visible in the start menu.



INFO

For more information about Microservices, please refer to its documentation.

Copyright © 2024 Flexxible. Todos los derechos reservados.

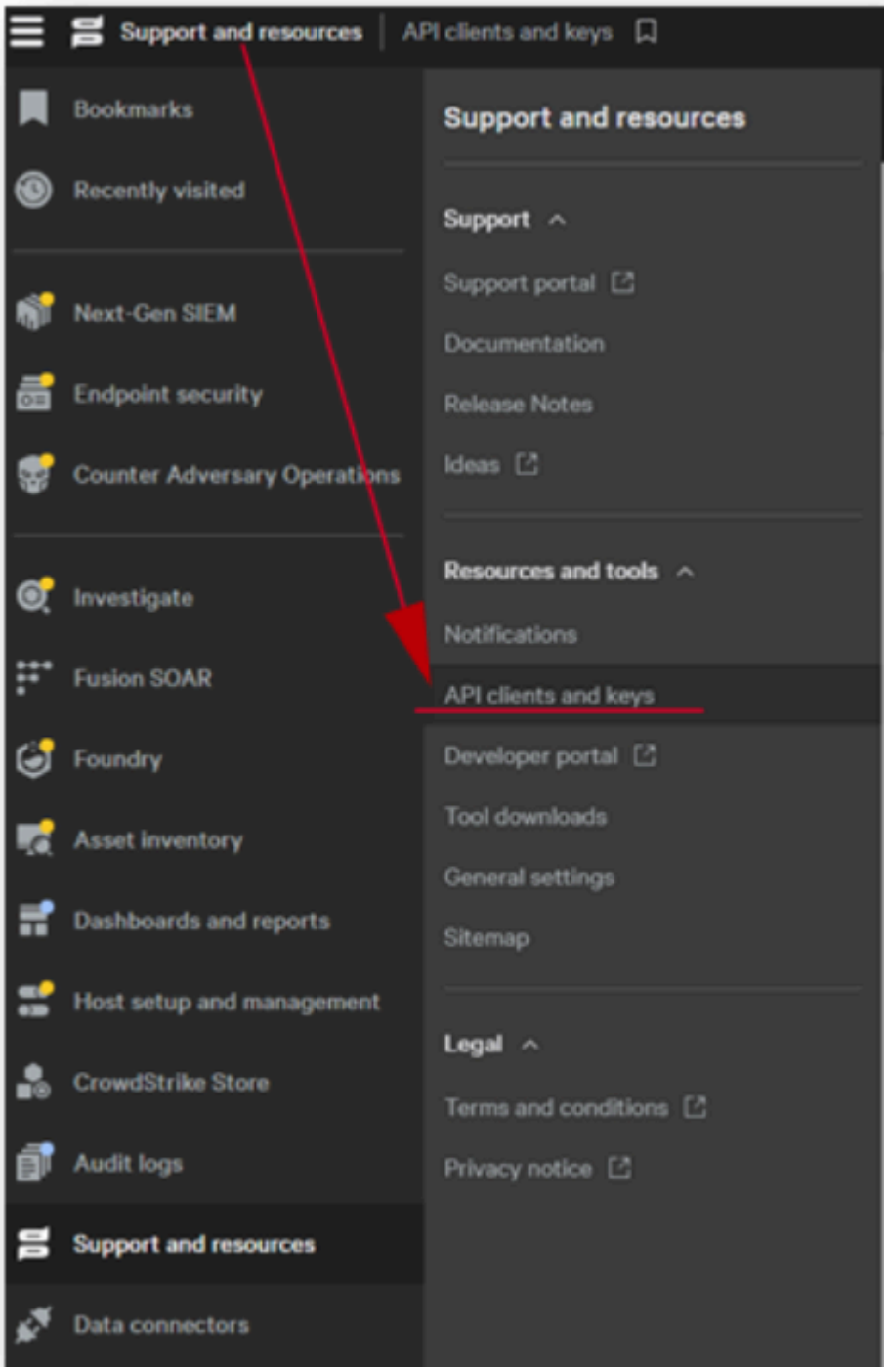
Portal / Guides / Set up integration with CrowdStrike

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`.

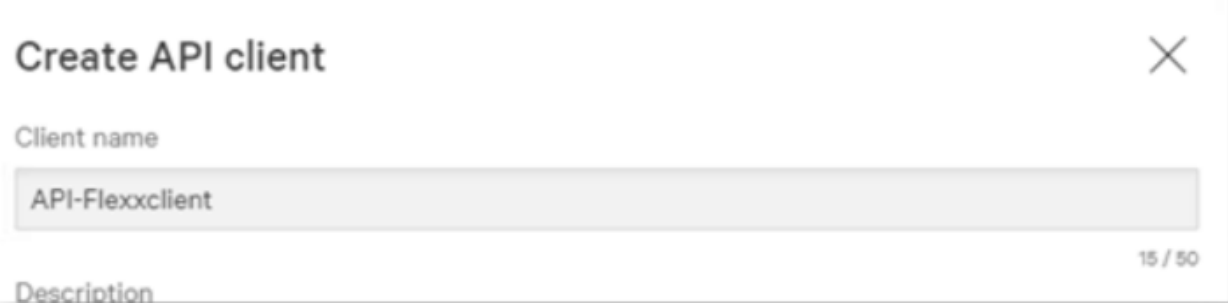
Copyright © 2024 Flexxible. Todos los derechos reservados.



3. Select `Create API client` on the right side of the menu.

4. Assign a name to the API; the standard is *API-Flexxclient*.

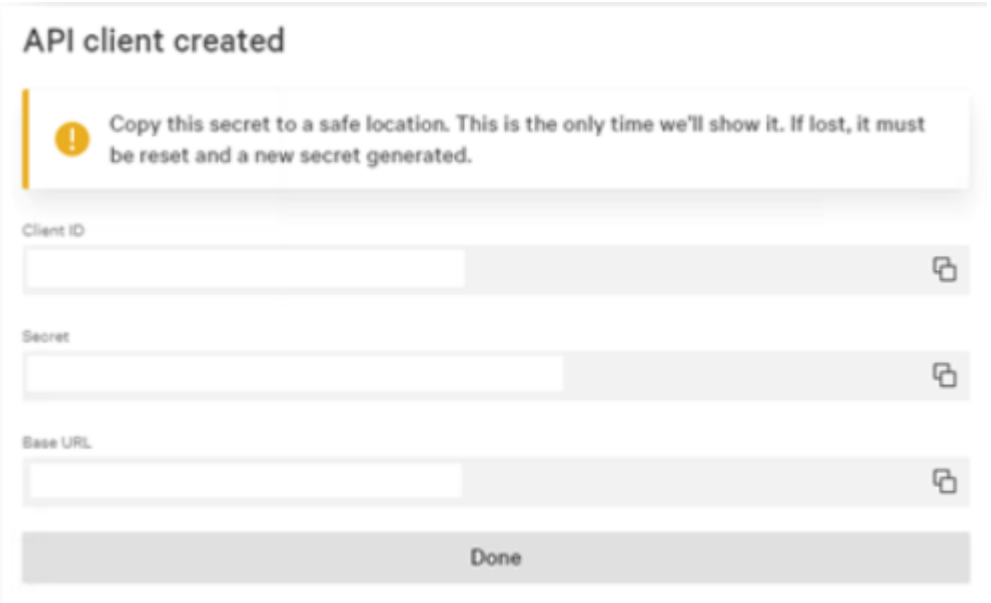
Copyright © 2024 Flexxible. Todos los derechos reservados.



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

Copyright © 2024 Flexxible. Todos los derechos reservados.

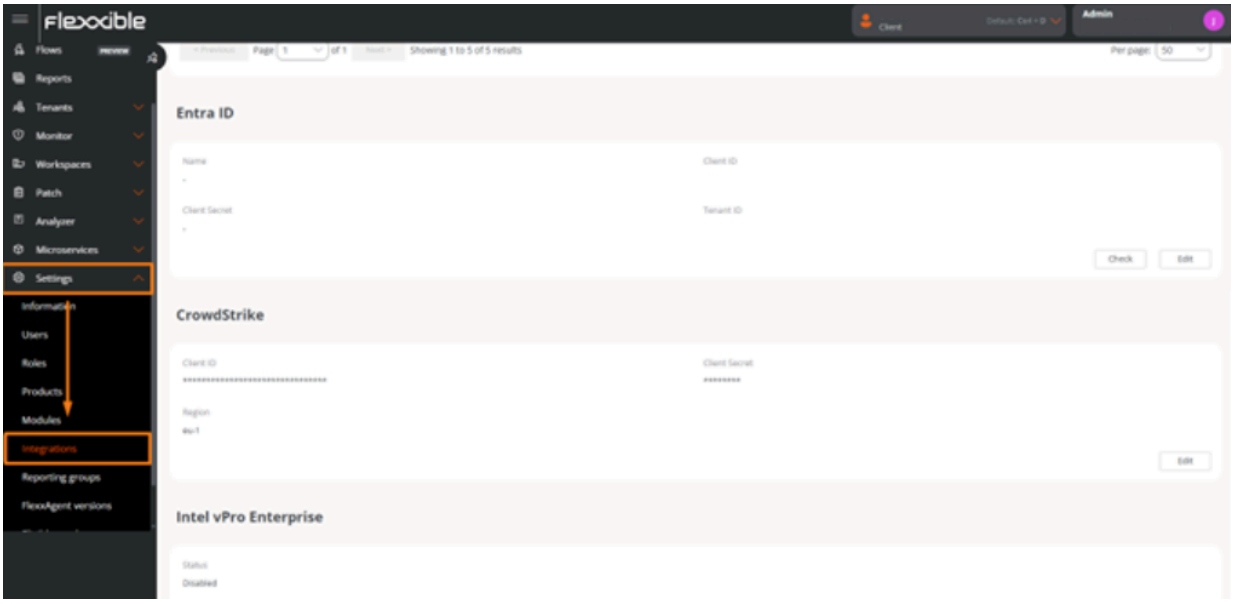


Configuration in Portal

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.



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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

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.

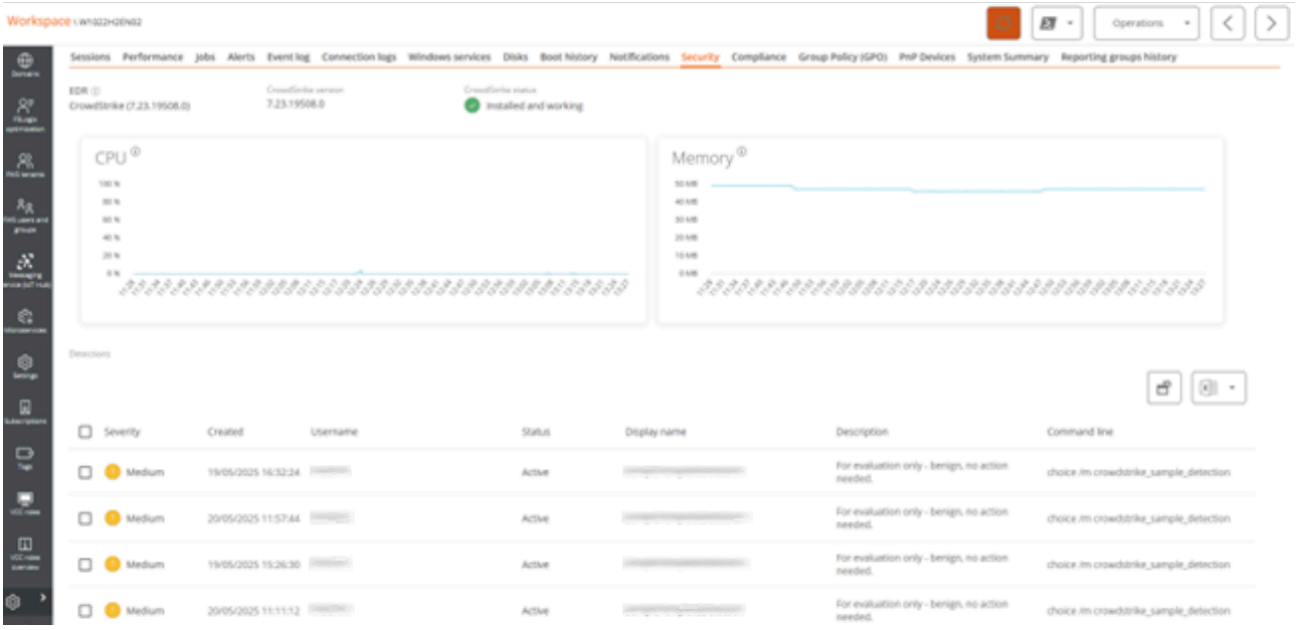
If the EDR generates an alert, the Falcon icon will appear red.

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.



Copyright © 2024 Flexxible. Todos los derechos reservados.

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

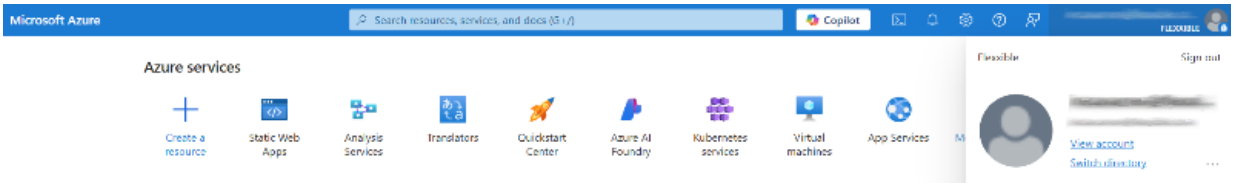
Integration with Entra ID requires the following steps to be followed in the Microsoft Azure environment:

- Create an application registration
- Create a client secret
- Configure permissions for the application registration
- Permissions in the Azure subscription

Create an application registration

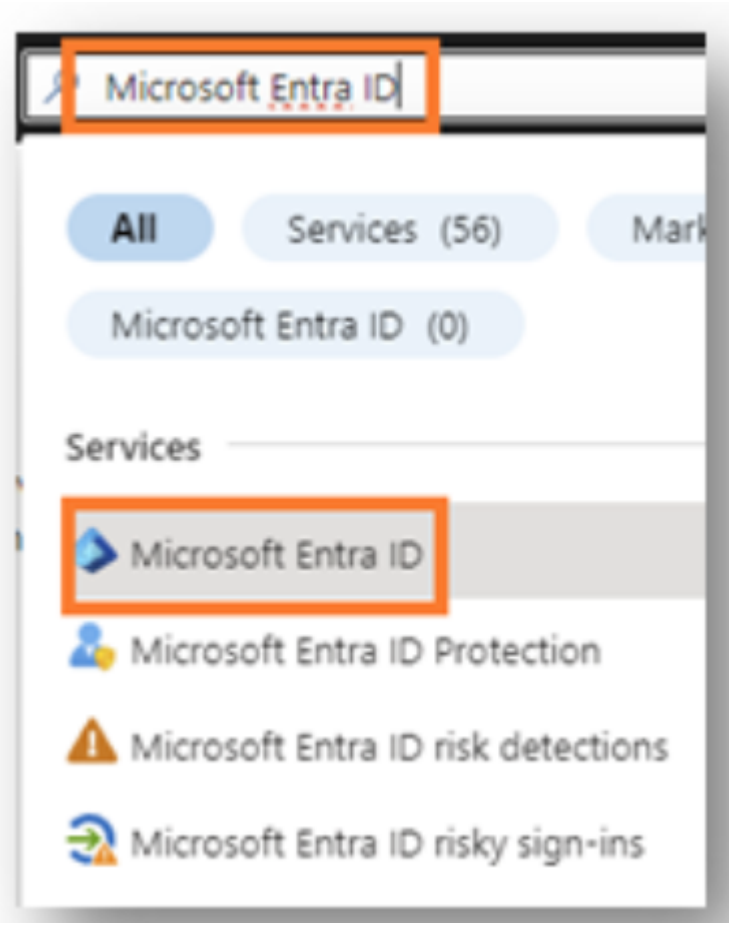
1. Log in to Azure Portal.

2. Select the tenant if you have access to multiple; to do this, click on `Switch directory` in the user menu.



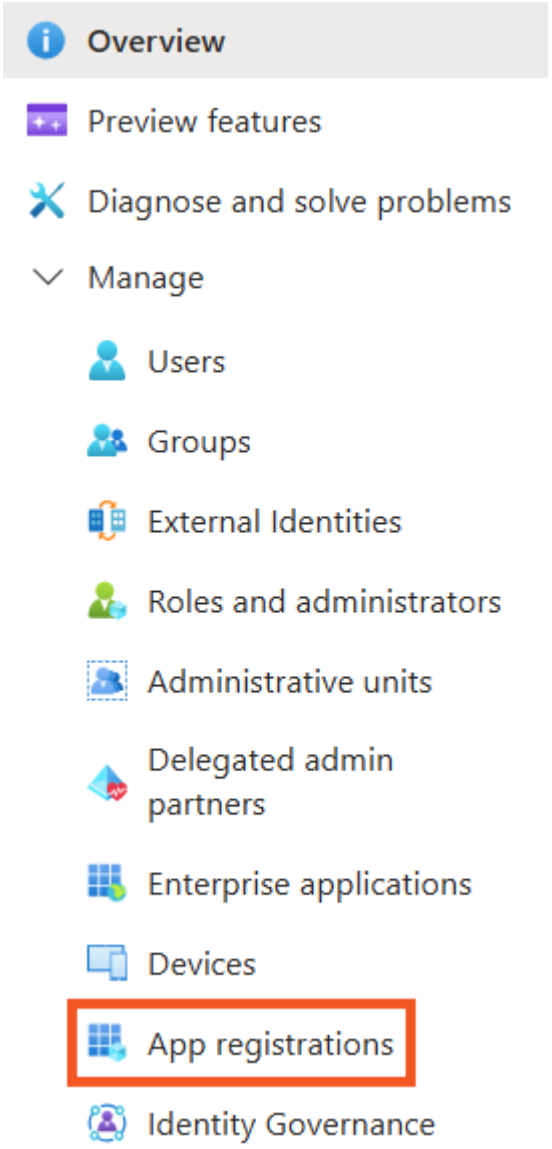
Copyright © 2024 Flexxible. Todos los derechos reservados.

3. Once the subscription is selected, search for *Microsoft Entra ID*.

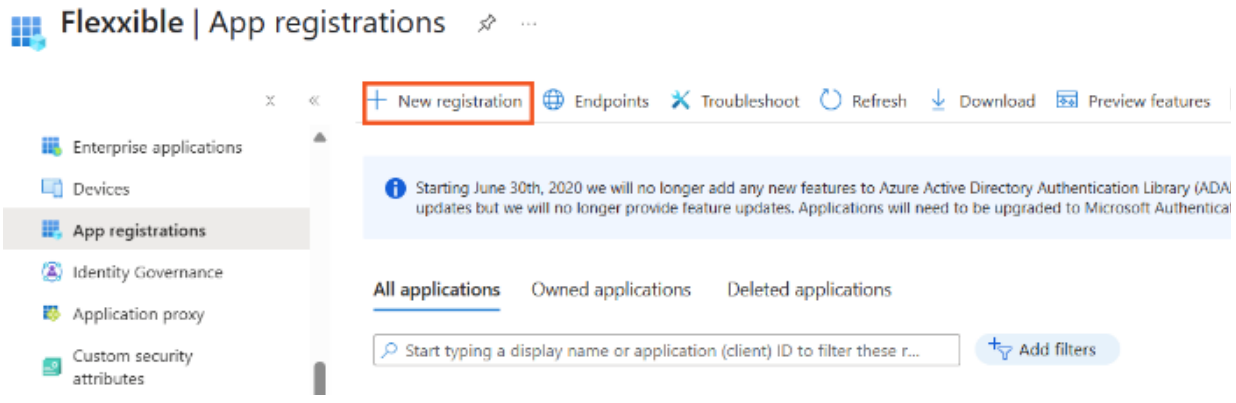


4. To the left of the interface, you will see the following menu:

Copyright © 2024 Flexxible. Todos los derechos reservados.

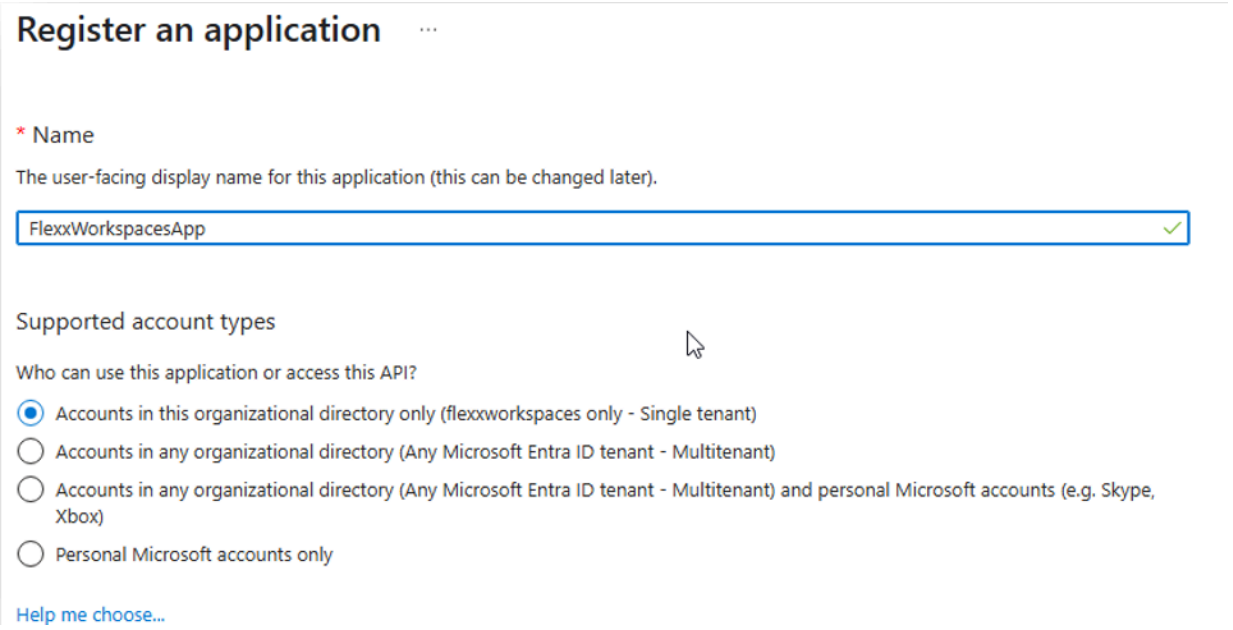


5. Click `Application registrations` -> `New registration`.



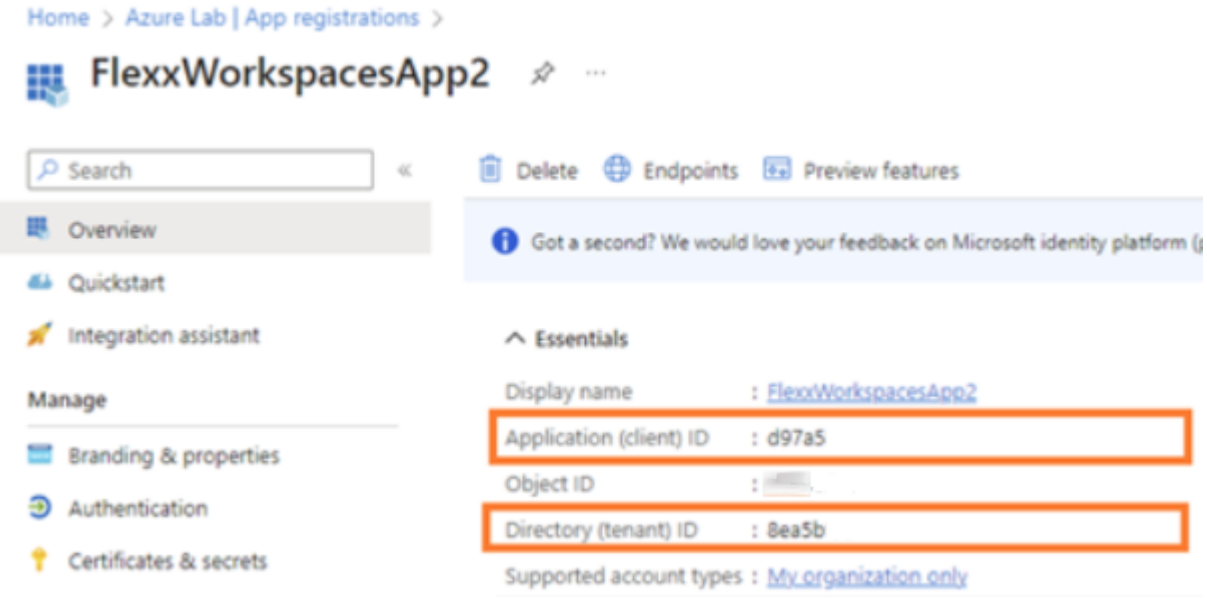
6. Enter a name to register the application and select the supported account type.

Copyright © 2024 Flexxible. Todos los derechos reservados.



7. Click `Register` to complete the application registration.

8. Copy and save the Application ID (App ID) and the Directory ID (tenant).

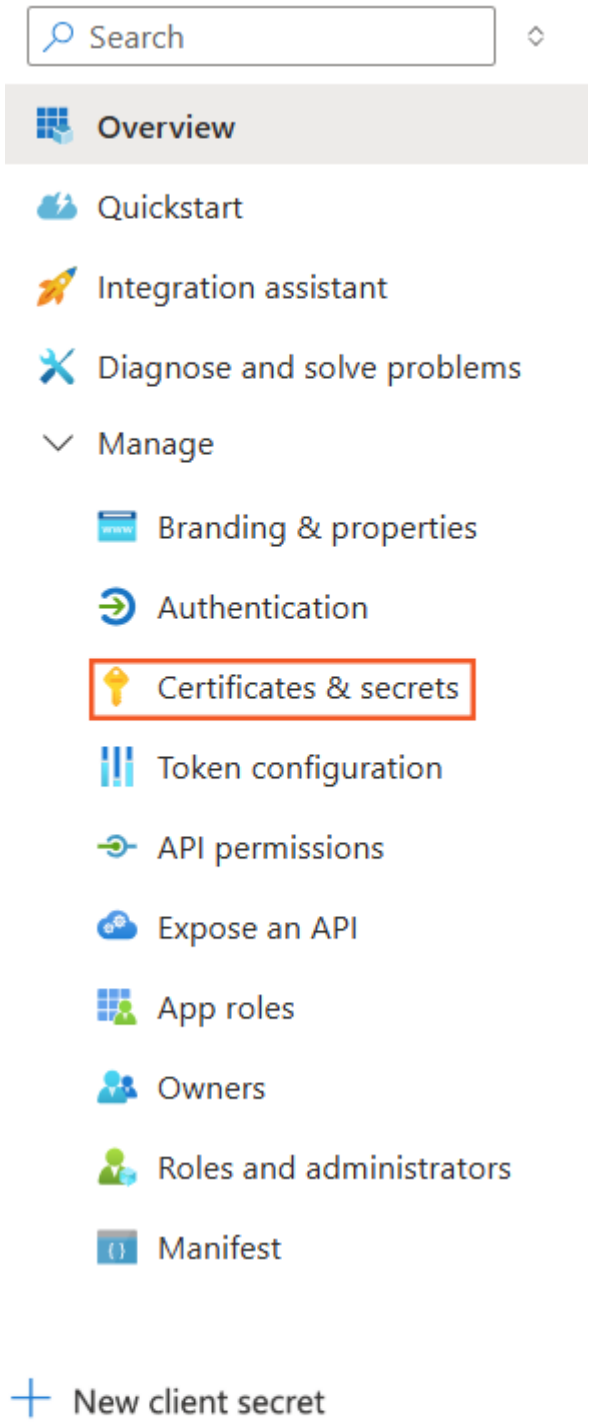


Create a client secret

1. Access `App registrations`.

2. In the menu, click `Manage` -> `Certificates & secrets` -> `New client secret`.

Copyright © 2024 Flexxible. Todos los derechos reservados.

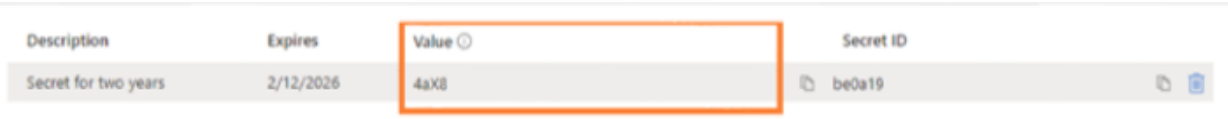


3. Add a description and in the *Expires* field, select 24 months.

4. Click `Add`.

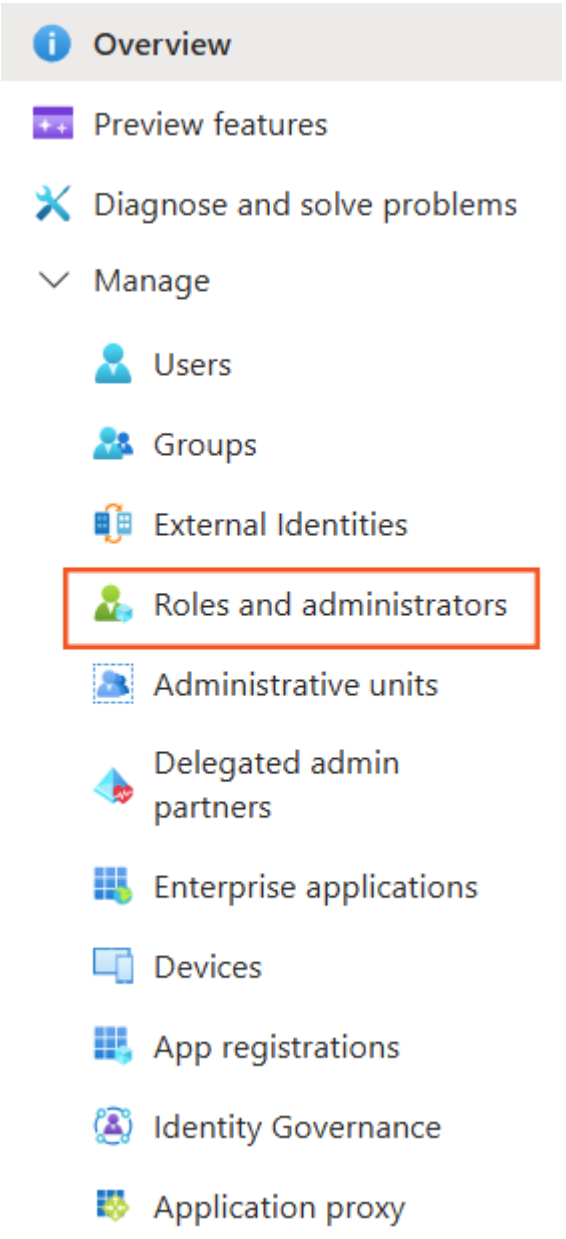
5. Microsoft will provide the client secret and the client ID. You need to save these values because they will not be shown again. If not saved, the client secret must be deleted and a new one created to obtain the value.

Copyright © 2024 Flexxible. Todos los derechos reservados.



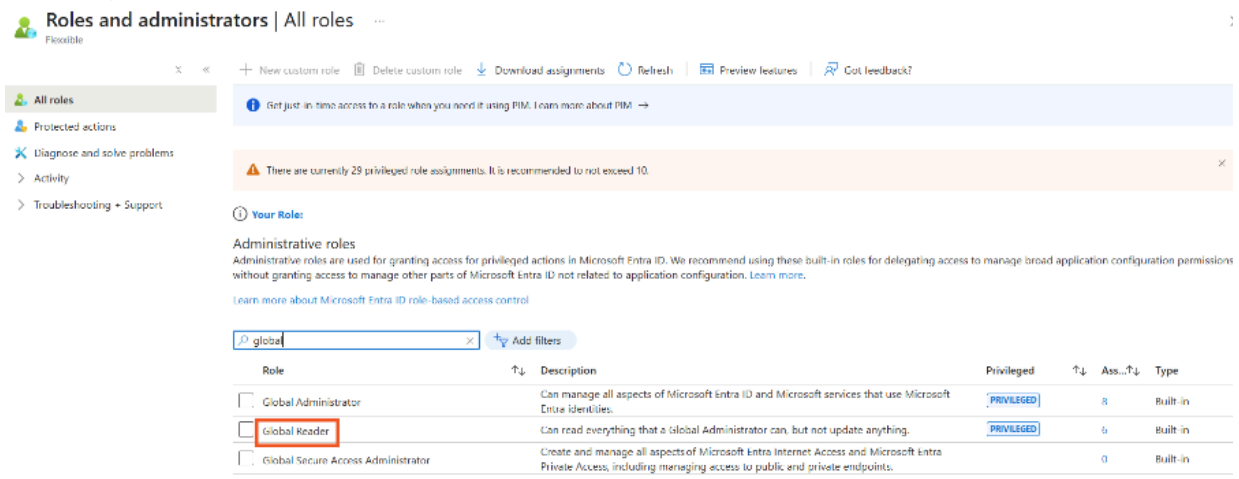
Configure permissions for the application registration

1. Log in to Azure Portal.
2. Click on Microsoft Entra ID.
3. Click `Manage` -> `Roles and administrators`.

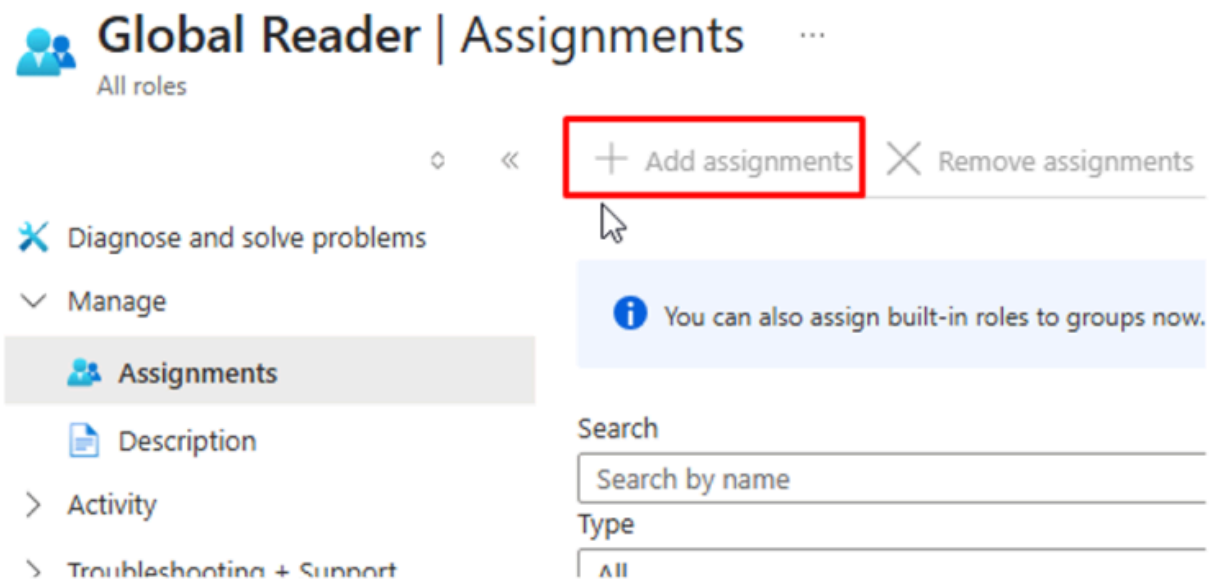


Copyright © 2024 Flexxible. Todos los derechos reservados.

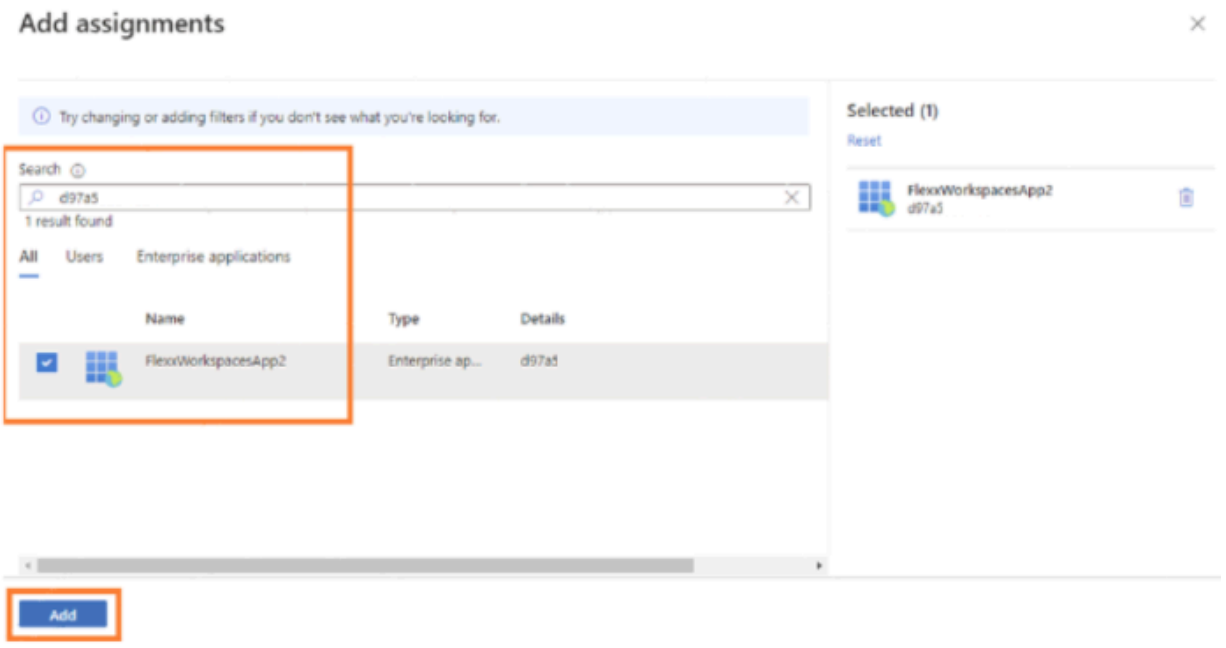
4. Search and select the `Global Reader` option.



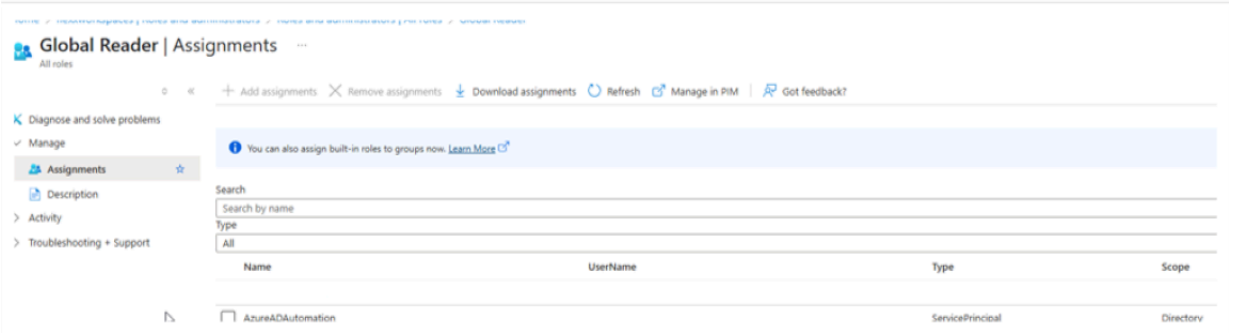
5. Click on `Add assignments` and add the application ID (App ID) created in the previous step.



Copyright © 2024 Flexxible. Todos los derechos reservados.



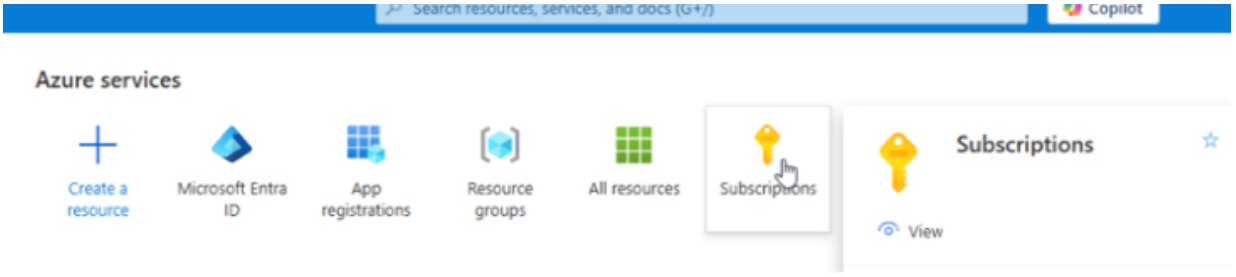
6. Verify that the application is configured on the main dashboard.



Permissions in the Azure subscription

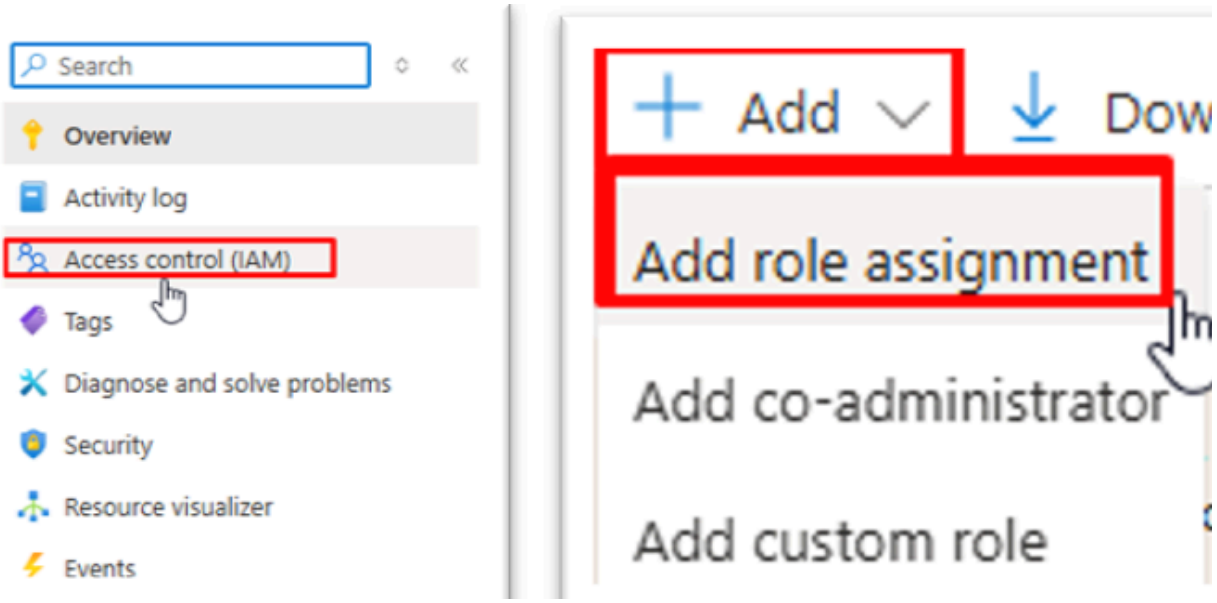
1. Log in to Azure Portal.

2. Click `Subscriptions`.

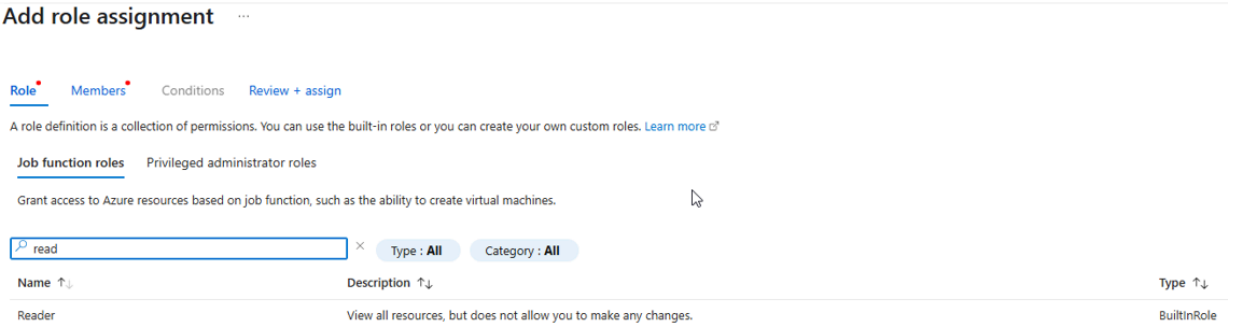


Copyright © 2024 Flexxible. Todos los derechos reservados.

3. Click `Access control (IAM)` -> `Add` -> `Add role assignment`.

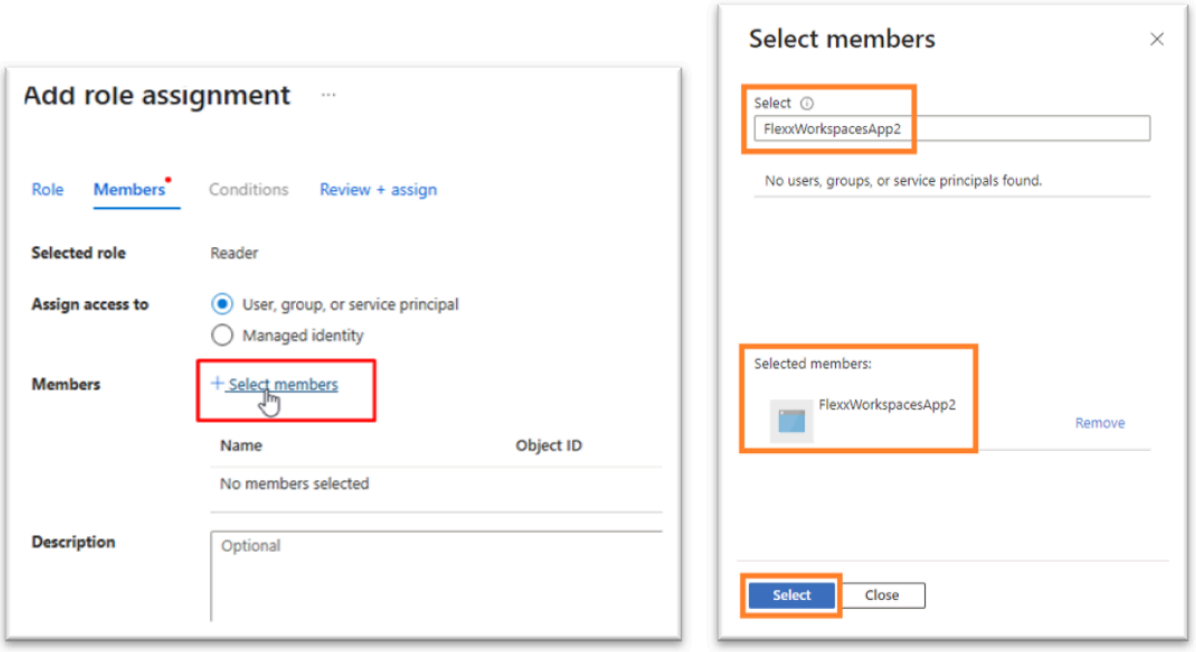


4. In `Role` -> `Function role`, search and select `Reader`.



5. In `Members` select the application ID (App ID) created in the previous step.

Copyright © 2024 Flexxible. Todos los derechos reservados.



6. Review and assign the role.

Configuration in Portal

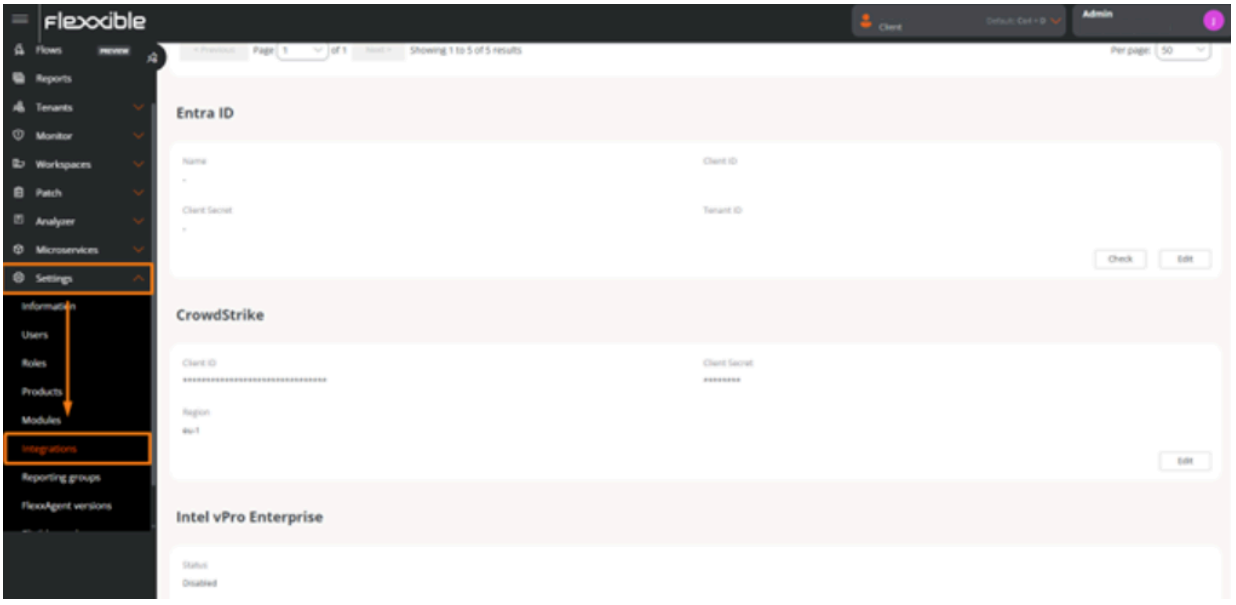
To perform the integration from Portal, the user must have at least the role of *Organization Administrator*.

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.

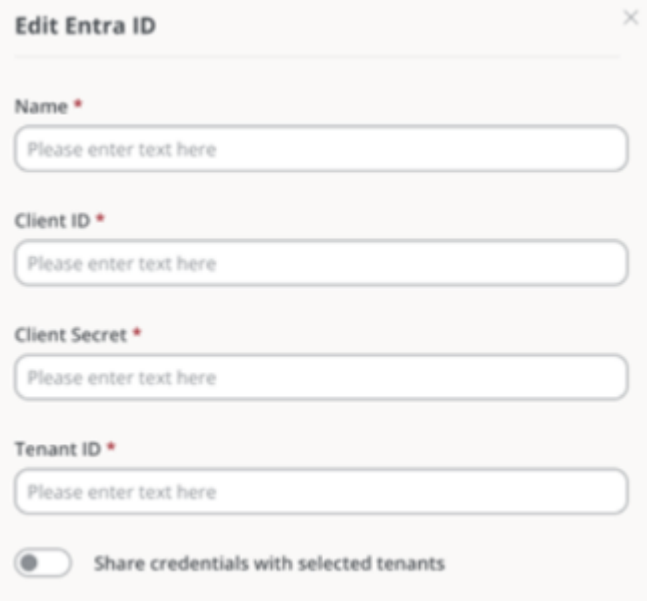
Copyright © 2024 Flexxible. Todos los derechos reservados.



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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

Portal / Guides / Set up Entra ID integration with Monitor

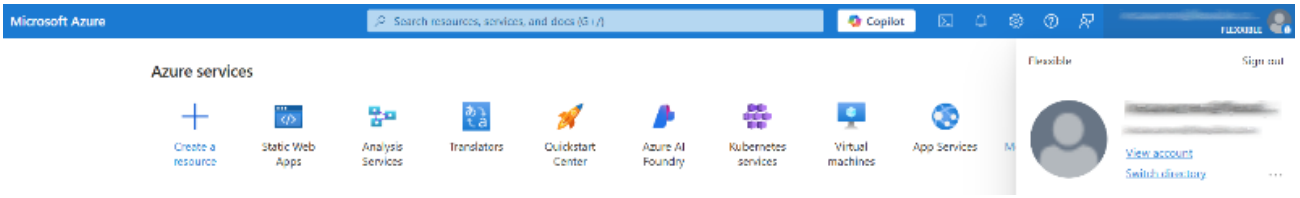
Monitor is the Flexxible monitoring module based on Grafana Cloud. Allows user access by invitation or through integration with Entra ID accounts. This guide describes the steps necessary to establish this integration.

Configuration in Microsoft Azure

- Create an application registration
- Create a client secret
- API permissions configuration
- Create application roles
- Review the manifest.xml file

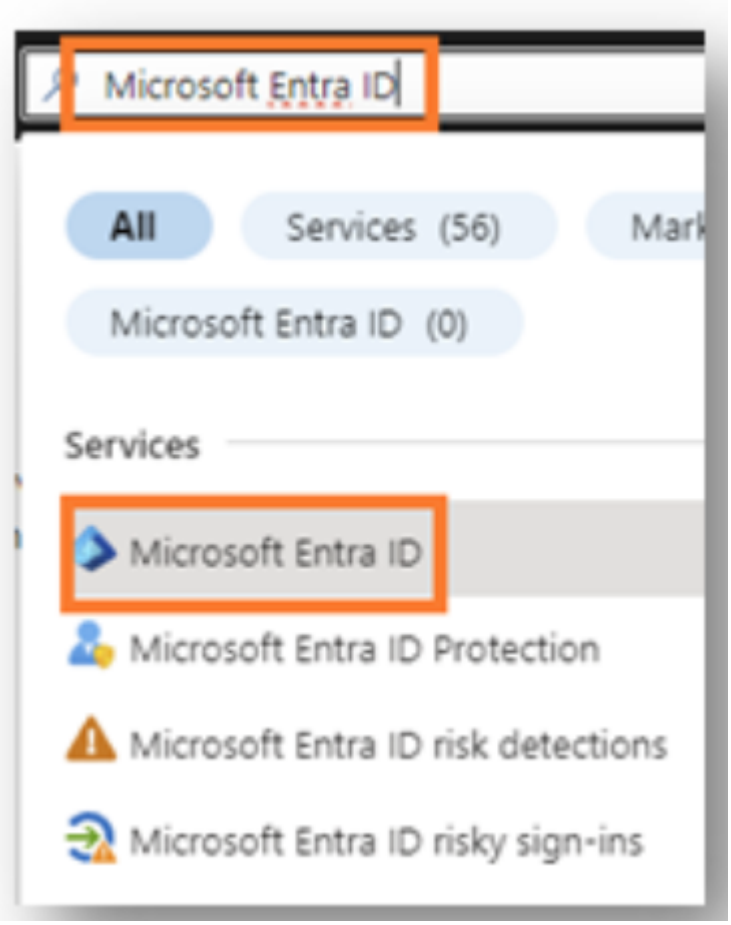
Create an application registration

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*.

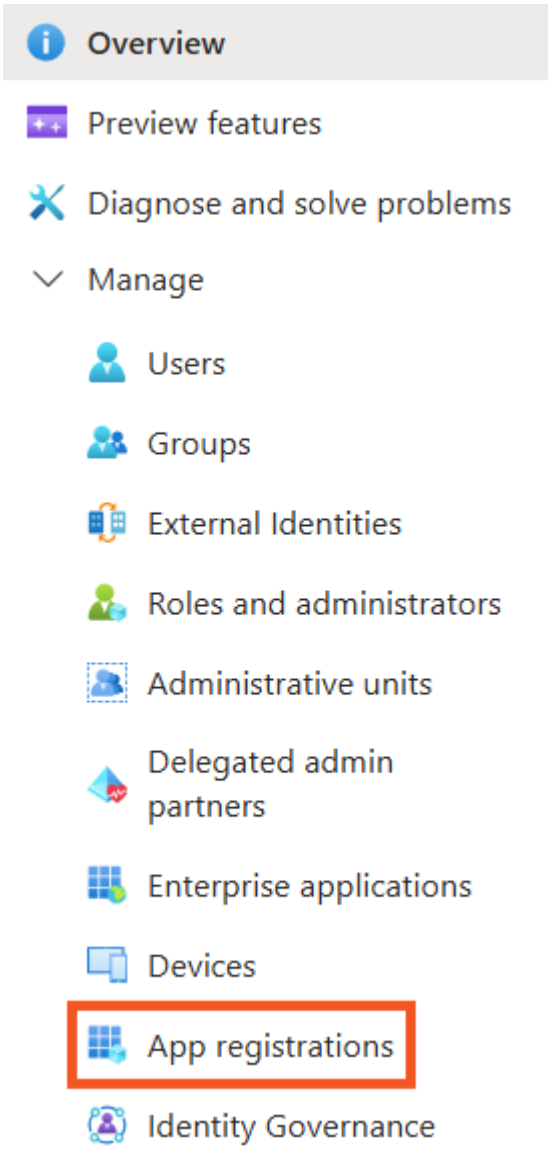
Copyright © 2024 Flexxible. Todos los derechos reservados.

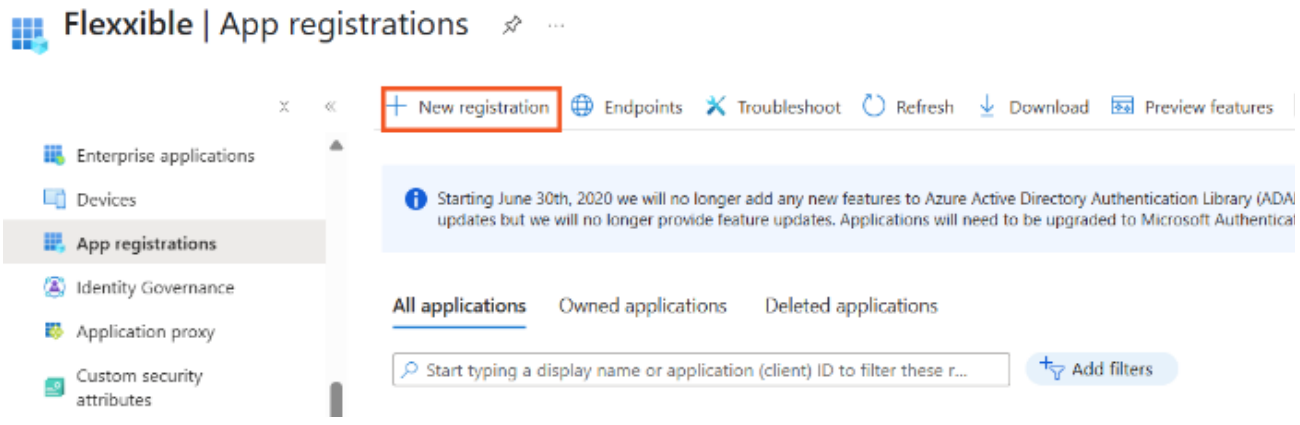


4. To the left of the interface, you will see the following menu:

5. Click `Application registrations` -> `New registration`.

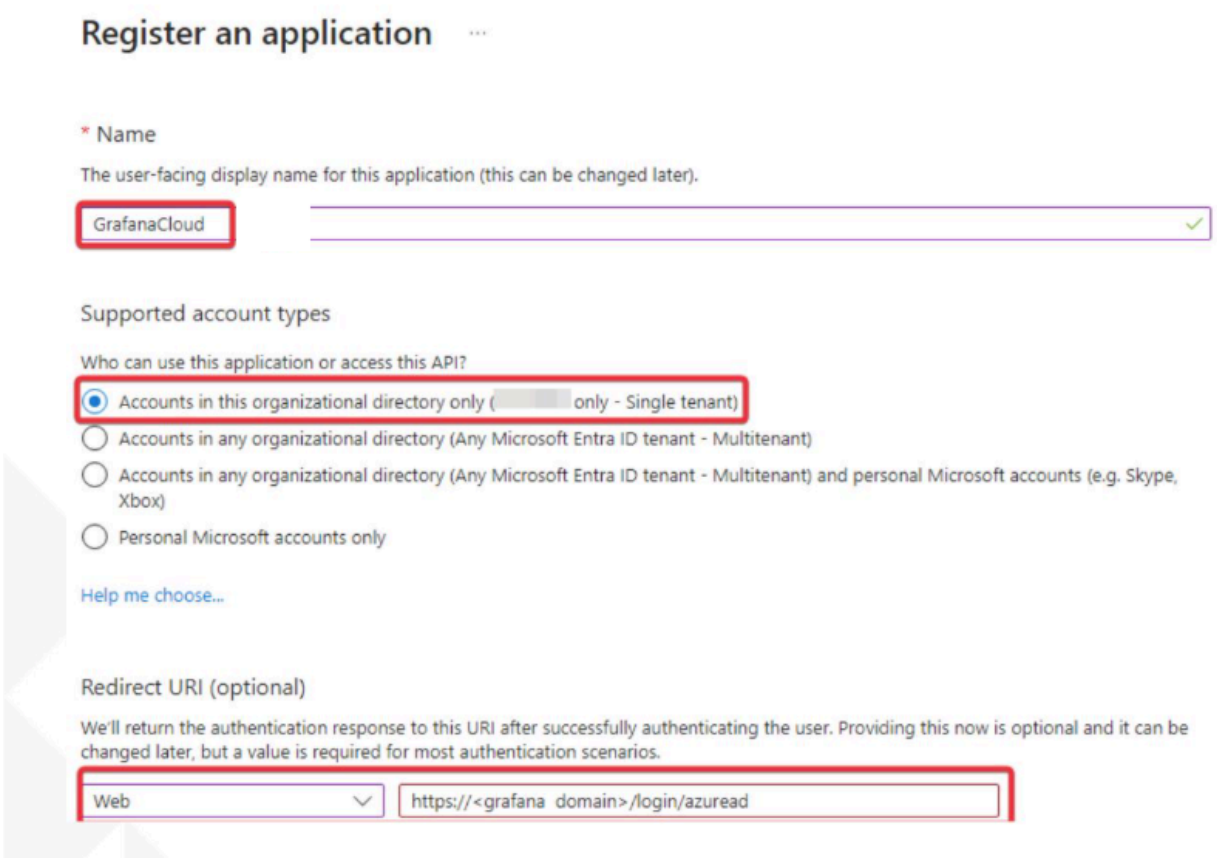
Copyright © 2024 Flexxible. Todos los derechos reservados.





6. Enter a name to register the application and select the compatible account type.

Copyright © 2024 Flexxible. Todos los derechos reservados.



7. In Redirect URI select *Web* and add the following redirect URL:

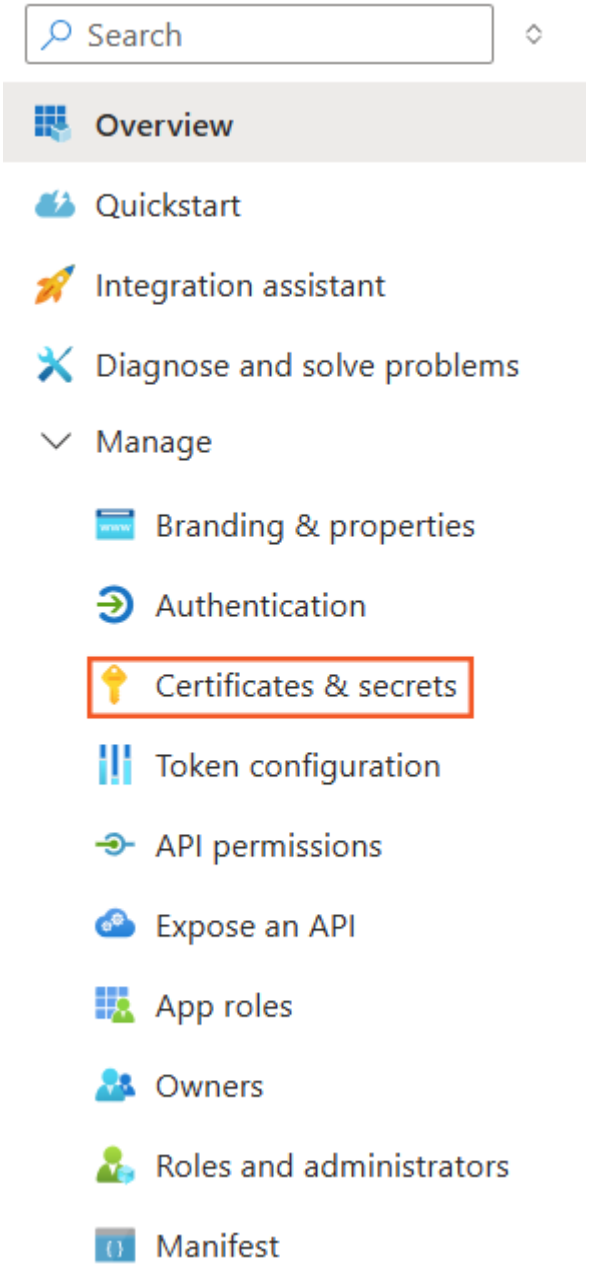
   `https://<grafana domain>/login/azuread`

8. Click `Register` to complete the application registration.

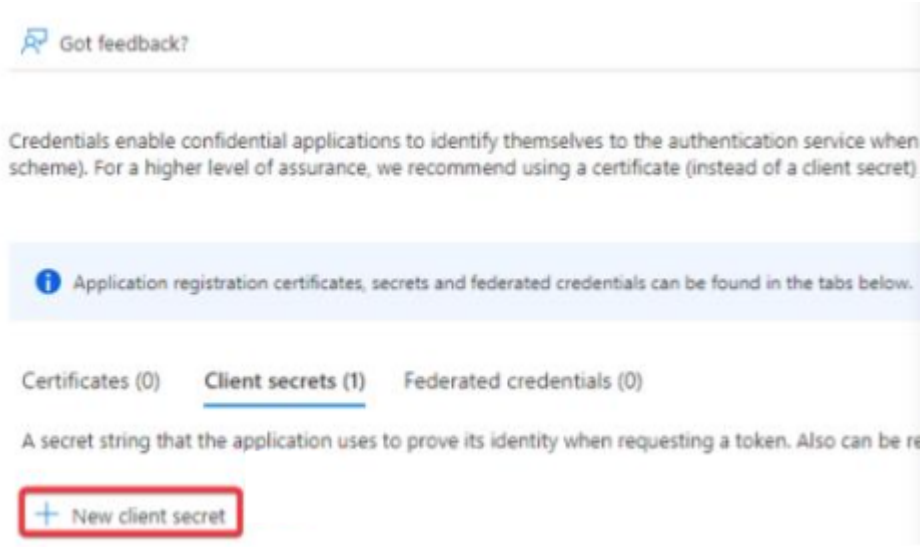
Create a client secret

1. Access `App registrations`.
2. In the registration menu, click on `Manage` -> `Certificates & Secrets` -> `New client secret`.

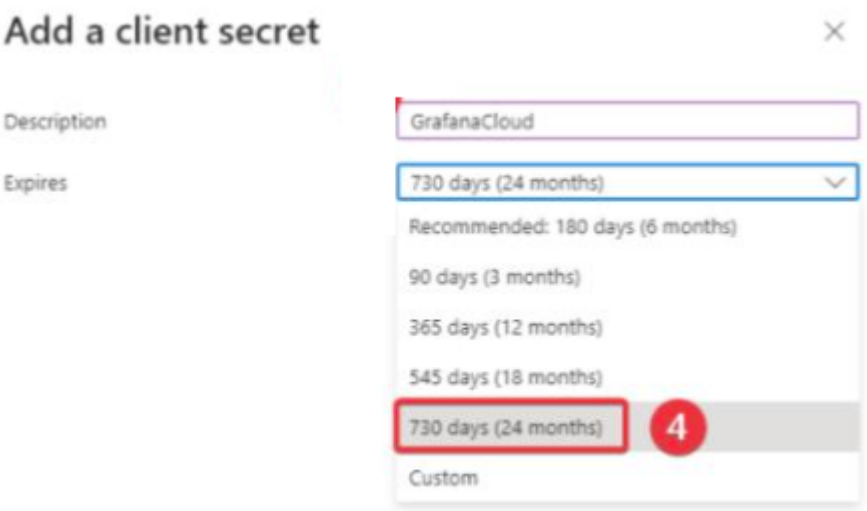
Copyright © 2024 Flexxible. Todos los derechos reservados.



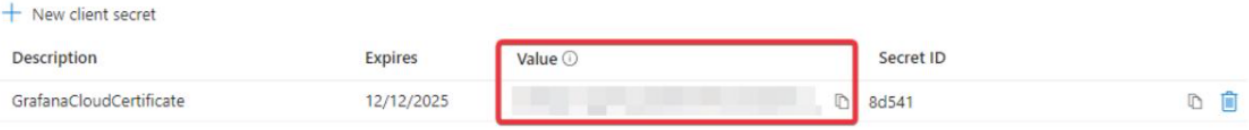
Copyright © 2024 Flexxible. Todos los derechos reservados.



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.

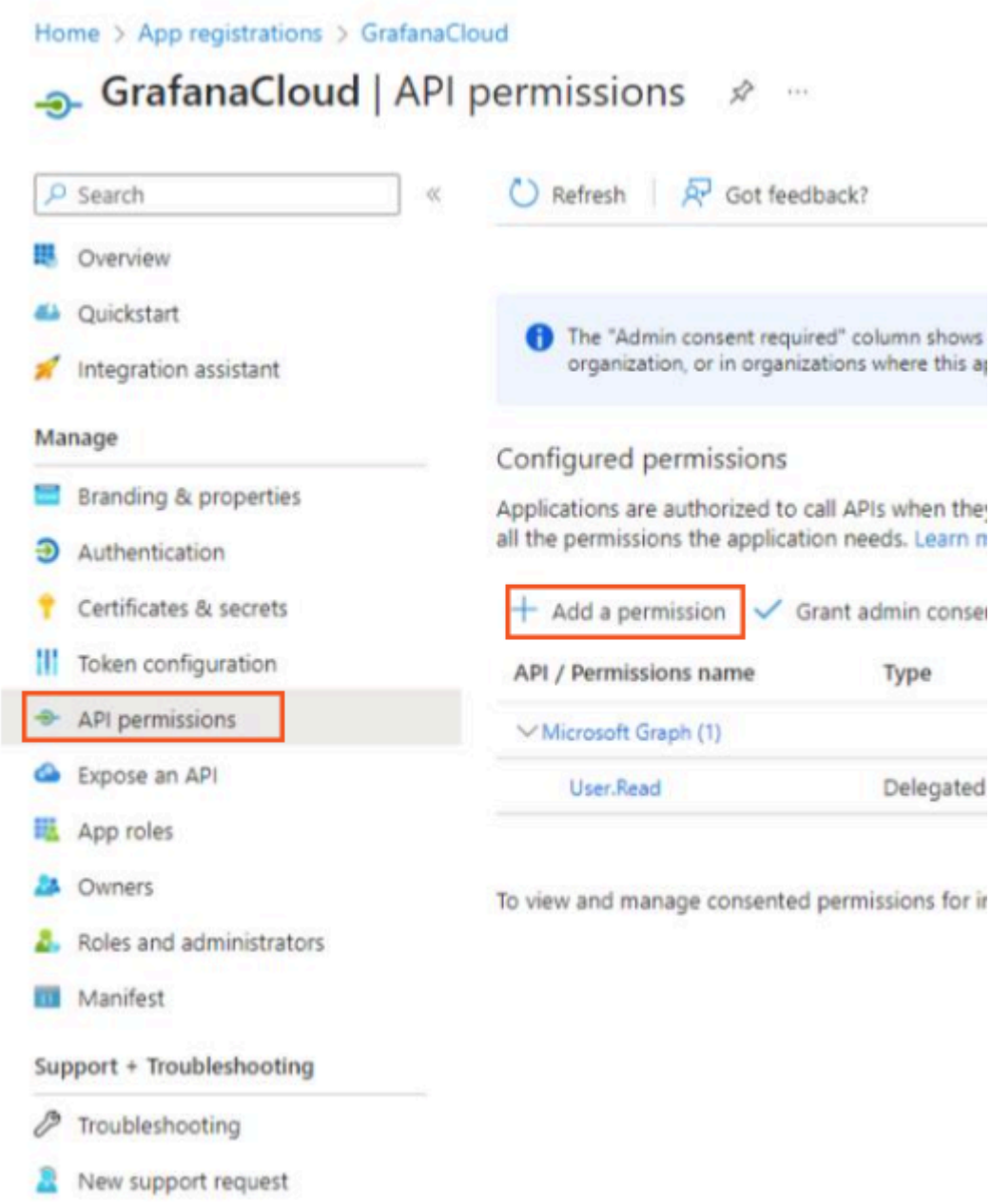


API permissions configuration

The necessary permissions for the API should be defined.

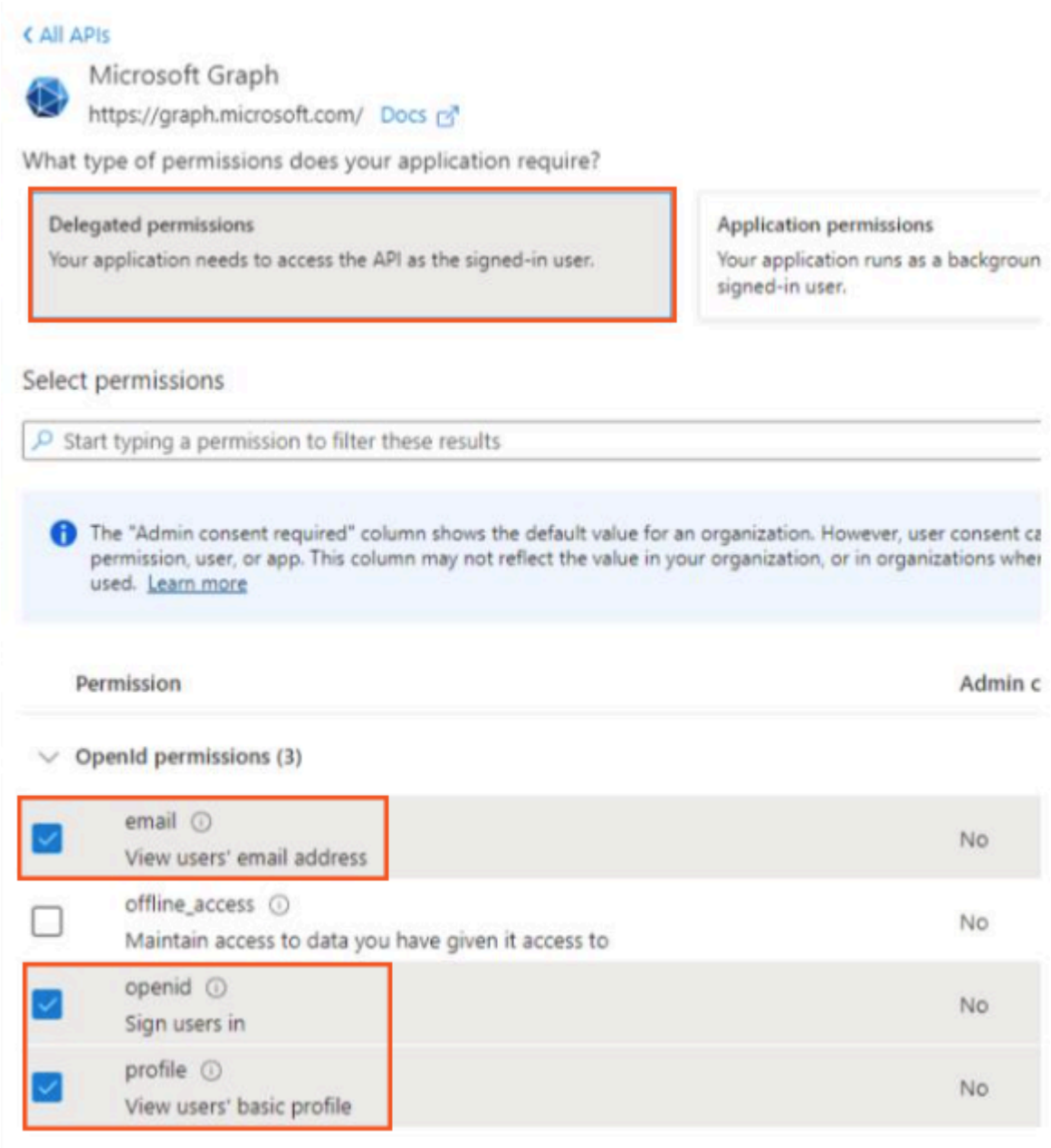
Copyright © 2024 Flexxible. Todos los derechos reservados.

1. Find the created application and in the menu click on `API Permissions` -> `Add a permission`.

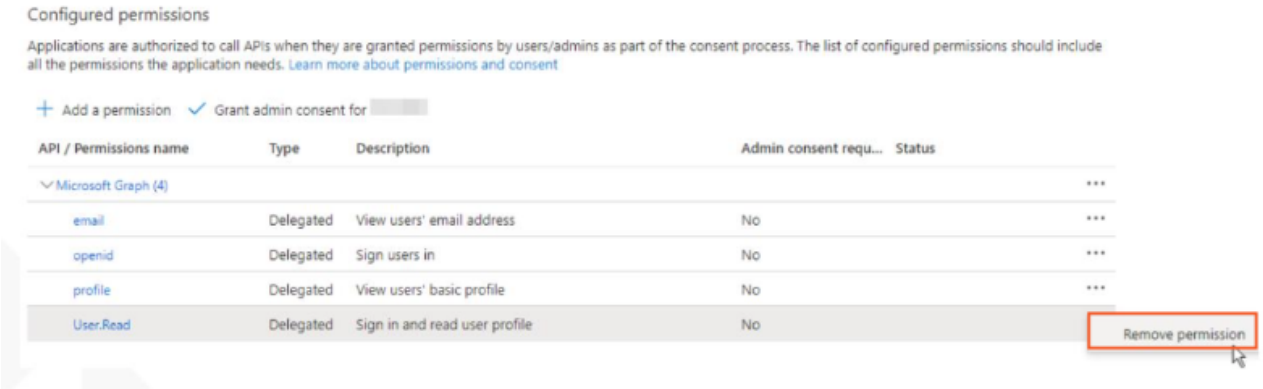


2. Click on `Microsoft Graph` -> `Delegated permissions`. Select `email`, `openid`, and `profile`.

Copyright © 2024 Flexxible. Todos los derechos reservados.

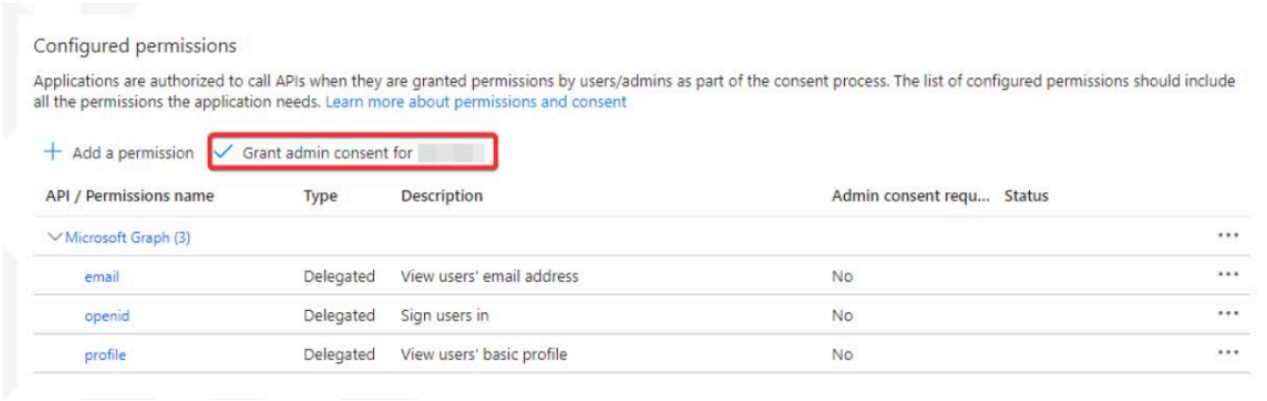


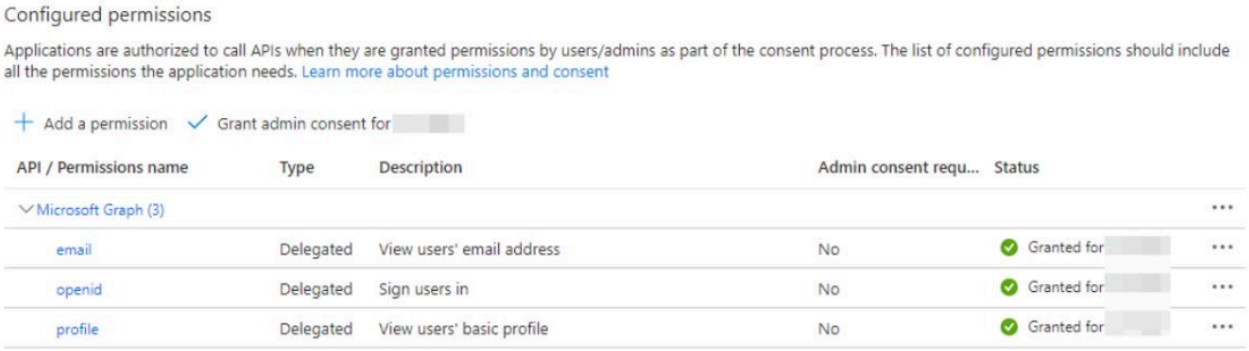
3. Once added, select the default created permission and click on `Remove permission`.



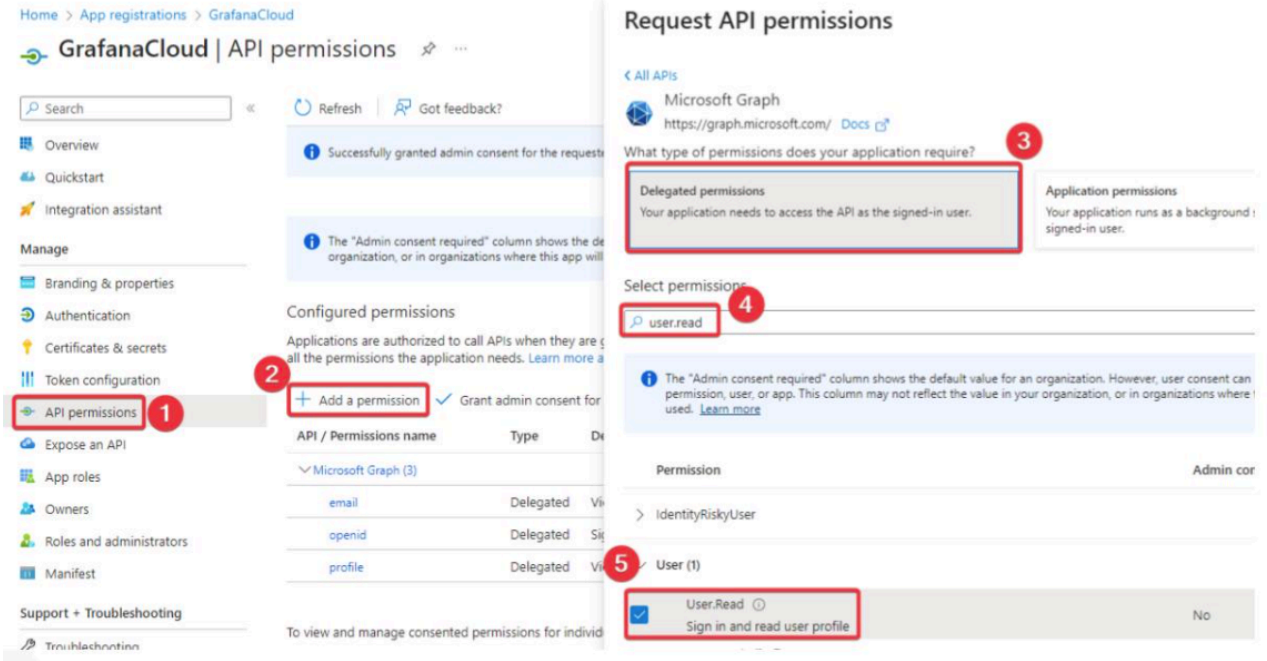
Copyright © 2024 Flexxible. Todos los derechos reservados.

4. Grant organizational permissions to `email`, `openid`, and `profile`.



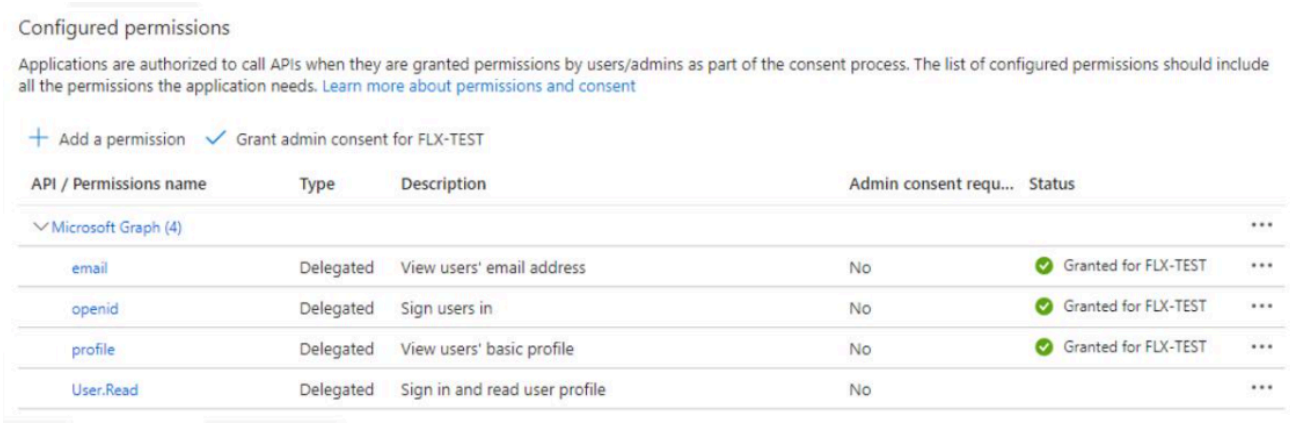


5. Find the `User.Read` permission and add it so it can perform profile reading only.



6. After the configuration is done, the image should look like the following:

Copyright © 2024 Flexxible. Todos los derechos reservados.


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`.

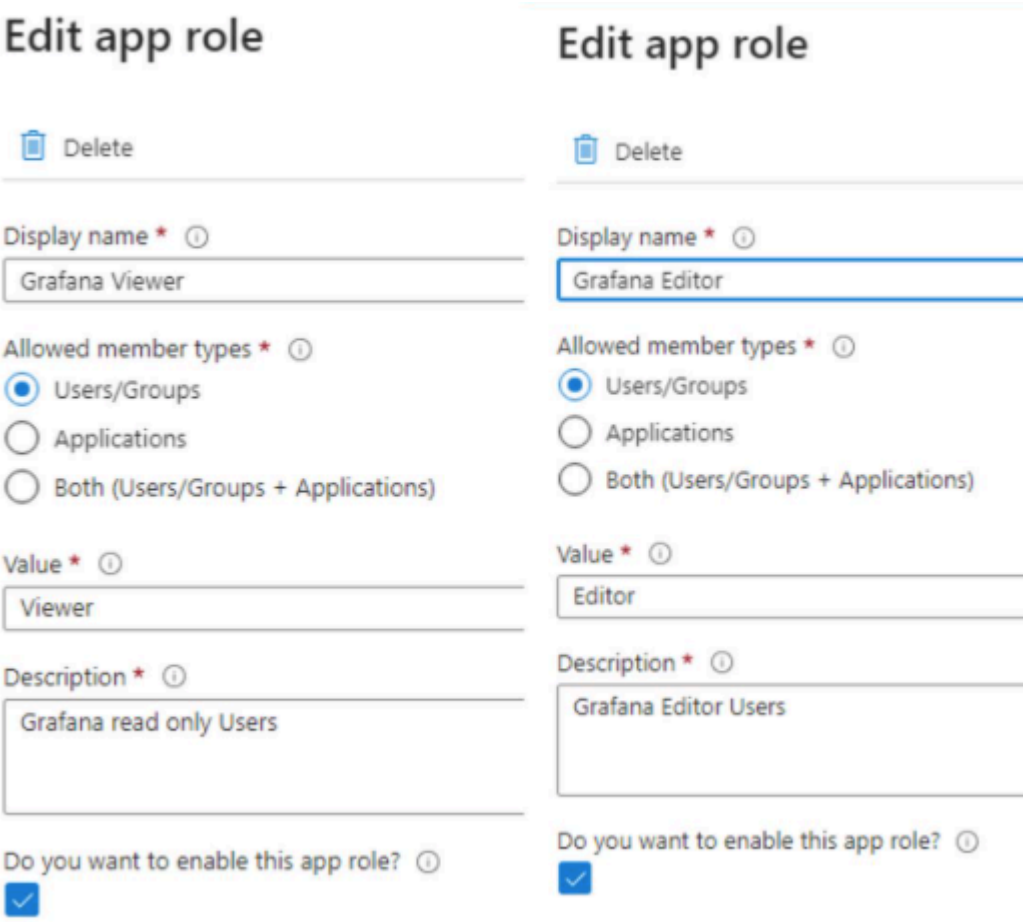
2. In the `Create application role` panel, configure each role.

   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:

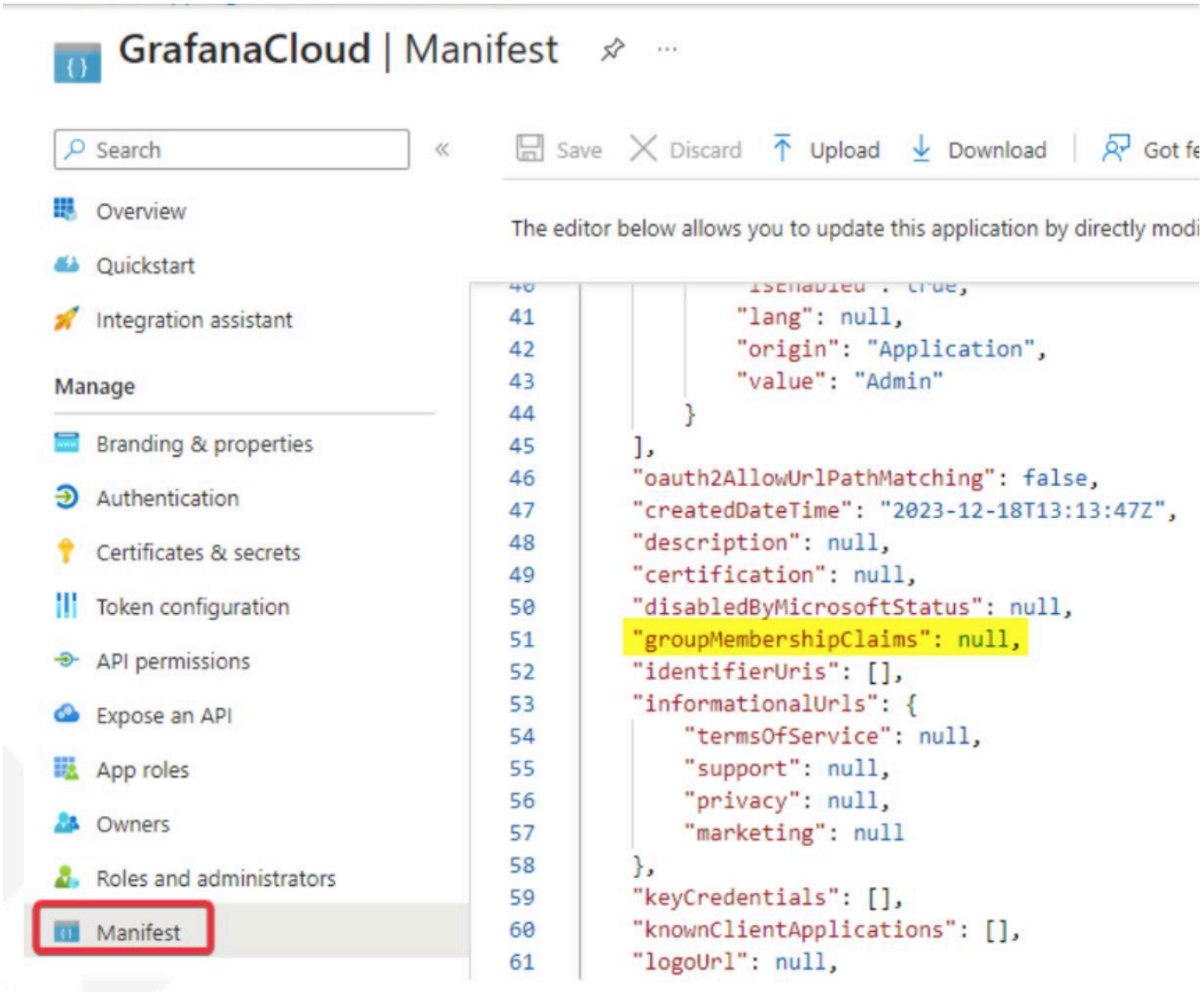
Copyright © 2024 Flexxible. Todos los derechos reservados.



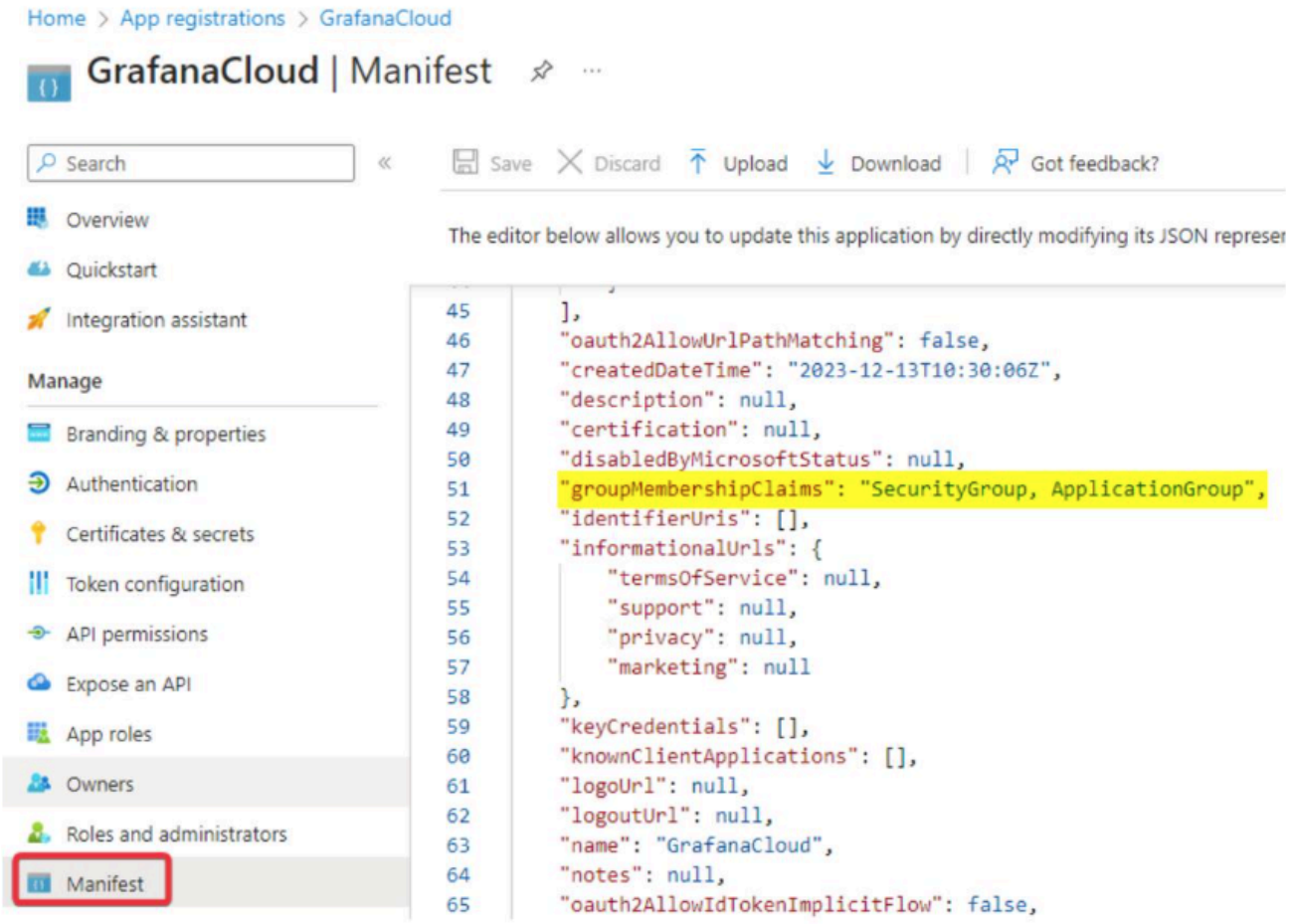
Review the manifest.xml file

The *manifest.xml* file must be reviewed to change the value of the key `"groupMembershipClaims"` from `null` (default value) to `"SecurityGroup, ApplicationGroup"`.

Copyright © 2024 Flexxible. Todos los derechos reservados.



Copyright © 2024 Flexxible. Todos los derechos reservados.



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

Copyright © 2024 Flexxible. Todos los derechos reservados.

- Group ID to be configured
- Domain to authorize

Copyright © 2024 Flexxible. Todos los derechos reservados.

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

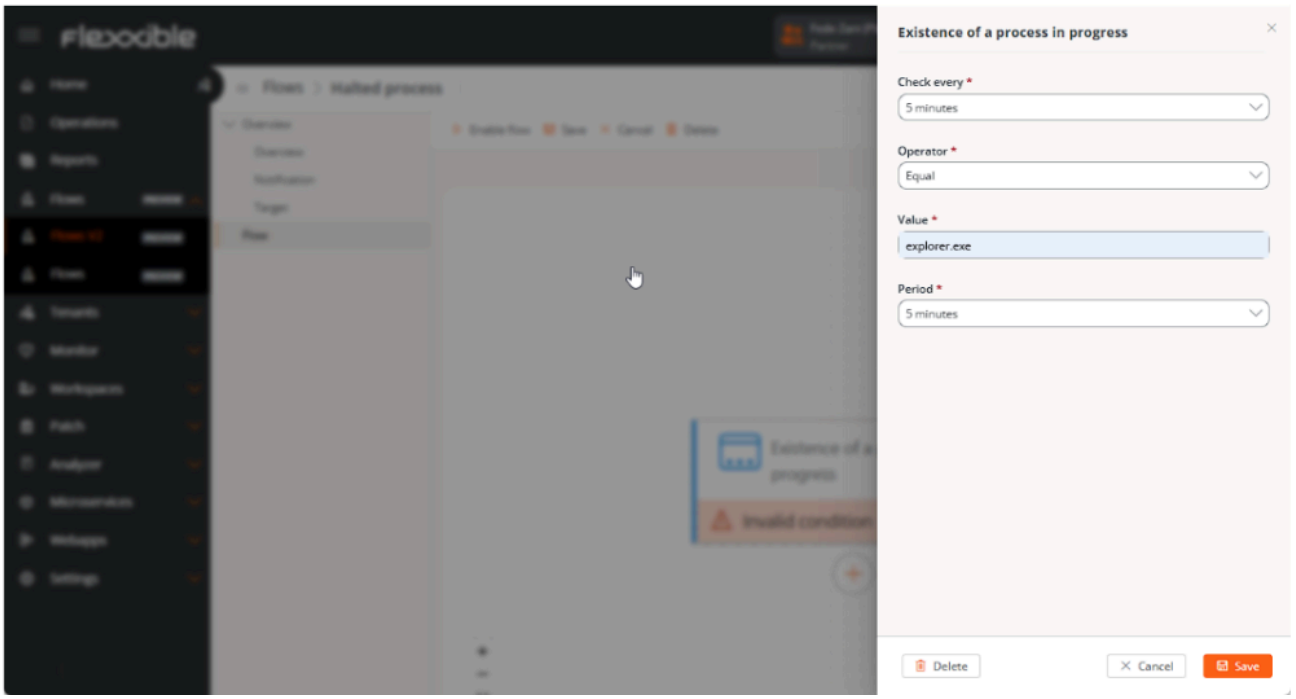
- Condition: User login.
- Action: Microservice execution.
- Maximum Recurrence: Once a day.

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

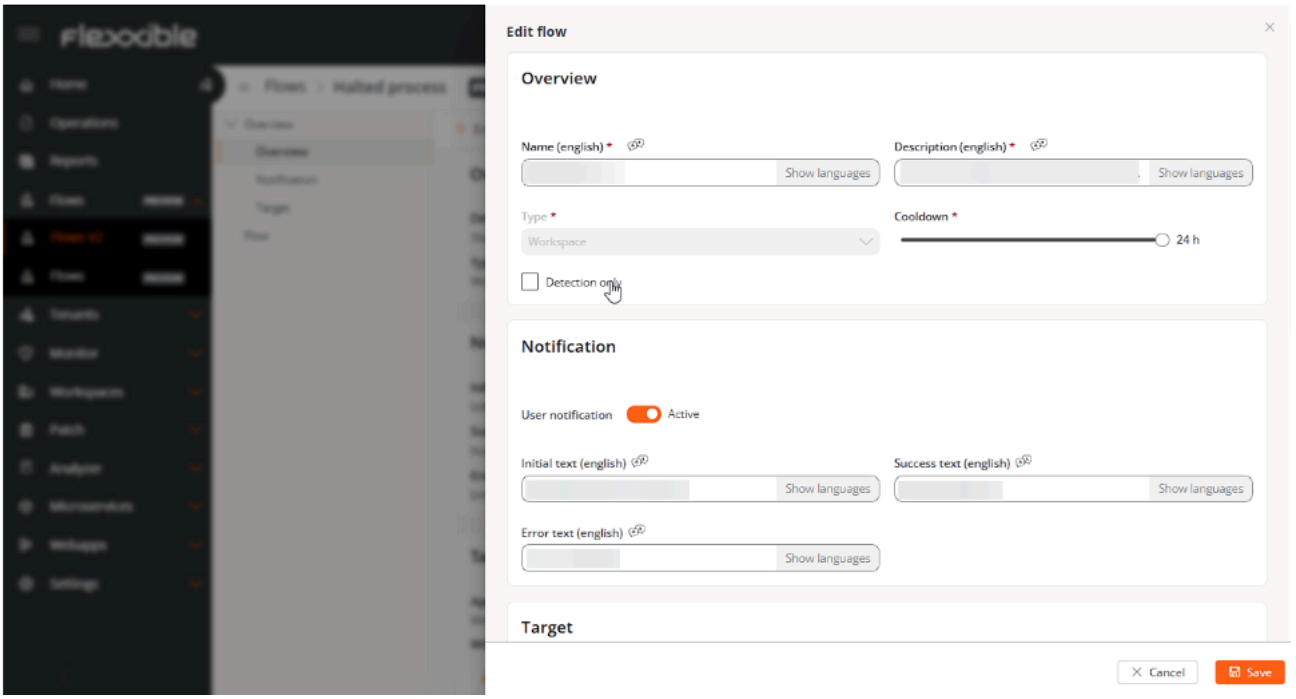


In the image above, the condition configuration indicates that every **5 minutes** (Check every), the existence of a process named **Equal** (Operator) to **explorer.exe** (Value) will be checked and verified if the process has been running for a minimum period of **5 minutes** (Period).

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.



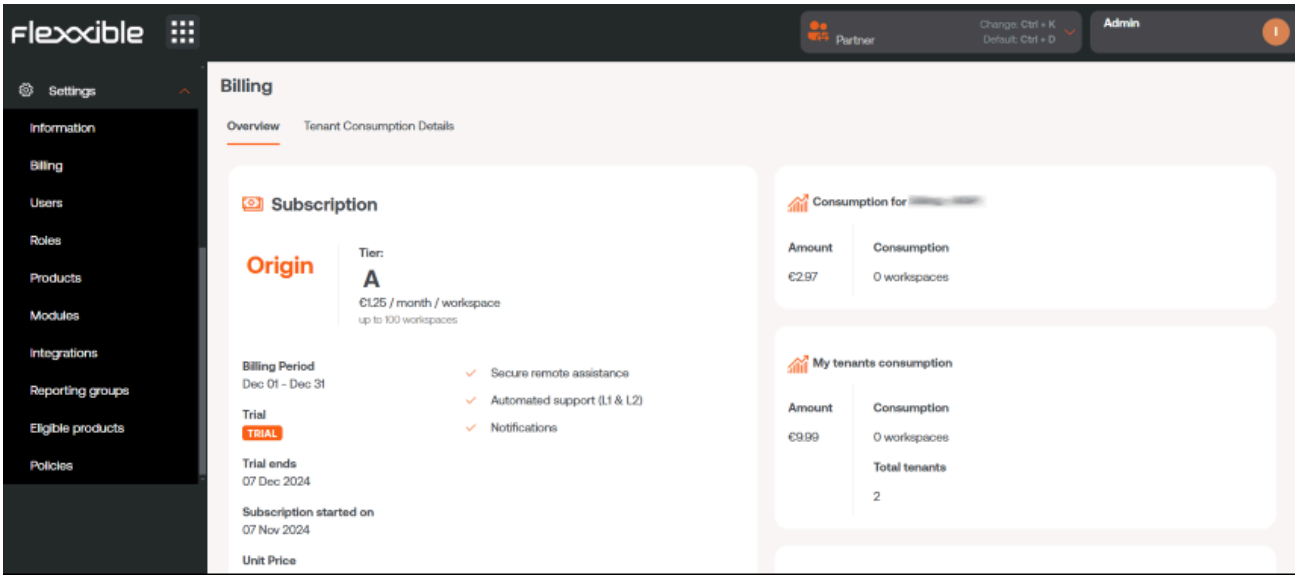
By setting a cooldown time, the flow will execute the action the first time the condition (login) is met but won't reactivate until 24 hours have passed since the last execution. This ensures that the microservice triggers at most once a day, fulfilling the required recurrence.

Copyright © 2024 Flexxible. Todos los derechos reservados.

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

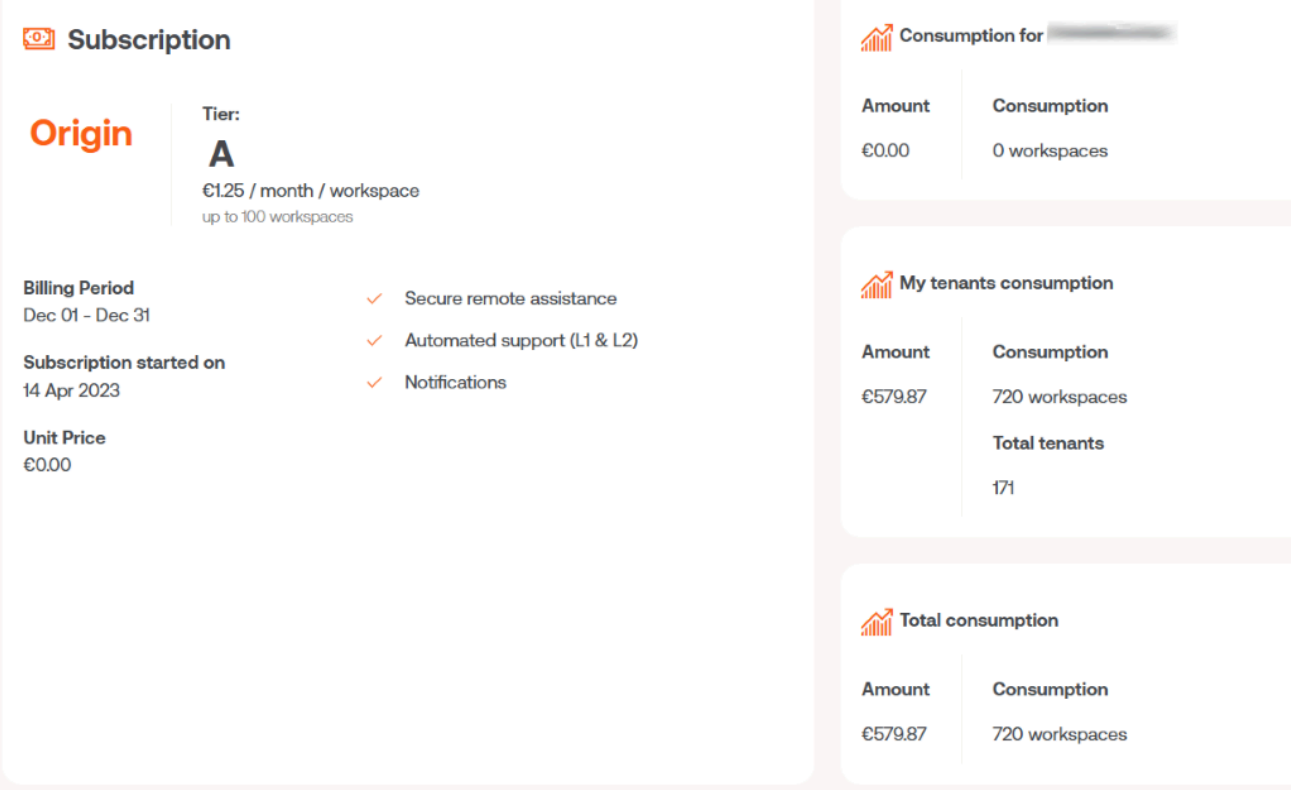
The `Billing` view for a user whose role is *Organization Administrator* in a partner-type organization presents two types of information:

- Overview
- Tenants consumption details

Overview

Copyright © 2024 Flexxible. Todos los derechos reservados.

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

> **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 remove it, see the steps to remove a device from a reporting 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.

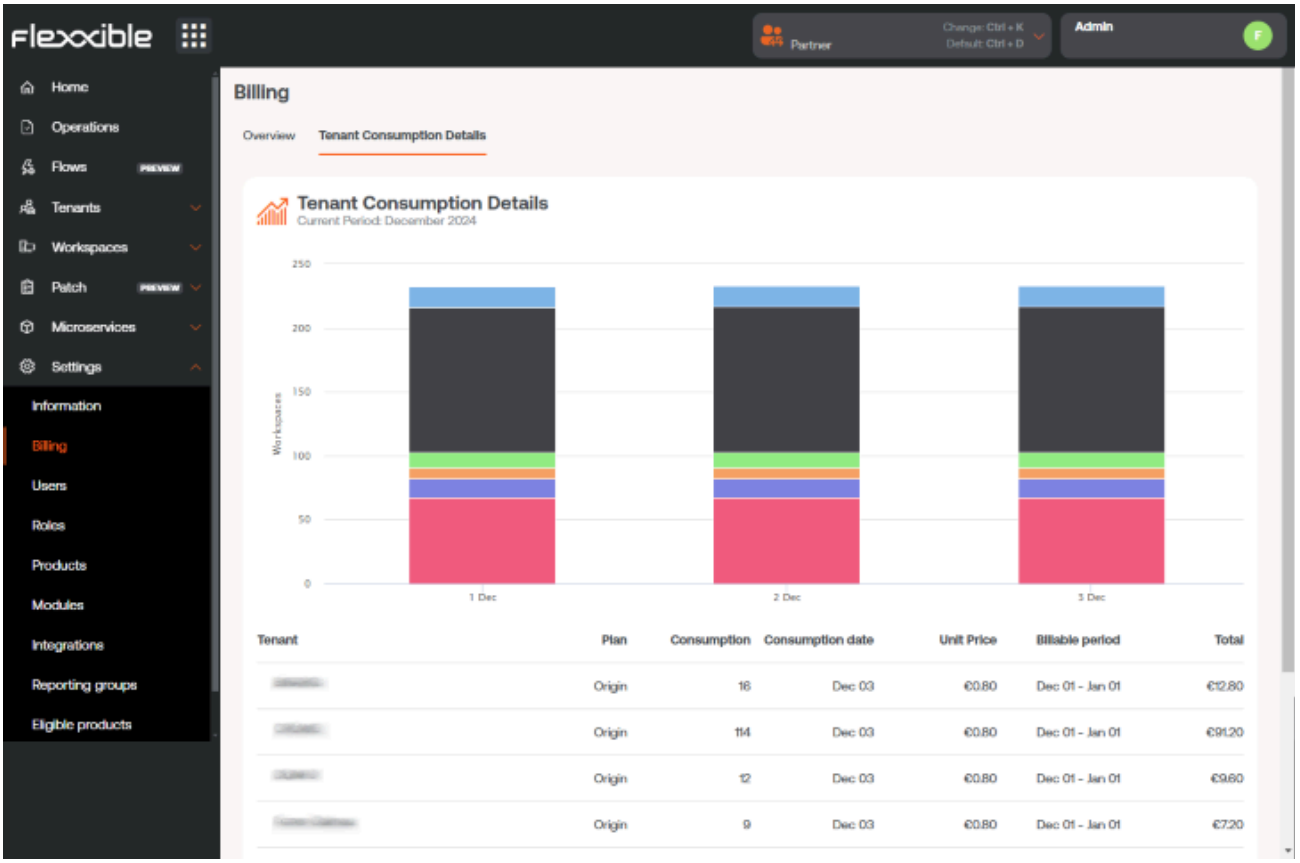
Tenants consumption details

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

Copyright © 2024 Flexxible. Todos los derechos reservados.



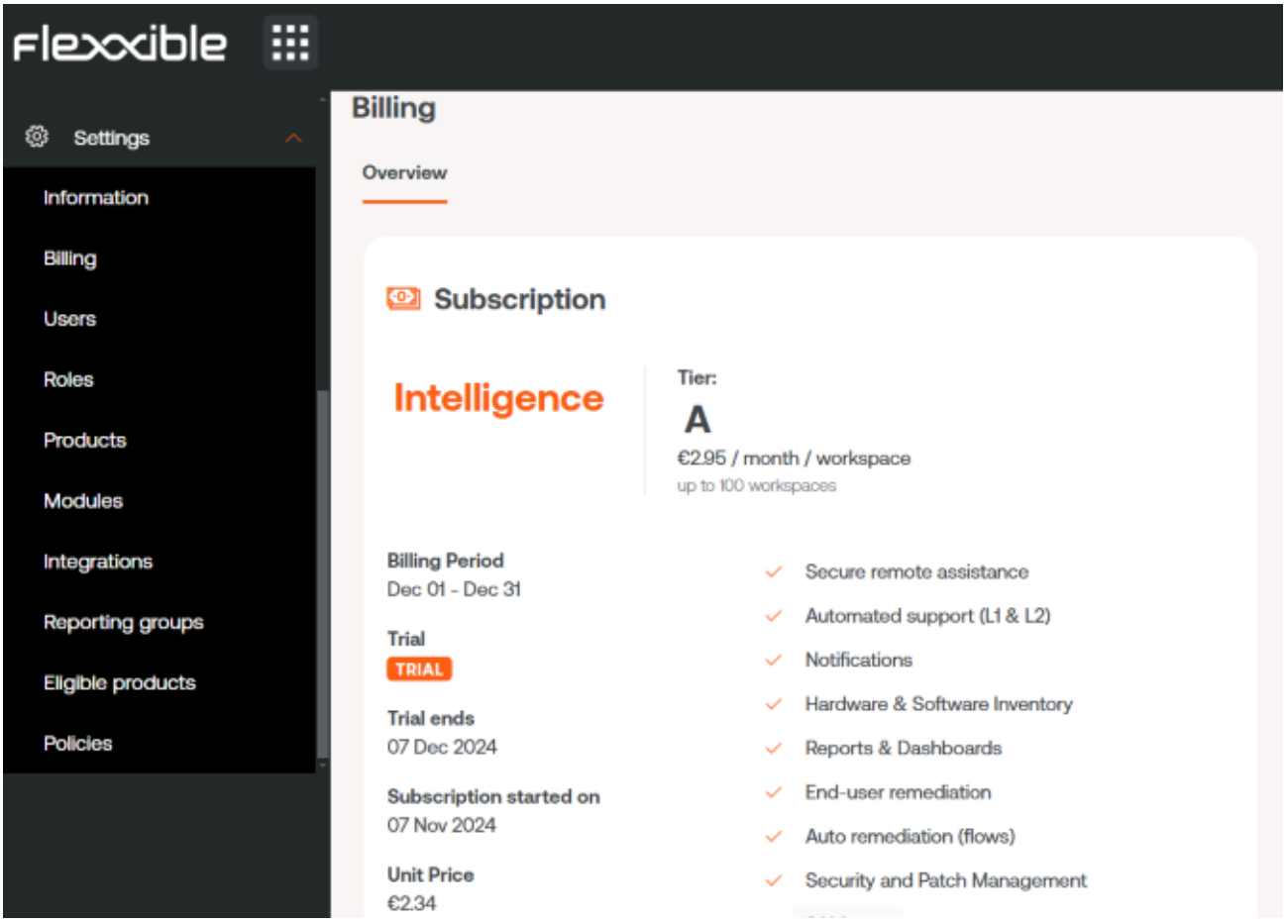
View from a client-type organization

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.



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.

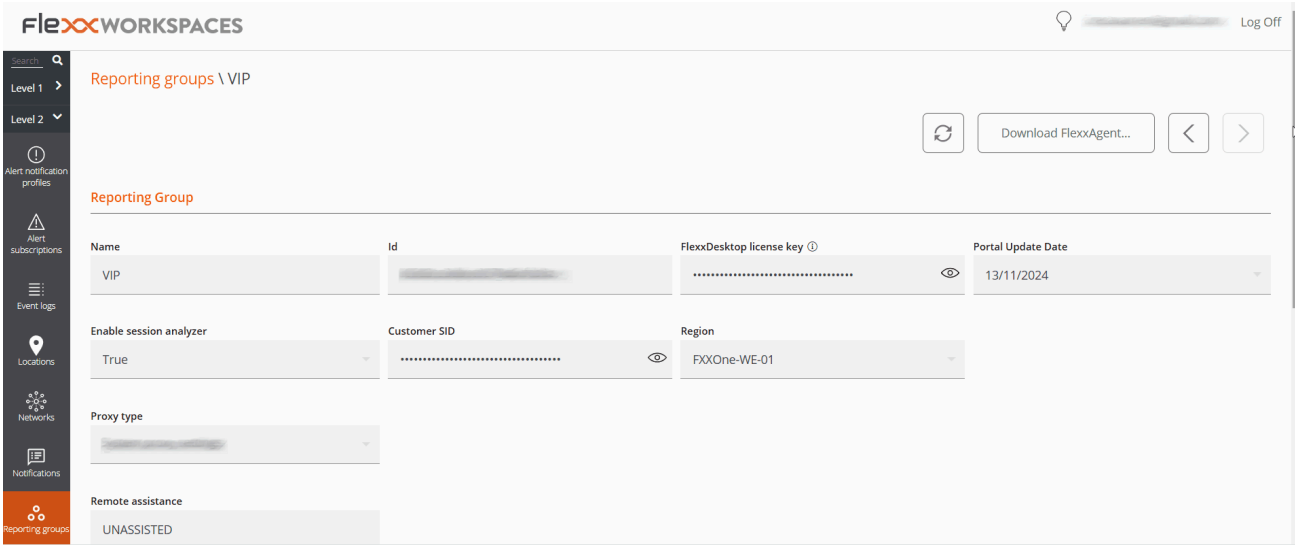
For a device to stop consuming at the billing level, it must not have FlexxAgent installed or belong to any reporting group. If FlexxAgent is not uninstalled from a device that is not in use, it will report to Workspaces again when it becomes active.

Copyright © 2024 Flexxible. Todos los derechos reservados.

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.

Steps to remove a device from a reporting group

- From the `Workspaces` module, go to `Level 2` -> `Reporting groups`.
- Click on the reporting group where the device you want to remove is located.
- On the `Devices` tab, select the device you want to remove.
- Go to `Operations` -> `Remove device`



Copyright © 2024 Flexxible. Todos los derechos reservados.

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:

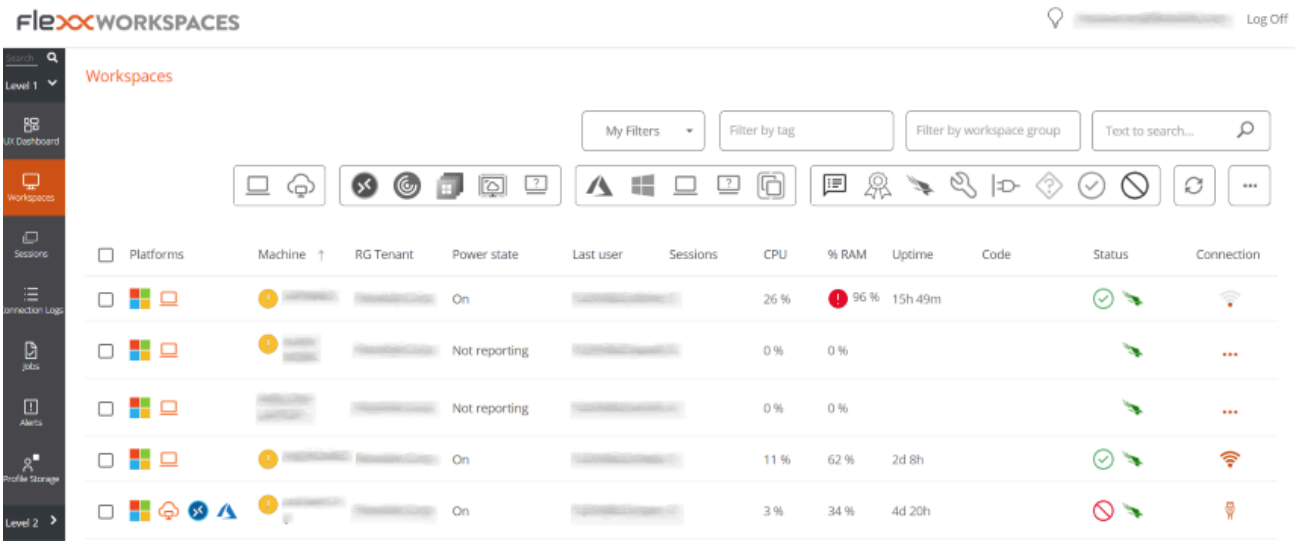
Copyright © 2024 Flexxible. Todos los derechos reservados.

- 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

Copyright © 2024 Flexxible. Todos los derechos reservados.

filtering of the columns.

Column sorting

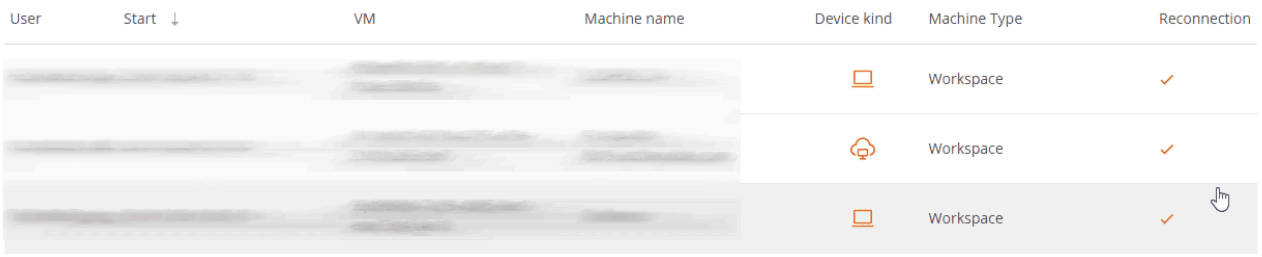
The options `Sort Ascending` and `Sort Descending` allow you to arrange the values of a column according to the letter or number they start with. For example, if the column `% RAM` is set to sort ascending, the column values will be arranged so that the first row corresponds to the device with the lowest 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.



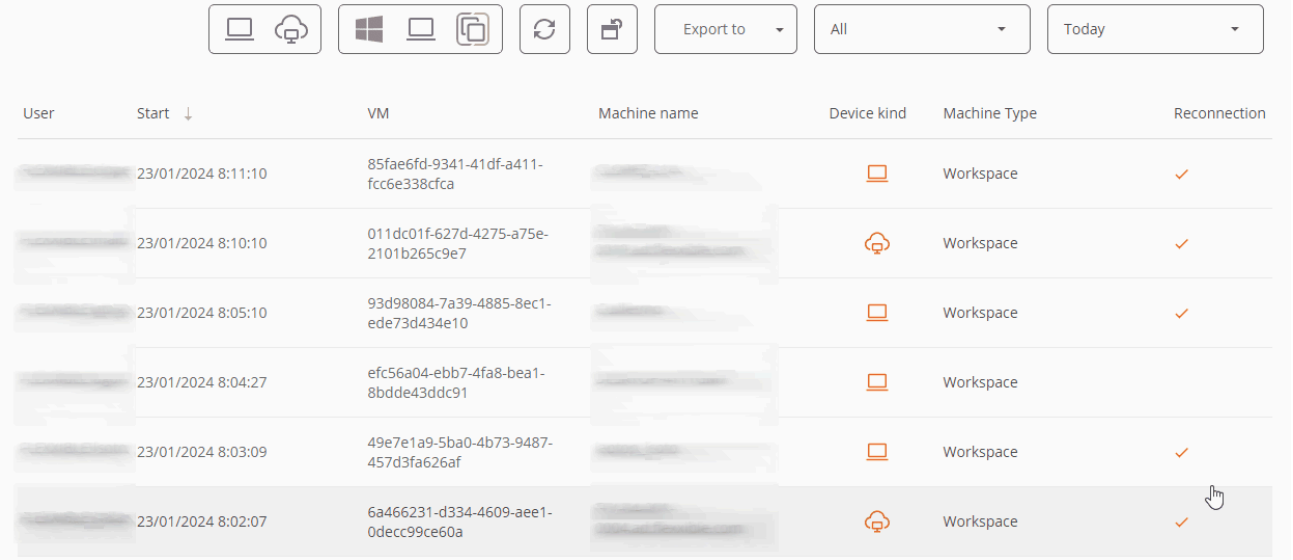
Column visibility

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

Copyright © 2024 Flexxible. Todos los derechos reservados.

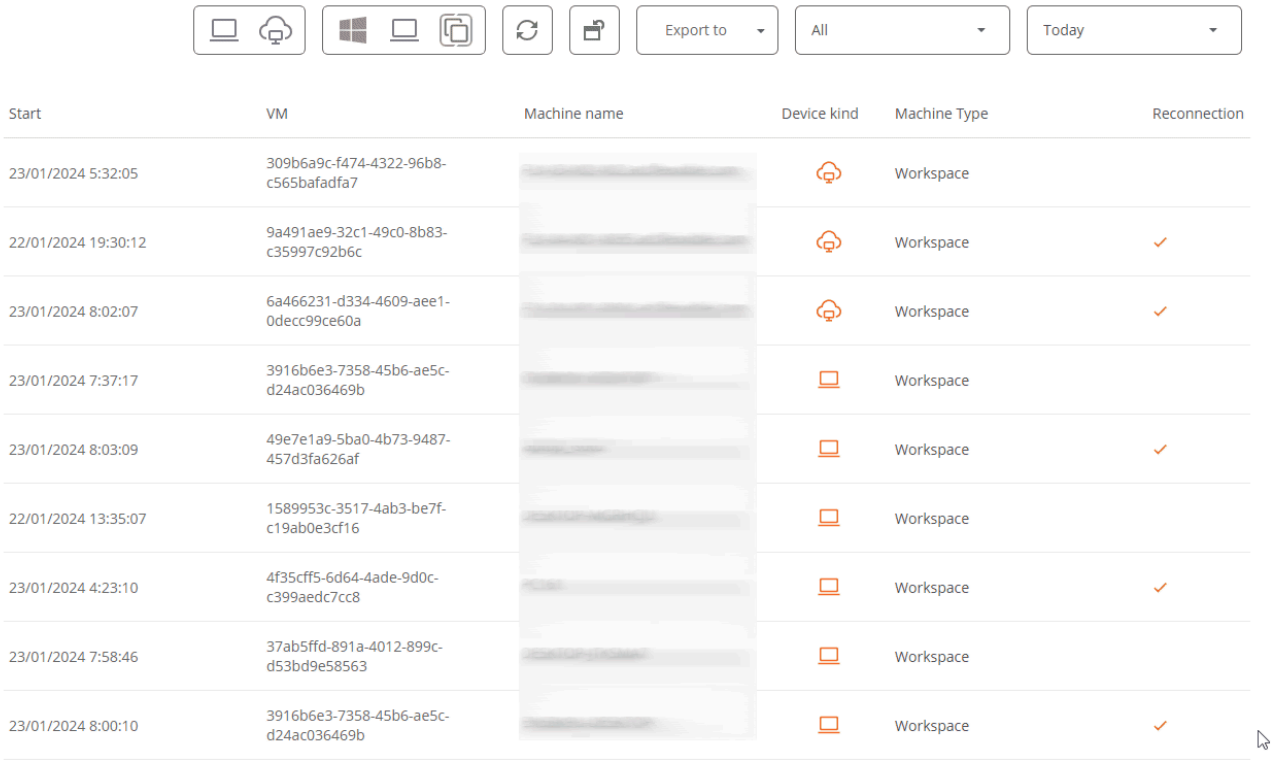
records they want to see in the table, they should click `Show customization dialog`, but if they prefer to add or remove columns, they can do so through the `Column selector`.



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.

Copyright © 2024 Flexxible. Todos los derechos reservados.



When the `Footer` option is selected, the total number of records found is displayed at the bottom left of the table.

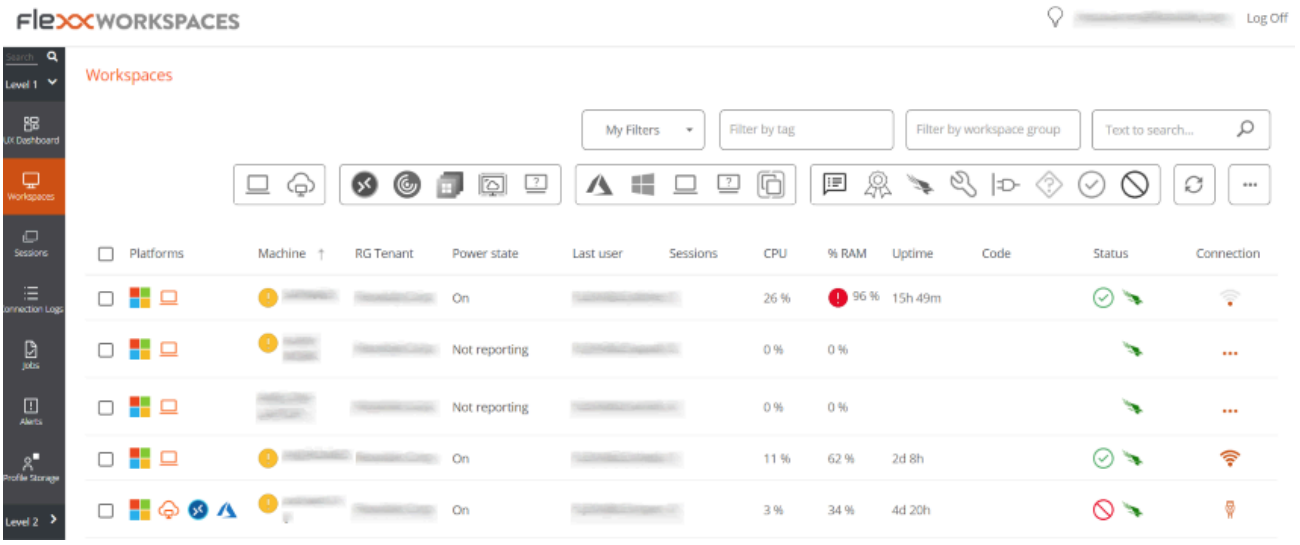
Detail Views

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

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.



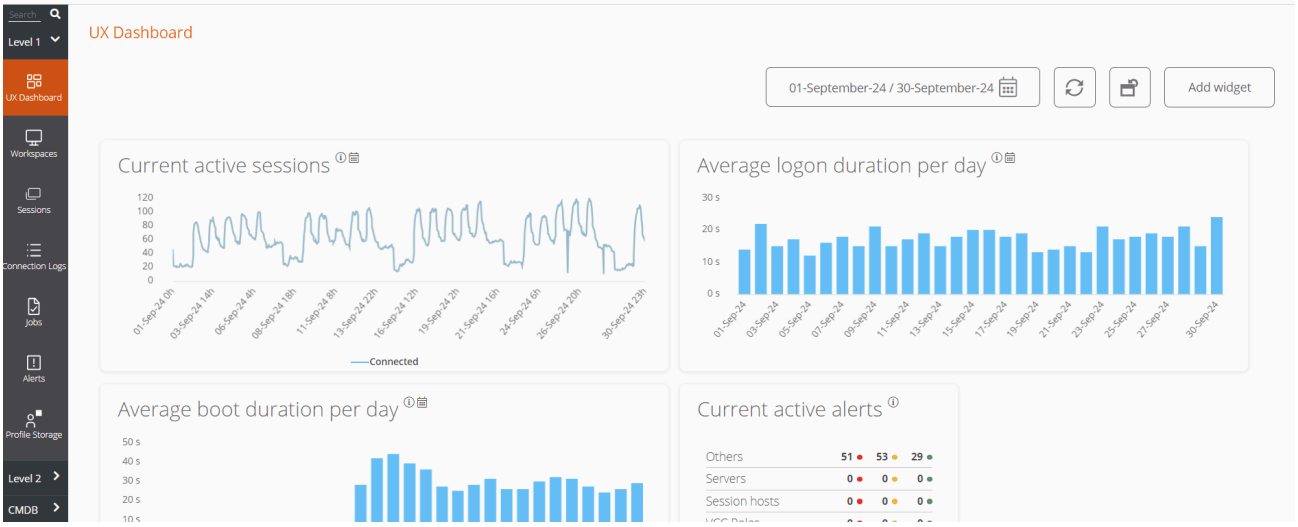
Functionalities available at this level:

- UX Dashboard
- Workspaces
- Sessions
- Connection Log
- Jobs

Copyright © 2024 Flexxible. Todos los derechos reservados.

Workspaces / Level 1 / UX Panel

The UX Panel section allows you to visually 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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

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

Copyright © 2024 Flexxible. Todos los derechos reservados.

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

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

Copyright © 2024 Flexxible. Todos los derechos reservados.

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.

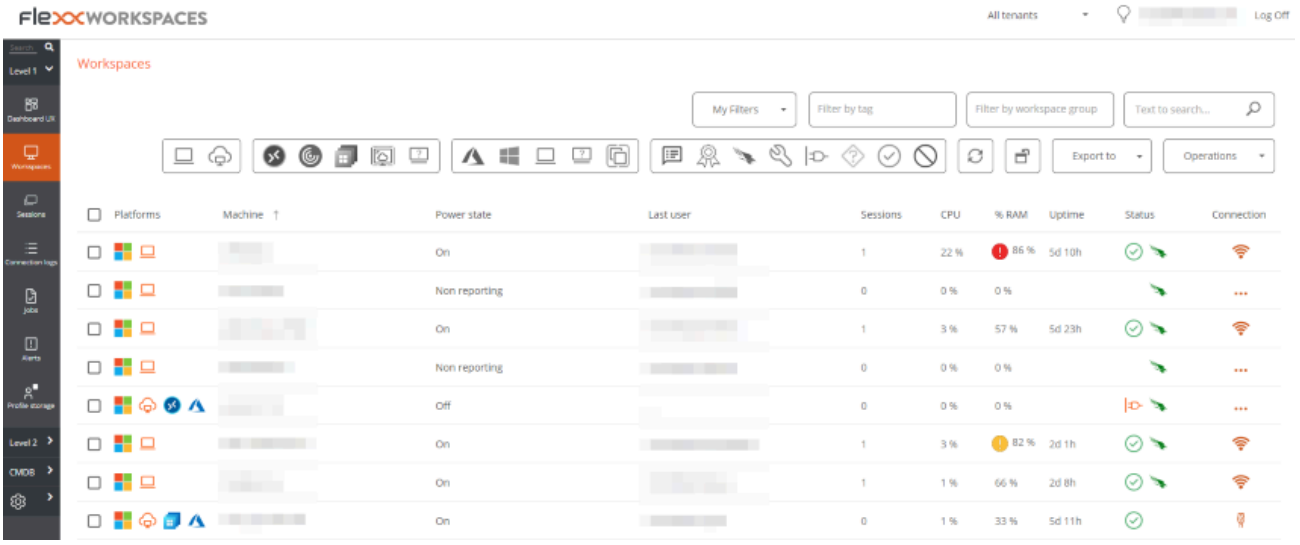
Workspaces by operating system and build number

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

Workspaces / Level 1 / Workspaces View

The Workspaces list view allows access to the list of devices that make up the organization. From there you can organize, filter, search, and send operations to the devices.



Filtering

The information displayed on the screen can be customized by adding or removing columns of information 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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

- 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*.

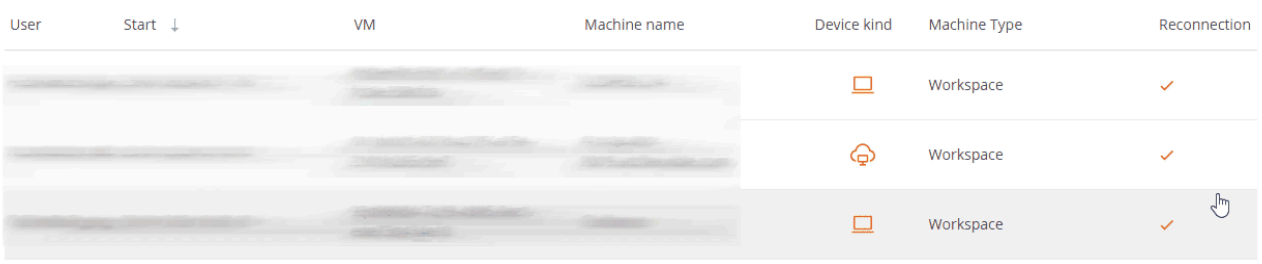
To reset the column sorting, click on `Clear sorting`.

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.

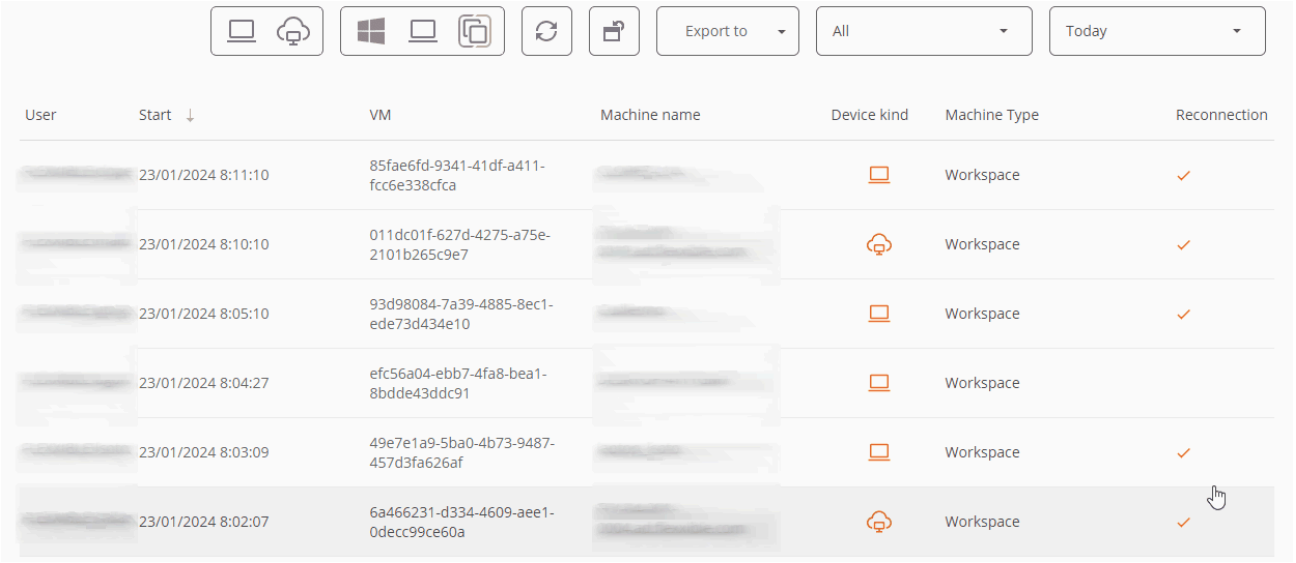
Copyright © 2024 Flexxible. Todos los derechos reservados.



Column visibility

The options `Hide column`, `Show customization dialog`, and `Column selector` allow modifying the column visibility in the table.

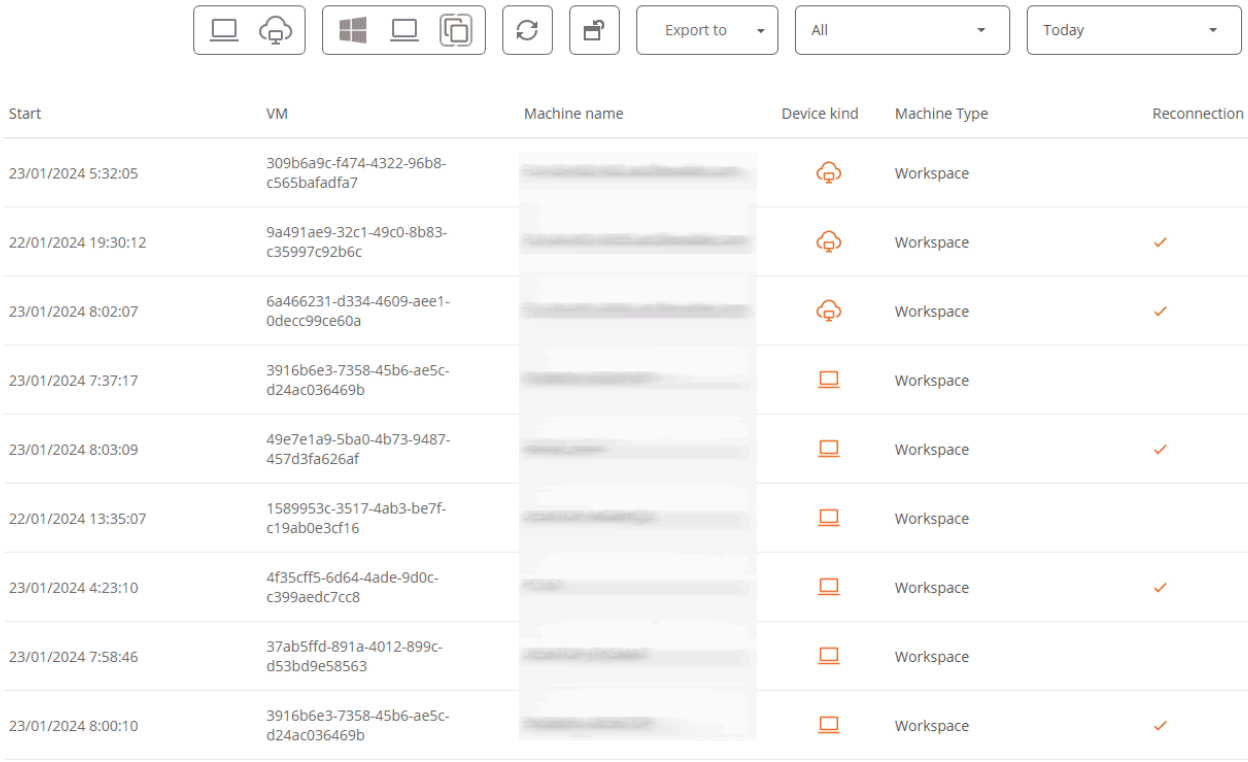
If the user doesn't want to see a specific column, they need to go to its header, right-click, and select the `Hide column` option. If they want to configure in detail the columns and records they want to see in the table, they should click `Show customization dialog`, but if they prefer to add or remove 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.

Copyright © 2024 Flexxible. Todos los derechos reservados.



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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

- **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.

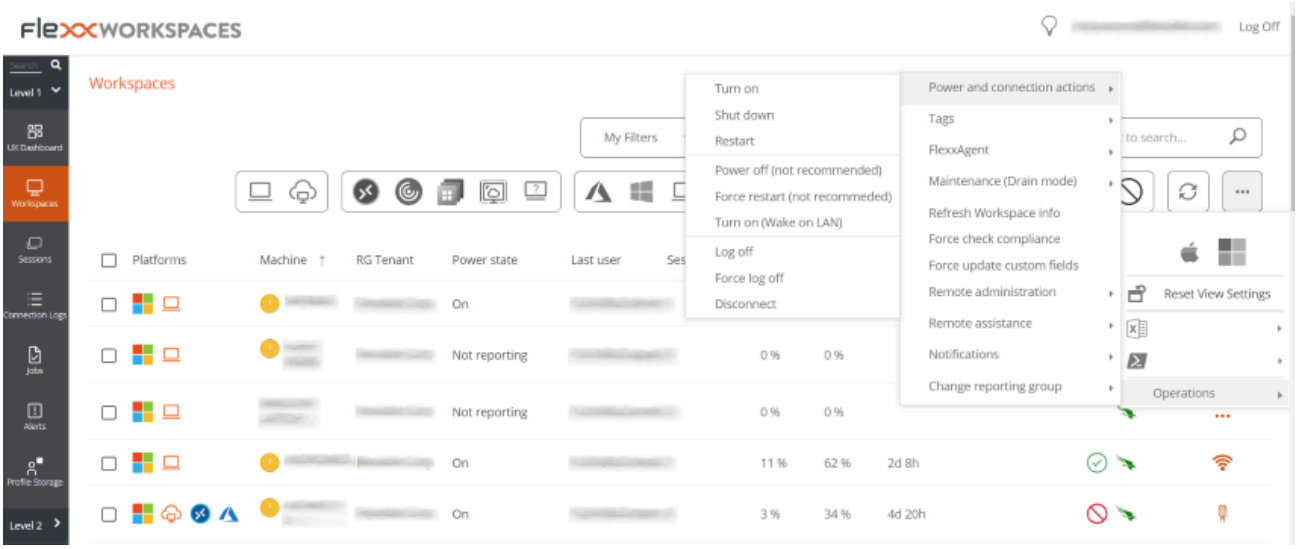
Microservices execution

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.



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.

Tags

Tags are keywords that can be assigned to one or more devices that share some common characteristic, in order to recognize and organize them for efficient management.

Copyright © 2024 Flexxible. Todos los derechos reservados.

To assign one or more tags, first select the devices and then click `Add` in `Operations`. From here, the available tags, if any, will be displayed so they can be associated with the device.

From `Edit` you can change the tag or assign another to the device. And `Delete` disassociates a tag from this.

The `Filter by tag` option in the top menu of the Workspaces list view allows filtering devices by tag name so that actions can be performed on them simultaneously.

FlexxAgent

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

Copyright © 2024 Flexxible. Todos los derechos reservados.

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`).

Remote Assistance

Allows launching three types of remote assistance:

- Interactive. Requires the user's consent to view and take control of their session.
- Unattended. Allows administrative access to server-type or self-service devices that do not necessarily have a user on the other side of the screen.
- Dynamic. Allows an operator to act on a device regardless of whether or not the user has an active session at that time.

> **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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

- **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:

- Remote Assistance configuration
- 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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

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`.

Copyright © 2024 Flexxible. Todos los derechos reservados.

Edit

This operation allows the user to assign an identification code to a device and/or a description.

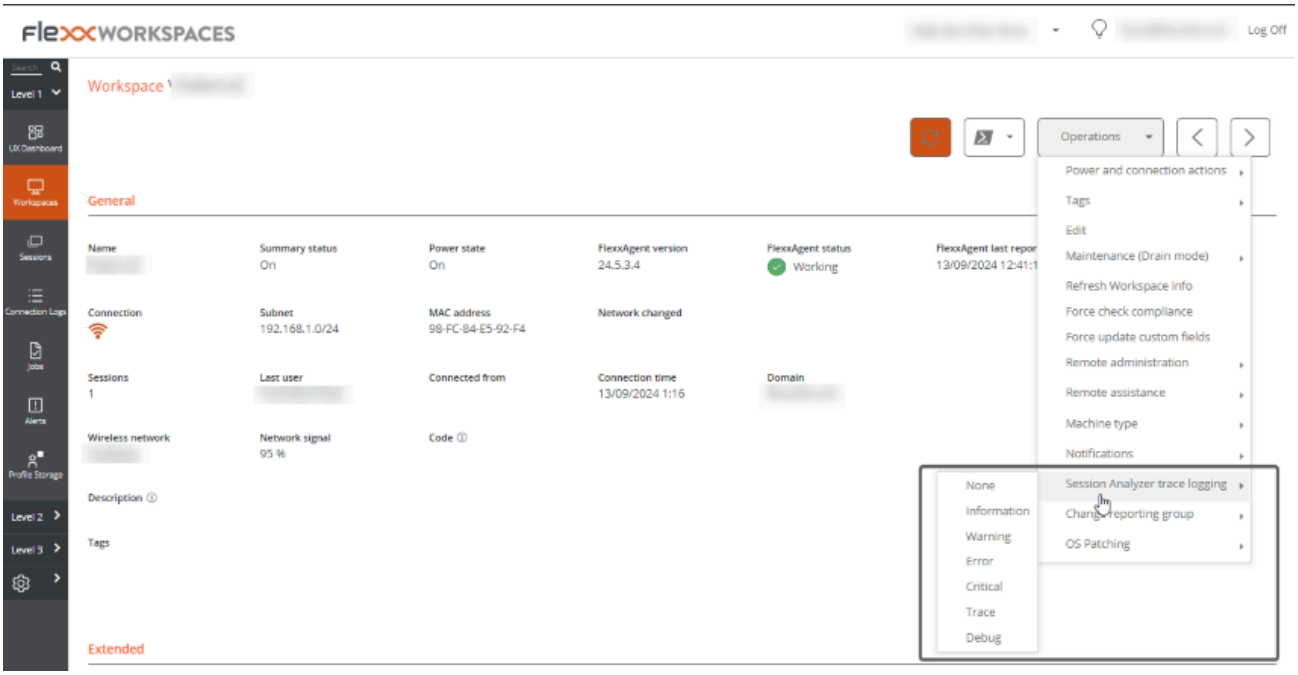
The code allows associating the device with an inventory item. To edit it, click on `Operations` -> `Edit` -> `Code`.

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.

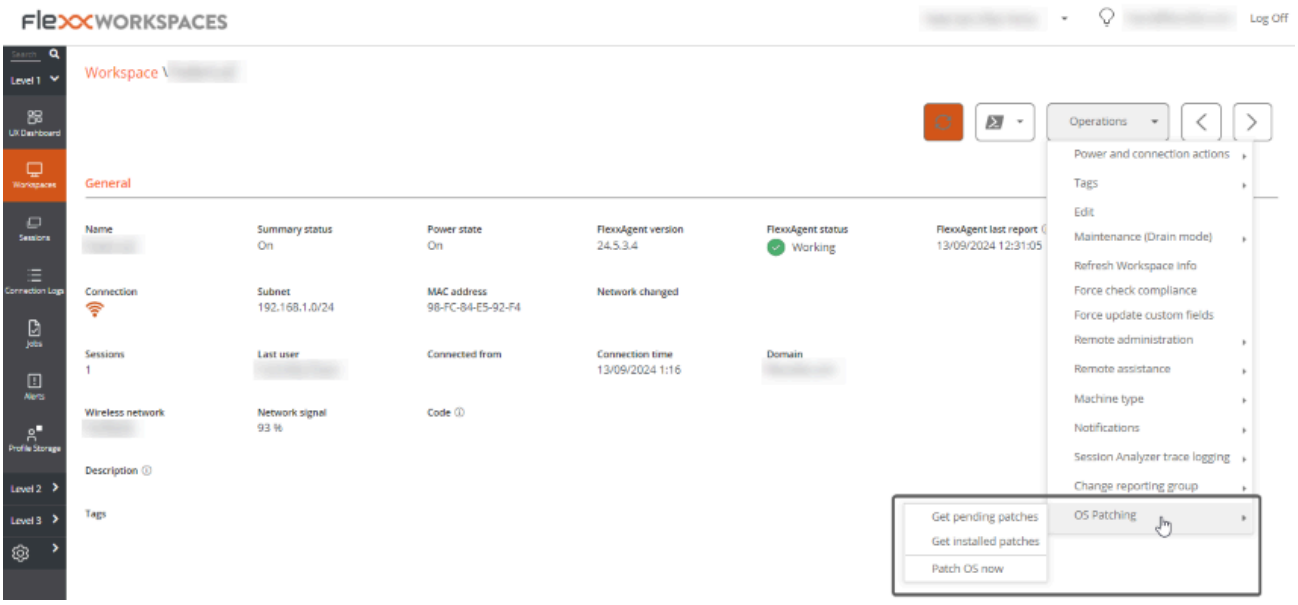


These logs are stored in the directory `%LOCALAPPDATA%\FAAgent\Logs`.

Operating system update

Copyright © 2024 Flexxible. Todos los derechos reservados.

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

Copyright © 2024 Flexxible. Todos los derechos reservados.

- Android

Copyright © 2024 Flexxible. Todos los derechos reservados.

Workspaces / Level 1 / Workspaces / Remote Assistance

Workspaces includes remote assistance tools so that an operator can efficiently access a device and take control of the user's session to solve problems and make system changes.

The operator can manage all the applications the user sees, including those requiring elevated permissions, launched with *Run as administrator* or executed under User Account Control (UAC).

Features

- It supports all types of sessions, such as users on physical devices, VDIs, shared desktops, and even in virtualized application environments.
- Remote assistance works with or without a proxy.
- It is designed to cover end-user devices and devices that do not have a user in front of them, like servers or kiosk-type customer service devices.
- It supports devices running Windows as an operating system.
- Thanks to its configuration options, it can be used for quick remote assistance sessions with users and as a remote access mechanism to infrastructure devices, like servers.

Privacy

To minimize the attack surface, exploit vulnerabilities, and maintain device security, FlexxAgent does not install any additional software, so there is no service "listening" for incoming connections. The process runs only (without installation) in real-time when requested from Workspaces.

During remote assistance, default audio redirection is disabled, preventing the operator from hearing any conversation when the user is on a video call.

Copyright © 2024 Flexxible. Todos los derechos reservados.

Types of remote assistance

There are three types of remote assistance:

- Interactive remote assistance
- Unattended remote assistance
- Dynamic remote assistance

Interactive remote assistance

Interactive remote assistance is aimed at end users. Allows a support operator to access the user's session to see what is happening on their screen or take control easily. This type of assistance requires user consent.

Unattended remote assistance

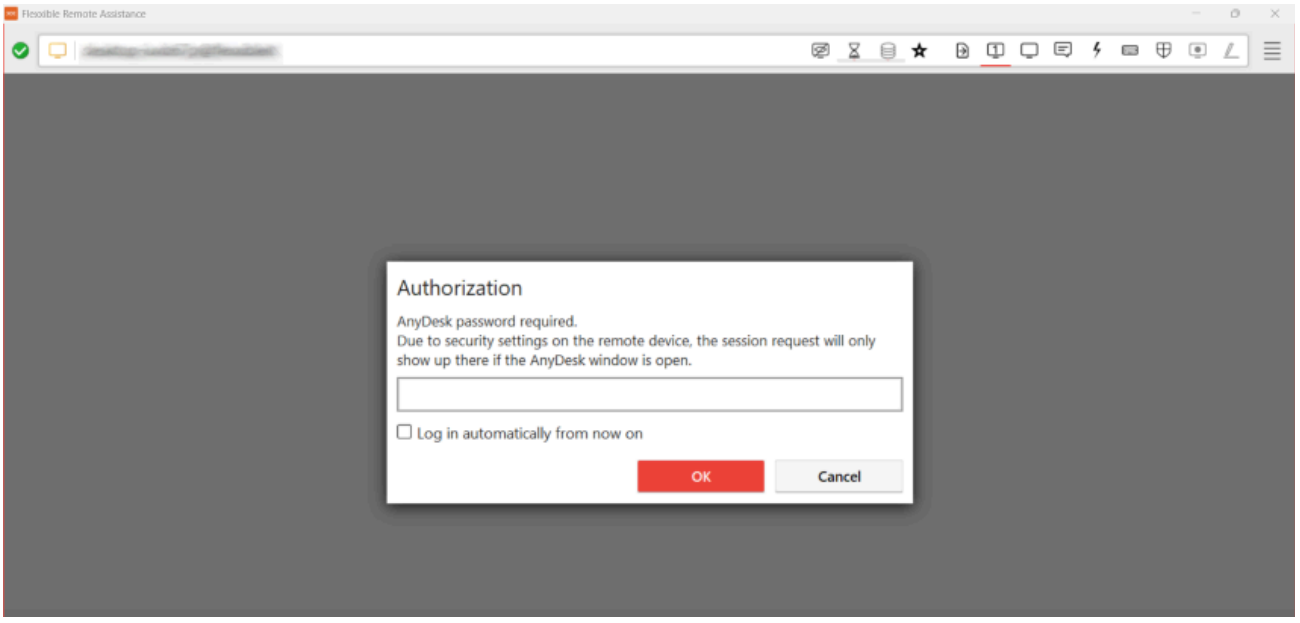
Unattended remote assistance allows access to server type or self-service kiosk computers, where no specific user is working.

Copyright © 2024 Flexxible. Todos los derechos reservados.

When the operator performs this action, Workspaces sends the order to FlexxAgent to install a custom Flexxible service, start it up, set up an access password, and inform the operator through the console that the session is already accessible with its respective authentication data:

- **Session ID.** Session identifier.
- **Password.** Dynamic password that regenerates every session. It's not recommended to store it.
- Download the remote assistance access file for the operator.

Copyright © 2024 Flexxible. Todos los derechos reservados.



Once the access file is activated by the support operator, you will need to enter the session password to take control of the device.

> **INFO**
>
> After 15 minutes since the end of the unattended remote assistance connection, it will no longer be possible to reuse the same authentication data or access file. The service will be deactivated from the device and the session password will have expired.

Dynamic remote assistance

Dynamic remote assistance allows an operator to act on a device regardless of whether the user has an active session at that time.

When a dynamic remote assistance is launched, FlexxAgent checks the active sessions on the device; if there is any, it launches the interactive remote assistance process. On the contrary, if there is no user session active, it will trigger the unattended remote assistance process, allowing the operator to access the device to perform maintenance tasks, even using other user accounts to log in, without interfering with the user's session or data.

Copyright © 2024 Flexxible. Todos los derechos reservados.

> **INFO**
>
> When a device is configured to receive dynamic remote assistance, the operator will not have the option to launch an unattended remote assistance process on any session of the device from the `Sessions` view.

To receive dynamic remote assistance, the device receiving the assistance must have version 24.9.2 or higher of FlexxAgent installed.

Although the reporting group to which the device belongs has been configured to receive **dynamic remote assistance**, Workspaces will display the three options to start remote assistance: interactive, unattended, and dynamic. In that specific case, the operator will not be able to activate interactive or unattended remote assistance. If attempted, Workspaces will display an error message.

Requirements to perform remote assistance

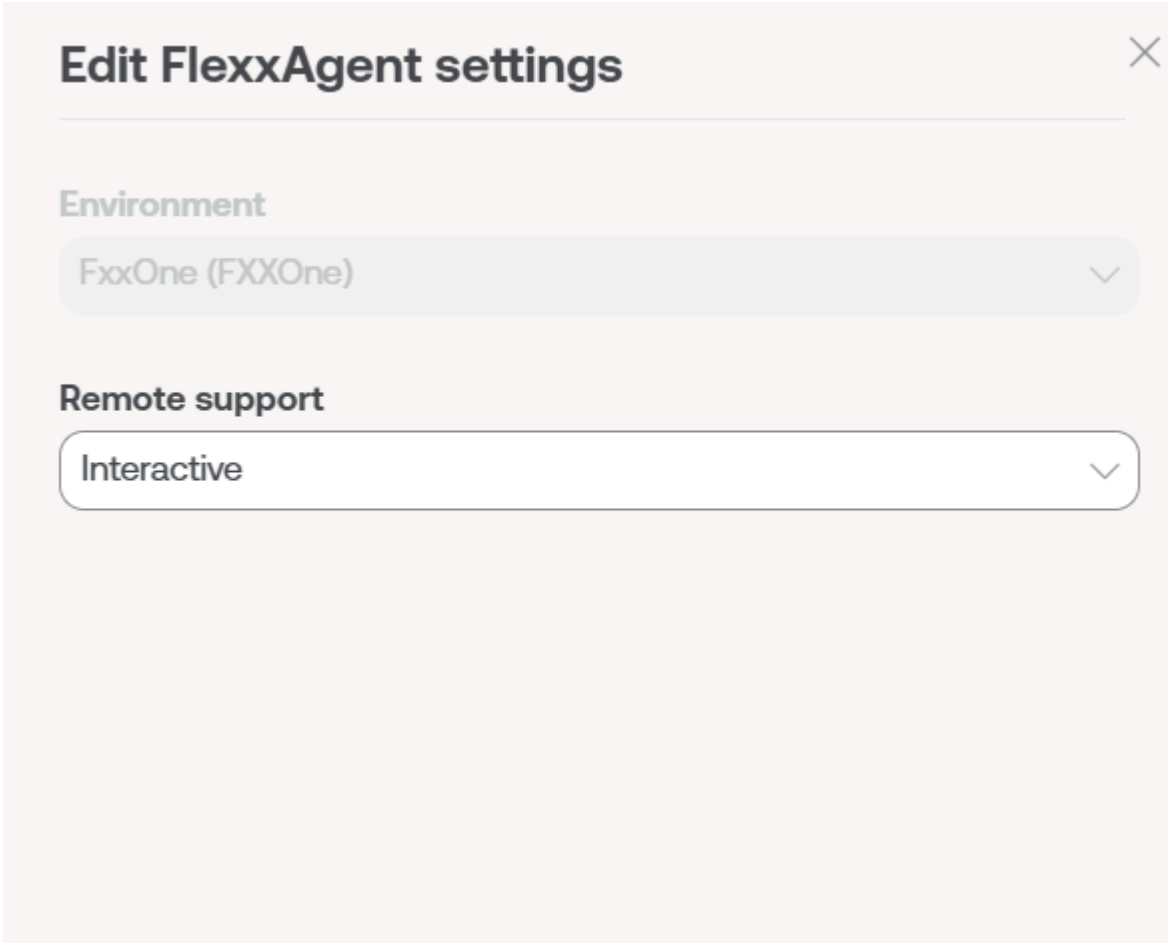
- The device receiving remote assistance must have **FlexxAgent version 23.7 or higher** (24.9.2 or higher for dynamic remote assistance).
- Connectivity of the devices to https://ras.flexxible.com, via TCP port 443.

> **INFO**
>
> If FlexxAgent restarts during a remote support session, the session will be interrupted.

Settings

For a device to receive remote assistance, it must be configured from the FlexxAgent Settings (Remote Assistance) of its reporting group. From there, you can choose which type of remote assistance devices will have access to.

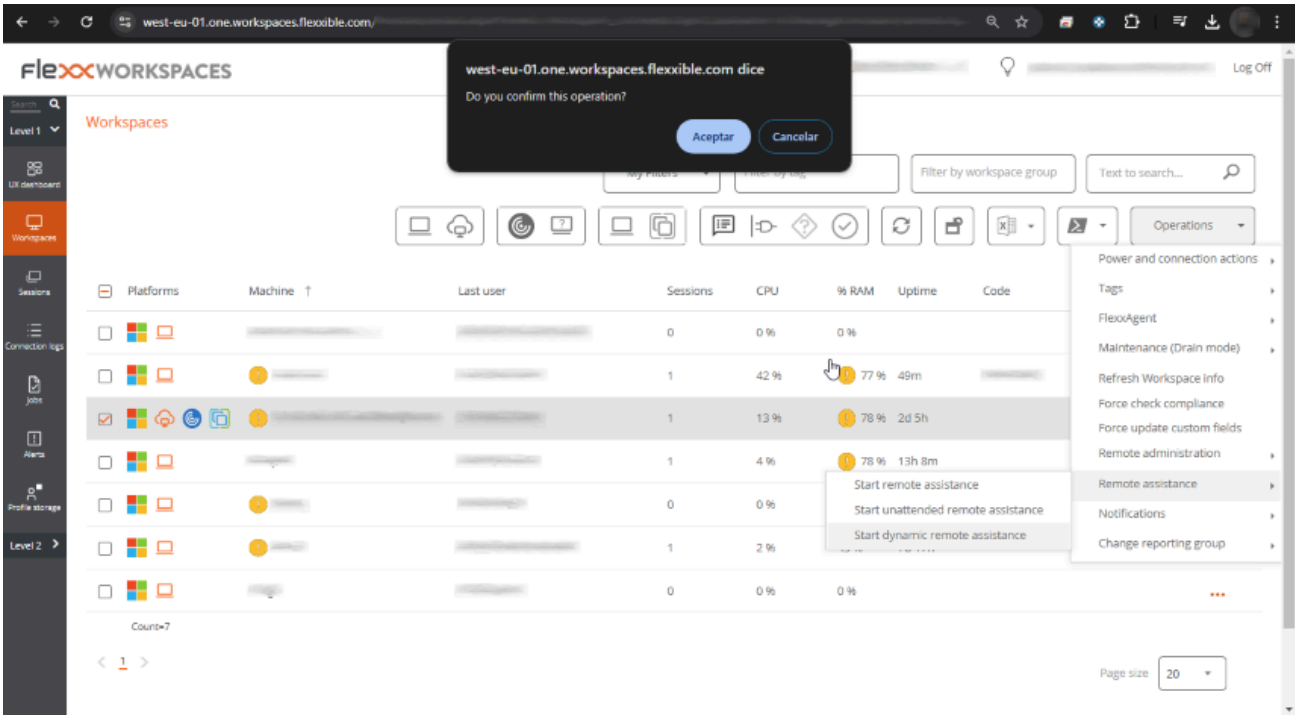
Copyright © 2024 Flexxible. Todos los derechos reservados.



Activation

Once the configuration is done, from the support side, when you want to activate remote assistance on a device, it should be done from the `Workspaces` module, having previously selected the device to be assisted. `Level 1` -> `Operations` -> `Remote Assistance`. And then choose the type of remote assistance to be provided: interactive, unattended, or dynamic.

Copyright © 2024 Flexxible. Todos los derechos reservados.



The remote assistance operation can be activated both from the `Sessions` view and from `Workspaces`.

When the operator launches the `Start remote assistance` request, FlexxAgent initiates a process (with the user's permissions) on the device and notifies the user.

Copyright © 2024 Flexxible. Todos los derechos reservados.

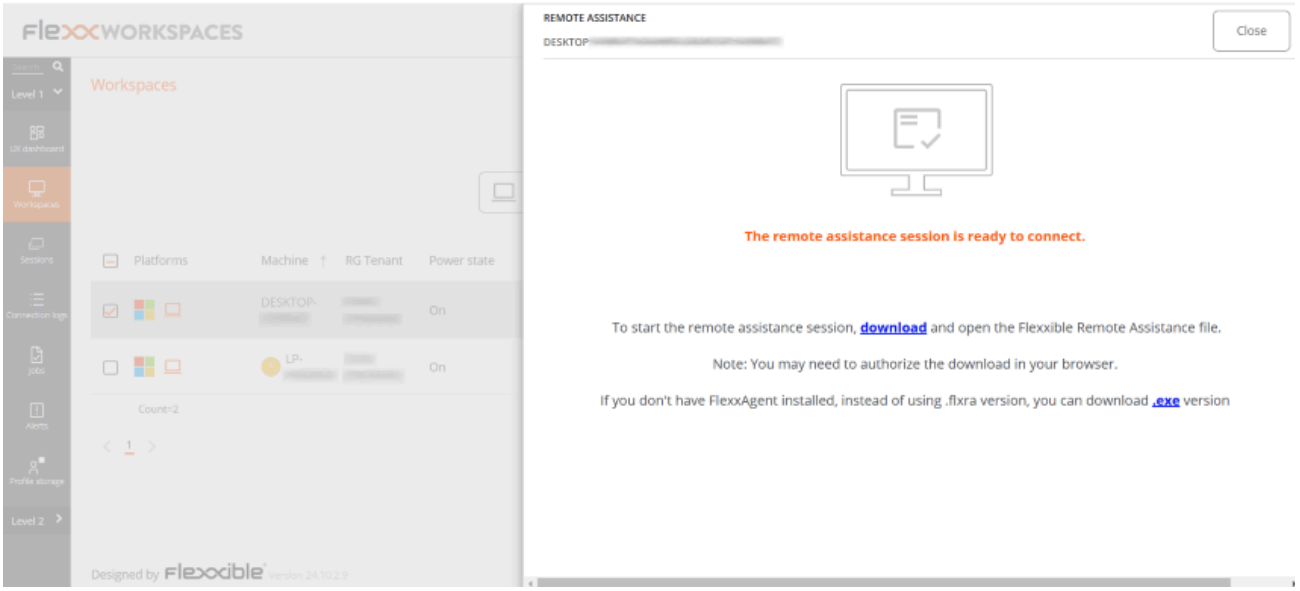
Activation file download

The support operator needs to download an activation file to provide the remote assistance service. The type of file will depend on whether the device providing support has FlexxAgent installed or not.

File for devices with FlexxAgent installed

If the support operator's device has FlexxAgent installed, they should download the Flexxible Remote Assistance file, with the extension ".flxra", and run it by double-clicking on it.

This file will run with the user's permissions, without installation, and will remain active for the duration of the remote assistance session. Once the session is over, the process will be stopped and the file will be automatically deleted from the filesystem.



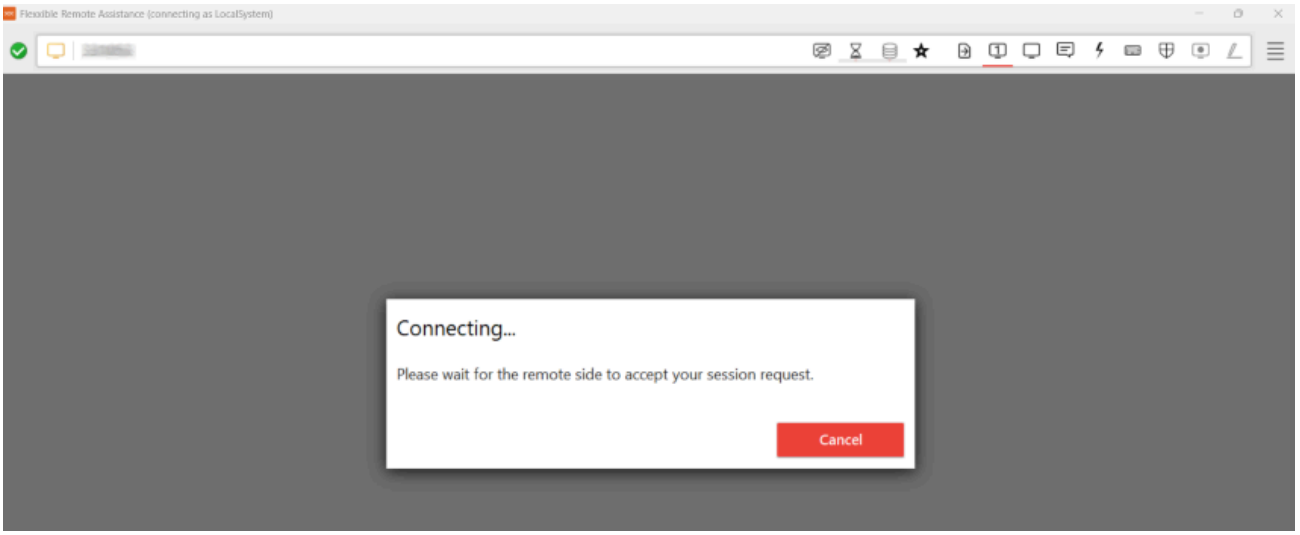
File for devices without FlexxAgent installed

If the support operator's device does not have FlexxAgent installed, they should download the file with the ".exe" extension and run it by double-clicking on it.

This file will run with the user's permissions, without installation, and will remain active for the duration of the remote assistance session. Once the session is over, the process will be stopped, but the file will not be automatically deleted from the filesystem.

Copyright © 2024 Flexxible. Todos los derechos reservados.

Next, in both cases, the consent request will be sent to the user.



Wait for the user's consent.

Once remote assistance is accepted, the support operator can gain control of the session.

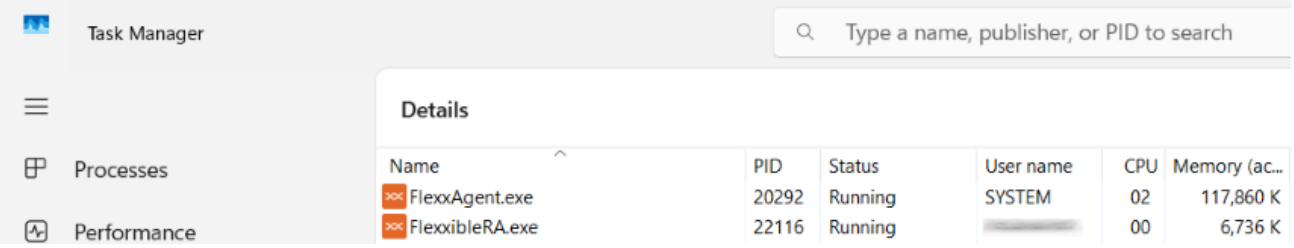
Copyright © 2024 Flexxible. Todos los derechos reservados.

> **INFO**
>
> Even if the file is executed without administrative permissions, access is not denied to the administrative tools needed for support delivery. These are in the `Flexxible Tools` menu, in the upper left corner of the remote assistance window.

Processes

When the operator downloads the remote assistance file from Workspaces, the following processes will be generated and run automatically:

- FlexxAgent.exe
- FlexxibleRA.exe



Behavior of remote assistance through proxy

From the operator's perspective, the operation is as follows:

- When executing the ".flxra" or ".exe" file, it is checked if the Proxy_Url key exists in the FlexxAgent keys. If yes, it uses it if accessible. Otherwise, the AnyDesk binary is launched with autodetect.

From the end user's perspective, when remote assistance is performed:

- FlexxAgent will detect if the proxy is configured, if it detects it and is accessible, it uses it. Otherwise, the AnyDesk binary is launched with autodetect.
- If the proxy configuration registry keys do not exist, it will detect if the operating system has the proxy configured. If it detects it and it is accessible, it uses it.

Copyright © 2024 Flexxible. Todos los derechos reservados.

Otherwise, the AnyDesk binary is launched with autodetect.

Flexxible Tools

The remote support file runs with the user's permission level; however, the user may not have local device admin privileges. To cover these cases, `Flexxible Tools` has been incorporated.

Flexxible Tools allows activation of administrative tools in remote assistance. These are a series of embedded functions that can be accessed from the top left of the interface.

These tools can be executed with the following administrative permissions:

- CMD
- PowerShell
- Registry editor
- Task Manager

Copyright © 2024 Flexxible. Todos los derechos reservados.

If the user has permissions on the Portal, Flexxible Tools can be activated for users by role. This can be done in two ways:

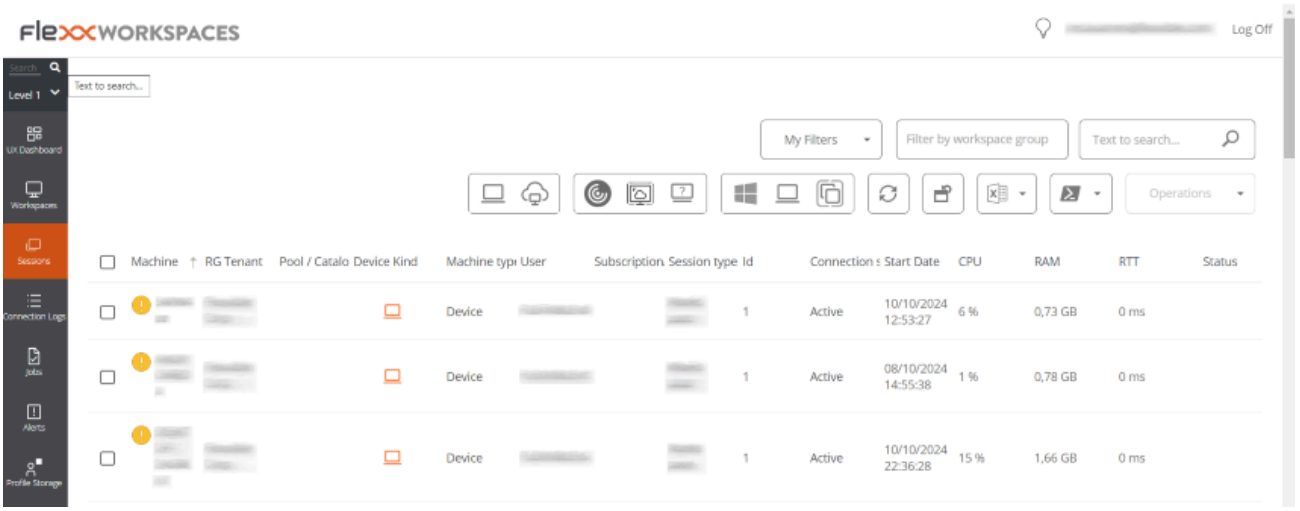
- From `Portal` -> `Settings` -> `Organization` -> In the menu, `Products` tab: for each product in the list there is a `FlexxAgent Configuration` button that allows applying the change to all report groups.
- From `Portal` -> `Configuration` -> `Reporting Groups`: for one or several reporting groups, functionality can be activated or deactivated.

> **INFO**
>
> The proper functioning of Flexxible Tools requires that both the operator's device and the device receiving remote support have FlexxAgent installed from the same environment.

Copyright © 2024 Flexxible. Todos los derechos reservados.

Workspaces / Level 1 / Sessions

The Sessions view allows you to organize, filter, search, and send operations to active user sessions.



The information displayed on the screen can be configured by adding or removing columns of information using the `Column Selector` and saving the filters used for future queries in the user profile.

Header filtering options

In the upper right area of the screen, you will find tools and icons for each attribute that, when clicked, allow you to filter the list based on the following criteria:

- **Session device type.** Physical or virtual.
- **Session broker used.** Citrix, RDP, or unknown.
- **Hypervisor.** Hyper-V, Nutanix, vSphere, physical or unknown.

Once the session is selected, or through multiple selection, the `Operations` button gives access to perform various session management tasks such as `Power and connection actions` or send `Notifications` to users. You can check the details of these functionalities in the section Actions on devices.

List filtering options

Copyright © 2024 Flexxible. Todos los derechos reservados.

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.
- Disconnect the session.

Remote Assistance

Allows launching remote assistance to users in interactive mode, which requires user consent to view and take control of their session; or execute unattended remote assistance, which allows administrative access to server or self-service type devices that do not necessarily have a user on the other side of the screen.

Notifications

Allows sending notifications to the selected devices. Notifications can be pop-up notifications or notifications that reserve a screen area.

Copyright © 2024 Flexxible. Todos los derechos reservados.

INFO

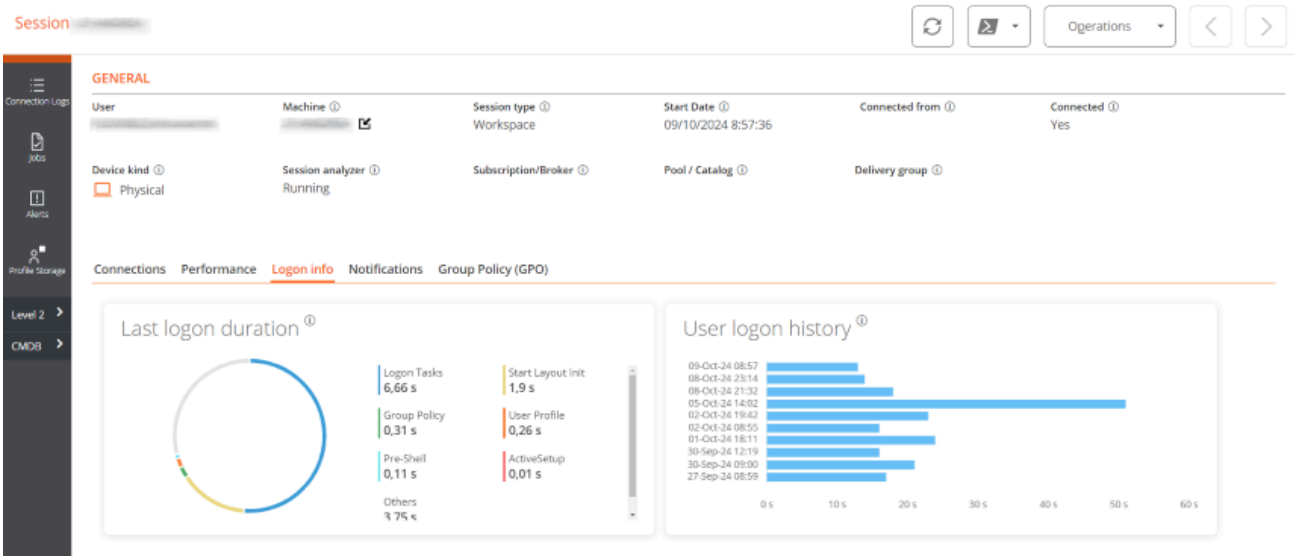
On some devices with Windows 10 1903+, the Automatic Restart Sign-On (ARSO) can create "ghost sessions" in the session view after an update restart. To adjust this behavior, please refer to this guide.

Copyright © 2024 Flexxible. Todos los derechos reservados.

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

Copyright © 2024 Flexxible. Todos los derechos reservados.

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.

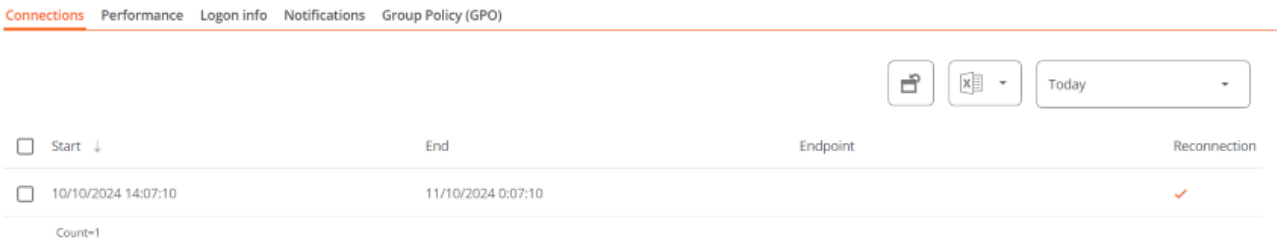
Copyright © 2024 Flexxible. Todos los derechos reservados.

Tabs

The tabs at the bottom show specific grouped information, including the following:

- Connections
- Performance
- Login information
- Notifications
- Group Policy (GPO)

Connections



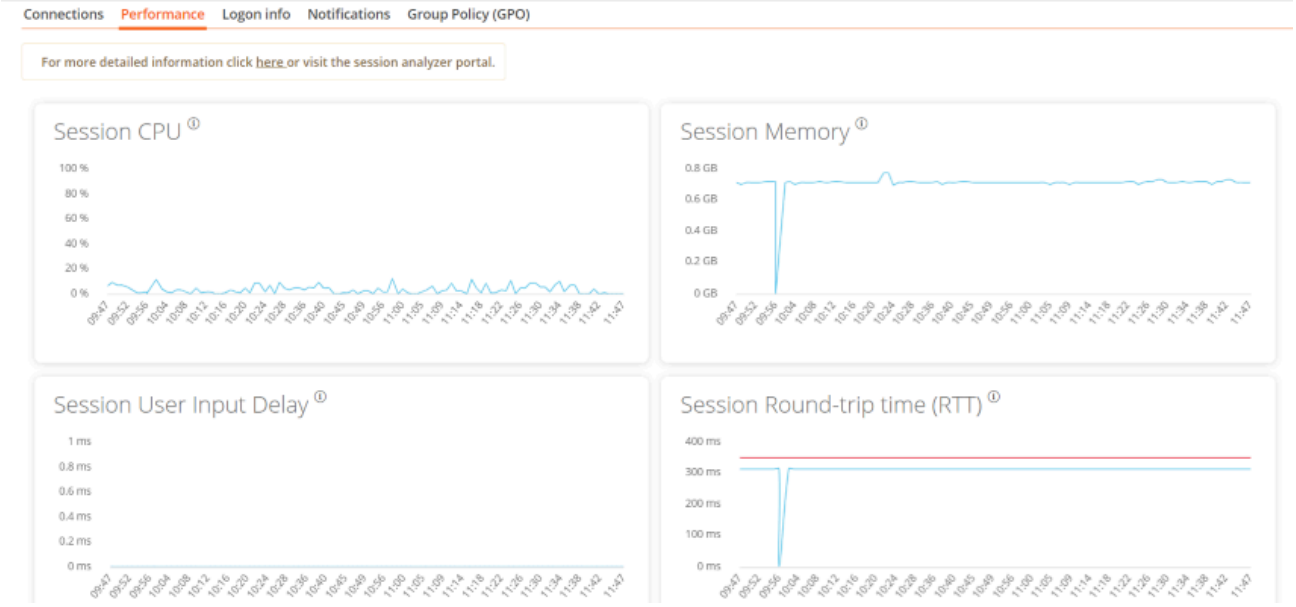
This tab contains information about the device's connections, i.e., each time a user starts or reconnects a disconnected session.

> 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

Copyright © 2024 Flexxible. Todos los derechos reservados.

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

Copyright © 2024 Flexxible. Todos los derechos reservados.

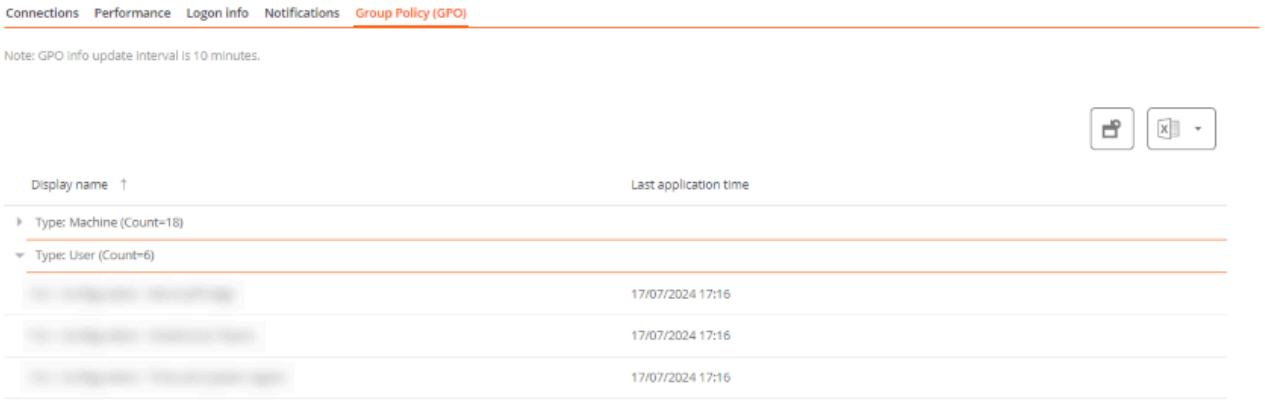
At the bottom, a table presents the details for each user login.

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)

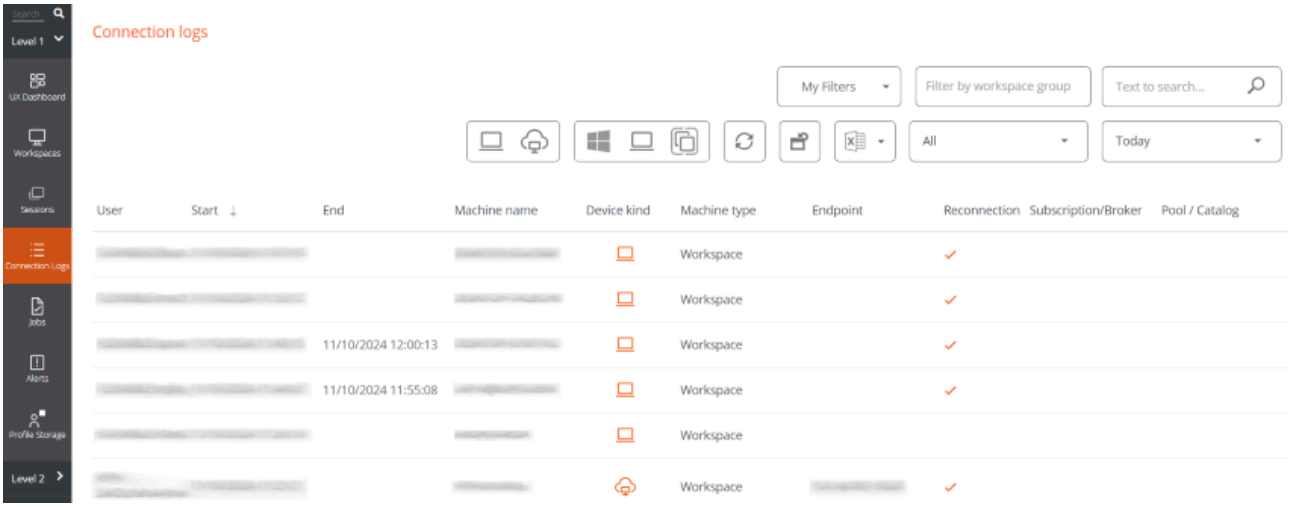
This tab shows the information of group policies applied in the active session. It shows the name of the applied policy both at the user level and device level.



Copyright © 2024 Flexxible. Todos los derechos reservados.

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.

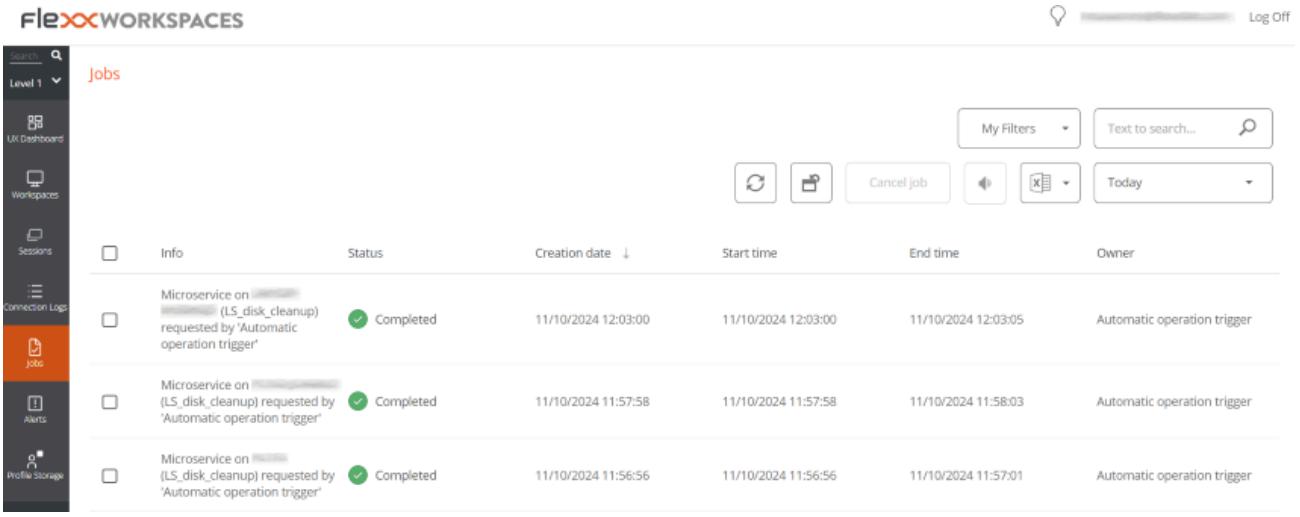
This section allows the use of the column selector and the Filtering options also available in the Sessions section.

Copyright © 2024 Flexxible. Todos los derechos reservados.

Workspaces / Level 1 / Job

Each 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` gathers all the jobs performed in the organization, so it also provides historical execution records, which allows it to be used as an audit log.

List view



The jobs view consists of the following elements:

- Options at the top of the interface
- Job list view

Top options

- Refresh the job list and show updated values.
- Resets all settings made for the jobs view.
- Filter jobs by age:
  - Today (default filter)
  - This week
  - This month
  - This quarter

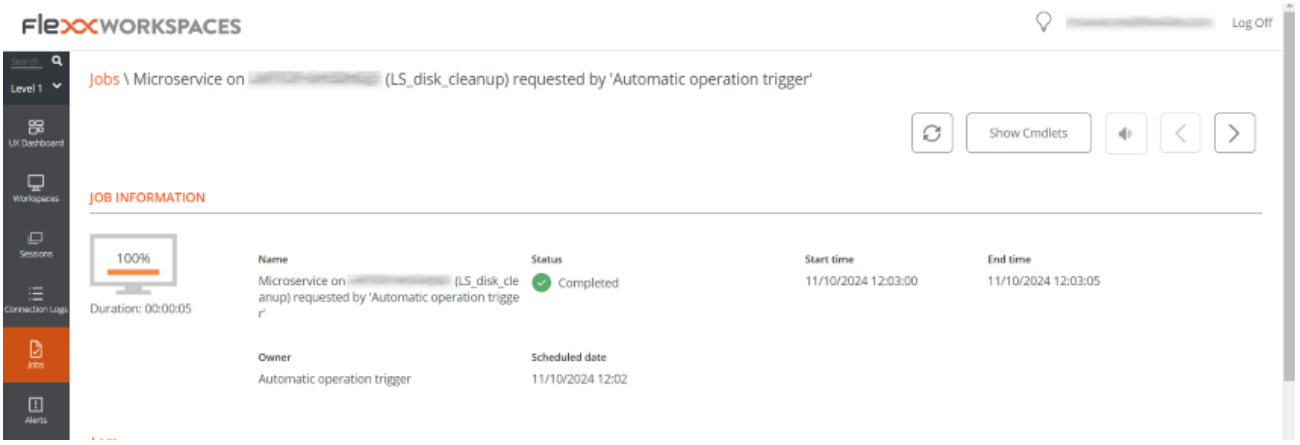
Copyright © 2024 Flexxible. Todos los derechos reservados.

    - This year
- The `Cancel` button allows canceling jobs in pending status.
- The `Notify` button allows you to subscribe to a specific job to receive an email notification when it is completed.
- The `Export to` button allows exporting in the selected type.
- The `My filters` button allows access to `Predefined filters` or user-created filters.
- Jobs can be filtered by any parameter in the list in the `Search` box.

Jobs list

The job list, like all list views in Workspaces, allows multiple filtering and customization options as defined in Filtering Options in Listings.

Detail view



The detail view includes a progress bar indicating the percentage of the job that has already been executed.

Statuses

A job can have several statuses:

- **Pending.** The task is pending to start.
- **In progress.** The task has started and is still ongoing.
- **Completed.** The task is finished.

Copyright © 2024 Flexxible. Todos los derechos reservados.

- **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`. More information at Considerations about the code to use.

Copyright © 2024 Flexxible. Todos los derechos reservados.

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

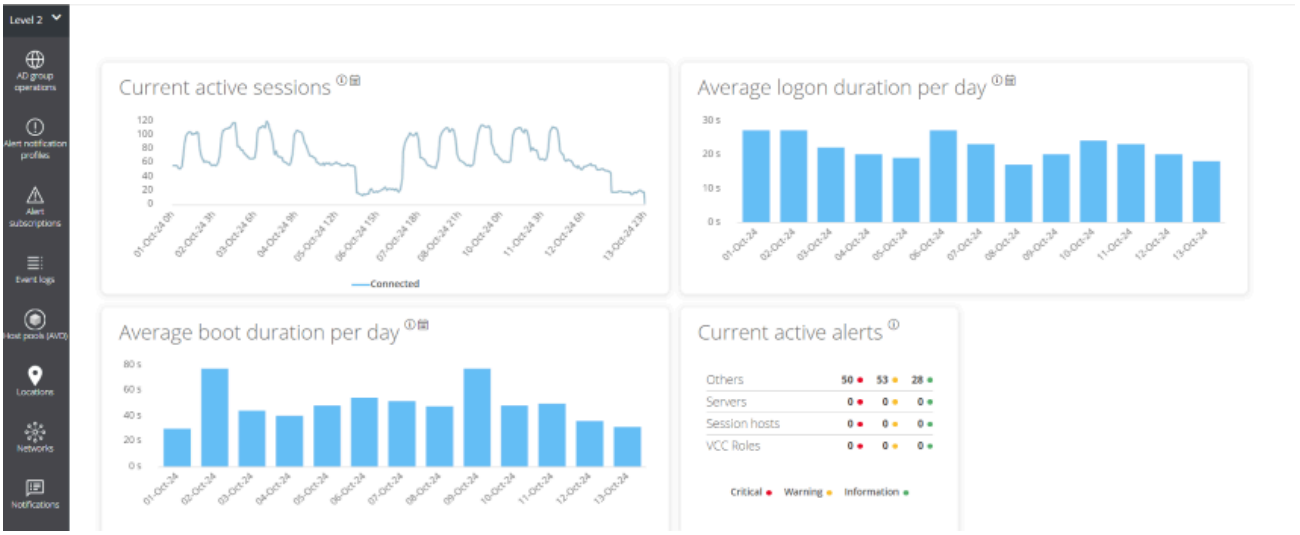
This feature allows subscribing to specific jobs, that have not yet started or are in progress. The system will notify by email when they are completed.

To subscribe, select the jobs from the list and activate the `Send notification` button.

Copyright © 2024 Flexxible. Todos los derechos reservados.

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.



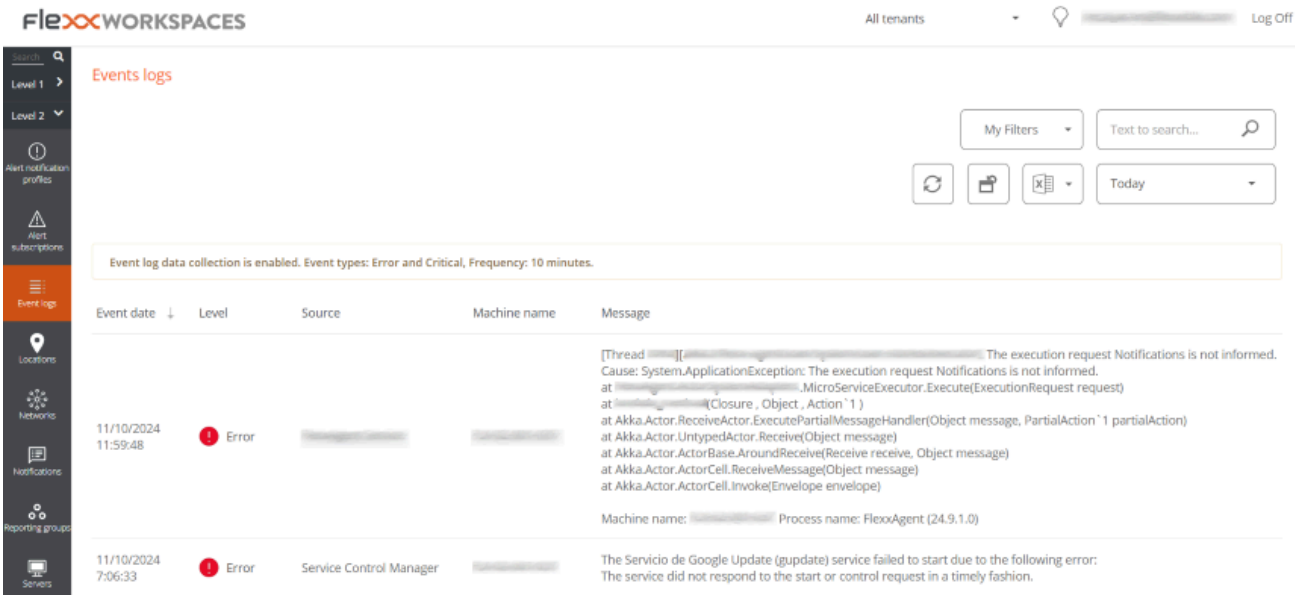
Functionalities available at this level:

- Event Logs
- Locations
- Networks
- Notifications
- Reporting groups
- Servers
- Wifi networks

Copyright © 2024 Flexxible. Todos los derechos reservados.

Workspaces / Level 2 / Event Logs

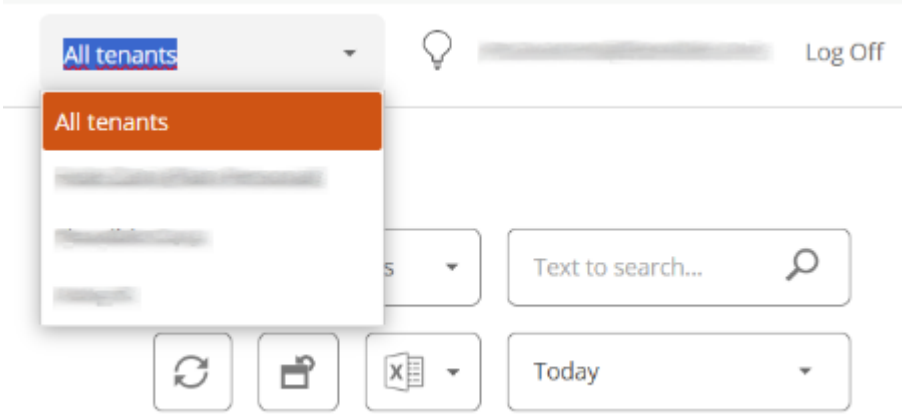
Event logging is a diagnostic tool designed to centralize events generated by the system. It shows exclusively those of type *Critical* and *Error* in Windows environments, from the Application, Security, and System logs.



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.



Copyright © 2024 Flexxible. Todos los derechos reservados.

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.

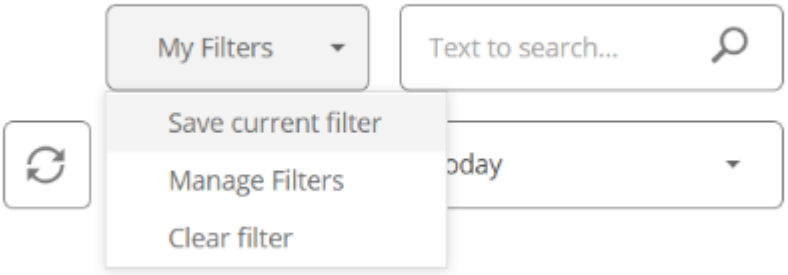
An example would be to filter by an event with a specific ID to obtain a list of affected devices, subsequently applying corrective actions.

My filters

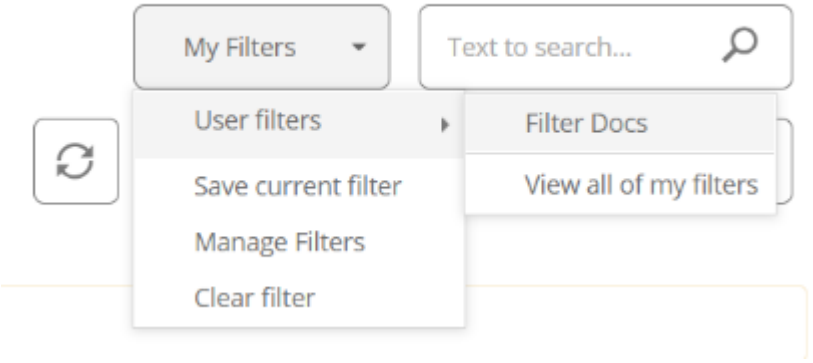
In the top menu, the option `My filters` allows access to three filter configuration options.

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.



Copyright © 2024 Flexxible. Todos los derechos reservados.

Manage filters

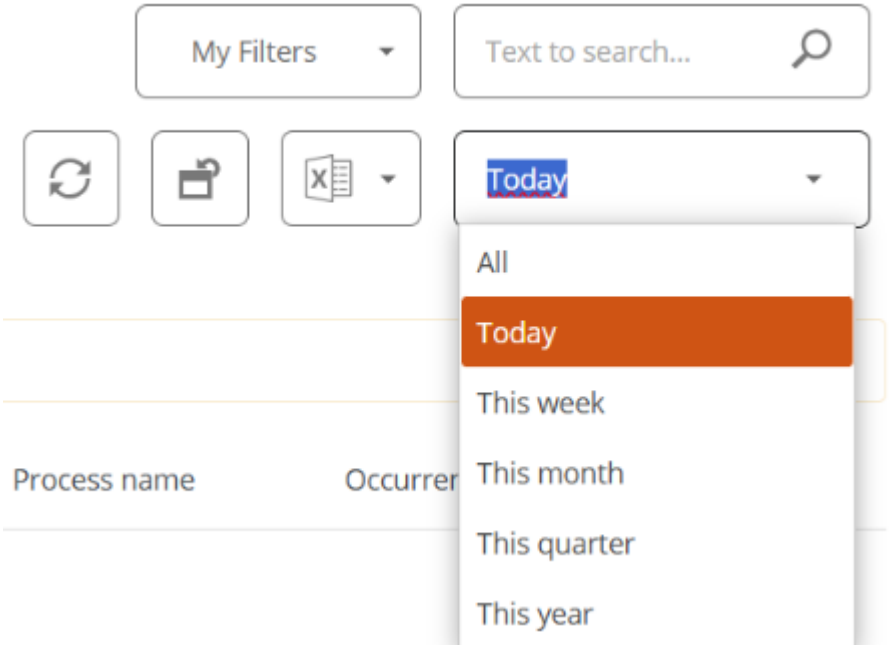
Allows you to apply value filtering on the event list and also edit or delete user saved filters.

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

Copyright © 2024 Flexxible. Todos los derechos reservados.

> **INFO**
>
> If the option *All tenants* is selected in the organization dropdown, only events from the current day (*Today*) can be seen.

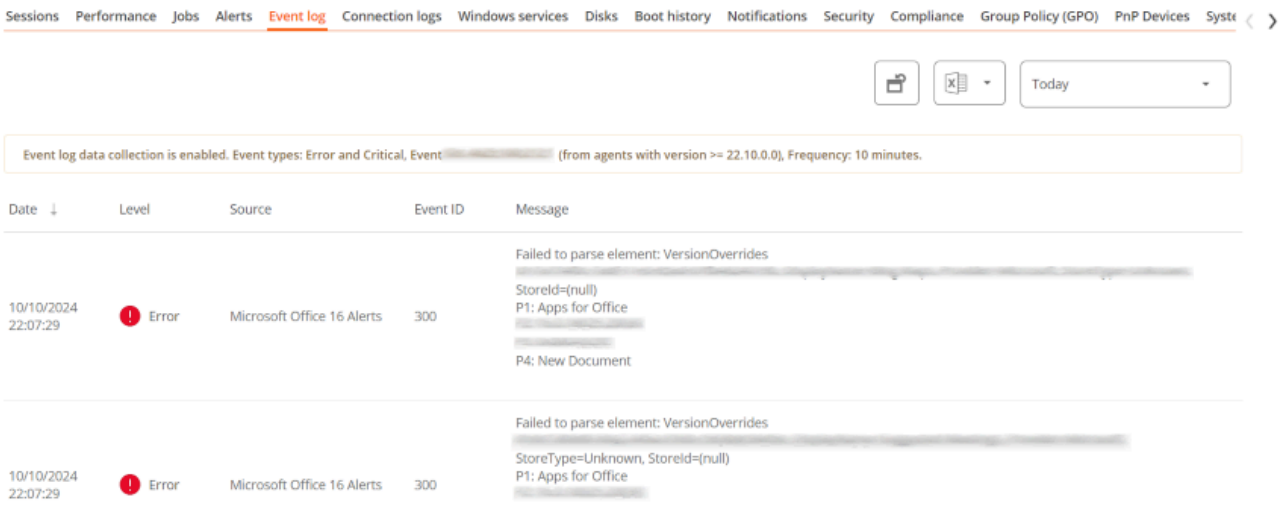
Detail view

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

Copyright © 2024 Flexxible. Todos los derechos reservados.

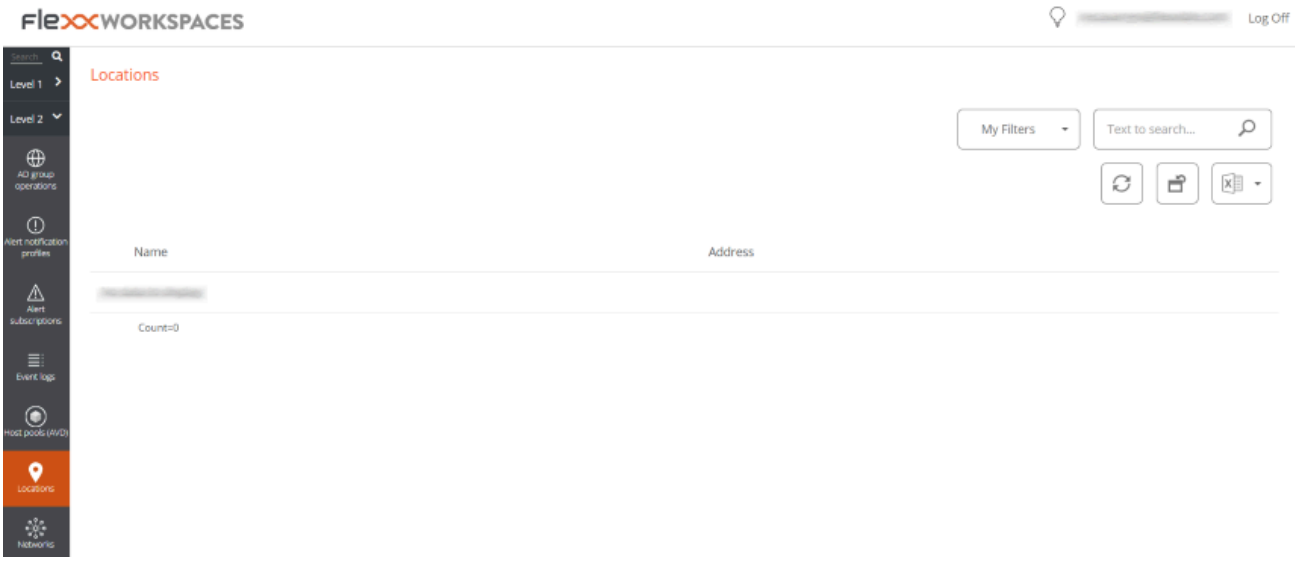
Users with the *Organization Administrator* role can add events that do not meet the default filtering conditions to, for example, add events with a specific ID that, although they have an informational severity level, are relevant to the organization, as well as change the log update time.

Copyright © 2024 Flexxible. Todos los derechos reservados.

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:

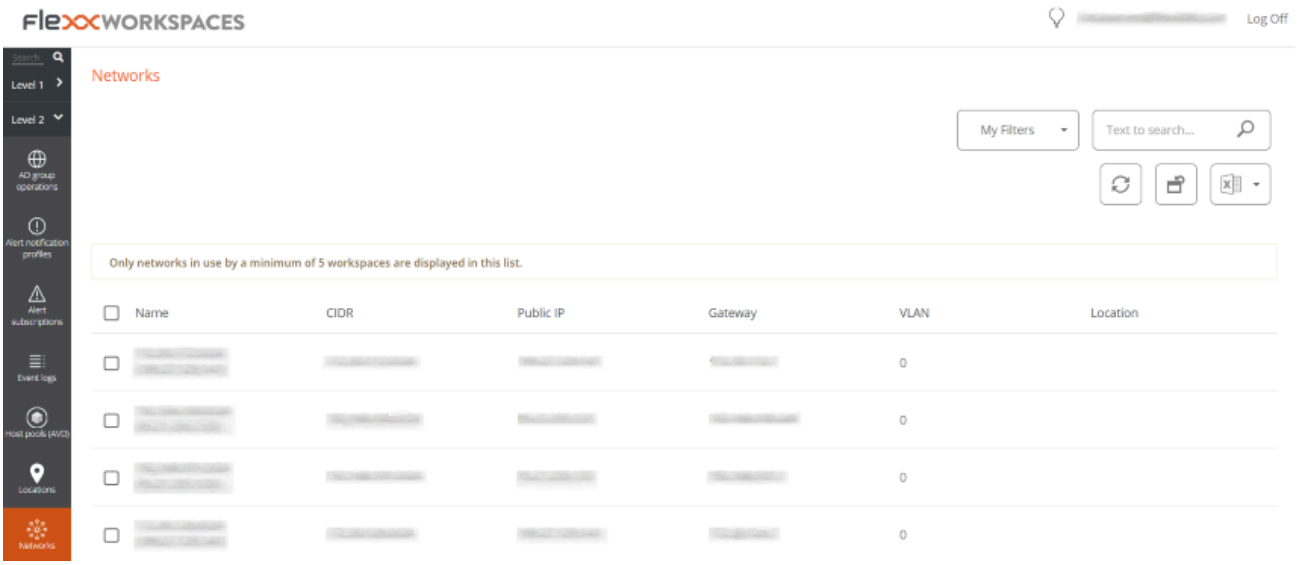
Copyright © 2024 Flexxible. Todos los derechos reservados.

- **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

Copyright © 2024 Flexxible. Todos los derechos reservados.

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.



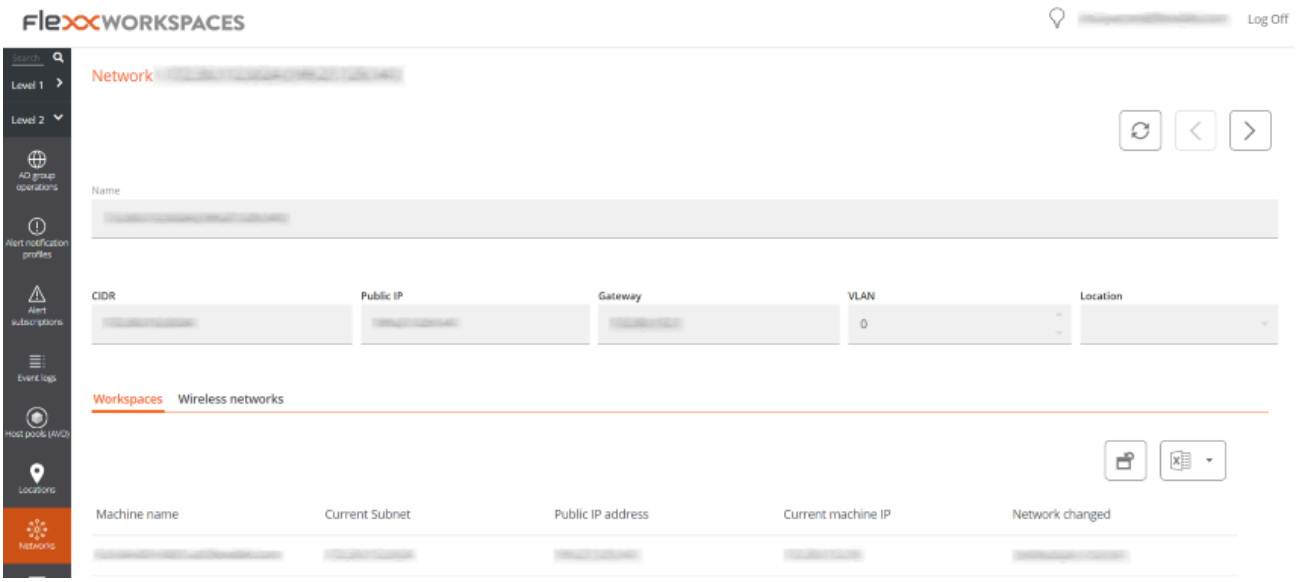
List view

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

Copyright © 2024 Flexxible. Todos los derechos reservados.



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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

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.

Close 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.

Types of notifications

Workspaces offers two types of notifications to effectively communicate messages to users.

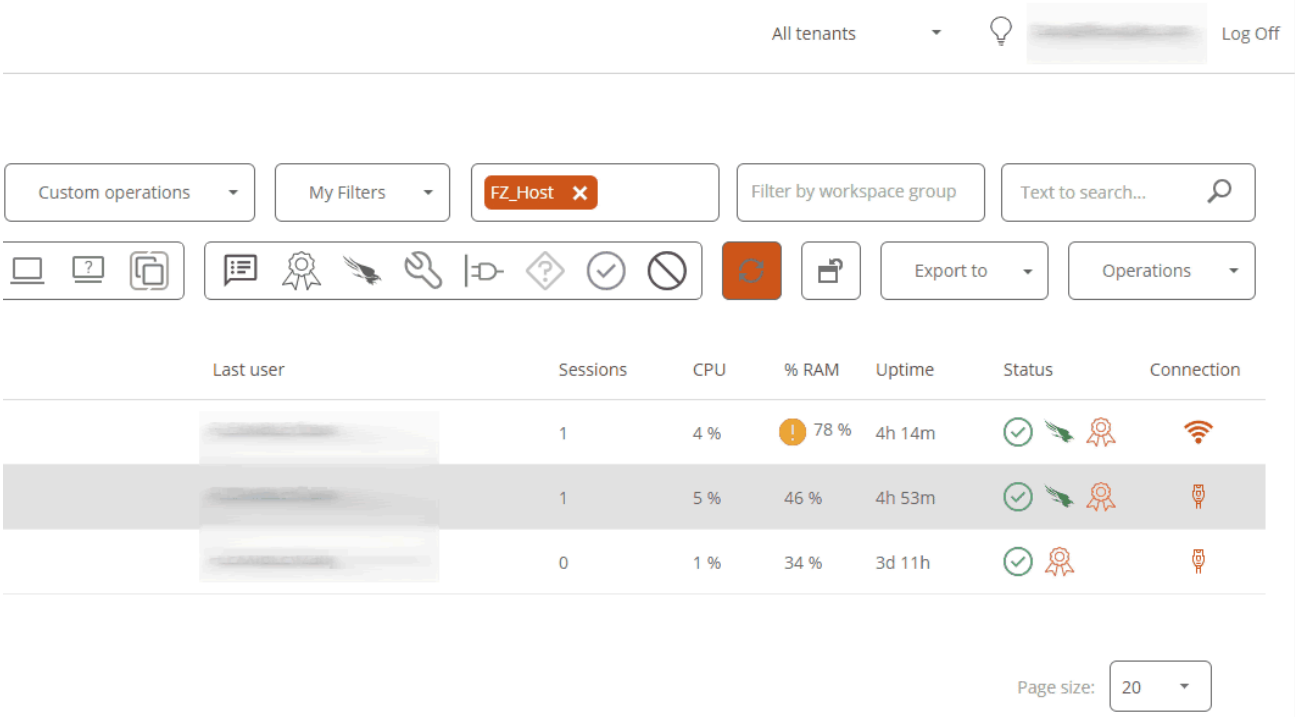
- Pop-up messages. They display a window to the user that appears over the interface and can be closed with just one click. Useful for communicating brief or specific information without permanently interrupting work.
- Notifications. Designed for critical situations, like service interruptions, where other corporate channels may 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.

Sending pop-up messages

1. Access the Workspaces module -> Section `Sessions` or `Workspaces`.
2. Select the target sessions or devices.
3. Click on `Operations` -> `Notifications`-> `Send pop-up message`.

Copyright © 2024 Flexxible. Todos los derechos reservados.

- Specify the message and click `OK`.



The user in the session will receive a window in the center of their screen with the configured message.

These notifications are based on Windows system tools. If all devices or sessions are selected and a message of this type is sent, the message will only reach the users who are working (in session) at that moment. If any user enters their session after the message is received, it will not be visible.

Copyright © 2024 Flexxible. Todos los derechos reservados.

Notifications

Notifications have many additional features aimed at maintaining effective communications and protecting the information transmitted to users.

While on screen, notifications reserve that space 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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

Notifications can be configured for time intervals; intervals can be defined in which all sessions already started and future sessions receive this notification and it remains active during that period of time.

Sending notifications

1. Access the Workspaces module -> Section `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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

- **Disable Minimize.** Activated prevents users from minimizing the notification.
- Message text
- **Information Text.** Additional message that will appear when hovering over the notification.
- **Link.** To include a status page, if applicable.
- **Blinking.** Allows setting blinking on the notification to increase visibility.

Copyright © 2024 Flexxible. Todos los derechos reservados.

Workspaces / Level 2 / Reporting groups from Workspaces

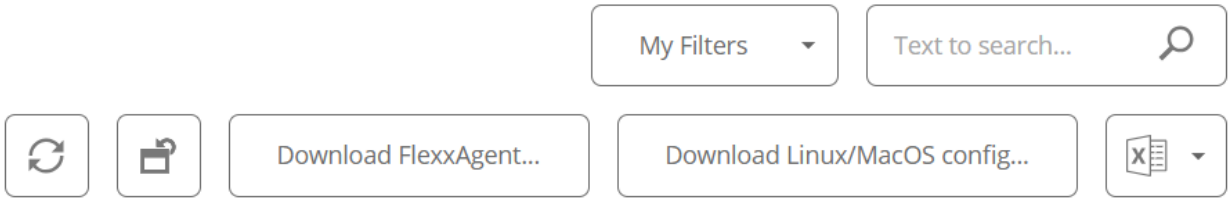
This section allows you to download FlexxAgent in the reporting groups configured in the organization, as well as access detailed information about the devices that integrate it.

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:



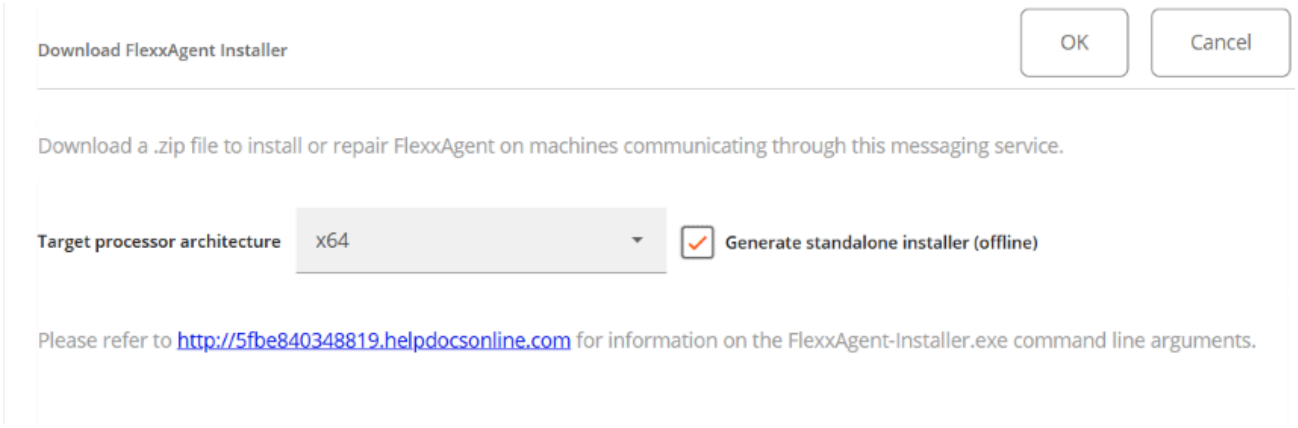
- **My filters.** Allows managing filters for searching reporting groups.
- **Text to search.** Free search box to find reporting groups based on the entered text.
- **Update.** Reloads the list of reporting groups after applying filters.
- **Reset all settings made for this view.** Returns to default 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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

Download FlexxAgent

Steps to download the 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

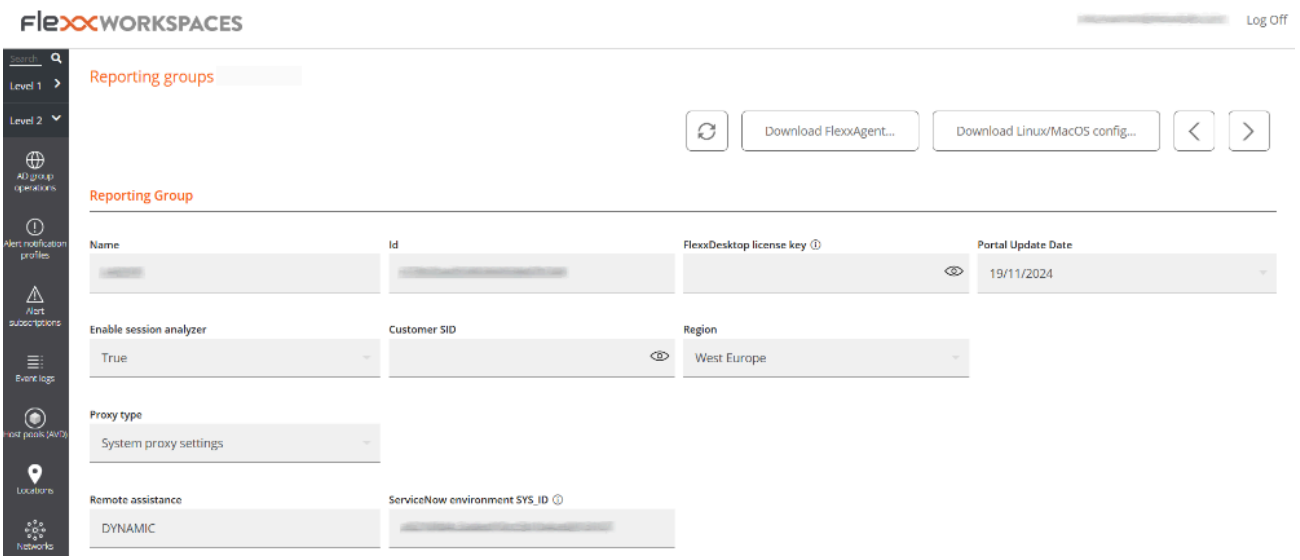
Steps to download the configuration file:

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

Detail view

When you select a reporting group from the list view, you'll access a detailed view that includes:



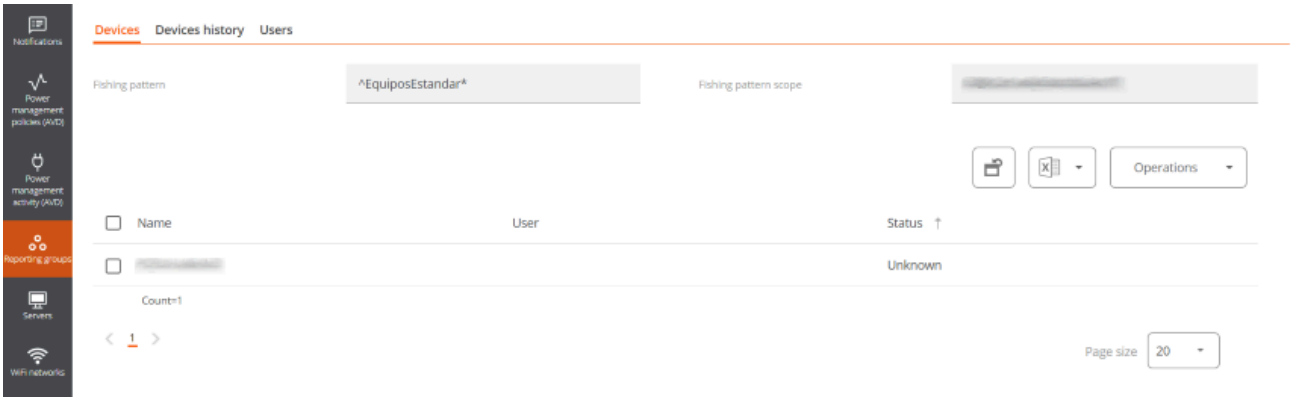
- **Name.** Name of the report group.
- **Id.** Reporting group identifier.
- **FlexxDesktop license key.** If available, the installed product license.
- **Portal update date.** The date on which the reporting group was updated.
- **Enable Session Analyzer.** Indicates if it's configured to launch Session 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 about the following elements is provided:

Devices

Copyright © 2024 Flexxible. Todos los derechos reservados.

List of devices included in the reporting group. If the reporting group was created using a phishing pattern, the configured RegEx term and associated Id will be displayed.



The `Operations` button allows executing actions on the selected devices.

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 Versions

List of operating systems on which FlexxAgent has been installed, along with the version configured in FlexxAgent Versions, both for the *Early* environment and *Production*.

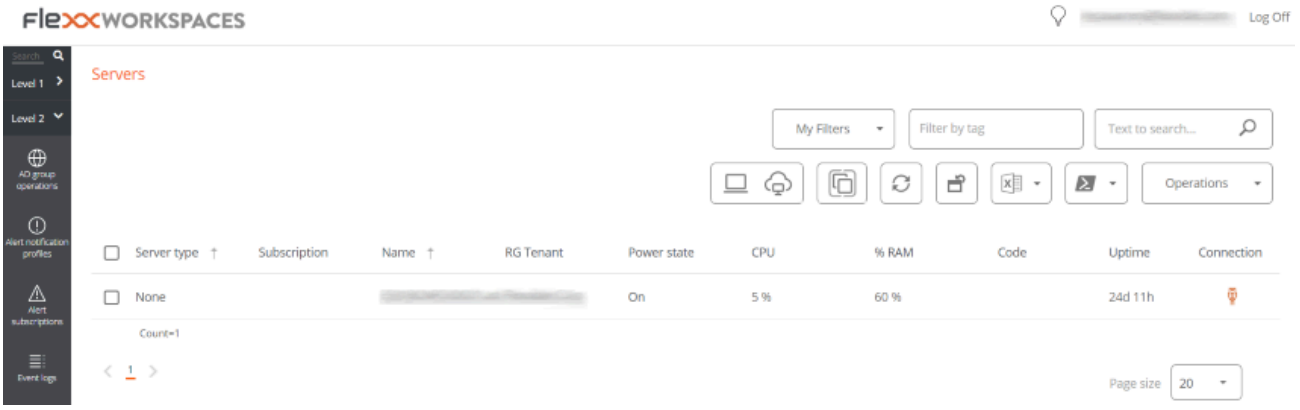
As indicated in the documentation of FlexxAgent Versions, *Early* is the test environment and *Production* is the real environment.

Copyright © 2024 Flexxible. Todos los derechos reservados.

Workspaces / Level 2 / Servers

Allows access to the environment's server list. 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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

Microservices

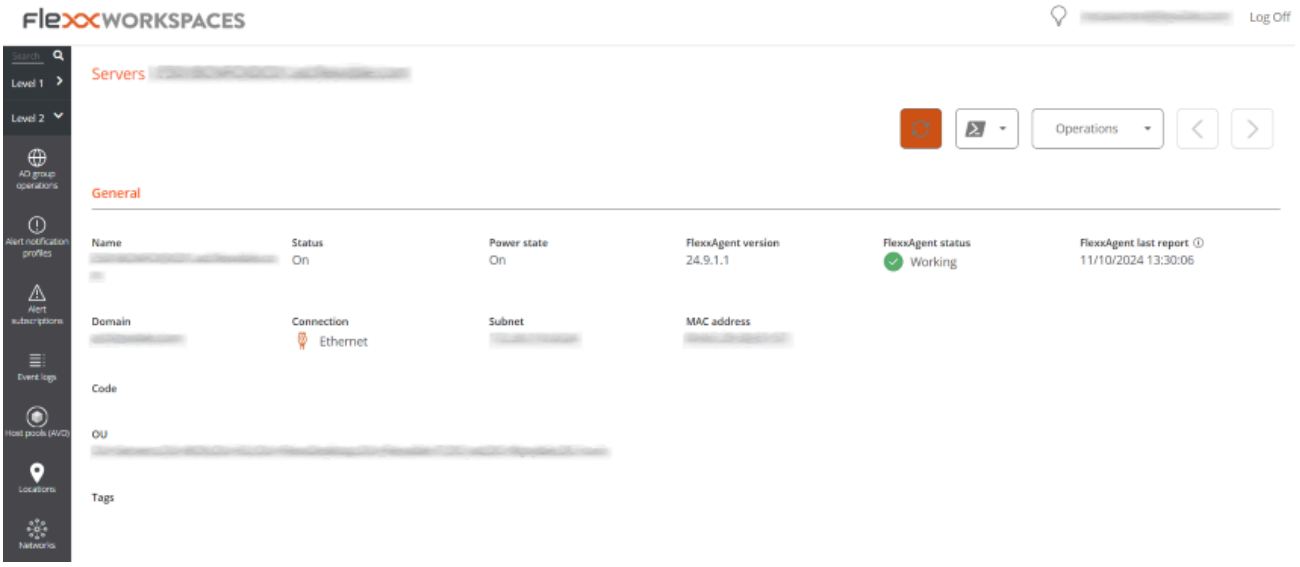
From the `>-` button it is possible to execute any of the microservices enabled for the organization that have `System` as the configured context. This allows the execution of microservices with administrative permissions on the devices. The actions of enabling, creating, modifying, or deleting microservices 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:

Copyright © 2024 Flexxible. Todos los derechos reservados.

- **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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

- **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

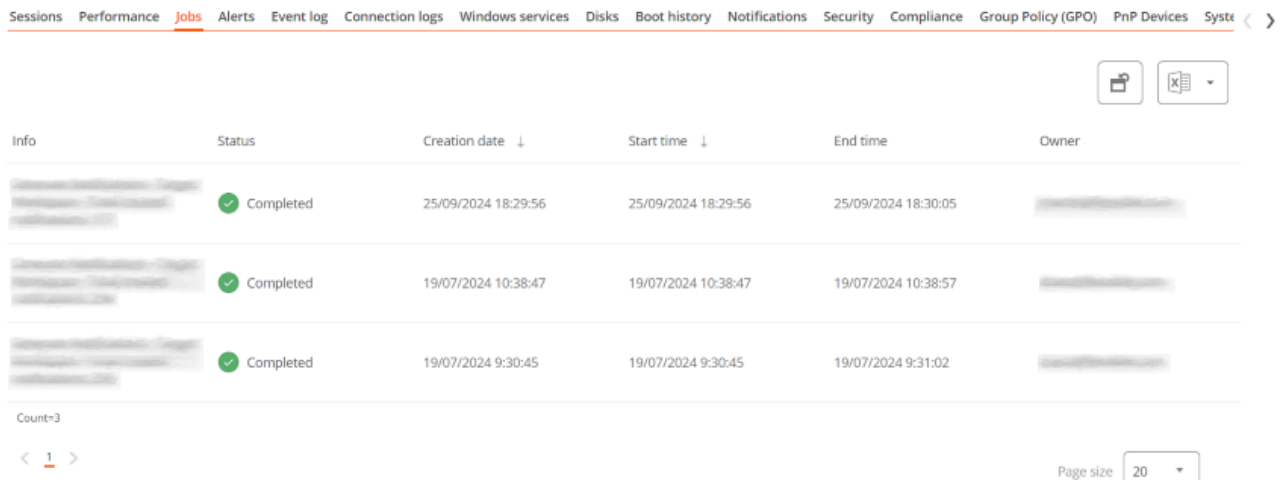
The tabs at the bottom show grouped specific information. The following are included:

- Jobs
- Performance
- Alerts
- Event logs
- Disks
- Boot history
- Security
- Group Policy (GPO)
- PnP Devices

Job

Copyright © 2024 Flexxible. Todos los derechos reservados.

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.

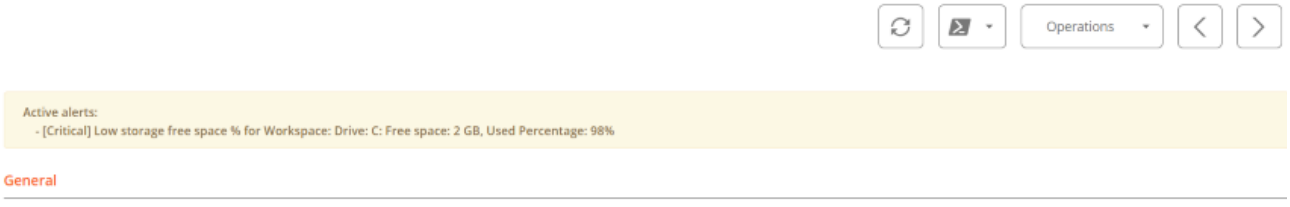


Performance

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

Copyright © 2024 Flexxible. Todos los derechos reservados.

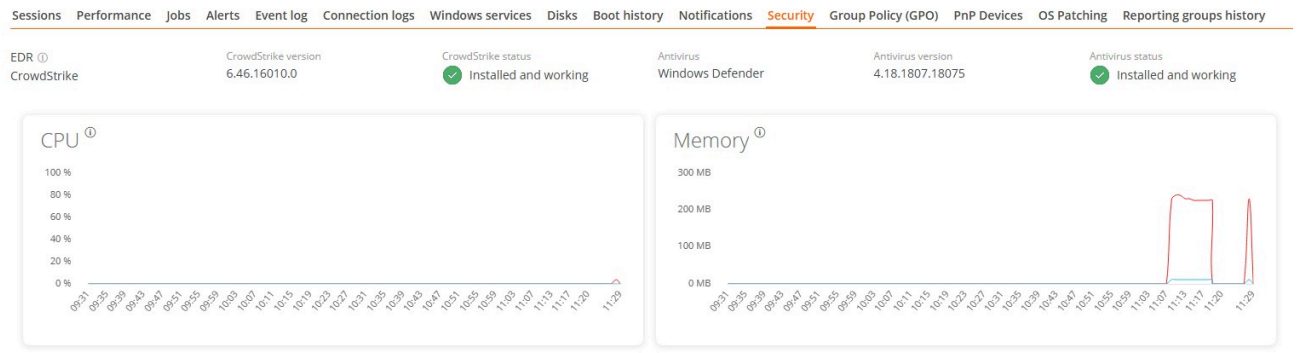
Displays a list of all partitions present on the disks identified in the system, as well as statistics of their capacity and occupancy levels.

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).



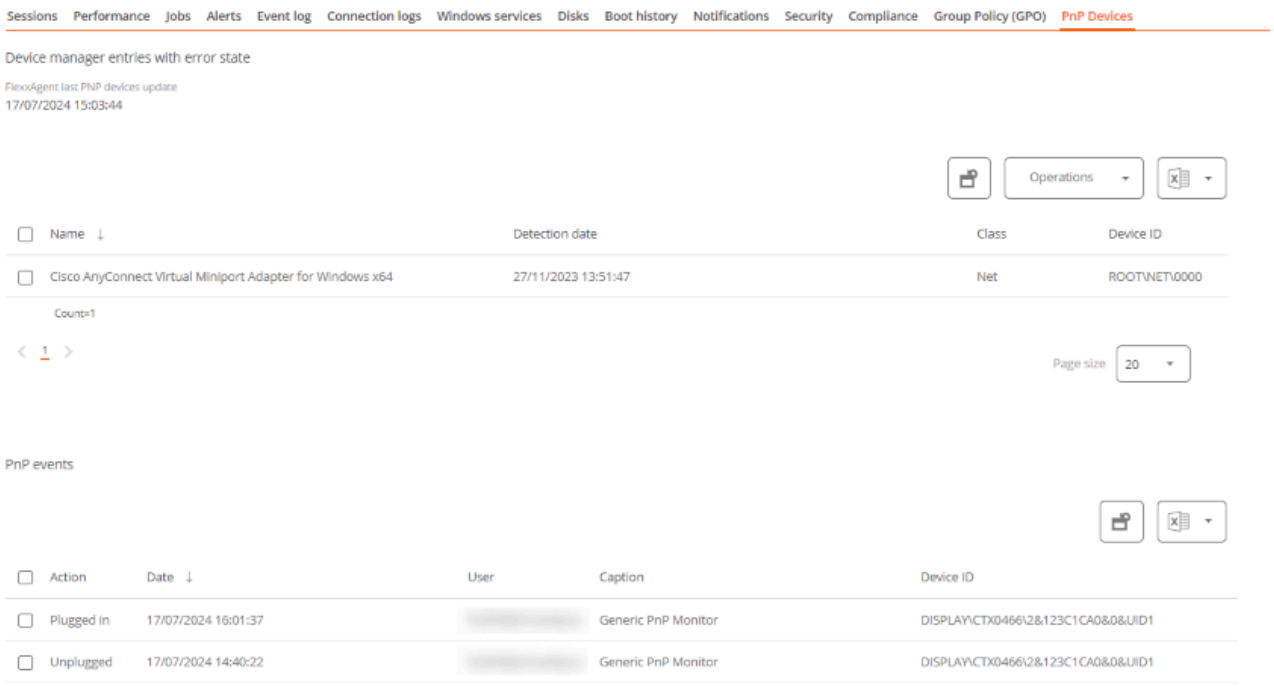
Group Policy (GPO)

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.



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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

Workspaces / Level 2 / Wireless networks

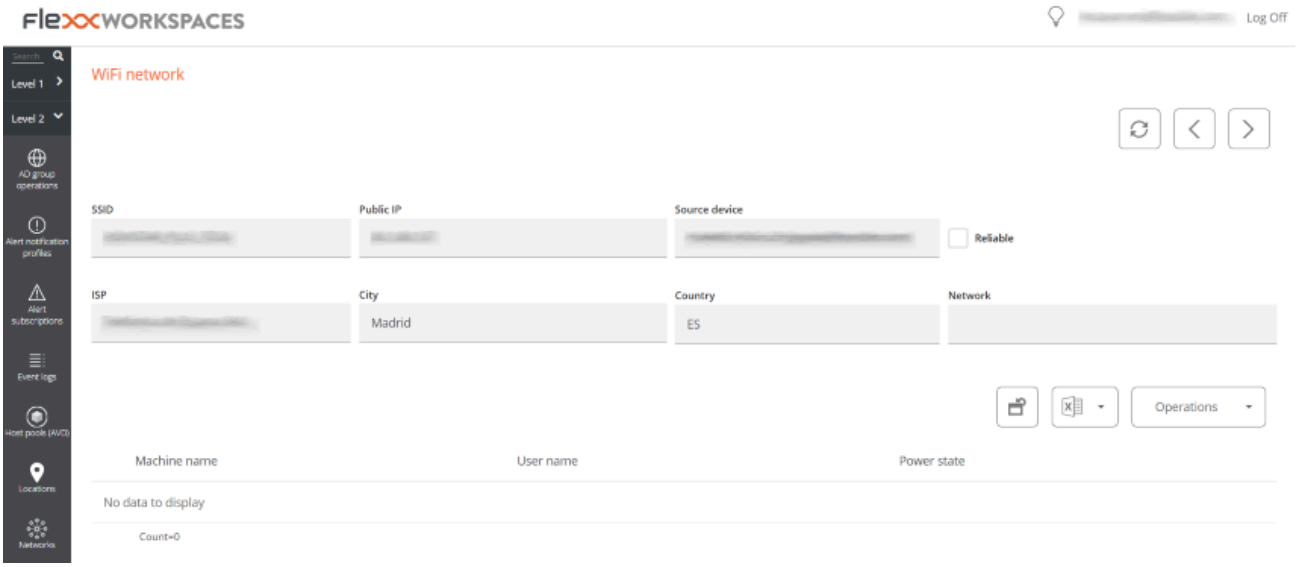
FlexxAgent collects network information from devices. When it detects the use of a wireless network, it is automatically registered in Workspaces. These networks are part of the detected networks inventory, allowing for more accurate location mapping based on connectivity data. Additionally, they can 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:

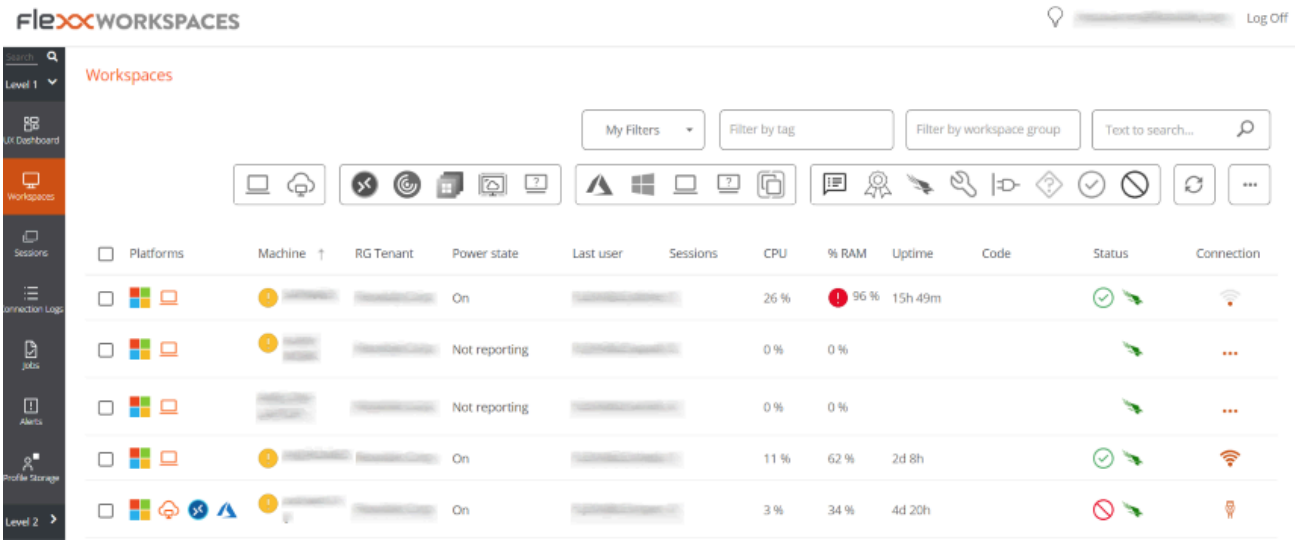
Copyright © 2024 Flexxible. Todos los derechos reservados.

- **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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

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.

Copyright © 2024 Flexxible. Todos los derechos reservados.

Workspaces / Guides / Provide remote assistance to a user

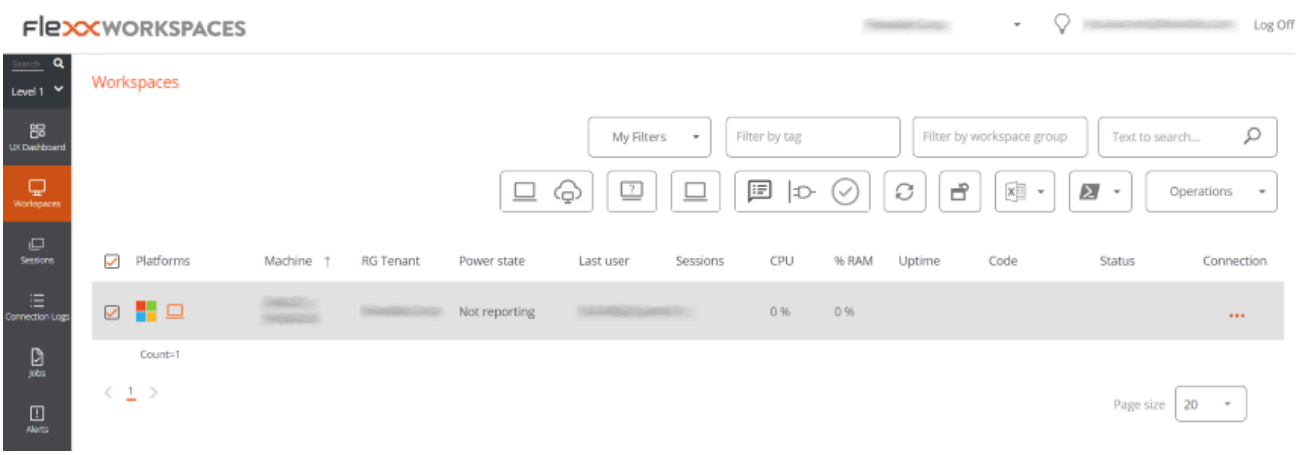
Remote assistance allows direct operation on a user's workstation desktop. The operator acts as the device administrator and works remotely with the user's desktop.

To provide remote assistance:

1. Access the `Workspaces` module.
2. Access the `Workspaces` or `Sessions` section from the navigation bar on the left side.

> Sessions allow searching for a specific user, while `Workspaces` lists the available devices. When performing remote assistance on a device, it will be conducted on the session that is currently active.

3. Search and/or select the device/session on which remote assistance will be performed.



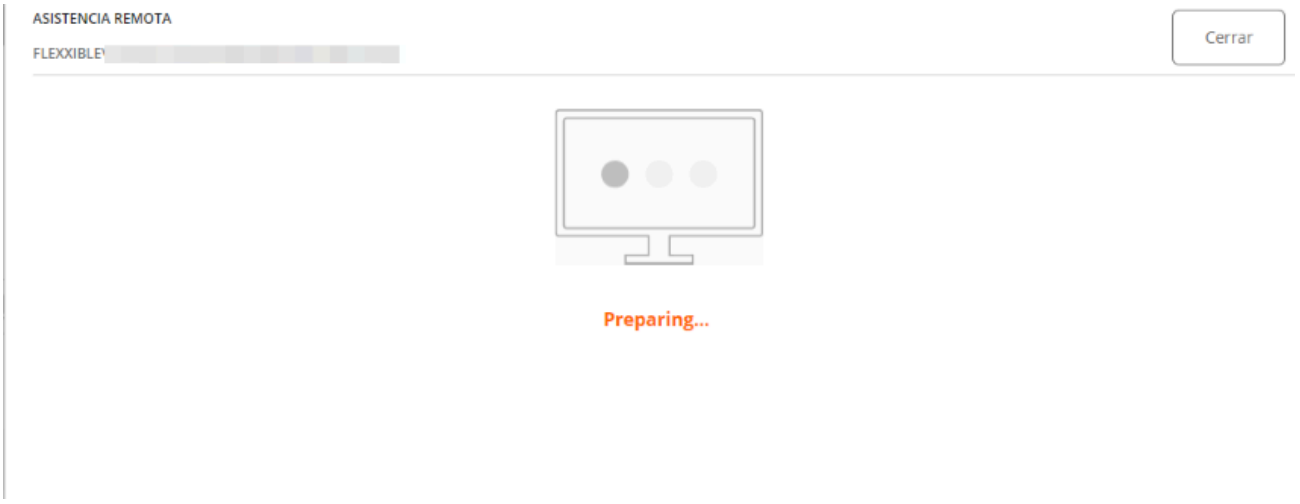
4. Open the `Operations` menu on the button in the upper bar of the equipment list. In some cases, as in the previous image, the button will be behind the button with three dots (...) on the mentioned bar. Next, select:

   `Operations` -> `Remote Assistance` -> `Start remote assistance`

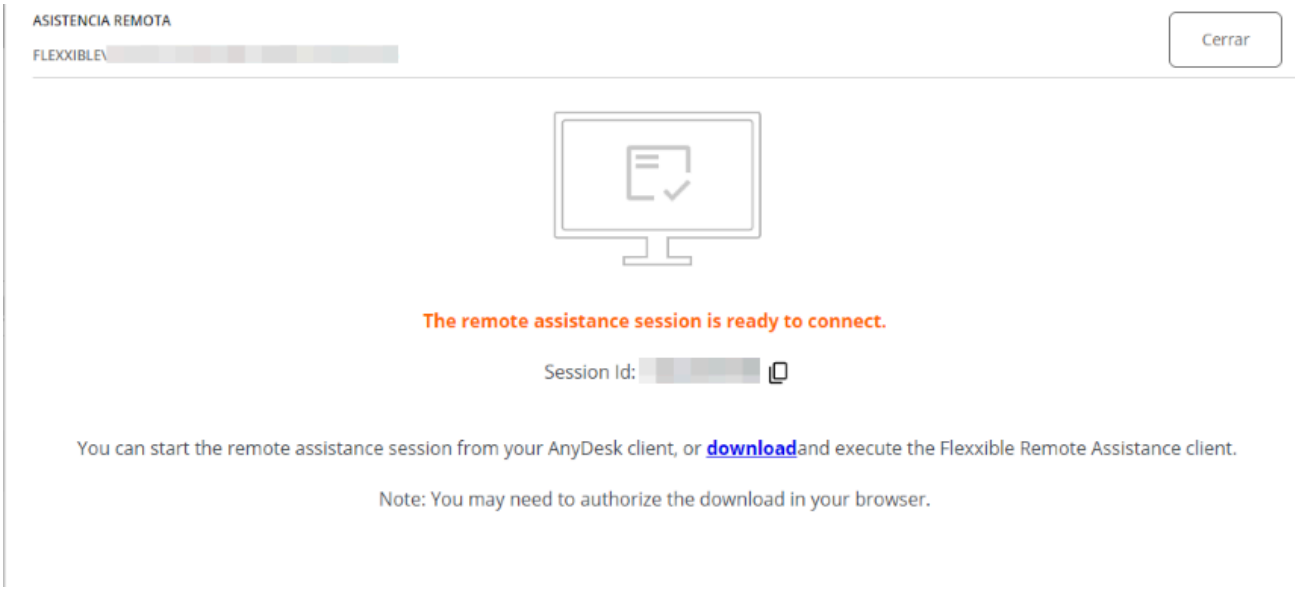
5. Select `Ok` to confirm the operation.

6. A floating panel will appear indicating that remote assistance is being prepared.

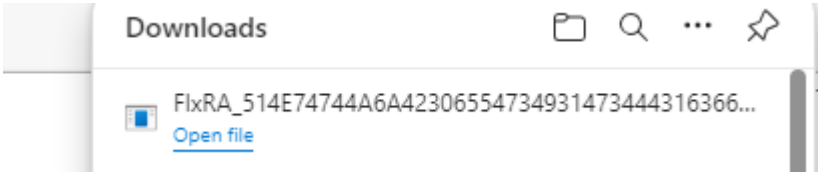
Copyright © 2024 Flexxible. Todos los derechos reservados.



7. Once prepared, the information will appear.

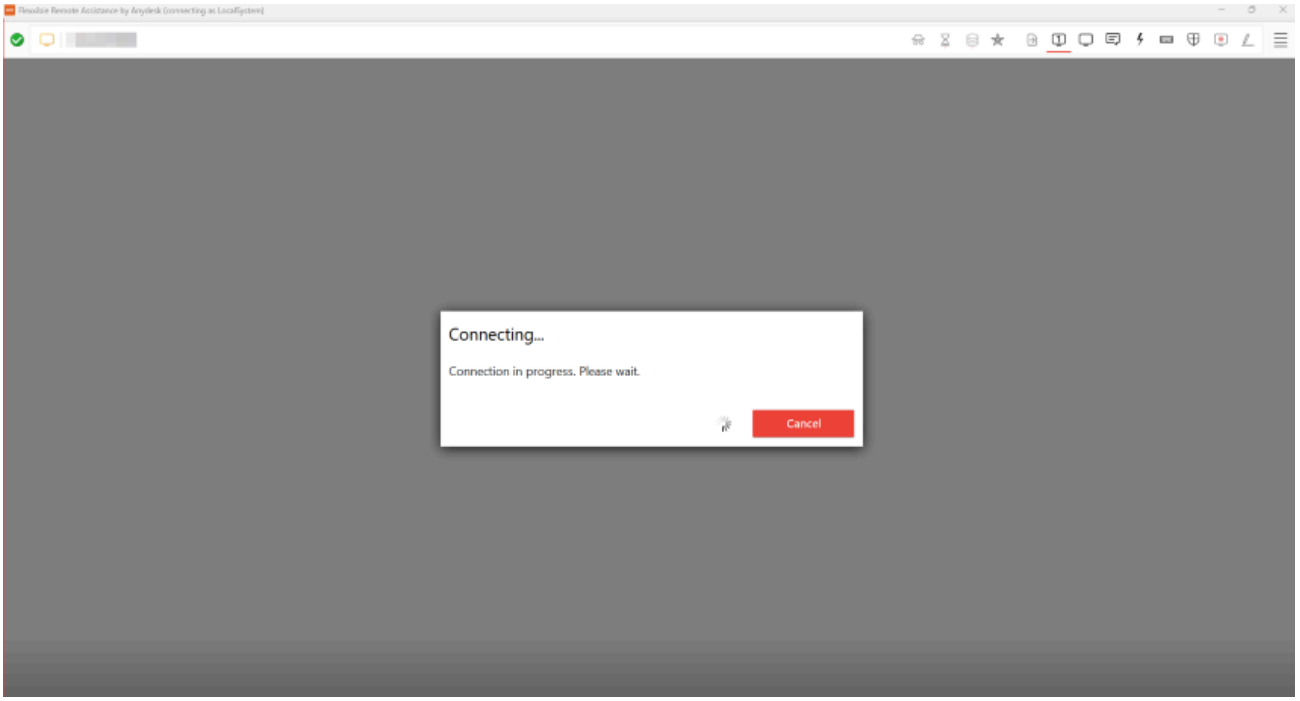


8. This assistance is temporary and the operator needs to download an executable file from the `download` link in this floating panel.



9. Download and run the file. This operation will run an application to facilitate remote assistance. The operator will have to wait for the user to give permission to perform remote assistance on their device.

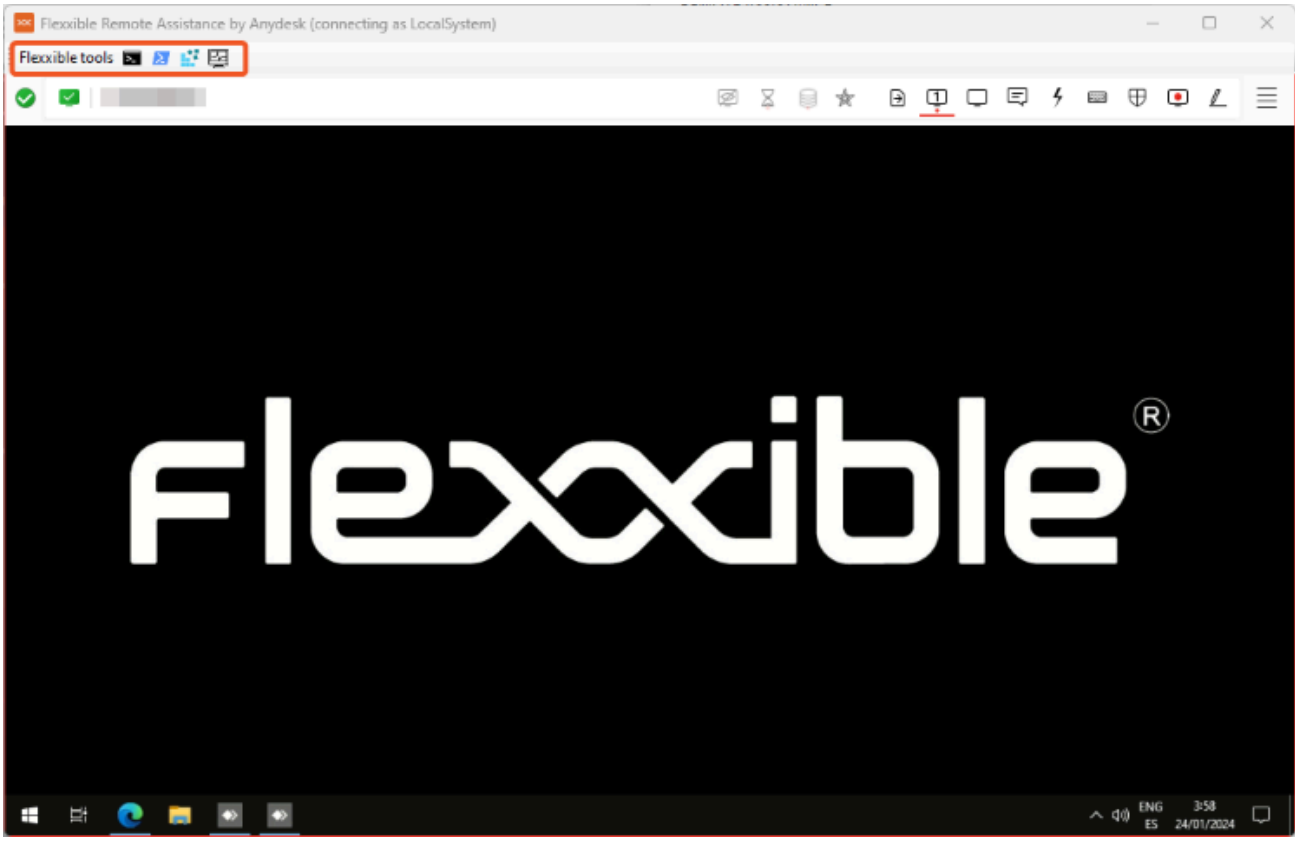
Copyright © 2024 Flexxible. Todos los derechos reservados.



10. Once the user grants their consent, the remote assistance session can be conducted. The operator has access to the user's desktop and can perform operations and provide the needed help to solve the user's problems.

If the operator has the necessary permissions and is in a user session without administrative permissions, they can use `Flexxible Tools` to act on the device with administrative permissions:

Copyright © 2024 Flexxible. Todos los derechos reservados.



Copyright © 2024 Flexxible. Todos los derechos reservados.

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

Copyright © 2024 Flexxible. Todos los derechos reservados.

- 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

Copyright © 2024 Flexxible. Todos los derechos reservados.