

Documentation FXXOne

Document generated on: 7/7/2025

Contents

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

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

Offline installation steps	<u>75</u>
install	<u>76</u>
Uninstallation script parameters	<u>76</u>
Examples	<u>76</u>
odate	<u>77</u>
ormation obtained from the device	<u>77</u>
General information	<u>78</u>
Extended Info	<u>78</u>
Information in tabs	<u>79</u>
gent / Supported Systems / ChromeOS	<u>81</u>
<u>quirements</u>	<u>81</u>
pported versions	<u>81</u>
nitations	<u>81</u>
wnload and installation	<u>81</u>
Installation	<u>82</u>
odate	<u>85</u>
ormation obtained from the device	<u>85</u>
General information	<u>86</u>
Extended Info	<u>87</u>
Information in tabs	<u>87</u>
gent / Supported Systems / Android	<u>90</u>
<u>quirements</u>	<u>90</u>
pported versions	<u>90</u>
nitations	<u>90</u>
ttings	<u>90</u>
stribution	<u>91</u>
wnload and installation	<u>91</u>
odate	<u>95</u>
ormation obtained from the device	<u>95</u>
General information	<u>96</u>
Extended Info	<u>97</u>
Information in tabs	<u>97</u>
gent / Network and Security	100
quired URLs and Ports	100
	install

	• <u>Security</u>	<u>102</u>
	Antivirus exclusions	<u>102</u>
	Deep SSL Inspection	<u>103</u>
	PowerShell process restriction	<u>103</u>
	 Wake on LAN (WoL) 	<u>103</u>
	Configure Wake on LAN (WoL) in Windows	<u>104</u>
	 <u>Remote assistance through a proxy</u> 	<u>105</u>
	∘ <u>vPro</u>	<u>105</u>
	Requirements for vPro operation via a proxy	<u>105</u>
•	FlexxAgent / Wake on LAN (WoL)	<u>106</u>
	• <u>Requirements</u>	<u>106</u>
	 Set up WoL in Windows 	
	 <u>Available actions</u> 	<u> 107</u>
	Power on devices on demand from Workspaces	<u> 107</u>
	Schedule power on using Workspace Groups	<u> 107</u>
	Schedule power on after applying updates	<u> 107</u>
•	FlexxAgent / FlexxAgent Guides	<u>111</u>
•	FlexxAgent / Guides / Validate FlexxAgent connectivity	<u>112</u>
	 <u>Creating a scheduled task</u> 	<u>112</u>
	 Validation of results 	<u>118</u>
•	FlexxAgent / Guides / Install FlexxAgent by configuring a proxy server	<u>120</u>
	• Example	120
	 Explanation of the options 	<u>121</u>
	proxyPersistConfig	<u>121</u>
٠	FlexxAgent / Guides / Set up a proxy server through group policies (GPO)	<u>123</u>
٠	FlexxAgent / Guides / Deploy FlexxAgent via group policy (GPO)	129
	 <u>Deploying</u> 	<u>129</u>
	• <u>Verification</u>	<u>132</u>
•	FlexxAgent / Guides / Deploy FlexxAgent with Microsoft Intune	<u>135</u>
•	FlexxAgent / Guides / Deploy FlexxAgent for Android with Microsoft Intune	<u>135</u>
•	<u>Analyzer</u>	<u>149</u>
	 Included tools 	149
	• <u>Web Interface</u>	<u>150</u>
	List Views	<u>150</u>
	Detail Views	<u>. 151</u>

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

٠	Analyzer / App Groups	<u>179</u>
	 <u>Group Types</u> 	<u>179</u>
	 Users consuming applications in the selected group 	<u>180</u>
	 Creating a New Application Group 	<u>180</u>
٠	Analyzer / App Versions	<u>. 181</u>
	 Graphical view 	<u>. 181</u>
	 <u>Table view</u> 	<u>181</u>
•	Analyzer / Polls	<u>183</u>
	 Poll Settings 	<u>183</u>
	 List view 	<u>183</u>
	 Detail view 	<u>183</u>
	Poll Execution	<u>185</u>
٠	Analyzer / Users in Analyzer	<u>186</u>
	• <u>List view</u>	<u>186</u>
	• <u>Detail view</u>	<u>186</u>
	User data in the detail view	<u>187</u>
٠	Analyzer / User Groups	<u>189</u>
	• <u>List view</u>	<u>189</u>
	 <u>Detail view</u> 	<u>189</u>
٠	Portal	<u>191</u>
	 <u>Sidebar menu</u> 	<u>191</u>
	Menu collapse	<u>192</u>
	 Organization selector 	<u>192</u>
	 <u>User Settings</u> 	<u>193</u>
	 <u>Operations List</u> 	<u>193</u>
	My logins	<u>193</u>
	 <u>Settings</u> 	<u>193</u>
	 Navigation bar 	<u>195</u>
	 Considerations about the navigation bar 	<u>195</u>
	• <u>Tables</u>	<u>196</u>
	Top bar	<u>196</u>
	Content	<u>197</u>
	 <u>Bottom bar</u> 	<u>198</u>
٠	Portal / Access and authentication	<u>199</u>
	 Authentication with a Microsoft Entra ID or Google account 	<u>199</u>

		 Enterprise Application Consent and Permissions in Entra ID 	<u>199</u>
	0	Authentication with email and password	<u>199</u>
		Login process	<u>202</u>
	0	Access to email and password authentication	<u>203</u>
		Enable access for a new user	<u>203</u>
		Enable access for a batch of users	<u>203</u>
		Enable access from the user table	<u>203</u>
		Reset the password from the user table	<u>205</u>
	0	Authentication security settings	<u>206</u>
	0	User-level authentication security settings	<u>207</u>
		 <u>Two-factor authentication</u> 	<u>207</u>
		Password	. 211
	0	Authentication security settings at the organization level	212
		Enable or disable the email and password authentication option at the	<u>212</u>
		organization level	
		 User table 	212
		 User authentication detail 	<u>213</u>
•	Port	tal / Analyzer in Portal	<u>213</u>
•	Port	tal / Analyzer / Installed apps	215
	0	Installed Apps Details	<u>216</u>
		<u>Overview</u>	<u>217</u>
		 Versions 	217
		 Workspaces 	217
		Installation history	<u>217</u>
		Report history	217
•	Port	tal / Analyzer / Licenses	217
	0	Types of licenses	221
	0	Create a License	221
	0	License list	221
	0	License detail view	<u>223</u>
		Details	<u>223</u>
		Installed apps	<u>223</u>
		 <u>Usage history</u> 	<u>224</u>
		Running Processes	
•	Port	tal / Analyzer / SAM	<u>226</u>

•	Portal / Monitor in Portal	<u>227</u>
•	Portal / Monitor / Active alerts	<u>229</u>
	• <u>Alert detail view</u>	<u>230</u>
•	Portal / Monitor / Alert Configuration	<u>231</u>
	 <u>Create a new alert setting</u> 	<u>232</u>
	 <u>Alert Severity</u> 	<u>233</u>
	 <u>Alert categories</u> 	<u>234</u>
	• Detail view	<u>234</u>
	 Edit alert settings 	<u>235</u>
	• <u>Sidebar menu</u>	<u>235</u>
	 Overview 	<u>236</u>
	 Active alerts 	<u>236</u>
	 Microservices 	<u>236</u>
	Send history	<u>236</u>
•	Portal / Operations	<u>237</u>
•	Portal / Flows	<u>238</u>
	• <u>Overview</u>	<u>240</u>
	Edit and delete a flow	. <u>241</u>
	• <u>Target</u>	<u>242</u>
	• <u>Flow</u>	<u>242</u>
	Flow conditions	<u>243</u>
	• Notification	<u>244</u>
•	Portal / Reports	<u>248</u>
	 Considerations about the reports 	<u>249</u>
	 <u>Report inventory</u> 	<u>249</u>
	Office 365, Chrome and Adobe Workspaces Inventory	<u>249</u>
	 Office 365 Versions List 	<u>249</u>
	 Workspaces Inventory 	<u>249</u>
	 Generate a report 	<u>249</u>
	 Share a report 	<u>253</u>
	Share the last report	<u>254</u>
	Delete a recipient	<u>254</u>
	 Share a specific report 	<u>256</u>
•	Portal / Tenants	<u>256</u>
	 <u>Types of organizations</u> 	<u>258</u>

	Partner-type organizations	<u>258</u>
	 <u>Client-type organizations</u> 	<u>258</u>
	 <u>Suborganizations</u> 	<u>258</u>
	 List of tenants 	<u>258</u>
	 Tenant interface 	<u>259</u>
•	Portal / Tenants / Activation	<u>260</u>
•	Portal / Workspaces in Portal	<u>261</u>
	• Device detail view	<u>263</u>
	 <u>Overview</u> 	<u>263</u>
	Installed apps	<u>264</u>
	 <u>Active alerts</u> 	<u>265</u>
	 <u>Operations</u> 	<u>266</u>
	Sessions	<u>267</u>
	 Windows services 	<u>267</u>
	Disks	<u>267</u>
	Reporting groups history	<u>268</u>
	Plug and Play (PnP) events	<u>268</u>
	Plug and Play (PnP) errors	<u>269</u>
	Group Policy (GPO)	<u>269</u>
	Boot history	<u>269</u>
•	Portal / Workspaces / Workspace groups	<u>269</u>
	 <u>Static workspace group</u> 	<u>271</u>
	 <u>Dynamic workspace group</u> 	<u>271</u>
	 Entra ID Workspace group 	<u>. 271</u>
	 <u>Group management</u> 	<u>272</u>
	 Workspace Group Details 	<u>272</u>
	 Workspaces 	<u>272</u>
	 <u>History</u> 	<u>272</u>
	Location	<u>272</u>
	Schedule	<u>272</u>
	■ <u>Sync</u>	<u>272</u>
	• <u>Create groups</u>	<u>276</u>
	Create a static workspace group from the Portal	<u>277</u>
	Create a static workspace group from Workspaces	<u>277</u>
	Create a dynamic workspace group	<u>279</u>

 Create a Workspace group Enter ID 	<u>279</u>
• <u>Group editing</u>	<u> 280</u>
 Edit a dynamic workspace group 	<u>281</u>
 Delete a workspace group 	<u>281</u>
Portal / Microservices	<u> 282</u>
Main characteristics of microservices in Portal	<u> 283</u>
Access to a centralized catalog	<u> 284</u>
 Creation of customized microservices 	<u>284</u>
 Execution scope configuration 	<u> 284</u>
Ways to consume microservices	<u>284</u>
 On-demand execution from Workspaces 	<u> 285</u>
 Scheduled execution through Flows 	<u>285</u>
Scheduled execution through Alert Settings	<u> 286</u>
End-user execution	<u>287</u>
Portal / Microservices / Enabled	<u> 287</u>
• <u>Microservice detail</u>	<u>291</u>
 Overview 	<u> 291</u>
 <u>Code</u> 	<u> 291</u>
 <u>Targets</u> 	<u> 291</u>
 <u>Settings</u> 	<u> 291</u>
 Alert Configuration 	<u>291</u>
License	<u>294</u>
Enabled Tenants	<u>294</u>
Portal / Microservices / Marketplace	<u>294</u>
 Microservice detail 	<u> 296</u>
 <u>Overview</u> 	<u>296</u>
Code	<u>296</u>
 <u>Targets</u> 	<u>296</u>
 <u>Settings</u> 	<u>296</u>
Alert Configuration	<u> 296</u>
■ <u>License</u>	<u>299</u>
Enabled Tenants	<u> 299</u>
Portal / Microservices / Designer	<u>299</u>
<u>Microservice creation</u>	<u>301</u>
Phase 1	<u> 301</u>

	Phase 2 - License	<u>301</u>
	Phase 3 - README	<u>302</u>
	Phase 4 - Script	<u> 302</u>
	 <u>Code</u> 	<u>304</u>
•	Portal / Microservices / Audit Log	<u></u>
•	Portal / Patch	<u> 306</u>
	 Patching management features 	<u>307</u>
	 Patching management considerations in Portal 	<u>307</u>
	FlexxAgent behavior in patch management	<u>307</u>
•	Portal / Patch / Summary	<u>308</u>
•	Portal / Patch / Reporting groups in patch management	<u>309</u>
	 <u>Total devices per reporting group</u> 	<u> 311</u>
•	Portal / Patch / Targets	<u>311</u>
	 <u>Create a new target</u> 	<u>313</u>
	 <u>Target details</u> 	<u></u>
	Details	<u></u>
	Schedule	<u> 314</u>
	 <u>Update process</u> 	<u>314</u>
•	Portal / Patch / Microsoft patches	<u>316</u>
•	Portal / Patch / Microsoft patch policies	<u>316</u>
	 <u>Create a new update policy</u> 	<u> 316</u>
	• <u>Details</u>	<u>318</u>
	 <u>Microsoft patches</u> 	<u>319</u>
	Approve or reject a Microsoft update	<u></u>
	 <u>Automatic Approvals</u> 	<u>320</u>
	 Create an automatic approval rule 	<u>321</u>
	 <u>Unlisted updates</u> 	
	Approve or reject an unlisted update	
	 <u>Unlisted automated approvals</u> 	
	 Create an automatic approval rule for unlisted updates 	
•	Portal / Settings	
•	Portal / Settings / Organization	
	• <u>General</u>	
	• <u>Branding</u>	
	 <u>Microservices Configuration</u> 	<u>329</u>

	 <u>Authentication</u> 	<u>329</u>
	 User table 	<u>329</u>
	 User authentication detail 	<u> 334</u>
	• Products	<u> 334</u>
	 View details 	<u>335</u>
	Agent settings	<u> 336</u>
	• Modules	<u> 336</u>
	Create module	<u> 338</u>
•	Portal / Settings / Roles	<u> 339</u>
	• Create a new role	<u>341</u>
•	Roles table	<u>341</u>
	<u>Roles Subtable</u>	<u> 342</u>
•	<u>Detail view</u>	<u>342</u>
	 <u>Details</u> 	<u> 343</u>
	 Permissions 	<u> 343</u>
	<u>All tenants</u>	<u> 343</u>
	Tenant	<u> 343</u>
	Portal Permissions	<u>343</u>
	 Workspaces permissions 	<u>344</u>
	Analyzer permissions	<u> 344</u>
	All reporting groups	<u> 345</u>
	Reporting Groups	<u> 345</u>
	• <u>Users</u>	<u>345</u>
•	Portal / Settings / Roles / Roles included by default	<u>345</u>
٠	Portal / Settings / Roles / Access levels	<u> 346</u>
	 Levels of access by modules 	<u>349</u>
	Portal	<u> 349</u>
	 Workspaces 	<u> 350</u>
	Analyzer	<u>350</u>
٠	Portal / Settings / Users	<u>350</u>
	• <u>Create users</u>	<u>362</u>
	<u>Create a batch of users</u>	<u></u>
	Export users	<u>363</u>
	Delete users	<u> 363</u>
	Email login actions	<u>364</u>

	 <u>Additional options</u> 	<u>364</u>
•	Portal / Settings / Integrations	<u>365</u>
	 Integration with Entra ID 	<u>366</u>
	Enable integration with Entra ID	<u>366</u>
	 Integration with Intel vPro[®] Enterprise 	<u>366</u>
	Requirements	<u>367</u>
	Enable integration with Intel vPro [®] Enterprise	<u>367</u>
	<u>CrowdStrike integration</u>	<u>369</u>
	Enable integration with CrowdStrike	<u>372</u>
•	Portal / Settings / Reporting Groups	<u>373</u>
	 <u>Reporting groups creation</u> 	<u>374</u>
	Fishing pattern	<u>374</u>
	 <u>Reporting groups list</u> 	<u>375</u>
	Auto update of FlexxAgent	<u>376</u>
	 View details 	<u>376</u>
	FlexxAgent configuration (Remote Assistance)	<u>376</u>
•	Portal / Settings / FlexxAgent Versions	<u>380</u>
	• <u>Version settings</u>	<u>382</u>
	Steps for configuration:	<u>382</u>
	Management from Workspaces	<u>382</u>
•	Portal / Settings / Directives	<u>384</u>
	• <u>New Directive</u>	<u>386</u>
•	Portal / Portal Guides	<u>386</u>
•	Portal / Guides / Create and manage workspace groups	<u>388</u>
	<u>Static workspace groups</u>	<u>389</u>
	 Create a static workspace group from the Portal 	<u>389</u>
	 Create a static workspace group from Workspaces 	<u>389</u>
	Dynamic workspace groups	<u>390</u>
	 Create a dynamic workspace group 	. <u>391</u>
	<u>Workspaces Enter ID groups</u>	<u>391</u>
	 Create a Workspace group Enter ID 	
	<u>Manage a workspace group from Portal</u>	<u>392</u>
	 Manage a workspace group from Workspaces 	<u>393</u>
•	Portal / Guides / Run microservices on a scheduled basis	<u>395</u>
	 Schedule a microservice execution 	<u>397</u>

٠	Portal / Guides / Patch policy	<u> 397</u>
	• Define the patch policy	<u>401</u>
•	Portal / Guides / Enable microservices for the end user	<u>401</u>
	 How to enable a microservice for the end-user 	<u>403</u>
	Rename the microservices folder	<u>403</u>
•	Portal / Guides / Set up integration with CrowdStrike	<u>406</u>
	 API Configuration in CrowdStrike 	<u>408</u>
	<u>Configuration in Portal</u>	<u>408</u>
	 <u>View from Workspaces</u> 	<u> 411</u>
•	Portal / Guides / Configure integration with Entra ID	<u>413</u>
	 <u>Requirements for integration</u> 	<u>415</u>
	<u>Configuration in Microsoft Azure</u>	<u>415</u>
	 Create an application registration 	<u>415</u>
	 Create a client secret 	<u>415</u>
	 Configure permissions for the application registration 	<u>415</u>
	 Permissions in the Azure subscription 	<u>415</u>
	<u>Configuration in Portal</u>	<u>415</u>
•	Portal / Guides / Set up Entra ID integration with Monitor	<u> 424</u>
	 Configuration in Microsoft Azure 	<u>426</u>
	 Create an application registration 	<u>426</u>
	 Create a client secret 	<u> 426</u>
	API permissions configuration	<u>426</u>
	 Create application roles 	<u> 426</u>
	Review the manifest.xml file	<u>426</u>
	 <u>Requirements</u> 	<u>426</u>
•	Portal / Billing	<u>438</u>
	 View from a partner-type organization 	<u>440</u>
	 <u>Overview</u> 	<u> 440</u>
	 Tenants consumption details 	<u>440</u>
	 <u>View from a client-type organization</u> 	<u>440</u>
	 Overview 	<u> 443</u>
	 FlexxAgent consumption 	<u>443</u>
	Steps to remove a device from a reporting group	<u> 444</u>
•	Workspaces	<u> 445</u>
	 Interface and Access Segmentation 	<u>445</u>

	Level 1	<u>446</u>
	Level 2	<u>446</u>
	 List Views 	<u>446</u>
	 Filtering Options 	<u>447</u>
	• <u>Detail Views</u>	<u>447</u>
•	Workspaces / Level 1	<u>450</u>
٠	Workspaces / Level 1 / UX Panel	<u>451</u>
	• <u>Organization filtering</u>	<u>452</u>
	• <u>Date filtering</u>	<u>452</u>
	• <u>Widgets</u>	<u>453</u>
	Default widgets	<u>453</u>
•	Workspaces / Level 1 / Workspaces View	<u>453</u>
	• <u>Filtering</u>	<u>458</u>
	 Header filtering options 	<u>458</u>
	Filtering Options	<u>458</u>
	Filter management	<u>459</u>
	 Microservices execution 	<u>461</u>
	 <u>Available operations</u> 	<u>462</u>
	• <u>Operations from the list view</u>	<u>462</u>
	Power and connection actions	<u>463</u>
	■ <u>Tags</u>	<u>463</u>
	FlexxAgent	<u>463</u>
	Maintenance (drain mode)	<u>464</u>
	Refresh device info	<u>464</u>
	Force compliance check	<u>464</u>
	Force update custom fields	<u>464</u>
	Remote Administration	<u>464</u>
	Remote Assistance	<u>465</u>
	Device type	<u>465</u>
	 Notifications 	<u>465</u>
	Change the report group	<u>466</u>
•	Workspaces / Level 1 / Workspaces / Detail view	<u>466</u>
	<u>Available actions</u>	<u>467</u>
	 Microservices execution 	<u>467</u>
	 <u>Operations</u> 	<u>467</u>

	0	Information obtained from the device	<u>467</u>
٠	Wo	rkspaces / Level 1 / Workspaces / Remote Assistance	<u>469</u>
	0	Features	<u>471</u>
	0	Privacy	<u>471</u>
	0	Types of remote assistance	. <u>471</u>
	0	Interactive remote assistance	<u>472</u>
	0	Unattended remote assistance	<u>472</u>
	0	Dynamic remote assistance	<u>472</u>
	0	Requirements to perform remote assistance	<u>472</u>
	0	<u>Settings</u>	<u>475</u>
	0	Activation	<u>475</u>
		 Activation file download 	<u>476</u>
	0	Processes	<u>478</u>
	0	Behavior of remote assistance through proxy	<u>480</u>
	0	Flexxible Tools	<u>480</u>
•	Wo	rkspaces / Level 1 / Sessions	<u>480</u>
	0	Available operations	<u>483</u>
		 <u>Session management</u> 	<u>484</u>
		Remote Assistance	<u>484</u>
		 Notifications 	<u>484</u>
•	Wo	rkspaces / Level 1 / Sessions / Detail view	<u>484</u>
	0	Available actions	<u>486</u>
		 Microservices execution 	<u>486</u>
		 <u>Operations</u> 	<u>486</u>
	0	General	<u>486</u>
	0	Tabs	<u>487</u>
		 <u>Connections</u> 	<u>488</u>
		Performance	<u>488</u>
		Login information	<u>488</u>
		 Notifications 	<u>488</u>
		 <u>Group Policy (GPO)</u> 	<u>488</u>
•	Wo	rkspaces / Level 1 / Connection Logs	<u>488</u>
•	Wo	rkspaces / Level 1 / Job	<u>491</u>
	0	List view	<u>492</u>
		Top options	<u>492</u>

	Jobs list	<u>492</u>
	• <u>Detail view</u>	<u>493</u>
	 <u>Statuses</u> 	<u>493</u>
	<u>Available information</u>	<u>493</u>
	Logs	<u>494</u>
	 Workspaces 	<u>. 494</u>
	 Job subscription 	<u>494</u>
•	Workspaces / Level 2	<u> 495</u>
•	Workspaces / Level 2 / Event Logs	<u>. 496</u>
	• <u>Detail view</u>	<u>497</u>
	Event log information on a device	<u> 500</u>
	 Additional event settings 	<u> 500</u>
•	Workspaces / Level 2 / Locations	<u> 500</u>
	• <u>List view</u>	<u> </u>
	• <u>Detail view</u>	<u> </u>
•	Workspaces / Level 2 / Networks	<u> </u>
	• <u>List view</u>	<u> 504 </u>
	• <u>Detail view</u>	<u>504</u>
•	Workspaces / Level 2 / Notifications	<u> 504</u>
	 Notifications section 	<u> 506</u>
	 <u>Types of notifications</u> 	<u>506</u>
	Popup notifications	<u>. 506</u>
	 <u>Notifications</u> 	<u>506</u>
•	Workspaces / Level 2 / Reporting groups from Workspaces	<u>506</u>
	• <u>List view</u>	<u> 511</u>
	Download FlexxAgent	<u>511</u>
	• <u>Detail view</u>	<u> 511</u>
	Devices	<u> 513</u>
•	Workspaces / Level 2 / Servers	<u>513</u>
	• <u>List view</u>	<u> 515</u>
	 <u>Available operations</u> 	<u>515</u>
	 <u>Detail view</u> 	<u> </u>
	 <u>General</u> 	<u> 516</u>
	Extended	<u> 516</u>
	 <u>Tabs</u> 	<u> 517</u>

•	Workspaces / Level 2 / Wireless networks	<u>518</u>
	• List view	<u>522</u>
	• <u>Detail view</u>	<u>522</u>
•	Workspaces / Workspace Guides	<u>522</u>
•	Workspaces / Guides / Provide remote assistance to a user	<u>524</u>
•	Workspaces / Guides / Change Automatic Restart Sign-On (ARSO) settings	<u>525</u>
	 Deactivate ARSO settings on a device 	<u>529</u>

Introduction

FXXOne is a SaaS Remote Monitoring and Management (RMM) platform that enables the analysis, management, and monitoring of your user's work devices.

It has many features, including secure remote assistance, detailed collection of diagnostic data, system status notifications, self-healing of known issues, and unattended implementation of support procedures.

FXXOne includes the following modules:

- Portal
- <u>Workspaces</u>
- <u>Analyzer</u>

To start using **FXXOne**, in addition to the subscription, the installation of <u>FlexxAgent</u> on user devices is required. As soon as it starts reporting, you'll be able to access the different modules that make up the platform.

Once the subscription is created, the steps to start enjoying the service are as follows:

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



From that moment, the devices will report to the service and can be managed from Workspaces; additionally, through Analyzer, analytical data of the applications, user experience, and other devices can be obtained.

We also recommend:

- Explore the microservices available in the Marketplace and activate the ones you prefer.
- Grant access to other technicians to the consoles.

We hope you enjoy **FXXOne** :)

Documentation in PDF

La documentación de FXXOne para esta versión se puede descargar aquí en formato PDF.

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

FlexxAgent

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

FlexxAgent is compatible with <u>Windows</u>, <u>Linux</u>, <u>macOS</u>, <u>ChromeOS</u>, and <u>Android</u> operating systems.

Flexxible 🛄	_		🔒 Mi organización 🗸	Administrador de Organización
ය Inicio		FxxOne Agent -	×	
启 Inquilinos	÷ F	🚾 rlexxible"		
Ø Microservicios				+ Nuevo
Settings ^		Downloading FlexxAgent		
Información	No		Ac	ción
Usuarios	Se	Copyright © Flexible	C	Ver detalle 🗘 Descargar agente
Productos	VIP	Interactivo	C	Ver detalle 🗘 Descargar agente
Módulos	Eamil	ia Interactivo	8	Ver detalle 🛛 🗘 Descargar agente

Features

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

Functionality

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

Feature	Windows	Linux	macOS	Android	ChromeOS
Storage information	***	***	***	**	**
Network information	***	***	***	**	**
System hardware information	***	**	**	*	*
System performance information	***	**	**	*	*
User session performance information	***	**	**	*	*
Diagnostic information	***	**	**	*	*
User notifications	***	**	**	*	*
Installed apps					

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

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



Data retention

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

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

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

FlexxAgent / Supported Systems

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

- <u>Microsoft Windows</u>
- Linux
- macOS
- <u>ChromeOS</u>
- <u>Android</u>

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.

	Administrador de tareas	Q. Busque un	nombre, publi	cador o P.			- 0	×
≡	Procesos	E Ejec	utar nueva tarea	0 F	inalizar tarea	🕼 Mode	de eficiencia	
I PP	^ Nombre	Estado	19% CPU	88% Memoria	0% Disco	0% Red		
ۍ ۲	 FlexxAgent FlexxAgent service 		0%	98,5 MB	0 MB/s	0 Mbps		
_	🐱 FlexxAgent Analyzer		0%	34,6 MB	0 MB/s	0 Mbps		

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

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.

Software Requirements

FlexxAgent also requires certain software components:

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

Considerations for Windows versions in EOL

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

Limitations

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

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

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

Windows 7 and 2008

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

- The update <u>KB4474419</u>: 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 <u>KB3140245</u>: 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.

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.

Flexcible III					·			•
ώ			Inicio Flexable					
焰	Inquilinos							
Ø	Microservicios	~	O	ଜ	.+.			
0	Settings	~	Workspaces	Analyzer	Descargar agente			
			Tus productos			J		
			Entorno		Tipo de	producto	Acción	
			ExcOne		Foot	One	Ver detalle	

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.

Flexxible 💷			💄 My a	Change: Ctrl + K rganization Default: Ctrl + D	Organization Admin	
là Home	Home					
Operations						
5 Flows PREVIEW		ଛ	.+.			
ස් Tenants 🗸 🗸	Workspaces	Analyzer	Download Agent	Generate magic link		
🖙 Workspaces 🗸 🗸						
🛱 Patch 🛛 🛤 🗸 🗸	Your products					
Ø Microservices	Environment 🔃			Product type 1	Action	
Settings ^	ONE			FXXOne	View Detail	
Information						
Billing						
Users						

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.

Flexodble III		La free free free free free free free fre	Create magic link ×
 A mean A mea	Nachland Andream A V Dank Nas van Maria - Com Charl (1995) - Com Charles (1995) - C	Magic link created The magic link has been created successfuly Imagic link will expire or: 1/1/1/4, 10224 PM Intersubing fink will expire or: 1/1/1/4, 10224 PM Intersubing fink will expire or: 1/1/1/4, 10224 PM States of the subing final expire or: 1/1/1/4, 10224 PM	API Key generated successfully

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.

Flexxible 🔢			All organization	Change: Ctrl + K Default: Ctrl + D	Organization Admin	
ය Home	Reporting groups > VIP					
Operations	VIP					
56 Flows PRIMEW	Details Roles Users Magic Links					
🖧 Tenants 🗸 🗸						
🗈 Workspaces 🗸 🗸	🕂 Create 📵 Export 🖔 Refresh					4
🛱 Patch 🛛 🛤 🗸 🗸	O Search by term	√ Filter				
🕅 Microservices 🗸 🗸	Created at 11 Created by 11	Magic link 🛍	Expires at 11 Revoked at 11	Last used al 🏦 🛛 Do	wnloads †↓ Action	
Settings ^	12/3/24, 1:02:24 F	https://oneflexxible.com/magic-link?key=b65	12/10/24, 1:02:24 -	-	0 🚫 Revoke	
Information	12/3/24, 12:08:33	https://one.flexxible.com/magic-link?key=91b	12/4/24, 12:08:33 -	12/3/24, 12:18:19	1 🚫 Revolue	
Billing	12/3/24, 11:06:01	https://oneflexxible.com/magic-link?key=at2	12/8/24, 11:06:01	12/3/24, 11:09:27	1 🚫 Revoke	
Users						

Use a magic link

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



Revoke a magic link

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

A window will appear to confirm the action.

Flexcible 🔛					Organization Admin	
Patch Peavew Patch Peavew Microservices Settings	Recording groups > VIP VIP Details Roles Users Magic Links					
Information Billing Usens	+ Create 🔮 Export 🕐 Refresh	 Created at: 12/3/24, 12:08:33 PM 				2
Roles	Created at ${\ensuremath{\mathbb T}}$	 Created by: Last used at: 12/3/24, 12:18:19 PM Downloads: 1 	Revoked at †↓ Last use	d at †∔ Downloads †∔	Action	
Products Modules	12/3/24, 102:24 F	OK Cancel	 - 12/3/24, t		⊗ Revoke	
Integrations	12/3/24, 11:06:01	https://oneflexxible.com/magic-lin 12/8/24, 1:06:01			⊗ Revoke	
Reporting groups						

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

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.

Fle×	WORKSPACES		C Log Off
Search Q Level 1 > Level 2 ~ Alert notification profiles	Reporting groups		My Filters
Alert subscriptions	🖃 id	Name †	Tenant
		physical	reactions
P Locations		(annulation)	(meclimanit)
			(measurement)
e e e e e e Networks	Count=3		
Notifications	< 1 >		Page size 20 *

A window will open to download the FlexxAgent installer.

Download FlexxAgent Installer				OK Cancel				
Download a .zip file to install	l or repair FlexxAgent on machines	comr	nunicating through this messaging s	ervice.				
Target processor architecture	x64	•	Generate standalone installer (offl	ine)				
Please refer to http://5fbe840348819.helpdocsonline.com for information on the FlexxAgent-Installer.exe command line arguments.								

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

Unattended Deployment

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

Installation

The unattended installation of FlexxAgent is done via PowerShell.

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

Uninstall

To uninstall FlexxAgent unattended:

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

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

Files

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

Folders

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

Reinstallation

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

FlexxAgent-Installer.exe -repairAgent

For example:

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

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 <u>Product level</u> and at the <u>Reporting Group level</u>.

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 -> Products.
- 2. In the table, choose the environment where you want to execute the functionality, and in the Action field click on Agent Settings.
- 3. In the form, enable or disable the FlexxAgent Uninstallation Protection button.
- 4. Click on Save.

Configuration at Reporting Groups Level

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

Enable protection for a reporting group

- 1. Go to Portal -> Settings -> Reporting Groups.
- 2. In the table, choose the reporting group where you want to execute the functionality, and in the Action field click on Agent Settings.
- 3. In the form, edit the FlexxAgent Uninstallation Protection feature (pencilshaped button) to choose whether to enable or disable it.
- 4. Click on Save.

() INFO

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

Edit FlexxAgent settings		×
Environment		
FlexxClient		\sim
Uninstall protection ①		0
Auto update		0
Remote support		
Interactive		0
Unified reporting URL		
Disabled		0
× c	ancel	Save

Enable protection for multiple reporting groups

1. Go to Portal -> Settings -> Reporting Groups.

- 2. In the table, select the reporting groups where you want to execute the functionality.
- 3. Click on Edit uninstallation protection. Three options will be displayed:
- Enable uninstallation protection. Protects the reporting groups against uninstallation of FlexxAgent (this option will not be available if the feature is already enabled in Product).
- **Disable uninstallation protection.** Allows users to uninstall FlexxAgent (this option will not be available if the feature is already disabled in Product).
- **Reset uninstallation protection.** Applies the <u>configuration that the Product has</u> to which the report group belongs, whether enabled or disabled.

🕂 Create 🥜 Edit auto-update 🗸	Edit uninstall protectEnable uninstall pro		Analyzer execution $ \smallsetminus $
Search by term	imes Disable uninstall pro	otection	
	🐯 Reset uninstall prote	ection	
Tenant ↑↓	Name ↑↓	Environment ↑↓	Product ↑↓
	PER Strangers	Laboration Constant of	FlexxClient
	the designment		FlexxClient
AND DECIDENT OF A DECIDENT	100		FlexxClient

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

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

Ways to uninstall FlexxAgent with protection enabled

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

1. Move the device to a reporting group that does not have protection enabled.

2. Via a token:

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

FlexAgent uninstallation	
Flexi	
Please enter the uninstall token for this device to pro uninstall process	ceed with the
	ceed with the
	ceed with the Show

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)

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:

C:\intune>FlexxAgent-Installer.exe
2025-01-30 09:43:02 - FlexxAgent version: installer
2025-01-30 09:43:02
ERROR: Clase no válida "Win32_BootConfiguration"
ERROR: No se puede llamar a un método en una expresión con valor NULL.
ERROR: No se puede llamar a un método en una expresión con valor NULL.
ERROR: No se puede llamar a un método en una expresión con valor NULL.
ERROR: No se puede llamar a un método en una expresión con valor NULL.
ERROR: No se puede llamar a un método en una expresión con valor NULL.
ERROR: No se puede llamar a un método en una expresión con valor NULL.
ERROR: No se puede llamar a un método en una expresión con valor NULL.
ERROR: No se puede llamar a un método en una expresión con valor NULL.
ERROR: No se puede llamar a un método en una expresión con valor NULL.
ERROR: No se puede llamar a un método en una expresión con valor NULL.
2025-01-30 09:43:03 - Path of current execution: .
2025-01-30 09:43:03 - Configuration file path: .\FlexxAgent-Configuration.conf
2025-01-30 09:43:03\FlexxAgent-Installer.exe
2025-01-30 09:43:03 - Preparing temp folder
2025-01-30 09:43:03 - Getting OS data
ERROR: Clase no válida "Win32_OperatingSystem"
ERROR: Clase no válida "Win32_ComputerSystem"
2025-01-30 09:43:03 - Windows version:
2025-01-30 09:43:03 - Windows OS:
2025-01-30 09:43:03 - OS Architecture:
2025-01-30 09:43:03 - OS language:
2025-01-30 09:43:03 - Portable OS system:
2025-01-30 09:43:03 - Total memory:
2025-01-30 09:43:03 - Total logical processors:
2025-01-30 09:43:03 - Temporary folder: C:\Windows\Temp\FlexxibleIT
2025-01-30 09:43:03 - Checking .Net Framework version
2025-01-30 09:43:03 - Checking OS architecture

Solution

Run the following commands:

Stop-Service winmgmt -Force

winmgmt /resetrepository

Start-Service winmgmt

Issue 2 - PowerShell process restriction

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

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

Solution

Exclude the following files from the device:

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

C:\Windows\Temp\UpdateFlexxAgent.ps1

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	Туре	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.

Parameter	Туре	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

() 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\Communica

Registry keys related to the proxy configuration:

- <u>Key Proxy_URL</u>
- <u>Key Proxy_User</u>
- <u>Key Proxy_Pwd</u>

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 '<u>http://192.168.1.1:3128</u>' or '<u>https://192.168.1.1:3128</u>'

Key Proxy_User

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

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

Key Proxy_Pwd

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

Manual Update

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

Workspaces

Custom oper	rations 🔹	My Filters	• Filte	er by tag	Fi	lter by wor	kspace group	!	Q ©
		□ ¢	S	6 🗊				?	<i>G</i>
Platforms	Machine ↑	Power state	Last user	Sessions	CPU	% RAM	Uptime	Status	Connection
No data to display									
Count=0									
									l

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
- <u>FlexxAgent service logs</u>

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

Installation and update logs

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.

Flex	WORKSPACES						• Q	Log O
Level 1 V	Workspace \					o 🛛 -	Operations +	>
Workspaces	General						Power and connection actions	
Sessions	Name	Summary status On	Power state On	FlexxAgent version 24.5.3.4	FlexxAgent status	FlexxAgent last repor 13/09/2024 12:41:1	Edit Maintenance (Drain mode) Refresh Workspace info	
ormection Lago	Connection	Subnet 192.168.1.0/24	MAC address 98-FC-84-E5-92-F4	Network changed			Force check compliance Force update custom fields Remote administration	
	Sessions 1	Last user	Connected from	Connection time 13/09/2024 1:16	Domain		Remote assistance Machine type	
A. Toffie Storage	Wireless network	Network signal 95 %	Code				Notifications Session Analyzer trace logging	
evel 2 🔸	Description ①					None	Changer properties of the changer of	> >
Level 3 >	Tags					Warning Error Critical	OS Patching	·
	Extended					Trace Debug		

FlexxAgent service logs

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

🛃 Visor de eventos						_		×
Archivo Acción Ver Ayuda								
🗢 🔿 🙍 🖬 🛛 🖬								
Visor de eventos (local)	Aplicación Número de	eventos: 28.145			A	cciones		
> 📑 Vistas personalizadas 🗸 👔 Registros de Windows	Nivel	Fecha y hora	Origen	ld. d	el evi ,	Aplicación		· .
Aplicación	Información	29/08/2024 13:37:32	FlexxAgent service	te		j Abrir registr	o guardad	J
Seguridad	(i) Información	29/08/2024 13:37:29	FlexxAgent service			Crear vista p	ersonaliz.	
Instalación	Información	29/08/2024 13:21:23	Outlook			Importar vis		
😭 Sistema	 Información 	29/08/2024 13:09:07	Security-SPP		11 -			·
Eventos reenviados	<u> </u>					Vaciar regist		
Registros de aplicaciones y s Suscripciones	Evento 1001, FlexxAgent	service			×	Filtrar regist	ro actual	·
uga Suscripciones						Propiedade	5	
	General Detalles					Buscar		
	International and the	and the March Street			— L	Guardar too	los los eve	
	FlexxAgent service 1	s up and running. No action re	iquired.			Adjuntar ta	an a este i	
							ea a este i	
	l .					Ver		-
	Nombre de registro:	Aplicación				Actualizar		
	Origen:	FlexxAgent service	Registrado:	29/08/2024 13:37:32		? Ayuda		•
	ld. del	1001	Categoría de tarea:	Ninguno	E	vento 1001, Fle	xAgent s	
	Nivel:	Información	Palabras clave:	Clásico		Propiedade	de event	0
	Usuario:	No disponible	Equipo:	FedericoZ	1	Adjuntar tai	ea a este .	.
	Código de operación:	Información			8	Copiar		•
	Más información:	Ayuda Registro de eventos			6	Guardar eve	ntos selec	
						Actualizar		
					· 1	Ayuda		• '
	-							

Information obtained from the device

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

General information

- Name. Device Name.
- Device Status. Device power state. It can be On, Off, or Not reporting.
- Summary status. If the device status is *Off*, it can indicate if it is *Under maintenance* or just *Off*. If the device status is *Unreported*, it can indicate if the reason is *Unknown*.
- FlexxAgent Version. Version number of FlexxAgent installed on the device.
- FlexxAgent Status. Running or Stopped.
- Last FlexxAgent report. Date and time of the last FlexxAgent report on the device. This date might not be recent if the FlexxAgent service is stopped or the device is off.
- Connection Type. Indicates if the device is connected via *Wireless LAN*, *Mobile Network*, *Ethernet*, or *Unknown*.

() INFO

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

Connection

Signal 0% - Wireless LAN

- **Network.** Network addressing of the device and public IP for internet access. These networks are created automatically when more than four devices are connected to the same network.
- Subnet. Device's network addressing.
- MAC Address. Unique identifier of the device's network card.
- Network Changed. Date and time of the last network change.
- Sessions. Number of user sessions established on the device.
- Last User. Last user logged into the device in domain\account format.
- **Connected From.** When the selected device is a VDI or similar, shows the device name from which the virtual device is accessed.
- Connection Time. Date and time when the session started.
- Domain. Domain to which the device belongs.
- **Code.** Lets identify the device with a personal code. This code must be manually filled in individually using the Edit option in the Operations menu of the workspace details.
- OU. Organizational unit of the domain where the device account resides.
- **Description.** Allows the user to identify the device with a personal description. This field must be assigned manually and individually using the Edit option in the Operations menu of the device details.

Extended Info

- **RAM.** Total amount of available RAM.
- Cores. Number of processor cores.
- IP Address. Device's IP address on the local network.
- OS. Type of operating system.
- Operating System. OS version.
- OS Build. Operating system build number.
- Uptime. Time the device has been running since the last boot or reboot. If fastboot is enabled, the device is only off when it is restarted.
- Idle time. Indicates the time elapsed since the last input event was received in the FlexxAgent user session. Shows 0 if the user is effectively using any input device connected to the device.
- Last Windows update. Date of the last updates applied on the device.
- Last boot duration. Duration of the boot of the last start.
- Pending reboot. Shows whether the device requires a reboot for updates.
- Type of Windows. Type of Windows operating system: *Client* or *Server*.
- System disk. Amount of free disk space relative to the total capacity.
- **ISP Public IP.** The ISP is obtained using the public IP. It might not be accurate if connected to a corporate network or using a VPN.
- **Region.** Obtained using the public IP. It might not be accurate if connected to a corporate network or using a VPN.
- Broker type. If detected, shows the session broker used.
- Hypervisor. If virtualization is detected, shows the hypervisor used.
- Delivery group. For VDIs, shows the delivery group to which the device belongs.
- Subscription / Broker. Microsoft Azure or Citrix service that manages user connections to the device.
- Registration status. Indicates the status of the virtual device registration.
- Maintenance mode. Indicates if the maintenance mode of the virtual device is *On* or *Off.*
- Virtual machine type. Indicates the type of virtual device.
- Session Analyzer. Indicates whether or not it's configured to launch session Analyzer in all user sessions.
- Session Analyzer Version. Version number of Session Analyzer.

- Report Group. Reporting group to which the device belongs.
- BIOS manufacturer. Name of the device's firmware manufacturer.
- BIOS version. Version of the device's firmware.
- SMBIOS version. Version of the System Management BIOS of the device.
- **BIOS serial number.** Unique number assigned to the device by its manufacturer. Available only if the manufacturer decided the device needed one.
- Google Chrome version. Build number of Google Chrome, if installed.
- Microsoft Edge version. Build number of Microsoft Edge, if installed.

Information in tabs

FlexxAgent groups information about the following aspects of the device:

Sessions

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

Performance

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



• CPU. Percentage of processor usage

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

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

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.

essions Performance Jobs	Alerts Event log Conne	ction logs Windows services Disk	s Boot history Notifications	Security Compliance	Group Policy (GPO) PnP Devices Syste
Info	Status	Creation date \downarrow	Start time 👃	End time	Owner
Reinan - Tablicant	Completed	25/09/2024 18:29:56	25/09/2024 18:29:56	25/09/2024 18:30:05	
antenan antenan antenan Antenan Antenan Antenan An	Completed	19/07/2024 10:38:47	19/07/2024 10:38:47	19/07/2024 10:38:57	
	Completed	19/07/2024 9:30:45	19/07/2024 9:30:45	19/07/2024 9:31:02	
Count=3					
< 1 >					Page size 20 *

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.

	Ø • Operations • • •
Active alerts: - [Critical] Low storage free space % for Workspace: Drive: C: Free space: 2 GB, Used Percentage: 98%	
General	

Event Logs

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

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

Connection Log

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

Connections	Performance	Logon info	Notifications	Group Policy (GPO)			
						Today	•
Start	Ļ			End	Endpoint		Reconnection
10/10/	/2024 14:07:10			11/10/2024 0:07:10			×
Count	-1						

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.

Session	ns Performance J	obs Alert	s Event log	Connection logs	Windows services	Disks	Boot history	Notifications	EDR	Compliance	Group Policy (GPO)	PnP <
								<u>ا</u>	Export to		Service operation	*
	Display name †		Status		Startup type		Loį	g on as		Ao	Start Service Stop Service	
	Actualizador de zona automática	horaria	Stopped		Disabled		NT	AUTHORITY\Loo	alServio	e	Restart service	
	Administración de ap	licaciones	Stopped		Manual		Lo	calSystem			No	

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.

>

Sessions	Performance	Jobs /	lerts	Event log	Connection logs	Windows services	Disks	Boot history	Notifications	Security	Compliance	Group Policy (GPO)	PnP Devices	Syste)
												(•	
De	evice ID †	Nam	ie †		Volume label	Total size	Used siz	te % Used	OS	Location	F	Partition	Physical disk siz	e	
						250 MB	0 MB	0 %		Integrated : Device 14 : : Adapter 0 Target 0 : L	Function 0 : Port 3 :	Disco #0, partición #0	MB		
						1.333 MB	0 MB	0 %		Integrated : Device 14 : : Adapter 0 Target 0 : L	Function 0 : Port 3 :	Disco #0, partición #2	MB		
						1.438 MB	0 MB	0 %		Integrated Device 14 : : Adapter 0 Target 0 : L	Function 0 : Port 3 :	Disco #0, partición #3	МВ		

Boot history

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

Alerts Event log	Connection logs	Windows services	Disks	Boot history	Notifications	Security	Compliance	Group Policy (GPO)	PnP Devices	System Summary
De et durat	ian ()									
Boot durat	ion -						_			
02-Oct-24 06:20 01-Oct-24 07:04 30-Sep-24 07:06 29-Sep-24 07:06										
28-Sep-24 07:03 27-Sep-24 07:03 26-Sep-24 07:02 25-Sep-24 07:02								-		
25-Sep-24-07:03 24-Sep-24-07:03 0 s	-	55	10 s		15 5	20	5	25 s	30 s	

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

DR ① rowdStrike	CrowdStrike version 6.46.16010.0	CrowdStrike status Installed and working	Antivirus Windows Defender	Antivirus version 4.18.1807.18075	Antivirus status Installed and working
CPU [©]			Memory [®]		
100 %			300 MB		
80 % 60 %			200 MB		
40 % 20 %			100 MB		
0% 8)81818	\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$	3 3 5 5 5 8 3 5 5 5 5 5 5 5 5 5 5 5 5 5	омв สาสาสาสาสาร์	8 8 8 8 8 8 5 5 5 5 6 5 5 5 8 5 5 5 5	1. 2. 2. 2. 2. 2. 2. 2. 2. 2. 2. 2. 2. 2.

() 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.

Sessions	Performan	ce Jobs	Alerts	Event log	Connection logs	Windows services	Disks	Boot history	Notifications	Security	Compliance	Group Policy (GPO)	PnP Devices
Device m	anager entri	es with erro	or state										
	last PNP device 24 15:03:44	s update											
												Cope	erations -
□ N	ame \downarrow					Deter	tion date	2				Class	Device ID
G	sco AnyConne	ect Virtual Mi	iniport A	dapter for	Windows x64	27/11	/2023 13	:51:47				Net	ROOT/NET/0000
c	ount=1												
< <u>1</u>	>												Page size 20 *
PnP even	ts												
Ac	tion	Date ↓				User		Caption			(Device ID	
D PI	ugged in	17/07/2024	16:01:3	37				Generic PnP M	onitor		t	DISPLAY\CTX0466\2&1	23C1CA0&0&UID1
	nplugged	17/07/2024	4 14:40:2	22				Generic PnP M	onitor		(DISPLAY\CTX0466\2&1	23C1CA0&0&UID1

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

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

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

Reporting groups history

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

FlexxAgent / Supported Systems / Linux

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

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

Proceso Nombre del proceso	Recenters				Q	=	х	III Process				mas de archivos	Q	= ×	
·		% CPU	ID	is de archives Memoria	Lectura tot	al (Esci	ritura I		Recurses	% CPU	ID		Lectura total (Escritura to	
📀 dm bufio cache	root	0,00	103	N/D	N	VD		dconf-service	cdo-test-fedor	0.00	3696	655,4 kB	32.8 kB	409.6 k	
edac-poller	root	0,00	58	N/D		VD	- 1	dleyna-renderer-service	cdo-test-fedor	0,00	5218	1,7 MB	N/D	N	000
ext4-rsv-conver	root	0,00	657	N/D	N	VD.	- 1	evolution-addressbook-factory	cdo-test-fedor	0,00	2214	3,9 MB	1,7 MB	86,0 k	
firewalld	root	0,00	866	25,0 MB	12,7 N	1B	- 1	evolution-alarm-notify	cdo-test-fedor	0,00	2295	13,9 MB	20,5 kB	N	
flatpak-system-helper	root	0,00	3557	95,7 MB	2,3 N	1B	66,3	evolution-calendar-factory	cdo-test-fedor	0,00	2180	3,9 MB	3,0 MB	N	
<ir><!-- record gent</td--><td>root</td><td>0,08</td><td>904</td><td>44,8 MB</td><td>273,1 N</td><td>1B</td><td>237,6</td><td>evolution-source-registry</td><td>cdo-test-fedor</td><td>0,00</td><td>2137</td><td>8,9 MB</td><td>40,0 MB</td><td>N</td><td></td></ir>	root	0,08	904	44,8 MB	273,1 N	1B	237,6	evolution-source-registry	cdo-test-fedor	0,00	2137	8,9 MB	40,0 MB	N	
fusermount3	root	0,00	2608	N/D	N	/D		C flexxagent-session	cdo-test-fedor	0,42	2530	68,4 MB	7,4 MB	8,2 k	
fusermount3	root	0,00	4415	N/D	N	/D	- 1	🔷 gdm-wayland-session	cdo-test-fedor	0,00	1826	393,2 kB	N/D	N	
💎 fwupd	root	0,00	2665	83,7 MB	6,7 N	1B	11,1	🔷 gjs	cdo-test-fedor	0,00	2397	5,1 MB	N/D	N/	
📀 gdm	root	0,00	1116	786,4 kB	1,1 N	1B	16,4	🔷 gjs	cdo-test-fedor	0,00	2232	4,9 MB	N/D	N	
📀 gdm-session-wor	root	0,00	1677	2,0 MB	999,4	kВ	4,:	gnome-boxes-search-provider	cdo-test-fedor	0,00	4964	1,2 MB	36,9 kB	N	
💎 gnome-keyring-daemon	root	0,00	4468	917,5 kB	4,1	kВ	16,4		cdo-test-fedor	0,17	4965	5,1 MB	876,5 kB	N	
gnome-system-monitor	root	0,84	4379	14,5 MB	118,8		36,9	gnome-calendar	cdo-test-fedor	0,00	4966	14,0 MB	23,8 MB	N	
💎 gpg-agent	root	0,00	3684	266,2 kB		/D	- 1	gnome-characters	cdo-test-fedor	2,34	4968	82,3 MB	4,7 MB	Ny	
gssproxy	root	0,00	914	782,3 kB	340,0		- 1	gnome-clocks	cdo-test-fedor	4,43	4975	10,6 MB	258,0 kB	N	
📀 gvfsd	root	0,00	4437	655,4 kB		νD		gnome-contacts-search-provid		0,00	4970	4,6 MB	921,6 kB	N	
📀 gvfsd-fuse	root	0,00	4442	655,4 kB		VD	- 1	or gnome-control-center-search-		0,08	4974	7,7 MB	24,6 kB	N	
hwrng	root	0,00	83	N/D		/D		= gnome-disks	cdo-test-fedor	0,00	5056	6,8 MB	274,4 kB	N	
<pre>oidle_inject/0</pre>	root	0,00	19	N/D		VD		ognome-keyring-daemon	cdo-test-fedor	0,00	1772	1,1 MB	36,9 kB	20,5 k	
<pre>oidle_inject/1</pre>	root	0,00	22	N/D		VD	- 1		cdo-test-fedor	0,00	1938	3,0 MB	200,7 kB	53,2 k	
<pre> dle_inject/2 </pre>	root	0,00	28	N/D		/D	- 1	gnome-session-binary gnome-session-ctl	cdo-test-fedor	0,00	1848	2,1 MB	102,4 kB 8,2 kB	N	
<pre> dle_inject/3 </pre>	root	0,00	34	N/D	N	/D		• gnome-session-cti	cdo-test-fedor	0,00	1933	393,2 kB	8,2 KB	N	
Finalizar proceso							Q	Finalizar proceso						Q	1.00
and the second se			<u> </u>		_	-					-	-	1		

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.

Activities	🖾 System Monitor							ago 7 09	:25					
6	E Processes	(T) Resources	© File System		Q =	_ 0	×	⊨ Processes (¹)	Resources	@ File	Systems	Q	= = (• ×
	Process Name	 User 	% CPU	D	Memory D	lsk read toti	Disk v	6	,					
165	devfreq_wq	root	0,00	82	N/A	N/A			4					
	ecryptfs-kthread	root	0,00	88	N/A	N/A		Process Name 🗸 🗸	User	% CPU	ID	Memory	Disk read tota	Disk write
	edac-poller	root	0,00	81	N/A	N/A		evolution-addressbook-factor	cdo-test	0,00	1619	3,7 MB	3,5 MB	36,9
	ext4-rsv-conver	root	0,00	226	N/A	N/A		evolution-alarm-notify	cdo-test	0,00	1705	15,3 MB	1,6 MB	
	Flexxagent				94,9 MB		5	evolution-calendar-factory	cdo-test	0,00	1576	4,3 MB	5,1 MB	
_	Infusermount3	root	0,00	1361	N/A	N/A		evolution-source-registry	cdo-test	0,00	1562	3,8 MB	3,8 MB	
0	🖻 gdm3	root	0,00	717	786,4 kB	2,5 MB		👏 firefox	cdo-test	0,05	11865	182,3 MB	202,9 MB	55,5
	gdm-session-wor	root	0,00	1308	1,7 MB	1,3 MB		🖸 flexxagent-session	cdo-test		2898	89,4 MB	766,0 kB	
	gnome-system-monitor	root	0,08	26532	16,2 MB	8,0 MB		gdm-wayland-session	cdo-test	0,00	1424	393,2 kB	N/A	
	hwrng	root	0,00	98	N/A	N/A		🖻 gjs	cdo-test	0,05	26338	16,7 MB	N/A	
	idle_inject/0	root	0,00	18	N/A	N/A		🛛 🗐 gjs	cdo-test	0,00	1645	5,0 MB	N/A	
~	idle_inject/1	root	0,00	21	N/A	N/A		🖸 gjs	cdo-test	0,00	1873	5,4 MB	N/A	
A	idle_inject/2	root	0,00	27	N/A	N/A		gnome-calculator-search-provi	cdo-test	0,00	27493	7,1 MB	N/A	
	idle_inject/3	root	0,00	33	N/A	N/A		🔤 gnome-calendar	cdo-test	0,00	26838	14,9 MB	1,5 MB	
_	idle inject/4	root	0,00	39	N/A	N/A		* gnome-control-center	cdo-test	0,00	2590	34,9 MB	16,3 MB	
2	idle_inject/5	root	0,00	45	N/A	N/A		gnome-control-center-search-p	cdo-test	0,00	27489	6,9 MB	N/A	
•	idle_inject/6	root	0,00	51	N/A	N/A		gnome-keyring-daemon	cdo-test	0,00	1341	946,2 kB	430,1 kB	4
	idle_inject/7	root	0,00	57	N/A	N/A		gnome-session-binary	cdo-test	0,00	1484	2,8 MB	6,6 MB	4
>_	Sinet_frag_wq	root	0,00	63	N/A	N/A		gnome-session-binary	cdo-test	0,00	1427	1,8 MB	2,3 MB	
	Dipv6_addrconf	root	0,00	101	N/A	N/A		gnome-session-ctl	cdo-test	0,00	1464	393,2 kB	20,5 kB	
	P													
	End Process						0	End Process						0
											~			

Supported versions

FlexxAgent supports the following distributions and versions:

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

More distributions are regularly validated.

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

Requirements

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

Package dependencies for Fedora and Debian:

- dmidecode
- imvirt
- systemd

Limitations

Certain functionalities are 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
```

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

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

Installation steps

- 1. Download the installer from the URL.
- 2. Grant permissions to the script.

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

3. Run the script.

sudo ./flexxagent-install.sh -c [configuration file]

4. Clean the files used.

Installation script parameters

Parameter	Caption
-v,version <version></version>	Use a specific version, by default latest.
-d,distro <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></conffile>	Applies the configuration from a configuration file by default, settings.conf.

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

Examples

Install FlexxAgent with the configuration file:

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

Install a specific version of FlexxAgent:

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

Force the FlexxAgent installation for a specific distribution:

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

Access the help:

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

Offline installation

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

Installation packages provided according to the distribution

```
Debian: flexxagent.deb
```

Fedora: flexxagent.rpm

Offline installation steps

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

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

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

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

4. Clean the files used.

Uninstall

The uninstallation script can be downloaded from

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

Steps for uninstallation:

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

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

3. Run the script.

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

4. Clean the files used.

Uninstallation script parameters

Parameter	Caption
-d,distro <distro></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></version>	Cleans configurations and logs; default is false.
-?,?,-h, help,-Help	Shows help.

Examples

Uninstall and clean up configurations and logs:

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

Force the uninstallation for a DISTRO:

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

Access the help:

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

Update

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

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

Logs

FlexxAgent can generate two types of logs:

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

Information obtained from the device

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

orkspace V					B + Opening +
veral					
	Kannary minis Qri	Power mete Om	Passalgare survive 24.7.2.160	Wanting	Recoluper fail report () 8/8/2004 1-28/10/PM
-	Manual () 192148100493178147.4 (8	Notices 102148310724	MAX ADDIVID AD DERIT DE DA AB	Network Anager Self-2004 12:42:10 PM	
-	Last volat	Connected from	Connector time MIN2024 12:30 PM	(terran	
day severi	Remark signal 100 lb	Com ()			
and and					
8	Com: A	P alleres 192 108 1142	the loss	Operating system. Realized Group 37 (Allociestation Edition)	DI Bulit number
n 0	Parallel salare No				
enda 1560 herur beitolik peruna)	No. PEP.	Nagan () Terranar () ()			
No trover detected	Rypervisor ()	Defense group 2	Subscription/Boston 🖓		
int and the () Against	Section and one variable 24.7.2.100	Rearing price Physical Devices			
sion Performance John Alert	n Convertionings Disks Bost histor	y Notifications ProPOnvices			
CPU ®			Memor	y.°	
			100		
107.6 47.6 47.6			148	1	
10% 4% 4% 2% 2%				F	
1076 476 476 476 476					
076 476 476 476 476				cton signal [©]	
Bandwidth usage [®]	n		1111 Conne		
Bandwidth usage ⁰			Conne		,,,,,,,,,,,,,,,,,
Bandwidth usage [®]	,			ction signal ®	

General information

- Name. Device Name.
- Device Status. Power status of the device, can be On, Off, or Not reporting.
- FlexxAgent Version. Version number of FlexxAgent installed on the device.
- FlexxAgent Status. Running or Stopped.
- Last FlexxAgent report. Date and time of the last FlexxAgent report on the device. This date might not be recent if the FlexxAgent service is stopped or the device is off.
- Connection Type. Indicates if the device is connected via *Wireless LAN*, *Mobile Network*, *Ethernet*, or *Unknown*.
- **Network.** Network addressing of the device and public IP for internet access. These networks are created automatically when more than four devices are connected to the same network.
- Network Signal. Network reception percentage.

- Subnet. Device's network addressing.
- MAC Address. Unique identifier of the device's network card.
- Wireless Network. Name of the network.
- **Connection signal.** Percentage of signal reception when the device connects using a wireless method.
- Network Changed. Date and time of the last network change.
- Sessions. Number of user sessions on the device.
- Last User. Last user logged into the device in domain\account format.
- **Connected From.** When the selected device is a VDI or similar, shows the device name from which the virtual device is accessed.
- Connection Time. Date and time when the session started.
- **Code.** Lets identify the device with a personal code. This code must be manually filled in individually using the Edit option in the Operations menu of the workspace details.
- **Description.** Allows the user to identify the device with a personal description. This field must be assigned manually and individually using the Edit option in the Operations menu of the device details.

Extended Info

- RAM. Total capacity of available RAM.
- Cores. Number of processor cores.
- IP Address. Device's IP address on the local network.
- OS. Type of operating system.
- Operating System. OS version.
- **Region.** Obtained using the public IP. It might not be accurate if connected to a corporate network or using a VPN.
- Broker type. If detected, shows the session broker used.
- Delivery group. For VDIs, shows the delivery group to which the device belongs.
- Subscription. If detected, subscription in use for Citrix Cloud, Azure services, etc.
- Hypervisor. If virtualization is detected, shows the hypervisor used.
- Session Analyzer. Indicates whether or not it's configured to launch session Analyzer in all user sessions.

- Session Analyzer Version. Version number of Session Analyzer.
- **Report Group.** Reporting group to which the device belongs.

Information in tabs

FlexxAgent groups information about the following aspects of the device:

Sessions

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

Performance

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

- CPU. Processor usage percentage.
- Memory. Amount of memory used and available.
- Bandwidth Usage. Amount of incoming and outgoing traffic.

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

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

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

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

Activity Monito All Processes, Hier		θ× c	PU Memory E	nergy Disk Netwo	rk Q :	Search					
Process Name	~ % CPU	CPU Time	Threads k	die Wake-Ups %	GPU	GPU Time	PID	User			
familycircled	0,0	0,12	2	0	0,0	0,00	488	cdo-test			
filecoordinationd	0,0	0,04	2	0	0,0	0,00	515	root			
fileproviderd	0,0	0,45	2	0	0,0	0,00	497	odo-test			
financed	0,0	0,31	2	0	0,0	0,00	572	cdo-test			
V 🍆 Finder	0,0	2,56	3	0	0,0	0,00	605	cdo-test			
QuickLookUlService (PID 0,0	0,08	3	0	0,0	0,00	609	cdo-test			
findmydeviced	0,0	0,08	2	0	0,0	0,00	229	root			
FindMyMacd	0,0	0,01	2	0	0,0	0,00	307	root.			
FlexxAgent.Service	0,3	12,19	25	6	0,0	0,00	308	root			
fmfd	0,0	0,15	2	0	0,0	0,00	508	cdo-test			
followupd	0,0	0,03	2	0	0,0	0,00	676	cdo-test			
fontd	0,0	0,22	3	0	0,0	0,00	464	odo-test			
fontworker	0,0	1,09	2	0	0,0	0,00	466	cdo-test			
fseventsd	0,0	0,72	8	1	0,0	0,00	91	root.			
gamecontrolleragentd	0,0	0,07	3	0	0,0	0,00	581	cdo-test			
gamecontrollerd	0,0	0,10	3	1	0,0	0,00	433	_gamecontrolk			
GSSCred	0,0	0,04	3	0	0,0	0,00	424	root			
heard	0,0	0,29	3	1	0,0	0,00	584	cdo-test			
blad	^^	0.04		^		0.00	994	alast.			
	System:	6,79%	CPULOAD	Threads:		1.198					
	Useri	5,54%		Processes	E.	359					
	ide:	87,67%									
		2	- Achila	Audio							
	A second				_				1		

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.

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/x
64/flexxagent-install.sh
```

Path to download the installation script for ARM architecture:

```
https://update.workspaces.flexxible.com/agents/FlexxAgent/latest/macos/a
rm64/flexxagent-install.sh
```

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

Installation steps

- 1. Download the installer from the URL.
- 2. Grant permissions to the script, open the terminal, and execute:

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

3. Run the script.

sudo ./flexxagent-install.sh -c [configuration file]

4. Clean files.

Installation script parameters

Parameter	Caption
-v,version	Use a specific version, by default, latest.
verbose,- Verbose	Displays diagnostic information.
-c,config <conffile></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 <u>Offline installation</u> section for more details.
-?,?,-h, help,-Help	Shows help.

Examples

Install FlexxAgent with the configuration file:

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

Install a specific version of FlexxAgent:

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

Access the help:

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

Offline installation

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

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

Offline installation steps

- 1. Place the FlexxAgent package file, the configuration file, and the installation script in the same folder.
- 2. Allow the Terminal application to access the disk where the files are located:
- Go to System preferences -> Security and Privacy -> Privacy.
- Select Full disk access.
- Add the Terminal application to the list.
- Close the Terminal application i it was running and open a new one.
- 3. Go to the folder where the FlexxAgent files are located, and grant permissions to the script:

sudo chmod +x ./flexxagent-install.sh

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

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

5. Clean the files used.

Uninstall

The uninstallation script can be downloaded from

```
https://update.workspaces.flexxible.com/agents/MacOS/FlexxAgent/latest/f
lexxagent-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></version>	Cleans configurations and logs; default is false.
-?,?,-h,help,-Help	Shows help.

Examples

Uninstall and clean up configurations and logs:

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

Access the help:

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

Update

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

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

Information obtained from the device

Fle)	WORKSPACES						Al tenants	• 🖓	Lug Of
Lead 1	Warkspace \						3	🛙 • Operation	
<mark></mark>	Central Kana	Sennery mess On	Protect marke On	Readigent version 24.0.1.104		Presidgent status	Sandger for room () 59/2014755:03 AM		
	Conversion V	Retrach () 192.1021.004(82.175.147.4)	Talant 192.168.1.0/24	INC address DC:49:04:02:00	3	Network shanged 5/9/2024 4:02107 PM			
9	Semiore 1	Let me	Connected from	Connection time 8/5/2824 7:44 A	м	Bonain			
	Piteles; estent	Retroch stand 100 %	Code (2)						
une: *	Econded								
(anai1) ⊛)	IL CE	60mi 4	# address 1921/68.1.125	05 💼 HMC		Operating system mecDS 13.6.8	05 Build sumber		
Č	ipina () -42%	handing railoon No							
	Nysteen alsis 100.2:08 Hear of 118.2 GB (15%) useds	Nation P & ICP ()	Region () Terresse (25)						
	Rolertope 2 No braker detected	Nyamian D Physical	Delivery group (1)	Subscription Text	w 3				
	Teniosaniper () Configured	Invalue analyses unvolue 20.8.1.100	Reporting group Physical devices						
	Sessions <u>Portomanos</u> Jobs Alerts	Connection logs Dialo Boet Natory	Notifications PriP Devices						
	For more detailed information slick into	gar shili tha service analyses partal.							
	CPU ®				Memory [®]				
	E %				818	A ===			
	10% 10%				428				
	111111			11.1	111	111111111		111111	11
	Bandwidth usage @				Connection	signal ^a			
	1000 404				10°5 10°5				
	1000 KBA 3000 KBA				0.5				
			111111111	111	-111				11

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

General information

- Name. Device Name.
- Device Status. Power status of the device, can be On, Off, or Not reporting.
- FlexxAgent Version. Version number of FlexxAgent installed on the device.
- FlexxAgent Status. Running or Stopped.
- Last FlexxAgent report. Date and time of the last FlexxAgent report on the device. This date might not be recent if the FlexxAgent service is stopped or the device is off.
- Connection Type. Indicates if the device is connected via *Wireless LAN*, *Mobile Network*, *Ethernet*, or *Unknown*.
- **Network.** Network addressing of the device and public IP for internet access. These networks are created automatically when more than four workspaces are connected to the same network.
- Network Signal. Network reception percentage.
- Subnet. Device's network addressing.
- MAC Address. Unique identifier of the device's network card.
- Wireless Network. Name of the network.
- **Connection signal.** Percentage of signal reception when the device connects using a wireless method.
- Network Changed. Date and time of the last network change.
- Sessions. Number of user sessions on the device.
- Last User. Last user logged into the device in domain\account format.
- **Connected From.** When the selected device is a VDI or similar, shows the device name from which the virtual device is accessed.
- Connection Time. Date and time when the session started.
- **Code.** Lets identify the device with a personal code. This code must be manually filled in individually using the Edit option in the Operations menu of the workspace details.
- **Description.** Allows the user to identify the device with a personal description. This field must be assigned manually and individually using the Edit option in the Operations menu of the device details.

Extended Info

- **RAM.** Total capacity of available RAM.
- Cores. Number of processor cores.
- IP Address. Device's IP address on the local network.
- OS. Type of operating system.
- Operating System. OS version.
- **Region.** Obtained using the public IP. It might not be accurate if connected to a corporate network or using a VPN.
- Session Analyzer. Indicates whether or not it's configured to launch session Analyzer in all user sessions.
- Session Analyzer Version. Version number of Session Analyzer.
- **Report Group.** Reporting group to which the device belongs.

Information in tabs

FlexxAgent groups information about the following aspects of the device:

Sessions

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

Performance

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

- CPU. Processor usage percentage.
- Memory. Amount of memory used and available.
- Bandwidth Usage. Amount of incoming and outgoing traffic.

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

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.

	Operations
Active alerts: - [Critical] Low storage free space % for Workspace: Drive: C: Free space: 2 GB, Used Percentage: 98%	
General	

Connection Log

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

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

Disks

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

Notifications

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

Reporting groups history

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

FlexxAgent / Supported Systems / ChromeOS

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

Requirements

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

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

Supported versions

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

Limitations

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

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

Download and installation

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

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

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

Installation

In broad strokes, the procedure is as follows:

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

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

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

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



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

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

✓ Instaladas ▼	Actualizaciones disponibles Juegos Archivadas		
	Aplicaciones (2)	Actualizadas recientemente 📻	
	Speech Recognition & Synthesis 172 MB • Actualizado hace 1 día	× 🗆	
	65 MB • Actualizado el 18 jul.	~ 🗆	

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



4. Close the window.

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



Update

FlexxAgent updates automatically from Google Play.

Information obtained from the device

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

ORKSPACES								All cenance	• • •	
rispace \										
								0	Denators -	<
er ál.										
	Summery status On	Power state On		xAgent version 37.02.097		Reckgent state		RexxAgent last report () 5/5/2004 1 40:09 PM		
ection	Network () 192 163 10/24 (93 176 147 4) 😢	Subret 1921681.5/24	MAG	Laddress.		Network change 8/5/2024 11:4	HE 7:08 AM			
	Lastwar	Connected Norm		rection time (2024 1:39 PM						
es much	Network signal. 99.%	Code 🖯								
nded										
0	Cares 2	IP address 182.168.1.135	os 😨	Chrome05		Operating syste ChromeOS 12		OS Build number		
n D	Panding ration ND									
m dak nown	Public IP & dF () 93.176.147.4 (Ibra Telecom S.A.)	Region (3) Terratte (85)								
ery group ①										
on analyzer () Igured	Session analyzer version 24/07/02/097	Reporting prova Physical devices								
ions Performance jobs	Alerts Connection logs Dealer	Boot history Notifications	PnP Devices							
									8	81
Device1D 1	Name 1	Volume label	Totalsize	Used size	NUsed	OS Loo	ation	Partition	Physical disk size	
0	/storage/emulated/0	Aimacenamiento interno compartido	32,000 MB	0.145	0%			Almacenamiento intr compartido	arro 32,000 MB	
Courter1										
L >									Page size 2	29

General information

- Name. Device Name.
- Device Status. Power status of the device can be On, Off, or Not reporting.
- FlexxAgent Version. Version number of FlexxAgent installed on the device.
- FlexxAgent Status. Running or Stopped.
- Last FlexxAgent report. Date and time of the last FlexxAgent report on the device. This date might not be recent if the FlexxAgent service is stopped or the device is off.
- Connection Type. Indicates if the device is connected via *Wireless LAN*, *Mobile Network*, *Ethernet*, or *Unknown*.
- Network. Network addressing of the device and public IP for internet access. These networks are created automatically when more than four devices are connected to the same network.
- Network Signal. Network reception percentage.
- Subnet. Device's network addressing.

- Network Changed. Date and time of the last network change.
- Sessions. Number of user sessions on the device.
- Last User. Last user logged into the device in domain\account format.
- **Connected From.** When the selected device is a VDI or similar, shows the device name from which the virtual device is accessed.
- Connection Time. Date and time when the session started.
- **Code.** Lets identify the device with a personal code. This code must be manually filled in individually using the Edit option in the Operations menu of the workspace details.
- **Description.** Allows the user to identify the device with a personal description. This field must be assigned manually and individually using the Edit option in the Operations menu of the device details.

Extended Info

- RAM. Total capacity of available RAM.
- Cores. Number of processor cores.
- IP Address. Device's IP address on the local network.
- OS. Type of operating system.
- Operating System. OS version.
- Uptime. Time the device has been running since the last boot or reboot. If fastboot is enabled, the device is only off when it is restarted.
- **Region.** Obtained using the public IP. It might not be accurate if connected to a corporate network or using a VPN.
- Session Analyzer. Indicates whether or not it's configured to launch session Analyzer in all user sessions.
- Session Analyzer Version. Version number of Session Analyzer.
- Report Group. Reporting group to which the device belongs.

Information in tabs

FlexxAgent groups information about the following aspects of the device:

Sessions

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

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.

		G	Σ	•	Operations	*	<	\geq
	Active alerts: • [Critical] Low storage free space % for Workspace: Drive: C: Free space: 2 GB, Used Percentage: 98%							
0	General							

Connection Log

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

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

Disks

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

Notifications

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

Reporting groups history

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

FlexxAgent / Supported Systems / Android

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

Requirements

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

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

Supported versions

FlexxAgent runs on Android devices version 9.0 or later.

Limitations

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

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

Settings

FlexxAgent configuration is managed through <u>Managed Configurations</u> 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.

	9:39 🚥		NI 🖘 al 5 0	0%=
			¢ (
	×	Google		tra
	G	CDO Test cdo-test@flexxible.com	C	
		Gestionar tu cuenta de Go	oogle	
	©	Acciones recomendadas	•	
		Gestionar apps y dispositivo)	
l	¢	Notificaciones y ofertas		
	8	Pagos y suscripciones		
	۲	Play Protect		
		Biblioteca		
	\diamond	Play Points		
	۲	Ajustes		
	0	Ayuda y comentarios		
	Politica	a de Privacidad • Términos d	el Servicio	
			<	

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



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





FlexxAgent se ha configurado de forma correcta. Puedes cerrar esta ventana.

CERRAR

() INFO

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

4. Close the window.

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



Update

FlexxAgent updates automatically from Google Play.

Information obtained from the device

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

Flex	WORKSPACES					All tenants	- 🗘 Log Df
evel 1 ~	Workspace \						Operations - < >
	General						
C.	tampung SMA127F	Summary status On	Power state On	FlexxAgent vention 24.07.02.098	Resolution Working	Resulting report () 8/9/2004 8:02:08 AM	
	Connection	Network (8 192.168.1.0/24 (93.176.147.4) 🖪	Subret 192.160.1.0/24	MAC address	Network changed 5/9/2024 7:56:59 AM		
jen Ann	Tersions. 1	Last user	Connected fram	Convection time 0/9/2024 7:21 AM			
Arra R ^a	Wantess network	Network signal 99.%	Code ()				
	Extended						
。 , ⊗ ,	8441 4 GB	Cores D	P address 192.168.1.140	os 🌳 Android	Operating system Android 15	05 Build number	
	Eptime () 40m	Fending reloat No					
	System diak Univnovm	Public IP & ISP (0)	Region (0) Terressa (ES)				
	Delivery group (3)						
	Session analyser () Configured	Section analyzer vention 24.07.02.098	Reporting group Physical devices				
	Sessions Performance Jobs Alerts	Connection logs Diales Boot history	Notifications PnP Devices				
							8 .
	Device ID 1	None 1	Volume label	Total size Used size % Use	d OS Location	Partition	Physical disk size
	•	/storage/emulated/0	Memoria de dispositivo	137,438 MB 0 MB 0 %	2 C	Nemoria de dispositivo	137,438 MB
	Caurort						
	< 1 >						Page size 20 -

General information

- Name. Device model.
- Device Status. Device power state. It can be On, Off, or Not reporting.
- FlexxAgent Version. Version number of FlexxAgent installed on the device.
- FlexxAgent Status. Running or Stopped.
- Last FlexxAgent Report. Date and time of the last FlexxAgent report on the device. This date might not be recent if the FlexxAgent service is stopped or the device is off.
- Connection Type. Indicates if the device is connected via *Wireless LAN*, *Mobile Network*, *Ethernet*, or *Unknown*.
- Network. Network addressing of the device and public IP for internet access. These networks are created automatically when more than four devices are connected to the same network.
- Network Signal. Network reception percentage.
- Subnet. Device's network addressing.
- MAC Address. Unique identifier of the device's network card.
- Network Changed. Date and time of the last network change.

- Sessions. Number of user sessions on the device.
- Last User. Last user logged into the device in domain\account format.
- **Connected From.** When the selected device is a VDI or similar, shows the device name from which the virtual device is accessed.
- Connection Time. Date and time when the session started.
- **Code.** Lets identify the device with a personal code. This code must be manually filled in individually using the Edit option in the Operations menu of the workspace details.
- **Description.** Allows the user to identify the device with a personal description. This field must be assigned manually and individually using the Edit option in the Operations menu of the device details.

Extended Info

- RAM. Total amount of available RAM.
- Cores. Number of processor cores.
- IP Address. Device's IP address on the local network.
- OS. Type of operating system.
- Operating System. OS version.
- **Uptime.** Time the device has been running since the last boot or reboot. If fastboot is enabled, the device is only off when it is restarted.
- **Region.** Obtained using the public IP. It might not be accurate if connected to a corporate network or using a VPN.
- Session Analyzer. Indicates whether or not it's configured to launch session Analyzer in all user sessions.
- Session Analyzer Version. Version number of Session Analyzer.
- **Report Group.** Reporting group to which the device belongs.

Information in tabs

FlexxAgent groups information about the following aspects of the device:

Sessions

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

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.

	C	2	•	Operations	•	<	\geq
Active alerts: - [Critical] Low storage free space % for Workspace: Drive: C: Free space: 2 GB, Used Percentage: 98%							
General							

Connection Log

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

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

Disks

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

Notifications

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

Reporting groups history

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

FlexxAgent / Network and Security

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

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

Bandwidth usage

FlexxAgent process

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

FlexxAgent Analyzer process

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

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

Required URLs and Ports

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

URL	Ambit	Port	Region
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
<u>https://south-br.agent-api.analyzer.flexxible.com</u> (Brazil Only)	Agent	443	Brazil South

*** unique identifier provided by Flexxible.

Security

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

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

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

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

Antivirus exclusions

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

The items to exclude from antivirus analysis are as follows:

Folders

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

Compute

• FlexxAgent.exe

- FlexxibleRA.exe
- FlexxibleRemoteAssistance_XXXX.exe

Files

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

Deep SSL Inspection

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
- <u>https://flxiothub***.azure-devices.net</u>
- https://agents-weu.flexxible.net
- <u>https://ras.flexxible.com</u>

PowerShell process restriction

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

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

To resolve it, Flexxible recommends excluding the following items:

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

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

Wake on LAN (WoL)

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

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

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

Configure Wake on LAN (WoL) in Windows

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

1. Check if WoL is On

In the CMD window, execute the following command:

powercfg /devicequery wake_programmable

2. On WoL

Run the command:

powercfg /deviceenablewake "Realtek PCIe GbE Family Controller"

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

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.

🖓 ТІР

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

FlexxAgent / Wake on LAN (WoL)

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

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

Requirements

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

() INFO

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

Set up WoL in Windows

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

1. Check if WoL is active.

In the CMD window, execute the following command:

powercfg /devicequery wake_programmable

2. Enable WoL.

Run the command:

powercfg /deviceenablewake "Realtek PCIe GbE Family Controller"

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

Available actions

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

- Power on devices on demand from Workspaces
- <u>Schedule power on using Workspace Groups</u>
- 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).
| | | 5 | | | | \Diamond | | Log Off |
|----------------|------------|-------------------------|---------------|----------------|---|--|----------|---------------------|
| Level 1 ~ | Workspaces | □ \$ 8 6 | , 0 | My Filters | Turn on
Shut down
Restart
Power off (not recommended)
Force restart (not recommeded)
Turn on (Wake on LAN) | Power and connection actio
Tags
FlexxAgent
Maintenance (Drain mode)
Refresh Workspace info | , | sarch P |
| Sessions | Platforms | Machine † RG Tenant | Power state | Last user Ses | Log off
Force log off
Disconnect | Force check compliance
Force update custom fields
Remote administration | · 6 | Keset View Settings |
| D
Joba | □ 👫 🗖 | | Not reporting | contract (| 0 % 0 % | Remote assistance
Notifications
Change reporting group | , X | Operations |
| Alerts | | attar | Not reporting | | 0 % 0 % | 18h | *
© * |
ج |
| vofile Storage | 0 🚦 🔶 🔇 🔺 | Contraction (Section 1) | On | (10)00.01000.0 | 3 % 34 % 40 | i 20h | 0 > | ۷ |

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.

Action *		
Wake On LAN Veek day * Select week day TC Time * ① -: Use specific Workspace for WoL Vorkspace		
Neek day *		
Select week day		\sim
JTC Time * 🕕		
		G
	for WoL	
Use specific Workspace Norkspace Select the Workspace	for WoL	~
Norkspace Select the Workspace	for WoL	
Norkspace Select the Workspace Search the Workspace		
Norkspace Select the Workspace Search the Workspace		
Norkspace Select the Workspace Search the Workspace		
Norkspace Select the Workspace Search the Workspace		

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

Schedule power on after applying updates

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

5. Click on Save.

Edit patch policy target	×
Name	
Target-Docs	
Reporting Groups *	
RT RP Training ×	
Microsoft patch policy	
Select Microsoft patch policy	\sim
Restart after patching ①	
Wake on LAN (i)	

FlexxAgent / FlexxAgent Guides

Flexcible III	Si organización	Administrador de Organización
û Inicio	FxxOne Agent - X	
۶å Inquilinos	📩 🔤 Flexcible	
Microservicios		+ Nuevo
Settings ^	Downloading FlexxAgent	
Información	Nd	Acción
Usuarios	Se Copyright © Flexible	🕑 Ver detalle 🛛 🗘 Descargar agente
Productos	VIP Interactivo	C Ver detalle 🗘 Descargar agente
Módulos	Eamilia Interactivo	Ver detalle

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

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

FlexxAgent / Guides / Validate FlexxAgent connectivity

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

Note: This procedure only applies to Windows systems.

Creating a scheduled task

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

💷 Ejeci	utar X
0	Escriba el nombre del programa, carpeta, documento o recurso de Internet que desea abrir con Windows.
<u>A</u> brir:	taskschd.msc ~
	Aceptar Cancelar <u>E</u> xaminar

- 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.

Create Basic Task Wizard				×
迿 Task Trigger	₽			
Create a Basic Task Trigger One Time Action Finish	When do you want the task to start? Daily Weekly Monthly One time When the computer starts When I log on When a specific event is logged			
		< Back	Next >	Cancel

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

Create Basic Task Wizard		×
Distance Action		
Create a Basic Task	What action do you want the task to perform?	
Trigger One Time		
Action	Start a program	
Finish	O Send an e-mail (deprecated)	
	 Display a message (deprecated) 	
1		
	< Back Next > Ca	ancel

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.

Create Basic Task Wizard					\times
5tart a Program					
Create a Basic Task					
Trigger	Program/script:				
One Time	C:\Program Files\Flexxible\FlexxAgent\FlexxAgen	nt.exe		Browse	
Action Start a Program	Add arguments (optional):		/TestMess	agingEngine	
Finish	Start in (optional):				
			-		
		< Back	Next >	Cance	el

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

Create Basic Task Wizard		×
5 Summary		
Create a Basic Task		
Trigger	Name:	fh
One Time	Description:	
Action		
Start a Program		
Finish		
	Trigger:	One time; At 1:32 on 28/08/2024
	Action:	Start a program; "C:\Program Files\Flexxible\FlexxAgent\FlexxAgent.exe" /Te
	🗹 Open the	Properties dialog for this task when I click Finish
	When you cl	ick Finish, the new task will be created and added to your Windows schedule.
		< Back Finish Cancel

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.

🕒 fh Propertie	s (Local Computer)					×
General Trigg	gers Actions Condi	ions Settings	History			
Name:	fh					
Location:	١					
Author:	FLEXXIBLE\fzani					
Description:						
- Security opt	ions					
When runn	ng the task, use the fo	llowing user ac	count:			
NT AUTHOR	RITY\SYSTEM			CI	hange User or G	roup
Run only	when user is logged o	n				
O Run whe	ther user is logged on	or not				
🗌 Do n	ot store password. Th	e task will only l	have access to local o	computer resou	rces.	
🗹 Run with	highest privileges					
🗌 Hidden	Configure for:	Windows Vista	™, Windows Server™	2008		\sim
				0	K	Cancel

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.

Task Scheduler		– 🗆 ×
File Action View Help		
🗢 🔿 🖄 📆 🔀 🗖		
 Task Scheduler (Local) Task Scheduler Library Lenovo Microsoft Mozilla 	Name Status Triggers Status Triggers Triggers Adobe Acrobat Update Task Ready Multiple triggers defined FlexxAgent check connectivity Ready At 11:51 on 28/08/2024 FlexxAgent Health Check Run ry day - After triggered MicrosoftEdgeUpdateTaskl End igers defined MicrosoftEdgeUpdateTaskl Disable / day - After triggered, OneDrive Per-Machine Sta Export 1/05/1992 - After triggered	Actions Task Scheduler ▲ Create Ba Create Tas Import Ta Display Al F Chable All
	General Triggers Actions Delete Dry (disabled)	Enable All
	inggers Actions	View
	Name: FlexxAgent check connectivity	Q Refresh
	Location: \ Author: FLEXXIBLE\Isanchez	Help
	Description: description	Selected Item
		 Run End Disable
	Security options When running the task, use the following user account:	Export Properties Celete

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:

 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.

🔶 📶 🔝 📷								
Event Viewer (Local)	Application Number	of events: 24.626						
Custom Views	Level	Date	and Time		Source	Event ID	Task Category	
Application	(1) Information	28/0	8/2024 12:17:36		Security-SPP	16384	None	
Security	Information	28/0	8/2024 12:16:39		Security-SPP	16394	None	
E Setup	Information	28/0	8/2024 12:16:33		FlexxAgent Service	0	None	
🛃 System	Information	28/0	8/2024 12:16:30		FlexxAgent Service	0	None	
Forwarded Events	Information	28/0	3/2024 12:16:29		FlexxAgent Service	0	None	
Applications and Services Lo	Information	28/0	8/2024 12:16:28		FlexxAgent Service	0	None	
Subscriptions	Information	28/0	8/2024 12:15:15		FlexxAgent Service	0	None	
	Event 0, FlexxAgent St	rvice						
	General Details							
	-Primary IoT Hub -Secondary IoT Hu	king messaging service o connection string ok ib connection string ok	onnectivity					
	Log Name:	Application						
	Source:	FlexxAgent Service	Logged:	28/08/2024 12:16:30				
	Event ID:	0	Task Category:	None				
	Level:	Information	Keywords:	Classic				
	User:	N/A	Computer:	LAPLSAN-PC181				
	OpCode:	Info						

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:

Event 0, FlexxAgent Service

General Details

12:16:23 Start checking messaging service connectivity	
-Primary IoT Hub connection string ok	
-Secondary IoT Hub connection string ok	
-Primary service bus connection string ok	
-Secondary service bus connection string ok	
12:16:30 Messaging service checking finished	

Machine name: LAPLSAN-PC181 Process name: FlexxAgent (24.5.3.1)

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

C:\Users\administrator\Desktop\FlexxAgent-Installer)>FlexxAgent-Installer.exe -proxyAbsoluteUri
-proxyUser -proxyPass -proxyPersistConfig -repairAgent true
2024-01-15 10:11:37 - FlexxAgent version: installer
2024-01-15 10:11:37
2024-01-15 10:11:37 - Required free space is 500 MB and current free space is 111320.82421875 MB
2024-01-15 10:11:37 - Path of current execution: . 2024-01-15 10:11:37 - Configuration file path: .\FlexxAgent-Configuration.conf
2024-01-15 10:11:37\FlexxAgent-Installer.exe
2024-01-15 10:11:38 - Preparing temp folder
2024-01-15 10:11:38 - Getting C data
2024-01-15 10:11:38 - Windows version:
2024-01-15 10:11:38 - Windows OS: Microsoft Windows 10 Enterprise
2024-01-15 10:11:38 - OS Architecture: 64-bit
2024-01-15 10:11:38 - OS language: 1033
2024-01-15 10:11:38 - Portable OS system: False
2024-01-15 10:11:38 - Total memory: 4193272
2024-01-15 10:11:38 - Total logical processors: 2
2024-01-15 10:11:38 - Temporary folder: C:\Windows\Temp\FlexxibleIT
2024-01-15 10:11:38 - Checking .Net Framework version
2024-01-15 10:11:38 - Checking OS architecture
2024-01-15 10:11:38 - 64-bit
2024-01-15 10:11:38 - Logon server: 2024-01-15 10:11:38 - Attempted to install FlexxAgent version 22 40 0 2
2024-01-15 10:11:38 - Attempted to install reakagent version 2021-01-15 10:11:38 - RepairAgent option is set to true. The current FlexxAgent version will be overwritten.
2024-01-15 10:11:38 - Configuring TLS 1.2 connection
2024-01-15 10:11:38 - FlexAgent online installation
2024-01-15 10:11:38 - Provided proxy:
2024-01-15 10:11:38 - Downloading file
2024-01-15 10:11:38 - Provided proxy settings:
2024-01-15 10:11:38 - Provided proxy port: 5100
2024-01-15 10:11:38 - Provided proxy authentication: :
2024-01-15 10:11:42 - Configuring FlexxAgent communications
2024-01-15 10:11:42 - Configuring FlexxAnalyzer
2024-01-15 10:11:42 - Uncompressing install package
2024-01-15 10:11:43 - Attempted to install FlexxAgent version: 2024-01-15 10:11:43 - Package detected version: (
2024-01-15 10:11:43 - Package detected version: V 2024-01-15 10:11:43 - FlexxAgent status: uninstalled
2024-01-15 10:11:43 - FlexAngent Status, uninstalled 2021-015 10:11:43 - Installing FlexAngent
2024-01-15 10:11:43 - MSI file: C:\Windows\Temp\FlexxibleIT\FlexxAgent_Setup.msi
2024-01-15 10:11:43 - Log file installation: C: Windows\Temp\FlexxibleIT\FlexxibeIT\FlexxAgentInstallation.log
2024-01-15 10:11:43 - Set persistent proxy configuration for FlexxAgent service 'Proxy URL'
2024-01-15 10:11:43 - Set persistent proxy configuration for FlexxAgent service 'Proxy User'
2024-01-15 10:11:43 - Set persistent proxy configuration for FlexxAgent service 'Proxy Pwd'
2024-01-15 10:11:47 - Installation completed.
2024-01-15 10:11:47 - Process completed.
C:\Users\administrator\Desktop\FlexxAgent-Installer →

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 <u>https://www.base64encode.org/</u>.

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 '<u>http://192.168.1.1:3128</u>' or '<u>https://192.168.1.1:3128</u>'

Key Proxy_User

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

Key Proxy_Pwd

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

FlexxAgent / Guides / Set up a proxy server through group policies (GPO)

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

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



- 2. Give the new policy an appropriate name and click the OK button.
- 3. Select the policy with the right mouse button and edit it (select Edit...)
- 4. In the edit window, expand Computer Configuration, Preferences, and Windows Settings. Select Registry and then New -> Registry Item.

Computer - Configure ElexxAge Computer Configuration Policies	💣 Registry				
 Preferences Windows Settings 	Processing (*)	Name	Order	Action	Hive
S Environment	Processing 🎗	There	are no items t	o show in th	is view.
Folders		<u>N</u> ew	>	Regist	ry Item
💣 Registry		All Tas <u>k</u> s	>	Collec	tion Item
Network Shares		<u>P</u> aste		Regist	ry Wizard

- 5. Add the following information and click OK.
 - Action: Update
 - Key path:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Flexxible\FlexxAgent\Communicati

- Value Name: Proxy_URL
- Value type: REG_SZ
- Value data: The proxy address (URL) and port. For example https://192.168.1.1:3128.

New Regi	stry Prope	rties	×
General	Common		
Ď	Ac <u>ti</u> on:	Update	~
<u>H</u> ive: <u>K</u> ey Path	1:	HKEY_LOCAL_MACHINE Policies\Flexxible\FlexxAgent\Communications	~
-Value r	name		
De	e <u>f</u> ault	Proxy_URL	
<u>V</u> alue ty	pe:	REG_SZ	~
Va <u>l</u> ue da	ita:	http://192.168.1.1:3128	
	0		Help

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

Na	me	Order	Action	Hive	
ah	Proxy_URL	1	Update	HKEY_LOCAL_MA	CHINE
	New	>	Regis	try ltem	
	All Tasks	>	Colle	ction ltem	
	Refresh		Regis	try Wizard	
	Export List				
	View	>			
	Arrange Icor Line up Icon				
	Help				

- 7. Add the following information and click OK.
 - Action: Update

• Key path:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Flexxible\FlexxAgent\Communicati

- 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\Communicati

- 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 <u>https://www.base64encode.org/</u>.

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

Computer - Configure FlexxAgent Proxy [FLEXXLABDCJ Figure Configuration Policies Policies	💣 Registry								
✓ IPreferences ✓ I Windows Settings	Processing (R)	Name		Action	Hive	-	Value Na		Value Data
Environment		Proxy_Pwd Proxy_URL				SOFTWARE\Policies\Flexxible\FlexxAgent\Communications SOFTWARE\Policies\Flexxible\FlexxAgent\Communications			
💁 Folders		Proxy_User	2	Update	HKEY_LOCAL_MACHINE	SOFTWARE\Policies\Flexxible\FlexxAgent\Communications	Proxy_User	REG_SZ	Administrator
Ini Files									

11. Close the editor.

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



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



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

📑 Registry Editor

<u>File Edit View Favorites H</u>elp

mputer	\HKEY_LOCAL_MACHINE\SO	FTWARE\Policies\Flexxible	FlexxAgent\Communi	cations
Compu		Name	Туре	Data
	Y_CLASSES_ROOT	ab (Default)	REG SZ	(value not set)
	Y_CURRENT_USER	ah	-	
	Y_LOCAL_MACHINE	ab		
	3CD0000000	au -		
	DRIVERS	ab		
> 🔤 H	HARDWARE	a		
> 🔤 S	SAM	ab		
- <mark>-</mark> S	ECURITY	~~		
Y 🔤 S	OFTWARE	ab		
>	Classes	ab Heartbeat	REG_SZ	2023-02-21 15:44:39
>	Clients	a		
	CVSM	ab]Proxy_Pwd	REG_SZ	&&&VGhpc0lzTjArQCQzY3VyZVBAJCR3MHJk&&&
	DefaultUserEnvironment	ab Proxy_User	REG_SZ	Administrator
>	Flexxible	ab Proxy_UTL	REG_SZ	http://192.168.1.1:3128
>	Google	ee Reportinterval	NEG 32	00
>	Intel	at		
>	Microsoft	ab		
>	Mozilla			
>	ODBC			
2	OpenSSH			
>	Partner			
~	Policies			
×	Flexxible			
	V FlexxAgent			
	Communications			

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.

Group Policy Management	
✓ ▲ Forest: AzureLabDomain.com	
🗸 📑 Domains	
✓ jii AzureLabDomain.com	
🛒 + COMPUTER Set Tim	ne Settings on all Domain Members v1.0
🛒 Default Domain Policy	у
> 📔 Domain Controllers	
🔪 🔚 Lab	
🗸 📑 Group Policy Obje	New
j≣[+ COMPUTER]	New
🗐 + SERVER Set P	Back Up All Se
+ SERVER Set T	Manage Backups rs \
🧾 Default Domai	Open Migration Table Editor
🧾 Default Domai	
> 🕞 WMI Filters	View >
> 🧊 Starter GPOs	New Window from Here
> 📫 Sites	
👸 Group Policy Modeling	Refresh
🕞 Group Policy Results	Help
	· ·F

- 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)

Computer Startup Script - Install the Flexxible FlexxAgent [.	Scripts (Startup/Shutdown)	
E Computer Configuration One Policies	Startup	Name
 Software Settings Windows Settings 	Display <u>Properties</u>	Startup
Scripts (Startup/Shutdown)	Description: Contains computer startup scripts.	

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

tartup Properties		?	×
Scripts PowerShell	Scripts		
	ows PowerShell Startup Scripts for Co - Install the Flexxible FlexxAgent	mputer Sta	artup
Name	Parameters		<u>J</u> p p <u>w</u> n
			<u>1</u> d dit
For this GPO, run s	cripts in the following order:	<u>R</u> er	nove
Not configured		/	
PowerShell s 2008 R2	scripts require at least Windows 7 or \	Windows S	
		how Files.	
	OK Cance	4	Apply

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.

📙 🛃 📙 🖛 Startup				
File Home Share	View			
\leftrightarrow \rightarrow \checkmark \uparrow \square > Net	twork → AzureLa	abDomain.com > SysVol	> AzureLabDomain.com > F	Policies → {146D2D
A Quick access	Name	Date modified	Туре	Size
Desktop	📓 Install.ps1	2/11/2024 9:06 AM	Windows PowerShell Script	1 KB

- 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 0k to close the dialog. The file will appear in the configuration modal window.
- 16. Select OK to close this window. You'll return to the group policy editor. This window can be closed.
- 17. Find the organization branch within the domain controller that contains the devices where you want to install FlexxAgent. Select the branch and right-click on it. Select Link an Existing GPO.



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

Verification

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

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

🛃 Event Properties -	Event 11707, Msilnstaller			×
General Details	nt Installation completed su	uccessfully.		
Log Na <u>m</u> e: <u>S</u> ource: <u>E</u> vent ID: Level: User: OpCode: More Information:	Application Msilnstaller 11707 Information SYSTEM Info <u>Event Log Online Help</u>	Logge <u>d</u> : Task Categor <u>y</u> : <u>K</u> eywords: Compute <u>r</u> :	2/12/2024 2:22:33 PM None Classic W10-22H2-SU-0.AzureLabDomair	•
Сору				<u>C</u> lose

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

						(2) Operations •
General						
Domain AzureLabDomain.com	Name W10-22H2-SU-0	Sammany status On	Pawer state On	Reconfigent version 23.6.0.1	Resultgent status	
Seasions 0	Last user AZURELABDOMAIN/flexxadmin	Connected from	Connection time			
OV OU=Computers, OU=Lab, DC=AzureLabDomair	n,DC=com					
Tago						
Extended						
RAM						
8 GB	Cares 2	Lacal disk (C) 96.9 GB free of 126.5 GB (23% use	P address 1) 172.16.2.8	Windows Microsof	edition It Windows 10 Enterprise 22H2	Windows Type Client (Workstation)
8 GB Upsime	2 Idle time	96.9 GB free of 126.5 GB (23% uses	d) 172.16.2.8 Last boot duration (i)			
8 GB Upsive 19m Resource group	2 Idle clime O Hours Size	96.9 GB free of 126.5 GB (23% user Last windows update 1/29/2024 Here peak	d) 172.16.2.8 Last boot duration (I) 107.5 Semion host type			
8 GB Uppine 19m Researce proop Ansar_Lab_RG Breker type	2 Bile Stree 0 Hours Standard_D23,y3 Hypervbor	96.9 GB free of 126.5 GB (221% user Last violetsen system 1/25/2024 Here yet Here yet Free	3) 172.152.8 Late boor division (0) 107.5 Seasilie Heat type Personal Subscription/Breker			

The installation log can be seen in detail in the file

C:\Windows\Temp\FlexxAgentInstallation.log.

FlexxAgentinstallation.log - Notepad	-		\times
e Edit Format View Help			
24-02-12 14:19:54 - FlexxAgent version: installer			
24-02-12 14:19:55			
24-02-12 14:19:59 - Required free space is 500 MB and current free space is 99666.828125	B		
24-02-12 14:19:59 - Path of current execution: \\azurelabdc\Software\FlexxAgent-Installer	-		
24-02-12 14:19:59 - Configuration file path: \\azurelabdc\Software\FlexxAgent-Installer\F	exxAgent-Configur	ration.c	onf
24-02-12 14:19:59 - \\azurelabdc\Software\FlexxAgent-Installer\FlexxAgent-Installer.exe			
24-02-12 14:19:59 - Preparing temp folder			
24-02-12 14:19:59 - Getting OS data			
24-02-12 14:20:00 - Windows version: 10.0.19045			
24-02-12 14:20:00 - Windows OS: Microsoft Windows 10 Enterprise			
24-02-12 14:20:00 - OS Architecture: 64-bit			
24-02-12 14:20:00 - OS language: 1033			
24-02-12 14:20:00 - Portable OS system: False			
24-02-12 14:20:00 - Total memory: 8388148			
24-02-12 14:20:00 - Total logical processors: 2			
24-02-12 14:20:00 - Temporary folder: C:\Windows\Temp\FlexxibleIT			
24-02-12 14:20:00 - Checking .Net Framework version			
24-02-12 14:20:01 - Checking OS architecture			
24-02-12 14:20:01 - 64-bit			
24-02-12 14:20:01 - Logon server:			
24-02-12 14:20:01 - Detecting if FlexxAgent is already installed			
24-02-12 14:20:02 - FlexxAgent is not installed			
24-02-12 14:20:02 - Configuring TLS 1.2 connection			
24-02-12 14:20:03 - FlexxAgent online installation			
24-02-12 14:20:03 - Downloading file			
24-02-12 14:22:06 - Configuring FlexxAgent communications			
24-02-12 14:22:07 - Provided proxy configuration is not persistent for FlexxAgent service			
24-02-12 14:22:07 - Configuring FlexxAnalyzer			
24-02-12 14:22:07 - Uncompressing install package			
24-02-12 14:22:15 - Attempted to install FlexxAgent version: 023.006.000.001			
24-02-12 14:22:15 - Package detected version: 023.006.000.001			
24-02-12 14:22:15 - FlexxAgent status: uninstalled			
24-02-12 14:22:15 - Installing FlexxAgent			
24-02-12 14:22:15 - MSI file: C:\Windows\Temp\FlexxibleIT\FlexxAgent_Setup.msi			
24-02-12 14:22:15 - Log file installation: C:\Windows\Temp\FlexxibleIT\FlexxAgentInstalla	ion.log		
24-02-12 14:22:36 - Installation completed.			
24-02-12 14:22:36 - Process completed.			
			2
Ln 38, Col 1 100%	Windows (CRLF) U	JTE-8	

FlexxAgent / Guides / Deploy FlexxAgent with Microsoft Intune

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

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

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

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

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



- 2. Download the Microsoft Win32 Prep Tool. For more information, see Prepare a Win32 app to be uploaded to Microsoft Intune.
- 3. Create an empty folder; for example: C:\Temp\FlexxAgent-Installer-output.

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

🚬 Ac	Iministrator: Windows PowerShell	-		×
S C:\	Users\manuelp\Downloads\Microsoft-Win32-Content-Prep-Tool-master> .\IntuneWinAppUtil.exe			
	specify the source folder: C:\Temp\FlexxAgent-Installer			
	specify the setup file: FlexxAgent-Installer.exe			
lease	specify the output folder: C:\Temp\FlexxAgent-Installer-output			
	want to specify catalog folder (Y/N)?n			
NFO	Validating parameters			
NFO	Validated parameters within 12 milliseconds			
NFO	Compressing the source folder 'C:\Temp\FlexxAgent-Installer' to 'C:\Users\manuelp\AppData\Local	\Temp\5	edb01c5	- 60
	-9b14-e47afb372dca\IntuneWinPackage\Contents\IntunePackage.intunewin'			
IFO	Calculated size for folder 'C:\Temp\FlexxAgent-Installer' is 42695475 within 3 milliseconds			
NFO	Compressed Folder 'C:\Temp\FlexxAgent-Installer' successfully within 2658 milliseconds			
IFO	Checking file type			
NFO NFO	Checked file type within 16 milliseconds Encrypting file 'C:\Users\manuelp\AppData\Local\Temp\5edb01c5-6098-486d-9b14-e47afb372dca\Intune	dif e Basi	kanal Ca	
	<pre>chcrypting file (C:\Users\manuelp\AppUata\Local\lemp\SedbolcS-0090-4000-9014-e4/arDS/2dca\Intune unePackage.intunewin'</pre>	wineac	kage\co	nce
	uneratkage_intunewin ':\Users\manuelp\AppData\Local\Temp\5edb01c5-6098-486d-9b14-e47afb372dca\IntuneWinPackage\Conte	ents\In	tunePac	kag
	ewin' has been encrypted successfully within 345 milliseconds	ines (an	currer de	NOF
IFO	Computing SH4256 hash for C:\Users\manuelp\AppData\Local\Temp\Sedb01c5-6098-486d-9b14-e47afb372c	ica\Inti	uneWinP	ack
	tents\cdcfbe6b-ab51-480a-858b-4d7e2919792b			
IFO	Computed SHA256 hash for 'C:\Users\manuelp\AppData\Local\Temp\Sedb01c5-6098-486d-9b14-e47afb3720	dca\Int	uneWinP	ack
e\Con	tents\cdcfbe6b-ab51-480a-858b-4d7e2919792b' within 727 milliseconds			
IFO	Computing SHA256 hash for C:\Users\manuelp\AppData\Local\Temp\Sedb01c5-6098-486d-9b14-e47afb372c	ica\Int	uneWinP	ack
:\Con	tents\IntunePackage.intunewin			
IFO	Computed SHA256 hash for C:\Users\manuelp\AppData\Local\Temp\5edb01c5-6098-486d-9b14-e47afb372dd	:a\Intu	neWinPa	icka
	ents\IntunePackage.intunewin within 726 milliseconds			
NFO	Copying encrypted file from 'C:\Users\manuelp\AppData\Local\Temp\Sedb01c5-6098-486d-9b14-e47afb			
	Contents\cdcfbe6b-ab51-480a-858b-4d7e2919792b' to 'C:\Users\manuelp\AppData\Local\Temp\Sedb01c5-6	5898-48	6d-9b14	- e4
	dca\IntuneWinPackage\Contents\IntunePackage.intunewin'	e		
IFO	File 'C:\Users\manuelp\AppData\Local\Temp\Sedb01c5-6098-486d-9b14-e47afb372dca\IntuneWinPackage\ intunewin' got updated successfully within 197 milliseconds	Conten	cs/Turn	ner
kage. NFO	Generating detection XML file 'C:\Users\manuelp\AppData\Local\Temp\Sedb01c5-6098-486d-9b14-e47a4	(b372dc)	a) Totuo	ودرس
	denerating detection with the crosses (manuely (apports (cots) (cmp) (seudores - 400-5014-64/an	057200	avrucan	ent
IFO	Generated detection XML file within 71 milliseconds			
NFO	Compressing folder 'C:\Users\manuelp\AppOata\Local\Temp\Sedb01c5-6098-486d-9b14-e47afb372dca\Int	tuneWin	Package	• t
	emp\FlexxAgent-Installer-output\FlexxAgent-Installer.intunewin'			
IFO	Calculated size for folder 'C:\Users\manuelp\AppData\Local\Temp\5edb01c5-6098-486d-9b14-e47afb33	/2dca\I	ntuneWi	nPa
ige'	is 42469690 within 2 milliseconds			
	Compressed folder 'C:\Users\manuelp\AppData\Local\Temp\Sedb01c5-6098-486d-9b14-e47afb372dca\Intu	uneWinP	ackage'	su
	lly within 1067 milliseconds			
IFO	Removing temporary files			
NFO	Removed temporary files within 13 milliseconds			
IFO	File 'C:\Temp\FlexxAgent-Installer-output\FlexxAgent-Installer.intunewin' has been generated suc	cessfu	11y	
	100%			
NFO	Done!!!			
s c:	Users\manuelp\Downloads\Microsoft-Win32-Content-Prep-Tool-master> _			
1				

5. Confirm that the package has been created correctly.

Loca	al Disk (C:) > Temp > FlexxAgent-Installer-o	~	5	Search F	FlexxAgent-Insta	
^	Name	Date modified	Тур	e		Size
	FlexxAgent-Installer.intunewin	20/03/2023 14:43	INT	UNEWIN	N File	41.475 KB

- 6. The created package is used to deploy an application within Intune.
- 7. Go to the Intune admin center.
- 8. Select Apps and then All Apps.

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

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

App package file

 \times



- 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.

FlexxAgent-Installer.intunewin					
FlexxAgent-Installer standalone					
~					
Enter a valid url					

- 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

25.6 / FXXOne Documentation / FXXOne

O App information O Program	③ Requirement	ts (4) Detection rules	③ Dependencies	€ Su	iper			
Specify the commands to install and uninstall this app:								
install command * 🕕	talier.exe 🗸							
Uninstall command * 🛈	%ProgramFiles%\F	lexxible\FlexxAgent\VDIServic	eUpdater.exe /uninstall "C	\Pro >	/			
Install behavior	System User	\supset						
Device restart behavior ①	No specific action			~	^			
Specify return codes to indicate post-instal	lation behavior:							
Return code		Code type						
0		Success		\sim (1			
1707		Success		~ 1)			
3010		Soft reboot		~ [1			
1641		Hard reboot	~ 1	1				
1618		Retry	~ (1				
+ Add								

- 13. On the Requirements tab, you need to include information about the operating system architecture:
 - Operating system architecture: 64-bit

Previous

Next

• Minimum operating system: Select according to the version used in the current installation (device fleet). For example, the minimum: Windows 10 1607.

App information	Program	3 Requirements	(4) Detection rules	5 Dependencies	6 Superseder
Specify the requirements that d	evices must r	meet before the app is i	nstalled:		
Operating system architecture *	•	64-bit			\sim
Minimum operating system * (0 [Windows 10 1607			\sim
Disk space required (MB) 🕕	[
Physical memory required (MB)	i [
Minimum number of logical pro required ①	ocessors [
Minimum CPU speed required (MHz) 🛈 [
Configure additional requirement	nt rules				
Туре		Pati	n/Script		
No requirements are specified	l.				
+ Add					

- 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

Detection rule

 \times

Create a rule that indicates the presence of the app.

Rule type	File	\sim
Path * 🛈	%ProgramFiles%\Flexxible\FlexxAgent	
File or folder * 🛈	FlexxAgent.exe	
Detection method * (i)	File or folder exists	\sim
Associated with a 32-bit app on 64-bit clients ①	Yes No	

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

Assignments Revie	w + save								
Any Win32 app de take explicit action	ployed using intune will not be a n on the device to remove the ap	automatically removed from th sp.	e device when the device is reti	red. The app and the data it	contains will remain on the o	device. If the app is not rem	oved prior to retiring the de	vice, the end user will need t	0
Required ①									
Group mode	Group	Filter mode	Filter	End user notifications	Availability	Installation deadline	Restart grace period	Delivery optimizatio	
Included	AAA-FlexxAgent-Installer	None	None	Show all toast notifications	As soon as possible	As soon as possible	Disabled	Content download in background	
+ Add group 🛈 + Add	all users 🛈 + Add all devices (0							
Available for enro	lled devices 🛈								
Available for enro	Group	Filter mode	Filter	End user	notifications Availa	bility	Restart grace period	Delivery optimizatio	
		Filter mode	Filter	End user	notifications Availa	bility	Restart grace period	Delivery optimizatio	
Group mode No assignments			Filter	End user	notifications Availa	bility	Restart grace period	Delivery optimizatio	
Group mode No assignments	Group		Filter	End user	notifications Availa	bility	Restart grace period	Delivery optimizatio	
Group mode No assignments + Add group ③ + Add	Group		Filter	End user	notifications Availa Availability	bility Installation deadline	Restart grace period	Delivery optimizatio	
Group mode No assignments + Add group ③ + Add Uninstall ④	Group all users () + Add all devices ()	0							

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

	Edit assignment AAA-FlexxAgent-Installer-deploym	ent
ired. The app and the data it contains wi	Assignment settings Mode ③	Included Excluded
End user notifications Availabi	App settings End user notifications Delivery optimization priority	Show all toast notifications
End user notificati		vailable as soon as it has been deployed, unless you specify an this is a required application, you may specify the installation
	App availability App installation deadline	As soon as possible \checkmark

- 17. Click on +Add all devices so that it is deployed on all devices enrolled in Intune.
- 18. Once you click Review+Create, the deployment will begin. You need to allow at least one hour for it to take effect and complete.


FlexxAgent / Guides / Deploy FlexxAgent for Android with Microsoft Intune

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

Select app type

Create app

Select app type	~
Store app	
Android store app	
Managed Google Play app	
Other	
Web link	
Built-In app	
Line-of-business app	
Android Enterprise system app	

X

Sync 2	Google Play
÷	Search
	FlexxAgent
	Flexxible
	Virrated
	This app offers managed configuration This app is only available in certain countries Select
	FlexxAgent is the Flexxible solution's local component, responsible for collecting information about the devices and applications, and sending it to the service's web consoles.

2. FlexxAgent will appear in the app list:



3. Configure the app:

App information	Review + save			
Name 🕕		FlexxAgent		
Description 🕕		FlexxAgent es el componente	e local de la solución Flexcible	
Publisher ①		Flexible		
Appstore URL ①		https://play.google.com/work	<pre>c/apps/details?id=com.flexxible</pre>	e.flexxagent.app& [
Logo 🕕		Change image		
		∞		
		\mathbf{x}		
Available licenses		0		
Available licenses Total licenses				
		0		
		0		
Total licenses		0		
Total licenses		0	Filter	Update Pris

Configuration policy management

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

lome > Apps App configuration		
Basics (2) Review + sav	e.	
Name *		
Description		
Device enrollment type	Managed devices	\sim
Platform 💿	Android Enterprise	~
Profile Type 🕕	All Profile Types	~
Targeted app * ③	FlexxAgent	

dit app configur	ation polic	у		
lot configured				
onfiguration Settings				
onfiguration settings format	Use co	onfiguration designer		~
ise the JSON editor to configu	re the disabled confi	guration keys.		
+Add				
Configuration key	Value type	Configuration value	Description	
IoT Hub Name	string			
Service Bus connection s	string			
Service Bus Queue Name	string			
Device Connection String	string			
Reporting Group	string			
Signed-in user's email a	string			
Signed-in user's domain	string			
First part (part before @)	string			
Device's directory ID	string			
Device's serial number	string			
Asset ID assigned to a d	string			
Location assigned to a d	string			
Environment	string	production		
onnected apps				

() INFO

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

Analyzer

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

FIEXCAN	ALYZER			¢ 0 ♥ »	lestern Europe
Care and a second secon	APP CATALOG & INVENTORY	diagnosis (Q	GREEN IT	USER EXPERIENCE	WORKSPACES
	Show less (6) APP GROUPS	APPS VERSION	POLLS	USERS	^ USERS GROUPS
				80	
				G.	
FlexxAna	lyzer 2024				

Included tools

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

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

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

Tools included in Analyzer:

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

- **Diagnosis.** Enables a diagnostic view and allows you to see the details of resource and application usage by devices in configurable time slots.
- **Green IT.** Allows evaluating the carbon footprint generated by printing and the electrical consumption of devices and their peripherals.
- User experience. Helps detect and solve problems by analyzing device performance and user sentiment.
- Workspaces. Offers an inventory view of the devices and collects information on detected issues.
- App Groups. Allows creating groups of applications for joint analysis.
- Apps version. Offers a condensed view of the applications with more versions over time.
- **Polls.** Allows configuring the sending of surveys to capture user sentiment and use this data to build the experience index (UXI).
- Users. Contains information on the detected users and for each one details the applications and devices used historically.
- User Groups. Allows creating groups of users.

Web Interface

List Views

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

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

Name 🛧	Unique Identifier	05	Workspaces	Users	Versions	Last Report	Discovered Date	Category	App Groups	Avg RAM	Max RAM
AnyDesk	anydeskolient_usr_7.0.14_inc_	Windows	1 (0%)	1 (1%)	1	2024-01-08	2024-01-08	NonCategor_		176 MB	277 MI
Anydesk.exe	anydesk.exe	Windows	21 (8%)	20(12%)	2	2024-02-16	2022-12-02	Teol	Departmental, Pro	104 MB	560 M I
Apache HTTP Server	http:/.exe	Windows	1 (0%)	1 (1%)	1	2024-01-05	2024-01-05	NonCategor_		57 MB	81 M
Apps20igital Agent (deprecated)	a2dagent.exe	Windows	2 (1%)	2 (196)	1	2024-02-16	2022-07-11	Teol	Departmental, Pro	35 MB	57 Mi
😝 Audacity	audacity exe	Windows	1 (0%)	1 (1%)	2	2024-02-17	2023-01-28	NonCategor		106 MB	210 MI
🐖 Autoplay	autoplay.exe	Windows	1.0%i	1 (196)	1	2024-02-20	2024-02-20	NonCategor		4 MB	4.149
Azure AD dsregcmd	dsregcmd.exe	Windows	1 (0%)	1 (1%)	1	2024-01-10	2022-09-13	Teol	Low Used, Produc	1 MB	1.04
Babel Obfuscator	babeloin.cos	Windows	1 (0%)	2 (1%)	1	2024-02-12	2023-02-10	NonCategor		94 MB	121 MI
Biometric Enrollment Host	bioenroilmenthost.exe	Windows	1 (0%)	1 (1%)	1	2024-02-20	2024-02-20	NonCategor		12 MB	12 M
🞯 Brave Browner	brave.ace	Windows	7 (2%)	6 (4%)	4	2024-02-21	2022-12-20	Commercial	Departmental	877 MB	5.36 GI

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.

Flex	CANALYZER			¢ 0 🛛	Western Europe		ĺ
GG Home	Sack to Previous Page						
	APP CATALOG & INVENTORY / APP DETA	ILS					I
Sectory	🔹 Microsoft PowerPoint					8	1
C RecoAnalyzer Users	Product Name	Category	Exe File		05		I
(?) Hielp	Microsoft PowerPoint	Commercial	powerpnt.exe		Windows		
Help	App Groups		Product Owners				I
	1 Necessary & Productivity	~					I
			W				
	Versions History					~	l
	Workspaces History					~	
	Users History					~	
	Usage History Last 60 Days					~	
	Workspaces Without Usage In The Last	30 Days				^	

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.

Avg GPU	Max GPU	
0 %	0 %	
O %	0 %	
0 %	0 %	Max GPU
0 %	0 %	Equals
0 %	0 %	Not equal
0 %	0 %	د Less than Less than or equals
0 %	0 %	⁹ Greater than
1 %	52 %	Greater than or equals 9 In range

Logical operators that can be operated with:

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

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

Page navigation

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

1 to 10 of 17	<<	Page 1 of 2 >>I	10 👻
---------------	----	-----------------	------

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.

Name 🛧	Unique Identifier	05	Workspaces	Users	Versions	Last Report	Discovered Date	Category	App Groups	Avg RAM	Max RAM
AnyDesk	anydeskolient_usr_7.0.14_inc	Windows	1 (0%)	1 (1%)	1	2024-01-08	2024-01-08	NonCategor		176 MB	277 MI
Anydesk.exe	anydesk.exe	Windows	21 (8%)	20 (12%)	2	2024-02-16	2022-12-02	Teol	Departmental, Pro	104 MB	560 M I
Apache HTTP Server	http:/.exe	Windows	1 (0%)	1 (1%)	1	2024-01-05	2024-01-05	NonCategor		57 MB	81 MI
Apps2Digital Agent (deprecated)	a2dagent.exe	Windows	2 (1%)	2 (196)	1	2024-02-16	2022-07-11	Tool	Departmental, Pro	35 MB	57 Mł
🔒 Audacity	audacity.exe	Windows	1 (0%)	1 (1%)	2	2024-02-17	2023-01-28	NonCategor		106 MB	210 MI
Autoplay	autoplay.exe	Windows	1.0%)	1 (196)	1	2024-02-20	2024-02-20	NonCategor		4 MB	4.03
Azure AD dsregcmd	dsregcmd.exe	Windows	1 (0%)	1 (1%)	1	2024-01-10	2022-09-13	Tool	Low Used, Produc	1 MB	1.00
Eabel Obfuscator	babaluin.eos	Windows	1 (0%)	2 (1%)	1	2024-02-12	2023-02-10	NonCategor		94 MB	121 MI
Biometric Enrollment Host	bioenrollmenthost.exe	Windows	1 (0%)	1 (196)	1	2024-02-20	2024-02-20	NonCategor		12 MB	12.1/1
🞯 Brave Browner	brave.exe	Windows	7 (2%)	6 (4%)	4	2024-02-21	2022-12-20	Commercial	Departmental	877 MB	5.36 GI

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.

Flex	ANALYZER			¢0	Vestern Europe	-
G Home	Sack to Previous Page					
망. Integrations	APP CATALOG & INVENTORY / APP DETAI	LS				
Sentraps	😐 Microsoft PowerPoint					8
Reconcentratives	Product Name Microsoft PowerPoint	Category Commercial	Exe File powerpnt.exe		os Windows	
() Help	Inclosed PowerPoint	Gommercial	,,			
	App Groups		Product Owners			
	Recessary & Productivity	~	۵			
	Versions History					~
	Workspaces History					~
	Users History					~
	Usage History Last 60 Days					~
	Workspaces Without Usage In The Last 3	30 Days				^ .

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

Version History

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

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

Workspaces history

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

- Device Name
- Reported version
- Report date

Users History

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

- Username
- Reported version
- Report date

Usage History Last 60 Days

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

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

Workspaces without usage in the last 30 days

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

- Device Name
- Installation date
- Last detection report

Analyzer / Diagnosis

From 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.

DESKTOP.	^
Q desktop	×
DESKTOP	1
DESKTOP-	
C DESKTOP.	
DESKTOP	
10 DESKTOP-	
DESKTOP-	
DESKTOP	
0 DESKTOP-	
DESKTOP-	-

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

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



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

Timeframe selection

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

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

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

Resource consumption charts

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



The charts show the total resources consumed by the device. If more than one user was using the device during that period, the charts will show the resources consumed by all users. Hovering over any of the charts will display a box with the resource consumption for that specific moment. You can click on any point of any of the charts to see which applications and processes were running at that specific moment; by default, the most recent data for the selected period will be displayed.

Performance Counters

Each counter on the screen includes several display options.

CPU

- % CPU. Total CPU usage on the system, equivalent to what the task manager shows.
- % User Time. Percentage of CPU time used by applications and processes running in user mode.
- % Privileged time. Percentage of CPU time used by the operating system and system services in privileged mode.
- % Processor time. Total CPU time used in all system processes and activities.

RAM

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

GPU

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

Network Latency

• Network Latency. Shows the system latencies.

Disk Usage

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

Applications and Processes Tables

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

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

-20 15:00									
ame	Process Name	Avg CPU	Avg RAM	Avg GPU	Avg Tota	Avg Read	Avg Writ	Max Network Latency	
Configuración	systemsettings.exe	0.0%	0.0%	0.0%					7
Microsoft Calculator	calculatorapp.exe	0.0%	0.0%	0.0%					7
Microsoft Edge	msedge.exe	6.1%	16.1%	3.1%	2890 IOPS	1307 IOPS	1583 IOPS	240 ms	7
Microsoft Office	hxputlook.exe	0.0%	0.0%	0.0%	-	-	-	14 ms	7
Microsoft Outlook	outlook.exe	0.2%	0.8%	0.0%	-	-	-	45 ms	*
Microsoft Teams (w	ms-teams.exe	0.0%	0.3%	0.0%	-	-	-	38 ms	7
Microsoft.MediaPla	microsoft.media.player.exe	0.0%	0.0%	0.0%	-	-	-		*
Visual Studio Code	code.exe	0.1%	2.3% (0.0%	12 IOP5	7 IOPS	5 IOPS	77 ms	7
Windows_DDM_v2.1	ddm.exe	0.0%	0.1%	0.0%	-	-	-	-	×
							1 to 9 a	d19 K € Page1d1 >>)	10

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

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

Analyzer / Carbon footprint analysis

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

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

Web Interface

This dashboard view is divided into three tabs:

- Overview. 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

25.6 / FXXOne Documentation / FXXOne

	ANALYZER			¢ ° 9	
e i s	Overview Printed copies Energy				(About our metrics)
	Carbon Footprint Tips Configure a power-saving policy in all workspaces to enter into sleep mode or hit	bernation when no	t in use for short period of times		
*	Carbon footprint of ordinary activities A travel by an average fossil-fueled car between Madrid and Barcelona (625,9km) equals	to 68 kgCO2e			
	Total carbon footprint in July 2024 18,73 kg CO2e ~ 109,58%	0	Carbon footprint in 2024 21		
	Printed copies carbon footprint in July 2024 2 6,97 kg CO2e × 46,39%	Θ	10 5 8	Narrah Agrad	
	Energy carbon footprint in July 2024 22 11,76 kg CO2e ~ 181,62%	0		🗧 Prentad pages 🛛 🖲 Energy	

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

Data contained in the view (current month):

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

Printed copies

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

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

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

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



- Total printed copies in [current month]. Displays short-term paper usage trends. Helps identify areas of intensive use, as well as opportunities to reduce the number of prints or promote duplex printing.
- Equivalent carbon footprint. Provides a direct idea of the environmental impact of printing activities. It can motivate the adoption of policies to reduce the carbon footprint, such as digitizing documents and implementing paperless initiatives.
- **Top printed copies by printer.** View of printers sorted by the number of prints in the current month.
- **Printed copies in [Current year].** View of the total black and white and color prints made month by month during the current year.
- Average copies per user. Average prints per user in the current month.
- Top printed copies by user. List of users sorted by the number of prints during the current month.

Energy

25.6 / FXXOne Documentation / FXXOne

	ANALYZER					¢ 9	0	
- 10 10	Overview Printed	d copies Energy					Radioactive Material ~	About our metrics
	Carbon footprint of A direct flight MAD-BCI	ordinary activities N equals to 139 kgCO2e						
0†	Total energy radioactiv			0	Radioactive material per day	y in July 2024		•
		aterial per workspace in July 2024		0				
					* 1 2 3 4 5 6 7 1	9 10 11 12 12 14 15 16 17		****
	Top workspaces by upt	time		0	Top workspaces by inactive	time		0
	Q. Search				Q, Search			
	Name	Uptime	Last User		Name	Afk Time	Last User	
		333h Sm 307h 35m				272h 28m 160h 9m		
		214h 25m				156h 57m		

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

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

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

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

Radioactive material

- Total energy radioactive material in [Current month]. Shows the total grams of radioactive material generated during the current month.
- Average radioactive material per workspace in [Current month]. Shows the average radioactive material per workstation in the current month.
- Radioactive material per day in [Current month]. Graph estimating grams of radioactive waste generated in the current month.

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

Analyzer / User experience

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



Basic concepts

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

- Workspace Reliability Index (WRI)
- User sentiment

Workspace Reliability Index (WRI)

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

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

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

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

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

Severity	Penalty
HIGH	0.2
MEDIUM	0.016
LOW	0.008

User surveys

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



Web Interface

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

Global view

The global numbers are offered at the top.

- UXI Average. 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.

USER EXPERIENCE							
UXI Average 3.21		Tendency Negative		8	Total users evaluated 138	Ţ	Total workspaces 233
UXI Average	ා ල UXI Tendency						
5							
4							
3	•	•	•				•
2							
1							
0							
0	JAN 21-28	JAN 28-4	FEB 4:		FEB 11-18	FEI	8 18-25

Two charts are also included:

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

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

Individual view

This view provides the user data under analysis, including:



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

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

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

Analyzer / Workspaces in Analyzer

The 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.

WORKSPACES							
9	⊕ 2 ∞ 6						
Total	Total Domains Operating Sys						
Q Search							
Name	Session Status	Last User	Domain	05	IP	Usage Days	Le
•	 Active 			Windows 11 Pro		43	20
•	Active			Windows 10 Pro		41	20
	 Inactive 		N/A	Windows 10 Pro N		49	20
•	 Inactive 		N/A	Windows 10 Pro		49	20
	 Inactive 		N/A	Windows 10 Enterprise		29	20
	 Inactive 		N/A	Windows 10 Enterprise		31	20
	Inactive		N/A	Windows Server 2016		17	20
	 Inactive 		N/A	Windows 10 Pro		2	20
•	 Inactive 		N/A	Windows 10 Enterpris		1	20
4							+

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



Workspace detail

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

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

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

Sack to Previous Page								
WORKSPACES / WORKSPACE DETAILS								
		() A	Active 🗇 9 🔗 2 🕛 0					
Name	Last User	Last Report	Domain					
DEDICTOR- DE CONCT	A (2008). 2 spatianes	2020-02-27 15:18	ad Recolline contr					
LogonServer	Vendor	Operating System	System Model					
DESCTOR DECEMBER	Dell Inc.	Windows 11 Pro	Latitude 3520					
System SKU	System Type	IP	Processor					
0B21	x64-based PC	192.168.1.99	11th Gen Intel(R) Core(TM) i5-1145G7 @					
			2.60GHz, 8 Logical Processor(s)					
Total Workspace Memory	WRI	RAM Usage	CPU Usage					
8GB	4.5 ★	91.9%	38.16%					
CPU Usage Mhz	IOPS Usage	FlexxAgent Analyzer Version						
2.16GHz	1483	2.10.6						
Diagnose workspace								

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:

- <u>Displays</u>.
- 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 <u>estimate the carbon footprint</u>.

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 <u>App Catalog & Inventory</u>.

The information about installed applications offered by Installed Apps is collected by <u>FlexxAgent Analyzer</u> 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 <u>FlexxAgent Analyzer</u> every 15 seconds and sent to the console every 5 minutes.

Issues in the last 30 days

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

Usage history

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

Analyzer / App Groups

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

Fle								Ļ ⁰	🖗 Maandaraa	00	sata a	$f_{\rm F} \sim {\rm d}$
பி Home	APP GROUPS											
먑. Integrations											Create A	pp Group
Settings												
C FlexxAnalyzer Users			段 CRITICAL	ණි DEPARTM		袋 INSTALLATION	ති LOW USED	袋 NECESSARY	र्छ system			
0		<				MEDIA				>		
Help			6	Apps	53 Apps	20 Apps	0 Арр	30 Apps	7 Apps			
	Critical											
						\searrow						
				4		0						
	Credential Manage credentialuibroker	Microsoft Manage mmc.exe	Microsoft OneNote onenote.exe	Microsoft Window systemsettings.exe	Task Manaį taskmgr.e:							
	Users Cons	uming Apps In	Critical									~
	FlexxAnalyzer 2024											

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

Group Types



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

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

Creating a New Application Group

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

Group Name									
				ß					
+									
Add APP									
ADD APPS									×
Q Search Apps									
	0	icon	icon	icon	icon	icon	٢	٢	Î
1password 1password.exe		Adobe Download I reader_install_setu	AnyDesk anydeskuninst30c	Cisco AnyConnect vpndownloader.ex	Cisco Secure Clien csc_ui.exe	ciscowebexstart.e: ciscowebexstart.e:	Citrix Receiver receiver.exe	Citrix Workspace wfica32.exe	
icon	icon		icon	Ø	٨		A	۵.	
Client Connector zsatray.exe	CrashingApp crashingapp.exe	Credential Manage credentialuibroker	CShelljavaLaunche cshelljavalauncher	DeepLdeepLexe	easeofaccessdialo, easeofaccessdialo,	FlexxNotification flexxnotification.ex	fontview.exe fontview.exe	GNU Image Manip gimp-2.10.exe	
icon		icon		kon	4	0	o	-	
IBM Lotus Notes/E ninotes.exe	installer.exe installer.exe	Lenovo System Up tvsukernel.exe	Logi Options+ Age logioptionsplus_ag	magnify magnify.exe	Microsoft Manage mmc.exe	Microsoft Office Cl officeclicktorun.ex	Microsoft Outlook outlook.exe	Microsoft Paint mspaint.exe	*
								ADD	Ju -

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

Analyzer / App Versions

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

Graphical view

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



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

Table view

Q Search...

		Versions >
App Name	App Executable	Total Versions
Microsoft Edge	msedge.exe	30
Google Chrome	chrome.exe	28
Microsoft Windows System Settings	systemsettings.exe	22
Microsoft Teams (work preview)	ms-teams.exe	17
Citrix Workspace	cdviewer.exe	16
Microsoft Teams	teams.exe	16
Microsoft Word	winword.exe	15
Task Manager	taskmgr.exe	14
Microsoft Edge View	msedgewebview2.exe	14
Microsoft Outlook	outlook.exe	13

1 to 10 of 142 IK K Page 1 of 15 > >I

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

- Application name
- Executable name
- Number of total versions

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

Analyzer / Polls

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

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

Poll Settings

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

List view

Fle×	X AN	ALYZER				Ų ₀	9	-			1 4	
	POLLS	DASHBOARD										
ingrations Settings	٩									CREATE	NEW P	DLL
oAnalyzer Users Help	1	Name	Status	Туре	Start Date	Last Respo	Responses	Av	g Score			
			in progress	Recurrent	2023-03-06 09:	2024-07-12 15:	533	1	4.04	п	/	Ϊ.
			Completed	One shot	2023-06-30 14:	N/A	0	*	0		1	Î
							1	to 2 of 2	ic c	Page 1 of 1	>	Я
	FlexxAn	alyzer 2024										

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

Detail view

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

rle <mark>></mark>	CANALYZER			Ų0	۰		-
	POLLS DASHBOARD / CREATE POLL						
۵	Name						
Settings RecoAnalyzer Users Help	Question Choose an audience Organization Custom Cocurrence One shot Recurrent						
	Recurrence pattern Weekly Monthly						
	Once Year Selet day Time zone * 16/07/2024	Starttime 09:44 (End time		0		
	○ End date: 17/07/2024					CANCEL	
	FlexxAnalyzer 2024						

The configuration options include:

- <u>Name</u>
- <u>Question</u>
- Audience
- Occurrence

Name

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

Question

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

Audience

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

Occurrence

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

- Weekly
- Monthly
- Yearly

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

Poll Execution

Google Chrome	
Recycle Bin 🔤 Floru Analyzer	×
FlexxEmployee UX Experience	
CA: Com ha anat la setmana amb el PC i l'escriptori virtual? EN: How was your experience with your computer and virtual desktop this week?	Jr.
W W W W W	R
Please, click on a star to send your answer to this poll	
1 Snooze	
This question will appear again in one hour	·
Decline to answer No response will be collected for this poll	>
Answer anonymously. Off UN Your answer will be collected but it will not be linked to your username Off	
📫 H 🕐 🗮	

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

Analyzer / Users in Analyzer

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

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

List view

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

lex/	NALYZER		Ų0	• — · · · · · · · · · · · · · · · · · ·	
	G Back to Previous Page				
-	USERS / USER DETAILS				
age adjaar S	☐ 91 _{Apps}				
2					Ø
1.1	Name	Username	Workspace		Profile Size
					21.8 GB
1.1	User Principal Name	Domain			
					33.9 GB
	Department	Email Address			31.9 GB
		Litten Augress			
					21.7 GB
					21.7 GB

User data in the detail view

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

- Total number of applications used by the user.
- Username. Username used for login in the session.
- Name. User's "Display name".
- UPN. User Principal Name.
- Domain. Domain of Entra ID or Active Directory where the device resides.
- Department. Department provided in Active Directory or Entra ID.
- Email Address. User's email address.

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

- Workspace. Device name.
- Profile size. Disk space occupied by the user's profile.

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

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

- Name. Application name.
- Workspace. Device where the application was detected.
- Version. Application version discovered.
- Last report. Date of last report from FlexxAgent.
- App Group. Group to which the application belongs.
- Category. Application category.

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

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

Analyzer / User Groups

Users Groups allows you to create user groups using the data of 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.

FlexANALYZER	¢ <mark>0</mark> 🕈	e Canadica
USERS GROUPS		
C Search		ADD
etimp Sangar Aralgar	MEMBERS	
iters Internet in the second		Ō
No Constantin		Ō
The part of the pa		ō
	1 to 3 of 3 ic < 1	lage1of1 > >l

Detail view

Within the details of a user group, it is possible to remove any user using the trashcanshaped 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.

25.6 / FXXOne Documentation / FXXOne

Fle	ANALYZER Å	-
Constanting	SERS GROUPS / USERS GROUP	ADD
NecoAnalyzer Users () Help		ō
		ō
		ō
		ō
		ō
		õ

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.

Fle	exxible				Change: Ctrl + K My organization Default: Ctrl + D	Organization Admin	
ଜ		Home					
Ð	Operations						
弦	Flows		୲୕	ال ناع	<u>88</u>		
Ē	Reports	Workspaces	Analyzer	Automate	Monitor		
яĜ	Tenants		· ·				
Ŀ	Workspaces	/					
盦	Patch	View more (13)					~ ~
2	Analyzer	Your products					
Ø	Microservices						
ŝ	Settings	Environment 1			Product type ↑↓	Action	

Sidebar menu

It consists of the following sections:

- <u>Home</u>
- <u>Operations</u>
- <u>Flows</u>
- <u>Reports</u>
- <u>Tenants</u>
- <u>Monitor</u>

- <u>Workspaces</u>
- <u>Updates</u>
- <u>Analyzer</u>
- <u>Microservices</u>
- <u>Configuration</u>

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.

= Flexit	ole			My organization	Change: Ctrl + K Default: Ctrl + D	
යි Home						
🔏 Flows		ଭ	<u>88</u>	<u>الج</u>		
🖬 Reports		Analyzer	Monitor	Automate		
മ്പ്പ് Tenants	\sim	·				
① Monitor	~					
🛱 Workspaces	~					~ ~
畠 Patch	\sim					
Analyzer	\sim			Des dust two s	Action	
Microservices	\sim			Product type ↑↓	Action	

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 <u>navigation bar</u>, by pressing Ctrl + K or Cmd + K (on Mac).

F	exxible						Change: Ctrl + K Default: Ctrl + D	Reparingion Admin	
ŵ			Home			Search organization			
Ð	Operations					-			
场	Flows		O	ଭ	Ę	.			
Ē	Reports		Workspaces	Analyzer	کې Automate				
Â	Tenants	\sim				.			
Ŀ	Workspaces	\sim				💄			
盦	Patch	\sim	View more (13)						~ ~
8	Analyzer	\sim	Your products			•			

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
- <u>FlexxAgent version</u>
- <u>My logins</u>
- <u>Settings</u>
- Log off

Operations List

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

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

My logins

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

Settings

The left side of this section shows the user's data: role, organization they belong to, email address, and the creation date of the user on the platform. On the right, account preferences can be managed: set the default organization to manage (if you have access to other organizations, such as tenants or partners), change the language, select the regional setting, and enable the advanced menu.

Trapadate Cong	
My organization	
elect default language	
English	~
elect regional settings	
nable advanced menu	
Access to this system is restricted to authorized personne access/session could be recorded.	el only. Please be informed that your

In this module, a level 1 or 2 technician will have the ability to update FlexxAgent in one or more reporting groups with the version proposals configured by the *Admin* or *Organization Administrator*.

It should be noted that current versions have new features. If a downgrade to an earlier version is made, these will be lost.

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

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 configuration.

Advanced menu

Allows you to expand the Portal side menu by adding shortcuts to specific features of the other modules.

Navigation bar

Allows you to go directly to specific sections and subsections of Portal or change the <u>organization to manage</u>. For example, a user who wants to access the Microservices section can do so efficiently by entering the characters of the word *microservice* in the search box; if the user wants to change the organization, they must type the characters that match the name of the organization they wish to manage, and then press Enter.

Fle	excible	2			Client	Default: Ctrl + D 💙	Organization Admin
俞			Home				
Ð							
			Г		_		Le la
5			Work	<mark>, ∼</mark> micros	>	gent	<u>ි</u> ල Generate magic link
Rê				RESULTS			
\Box						's	
Ē.,			Your products	Microsoft patch policies	Pato	h	
			Environment	🗞 Microsoft Patches	Pate	h e ↑↓	Action
鈲						XXOne	☑ View Detail
2						AXONE	
Ŷ							

Considerations about the navigation bar

- Access it using Ctrl + K (Cmd + K on Mac).
- Allows access to recent navigations. The history will change if the user switches organizations.

- Searches must be conducted in the same language set in the Portal.
- To exit, press Esc.

Tables

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

Top bar

It is composed of the following buttons:

+ Create	😰 Export	🕐 Refresh	
O Search	by term		√ Filter

New

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

Export

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

Reload the table

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

Search by term

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

Filter

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

Full screen



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

Flexcible ⅲ		My organization	(Ctrl + K) 🗸	Organization Admin	
යි Home	Designer				
Operations	+ Create 💼 Export 💍 Refresh				2
² / ₂₆ Flows PREVIEW ² / ₆₆ Tenants ∨	✓ Search by term ✓ Filter				
🗗 Workspaces 🗸 🗸	Name 🏗	Category ↑↓	Library ↑↓	Archived ↑↓ Ac	tions
🛱 Patch 🛛 PREVIEW 🗸	List Installed User Certificates	Certificates	Flexxible Corp	 Unarchived 	
O Microservices ^	Borrar cache Teams	Collaboration	Flexxible Corp	 Unarchived 	
🖾 Enabled	Windows Update - No restart	Updates	Flexxible Corp	 Unarchived 	
Marketplace	Windows update - with reboot ${}^{O\!\overline{N}}$	Updates	Flexxible Corp	 Unarchived 	
Designer	Clear Microsoft Edge Cache (57)	Browsers	Flexxible Corp	 Unarchived 	
🗟 Audit log	Force Synchronization with SCCM $\ ^{C\!P}$	SCCM	Flexxible Corp	 Unarchived 	
	Intune - Enroll Device ፡፡፡፡፡፡፡፡፡፡፡፡፡፡፡፡፡፡፡፡፡፡፡፡፡፡፡፡፡፡፡፡፡፡፡፡	Intune	Flexxible Corp	 Unarchived 	
	< Previous Page 1 v of 1 Next > Showing 1 to 50 of 50 results			Per page:	50 ~

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.

Name 11	Product 1	Policy ↑↓	Creation date $\uparrow\downarrow$	Action	
	FlexxClient		7/25/24	View Detail	Î
			2/28/24	View Detail	
•• ••	FlexxClient		7/23/24	View Detail	
	FlexxClient		8/27/24	View Detail	
	FlexxClient		7/25/24	View Detail	
8• 444	FlexxClient		7/15/24	View Detail	
44 44	FlexxClient		8/13/24	View Detail	
	ElexxClient		7/17/24	12 View Detail	*

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.



→ Per page: 50 →

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

enough for the administrator to attempt to log in to the Portal for the first time to trigger the consent request.



Does this app look suspicious? Report it here



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

Permission	Caption
Directory.Read.All	Read directory data

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. Thus, these users can choose between logging in with a Microsoft Entra ID, Google, or via email and password.

rlexxible°
Welcome
G Continue with Google
Continue with Microsoft
OR CONTINUE WITH EMAIL AND PASSWORD
Email address*
Continue with email
uu miinnilli

Login process

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

- 1. Enable <u>access to email and password authentication</u> for the user. This step must be done by an *Organization Administrator*.
- 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 <u>authentication app</u>. The first time the user attempts to log in with email and password, the platform will prompt them to do so.
- 5. Log in.

Access to email and password authentication

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

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.

🖓 тір

You can find more information on how to create a user in <u>Users</u>.

	Flexxible			Name * Please enter text here
	t Cont 1 Martine	🖷 Espertusers 🕤 Refrash	Surname * Please enter text here	
	Planting and			E-mail *
				Please enter text here
	Automatic S	E mail 1 Begarine	ee ()	User role *
				Select user role
				Language *
		again and the state of the		Select language
				Department
period fronts	Marrie Carlle			Please enter text here
	Real Processing Streeting			Enable email/password login

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	٣	Department 👻		Role	•	Language 👻	Email login enabled 🔻
Add/Update	contraction of the second seco	And in case of the second second	A AD IN COMPANY AND ADDRESS		and the second data in the secon	Po	rtal Admin		en	Y
Add/Update	and share	a given much being	And the other designs in the local division of the local divisione			Cu	stom Admin Role 2		en	N
Add/Update	Canadian Providence	- and a second second second	Congent and in succession of the			Po	rtal Admin		en	Y
Add/Update	Contraction in the second	- and the second second	strange and supply and			Cu	stom Admin Role 4		en	N
Add/Update	All and a second	and entry (resulting)	species with the same of the			Cu	stom Admin Role 5		es	N
Add/Update	(Marriel)	(oppose)	NAMES OF TAXABLE PARTY.			Ma	ajaras		en	N
Add/Update	realizes.	survey of the local division in which the	successive spectrum statements and the			Cu	stom Admin Role 6		es	N
Add/Update	Contraction of Contra	Stationer, Consulation	comptoner of the section - carries			Cu	stom Role 7		es	N
Add/Update	Designation of the	(see	second			Ma	ajaras		en	Y
Add/Update	Contraction of the local division of the loc	Lines-	NAME OF TAXABLE PARTY.			Cu	stom Admin Role 9		es	N
Add/Update	Ministry	and the second s	Contraction of the local division of the loc			Ma	ajaras		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.

Import users		×						
Select file	Selected file: No file selected)						
Summary								

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.

Flexible							📸 My organ	ization Defau	lt: Ctrl + D 🗸	nization Admin	
聞 Patch ^図 Analyzer	~ ~	Fle	exxible - Us	ers							
 Microservices Settings 	× ^		te ↑ Import users		E-mail login actions \checkmark Enable e-mail login Disable e-mail login	🕐 Refresh					2
Information Users			Full name ↑↓	E-mail ↑↓	Department ↑↓	Role ↑↓	E-mail login ↑↓	Created by $\uparrow\downarrow$	Updated by ↑↓	Action	
Roles		0	Name Canality			Transie .	Disabled			🖸 View Detail	î
Products		0	Alla Contern (Per-	againtee at the set		Contare Admin. No	Disabled			🛛 View Detail	
Modules		0	Alart Deregan	damagan bilan.		inspector.	Disabled			🛛 View Detail	
Integrations			Harts Carlls		Local Solution and Control of Con	Custom Role 21	Disabled			🛛 View Detail	
Reporting groups			tes (gene Seat.		100	Portal Admin	Enabled			View Detail	
						Role QA	Disabled		Carlina Martine (C.)	🖸 View Detail	
			vious Page 1	∽ of 1 Next >	Showing 1 to 39 of	39 results				Per page: 50	~

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.
```

Flexcible						
ຝ Home						
Operations	ቘ Flex)	cible - Users				
🖶 Reports	+ Create	🕆 Import users 🔞 Expo	ort users 🔗 E-mail login action			
绪 Flows	Search I	wtorm	✓ Resend password ✓ Enable e-mail log			
^β ≜ Tenants	V Jeardin	y term	V Chable e-mail log X Disable e-mail log			
① Monitor	V Ful	l name ↑↓	E-mail †↓	Department ↑↓	Role †↓	E-mail login ↑↓
🔛 Workspaces	~	and the second second			Custom Admin Role 6	 Disabled
û Patch	~	1000				Disabled
Analyzer	· · ·				Custom Admin Role 5	Disabled
Microservices	~					Disabled
Settings	^				Custom Role 21	Disabled
Information	•				Portal Admin	Enabled
Billing					Role QA	 Disabled
Users	200				Custom Admin Role 2	• Disabled



() INFO

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

Authentication security settings

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

User-level authentication security settings

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

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

Authentication security settings Manage your account security settings, including two-factor authentication and password.
Two-Factor Authentication
Two-factor authentication adds an extra layer of security to your account by requiring more than just a password to sign in.
Authentication Methods
Authenticator app • Active Last used Apr 24, 2025, 4:57 PM Added on Apr 24, 2025
Recovery code • Active Not used yet Added on Apr 24, 2025
Email verification • Active Not used yet Added on Apr 24, 2025
Reset Two-Factor Authentication
If you've lost access to your two-factor authentication devices, you'll need to reset it.
${\mathscr S}^{\sigma}$ Reset Two-Factor Authentication
Last modified: Apr 24, 2025, 4:57 PM
Password
Ensure your account stays secure by regularly updating your password.
명 Resend reset password email
Password last changed: Apr 16, 2025, 1:17 PM
Last login: Apr 24, 2025, 4:53 PM
Last IP address:

Two-factor authentication

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

Authentication Methods

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

- Authentication app
- <u>Recovery code</u>
- 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. Next, 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.

Flexcible°	
Secure Your Account	
Scan the QR Code below using your preferred authenticator app and then enter the provided one- time code below.	
Trouble Scanning?	MILL
THEN	1111
Enter your one-time code*	
Continue	11111
	((0))

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.

rlexxible°
Almost There!
Copy this recovery code and keep it somewhere safe. You'll need it if you ever need to log in without your device.
Copy code
I have safely recorded this code
Continue

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

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

() INFO

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

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

Recovery code

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

authentication app is downloaded. The *Recovery Code* option allows regenerating this code if it is lost, to verify the user's identity when they wish to log in.

Email verification

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

<	Select a method to verify your identity				
	Google Authenticator or similar	S			
	🖂 Email	>			
	Recovery code	>			

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

Reset two-factor authentication

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

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

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

Password

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

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

Authentication security settings at the organization level

An *Organization Administrator* can enable or disable the option to log in 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.

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. Disable email/password authentication

Contemporary conte	
 Export Refresh Search by term 	
Name î↓	ੁ : Email/Password Login ੀ↓ ੁ :

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 <u>Authentication security</u> <u>settings</u> for that specific user, which includes <u>Two-factor authentication</u> and <u>Password</u>.

		User authentication details
		IR
🖲 lagest 🔘 Balanti		
		Microsoft Entra ID
	And S. Y. I. Brathanerings S. Y. I. Approx	Job title Phone Last login 6 may 2025, 18:51
		Login count Last IP address
		an Provincest
		📉 Email and password
		Last login Login count Last IP address 6 may 2025, 15:56
A CONTRACTOR OF A	The Real Procession	,

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.

= rlexxib	ple				My organizat	tion	efault: Ctrl + D 🗸	ion Admin
Operations	Ŕ	nstalled apps						
ය Flows		😰 Export 🕐 Refresh						2
ද Tenants	~	O Search by term	▽ Filter					
 Monitor Workspaces 	× ×	Product name ᡝ	Publisher ᡝ	Installed at (UTC) $\uparrow \downarrow$	Last report (UTC) $\uparrow \downarrow$	os †↓	No. of installations $ \mathbb{O} \downarrow $	View detail
箇 Patch	\sim	FlexxAgent	Flexxible	8/21/23, 12:00:00 AM	5/12/25, 11:38:23 AM	Windows	179	🖸 View Detail
Analyzer	~	Microsoft Edge	Microsoft Corporation	5/9/25, 12:00:00 AM	5/12/25, 11:38:23 AM	Windows	178	View Detail
Installed apps		Microsoft OneDrive	Microsoft Corporation	5/8/25, 9:08:29 AM	5/12/25, 11:38:23 AM	Windows	164	☑ View Detail
Licenses		CrowdStrike Windows Sensor	CrowdStrike, Inc.	4/29/25, 12:00:00 AM	5/12/25, 11:38:23 AM	Windows	162	View Detail
SAM		Microsoft Update Health Tools	Microsoft Corporation	5/22/23, 12:00:00 AM	5/12/25, 11:38:23 AM	Windows	152	View Detail
	*	Microsoft Intune Management Extension	Microsoft Corporation	4/30/25. 12:00:00 AM	5/12/25. 11:38:23 AM	Windows	140	☑ View Detail
		< Previous Page 1 v of 37	Next > Showing 1	to 50 of 1803 results			Ρ	er page: 50 v

This information can also be accessed from the <u>Workspaces</u> section of the <u>Analyzer</u> module.
Portal / Analyzer / Installed apps

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

\equiv Flexcible				My organiza	tion	efault: Ctrl + D 🗸	tion Admin
	۶ Installed apps						
ය Flows 鲬 Reports	🗈 Export 🕐 Refresh						2
ස් Tenants 🗸	Search by term	∀ Filter					
MonitorMorkspaces	Product name 🏌	Publisher ᡝ	Installed at (UTC) ᡝ	Last report (UTC) ᡝ	OS ↑↓	No. of installations $ \mathbb{O} \downarrow $	View detail
🗐 Patch 🗸 🗸	FlexxAgent	Flexxible	8/21/23, 12:00:00 AM	5/12/25, 11:38:23 AM	Windows	179	View Detail
🖻 Analyzer 🔨 🔨	Microsoft Edge	Microsoft Corporation	5/9/25, 12:00:00 AM	5/12/25, 11:38:23 AM	Windows	178	View Detail
Installed apps	Microsoft OneDrive	Microsoft Corporation	5/8/25, 9:08:29 AM	5/12/25, 11:38:23 AM	Windows	164	View Detail
Licenses	CrowdStrike Windows Sensor	CrowdStrike, Inc.	4/29/25, 12:00:00 AM	5/12/25, 11:38:23 AM	Windows	162	View Detail
SAM	Microsoft Update Health Tools	Microsoft Corporation	5/22/23, 12:00:00 AM	5/12/25, 11:38:23 AM	Windows	152	View Detail
	Microsoft Intune Management Extensi	ion Microsoft Corporation	4/30/25. 12:00:00 AM	5/12/25. 11:38:23 AM	Windows	140	☑ View Detail
	< Previous Page 1 v or	f 37 Next > Showing 1	to 50 of 1803 results			Ρ	er page: 50 V

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.

() 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:

- <u>Overview</u>
- <u>Versions</u>
- <u>Workspaces</u>
- Installation history
- <u>Report history</u>

() 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.

Fle	exxible	2 111			My organization	Change: Ctrl + K Default: Ctrl + D	User	
Ð	Home Operations		Installed apps > Microsoft Visual Studio Code Microsoft Visual Studio Code					
	Workspaces	PREVIEW	Overview Versions Workspaces					
£	Analyzer	PREVIEW ~	Product name Microsoft Visual Studio Code Publisher	OS Windows		Discovered at 12/12/24		
Ŷ	stalled apps Microservices	PREVIEW V	Microsoft Corporation			Last report 12/19/24		
ŝ	Settings	~			Edit			
							[⋧	

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.

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.

4	Flows	۶	Installed app	a > Microsof	t Visual Studio Co	de						
Ē	Reports		Micros	oft Visu	al Studio	Code						
Å	Tenants		Overview	Versions	Workspaces	Installations history	Report histor	y				
	Monitor											
Þ	Workspaces		Аррі	nstallat	ions histo	ory (max. 120 c	lays)					
盆	Patch		i Da	ly installation	data is computed	d at 2:30 AM						
2	Analyzer		8									
Ir	nstalled apps			1								
Li	icenses		lations									
S	AM		of Instal									
Ø	Microservices		Number of Installations									
			Z 2									
			0									
				-484 ^{15,2025}	⁵ 6-	N162225 Marth	2015	May 18,2025	181 ^{19.2025}	18420,2025	184 ^{27,2025}	18422,2025

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.

() 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.

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 <u>list view</u>. Next, a form will open requesting to fill in the following fields:

Create new license		×
Name *		
Name		
License type *		
Select a license type		~
Purchased licenses		
Purchased licenses		
License cost		
License cost		€
Notes		
Notes		
		ls
Expires at		
Select date		
	imes Cancelar	+ Nuevo

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

License list

	Flexit	ole				1	My organization	Default: Ctrl + D	Organization Admin	
ሴ	Home	众								
Ð	Operations		Licenses							
经	Flows Previe	EW	🕂 Create 📵 Export (🕐 Refresh						2
■	Reports		Search by term	∑ Filter						
Rea	Tenants	\sim								
	Monitor	\sim	Name ᡝ	License type $\uparrow \downarrow$	Purchased license: $\uparrow \downarrow$	Usage (current month $\uparrow\downarrow$	Usage (last month) $\uparrow\downarrow$	Expires at $\uparrow\downarrow$	Action	
Đ	Workspaces	\sim	Licencia OB	Workspace installation license	24	0	0	10/31/24	View Detail	
龠	Patch	\sim	Microsoft Office	Workspace installation license	125	112	132	2/3/25	View Detail	
2	Analyzer	~	Microsoft Project	Workspace installation license	6	0	0	-	☑ View Detail	
Ir	stalled apps		Microsoft Visio	Workspace installation license	7	0	0	-	View Detail	
U			Notepad++	Workspace installation license	0	99	123	-	View Detail	
		*	Outlook	User-Specific execution license	50	50	56		☑ View Detail	

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
- <u>Usage history</u>

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

• <u>Running processes</u>

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.

= rlexxible		My organization	Default: Ctrl + D V Organization Admin
🖬 Reports	Licenses > Microsoft Office		
🖉 Tenants 🗸 🗸	Microsoft Office		
🛈 Monitor 🗸 🗸	Details Installed apps Usage history Workspace usage Purchase	d licenses history	
🛱 Workspaces 🗸 🗸			2
🛍 Patch 🗸 🗸	+ Link 🟚 Export 💍 Refresh		2
🖻 Analyzer 🔨 🔨	Search by term		
Installed apps	Name ↑↓ Publisher ↑↓	OS ↑↓ No. of installations	↑↓ View detail
Licenses	Aplicaciones de Microsoft 365 pa Microsoft Corporation	Windows 83	🔩 Unlink
SAM	Microsoft 365 Apps for business Microsoft Corporation	Windows 45	🗞 Unlink
🏵 Microservices 🗸 🗸	Aplicaciones de Microsoft 365 pa Microsoft Corporation	Windows 12	🗞 Unlink
Settings	Microsoft 365 Apps for business Microsoft Corporation	Windows 17	😪 Unlink

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

= rlexxi	ble _						My o	rganization	Default:	Ctrl + D 🗸	Organization	Admin
🖬 Reports	Ŕ	Details Installed apps	Usage history	Workspace usage	Purchased license	s history						
ස් Tenants	\sim											
	\sim	Licenses used	in the past	12 months								
🛱 Workspaces	\sim	150										
箇 Patch	\sim											
🖻 Analyzer	^	125										
Installed apps		100			_/					-	-	-
		75			_/				_			_
SAM		50										
Microservices	\sim	10										
慾 Settings	~	25			/							
		0 Jun 2024	Jul 2024 Au	ıg 2024 Sep 2024	Oct 2024	Nov 2024	Dec 2024	Jan 2025	Feb 2025	Mar 2025	Apr 2025	May 2025

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

= rlexcibl	2	My organization	Default: Ctrl + D V
🖬 Reports	お Licenses > Outlook		
ജ്ജ് Tenants	Outlook		
T Monitor	Details Installed apps Running processes Usage history User usage Purchased li	censes history	
🖾 Workspaces	+ Link 😧 Export 🕐 Refresh		
Analyzer	Search by term Y Filter		
Installed apps	Name †↓ Exe file ↑↓	Operating system ↑↓	Actions
	Microsoft Office hxoutlook.exe	Microsoft Windows 11 Pro 24H2	😪 Unlink
SAM	Microsoft Office hxoutlook.exe		😪 Unlink
	Microsoft Office HxOutlook.exe	Microsoft Windows 11 Pro 23H2	😪 Unlink
Settings	Microsoft Outlook outlook.exe	Nicrosoft Windows 10 Pro 22H2	😪 Unlink
	Microsoft Outlook outlook.exe	Nicrosoft Windows 11 Pro 24H2	😪 Unlink

Running Processes

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

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

Portal / Analyzer / SAM

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:

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

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

- The total monthly cost of the license
- The potential savings that can be applied to the license, according to its usage in previous periods.
- The total number of licenses purchased, segmented by licenses in use and inactive licenses.

Portal / Monitor in Portal

Monitor is the alerts and monitoring section of Portal. It consists of two sections: <u>Active</u> <u>alerts</u> and <u>Alert settings</u>. 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.

∝ible _				-	lient	Change: Ctrl + K Default: Ctrl + D	
ame		Active Alerts					
perations	+	Active Alerts					
ws							
ports	👩 Export 🕚 Refres	h					
nants 🗸 🗸	Search by term	∀ Filter					
onitor 🔨	Workspace 1	: Severity 1 1	i Alert name 14 i i	Information 2 1	Alert start 11	: Date notified 14	Element
e alerts	10000	Critical	Duración del arranque	Boot duration 149 seconds	2/19/25, 8:01:40 AM	2/19/25, 8:01:40 AM	Device
Settings	(Malline)	O Critical	Porcentaje bajo de espaci	Drive: C: Free space: 14 G	2/15/25, 0:51:28 PM	2/15/25, 6:51:28 PM	Device:
orkspaces 🗸 🗸	10000	Critical	Porcentaje bajo de especi	Drive: D: Free space: 5 GB	2/16/25, 6:01:34 PM	2/16/25, 6:01:35 PM	Devices
tch 🗸	10000	() Critical	Porcentaje bajo de espaci	Drive: D: Free space: 11 G	2/16/25, 7:41:01 PM	2/16/25, 7:41:01 PM	Device:
alyzer Reiniar 🗸	104404	Critical	Duración del arranque	Boot duration 125 seconds	2/19/25, 4:37:00 PM	2/19/25, 4:37:01 PM	Device:
croservices 🗸	10000000000	Critical	Porcentaje bajo de espaci	Drive: D: Free space: 1 GB	2/17/25, 8:25:04 PM	2/17/25, 8:25:04 PM	Device:
ttings 🗸 🗸	10000	() Critical	Porcentaje bajo de espaci	Drive: G: Free space: 0 GB	2/18/25, 9:13:02 AM	2/18/25, 9:13:02 AM	Device:
	1000000000	Critical	Porcentaje bajo de espaci	Drive: E: Free space: 112	2/18/25, 5:59:01 PM	2/18/25, 5:59:02 PM	Device:
	(managements)	() Critical	Porcentaje bajo de espaci	Drive: D: Free space: 1 GB	2/18/25, 6:41:07 PM	2/18/25, 6:41:07 PM	Device: III
	10000	Critical	Duración del arranque	Boot duration 242 seconds	2/19/25, 4:33:51 PM	2/19/25, 4:33:52 PM	Device:
		Critical	Duración del arranque	Boot duration 188 seconds	2/19/25, 4:08:35 PM	2/19/25, 4:08:35 PM	Device:
	10000	() Critical	Porcentaje bajo de espaci	Drive: D: Free space: 84 G	2/19/25, 5:12:45 PM	2/19/25, 5:12:45 PM	Device:
	10000400	Critical	Duración del arranque	Boot duration 274 seconds	2/19/25, 5:23:20 PM	2/19/25, 5:23:21 PM	Device:
	Contraction of the local division of the loc	Critical	Porcentaje bajo de espaci	Drive: D: Free space: 14 G	2/19/25, 9:04:50 AM	2/19/25, 9:04:50 AM	Device:

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.

ome 💄	Act	ive Alerts					
perations							
ows	oort 🕐 Refresh						
eports	on Unenesn	_					
enants 🗸 🖉	arch by term	Titer					
	kspace 14 💠 🕴	Severity 1 1 :	Alert name 11 💠	Information 2 1 :	Alert start 1	: Date notified 14	Element
e alerts	-	Critical	Duración del arrangue	Boot duration 149 seconds	2/19/25, 8:01:40 AM	2/19/25, 8:01:40 AM	Device
s Settings	Erec.	() Critical	Porcentaje bajo de espaci	Drive: C: Free space: 14 G	2/15/25, 6:51:28 PM	2/15/25, 6:51:28 PM	Device:
forkspaces 🗸	ninter.	Critical	Porcentaje bajo de espaci	Drive: D: Free space: 5 GB	2/16/25, 6:01:34 PM	2/16/25, 6:01:35 PM	Device:
atch 🖌		() Critical	Porcentaje bajo de espaci	Drive: D: Free space: 11 G	2/16/25, 7:41:01 PM	2/16/25, 7:41:01 PM	Device:
nalyzer insonow 🗸	1000	Critical	Duración del arranque	Boot duration 125 seconds	2/19/25, 4:37:00 PM	2/19/25, 4:37:01 PM	Device:
icroservices 🗸		Critical	Porcentaje bajo de espaci	Drive: D: Free space: 1 GB	2/17/25, 8:25:04 PM	2/17/25, 8:25:04 PM	Device:
ettings 🗸 👘	and the second se	() Critical	Porcentaje bajo de espaci	Drive: G: Free space: 0 GB	2/18/25, 9:13:02 AM	2/18/25, 9:13:02 AM	Device:
	and the second se	() Critical	Porcentaje bajo de espaci	Drive: E: Free space: 112	2/18/25, 5:59:01 PM	2/18/25, 5:59:02 PM	Device:
	and the second se	Critical	Porcentaje bajo de espaci	Drive: D: Free space: 1 GB	2/18/25, 6:41:07 PM	2/18/25, 6:41:07 PM	Device:
	-	O Critical	Duración del arranque	Boot duration 242 seconds	2/19/25, 4:33:51 PM	2/19/25, 4:33:52 PM	Device:
	100714	O Critical	Duración del arranque	Boot duration 188 seconds	2/19/25, 4:08:35 PM	2/19/25, 4:08:35 PM	Device:
		() Critical	Porcentaje bajo de espaci	Drive: D: Free space: 84 G	2/19/25, 5:12:45 PM	2/19/25, 5:12:45 PM	Device:
		O Critical	Duración del arranque	Boot duration 274 seconds	2/19/25, 5:23:20 PM	2/19/25, 5:23:21 PM	Device:
		Critical	Porcentaje bajo de espaci	Drive: D: Free space: 14 G	2/19/25, 9:04:50 AM	2/19/25, 9:04:50 AM	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 <u>here</u>.
- Alert name. Name assigned to the alert.

• Category. Name of the category the alert belongs to. The categories can be checked <u>here</u>.

() INFO

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

Alert detail view

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



Portal / Monitor / Alert Configuration

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.

lexcible					My organization	Change: Ctrl + K Default: Ctrl + D	Admin
ය Home	Í		C 443				
Operations	- 1	器 Flexxible - Alerts	s Settings				
缘 Flows	- 1						
Reports	- 1	+ Create 🔞 Export 🖒 Refresh	1				
🖁 Tenants	~	Search by term	Category: Any	√ Filter			
D Monitor	^	Name 1 :	Severity 1↓	: Category 1	: î↓Threshold	Threshold unit 1	: i îl Authorized time.
Active alerts		Boot duration	Oritical	Performance	90	seconds	
Alerts Settings		Critical event log	O Critical	Event Logs	1		
Workspaces	×	FlexxAgent not reporting	📥 Warning	FlexxAgent	0		
Patch	× •	High CPU usage for Workspace	📥 Warning	Performance	80	%	
Analyzer	×.	High RAM usage for Workspa	📥 Warning	Performance	90	%	
		High User input delay	📥 Warning	Performance	350	miliseconds	
		K < Page1of1 > >	1 to 20 of 20 results				Page Size: 50 🔻

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

Create a new alert setting

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

Create Alert settings		\times
Name *		
Enter name		
Description		
Enter description		
Litter description		
		li
Severity *		
Warning		\sim
Category *		
Select category		~)
D		
Repeat every (minutes) *		
0		
Threshold *	Threshold unit *	
720	Minutes	\sim
Mail list		
Enter mail list		
	imes Cancel	+ Create

The form requests the following information:

• Name. Name of the alert.

- Description. Brief explanation of the meaning of the alert.
- Severity. Allows you to choose the severity level of the alert. Severity levels can be consulted <u>here</u>.
- **Category.** Allows you to choose the category the alert corresponds to. The categories can be consulted <u>here</u>.
- **Repeat every (minutes).** Time that will pass before sending a new alert if the event that triggers it is not resolved.
- Threshold. Numerical value that defines the condition to trigger an alert.
- Threshold unit. Unit associated with the threshold (time, percentage, or megabytes).
- Mail recipient list. Email addresses of users who will receive an alert notification (separated by commas).
- Alert message. Alert notification message that recipients will receive.
- Event ID. Number that identifies an event in the event log. An alert will be issued when an event with that ID is generated.
- Search text. Text string that will trigger an alert when it appears in the device's event log.
- Source. Part of the system where the event that generates the alert occurs.

Alert Severity

There are three levels of severity:

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

Alert categories

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

• Connectivity

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

Detail view

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

	= Alerts Settings $>$	Multiple	e errors in event log Er	nabled			
~	 Overview 		Disable Edit Delete				
	Overview						
	Notifications		Overview				
	Active Alerts	0	Overview				
	Microservices	0	Name	Description	Category	Severity	Threshold
	Mailing History	0	Multiple errors in event log	The system reported many event lo	Event Logs	Warning	50
			Authorized time (minutes)	Repeat every (minutes)			
			60	0			

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

() INFO

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

Edit alert settings

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

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

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

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

Sidebar menu

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

Overview

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

Active alerts

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

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

Microservices

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

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

Link Microservice	>
Microservice	
Select a microservice	\sim
Order *	
1	

Send history

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

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

Portal / 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 <u>Jobs</u> 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.

Flexcible III		My organization Admin
ය Home	Operations	
Operations		Last 30 days V (Jul 9, 2024 (iii) (Aug 8, 2024 (iii)
56 Flows preview		
கீ Tenants 🗸 🗸	Operation Aggregates By Types	Total Operations
🗈 Workspaces 🗸 🗸	1000	1151
🛱 Patch 🛛 🛤 🖌 🗸		1101
Microservices PERVIEW	800	Failed
© Settings ∨	600	Warning
		Success
	200	End User Self Service
		ੇ ਹੋ ਦੇ ਹੋ ਹੈ ਹੈ ਦੀ ਦੀ ਦੀ ਦੀ ਦੀ ਦੀ ਦੀ ਦੀ ਸਿਆ Au

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.

• 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.

Fle	exxible					(My organization	(Ctrl + K)	Organization Admin	
۵	Home									
₽	Operations									
缗	Flows (PREVIEW								
А	Tenants		😥 Export 🕐 Refresh							1
Ð	Workspaces		Search by term	√ Filter						
自	Patch (PREVIEW 🗸								
¢	Microservices		Name †↓	Туре †↓	Status †↓	Module †↓	Started At †↓	Ended At \downarrow	User FQDN †↓	
0	Settings		Jines.	Automated Support Operation	Success	FlexxWorkspaces	10/26/24, 2:02:45 AI	10/26/24, 2:02:45 AI	Inside Constitute	
			THEFT	Automated Support Operation	Success	FlexxWorkspaces	10/25/24, 2:01:34 AM	10/25/24, 2:01:34 AM	Contract Constants	
			100m	Automated Support Operation	Success	FlexxWorkspaces	10/19/24, 2:02:44 AM	10/19/24, 2:02:44 AM	Transform - Longitude -	
			None:	Automated Support Operation	Success	FlexxWorkspaces	10/18/24, 10:36:18 AJ	10/18/24, 10:36:18 AI	Contract Contractory	
			Tremadiaties:	Automated Support Operation	Success	FlexxWorkspaces	10/15/24, 11:02:44 At	10/15/24, 11:02:44 At		
			< Previous Page 1	of 1 Next > Showing 1 to 5	5 of 5 results				Per page: 50	~

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

Portal / Flows

This feature allows creating automation flows to detect specific situations on the devices. By evaluating certain conditions, the system determines whether actions should be executed based on the result obtained.

Fle	عكمناهاه	2 🔢					My organization	Change: Ctrl + K Default: Ctrl + D	Organization Admin	0
ଜ	Home		i in the second s	- Flows						
Ð	Operations		•	- FIOWS						
扬	Flows	PREVIEW	+ Create 🏚 Export 🤇) Refresh						1
	Reports	PREVEW	Search by term	Y Filter						
AL.	Tenants									
Ø	Monitor		Name 11	Description 1	Туре 🕄	Detection only 11	Cooldown 13	Enabled 11	Action	
Ð	Workspaces				Workspace	Yes	5 minutes	Enabled	View Detail	
ß	Patch	PREVIEW 🗸	10000-0010-0		Session	Yes	1 hour	Enabled	View Detail	
Ø	Analyzar	PREVIEW 🗸	100.000	the second second	Session	No	42 minutes	Disabled	View Detail	
ø	Microservices	PREVIEW 🗸	10000		Workspace	Yes	25 minutes	Enabled	View Detail	
0	Settings		-		Workspace	Yes	30 minutes	Disabled	View Detail	
					Workspace	No	10 minutes	Disabled	View Detail	
			committee (Workspace	Yes	1 minute	Enabled	🖸 View Detail	
			Second Contract		Workspace	Yes	1 hour	Enabled	View Detail	
			< Previous Page 1	✓ of 1 Next >	Showing 1 to 8 of 8 results				Per page: 60	~

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

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

- Name. Name of the flow.
- Description. Purpose of the flow.
- **Type.** The 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. Evaluates conditions as a "sampling" method. Detects those devices where the conditions are met but does not execute the microservice defined in the

flow.

- **Reusability time.** Marks the minimum time that must pass, once the evaluated condition is met, for the evaluation to be executed again.
- Enabled. Indicates if the flow is *Enabled* or *Disabled*.
- Action. Contains the See details button, which allows customizing the flow's behavior through the following options: <u>Overview</u>, <u>Destination</u>, <u>Flow</u>, and <u>Notification</u>.

() INFO

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

Overview

Fl	exxible	2 111			My organization	Change: Ctrl + K Default: Ctrl + D	Organization Admin	
	Home Operations		Elows >					
		PREVIEW	Configure corporate MS has	ns background				Disable
	Reports Tenants	PREVIEW	Overview Target Flow Notification					
Ø	Monitor		Description			Status • Enabled		
	Workspaces Patch	PREVIEW V	Type Session	Version 18		Created at 10/30/24, 6:23:26 PM		
		PREVIEW 🗸	Cooldown 1 hour	Detection only Yes		L3 10/30/24, 6:23:26 PM		
	Microservices Settings			100	Edit	Updated at 11/6/24, 5:01:28 PM		

Stores general information of the flow.

- Description. Purpose of the flow.
- **Type.** The 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.

- Version. Version number of the flow. Every time it is edited, the counter increments by
 1.
- **Reusability time.** Marks the minimum time that must pass, once the evaluated condition is met, for the evaluation to be executed again.
- **Detection only.** Evaluates conditions as a "sampling" method. Detects those devices where the conditions are met but does not execute the microservice defined in the flow.
- Status. Indicates if the flow is enabled or disabled.
- Created on. Date the flow was created.
- Update date. Date the flow was updated.

Edit and delete a flow

Fle	exxible	2 11			My organization	Change: Ctrl+K Default: Ctrl+D	Organization Admin	
ක	Home		Edit flow					
₽	Operations		Name (english) *					
猛	Flows	PREVIEW	(Sh	ow languages
	Reports	PREVEW	Description (english) *					
si a	Tenants						Sh	ow languages
Ø	Monitor		Type * Session		Cooldown *			1h
₽	Workspaces			R				
ė	Patch	PREVIEW V	C Detection only	<i>u</i> 2				
Ø	Analyzer	PREVIEW V						
ø	Microservices	PREVIEW 🗸				1 Delete	e X Cancel	Save
۲	Settings	~						

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

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

Target

Fl	exxible	2 111		My organization	Change: Ctrl + K Default: Ctrl + D	Ornanization Admin
ŵ	Home		Firme >			
Ð	Operations		Conference concerning ME Transa Incidence and			Disable
络	Flows	PREVIEW	Considers reduced and press resultance			
-	Reports	PREVIEW	Overview Target - Flow Notification			
Æ	Tenants					
Φ	Monitor					X Cancel
Ð	Workspaces		Apply to * Workspace groups			
Ê	Patch	preview 🗸	Workspace groups *			
2	Analyzer	PREVIEW 🗸	Intune Devices			
¢	Microservices	PREVIEW 🗸				
8	Settings					

This setting defines the device groups on which the flow will be executed. It supports the following configuration options:

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

Flow

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

=le	exxible	2 11																								Ĩ	ì ,	ly o	rgan	izat	ion		(0	tri -	K)	×	Or	gar	iza	tio	n A	dmi	n		
ŵ	Home		Over	view	Targ	et	Flo	w	No	tific	atio	1																																	
Ð	Operations																																												
£		PREVIEW																																									Ed	fit	
8	Tenants																																												
Þ	Workspaces																																												
î	Patch	PREVIEW V														1	F		Exi				fa	pro	ce	ss	in																		
ð	Microservices														:			·	pro	ogn	ess	3	-																						
8	Settings														Ľ								Eq	ual		ann ,	ome	.ex	e 																
																						:																							
																		7	Up	da	te (God	ogle	e C	hro	me	9																		
															I.	-		_																											

Flow conditions

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

Existence of an ongoing process

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

Detected Windows event log record identifier

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

Events are identified by the format:

<logName>:<Provider>:<id>

Example:

System:Microsoft-Windows-Winlogon:7001

Where:

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

System Numbe	er of events: 45,433						
Filtered: Log:	System; Source: Micro	soft-Windows-Winlogor	n. Number of events: 18				
Level		Date and Time		Source		Event ID	Task Category
Information		6/26/2025 7:37:15 AM		Winlogon		7001	(1101)
Į –							
Event /001, Winlog	jon						
General Details							
General Details							
 Friendly View 	v 🔹 XML View						
- <syst< th=""><th>em></th><th>hemas.microsoft.</th><th>com/win/2004/08/</th><th>events/eve</th><th>ent"></th><th></th><th></th></syst<>	em>	hemas.microsoft.	com/win/2004/08/	events/eve	ent">		
	entito>7001 <td></td> <td>and got to b</td> <td></td> <td></td> <td></td> <td></td>		and got to b				
	rsion>0						
	vel>4						
	sk>1101 code>0						
		> 000000000000 Ке</td <td>vwords</td> <td></td> <td></td> <td></td> <td></td>	vwords				
			T05:37:15.9386301	Z" />			
		9975 <td>ID></td> <td></td> <td></td> <td></td> <td></td>	ID>				
	rrelation />		1406001 /				
	annel> System <td>="17436" ThreadID</td> <td>=.15695. /></td> <td></td> <td></td> <td></td> <td></td>	="17436" ThreadID	=.15695. />				
	mputer>	/Computer	>				
	curity UserID=						
<td>tem></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>	tem>						
- <even< td=""><td></td><td></td><td></td><td></td><td></td><td></td><td></td></even<>							
	ta Name= 'TSId '>						
	ta Name= 'UserSid ntData>						
<td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>							
Ar vent	-						

Operating system version

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

Operating system language

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

Operating system disk free space percentage

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

Cron Match

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

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

The form allows defining a *Recurrence Pattern* with 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.

Contraction Contraction	Cron Match	×
	Check every *	<u> </u>
		between 08:00 AM and 07:59 PM, only on Wednesday, Thursday, and Friday
Coun March Kerry 25 minutes, between 0000 AM an.	Recurrence pattern Daily Neekly Monthly Interval Custom cron	Run every 25 minute(s) Run all day Run all day Run in interval of hours From To 8 19 hour(s) On the Monday Tuesday Wednesday Thursday Friday Saturday Sunday

At the top of the form, a (text) summary of the configured schedule is displayed to confirm 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 standard UTC (Coordinated Universal Time).

() INFO

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.

Actions

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

Notification

excible	2 111		My organization	Change: Ctrl + K Default: Ctrl + D	Organization Admin
Home		Etrong >			
Operations		for the second second second second			Disable
Rows	PREVIEW	coulties reduces an anno residence.			
Reports	PREVIEW	Overview Target • Flow Notification •			
Tenants					
Monitor					X Cancel 🗟 Save
Workspaces		User notification C Active			
Patch	PREVIEW 🗸	initial text (english) *			
Analyzer	PREVIEW 🗸	Configuring corporate MS Teams background			Show languages
Microservices	PREVIEW 🗸	Success text (english) *			
Settings		Successfully configured corporate MS Teams background			Show languages
		Error text (english) *			
		Error to configure corporate MS Teams background			Show languages
	Home Operations Flown Reports Tenants Monitor Workspaces Patch Analyzer	Home Operations Reports persent Tenants C Monitor C Patch Persent C Analyzor Persent C	Home Etxes Operations Foxes Roors restream Roports restream Roports restream Monitor Verview Target * Flow Notification * Workspaces User notification * Patch restream Nearbard * Analyzer restream Settings success text (english) * Settings Success text (english) *	Home Eben Operations Eben Roors Mexical Roports Mexical Nonitor Overview Vorkspaces Viser notification Patch Mexical Viser notification Active Initial text (english)* Configuring corporate MS Teams background Settings Successfully configured corporate MS Teams background Error text (english)* Successfully configured corporate MS Teams background	Home Paration Operations Reports Personts Moritor Workspaces Workspaces Patch Patch Patch Microservices Microservices Settings

This parameter is optional and can be disabled. It is used to send notifications to users at the start and end of the flow executions, using the operating system's notifications. Once enabled, you can set:

- Initial message. It will be sent to users at the start of the execution.
- Success message. It will be sent to users upon a successful execution.
- Error message. It will be sent to users upon an execution with errors.

() INFO

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

📿 тір

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

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

Reports		
Type: Any Tilter		
✓ Inventory (3)		
~	×	×
Office 365, Chrome and Adobe Workspaces Inventory	Office 365 Versions List	Workspaces Inventory
Tracks usage, versions and licenses of software tools within a workspace	List of all Office 365 versions installed on devices	existing in your organization and your Tenants.

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.

			My organ	Change: Ct nization Default: Ct		zation Admin	1
Reports Flexible							
Type: Predefined V Filter	2	Office 365, Chrome and	Adobe Workspaces Inventory				×
V Inventory (4)	T.	+ Generate new report 💡	දී Share 🙁 Refresh				
××	н.	Created at	Author	Expires at	Status	Actions	
Office 365, Chrome and Adobe Workspaces Inventory Tracks usage, versions and Ilcerses of software tools within a workspace			receiver and the same of the same		 Generating 		^
		2/16/25, 1:00:17 AM		4/17/25, 2:00:17 AM	 Available 		
	0	2/5/25, 12:05:21 PM	New Yorks of the second descent second	4/6/25, 1:05:21 PM	 Available 		
	12/20/24, 1:10:46 PM	March Theory of Care (1999) and the second	2/18/25, 1:10:46 PM	 Available 			
		12/20/24, 1:10:04 PM		2/18/25, 1:10:04 PM	 Available 		
		12/19/24, 4:13:35 PM	And the product in the second	2/17/25, 4:13:35 PM	 Available 		
		12/9/24, 11:13:36 AM		2/7/25, 11:13:36 AM	Expired		-

Office 365, Chrome and Adobe Workspaces Inventory

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

- Host number. Device name.
- Serial number. Device serial number.
- CPU cores. Number of central processing unit cores.
- RAM. Total amount of RAM (in megabytes).
- Disk used (%). Percentage of system disk occupancy.
- Total disk capacity. Total disk capacity (in gigabytes).
- Operating system Type of operating system.
- Microsoft 365. Installed Office version.
- Google Chrome. Installed Google Chrome version.
- Adobe Acrobat. Installed Adobe Acrobat version.
- Last user. User of the last session detected on the device.
- Created on. Date of report execution (creation).
- Date of last report. Date of execution (creation) of the last report.

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

Workspaces Inventory

Displays a list of existing devices in the organization and their tenants. The table offers the following information:

- Name. Device Name.
- Domain. Active Directory or EntralD domain to which the device belongs.
- Last user. User of the last session detected on the device.
- Device type. Physical or Virtual Desktop.
- Operating system.: Operating system name.
- Motherboard manufacturer. Name of the motherboard manufacturer.
- Motherboard model. Name of the motherboard model.
- BIOS Manufacturer. Manufacturer of the basic input/output system (BIOS).
- Processor. Processor name.
- CPU cores. Number of central processing unit cores.
- Regulatory compliance. Compliance policy applied to the device.
- Hypervisor. Type of hypervisor detected on the device.
- Broker. Type of broker detected on the device.
- Antivirus. Name of antivirus detected on the device.
- Antivirus status. Antivirus status on the device.
- BIOS mode. BIOS mode.
- Organization. Organization to which the device belongs.
- Client version. Installed version of FlexxAgent.
- Country. Country where the device is located.
- Created on. Date of device creation in Portal.
- Active CrowdStrike detections. Active detections from CrowdStrike.
- CrowdStrike status. Installed and functioning, Not installed, or Unknown.
- CrowdStrike version. Version number of CrowdStrike installed on the device.
- Subnet. Subnet in which the device resides.

- **Default gateway.** Default gateway.
- Desktop type. For VDIs, defines the desktop type.
- EDR. Type of Endpoint Detection and Response (EDR) detected on the device.
- Farm/Cluster. For VDIs, shows the farm to which it belongs.
- Delivery group. For VDIs, shows the delivery group to which it belongs.
- Fast startup. Shows if the device has Fast Startup enabled.
- FLXMID. Device identifier.
- IP address. Number of IP address detected on the device.
- Intel AMT compatible. Indicates if the device is compatible with Intel AMT.
- Is portable. Indicates if the device is portable.
- Total RAM (GB). Total amount of RAM (in gigabytes).
- Number of days since the last Windows update. Indicates the number of days since the last Windows update.
- Number of pending updates. Indicates the number of pending updates.
- OS Build. Operating system build number.
- Operating system manufacturer. Name of the operating system manufacturer.
- Operating system version. Version number of the operating system.
- OU. Organizational unit of the domain where the computer account resides.
- Platform type. Windows, Linux, Mac, etc.
- Windows type. Workstation or Server.
- Encryption. Indicates if BitLocker disk encryption is active.
- Pending restart. Indicates if the device has a pending restart for updates.
- IoT Hub configuration sync. Synced or Not synced.
- Custom field 01. Displays the content of the first custom field.
- Custom field 02. Displays the content of the second custom field.
- Last restart. Date of last device restart.
- Last Windows update. Date of the last Windows update applied.
- Report Group. Reporting group to which the device belongs.

Generate a report

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

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

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

Share a report

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

Reports can be shared with one or more recipients.

Share the last report

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

- 1. Go to Portal -> Reports and select a report type in the inventory.
- 2. In the top menu of the table, click the Share button.

0	ffice 365 Versions List	:			
	+ Generate new report	🔥 Share 🜔 Refresh			
	Created at	Author	Expires at	Status	Actions
	5/19/25, 2:08:18 AM	Automatically generated	7/18/25, 2:08:18 AM	Available	
	5/12/25, 2:08:18 AM	Automatically generated	7/11/25, 2:08:18 AM	 Available 	
	5/5/25, 2:08:27 AM	Automatically generated	7/4/25, 2:08:27 AM	 Available 	

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

	Share Report - Office 365 Versions List
	The people introduced below will receive an email with the report attached as a file.
	Frequency: Weekly
me	* Next execution on: 5/26/25
nto	Recipients
s an	john.smith@testemail.com ×
e	Send the latest generated report to recently added users
	Save Changes Close

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

e Corp		
ter	Share Report - Office 365 Versions List	
	The people introduced below will receive an email with the report attached as a file.	
	Frequency: Weekly	
	* Next execution on: 5/26/25	Ex
Chrome	Recipients	7/1
obe nvento	john.smith@testemail.com ×	7/1
rsions an vare tools	Send the latest generated report to recently added users	7/4
kspace	 An email with the last execution will be sent to: john.smith@testemail.com 	6/2
		6/2
	Save Changes Close	6/1
ersions	A17175 3:30:47.884 A	***

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 <u>Save changes</u> is clicked without selecting <u>Send</u> 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.

5/13/25, 2:11:22 AM	Automatically generated	7/12/25, 2:11:22 AM	Available
5/12/25, 2:19:25 AM	Automatically generated	7/11/25, 2:19:25 AM	View detail Availabl Download Excel
5/11/25, 2:06:11 AM	Automatically generated	7/10/25, 2:06:11 AM	Availabl Download CSV
5/10/25, 2:10:08 AM	Automatically generated	7/9/25, 2:10:08 AM	• Availabl 🔄 Share
5/9/25, 2:09:03 AM	Automatically generated	7/8/25, 2:09:03 AM	• Availabl 🔟 Delete Report
5/8/25, 2:08:00 AM	Automatically generated	7/7/25, 2:08:00 AM	Available

3. Enter the email addresses.

5, 2:07:25 A	AM Automatically generated
5, 2 Sha	re Report - Workspaces Inventory
	people introduced below will receive an email with the report the as a file.
5, 2	
Rec	ipients
i, 2 jo	hn.smith@testemail.com
2:1	
	Send Close
, 2:1	
, 2:11:58 AM	M Automatically generated

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

Share Report - W	orkspaces Invent	ory		
The people introc attached as a file.	luced below will n	eceive an er	nail with the re	port
Recipients				
J john.smitl	n@testemail.com	\times		
M mary.jone	s@testemail.com	\times		
			Send	Close

5. Click Send.

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
- <u>Client-type organizations</u>
- <u>Suborganizations</u>

Partner-type organizations

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

Client-type organizations

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

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

Suborganizations

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

() INFO

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

List of tenants

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

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

Flexxible III				Ĩ	My organization	(Ctrl + K) 🗸	Organization Admin	1
	🛍 Tei	nants						
Operations		nants						
² / ₆ Flows ■REVIEW	🕂 Create 🔞 Export 💍 Refresh							2
🔏 Tenants 🔨 🔨	Search by term	Y Filter						
Tenants								
Activation	Name †↓	Product 11	Policy 1	Creation date 🕆	Action			
🗈 Workspaces 🗸 🗸	Contraction of the local distance of the loc	FXXOne	FxxOne estándar	4/23/24	View Detail		1	
🗐 Patch 🛛 🛤 🗸 🗸	L Mart Designer (Par Personal)	FXXOne	FxxOne estándar	3/7/24	View Detail			
🗘 Microservices 🗸 🗸	 Head Televise 	FXXOne	FxxOne estándar	3/20/24	View Detail			
Ø Settings	L Instanti	FXXOne	FxxOne estándar	5/6/24	View Detail			
	1 mm	FXXOne	FxxOne estándar	3/6/24	View Detail			
		FXXOne	FxxOne estándar	3/12/24	View Detail			
	< Previous Page 1 v of 1	Next > Showing	1 to 40 of 40 results				Per page: 50	~

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 <u>Policy</u>. 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 + 0 (Cmd + K + 0 on Mac).
- Directly select the default organization (My organization) from the Organization Selector, located at the top of the interface.

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

Portal / Tenants / Activation

Activation allows Managed Service Providers (MSP) to 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.

Flexxible 🗰						💼 🐂	organization	(Ctrl + K)	 ✓ Organiz 	ation Admin
	Activation									
Operations	👰 Export 🕐 Refresh									1
යි Flows PREVIEW	Search by term		₽ Filter							
Tenants	Neme †↓	Product 11	Туре ↑↓	Status 11	90 days a <u>c</u> †↓	60 days aç 🛝	30 days ag 🏗	7 days age 🕄	Yesterday 치	Creation d 11 Deletio
Activation	Constant Const - Oppose	FXXOne	🚼 Partner	 Active 	0	0	0	0	0	3/12/24
🗟 Workspaces 🗸 🗸	Transport Concerning on	FXXOne	End customer	 Active 	67	62	67	70	72	3/12/24
🛱 Patch 🛛 PREVNEW 🗸	Transfer Concerningen	FXXOne	End customer	 Active 	16	15	15	15	15	3/13/24
🗘 Microservices 🗸 🗸	Statistic Cont Span.	FXXOne	End customer	 Active 	9	9	9	9	9	3/22/24
🕲 Settings 🗸 🗸	Tradition Concerning to	FXXOne	End customer	 Active 	17	17	16	18	18	3/26/24
	Constant Constanting	FXXOne	End customer	 Active 	0	0	0	0	0	5/9/24
	A second se	EVVOna	End customer	 Action 	0	0	0	R	61	40/H2/D4
	< Previous Page	1 ~ of 3	Next > Showing 1 to	50 of 125 results						Per page: 50 V

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

In cases where 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:

Flexcible	2 111								Client	Change: Cl Default: Cl			0
⊖ Home		Activations											
Operations		🚱 Export 🕚 Refresh											\mathbf{z}
∯ ₆ Flows	PRIME												
🖬 Reports	PRIVEW	Search by lerm	Filter										
<i>s</i> ∯ Tenants	~	Name †	Product 11	Туре 🔱	Status 11	90 days ago 🕸	60 days ago 🟗	30 days ago 🟗	7 days ago ‡	Yesterday 11	Creation date $\uparrow\downarrow$	Deletion date 11	
Tenants			Flexa Client	End customer	 Active 	28,182 (28,182)	28,656 (28,656)	27,807 (27,807)	0 (20,317)	895 (27,757)	2/28/24		ĵ.
Activations			FloorClient	End customer	 Active 	0	0	0	676	683	12/12/24		
① Monitor		Contraction of the second	FlexxClient	💄 End customer	 Active 	0	0	0	56	58	12/12/24		
🖾 Workspaces			RecrClient	End oustomer	 Active 	٥	0	0	3,840	3,675	12/12/24		
🛱 Patch	PRIME Y		Flexiclient	End customer	 Active 	0	0	0	304	306	12/12/24		
凹 Analyzer	PREVEW V		Flexa Client	End oustomer	 Active 	0	0	0	0	320	12/12/24		
Ø Microservices	PRIVEW V		FlexorClient	End customer	 Active 	0	0	0	0	137	12/12/24		
S Settings			Flexo/Client	End customer	 Active 	0	0	0	0	304	12/12/24		
			FloorClient	End oustomer	 Active 	٥	0	0	4,053	4,084	12/12/24		
			FlexorClient	End customer	 Active 	0	0	0	594	507	12/12/24		
			FlexorClient	End customer		0	0	0	0	958	12/12/24		
			Flexiclient	End customer		0	0	0	0	703	12/12/24		
		10. 10. 10. doc 10. or 10.	FlexxClient	End customer		0	0	0	240	242	12/12/24		
			RecrClient	End oustomer	 Active 	0	0	0	1/63	1/56	12/12/24		¥
C Prev	ew.	< Previous Page 1 V	of1 Next> S	howing 1 to 26 of 26 re	sults							Per page: 50	\sim

Tenant interface

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

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

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

Portal / 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 <u>Intel vPro Enterprise integration</u>.

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).



Online

The detail view includes the following tabs:

- Overview
- Installed applications
- <u>Current active alerts</u>
- **Operations**
- <u>Sessions</u>
- Windows Services
- <u>Disks</u>
- <u>All reporting groups</u>
- PnP Events
- PnP Errors
- <u>GPO</u>
- 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.*

					Change: Ctrl + K Organization Admin Default: Ctrl + D
Workspaces >	-	Online			
Overview		Power actions 🗸 Notification	actions 🗸		
General					
Device		Status		OS	Туре
Resources		Online		Microsoft Windows 11 Pro 24H2	Physical device
Connectivity					
Security		O User		Intel vPro Enterprise	Connection
Patching		X	inter	Not Supported	Wifi
OS					
FlexxAgent		IP Address		FlexxAgent Version 25.1.2.1	FlexxAgent Last report 2/7/25, 11:54:58 AM
Extended				EVITED	21723, 113430 AM
Installed Apps	105	General			
Active Alerts	0	General			
Operations	0	Name	Domain	OU	Connection Time
Sessions	1	Last User	flexxible.com CPU	RAM	2/7/25, 8:42:59 AM Code
Windows Services	287	Last User	17 %	RAM 14.09 GB (45%)	- Code
Disks	3	Description	Uptime	Idle Time	Last Restart
Reporting Group History	0		4d 2h 48m 37s	-	2/3/25, 9:53:11 AM

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.

						ange: Ctrl + K fault: Ctrl + D	ation Admin
= Workspaces $>$	-	Online					
> Overview		Power actions 🗸 Notifica	ition actions 🗸				
Installed Apps	105						
Active Alerts	0						
Operations	0	💼 Export 💍 Refr	esh				
Sessions	1	O Search hu term					
Windows Services	287	Search by term.					
Disks	3						
Reporting Group History	0	Name î	: Publisher î↓	Version 1↓	Installed at 🗍	Install location ↑↓	E Last rep
		Adobe Acrobat (64	I-bit) Adobe	24.005.20399	2/3/25	C:\Program Files\Ado	beVA 2/7/25
		Aplicaciones de M	icroso Microsoft Corpora	16.0.18227.20222	4/12/24	C:\Program Files\Mic	rosof 2/7/25
		Aplicaciones de M	icroso Microsoft Corpora	16.0.18227.20222	4/12/24	C:\Program Files\Mic	rosof 2/7/25
		Aplicaciones de M	icroso Microsoft Corpora	16.0.18227.20222	12/30/22	C:\Program Files\Mic	rosof 2/7/25
		Asistencia rápida	Microsoft Corp.	2.0.0	9/13/24	C:\Program Files\Win	dow 2/7/25
		4					*

The information includes:

- Name. Name of the application installed on the device.
- Publisher. Company that developed the application.
- Version. Version of the application.
- Installed on. Date it was first reported on the device.
- Installation location. Folder where the application is located.
- Last report. Date of its last report on the device.

Active alerts

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

					Change: Ctrl + K Default: Ctrl + D	Organization Admin	
Workspaces >	-	Online					
> Overview		Power actions \checkmark Notification a	ctions 🗸				
Installed Apps	113						
Active Alerts	3						
Operations	0	🔨 Export ՝ Refresh					
Sessions	0	Search by term					
Windows Services	274	Search by term	∀ Filter				
Disks	5	Severity 1	: Alert name 1↓ :	Information 1↓	Alert start 1↓	: Date notified	1
Reporting Group History	0	seveny			rucit start it	. Dute notified	
		O Critical	Low storage free space %	Drive: C: Free space: 28 G	2/2/25, 6:44:27 PM	2/2/25, 6:44:27	Р
		① Critical	Boot duration	Boot duration 151 seconds	2/7/25, 12:14:07 PM	2/7/25, 12:14:08	l.
		🔥 Warning	Workspace with Plug and	Workspace with 1 Plug an	12/17/24, 5:13:11 AM	M 12/17/24, 5:13:1	2
		4				•	
		K ← C Page 1 of 1 →	> 1 to 3 of 3 results			Page Size: 50 🔻	

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.

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:

- 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.

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.

Group Policy (GPO)

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

- Display Name: Name assigned to the policy.
- Last Applied Time: Date and time of the policy's last application.

Boot history

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



() INFO

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

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.

Flexxible III			My organization	Change: Citrl + K Default: Citrl + D	tzation Admin
l Home D Operations	🍓 – Wo	rkspace Groups			
중 Flows PREMEW 國 Reports PREMEW	+ Create 🔞 Export 🕐 Refresh				2
🖧 Tenants 🔊	Name 14	Y Fiter Type 1↓	Entra ID resource name 14	# Workspaces 11	Action
Co Workspaces		Dynamic Static			View Detail View Detail
Workspace Groups	1.00	Static Dynamic		0	View Detail View Detail
Patch Peterson Patch Peterson Image: Analyzer Peterson	10.000	Dynamic		0	🖸 View Detail
Microservices PREMIER Settings	Test Test	Entra ID Entra ID			View Detail View Detail
	Transmission (Constrained)	Static Dynamic			☑ View Detail ☑ View Detail
	< < < <pre>evicus Page(1 >>) at1</pre>	Next > Showing 1 to 27 of 27 results			Per page: 60 V

There are three types of groups:

- <u>Static</u>
- <u>Dynamic</u>
- Entra ID

Static workspace group

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

Dynamic workspace group

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

() INFO

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

Entra ID Workspace group

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

Group management

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

- Workspace group details
- <u>Workspaces</u>
- <u>History</u>
- Location
- <u>Schedule</u>
- <u>Synchronizations</u>

Workspace Group Details

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

Fle	excible	e III		My organization Dr	anges Citrl + K Viganization Admin
	Home Operations		> Workscore Groups >		
齿	Rows	PREVIEW	Workspace Group Details Workspaces History Location Schedules Synchronizations		
	Reports Tenants		Name		# Workspaces
	Monitor	~	The second		≫ 4
	Workspaces	^	Description		Created by
	orkspaces v2 orkspaces	PREVIEW	Entra ID (Group)		Constitut data
w	orkapace Group	xe	Entra ID resource name Entra ID resource id		Creation date 10/28/24
	Patch	Menew ~		Edit	
	Analyzar Microservices	PREVIEW V			
0	Settings	~			

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.

Flexcible 🔛					ti de	My organization	Change: Ctrl+K Default: Ctrl+D	Organization Admin	•
ය Home	> Workspace Gro.	105 >							
Operations	Ballon Replica								
G Rows PREMEN	Workspace Group Details	Workspaces Histo	ry Location Sc	hedules Synchronizations	3				
Reports PREMEW									
🖧 Tenants 🗸 🗸	🖻 Eyport 🕐 Refresh								ſ.,
🛈 Monitor 🗸 🤟	P Search by term		Iter						
🗈 Workspaces 🔨 🔨	Name 11.	FQDN 11	IP Address 1.	Operating System 11	CPU Cores 11	RAM 11	Туре 🏨	Last User 11	
Workspaces v2 PREVNEW				Microsoft Windows	12	16055	Physical device		
Workspaces PREVIEW				Microsoft Windows	12	15812	Physical device		
Workspace Groups				Microsoft Windows	8	7976	Physical device		
🛱 Patch PREMEW 🗸				Microsoft Windows	8	16145	Physical device		
🖾 Analyzer 🛛 🛛 🗠 🤟				Microsoft Windows	12	32425	Physical device		
Microservices PREMEW V				Microsoft Windows	8	7915	Physical device		
⊚ Settings ∨				Microsoft Windows	16	32389	Physical device		
		-	-	Microsoft Windows	8	7915	Physical device	10000	
	< Previous Page (1 V of 2 Ne	xt > Showing 1 to 5	50 of 56 results				Per page: 50	~

History

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



Location

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



Schedule

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

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

lew scheduled action	
ction *	
Wake On LAN	~
/eek day *	
Select week day	\sim
TC Time * 🕕	
:	Q
Use specific Workspace fo	rwol
Select the Workspace	~
Search the Workspace	
Type at least 3 characte	ers to load workspaces

Sync

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

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

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

Date 11	Entra ID workspace 🛝	Workspaces added $\uparrow\downarrow$	Workspaces removi 🔱	Existing workspace ${\uparrow}{\downarrow}$	Workspaces not fou 🕸	Duplicated workspa	Execution time $\uparrow\downarrow$	Action
	118	0	0	57	61	7	0.901 s	View Detail
	118	0	0	57	61	7	0.374 s	View Detail
	118	0	0	57	61	7	0.631 s	View Detail
	118	0	0	57	61	7	1.286 s	View Detail
	118	0	0	57	61	7	0.975 s	View Detail
	118	0	0	57	61	7	0.726 s	View Detail
	118	0	0	67	61	7	0.441 s	View Detail
	118	0	0	57	61	7	0.296 s	View Detail
	118	0	0	67	61	7	0.763 s	View Detail
	118	0	0	57	61	7	0.414 s	View Detail
	118	0	0	67	61	7	0.694 s	View Detail
	118	0	0	57	61	7	0.748 s	View Detail
	118	0	0	57	61	7	0.758 s	View Detail

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.

Create workspace group

Name *

Please enter text here

Description

Please enter text here

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.

Flexodble III		Import Workspaces
a	Indian Manalage Mana	Workspaces list *
D Operation	Minimum	workspace,2 workspace,3
·	Writzer-Drag little Molegane Milling London	
4 trats 1 D magaza 2	1 mart Melagana of Sill (2 Same	
Robuston Ballio		
Bohgasa Grogo		1/20000
8 man		
C Monardon -	50	
· · · · ·	Đ	
	No workspaces found	
		× Cancel + Import

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.

Flexcible 🔛					Ny o	rganization	(Ctrl + K) 🗸	nization Admin	1
	Elexable Corp > Workspace Groups								
Operations									
² ₀ Flows ■REVIEW	Workspace Group Details We	orkspaces History	Location						
A Tenants 🗸 🗸	-								
🕼 Workspaces 🔨 🔨	🗙 Cancel 🔙 Save 🔞 E	xport 💍 Refresh							2
Workspaces PREVIEW	Search by term	Show work	spaces: Any	Filter					
Workspace Groups	Name †1	FQDN 11	IP Address 🕄	Operating Syste †↓	CPU Cores 13	RAM 11	Туре 1↓	Last User 🔃	
🔋 Patch 🗰 🗰 🗸 🗸		-	1000000000	Microsoft Windo	12	32581	Physical device	-	
Microservices V	•		1000000	Microsoft Windo	4	8073	Physical device	-	
Settings		1000000-00	10200027	Microsoft Windo	4	3985	Physical device	International Contracts	
	1000021	100mmill	THE R. L.	Microsoft Windo	4	8141	Virtual Desktop	CONTRACTOR NAMES	
	(classic)	mail	Hamain .	Microsoft Windo	4	8141	Virtual Desktop		

() 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 -

rle <mark>×</mark>	× WORKSPACE	S							◊	Log Off
search Q Level 1	Workspaces									
ER UK dashboard						My Filters 👻	ilter by tag	; Filter by workspace grou	p Text to searc	h , P
Workspaces		□ Ø	ø 6	1		Predefined filters Save current filter	Ì	· <=	$\oslash \oslash \bigcirc$	Ø
Sessions	Platforms	Machine †	RG Tenant	Power state	La	Manage Filters Clear filter	U	% RAM Uptime Code	Status	Connection
E Connection logs		C satissain	Street Street	On	5	Workspace Groups		Save as workspace group Save as dynamic workspace group	0 🛰	Ŷ
D Jobs				Not reporting	15.	Filter by OS	► tá	0 %	*	
L. Alerts			(Insertion Corp.)	Not reporting	-	Filter by installed apps	0 %	0 %	*	
Profile storage			(Resolution Corp.	On	1001		13 %	67 % 9d 21h	0 🥆	(]
Level 2 >				Not reporting		-	0.95	0 %	*	

Create a dynamic workspace group

> Workspace group -> Save as workspace group.

From the list view of Workspaces, in the Workspaces module, right-click any field in the table to access <u>Filter builder</u> 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.

Flex	× WORKSPACES						Todos los tenants 🔹 🖓	Cerrar	r sesión
Search Q Nivel 1 V Panel de UK	Workspaces				ſ	Mis filtros 🔹 Filtrar por etiq	ueta Filtrar por grupo de workspa	Text to search	2
Wardapasees		1 🖓 🚳 🗊		_ 0 (j		Filtros predefinidos Guardar el filtro actual Administrar filtros	CPU consumption over 80% CrowdStrike active detections FlexxAgent reporting errors] • D • •	
Sesiones	Plataformas	Máquina	Tenant del RG	Estado	Último usuario	Borrar el filtro	FlexxAgent version summary Network signal below 40%	Estado Conexión	4
:= Registras de coneción	ㅁ 🚦 🔶 🕒 🕅			Encendido		Grupos de Workspaces Filtrar por unidad organizativa	No Windows Updates during last 30 days Not restarted in the last 15 days	o 🖌 🛛 🕴	
D. Tradingos	🗆 🚦 🔷 🍥 🔯	O 10 10 10 10 10 10 10 10 10 10 10 10 10		Encendido		Filtrar por sistema operativo Filtrar por aplicaciones instaladas	 Notificaciones aceptadas Notificaciones pendientes de aceptación 	⊘ ➤ 🕴	
E Alertas	🗆 🚦 🔶 🖾 🚺			Encendido		0 2%	Outdated FlexxAgent Power State is ON	o 🔺 🛛 🕴	
g. Amagenamiente de perfiles	ㅁ 🚦 🔷 🕒 🔯	0		Encendido		1 2%	RAM consumption over 90% Reboot-pending workspaces	I 👻 🔸	
Nivel 2	0 🚦 🔶 😐 👩	O the first second price		Encendido		0 5 %	Unattended remote assistance enabled With session	Ø 💊 🛛 🕴	
144612	n 📕 🛆 m 🛤	A		Presendida		A 44	ad W - NY I AF	○ ►	

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 <u>Job</u> 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.

Flexodale III				Create workspace group $\qquad \qquad \qquad$
a	C Thursday - Wor	kspace Groups		Name * Please enter text here
A track and	e Crais @ Squar () fam			Description Please enter text here
D magain in	A factory ten.			Entra ID
-	Record C	Type 1. Error & measurements 1.	a Malagaran 1. An	Туре
I tan men r	forest de p	from the second s		Entra ID group Entra ID administrative unit
0 August 1000 12	AP 301	ten .	11	Entra ID group
0 three 10 the 1	Non-April 10	Sparts		
	Sales Days			
	Contract of the local division of the local	of the Barry's Del South		× Cancel + Create

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 <u>Filter</u> <u>builder</u>. From there you can choose the new filters for the group. Please note that Workspaces will overwrite the original filters; that is, it will remove all old filters and replace them with the new ones. Press OK.
- 3. With the new device list, go to My filters -> Workspace Groups -> Save as dynamic workspace group. It is important to save the group with the same name it

had before so a new group is not created.

Delete a workspace group

In the list view of the Workspace groups section, in Portal, click on Detail view of the desired group. In the Group Details tab -> Edit, a form will open with the Delete option.

() INFO

For more information on how to create or manage workspace groups, please refer to <u>this guide</u>.

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.



(i) 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:

- <u>Enabled</u>. Describes how to activate a microservice for execution by an end user or from Workspaces.
- Marketplace. Shows the catalog of available microservices.
- <u>Designer</u>. Explains how to create new microservices and configure existing ones.
- Audit log. Describe what the user microservices execution tracking consists of.

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 <u>Marketplace</u> 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 <u>Designer</u> 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.

Fle	excible	2 111			My organization (Ctrl + K) V	zation Admin	
ŵ	Home	Í	Create new microservice (1/4)				
Ð	Operations		Name (english)		Library *		
窈	Flows .	PREVIEW	Enter the name of the microservice (english) Show I	anguages	Fleroible Corp		
瘤	Tenants	~	Colour		loon		
Ð	Workspaces	~	Select the color of the microservice icon)	Select the icon of the microservice	~	9
Ô	Patch	HIEVIEW 🗸	Description (english)				
Ø	Microservices	~	Enter the description of the microservice (english)			Show languages	
ಷ	Enabled		Language *		Version		
G	Marketplace		Enter the language of the microservice		1)
	Designed	_	Scope *		Context (for Workspace scope)		
	Designer	_	Enter the scope of the microservice)			
	Audit log		Operating system *		Category (english)		
			Enter the operating system of the microservice	~)	Enter the category of the microservice (english)	Show languages	
			Efficiency *				
			Enter the number of minutes that the microservice saves				

Execution scope configuration

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

Execution from the local administrator

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

Execution from user session

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

Ways to consume microservices

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

On-demand execution from Workspaces

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

- 1. Access the Workspaces module -> Workspaces or Sessions section.
- 2. Select the devices 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 Session section when the configuration has selected the *Session* context.

Flex	×wo	ORKSPACES							Flex	xible Team	Ŧ		ible.com Cerrar sesión
Search Q Nivel 1 V Panel de control de experiencia de usuario Workspaces	Work	ispaces			- ¢ (- <>			Mis filtros	Text to	operaciones
D		Plataformas	Máquina †	Tenant del GR	Estado	Último usuario	Sesiones	CPU	% de RAM	Tiempo activo	Código	Estado	Conexión
Sesiones			DESKTOP-NCLOVHL	Flexxible Team	Sin reportar	DESKTOP-NCLOVHL\EXO	0	0 %	0 %		Bigote		
Registros de conexión			DESKTOP-OM7GPTN	Flexxible Team	Sin reportar	DESKTOP- OM7GPTN\Mabel	0	O 96	0 %				
Trabajos			FLX-02-001- 037.ad.flexxible.com	Flexxible Team	Encendido	FLEXXIBLE\fzani	1	4 %	52 %	7h 42m		\oslash	ę
! Alertas			🕛 ideapad	Flexxible Team	Sin reportar	IDEAPAD\luzma	0	0 %	0 %				
Almacenamiento			🕛 Raven	Flexxible Team	Sin reportar	RAVEN\Fede	0	0 %	0 %				
de perfiles			v15g2	Flexxible Team	Sin reportar	V15G2\yami	0	0 %	0 %				
Nivel 2 > Nivel 3 >	< _	Count=6				6						Page siz	ze: 20 •

Management of the execution scope of the microservice and permissions can be done from the <u>Designer</u> 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 automating and executing a microservice automatically when certain conditions are met on the device. Its main characteristic is that it simplifies diagnostic actions and quickly resolves problems through the execution of a microservice.

Fle	exxible														1	ly orga	nizatik	in	(Ctr	I + K)	~	Or	ganiz	ation	Admi	n	
ធ៌	Home		Overview	Target	Flow	Notificati	'n																				
۵	Operations				_																						
6	Flows m	EVEW																								Edit	
rê.	Tenants	~																									
₽	Workspaces	~																									
Ê	Patch 🛤	eview 🗸									Exist	ence	ofap	roces	ss in												
Ø	Microservices	~								•••	prog																
-	Settings	~											Equa	al C	hrome	e.exe											
													EE														
								8	i i		Update Google Chro	*															
								:::		\sim		Chro	me														

For more information on executing a microservice through a flow, please consult <u>this</u> <u>guide</u>.

Scheduled execution through Alert Settings

Through <u>Alert Settings</u>, 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 <u>Alert Settings</u> 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.
| Fle | excible | ::: | | | | My organization | (Ctrl + K) 🧹 | Organization Admin | |
|-----|---------------|-----|-------------------|------------------|---------------------------------|-----------------|--------------|--------------------|-----|
| ඛ | Home | | Overview Script | Targets Settings | License | | | | |
| Ð | Operations | | | | | | | | |
| 绤 | Flows PREV | | FlexxWorks | paces execution | | | | | |
| rê. | Tenants | | | | | | | | |
| Ð | Workspaces | | | Allow to execute | Allow to execute (individually) | | | | - 1 |
| ß | Patch Piev | | L3 | ~ | ~ | | | | - 1 |
| Ø | Microservices | ^ | L2 | ~ | ~ | | | | - 1 |
| 4 | Enabled | | и | ~ | ~ | | | Edit | |
| G | Marketplace | | | | | | | Edit | |
| M | Designer | | End-user ex | recution | | | | | |
| 11 | Audit log | | | ooddon | | | | | |
| | | | End-user executio | n | | | | | |
| | | | Disabled | | | | | | |
| | | | | | | | | Edit | |

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.
- On the left side menu, click the Microservices configuration tab -> Edit Microservices configuration.
- 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.

pine in the second s	
Q Buscar aplicaciones, configuraciones y documentos	CONTRACTOR OF
	and the second
Todos	(Atrès
	Licencia
Flexible	^
Borrar Cache Google Chrome	Icono
🐱 Desinstalar AnyDesk	
🐱 Limpiar disco (incluye caches de Spotify)	
	Versión 1
	Contexto
	Sesión
	Categoria
	Red (CSP)
	O
🔠 📮 🥺 🦉 🦉 🥵 👰 📢	

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.

O Sear	rch for apps, settings, and documents
A bear	cirior apps, settings, and documents
All	
0	Outlook
Ρ	
- 🖓	Paint
	Phone Link System
<u>~</u>	Photos
\sim	Ping google New
Q	
	Quick Assist

Û LIÞ

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

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.

Flexxible 🔢			My organization	(Ctrl + K) VOrganization Admin	
ය Home	Enabled microservices				
Operations	😥 Export 🕐 Refresh 🛛 🛑 Blocks				2
50 Flows Preview					
ළේ Tenants 🗸 🗸	P Search by term ⊽ Filter				
🗈 Workspaces 🗸 🗸					^
🗐 Patch 🛛 PREVIEW 🗸	1				- 11
🗘 Microservices 🔨	List Installed User	40	Windows Update - No	Windows update - with	
🕰 Enabled	Certificates This script lists the certificates	Borrar cache Teams This script clears Teams caches.	restart This script applies available Windows	reboot This script applies available Windows	
Marketplace	installed in the user's local trunk and displays their name, certificate Certificates	Collaboration	updates without rebooting the system. Updates	updates by rebooting the system. Updates	
Designer					
Audit log					
				6	
	< Previous Page 1 vort Next > S	howing I to 46 of 46 results		Per page: 60	~

Microservice detail

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

- <u>Overview</u>
- <u>Code</u>
- <u>Targets</u>
- <u>Settings</u>
- <u>Alert configuration</u>
- <u>License</u>
- 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.

≡	Flexi	ole			My organization	Defauli: Ctrl + D V Organization Admin
ŵ	Home	18	Enabled microservices > List installed user certificates			
Ð	Operations		List installed user certificates			
Ē	Reports		List instaned user certificates			
绤	Flows	\sim	Overview Script Targets Settings Alert settings	License Enabled tenants		Go to designer Clone Disable
Æ	Tenants	~				
Ū	Monitor	\sim	Description	lcon		E Author
œ۵	Workspaces	\sim	This script lists the certificates installed in the user's local trunk and displays their name, certificate authority, and expiration date.			
Ê	Patch	~		Version		Published
Ø	Analyzer	\sim	Language PowerShell	2		11/5/24
Φ	Microservices	^	Scope	Context		ticense
64	Enabled		Workspace	Session		
			Operating system	Category		
			Windows	Certificates ශ්ව		Category Certificates

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.

• License. Allows configuring the microservice's license type.

2. Clone

Allows the general configuration of the microservice to create a new one, based on its current information.

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 <u>Designer</u> section.

Code

Displays the source code of the microservice, including the logic and instructions that define its behavior.

Targets

Defines the conditions for the execution of the microservice.

Execution of FlexxWorkspaces

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

End-user execution

Specifies whether the microservice is enabled to be executed directly by the end user. This permission can also be modified using the Edit button.

() INFO

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 <u>Alert Settings</u>.

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.

=	Flexit	ole			My organization	Default: Ctrl + D 🗸 Organ	ization Admin
ŵ	Home	5	Enabled microservices > List installed user certificates				
Ø	Operations		List installed user certificates				
Ē	Reports		List installed user certificates				
绪	Flows		Overview Script Targets Settings Alert settings L	icense Enabled tenants			
я <mark>я</mark>	Tenants						
Ø	Monitor		🧹 Enable 🗙 Disable 🏚 Export 💍 Refresh				
Þ	Workspaces		Search by term 2 rows selected				
自	Patch						
8	Analyzer		■ Name 1↓	च ः Enabled ी↓		ecution î↓ \Xi 🗄 🛛 Min gr	
¢	Microservices			Yes	u	L1	Û
ŝ	Enabled		×	No			
				No			
			4				*
			K < Page 1 of 4 > > 1 to 50 of 162 results				Page Size: 50 🔻

The table contains the following information:

- Name. Tenant name. If it has sub-organizations they are presented in tenant*>*suborganization 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 <u>Targets</u> is done independently for each tenant.

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.

Portal / Microservices / Marketplace

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

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 <u>run directly</u> 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:

- <u>Overview</u>
- <u>Code</u>
- <u>Targets</u>
- <u>Settings</u>
- Alert configuration
- License
- Enabled tenants

Overview

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



From this tab, three main actions are available:

1. Go to designer

Opens the Designer section. Allows editing the microservice configuration through the following tabs:

- Overview. General data of the microservice.
- Code. Source code of the microservice.
- Privacy. Information about the visibility of the microservice.
- Targets. Conditions for the execution of the microservice.
 - Execution of FlexxWorkspaces
 Shows roles with permissions to execute the microservice in the Workspaces module. The column *Allow execution* indicates the roles authorized to execute it at the Workspace group level, while *Allow execution (individual)* shows roles with permission for execution on individual devices. Both can be modified using the Edit button.

- Execution by the end user
 Specifies whether the microservice is enabled to be executed directly by the end user. This permission can also be modified using the Edit button.
- License. Allows configuring the microservice's license type.
- 2. Clone

Opens the Designer section. Allows general configuration of the microservice to create a new one based on its current information.

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 <u>Designer</u> section.

Code

Displays the source code of the microservice, including the logic and instructions that define its behavior.

Targets

Defines the conditions for the execution of the microservice.

• Execution of FlexxWorkspaces

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

• End-user execution

Specifies whether the microservice is enabled to be executed directly by the end user. This permission can also be modified using the Edit button. () INFO

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

Settings

Reports the estimated time (in minutes) that the use of the microservice has saved the user compared to a manual solution for the same situation.

Alert Configuration

Presents a table with alerts linked to the microservice. For more information, please consult the documentation on <u>Alert Settings</u>.

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.

= F	rlexxibl	👊 My organiz	tation Default: Ctrl + D 🗸 Organization Admin
ය Ho	ome	Enabled microservices List installed user certificates	
D Op	perations	List installed user certificates	
🖬 Re	eports	List installed user certificates	
绪 Flo	ows	Overview Script Targets Settings Alert settings License Enabled tenants	
A Ter	enants		
1 Mo	lonitor	🗸 Enable 🗙 Disable ᡚ Export 🚫 Refresh	
⊫ wa	/orkspaces	Search by term 2 rows selected	
館 Pa	atch		
🖾 An	nalyzer	■ Name ↓	n Individual execution ᡝ 후 🗄 👘 Min group execution 🏦 후 🗄
Ф Mi	licroservices	Yes U	u 🔒
62 En	nabled	No No	
		No No	
			×
		K ⊂ Page 1 of 4 → N = 1 to 50 of 162 results	Page Size: 50 🔻

The table contains the following information:

- Name. Tenant name. If it has sub-organizations they are presented in tenant*>*suborganization 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 <u>Targets</u> is done independently for each tenant.

Enable/Disable a microservice for tenants

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

Portal / Microservices / Designer

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:

Fle	exxible				My organization (Ctrl + K) 🗸	Organization Admin
ŵ	Home	Í	Create new microservice (1/4)			
Ð	Operations		Name (english)		Library *	
56	Flows PREM	w		languages	Fleodble Corp	
唏	Tenants	~	Colour		loon	
Đ	Workspaces	~	Select the color of the microservice icon		Select the icon of the microservice	v)
â	Patch MIEM	ew 🗸	Description (english)			
Ø	Microservices	~	Enter the description of the microservice (english)			Show languages
€4	Enabled		Language*		Version	
Ð	Marketplace		Enter the language of the microservice		[1	
ы	Designer		Scope * Enter the scope of the microservice		Context (for Workspace scope)	
	Audit log		Operating system *		Category (english)	
			Enter the operating system of the microservice	~	Enter the category of the microservice (english)	Show languages
			Efficiency *			
			Enter the number of minutes that the microservice saves			

- Name. Enter the name of the microservice.
- Color. Microservice icon color.
- Icon. Microservice icon type.
- Description. Brief text explaining what the microservice does.
- Language. Programming language it is developed with.

- 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.
- **Category.** Directory or group of microservices accessible from Workspaces where this microservice will be hosted.
- Efficiency. Number of minutes the microservice saves with each execution.
- 4. Click Next.

() INFO

If the microservice is to be used as an end-user microservice, the **name of the microservice should not contain special characters** (such as \ / : * ? " < > and other language-specific characters for certain keyboard layouts).

Phase 2 - License

- 1. Choose from the dropdown options the type of license the microservice will have.
- 2. Click Next.

Fle	excible	2 111			🔞 My organization		Organization Admin	
ŵ	Home		Create new microservice (2/4)	- License				
Ð	Operations							
鍲	Flows	PREVIEW	License *				X Cancel	- II
ഷ്ട്	Tenants						X Cancel D1 Ne	<u></u>
æ	Workspaces		A short and simple permissive license with condi different terms and without source code.	itions only requiring preservation of copyright and license notices.	Licensed works, modification	s, and larger work	s may be distributed under	
â	Patch	PREVIEW	Permissions	Limitations	Co	nditions		
Ø	Microservices		 Commercial use Modification 	× Liability × Warranty	0	License and copy	right notice	
۲	Settings		✓ Distribution ✓ Private use	i i constante a g				
			MIT License Copyright (c) 2024 [Organization name] Permission is hereby granted, free of cl of this software and associated documen in the software without restriction, in to use, copy, molify, merge, publish, d copies of the Software, and to permit po- furnished to do so, subject to the foll The above copyright notice and this per copies or substantial portions of the So	tation files (the "software"), to deal cluding without limitation the rights istribute, sublicense, and/or sell ersons to whom the Software is working conditions: mission notice shall be included in all				

Phase 3 - README

- 1. Insert a description of the microservice in <u>Markdown</u> format.
- 2. Click Next.

() INFO

To set a title with Markdown, simply start the line with **# Title**. Here are some examples of its syntax:

ltem	Markdown Syntax	Preview
Bold	**bold**	bold
Italic	*italic*	italic
List	- List item	- List item
Link	[text](url)	text
Image	![alt](url)	ford
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 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.

Portal / Microservices / Audit Log

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

Flexcible III				y organization	(Ctrl + K) 🗸 Organ	ization Admin
බ Home	Audit log					
Departions	😥 Export 🕐 Refresh					2
යි Flows mienew නී Tenants V	✓ Search by term					
🕞 Workspaces 🗸 🗸	Microservice 11	Туре †⊥	Status 🏗	Initiated by $\uparrow \downarrow$	Logged at †↓	Actions
🛱 Patch 🛛 🛤 🗸 🗸	Listar redes Wifi available (97)	Activated	Success		11/3/24, 12:58:41 PM	View Detail
Microservices	Flush & register DNS 1970	Activated	Success		11/3/24, 12:58:11 PM	View Detail
ස් Enabled	List Installed User Certificates 🕬	Activated	Success		tt/3/24, 12:57:45 PM	View Detail
Marketplace	Windows Update - No restart 🧐	Activated	Success		10/31/24, 12:42:14 PM	View Detail
N Designer	Clean Disk ^{양한}	Activated	Success		10/31/24, 10:55:53 A	View Detail
Audit log	Get Sessions	Archived	Success		10/30/24, 1:11:46 PM	View Detail
	Get Sessions	Deactivated	Success		10/30/24, 1:10:53 PM	🖸 View Detail 🗸 🗸
	< Previous Page 1 of 7 Next > Showing 1 to 5	0 of 301 results				Per page: 50 ~

- 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.



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.

Flexxible		Client Change: Ctrl + K Crganization Admin
යි Home	Summary	
Operations	Targets	Workspaces
ය Flows	▲ Alerts (1) ✓	① Information (1)
🔏 Tenants 🛛 🗸 🗸	Aler to (T) Some targets have missing schedules. Please ensure all targets have a schedule assigned. Without scheduling, the workspaces will not receive	Excellent work! All workspaces have a reporting group assigned
🖨 Workspaces 🗸 🗸	patches.	Every workspace is assigned to a reporting group.
🗯 Patch 🗸 🗸	\odot Information (1) \checkmark	0 ~
🍄 Microservices 🗸 🗸	Excellent work! All reporting groups are currently under control. All reporting groups have a patch policy assigned.	22 total workspaces
Settings	0 % ✓ 75 % O reporting groups without a patch policy Fix	Workspaces without Reporting Group

Patching management features

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

Patching management considerations in Portal

- Allows scheduling time windows for performing update processes.
- It is available for devices with Windows operating systems. Includes Windows 10, Windows 11, Office 365, Office 2019, Microsoft Edge, Microsoft Defender, Drivers, etc. Does not include patching Windows server roles.
- Allows managing updates of Microsoft components. Optionally allows selecting which ones to install on the device.
- The functionality is aimed at environments where there is no prior patch management system.
- Allows auditing update processes to manage exceptions and errors.

() INFO

Activating patch functionality in an environment that already has an update system running could create conflicts or unexpected behaviors. It is recommended to maintain a single active patch system.

FlexxAgent behavior in patch management

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

If a user decides to deny the installation of a patch, but FlexxAgent finds that update on the device, in the next update process FlexxAgent will try to uninstall it, although it should be noted that there are patches that the operating system does not allow to uninstall due to their nature.

() INFO

If the device has a system proxy, it must allow communication with Windows Updates.

Portal / Patch / Summary

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

- <u>Targets</u>
- <u>Workspaces</u>

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).

Targets	
🛆 Alerts (2)	\sim
Reporting groups without a patch po Please assign a patch policy to all report	
Some targets have missing schedule Please ensure all targets have a schedu patches.	s. Ile assigned. Without scheduling, the workspaces will not receive
50 %	75 %
5 reporting groups	3 targets
Reporting groups without a patch policy	Targets without a schedule
Fix	Fix

Workspaces

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



Portal / Patch / Reporting groups in patch management

Reporting groups classify devices according to their functions, departments, or locations. When they are assigned a target to configure their patch policy, an organization ensures coverage of its entire computer network.

At the top of this section, you can see an information panel showing the total number of devices that are part of the organization, divided according to their operating system.

317 ⁽¹⁾	Þ	306 ^①		11 ⁽ⁱ⁾	۵
Total workspaces		Windows workspa	ces	Linux workspaces	

() INFO

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

Total devices per reporting group

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

Total workspaces by reporting group \odot



Portal / Patch / Targets

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

Flexxible		a	My organization	Change: Ctrl + K Default: Ctrl + D	Organization Admin	1
Operations	Targets					
G Flows preview	+ Create 📵 Export 🕐 Refresh					2
📾 Reports	Search by term					
മ്പ് Tenants 🗸 🗸						
🛱 Workspaces 🗸 🗸	Name ↑↓	Reporting Groups $\uparrow \downarrow$	Ha	s Schedule set $\uparrow\downarrow$	Actions	
🛱 Patch 🔨	Patch	Presales		\checkmark	View Detail	
Summary	Patch validation	OS Patch		×	View Detail	
Reporting Groups						

The overview of this section displays a table with the list of created targets, along with the following information:

- Name. Name assigned to the target.
- **Reporting groups.** Name of the reporting group (can be more than one) to be targeted by the patch 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 <u>target details</u> and its configuration options.

Create a new target

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

Patch policies are applied to report groups; it's not possible to apply a patch policy to an individual device from Portal. To force the update of a specific device, it must be done from

the Workspaces module: Workspaces -> Operations -> OS patching -> Patch OS now.

💭 ТІР

For more information on how to create a new patch policy in Portal, please refer to <u>this guide</u>.

Target details

From this view, you can configure the target's patch policy in two areas:

- Details
- <u>Schedule</u>

Details

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

- 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). Allows patches to be applied even when the devices are suspended or turned off.
- Microsoft update policy. Name of the Microsoft update policy being applied to the target.
- **Reporting groups.** Shows the reporting groups to which the patch policy has been assigned.

INFO

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

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

Edit patch policy target		×
Name		
Target-Docs		
Reporting Groups *		
RT RP Training ×		
Microsoft patch policy		
Select Microsoft patch policy		\sim
Restart after patching i		
Wake on LAN 🛈		
🖻 Delete	\times Cancel	🔒 Save

The Delete button discards the target's patch policy.

Details also provides information about the creation date of the target's patch policy and the user who created it.

Schedule

From this section, you can schedule when updates will be applied to devices that are part of a report group. And also the established scheduling calendar.

The Edit button allows configuring the time zone and the patching time frequency, which can be limited by weeks of the month, days, and hours.

																	Edit
ecurrence								Ti	me zone								
eek 1								(U	TC) Coordi	nated Unive	ersal Time						
	0h	1h	2h	3h	4h	5h	6h	7h	8h	9h	10h	11h	12h	13h	14h	15h	1
Sunday																	
Monday																	
Fuesday																	
Wednesday																	
Thursday																	

() 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 <u>Jobs</u> section of the Workspaces module.

Portal / Patch / Microsoft patches

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

F	exxible					My organization	Change: Ctrl + K Default: Ctrl + D	Organization Admin	
ଜ	Home	Microsoft	Patches						
Ð	Operations	Microsoft patc	h list						
强	Flows preview								
焰	Tenants 🗸 🗸	Classifications	tions	Products Select products			everity Severity		\sim
Ŀ	Workspaces 🗸 🗸		(0)15 V	Secerproduces			Jeventy		
盦	Patch 🔨	Release Date	\sim						
S	ummary)						
R	eporting Groups	КВ	Patch description		Classification	Product	Severity	Release Date	
Ν	licrosoft Patches	2267602	Security Intelligence Update for Microsoft Defend	der Antivirus - KB2267602 (Definition Updates	Microsoft Defende	r Antivirus -	3/18/25	
Ν	licrosoft patch policies		Intel(R) Corporation - System - 10.29.0.11750		Drivers	Windows 11 Client,	version 22	3/18/25	
Т	argets		Intel(R) Corporation - System - 10.29.0.11750		Drivers	Windows 11 Client,	version 24	3/18/25	
	-		Intel(R) Corporation - MEDIA - 10.29.0.11750		Drivers	Windows 11 Client,	version 22	3/18/25	
			Intel(R).Corporation - MEDIA - 10.29.0.11750		Drivers	Windows 11 Client,	version 24	3/18/25	
		< Previous	Page 1 v of 19718 Next >					Per page: 20	~

- **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.

Portal / Patch / Microsoft patch policies

While <u>Targets</u> 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.

= Flexcible				Partner	Default: Ctrl + D V
🗈 Workspaces 🗸 🕫	Microsoft patch	policies			
🛱 Patch 🔨	🔎 Search for a windows p	atch policy			+ Create
Summary					
Reporting Groups	Name	Target policy targets	Automatic approvals	Actions	
Microsoft Patches	QA	QA	Enabled	🖪 View Detail	
Microsoft patch policies	ILP patch policy	ILP patch target	Disabled	View Detail	
Targets					

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:

绤	Flows	× %	Microsoft p	atch policies > QA					
яå	Tenants	\sim	QA						
	Monitor	~1	Details	Microsoft patches	Automatic approvals	Unacatalogued patches	Uncatalogued automatic approvals		
B:	Workspaces	\sim							Creation date
Ê	Patch	~	Name						Creation date 3/14/25
S	ummary		QA						
R	eporting Groups							Edit	Created by
Μ	icrosoft Patches								
N	icrosoft patch policie	s	Targets						
Та	urgets	1	Nam	ne					
E	Analyzer	\sim	ΔQ						

- Details
- <u>Microsoft patches</u>
- <u>Automatic approvals</u>
- 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.

- **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.

ifications	Products	Su	perseded	Re	lease date	
ect classifications	Select products	~ (s	elect superseded		Mar 19, 2024	
Search patches			All Pending approval Appr —	oved Decl	ined 🗸 Approv	re X Decline
					Last updated at	3/18/25, 1:16:05 PM
КВ	Patch description	Status	Product	Severity	Release Date	Classification
2267602	Security Intelligence Update for Microsoft Defender Antivirus	 Approved 	Microsoft Defender Antivirus	-	3/18/25	Definition Upd
0	Intel(R) Corporation - System - 10.29.0.11750	Pending	Windows 11 Client, version 22	-	3/18/25	Drivers
0	Intel(R) Corporation - System - 10.29.0.11750	Pending	Windows 11 Client, version 24	-	3/18/25	Drivers
	Intel(R) Corporation - MEDIA - 10.29.0.11750	 Pending 	Windows 11 Client, version 22	-	3/18/25	Drivers
	Intel(B) Corporation - MEDIA - 10.29.0.11750	Pending	Windows 11 Client, version 24	-	3/18/25	Drivers

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

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.

Upgrades V	Create new automatic approval rule	×
Products Select products Microsoft 365 Apps/Office 2019/Office LTSC Windows 10 Windows 10 LTSB Windows 10, version 1903 and later Microsoft Edge	Classifications	
Select products Microsoft 365 Apps/Office 2019/Office LTSC Windows 10 Windows 10 LTSB Windows 10, version 1903 and later Microsoft Edge	Upgrades	~)
 Microsoft 365 Apps/Office 2019/Office LTSC Windows 10 Windows 10 LTSB Windows 10, version 1903 and later Microsoft Edge 	Products	
 Windows 10 Windows 10 LTSB Windows 10, version 1903 and later Microsoft Edge 	Select products	
Windows 10 LTSB Windows 10, version 1903 and later Microsoft Edge	Microsoft 365 Apps/Office 2019/Office LTSC	Î
Windows 10, version 1903 and later	Windows 10	
ME Microsoft Edge	Windows 10 LTSB	
	Windows 10, version 1903 and later	
M Microsoft Defender Antivirus	ME Microsoft Edge	
-	MA Microsoft Defender Antivirus	
Windows 11	Wi Windows 11	
		_
	× Cance	+ Create

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.

() 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 <u>Microsoft Updates</u>; 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 <u>Microsoft Updates list</u>.

() 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.
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.

🗅 Workspaces 🗸 🖄	Microsoft patch pol	icies > qa						
🛱 Patch 🔨	QA							
Summary	Details Micro	osoft patches	Automatic approvals Unacatalogued patches	Uncatalogued a	automatic approvals			
Reporting Groups	Classifications		Products	Arri	val date			
Microsoft Patches	Select classificati	ions	Select products	<u> </u>	🖞 Jun 30, 2024	×		
Microsoft patch policies	Search pate	hes)		All Pending approval Appr	oved Declin	ied 🗸 Approv	e X Decline
Targets					-			
🖾 Analyzer 🛛 🗸								
🏵 Microservices 🗸 🗸	KB	P	atch description	Status	Product	Severity	Release Date	Classification
8° Webapps 🗸 🗸	🗢 кв	2267602 <u>S</u>	ecurity Intelligence Update for Microsoft Defender Antivir	• Pending	Microsoft Defender Antivirus		6/30/25	Definition Up
Settings	KB	5060533 2	025-06 Cumulative Update for Windows 10 Version 22H2 fo	 Declined 		-	6/11/25	Security Updat
	😒 КВ	890830 <u>V</u>	Vindows Malicious Software Removal Tool x64 - v5.134.(KB	Pending	Windows 7	-	6/10/25	Update Rollups
	кв	3152281 <u>A</u>	sistencia para actualizaciones de Click-to-Run	Approved	Office 365 Click-to-Run		6/6/25	Critical Updates

Unlisted automated approvals

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

🕒 Workspaces 🗸 🖄 聞 Patch へ	Microsoft patch policies > 0A QA					
Summary	Details Microsoft patches	Automatic approvals Unacatalogue	d patches Uncatalogued automatic app	provals		
Reporting Groups Microsoft Patches					I	+ Create
Microsoft Patches	Classification	Products	Include patches without products	Days after arrival	Actions	
Targets	Critical Updates	Office 365 Click-to-Run	Yes	0	😢 View Detail	
🖺 Analyzer 🗸 🗸	Security Updates	Windows 11, Microsoft Defender Antivir	Yes	0	🖸 View Detail	

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.

Classifications		
Drivers		~
Products		
Select products		
Include patches without pro Days after arrival	oducts	
Enter days after arrival		Days

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.

() INFO

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

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.

Flexxible							My organi	Zation Defau	ilt: Ctrl + D 🗸	Organization Admin	
自 Patch	~	🐞 Fl	exxible - Us	ers							
AnalyzerMicroservices	~	+ Crea	ate Import users	🔁 Export users 🔗 E-	mail login actions $ \smallsetminus $	🕐 Refresh					2
ℬ Settings Information	^	O Se	arch by term	∀ Filter							
Users			Full name ᡝ	E-mail ↑↓	Department ᡝ	Role ↑↓	E-mail login ↑↓	Created by $\uparrow \downarrow$	Updated by $\uparrow\downarrow$	Action	
Roles						and the second second	Disabled			View Detail	Î
Products			And Contraction			(ingener)	Disabled			View Detail	
Modules			the Course (rec.			Contern Address Ref.	Disabled			View Detail	
Integrations			NAME OF TAXABLE	deregantiles.		Trageton:	Disabled			🖸 View Detail	
- Reporting groups							 Disabled 			🛛 View Detail	
			March States			Portal Admin	Enabled			View Detail	
📕 Preview			evious Page 1	✓ of 1 Next >	Showing 1 to 39 of	39 results				Per page: 50	~

The Configuration section consists of the following subsections:

- Organization
- <u>Users</u>
- Roles
- Integrations
- <u>Reporting Groups</u>
- <u>FlexxAgent Versions</u>
- Policies

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.

≡	Flexcibl	le				🐞 My organizatio	n Default: Ctrl + D 🗸	Organization Admin	
Ð	Operations	*	= Organization >						
缢	Flows		✓ General Details	🥖 Edit					
₩	Reports	1	> Branding	O Memb	ers		Products		
焰	Tenants	\sim	> Microservices settings	A Memb			S Products		
Ø	Monitor	\sim	Authentication 87 Products	rth Create	d at		Partner		
Ð	Workspaces	\sim	Modules	Create 11/25/2	2, 2:28:01 PM		Partner		
ġ	Patch	~ '		م Type					
ß	Analyzer	\sim		C Type Wholes	aler				
Ø	Microservices	~		Details					
۲	Settings	~							
o				Name	E-mai		Language en	Country ES	
				Industry Financial service	Defau tes; professional s		Unique code		
	т. 			Description					

Management can be done from the following sections:

- <u>General</u>
- Branding
- Microservices Configuration
- <u>Authentication</u>
- 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.

- 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.

Branding		×
Logo		
Select file	Selected file: No file selected	
Cover image		
Select file	Selected file: No file selected	
Primary color		
0		
Hex Rec	d Green Blue Alpha	
(ffffff 25		
Secondary color		
0		
	🗙 Cancel 🔙 Sa	ve

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.

ρ 	
Q Buscar aplicaciones, configuraciones y documentos	
	Same and the second second
Tados	Imacenadas
	inacenadas
F	Licencia
Flexible	A
	Icono
Desinstalar AnyOesk	
🐱 Limpiar disco (incluye caches de Spotify)	
	Versión 1
	Contexto
	Sesión
- eros	Categoria
•	Red (SP)
• • • • • • • • • • • • • • • • • • •	
E company	
	Q
📑 🚍 🧿 刘 🖻 💁 🖨 😌 🖻	9

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

Microservices settings		×
Folder name (i)		
Enter the folder name		
	🗙 Cancel 🔛 S	ave

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.

Q Sea	rch for apps, settings, and documents
All	
O	Outlook
Ρ	
- 🧠	Paint
	Phone Link System
	Photos
**	Ping google New
Q	
e 🗭	Quick Assist

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.

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.

Disable email/password authentication

Login with email/password enabled Enabled	
 Export C Refresh Search by term 	
Name ↑↓	〒 : Email/Password Login ↑ 〒 :
New Colones (New York, New Yor	\checkmark
	\checkmark

User table

Shows the list of organization members. At a glance, you can see which members have the option to log in via email and password enabled.

User authentication detail

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

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

		User authentication details
		IR
🖷 lagast 🔘 Ballach		
		Microsoft Entra ID
Aug 2 7 1	Brad S Y I. Brad/Association S. Y I. Opp	Job title Phone Last login 6 may 2025, 18:51
		Login count Last IP address
		Email and password
		Last login Login count Last IP address 6 may 2025, 15:56
A CONTRACTOR OF A CONTRACTOR OFTA CONTRACTOR O	1 to 40 of 40 mills	

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.

≡	Flexi	ble						My organization	Default: C	ori	ganization Admin	
Ð	Operations	Â	= Organization >									
绪	Flows		> General > Branding	AL Even	ort 🔿 Refresh							2
Ē	Reports		Sranding Microservices settings	6		2						
я	Tenants		Authentication 87	P Sea	arch by term	`	V Filter					
Ø	Monitor		Products Modules	Enviro	nment 📢	Product type 1	Region †↓	Creation date 🏦	Status †J	Action		
æ	Workspaces			\rightarrow	-	I FlexxClient	West EU Flexxible	10/28/22	 Active 	🖸 View Detail	😂 Agent Settings	
自	Patch			>	in laser	🖬 FlexoDesktop A		10/18/22	Inactive	🗈 View Detail	Agent Settings	
	Analyzer			1.000	-	🚟 FlexxDesktop E		7/22/22	 Active 	🖸 View Detail	🍣 Agent Settings	
Ø	Microservices			>	and the second	RexxCloud		11/3/22	Inactive	😆 View Detail	Agent Settings	
8	Settings	^		>	dan territ	I FlexxClient		10/30/23	 Active 	🛛 View Detail	Agent Settings	
C												

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.

Agent settings

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 <u>remote assistance</u> the organization will use globally. It can be configured to be interactive, unattended, dynamic, or to have no access at all.

Each <u>reporting group</u> that the organization has can edit its own remote assistance configuration to suit its needs.

Edit FlexxAgent settings Environment FxxOne (FXXOne) Remote support Interactive

FlexxAgent Settings - Proxy

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

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

In the FlexxAgent settings, a user with the *Organization Administrator* access level can find two configuration options for the *FlexxAgent* process:

• System proxy settings

- *FlexxAgent Analyzer* automatically detects and uses the proxy settings.
- Flexxible recommends this configuration for the system proxy.

• FlexxAgent detected config

- In this case, FlexxAgent uses the credentials found in the registry if they are defined during installation.
- If not configured, FlexxAgent automatically detects the proxy settings.
- *FlexxAgent Analyzer* uses the detected settings for the Uniform Resource Identifier (URI), user, and password.

Analyzer proxy		
Proxy type		
System proxy settings		\sim
	imes Cancel	🔚 Save

Modules

This tab shows a list of Flexxible product modules available for the organization, as well as those created by the users themselves.

≡	Flexxit	ole				My organization Default:	Ctrl + D V	anization Admin
Ð	Operations	Â	= Organization > Flexxib	le Corp				
嚣			> General > Branding	🔎 Sear	rch for module		All Featured	Secondary + Create
			> Microservices settings				-	
rfe a	Tenants	\sim	Authentication 87 Products			1151	10.00	
Ū	Monitor	\sim	Modules	ţ1	Name	URL	Visibility	Action
B.	Workspaces	\sim	House a	÷	Workspaces		Featured	View Detail
ġ	Patch			÷	Analyzer		Featured	2 View Detail
	Analyzer			÷	8 Monitor	The second second second second	Featured	🗹 View Detail
φ	Microservices			÷	👯 Automate		Featured	C View Detail

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.

Create module	\times
Module type	
Custom	\sim
Name *	
Documentation	
Url *	
https://docs.flexxible.com	
● Featured Secondary	
	× Cancel + Create
Flexible	



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.

Flexxible III					My organization	Change: Ctrl + K Default: Ctrl + D	Organization Admin	
ය Home		Roles						
Operations Flows Preview	+ Create 🗿 Export () Refreed							2
A Tenants V	Create in Export () Refress	¶ Filter						ŕ
B⊐ Workspaces ✓	Name 1↓ Assigned u	sers †↓ Assigned ten	ani†↓ Created by †↓	Updated by $\uparrow \downarrow$	Created at †↓	Updated at 11	Action	
🗘 Microservices 🗸 🗸	Organization Ad	1	1 PLATFORM User	(resultant)	9/9/24	9/9/24	🛛 View Detai 🔑 Permissi 🔨	1
Settings ^	Level 3 Read Only	0	1 PLATFORM User	PLATFORM User	9/9/24	9/9/24	🛛 View Detai 🔑 Permissi 🔨	
Information	Level 3	0	1 PLATFORM User	PLATFORM User	9/9/24	9/9/24	🗹 View Detai 🔑 Permissi 🔨	
Users	Level 2 Read Only	0	1 PLATFORM User	PLATFORM User	9/9/24	9/9/24	🖸 View Detai 🔑 Permissi 🔨	
Roles	Level 2	1	1 PLATFORM User	PLATFORM User	9/9/24	9/9/24	🖸 View Detai 🔑 Permissi 🔨	
	Level 1 Read Only	0	1 PLATFORM User	PLATFORM User	9/9/24	9/9/24	🖸 View Detai 🔑 Permissi 🔨	
	< Provious Page 1 V	of 1 Next > Show	wing 1 to 25 of 25 results				Per page: 50	~
ttps://one.flexxible.com/organization/6439	bee52/c0c0051f17862/home							

Create a new role

To create a new role, click on the New button. A form will open requesting a name for the new role. Once assigned, it will appear in the roles table.

Roles table

The roles table displays the following information:

- Name. Name assigned to the role.
- Assigned users. Users who have this role assigned.
- Assigned tenants. Tenants who have this role assigned.
- Created by. User who created the role.
- Updated by. User who updated the role information.
- Created on. 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.

🕂 Create 🟚 Export 💍	Refresh								×
Search by term	∑ Filter								
Name ᡝ	Assigned users $\uparrow\downarrow$	Assigned tenants $\uparrow\downarrow$	Created by $\uparrow\downarrow$	Updated by $\uparrow \downarrow$	Created at $\uparrow\downarrow$	Updated at $\uparrow\downarrow$	Action		
Organization Admin	1	1	PLATFORM User	1000.000	9/9/24	9/9/24	View Detail	Permissions	^
Level 3 Read Only	0	1	PLATFORM User	PLATFORM User	9/9/24	9/9/24	View Detail	Permissions	
Level 3	0	1	PLATFORM User	PLATFORM User	9/9/24	9/9/24	View Detail	Permissions	
Level 2 Read Only	0	1	PLATFORM User	PLATFORM User	9/9/24	9/9/24	🖸 View Detail	✓ Permissions ∧	
Level 2	1	1	PLATFORM User	PLATFORM User	9/9/24	9/9/24	View Detail	Permissions	
Level 1 Read Only	0	1	PLATFORM User	PLATFORM User	9/9/24	9/9/24	View Detail	Permissions	

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
- <u>Users</u>

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
- <u>Tenant</u>
- Permissions in Portal
- <u>Permissions in Workspaces</u>
- Permissions in Analyzer
- <u>All reporting groups</u>
- <u>Reporting Groups</u>

All tenants

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

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

Tenant

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

Portal Permissions

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

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

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

Workspaces permissions

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

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

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

Analyzer permissions

Gives the option to allow or deny access to Analyzer.

All reporting groups

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

Reporting Groups

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

Users

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

Portal / Settings / Roles / Roles included by default

The default role configurations affect all the reporting groups of the current organization. If the organization is of partner type and has client-type organizations below, or is client type and has sub-organizations below, these should be included as a new entry in the Permissions tab, in two formats:

- All tenants. Allows setting a unified level of access and visibility for all organizations under the root organization.
- Individually. Allows setting different levels of access and visibility for each organization.

Default included roles:

- Level 1
- Level 1 Read Only
- Level 2
- Level 2 Read Only
- Organization admin

This role setting only affects the current organization. It is possible to assign more organizations with different permission levels in the Permissions tab of the same role in edit mode.

Level 1

Users with the Level 1 role assigned will have the following accesses for their organization:

- Portal: User
- Workspaces: Level 1
- Analyzer: No access

This role allows the most common support actions in the Workspaces module, such as providing remote support, sending microservices, power actions, or querying device information. It does not enable access to Analyzer and allows the user to consult information without modifying it in Portal.

Level 1 Read Only

Users with the Level 1 Read Only role assigned will have the following accesses for their organization:

- Portal: User
- Workspaces: Level 1 Read Only
- Analyzer: No access

This role is identical to Level 1, but additionally restricts access to the Workspaces module to visibility only, allowing information consultation in Read-only mode without the possibility of performing support or modification actions.

Level 2

Users with the Level 2 role assigned will have the following accesses for their organization:

- Portal: User
- Workspaces: Level 2
- Analyzer: Access

This role provides access to the Workspaces module at Level 2, which includes all Level 1 support functionalities plus Level 2 functionalities, among which are server, network, location management, wifi networks, and alert configuration. Allows access to Portal as a user and also access to the Analyzer module to query application or device inventory information, as well as user experience, carbon footprint, and more.

Level 2 Read Only

Users with the Level 2 Read Only role assigned will have the following accesses for their organization:

- Portal: User
- Workspaces: Level 2 Read Only
- Analyzer: No access

This role is identical to Level 2, but additionally restricts access to the Workspaces module to visibility only, allowing information consultation in Read-only mode without the possibility of performing support or modification actions.

Organization admin

Users with the Organization admin role assigned will have the following accesses for their organization:

- Portal: Organization admin
- Workspaces: Level 2
- Analyzer: Access

This level is the highest level of access that can be granted to a user. Allows full visibility in the Analyzer module, all Level 2 actions in the Workspaces module, and the ability to modify organization properties in Portal, including the creation and activation of microservices or flows, update policies, and more.

Portal / Settings / Roles / Access levels

Roles allow grouping different levels of access for several organizations and, at the same time, allow grouping different levels of access by module to manage them in a simplified way.

Multiclient environments

The roles of an organization allow configuring access and visibility for the users of the organization, and also allow including the permissions to configure access and visibility to dependent organizations.

An organization is dependent when:

- It is client type and the roles and users are in the partner organization at a higher level.
- It is a sub-organization of a client organization.

Roles are assigned to users and contain the definition of levels of access and visibility, being able to establish different configurations for the root organization and its suborganizations 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

Create a new permission	\times
All tenants	
Tenant *	
Select a tenant	
Portal permissions *	
Select portal permissions	
Workspaces permissions *	
Select workspaces permissions	\sim
Analyzer permissions *	
Select analyzer permissions	\sim
All reporting groups	
Reporting groups	
Select reporting groups	

The levels of access are also defined for each module of the solution:

- Portal
- Workspaces
- <u>Analyzer</u>

Portal

The following roles are distinguished in Portal:

- 0. No access
- 1. Organization Administrator or 1 in the table below

- 2. Read-only organization administrator or 2 in the table below
- 3. User or 3 in the table below
- 4. L1 support team or 4 in the table below
- 5. L1 support team read-only or 5 in the table below
- 6. L2 support team or 6 in the table below
- 7. L2 support team read-only or 7 in the table below
- 8. L3 Engineering Team or 8 in the table below
- 9. L3 Engineering Team Read Only or 9 in the table below
- 10. Billing or 10 in the table below

To access certain functionalities, in addition to access permissions in Portal, access to Workspaces is required, depending on the functionality, with Level 1 or Level 2 role.

These role levels allow configuring visibility and segmented access according to the needs of each organization. The details of the visibility and actions available for each Portal access level are defined in the table below:

Section	Functionality	Action	1	2	3	4	5	6	
Home		Read							1
Operations		Read			*				1
Flows		Read			*	×	×	×	(
		Create		×	**	×	×	×	•
		Refresh		×	**	×	×	×	(
		Delete		×	**	×	×	×	•
Reports	List	Read			×				1
	Detail	Read			×				

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			*			

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				×	×		

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		×	×	×	×	×

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		×	×	×	×	×

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		×	×	×	×	×



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		×	e	×	×		×		×	×
Change to public or private	×	×	×	×	×	×	×	×	×	×
Edit visibility when private		×	0	×	×		×		×	×

(!) IN	IFO
٠	✓ 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.

×
×
×

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 R0 in the table below
- Level 2 or L2 in the table below
- Level 2 read-only or L2 R0 in the table below

Available actions by each role:

Functionality	Action	Ц	L1 RO	L2	L2 RO
UX Panel	View				
Workspaces	View				
Workspaces	Execute operations		×		×
Sessions	View				
Sessions	Execute operations		×		×
Connection Logs	View				
dol	View				
dol	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	×	×		×
Functionality	Action	Ц	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	×	×		

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



Analyzer

The Analyzer module does not allow modifications to the organization or its devices, nor does it segment the functionalities it contains.

Therefore, there are two options:

- You have access.
- You don't have access.

Portal / Settings / Users

User management can be done from Portal -> Settings -> Users. From there, you can view, modify, create, or delete users, as well as assign them a role.

The table shows a list of all the users of an organization. Each row provides the following information:

- Full name. User's first and last name.
- Email address. User's email address.
- Department. Department to which the user belongs within their organization.
- Role. Role type assigned to the user.
- Email login. Indicates if the user has *Enabled* or *Disabled* email and password login to Flexxible consoles.
- Created by. Name of the person who created the user.
- Updated by. Name and email address of the last user who updated the user's information in the Portal.
- View details. Opens a form to edit the user's data or even delete it, depending on the assigned role in the Portal.

Flexxible					My organ	ization Defau	ult: Ctrl + D 🗸	Drganization Admin	
Ê Patch ∨ ◎ Analyzer ∨	🕯 Flexxible - U	sers							
 ♥ Microservices ♥ Settings 	+ Create ↑ Import users	Export users & E	-mail login actions $ \smallsetminus $	🕐 Refresh					2
Information Users	Full name †↓	E-mail ↑↓	Department ᡝ	Role ↑↓	E-mail login ↑↓	Created by ↑↓	Updated by ↑↓	Action	
Roles Products				Taganan Antonio Maria	DisabledDisabled			View DetailView Detail	Î
Modules	No. Conceptor			Taganan	DisabledDisabled			View DetailView Detail	
Reporting groups	-			Portal Admin	 Disabled Enabled 			View Detail	
Preview	< Previous Page 1	✓ of 1 Next >	Showing 1 to 39 of					Per page: 50	~

Create users

In the list view, the New button will open a window with a form to fill out the fields with the information of a new user. In addition to the first name, last name, and email address, you must assign a <u>user role</u> 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.

Flexocible				1		Create user	×
						Name *	
	Flexxible					Please enter text here	
C Analyses managers						Surname *	
O Monarrisa 🤟	· Crass I separate	s 🖷 Esperisson 🔘 Aut				Please enter text here	
0 temp in in	P tagent by tarm.					E-mail *	
Information						Please enter text here	
-	Refinance S	E-mail 1	Department 1	And S	County by	User role *	
Refer	And a Real Processing					Select user role	~
Products	Also Padda					Language *	
Modules	Machinese Province	-				Select language	~
Integrations	the beautre					Department	
Reporting groups	Marco Cardio					Please enter text here	
	Rev Canada Provident					Enable email/password login	
	-	-) at 1 (100)	Density 1 to 20 of 20				× Cancel + Create

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 <u>export</u> to get the Excel file with the correct format. From there you only need to complete it with the required changes, and finally import it.



Export users

To export the user list seen in the list view, just press Export users. This action will download an Excel file with the list of users of the organization and their respective data.

Delete users

To delete a user:

- 1. Go to Portal -> Settings -> Users
- 2. In the table, click View detail.

To delete a batch of users:

- 1. Go to Portal -> Settings -> Users
- 2. Select the users you want to remove.
- 3. In the top menu, the Delete button will be enabled.
- 4. Click Delete.

= rlexxit	ole					Í	My organization	Default: Ct	rl + D 🗸	anization Admin	
🛍 Patch	× ×) 🔊 EL	exxible - Use	**							
Analyzer	\sim		excible - Ose	15							
Microservices	\sim	+ Crea	te Import users 🧕	Export users 🛛 윢 E-mail login ac	tions 🗸 📋 Delete	Ċ Refresh					2
Settings	^	O Sea	irch by term	√ Filter							
Organization											
Information			Full name ↑↓	E-mail ↑↓	Department ᡝ	Role ↑↓	E-mail login ↑↓	Created by \downarrow	Updated by $\uparrow \downarrow$	Action	
Users		0	and Salarian			Custom Admin	Disabled			View Detail	•
Roles		0	Displace	Congramme discontinuous	Development	Custom Admin	Disabled			🖸 View Detail	
Products		0	Namilia Garris			Role	Disabled			🗹 View Detail	
Modules		0	Allerta Cartlin		Lambdaloopers	Custom Role	Disabled			View Detail	
Integrations			1441			Custom Admin Rol	 Disabled 			🛛 View Detail	
	*		Sec. and			Custom Admin Rol	Disabled			View Detail	

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.

= Flexxit	ole						My organization	Default: Ct	trl + D 🗸	rganization Admin	
Patch	×,		exxible - Use								
Analyzer	\sim		exxible - Ose	215							
Microservices	\sim	+ Cre	ate Import users 🕻	🖹 Export users 🤌 E-mail login ac	tions 🖂 📋 Delete	🖒 Refresh					2
Settings	^ I	∫ ⊃ Se	arch by term	Filter							
Organization											
Information			Full name ↑↓	E-mail ↑↓	Department $\uparrow \downarrow$	Role ↑↓	E-mail login ↑↓	Created by \downarrow	Updated by ↑	↓ Action	
Users		0	Last Campber	Sancher of Associate com-		Custom Admin	Disabled			🖸 View Detail	•
Roles		0	Ingelier	Company of the Owner of Street, or other	Development	Custom Admin	Disabled			View Detail	
Products		0	Name and Address of States			Role	Disabled			🖸 View Detail	
Modules		0		sure that the same	Lambdaloopers	Custom Role	Disabled			🖸 View Detail	
Integrations			(second	Contract Contraction Contra		Custom Admin Rol	Disabled			🖸 View Detail	
	•		interime.			Custom Admin Rol	Disabled			View Detail	

Additional options

The options menu in the list view also allows you to Reload the table, which is very useful when you want to refresh the user list, especially when new ones have been created or imported from an Excel file.

The Search by term field allows more precise searches, just enter words corresponding to any user data to quickly access them.

Filter is a more complete alternative to access specific users according to the fields that correspond to their data: full name, email, department, or role.

Portal / Settings / Integrations

From 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 <u>application registration in Azure</u>.
- 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.
- 1. Click on Save.
- 2. Click on Check to verify that the integration has been registered correctly.

Flexocible	Ш					Edit Entra ID	×
0		- Instan	and the second second		And in the	Client ID * Please enter text here	
the radius		* 5,000		Patron	-		
10010		* 5.00	81-85-87-87-97-94	Patron	ARTING A	Please enter text here	
tions.			Name and Address of Street, St	r'n Toffinada		Tenant ID * Please enter text here	
Products							
Workday		Entra ID					
Association and a							
Oglik protots							
-							
						XQ	ancel 🔄 Save

Integration with Intel vPro® Enterprise

Intel vPro[®] is a set of hardware and firmware technologies designed to enhance the security, manageability, and productivity of business computers. The integration of Flexxible Odin with Intel vPro[®] Enterprise will allow you to perform useful additional manageability operations on the physical Windows workspaces that provide support to Intel AMT[®] technology.

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

Requirements

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

Supported operating systems

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

Compatibility with Intel® AMT

Enabling the integration will perform automated operations in all the physical workspaces in your organization to check for Intel[®] AMT support. This process includes the unattended install and uninstall of the <u>Intel[®] EMA Configuration Tool</u> 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 <u>Intel EMA Agent</u> section below to see how to proceed.
- **Ready.** The device supports Intel[®] AMT technology, and Intel EMA Agent has been installed and configured correctly.

😥 Export 🕐 Refresh							
Search by term	Intel vPro: Any	Status: Any	r				
Name î↓	: Intel vPro		IP Address 11	Operating System 1 :	CPU Cores 11	RAM 1	
	Any		192.168.1.107	Microsoft Windows 11 Pro	12	15812	
	O Ready		1921681108	Microsoft Windows fl Pro	6	32565	
	Not supported		192.168.101.31	Microsoft Windows 10 Pr.,	4	8076	
	Requires attention		192.168.15.6	Microsoft Windows fl Pro	8	7945	
		🗸 Update filter	192.168.1.39	Microsoft Windows 11 Pro	12	15812	
	Online	Requires Attention	1921681.40	Microsoft Windows 11 Pro	12	15812	
	Online	Requires Attention	192168.0100	Microsoft Windows fl Pro	12	15812	
	Offline	Requires Attention	192.168.1.77	Microsoft Windows 11 Pro	8	0	
	Online	Ready	192.168.100.20	Microsoft Windows 11 Pro	20	18059	
	Online	Ready	192.168.100.12	Microsoft Windows 11 Pro	20	18054	
	Online	Ready	192168.254109	Microsoft Windows fil Pro	12	15812	
	Offline	Not Supported	192.168.1.37	Microsoft Windows 11 Pro	8	7927	
	Online	Not Supported	172.30.112.45	Microsoft Windows 10 Pr.,	4	0	
	Offline	Not Supported	172.30.126.19	Microsoft Windows Serve	4	16383	

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 <u>Intel® Endpoint</u> <u>Management Assistant (Intel® EMA)</u> 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.

Flexcible 🔛			Partner	Chango Citrl + K Detault: Citrl + D
 Arme Operations Bows receiver 				-
জী Reports असलस्स अन्ते Tenants ৺ ত Monitor ৺ टिंट Workspaces ৺		Enable Intel vPro Enterprise		
Image: Participation PREMIEW > Image: Participation Analyzor HENNEW > Image: Participation HENNEW >	<prestown (1="" 1="" next="" of="" page="" v)=""> Showing it to 4 of 4 re</prestown>	Integration Enabling the integration will provide you with additional information and actions on the workspaces which support the inter vitro* Entegrates technology. The anablement process includes performing automated takes		Per page. (80)
 Settings Information Usons 	Entra ID	In all the workingpaces in your transit to check the support to intel vPoP. Check the following documentation for more defails about this process and please validate the sequirements to make sure that your workspaces are ready to benefit from this feature.		
Roles Products	Cleve ID - Invest ID	Confirm Cancel		
Modulos Integrationa Reporting groups				Check Edit
Eligible products	Intel vPro Enterprise			
🕒 Provlaw	Disabled			Enation

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.

Intel vPro Enterprise	
Status Provisioning Updated by	Updated at 12/12/2024, 9:40:07 AM
Intel vPro Enterprise	
Status Enabled	Updated at 12/12/2024, 9:40:25 AM
Updated by	

Gradually, FlexxAgent will start performing internal checks on the workspaces to determine which ones support Intel® AMT technology. You should wait a few minutes before the information appears in Portal. The wait time depends on the tenant's FlexxAgent configuration and reporting groups.

Go to the Workspaces section and check the information in the Intel vPro Enterprise column. You can also filter the devices by the field value to easily find which ones support Intel[®] AMT technology.

🚱 Export 🕐 Refresh							
Search by term	Intel vPro: Any	Status: Any 🛛 🍸 Fit	or				
Name 11	: Intel vPro		IP Address	: Operating System 1↓ :	CPU Cores 1↓	: ∣ RAM Î↓	:
	🖲 Алу		192.168.1.107	Microsoft Windows 11 Pro	12	15812	
	O Ready		1921681108	Microsoft Windows 11 Pro	6	32565	
	Not support		192.168.101.31	Microsoft Windows 10 Pr.,	4	8076	
	O Requires at	tention	192.168.15.6	Microsoft Windows fl Pro	8	7915	
		🗸 Update filter	192.168.1.39	Microsoft Windows 11 Pro.,	12	15812	
	Online	Requires Attention	1921681.40	Microsoft Windows 11 Pro	12	15812	
	Online	Requires Attention	192168.0100	Microsoft Windows 11 Pro	12	15812	
	Offline	Requires Attention	192.168.1.77	Microsoft Windows 11 Pro.,	8	0	
	Online	Ready	192.168.100.20	Microsoft Windows 11 Pro	20	16059	
	Online	Ready	192.168.100.12	Microsoft Windows 11 Pro	20	16054	1
	Online	Ready	192168.254.109	Microsoft Windows 11 Pro	12	15812	
	Offline	Not Supported	192.168.1.37	Microsoft Windows 11 Pro	8	7927	
	Online	Not Supported	172.30.112.45	Microsoft Windows 10 Pr.,	4	0	
	Offline	Not Supported	172.30.126.19	Microsoft Windows Serve	4	16383	

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.

25.6 / FXXOne Documentation / FXXOne

Flex	× WORKSPACE	s						Cog Off
Level 1 V	Workspaces			▲ # □ □	 1 & ID ()	My Filters •	Filter by workspace group	Text to search P
C. Sensors	Platforms	Machine †	RG Tenant	Power state Last user	Sessions CPU	% RAM	Jptime Code	Power and connection actions + PiexxAgent +
	e 1				 0 0%	0 %		Maintenance (Drain mode)
				interrupte ang	0 010			Refresh Workspace info
La poss	Courte+1							Force check compliance
	$\langle \underline{1} \rangle$							Force update custom fields
								Remote administration +
A6466								Remote assistance
A.								Machine type +
Profile storage					-			Notifications +
Level 2 🕈								Change reporting group
Level 3 >							Instal Intel EMA Agent	Intel vPro (PREVIEW) +
\$ °								

3. Once completed, the device's Intel vPro Enterprise field will show Ready.

-	- Workspaces						
😥 Export 🕐 Refresh							
Search by term	Intel vPro: Ready	Status: Any	Filter				
Name 1	: Status ↑↓ :	Intel vPro Enterp ↓	IP Address	: Operating System 1	CBU Carpa [†]	RAM Î↓	: ∣Туре 1↓
		mentric Enterpri			CPU Cores 1.	KAM I↓	. We It
	Online	Ready	192.168.254.109	Microsoft Windows 11 Pro		15812	Physical
	Online	Ready	192.168.254.109	Microsoft Windows 11 Pro	12	15812	Physical

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.

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.

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.

Flexxible	:::							Hy organi	ization		(Ctrl + K) 🚿	Organization Admin	0
Microservices	~	±		Reporting	groups	3							
Settings	^	+ Create 🏚 Export	💍 Refresh										2
Users		Search by term		√ Filter									
Roles Products		Tenant 🟗	Name †‡	Environment †↓	Product †↓	Fishing p î	Patch policy targ $\uparrow\downarrow$	Policy 11	Action	n			
Modules		[here:[Personal]	1001	10.1000.001	FXXOne		-	VIP		@ A			
Integrations		ine (Trees)	Conception of		FXXOne		-	Ofimático Servidores		(6) A (6) A			
Reporting groups		ton (Trianal	(market)	(Michaeler)	FXXOne		-	-		() A			
Policies		ine (Trice)	1007	(Michelense)	FXXOne		-	-	۳V	@ A	ΦD		
		< Previous Page	1 v of	1 Next > Show	ving 1 to 5 of 5 r	esults						Per page: 50	\sim

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

(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 <u>Reporting Groups</u> section, in the Workspaces module. And the history of a reporting group can be queried from the <u>device detail view</u>, in the same module.

4		Reporting	groups			Tenant *	
+ Courts # Court						Name *	
						Please enter text here	
P least by law.		A same				Environment *	
Seat 1	Rear 1	Enternant 1	Postari : Patrage 1	Party and spinsters in spin-	-	Select environment	
Inco Personal	-	CHE Present B	FEED A		-	Fishing pattern ① Enter a regular expression	
Inco Present	-	CHE Present B	FEEDra		-		
Inc. Proceed	Second second	CHL Personal B	FREAK		-		
Inco Personal		Old Property B	Children .				
Inc. Proceed	-	Chill Present B	Filler				

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 <u>FlexxAgent Version settings</u>, the automatic update will always target the *Production* environment, not the *Early* one.

00 1245	Repor	ting groups	;
+ Create / Edit auto-update		protection \vee 😥 Exp	oort 🜔 Refresh
Search X Disable auto up	date 🌱 Filter		
🮯 Reset auto upd Name †↓	ate Environment †↓	Product ↑↓	Fishing pattern $\uparrow\downarrow$
•	FlexxDesktop	FlexxDesktop Edge	
	FlexxDesktop	FlexxDesktop Edge	

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.

Flexcible	:::					🛍 My org		nange: Ctrl + K efsult: Ctrl + D	Organization Admin	
i Settings	^	Reporting.grou	29 > Oficina							
Information		Oficina								
Billing		Details Roles Users	Magic Links							
Users		🕞 Export 🍐 Refresh								2
Roles										
Products		P Search by term	▼	Filter						
Modules		Name †↓	Assigned users †↓	Assigned tenant: 11	Created by 11	Updated by †↓	Created at 11	Updated at $\uparrow\downarrow$	Action	
Integrations		Admins	Б	1	PLATFORM User		9/9/24	9/12/24	View Detail	1
Reporting groups		Admins2	2	1	PLATFORM User	Industries (Int.	9/9/24	9/25/24	View Detail	
Eligible products		Custom Admin Rol	0	1	PLATFORM User	Collection of the local division of the loca	9/9/24	9/9/24	View Detail	
Policies		Custom Admin Rol.	1	2	PLATFORM User	(openine)	9/9/24	11/21/24	View Detail	

- **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 <u>Magic links</u> 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.

Flexxible 🔢			S My org	anization	Change: Ctrl + K Default: Ctrl + D	Organization Admin	
ය Home	Reporting groups > VIP						
Operations	VIP						
56 Flows PREVIEW	Details Roles Users Magic Links						
بد Tenants 🗸							
🗈 Workspaces 🗸 🗸	🕂 Create 📵 Export 🕐 Refresh						1
🛱 Patch 🛛 🛛 🖉	O Search by term	√ Filter					
🕅 Microservices 🗸 🗸	Created at †↓ Created by ↑↓	Magic link 🏦	Expires at 11	Revoked at 11	Last used al 11	Downloads 11 Action	
Settings ^	12/3/24, 1:02:24 F	https://oneflexxible.com/magic-link?key=b65	12/10/24, 1:02:24	-	-	0 🚫 Revoke	
Information	12/3/24, 12:08:33	https://one.flexxible.com/magic-link?key=91b	12/4/24, 12:08:33	-	12/3/24, 12:18:19	1 🚫 Revolve	
Billing	12/3/24, 11:06:01.	https://one.flexxible.com/magic-link?key=at2	12/8/24, 11:06:01.	-	12/3/24, 11:09:27	1 🚫 Revolve	
Users							

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.

Flexosible III			L Section Process	Create magic link	×
0 may -	technol between H			Expiration * Select expiration 1 day	~
-	from the last Maple			2 days	
teen	+ Cruzz 🗶 Cause 🔿 Refram			3 days	
Pedate) v		7 days 14 days	
Modula .	Departure - Departing to	Magin Ref. 1.	Entrant . Bandine at 1	30 days	
Hagatora	USIA ADAD Ann Bearing	Enter frederingen in	100.000		
Reporting groups	USER HERE AND ADDRESS	Enterferstersterstersteren in			
Ogdate products	USA DEE Anchesen	Collecter Sector Sector Sector Sector			
Page 10	UNIX NOT incheses	Engestrankentik contrage ik			
		a Santa in Colombia		× Cance	el + Create

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

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.

nvironment	
FxxOne (FXXOne)	\sim
Remote support	
Interactive	~

This configuration is set from <u>Products</u>, however, very specific and particular configurations can be made for the reporting 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 <u>installation steps</u>.

Flexxible 🔛			🐞 Mi organización	Administrador de Organización
lnicio				
Operations	i Grup	oos de reporte		
50 Flows PREVIEW				+ Nuevo
න් Inquilinos 🗸 🗸				
🖾 Workspaces 🗸 🗸	Nombre	Patch policy target	Acción	
🛱 Patch 🛛 🛤 🗸	Oficina Barcelona		Ver detalle	Agent Settings
🏵 Microservicios 🗸 🗸				
🕲 Settings 🔷 🔨				
Información				
Usuarios				
Productos				
Módulos				
Integraciones				
Grupos de reporte				

This action can also be performed from the <u>Portal</u> home page.

Flexcible III			Ni Mi	organización	Administrador de Organización	•
	Inicio					
 Operations ^β₀ Flows ■REVIEW ^β₀ ^β	O	<u> </u>	±			
🖾 Workspaces 🗸 🗸	Workspaces	Analyzer	Descargar agente			
Patch PREVIEW Microservicios	Tus productos					
Settings ^	Entorno			Tipo de producto	Acción	
Información	ExxOne			FXXOne	Ver detalle	
Usuarios						
Productos						
Módulos Integraciones						
Grupos de reporte						

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.

= Flexxible					Client	Default: Ctrl + D 💙	Organization Admin
③ Settings スパ	÷	Fle	xxAgent vers	ions			
Users	Ø Set	FlexxAgent versions	🕫 Export 💍 Refresh	Show early versions			
Roles			Export O herresh				
Products	∠ Se	arch by term					
Modules		Name ↑↓ \Xi 🗄	Windows Production	n ी↓	N 코 : I Linux Production ´	치 후 : 🗌 Auto update î	↓ = i i
Integrations		The second second	25.4.1.0	Latest	Latest	No	L
Reporting groups		(Institute)	25.2.1.0	Latest	Latest	No	L
FlexxAgent versions		ing south	Latest	Latest	Latest	No	L
Eligible products		and the second	Latest	Latest	Latest	No	L

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

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

Set FlexxAgent versions	
Windows	
Production	Early
Keep current values	Keep current values
macOS	
Production	Early
Keep current values	Keep current values
Linux	
Production	Early
Keep current values	Keep current values
Auto update	Latest
Keep current values	25.02.502.134
	25.02.502.133
	25.02.501.132
	24.12.501.127
	X Cancel ⊟ Save

The form will also allow you to choose whether or not to set the <u>automatic update of</u> <u>FlexxAgent</u>.

4. Click on Save.

() INFO

When an older version of FlexxAgent (downgrade) is applied to the devices, the current version is automatically uninstalled to install the configured version; additionally, the devices lose access to features corresponding to more recent versions.

Management from Workspaces

Since the FlexxAgent versions are configured for the *Production* and *Early* environments, a user can decide which will apply to the selected devices in the Workspaces module.

Workspaces -> Operations -> FlexxAgent -> Update FlexxAgent

A modal window will request to indicate in which environment this update will be applied: *Early* or *Production*.

se				OK
Production				
Early				
sumen de versiones				
sumen de versiones				
	FlexxAgent	Workspaces	Versión actual	Nueva versión
🖌 Grupo de reporte 🕆	FlexxAgent †	Workspaces	Versión actual 24.10.2.10	Nueva versión 25.4.1.1
Grupo de reporte ↑		Workspaces		

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.

25.6 / FXXOne Documentation / FXXOne

Flexocible III		Crear una nueva directiva $\qquad \qquad \qquad$
0 None None None 4 None None None 5 None None None 6 None None None	C - Directivas	Nombre * Por favor introduce el texto aquí Descripción Por favor introduce el texto aquí
0 Manufacture (1998) 0 Manufacture (1998)	Roman Barrigana Roman and	Belect product
Transfer Production		Grant Access to users to related Organizations 🛛 Yee
Magastern Grapes de reporte Protectos deglines		
		× Cancelar + Nucro

Portal / Portal Guides

rlexxibl	e 🔢			🛍 My	v organization	Organization Admin	
la Home		Home Flexxible Corp					
Operations							
Å Flows	PREVIEW	O	ଭ	<u>ال</u> ع	81	88	
A Tenants		Workspaces	Analyzer	Automate	Monitor	FlexxSecurity	
D Workspaces							
🛱 Patch	PREVIEW 🗸	10 000					
Microservices	PREVIEW 🗸	View more (t2)					Ň
Settings		Your products					
		Environment			Product type	Action	
					FlexxClient	🖸 View Detail	
					Flexo/Desktop Edge	🖸 View Detail	
					FlexoxClient	View Detail	

This section offers resources designed to maximize the use of Portal. It includes detailed instructions on initial and advanced configuration, allowing it to be tailored to specific needs.

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

Portal / Guides / Create and manage workspace groups

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

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).

Flexxible 🔡		My organization (Ctrl + K) ~ Organization Admin
ය Home		
Operations	Contemporation Workspace Groups	
58 Flows PREVIEW	+ Create 😥 Export 🕐 Refresh	2
ස් Tenants 🗸 🗸	Search by term	
🖾 Workspaces 🔨 🔨		
Workspaces PREVIEW	Name †↓ Type †↓	# Workspaces 🕸 Action
Workspace Groups	Static	0 🖸 View Detail
🛱 Patch 🛛 PREVIEW 🗸	Static	0 🖸 View Detail
Microservices		
Settings		
	< Previous Page 1 Volt Next > Showing 1 to 2 of 2 results	Per page: 50 V

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.

 \times

Create workspace group

Name *

Please enter text here

Description

Please enter text here

- 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.

Flexxible 🔛		My organization (Ctrl + K	Organization Admin
	<u>Workspace Groups</u> > Windows		
Operations	Windows		
So Flows Preview	Workspace Group Details Workspaces History Location		
я <mark>е</mark> Tenants 🗸 🗸			
🗈 Workspaces 🔨	Name Windows		♥ 0
Workspaces PREVIEW			O Created by
Workspace Groups	Description		<u> </u>
🛱 Patch 🛛 PREVIEW 🗸	Type Static		Creation date
🋈 Microservices 🗸 🗸		Edit	Creation date 6/6/24
🕲 Settings 🗸 🧹		LOA	

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.

Flex	×wo	ORKSPACES	5						(2	Log Off
Level 1 Y	Work	spaces									
CK dashboard								ter by tag	Filter by workspace group	Text to sear	rch 🔎
Workspaces			□ ♤	ø 6	1 2		Predefined filters Save current filter	ľ) <= <i>∅ ≠ </i> & ■	$\oslash \oslash \bigcirc$	Ø
Sessions		Platforms	Machine †	RG Tenant	Power state	La	Manage Filters Clear filter	U.	% RAM Uptime Code	Status	Connection
Connection logs			Distanci:	(inclusion)	On	5	Workspace Groups Filter by OU		ave as workspace group ave as dynamic workspace group	0 🛰	Ŷ
D jobs					Not reporting	15.	Filter by OS	► 15	0.%	*	
[] Alets				(Insertion Corp.	Not reporting	-	Filter by installed apps	0.96	0 %	*	
Profile storage				(Texasion Corp.	On	1007	100010001	13 %	67 % 9d 21h	0 🛰	Ş
Level 2 >			0	feinder Gerr	Not reporting	1948		0 %	0 %		

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.

Flex	× WORKSPACES						Todos los tenants 🔹 🗘	Cerrar sesión
Ranel de LUX	Workspaces					Mis filtros •		Text to search P
Wardingsamers		9 8 9 7) F <u>r</u>	Filtros predefinidos Guardar el filtro actual Administrar filtros	CPU consumption over 80% CrowdStrike active detections FlexxAgent reporting errors	∰ • ⊠ • •••
Sectores	Plataformas	Máquina	Tenant del RG	Estado	Último usuario	Borrar el filtro Grupos de Workspaces	FlexxAgent version summary Network signal below 40%	Estado Conexión
E Registros de conexión	🗆 🚦 🧼 🍥 🕅			Encendido		Filtrar por unidad organizativa	No Windows Updates during last 30 days Not restarted in the last 15 days	⊘ ブ 🕴
Distance	o 📲 🔶 🎯 🔯	0		Encendido		Filtrar por sistema operativo	Notificaciones aceptadas Notificaciones pendientes de aceptación	⊘ ➤ 🕴
	o 🚦 🔶 🖾 👸			Encendido		0 2%	Outdated FlexxAgent Power State is ON	⊘ 🔻 🕴
	D 🚦 🗇 🕲 🔯	• · · · · · · · · · · · · · · · · · · ·		Encendido		1 2 %	RAM consumption over 90% Reboot-pending workspaces	⊘ 🔻 🕴
Nivel 2	0 🚦 😔 🖾 👸			Encendido		0 5%	Unattended remote assistance enabled With session	⊘ ブ 🕴
	- • • • •	^		Parametrica		A 10	and and and	A ► ■

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

Fle×	WORKSPACES				Todos los tenants • Q Cerrar set	sión
Search Q Nivel 1 Y	Workspaces					
88 Percel do LDC			[Mis filtros +	eta Filtrar por grupo de workspa) Text to search 👂)
Norice aces	🗆 🖓 🔕 👩 🗊			Filtros predefinidos Guardar el filtro actual]
ø				Administrar filtros		<u></u>
Secones	Plataformas Máquina	Tenant del RG	Estado Último usuario	Borrar el filtro	% de RAM Tiempo de acth Código Estado Conexión	
=				Grupos de Workspaces	Guardar como grupo de workspaces	
Registrus de conexión	o 📑 🗇 🕲 🛅 🤒		Encendido	Filtrar por unidad organizativa	Guardar como grupo de workspaces dinâmico 🔉	
_				Filtrar por sistema operativo		
Trabajas	ㅁ 👫 🗇 🚳 🕅 🤒		Encendido	Filtrar por aplicaciones instaladas	_63 % 41d 6h 🥑 🦐 🏺	
	o 📲 \ominus 🔯 🔞 😐		Encendido	0 2%	33 % 41d Sh 🥥 🥆 🏺	

- 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.

Grupos de Workspaces Floxelble Corp		
+ Nuevo 🏮 Exportar		
Nombre 11	Type †↓	# Workspaces 11 Acctón
15 dias sin reiniciar	Dynamic	21 🕑 Ver detaile
	Static	0 🖸 Ver detalle
	Static	0 🖸 Ver detalle
	Dynamic	5 🕐 Ver detalle
	Static	0 🖸 Ver detalle

Workspaces Enter ID groups

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

Create a Workspace group Enter ID

Entra ID groups are created from Portal.

- 1. Go to Workspace groups in the side menu.
- 2. Click on the New button located at the top of the list view.
- 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.

Flexodile III			Create workspace group
·	Q Thursday Wor	kspace Groups	Name * Please enter text here
4	+ Craster # Supert () that		Description Please enter text here
	A fact by term	Type 1 Annual Second Se	Entra ID
Strangers Straps	Sectore 100	ten trans	Type Entra ID group Entra ID administrative unit
t and the second	AT USA		Entra ID group Select group
0 1	New April 10	lyan la	
		ar (100) Basey's Deltants	× Cancel + Create

Entra ID groups require an API connection, which can be configured from Portal -> Settings -> Integrations. Only from there can you check the created Enter ID Group and Enter ID Administration Unit and, therefore, perform operations on them from the Workspaces module.

Manage a workspace group from Portal

To manage a workspace group, click on the name of the desired group and access the following tabs:

- **Details.** Provides general information about the group. From here you can delete the group by clicking on the Edit button.
- Workspaces. Displays the devices that are part of this group. This option allows exporting the list of devices comprising it.

- **History.** Shows a bar graph with the daily number of workspaces that have comprised the group during the last month. You can zoom in on the chart for better reading by selecting the bars you want to enlarge with the mouse. By Reset zoom, the information returns to its original state.
- Location. A geographical location can be added to the group of devices. This value is just a reference, it does not update if users change location.
- Scheduling. From this tab, you can schedule the automatic power-on (Wake on LAN) or shutdown of a group of devices. If the user wants to schedule one of these actions, they must click on the New button and fill in the form fields for Action, Day of the week, and Time UTC.
 - Action. Allows you to choose between Wake on LAN or Shutdown.
 - **Day of the week.** Allows you to select which day of the week the action will take place.
 - **UTC time.** Allows you to specify the exact time to start the action, in the Coordinated Universal Time standard.

The created action will then be displayed in a table, with columns showing the information entered in the form, as well as which user created the action and who updated the schedule and when.

From View details you can edit and delete the scheduled action.

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

Add devices to the static workspace group

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

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

25.6 / FXXOne Documentation / FXXOne

Flexosble III		Import Workspaces ×
0 0	Andream Annual A	Workspaces list * workspace_1 workspace_2 workspace_3
to manyana di	f spottingens ≓in €ipot () bins	
Workspacer Strage		1/20000
8 No		1/2000
0 temp	3	
	to antique the d	
		× Cancel + Import

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.

Flexxible III					🛍 My o	rganization	(Ctrl + K) 🗸 Orga	nization Admin
⊜ Home	Elexable Corp > Workspace Groups							
Departions								
S Flows PREVIEW	Workspace Group Details Wor	kspaces History I	Location					
Aa Tenants 🗸 🗸	_							
🖾 Workspaces 🔨 🔨	🗙 Cancel 🔚 Save 📵 Eq	port 💍 Refresh						
Workspaces PREVIEW	Search by term	Show worksp	baces: Any 🛛 🍸 Fit	ler				
Workspace Groups	Name 11	FQDN 11	IP Address 1↓	Operating Syste 1	CPU Cores 11	RAM 11	Туре †↓	Last User 11
🛱 Patch 🛛 🕅 Patch 🔍		and the second second	10.000.000	Microsoft Windo	12	32581	Physical device	International Contemporation
Ø Microservices V			The party of the local division of the local	Microsoft Windo	4	8073	Physical device	-
Settings		assessment of	100000	Microsoft Windo	4	3985	Physical device	Internet and a second second
	(mage)	100mmillion 1	10022	Microsoft Windo	4	8141	Virtual Desktop	Constanting and the
	trimit:	mail I	interior in the second	Microsoft Windo	4	8141	Virtual Desktop	(contraction)

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.
| rle) | | ES | | | | | \Diamond | Log Off |
|-----------------------|------------|--|----------------------|--------------------|---------------|----------------------------|------------------------|------------|
| Search Q
Level 1 Y | Workspaces | | | | | | | |
| UK deshboard | | | | My Filters 🔹 | Filter by tag | Filter by workspace (| group Text to search | , p |
| workspaces | | |) 🗊 🗊 🖸 | ▲ ■ □ ⊇ | | 🙊 🛰 intel 🖏 :D- | $\odot \odot \bigcirc$ | 3 |
| C
Sessions | Platforms | Machine † RC | i Tenant Power state | Last user Sessions | CPU | % RAM Uptime Code | Status | Connection |
| | o 🚦 🗖 | () :===== :::::::::::::::::::::::::::::: | On | 1 | 63 % | <mark>()</mark> 77% 1h 43m | 💉 ⊘ | Ŷ |

3. Choose the workspace group on which you want to perform actions. 4. Use the multiple options offered by the Workspaces module.

() INFO

For more information about workspace groups, please consult their documentation.

Portal / Guides / Run microservices on a scheduled basis

Microservices allow actions (queries or corrections) on devices. They can be executed directly, from the Workspaces module, or scheduled through Flows, which allow conditional microservices execution.

Schedule a microservice execution

- 1. Click on the Flows option in the left menu of Portal.
- 2. Click on + New to create a new flow. Or select an existing flow if you want to modify it.
- 3. Fill in the fields. Choose whether the flow will be executed at the operating system level or at the user session level.
- 4. Once the fields are filled in, click on Save.

Create new flow	
Name (spanish) *	
TestRow	Show languages
Description (spanish) *	
this is a flow for documentation	Show languages
Type * Cooldown *	10 minutes
Detection only	
	X Cancelar 🔚 Guerdar

- 5. In the flow list view, select the one you just created.
- 6. Click on the Flow tab.
- 7. In the panel, click on the Edit button located on the right.
- 8. To add the first condition, go to the + symbol and click on Add condition. A panel with all available conditions will appear on the right side of the screen. Select Cron Match.

25.6 / FXXOne Documentation / FXXOne



- 9. Add the condition check fields: Check every, Operator and Value, the latter in "cron" programming syntax. Keep in mind that hours are defined in Coordinated Universal Time (UTC).
- 10. Click on Save at the bottom of the panel. In this example, the condition is checked every half hour and the "cron" condition is "every Monday at eight in the morning".

There are many references available to check "cron" scheduling syntax. For example: <u>crontab.guru</u>

Cron Match	×
Check every *	
30 minutes	\sim
Operator *	
At	~)
Value *	
08**1	

- 11. Click on the + symbol located below the condition and select Add action to add the microservice to be scheduled. At this point, additional conditions can be added if needed.
- 12. Select the microservice you want to schedule. In this example, "Clean Disk". Click on the Save button in the upper right corner.

TestFl	ow																							
Overview	Target	Flow •	Notification																					
																			×c	ancela	r í	B	Guardar	
																						_		
						1.1.1		~																
									hon h	/latch														
								5	TON IN	laten														
								<u> </u>																
												A+	0.0 *											
												AL	08											
										1														
										-(+														
										.(T	1													
								A -																
									lisco I	limpio														
							1.1.1																	

In this example, the disk cleaning microservice has been scheduled to be executed every Monday at eight in the morning. To activate the periodic execution of this microservice on devices, it is also necessary to configure the Destination of the flow, including the report groups, devices or groups of devices where execution is required.

There is also the option to notify users about the execution of the flow. To do this, you need to enable the option and fill in the Initial text, Success text, and Error text fields.

(!) INFO

For more information about Flows, please refer to their documentation.

Portal / Guides / Patch policy

The patch policy indicates how the operating system patching of a set of devices belonging to a report group will be managed. Therefore, patching is not done on devices individually.

Define the patch policy

- 1. In the Portal menu, select the Patch -> Targets option.
- 2. Create a new recipient by clicking on the + New button (or select one from the list if you want to modify it). Give it a name and specify the reporting group to which this policy will apply, as well as whether you want to apply a Microsoft update directive.

ame *	
TestPatch	
eporting Groups *	
Select reporting groups	
D Intune Devices	
F FlexxClient	
FE FlexxDesktop Edge	

- 3. Click on the Save button.
- 4. The information of the new policy will appear on the screen.

_		-		
Te	et	Do	te	h
16	οı	га		

Details Schedules		
Name TestPatch	Reporting Groups 1	
Restart after patching No		
Wake on LAN No		
		Edit
Reporting Groups		
Name Intune Devices		

5. To change the behavior of the policy, you can use the Edit button, which allows you

to:

- Change the name of the policy.
- Change the report groups to which the policy applies.
- Select if the devices will restart or wake up via the network (Wake on LAN) after applying updates.
- 6. To change the scheduling of the patch policy application, go to the Scheduling tab -
 - > Edit.

																				Cancelar	Gua
eeks *											Time zon	e *									
nter weeks)	(UTC) C	oordinated	Universal Ti	me							
	Oh	1h	2h	3h	4h	5h	6h	7h	8h	9h	10h	11h	12h	13h	14h	15h	16h	17h	18h	19h	20h
iunday																					
tonday																					
uesday																					
Vednesday																					

() INFO

For more information about Updates, please check its documentation.

Portal / Guides / Enable microservices for the end user

Microservices allow actions (queries or corrections) to be performed on devices, giving the end-user the ability to run them on-demand.

How to enable a microservice for the enduser

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

Fle	exxible	:::		My organiz	Change: Ctrl + K Detault: Ctrl + D	Organization Admin
ŵ	Home		Enabled microservices (PREVIEW)			
₽	Operations		👰 Export 🕐 Refresh 🛛 💿 Table			2
绤	Flows PREVE	•				
₩	Reports PREVI	w	Search by term			
ഷ്ട	Tenants		Name 11	Category †↓	Library 🔃	Actions
æ	Workspaces		Install Windows Updates (Force Restart)	Windows Updates	Flexxible Corp	View Detail
â	Patch PREVI	w ~	Install Windows Updates (Shutdown)	Windows Updates	Flexxible Corp	View Detail
8	Analyzer Meve	• ×	Install Windows Updates (No Restart)	Windows Updates	Flexxible Corp	View Detail
Ø	Microservices PREVI	W ^	Install Windows Updates (Restart Only if it's nedded)	Windows Updates	Flexxible Corp	🖸 View Detail
3	Enabled		Gear Cache Google Chrome	Web Browsers	Flexxible Corp	🕑 View Detail
6	Marketplace		Clear Cache Microsoft Edge	Web Browsers	Flexuble Corp	View Detail
			4			
			< Previous Page 1 Vot Next > Showing 1 to 44 of 4	44 results		Per page: 50 V

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").

Fle	exxible				My organization	Change: Ctrl + K V Organization Admin
ŵ	Home	Í	Enabled microservices > Clean disk			
Ð	Operations		Clean disk PREVIEW			
\$6	Flows PREM	EW				
Ē	Reports PREM		Overview Script Targets Settings License			Go to designer Clone Disable
яã	Tenants	~				
æ	Workspaces	~	Description Clean disk deleting files from temp folders, recycle bin,	lcon		E Author
â	Patch PREM	ew 🗸	vindows updates and execute dism.exe	•		
Ø	Analyzer PREV		Language	Version 3		Published
Ø	Microservices PREM	ew 🔺	PowerShell	3		C 7/17/24
e a	Enabled	-	Scope Workspace	Context System		the literate
						MIT License
G	Marketplace		Operating system Windows	Category Maintenance		
			THINNYS	PPINAR INVESTIGATION		Category Maintenance

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

Fle	اطنكك	2 111				My organization	Change: Ctrl + K Default: Ctrl + D	Organization Admin	
ŵн			Enabled microservices	Clean disk					
Ðo	Operations		Clean disk	PREVIEW					
统 FI	Tows I	PREVIEW	erour aron						
₩ R	Reports (PREVIEW	Overview Script	Targets Settings	Ucense				
я <mark>8</mark> а Ті	l'enants		FlexxWorks	paces executio	on				
R⊃ v	Norkspaces								
₿ P	Patch	PREVIEW 🗸		Allow to execute	Allow to execute (individually)				
× •	Analyzer 🛛	PREVIEW 🗸	L3	~	 ✓				
	Microservices	MIEVIEW 🔨	L2	~	~				
é) B	Enabled		ы	~	~				
	Varketplace							E	Edit

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.

e li	exodble III			Edit end-user execution ×
		a	Discontractification distant	End-user execution Chabled
				Workspace Groups
			international in	FC_Presales_Group,
			Interclated	
4		End on an annual trans	Inclanção:	
		End-user execution		
٠		for our menter		
		transf.	FC_Presales_Group	
		framer annapasi graan		
÷.		No.	Constant with sites in	
3		K.Peaksleve		
		Microsoftine Unarth Find		
				X Cancel

- 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.

All	< Back
File Explorer System	
ڬ Firefox	
Flexible New	^
Borrar caché Google Chrome New	
Borrar caché Microsoft Edge	
🔀 Disco limpio	
Reparación MS Office 365	
Restablecer Microsoft Edge	
🔀 Fotos	
G	
Game Bar System	
Get Started System	
Grabadora de sonido	

Rename the microservices folder

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

Considerations

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

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

Q Sea	Q Search for apps, settings, and documents			
All				
0	Outlook			
Ρ				
- 49	Paint			
	Phone Link System			
<u>></u>	Photos			
×	Ping google New			
Q				
•	Quick Assist			

() INFO

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

Portal / Guides / Set up integration with CrowdStrike

This guide details the processes for establishing CrowdStrike integration on the Flexxible platform.

API Configuration in CrowdStrike

- 1. Access the CrowdStrike portal.
- 2. In the menu, click on Support and Resources -> Api clients and keys.



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



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

 \times

15 / 50

Create API client

Client name

API-Flexxclient

Description

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

API client created					
0	Copy this secret to a safe location. This is the only time we'll show it. If lost, it must be reset and a new secret generated.				
Client ID					
	6				
Secret					
	ප ප				
Base URL					
	ත ව				
	Done				

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.

=	Flexcible			A Cive	Default Call + D 🗸	imin 🔋 🕕
	flows movem rd	<pre> Page 1 viol Showing 1 to 5 of 5 results </pre>				Per page: 50 🔍
4	Reports Tenants V Monitor V	Entra ID				
в) 8	Workspaces 💙 Patch 💙	Name -	Chent ID			
۵	Analyzer V Microservices V	Ciart Secut	Tenant ID			Orek Edit
	Settings A	CrowdStrike				
	kes Klucts Klukes	Chert D Hegon	Client Secret			
Re	ngrations porting groups	eu.t				- 681
rie -	oxigent versions	Intel vPro Enterprise				
		Status Disatiled				

- 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.

Edit CrowdStrike Settings		×
Client ID *		

Client Secret *		
Region *		
eu-1		\sim
2 Delete	× Cancel	E Save

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.

o 📕 🧇 💷 🕅 🚥 📷	On	1	6 %	72.%	4h 14m	\odot >	Φ
o 📕 🗇 😐 🕅 🚥	On	1	3 %	60 %	1d 22h	0 🥆	φ
🗆 📑 🗇 💴 👸 🚥 🛲	On	0	4.%	39.%	1d 22h	⊘ ➤	Φ

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

o 🚦 🧇 💴 🔯 💷	On	1	6 %	72 %	4h 14m	\odot >	Φ
o 📕 🧇 😐 🔯 👘	On	1	3 %	60 %	1d 22h		©
o 📲 🗇 💴 👸 💷	On	0	4.%	39.%	1d 22h	\odot >	Ŷ

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.

Workspa	CE 1.W1022H2EN02					0	₽ · Operations · < >
	Sessions Performance EDR () CrowdStrike (7.23.19508.0)	Crowdints	a sandon	Indows services Diaks Boot history N Creatifier mass installed and working	actifications Security Compliance	Group Policy (GPO) PriP Devices System Sum	nary Reporting groups history
	CPU 0 1015 1015 1017 1017 1017 1017 1017 101		111000000	1333333333333333333333	Memory [©] ***** ***** ***** ***** ***** ***** ***** ***** ***** ******		
	Detections						8.
	Severity	Created	Username	Status	Display name	Description	Command line
0	🗆 🤒 Medium	19/05/2025 14:32:24		Active	1	For evaluation only - benigh, no action needed.	choice /m crowdstrike_sample_detection
	🗆 🤒 Medium	20/05/2025 11:57:44		Active		For evaluation only - benign no action needed.	choice.im.crowdsbilke_sample_detection
	🗆 🤒 Medium	19/05/2025 15:26:30		Active		For evaluation only - benign, no action needed.	choice.im.crowdstrike_sample_detection
© ,	🗆 🥚 Medium	20/05/2025 11:11:12	1000	Active		For evaluation only - benign, no action meeded.	choice /m crowdstrike_sample_detection

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.

Microsoft Azure			,₽ Search	resources, services	, and does (G (/)			🔕 Copil	ot 🛛 🗘	8)	TEXABLE 👫
А	zure service	s									Flexible	Sign out
	+	45	물의	ð á	×		***	•	۲			Concession of Concession, Name
	Create a resource	Static Web Apps	Analysis Services	Translators	Ouickstart Center	Azure Al Foundry	Kubernetes services	Virtual machines	App Services	м	\sim	View account Switch directory ····

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

	Microsoft Entra ID
	All Services (56) Mark
L	Microsoft Entra ID (0)
ļ	Services
ł	Microsoft Entra ID
L	A Microsoft Entra ID Protection
L	🛕 Microsoft Entra ID risk detections
L	Microsoft Entra ID risky sign-ins

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



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

۱

attributes

Register an application	
* Name	
The user-facing display name for this application (this can be changed later)	L.
FlexxWorkspacesApp	 ✓
Supported account types	\r \r
Who can use this application or access this API?	<i>v</i> 0
Accounts in this organizational directory only (flexxworkspaces only - S	ingle tenant)
O Accounts in any organizational directory (Any Microsoft Entra ID tenan	t - Multitenant)
 Accounts in any organizational directory (Any Microsoft Entra ID tenan Xbox) 	t - Multitenant) and personal Microsoft accounts (e.g. Skype,
O Personal Microsoft accounts only	
Help me choose	

- 7. Click Register to complete the application registration.
- 8. Copy and save the Application ID (App ID) and the Directory ID (tenant).

Home > Azure Lab App registration	
₽ Search «	📋 Delete 🜐 Endpoints 🔙 Preview features
Soverview	Got a second? We would love your feedback on Microsoft identity platform ()
Quickstart	
💉 Integration assistant	
Manage	Display name : <u>FlexxWorkspacesApp2</u>
Branding & properties	Application (client) ID : d97a5
-	Object ID :
Authentication	Directory (tenant) ID : 8ea5b
Certificates & secrets	Supported account types : My organization only

Create a client secret

- 1. Access App registrations.
- 2. In the menu, click Manage -> Certificates & secrets -> New client secret.



+ New client secret

- 3. Add a description and in the *Expires* field, select 24 months.
- 4. Click Add.
- 5. Microsoft will provide the client secret and the client ID. You need to save these values because they will not be shown again. If not saved, the client secret must be deleted and a new one created to obtain the value.

Description	Expires	Value 🛇	Secret ID	
Secret for two years	2/12/2026	4aX8	D be0a19	0

Configure permissions for the application registration

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

0	Ove	erview							
++	Preview features								
×	Diagnose and solve problems								
\sim	Manage								
	2	Users							
	🎥 Groups								
	Ĵ	External Identities							
	2	Roles and administrators							
	2	Administrative units							
	-	Delegated admin partners							
		Enterprise applications							
	Devices								
		App registrations							
	(ک)	Identity Governance							
	\$	Application proxy							

4. Search and select the Global Reader option.

Roles and administra	ators All roles						3
x «	🕂 New custom role 📋 Delete custom role 🞍 D	Downlo	ad assignments 💍 Refresh 🖬 Preview leatures 🔗 Got leedback?				
🕹 All roles	() Get just in-time access to a role when you need it usin	ing PIM.	Learn more about PIM \rightarrow				
Protected actions							
 X Diagnose and solve problems > Activity 	A There are currently 29 privileged role assignments. It is	is recon	imended to not exceed 10.				×
> Troubleshooting + Support	(i) Your Role:						
		soft Ent	actions in Microsoft Entra ID. We recommend using these built-in roles for delegating access t rs ID not related to application configuration. Learn more.	o manage broad a	pplicati	ion configu	ration permissions
		^k ⊋ Add	filters				
	Role	τĻ	Description	Privileged	Ťψ	Ass↑↓	Туре
	Global Administrator		Can manage all aspects of Microsoft Entra ID and Microsoft services that use Microsoft Entra identities.	PRIVILEGED		8	Built-in
	Global Reader		Can read everything that a Global Administrator can, but not update anything.	PRIVILEGED		6	Built-in
	Global Secure Access Administrator		Create and manage all aspects of Microsoft Entra Internet Access and Microsoft Entra Private Access, including managing access to public and private endpoints.			0	Built-in

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

<u>step</u>.

Global Reader Assig	Inments
○ ≪	+ Add assignments $ imes$ Remove assignments
🗙 Diagnose and solve problems	
∨ Manage	You can also assign built-in roles to groups now.
Assignments	
Description	Search
> Activity	Search by name
> Troubleshooting + Support	Туре

 \times

Add assignments

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

Global Reader Assi	gnments			
0 «	+ Add assignments $ imes$ Remove assignments	🛓 Download assignments 🖒 Refresh 📑 Manage in PIM 🔗	Got feedback?	
Cliagnose and solve problems				
 Manage 	You can also assign built-in roles to groups now.	eam More 🗗		
🚨 Assignments 🔹 🖈				
Description	Search			
Activity	Search by name Type			
Troubleshooting + Support	All			
	Name	UserName	Туре	Scope
Ь	AzureADAutomation		ServicePrincipal	Directo

Permissions in the Azure subscription

- 1. Log in to Azure Portal.
- 2. Click Subscriptions.

		Sea کر	arch resources, se	rvices, and docs (G+	+/)		👽 Copilot	
Azure servic	es							
+	4	Щ,	[)		†	e	Subscriptions	☆
Create a resource	Microsoft Entra ID	App registrations	Resource groups	All resources	Subscriptions	View		

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



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

Add role assignment		
Role Members Conditions Review + assign A role definition is a collection of permissions. You can use the Job function roles Privileged administrator roles Grant access to Azure resources based on job function, such	e built-in roles or you can create your own custom roles. Learn more 🕫	
P read Name ↑↓	× Type : All Category : All Description 14	Type ↑↓
Reader	View all resources, but does not allow you to make any changes.	BuiltInRole

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

		Select members ×
Add role assi	gnment	Select ① FlexxWorkspacesApp2
Role Members	Conditions Review + assign	No users, groups, or service principals found.
Selected role	Reader	
Assign access to Members	User, group, or service principal Managed identity <u>Select members</u>	Selected members:
Wembers	Name Object ID	FlexxWorkspacesApp2 Remove
Description	No members selected Optional	
		Select Close

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.

=	Flexcible			Siret .	Default Def + D 🤟	Admin 📀
<u>6</u>	Hows Month A	<pre> / Previous Page 1 vint > Showing 1 to 5 of 5 results</pre>				Perpage: 50 V
4	Reports Tenants V					
	Monitor V	Entra ID				
в	Workspaces 🗸 🤟	New .	Chart (D			
	Patch 💙	Client Secret	Terunt ID			
	Analyzer V Microservices V					
	Settings ^					Check Edit
	formation	CrowdStrike				
	Hers					
	oles roducts	Clart G	Client Secret			
	lodules	Region 40-1				
	tegrations	an-1				Edit
	eporting groups					
	exulgent versions	Intel vPro Enterprise				
		Status				
		Disabled				

- 4. Click on Edit and enter the following information:
 - Id. of application (client). Client ID.
 - Secret string. Client secret used for authentication.
 - Id. of directory (tenant). Azure tenant ID.
- 5. Click on Save.



For these credentials to be used in sub-organizations, Share credentials with the selected tenants must be enabled; otherwise, new credentials must be created for each sub-organization.

Portal / Guides / Set up Entra ID integration with Monitor

<u>Monitor</u> 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.

Microsoft Azure			P Search	resources, services	; and does (G (f)			🔮 Copil	ot 🛛 🗘	۲	0 R	FIEXABLE 👫
	Azure servic	es									Fleasible	Sign out
	Create a resource	Static Web Apps	Analysis Services	ঠুু t a Translators	X Quickstart Center	Azure Al Foundry	Rubernetes services	Virtual machines	Co App Services	м	0	View account Switch directory

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

Microsoft Entra ID
All Services (56) Mark
Microsoft Entra ID (0)
Services
Microsoft Entra ID
Apple: Microsoft Entra ID Protection
Microsoft Entra ID risk detections
Microsoft Entra ID risky sign-ins

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

5. Click Application registrations -> New registration.



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

Register an application

GrafanaCloud			
Supported account types			
Who can use this application or access th	his API?		
 Accounts in this organizational direct 	ctory only (only - Single tenant)	
Accounts in any organizational direction	ctory (Any Micros	soft Entra ID tenant - Multitenant)	
 Accounts in any organizational direct Xbox) 	ctory (Any Micros	soft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g.	kyp
Personal Microsoft accounts only			
Help me choose			
Redirect URI (optional)			
We'll return the authentication response changed later, but a value is required for		successfully authenticating the user. Providing this now is optional and it ation scenarios.	can
Web	hat an () a market of	a domain>/login/azuread	

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

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

8. Click Register to complete the application registration.

Create a client secret

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





3. In the *Description* field, write GrafanaCloud, and in *Expires* select 24 months.

Add a client secret		×
Description	GrafanaCloud	
Expires	730 days (24 months)	\sim
	Recommended: 180 days (6 months)	
	90 days (3 months)	
	365 days (12 months)	
	545 days (18 months)	
	730 days (24 months)	
	Custom	

4. Click Add.

5. Copy the key value. This is the client secret value for OAuth.

+ New client secret				
Description	Expires	Value ①	Secret ID	
GrafanaCloudCertificate	12/12/2025	D	8d541	0

API permissions configuration

The necessary permissions for the API should be defined.
1. Find the created application and in the menu click on API Permissions -> Add a permission.

₽ Search «	🕐 Refresh 🛛 🕂 Got feed	lback?
Overview		
Quickstart	The "Admin consent requi	red" column show
Integration assistant	organization, or in organiz	
Manage	Configured permissions	
Branding & properties	Applications are authorized to	call APIs when the
Authentication	all the permissions the applicat	ion needs. Learn i
Certificates & secrets	+ Add a permission 🗸 G	ant admin conse
Token configuration	API / Permissions name	Туре
API permissions	✓ Microsoft Graph (1)	
Expose an API	User.Read	Delegated
App roles		
Mowners	To view and manage consented	permissions for
Roles and administrators	10	8
Manifest		
Support + Troubleshooting		
P Troubleshooting		

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

	PIs Microsoft Graph https://graph.microsoft.com/ Docs 🗗	
What	type of permissions does your application require?	
20000	egated permissions r application needs to access the API as the signed-in user.	Application permissions Your application runs as a backgroun signed-in user.
elect	t permissions	
₽ Sta	art typing a permission to filter these results	
P	Permission	Admin
~ 0	OpenId permissions (3)	
2	email 💿 View users' email address	No
	offline_access ① Maintain access to data you have given it access to	No
~	openid ① Sign users in	No
~	profile ① View users' basic profile	No

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

Configured permissions					
		are granted permissions by users/admins as part of the re about permissions and consent	consent process. The list of configured perm	issions should include	
+ Add a permission 🗸 Gra	nt admin consent	for			
API / Permissions name	Туре	Description	Admin consent requ Status		
∽ Microsoft Graph (4)					
email	Delegated	View users' email address	No		
openid	Delegated	Sign users in	No		
profile	Delegated	View users' basic profile	No		
User.Read	Delegated	Sign in and read user profile	No	Remo	ove permission

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

		pre about permissions and consent	art of the consent process. The list of configured pe	in the should metal
+ Add a permission 🗸 Gra	ant admin consent	t for		
API / Permissions name	Туре	Description	Admin consent requ Status	
✓ Microsoft Graph (3)				
email	Delegated	View users' email address	No	
openid	Delegated	Sign users in	No	
profile	Delegated	View users' basic profile	No	

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 🗸 Gr	ant admin consent	t for			
API / Permissions name	Туре	Description	Admin conser	t requ Status	
✓ Microsoft Graph (3)					
email	Delegated	View users' email address	No	Granted for	
openid	Delegated	Sign users in	No	Sranted for	
profile	Delegated	View users' basic profile	No	🕑 Granted for	

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

Home > App registrations > Grafana			Request API permissions	
Search Overview		lback?	CAll APIs Microsoft Graph https://graph.microsoft.com/ Docs 🔊 What type of permissions does your application require?	
 Quickstart Integration assistant Manage 	The "Admin consent requi organization, or in organiz		Your application needs to access the API as the signed-in user. Your	ication permissions application runs as a background : td-in user.
 Branding & properties Authentication Certificates & secrets 	Configured permissions Applications are authorized to a all the permissions the applicat	call APIs when they are g	Select permission	
API permissions API permissions Expose an API	Add a permission of G	rant admin consent for Type De	The "Admin consent required" column shows the default value for an organic permission, user, or app. This column may not reflect the value in your organ used. <u>Learn more</u>	
K App roles	→ Microsoft Graph (3)		Permission	Admin cor
A Owners	email	Delegated Viv	> IdentityRiskyUser	
8 Roles and administrators	openid	Delegated Sig		
Manifest	profile	Delegated Vi	5 User (1)	
Support + Troubleshooting	To view and manage consented	permissions for individ	User.Read ① Sign in and read user profile	No
13 Troubleshooting	in the second seco			

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

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

API / Permissions name	Туре	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:

Edit app role

Edit app role

Delete	Delete		
Display name * 🕡	Display name * 🕡		
Grafana Viewer	Grafana Editor		
Allowed member types * 🕕	Allowed member types * ①		
 Users/Groups 	 Users/Groups 		
Applications	Applications		
Both (Users/Groups + Applications)	O Both (Users/Groups + Applications)		
Value * ①	Value * 🛈		
Viewer	Editor		
Description * (i)	Description * 🕕		
Grafana read only Users	Grafana Editor Users		
Do you want to enable this app role? ①	Do you want to enable this app role? ①		

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".

♀ Search	« 🔒 Sa	ve 🗙 Discard 🛧 Upload 🚽 Download 🛛 🔊 Go
Overview	The ed	itor below allows you to update this application by directly m
Quickstart		
	40	"long", pull
Integration assistant	41	"lang": null, "origin": "Application",
-	42	"value": "Admin"
lanage	- 44	value : Admin
Branding & properties	44	1
branding & properties	45], "oauth2AllowUrlPathMatching": false,
Authentication	40	"createdDateTime": "2023-12-18T13:13:47Z"
	48	"description": null,
Certificates & secrets	49	"certification": null,
Token configuration	50	"disabledByMicrosoftStatus": null,
Token comgaration	51	"groupMembershipClaims": null,
 API permissions 	52	"identifierUris": [],
	53	"informationalUrls": {
Expose an API	54	"termsOfService": null,
App roles	55	"support": null,
App roles	56	"privacy": null,
Owners	57	"marketing": null
	58	},
Roles and administrators	59	"keyCredentials": [],
Manifest	60	"knownClientApplications": [],
mannest	61	"logoUrl": null,

₽ Search	« 🛛 🖓 Sa	ve 🗙 Discard Upload 🛓 Download 🕴 🛜 Got feedback?
Overview	The ed	itor below allows you to update this application by directly modifying its JSON represe
4 Quickstart		
💉 Integration assistant	45],
integration assistant	46	"oauth2AllowUrlPathMatching": false,
Manage	47	"createdDateTime": "2023-12-13T10:30:06Z",
vanage	48	"description": null,
Branding & properties	49	"certification": null,
	50	"disabledByMicrosoftStatus": null,
Authentication	51	"groupMembershipClaims": "SecurityGroup, ApplicationGroup",
Certificates & secrets	52	"identifierUris": [],
	53	"informationalUrls": {
Token configuration	54	"termsOfService": null,
	55	"support": null,
 API permissions 	56	"privacy": null,
Expose an API	57	"marketing": null
	58	}, "hundresdestdister": [1]
App roles	59	"keyCredentials": [],
Owners	60 61	<pre>"knownClientApplications": [], "logolpl", pull</pre>
- Owners	62	"logoUrl": null, "logoutUrl": null,
Roles and administrators	63	"name": "GrafanaCloud",
	64	"notes": null.
11 Manifest	65	"oauth2AllowIdTokenImplicitFlow": false,

Home > App registrations > GrafanaCloud

Requirements

Once the application registration is done, the organization must provide the following parameters to Flexxible so that they can create the configuration in Grafana.

- Endpoints
 - OAuth 2.0 authorization endpoint (v2)
 - OAuth 2.0 token endpoint (v2)
- App registration
 - Application (client) ID
- Certification & Secrets
 - Secret Value

- Group ID to be configured
- Domain to authorize

Portal / 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:

- <u>Overview</u>
- Tenants consumption details

Overview

Provides global information about the FXXOne subscription that the organization has contracted. It is divided into four sections: Subscription, Consumption for organization, My tenants consumption and Total consumption.

🔯 Subscrip	otion	Consur	nption for
Origin	Tier: A €1.25 / month / workspace up to 100 workspaces	Amount €0.00	Consumption 0 workspaces
Billing Period Dec 01 - Dec 31 Subscription start 14 Apr 2023 Unit Price €0.00	 Secure remote assistance Automated support (L1 & L2) Notifications 	My tena Amount €579.87	ants consumption Consumption 720 workspaces Total tenants 171
		MTotal co Amount €579,87	Consumption 720 workspaces

Subscription

This is an overview of the subscription features. It provides information about the billing period, subscription start date, unit price, and available services. The subscribed plan name is highlighted in orange and Tier specifies the price for a device per month.

The Tier is set considering the service consumption of the partner-type organization plus the consumption of its tenants. Regardless of the plans the tenants are subscribed to, they will always be in the Tier of the organization that manages them.

Consumption for organization

It informs about the number of devices a partner-type organization has subscribed and the billable amount it represents.

() INFO

A device that has uninstalled FlexxAgent will continue to count at the billing level as long as it continues to appear in its reporting group. To remove it, see the <u>steps to</u> <u>remove a device from a reporting group</u>.

My tenants consumption

It informs about the number of devices a partner-type organization has subscribed, the number of tenants these are distributed in, as well as the billable amount they represent.

Total consumption

It informs about the total sum of devices the partner-type organization has subscribed, including its tenants, and the billable amount they represent.

Tenants consumption details

This tab offers a dashboard that graphs the consumption by devices of each of the organization's tenants during the current billing period.

The bottom part shows a table with detailed information about each tenant's subscription:

- Tenant: tenant name
- Plan: name of the FXXOne subscription plan they have
- Consumption: number of devices whose agents have reported in Workspaces
- Consumption date: date of maximum device reporting in Workspaces
- Unit Price: consumption price per agent on a device
- Billable period: subscription billing period
- Total: total billable amount for the subscription



View from a client-type organization

The Billing view of a user whose role is *Administrator* within a client-type organization can only obtain general information about the FXXOne subscription through the Overview tab.

Overview

Provides global data about the FXXOne subscription that the organization has contracted.



Subscription

It provides information about the billing period, subscription start date, unit price, available services and also the trial period of the service, if applicable. The subscribed plan name is highlighted in orange and Tier specifies the price for a device per month. Regardless of the plans the tenants are subscribed to, they will always be in the Tier of the organization that manages them.

FlexxAgent consumption

FlexxAgent consumption is based on the maximum number of devices reporting in the Workspaces module on the same day, for a billing period.

For a device to stop consuming at the billing level, it must not have FlexxAgent installed or belong to any reporting group. If FlexxAgent is not uninstalled from a device that is not in use, it will report to Workspaces again when it becomes active. If the user has uninstalled FlexxAgent from one or more devices and wants them to stop appearing immediately in Workspaces, they must go to Reporting groups in the Workspaces module to remove them. If the user does not perform this action, the device will be automatically removed 21 days after its last report.

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

Flex	× WORKSPACES			Log Off
Search Q Level 1 >	Reporting groups \ VIP			
Level 2 💙			C	Download FlexxAgent
Alert notification profiles				
⚠	Reporting Group			
Alert subscriptions	Name	ld	FlexxDesktop license key ①	Portal Update Date
≣⊨	VIP			> 13/11/2024 -
Event logs	Enable session analyzer	Customer SID	Region	
Locations	True		FXXOne-WE-01	
စွင့် Networks	Proxy type			
IE Notifications				
.	Remote assistance			
O O Reporting groups	UNASSISTED			

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
- <u>Workspaces</u>
- <u>Sessions</u>
- <u>Connection log</u>
- <u>Jobs</u>

Level 2

Offers tools that enable a more detailed diagnosis, such as monitoring, event log filtering, server management, and more. Functionalities available at this level:

- Event log
- Locations
- Networks
- <u>Notifications</u>
- <u>Servers</u>
- <u>Wireless networks</u>

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.

rle <mark>×</mark>		S				\bigcirc		Log Off
Search Q Level 1 💙	Workspaces							
8금 UX Dashboard				My Filters 🔹	r by tag	Filter by workspace group	Text to search	Q
Workspaces		□ \$ 6 1	?	▲ 🗉 🗆	ß	(今 여 / 2 💉 🙊 🗉	00	
Sessions	Platforms	Machine † RG Tenant	Power state	Last user Sessions	CPU	% RAM Uptime Code	Status C	connection
:≡ Ionnection Logs	o 🚦 🗖	Committy (management	On		26 %	0 96 % 15h 49m	⊘ ≫	
D jots	o 👫 🗖	 Matter Matter Matter 	Not reporting	Contract of Contra	0 %	0 %	*	
1 Alerts	D 👫 🗖		Not reporting		0 %	0 %	*	
A. Profile Storage	D 🚦 🗖	C residence manufactures	On		11 %	62 % 2d 8h	⊘ ≫	?
Level 2 >	o 📙 🔶 🛯 🖉	Constant Production	On	and the second se	3 %	34 % 4d 20h	0 >	

In addition to filtering, list views also offer other options, such as exporting the listings and saving the applied filters as user filters.

Filtering Options

To access the grouping and filtering options of the item list, right-click on the header of a column. Below, options will be shown according to the sorting, grouping, visibility, and

filtering of the columns.

Column sorting

The options Sort Ascending and Sort Descending allow you to arrange the values of a column according to the letter or number they start with. For example, if the column % RAM is set to sort ascending, the column values will be arranged so that the first row corresponds to the device with the lowest percentage of RAM used and the last row with the highest percentage. Or if the column Status is set to sort descending, the first row will correspond to the device whose status is *Not reporting* and the last row will correspond to the device whose status is *Off.*

To reset the column sorting, click on Clear sorting.

Grouping by Column

The options Group by this column and Group panel allow creating a group of records for each value of the selected column field.

The difference between them is that Group by this column only considers the selected column for grouping the records, while Group panel allows selecting more than one column for grouping.

User Start ↓	VM	Machine name	Device kind	Machine Type	Reconnection
				Workspace	~
			Ģ	Workspace	~
	energia sue la			Workspace	ب ۲

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.

			Export to 🔹	All	▪ Today	•
User	Start 🔱	VM	Machine name	Device kind	Machine Type	Reconnection
	23/01/2024 8:11:10	85fae6fd-9341-41df-a411- fcc6e338cfca			Workspace	~
	23/01/2024 8:10:10	011dc01f-627d-4275-a75e- 2101b265c9e7	Contraction of the second second	Ģ	Workspace	~
	23/01/2024 8:05:10	93d98084-7a39-4885-8ec1- ede73d434e10			Workspace	~
	23/01/2024 8:04:27	efc56a04-ebb7-4fa8-bea1- 8bdde43ddc91			Workspace	
	23/01/2024 8:03:09	49e7e1a9-5ba0-4b73-9487- 457d3fa626af	Andrew Justice		Workspace	~
	23/01/2024 8:02:07	6a466231-d334-4609-aee1- 0decc99ce60a	COD4.ad.flexible.com	Ģ	Workspace	 ✓

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.

			t to 🔹 All	•	Today •
Start	VM	Machine name	Device kind	Machine Type	Reconnection
23/01/2024 5:32:05	309b6a9c-f474-4322-96b8- c565bafadfa7		Ģ	Workspace	
22/01/2024 19:30:12	9a491ae9-32c1-49c0-8b83- c35997c92b6c	and the second	Ģ	Workspace	~
23/01/2024 8:02:07	6a466231-d334-4609-aee1- 0decc99ce60a		Ģ	Workspace	~
23/01/2024 7:37:17	3916b6e3-7358-45b6-ae5c- d24ac036469b			Workspace	
23/01/2024 8:03:09	49e7e1a9-5ba0-4b73-9487- 457d3fa626af	analy and		Workspace	~
22/01/2024 13:35:07	1589953c-3517-4ab3-be7f- c19ab0e3cf16	ISHIOP MGREGI.		Workspace	
23/01/2024 4:23:10	4f35cff5-6d64-4ade-9d0c- c399aedc7cc8			Workspace	~
23/01/2024 7:58:46	37ab5ffd-891a-4012-899c- d53bd9e58563	DESKTOPUTKSMAT		Workspace	
23/01/2024 8:00:10	3916b6e3-7358-45b6-ae5c- d24ac036469b			Workspace	~

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

Detail Views

By clicking on an item in the table, you can access detailed information. The data is organized into inventory blocks and tabs that facilitate navigation.

Workspaces / Level 1

This level of Workspaces brings together tools for teams that have more direct contact with end users. Includes views of UX Panel, Workspaces, Sessions, Connection Logs, Jobs, Alerts, and Profile Storage.

Flex	×wc	ORKSPACE	S							\bigcirc		Log Off
Search Q Level 1	Work	spaces										
53 UK Deshboard						My Filters	• Filter by tag	5	Filter by wor	kspace group	Text to sear	rch P
Workspaces			□ ♤	S 6	?	▲ ■ □] []	F Z	2 🗯 C	₽ ◊	$\odot \odot$	<i>G</i>
Sessions		Platforms	Machine †	RG Tenant	Power state	Last user Ses	sions CPU	% RAM	Uptime 0	Code	Status	Connection
i Ionnection Logs			()	(Involution)	On		26 %	96 %	15h 49m		0 🛸	÷
D Jobs				Investoria	Not reporting	100000000000	0.95	0 %			*	
L Alerts				-	Not reporting		0 %	0 %			*	
A. Profile Storage				Resultin Colors	On		11 %	62 %	2d 8h		⊘ ≫	(î•
Level 2 >		<mark></mark> 🖓 🖉	 Internet of the second s	Provide Carp	On		3 %	34 %	4d 20h		⊘ ≫	9

Functionalities available at this level:

- <u>UX Dashboard</u>
- Workspaces
- <u>Sessions</u>
- <u>Connection Log</u>
- Jobs

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.

Search Q Level 1 ❤	UX Dashboard	
UX Dashboard		01-September-24 / 30-September-24 🛗 📿 Add widget
Workspaces	Current active sessions ^O ^B	Average logon duration per day ^D
Alerts Alerts Profile Storage Level 2 CMDB	Average boot duration per day [©] [©] ^{50s} ^{40s} ^{30s} ^{20s}	Current active alerts ⁽¹⁾ Others 51 • 53 • 29 • Servers 0 • 0 • 0 • Session hosts 0 • 0 • 0 •

The view is configurable and allows you to segment the data by organization, filter by dates, and select the widgets that will be part of the panel.

The configuration of the widgets included in the panel, as well as their position and size, persists between user sessions, so this configuration only needs to be applied once.

Organization filtering

By default, the organization selector located at the top right of the screen has the 'All tenants' option enabled, allowing the aggregated information of all organizations the user has access to in Workspaces to be viewed. To view the data of only one organization, it must be selected.

() INFO

The organization selector is only visible when the user has access to more than one organization.

Date filtering

The date selector allows you to apply temporary filters to the panel data:

- Predefined filters:
 - Today
 - Yesterday
 - Last 7 days
 - Last 30 days
 - This month
 - Last month
- Custom filters allow you to select start and end date and time.

Widgets

The different information boxes within the panel are called widgets, which can be repositioned, resized, or directly deleted by clicking the \mathbf{x} that appears when hovering the mouse over.

Default widgets

The widgets offered by default in Workspaces are the following:

Current active sessions

Aggregated concurrent active user sessions on the platform over time. This widget displays data filtered according to the date selector.

Average boot duration per day

Organization average boot time (boot) of their devices. This widget displays data filtered according to the date selector.

Average logon duration per day

Organization average login time (login) of their users. This widget displays data filtered according to the date selector.

Maximum concurrent sessions

Maximum number of simultaneous sessions on the platform during the last month, last week, and today (connected and disconnected users). This widget displays data for a specific time period. Not filtered according to the date selector.

Active alerts

Summary of simultaneous active alerts related to different environment elements. Information alerts are shown in green, warnings in yellow, and critical alerts in red. This widget shows real-time data. Not filtered according to the date selector.

Inactive users (last seven days)

Users who have ever connected to a session but did not connect during the previous seven days. This widget displays data for a specific time period. Not filtered according to the date selector.

Workspaces by Internet Service Providers (ISP)

A view of the different Internet service providers in use by the devices. Since these are real-time data, date filtering is omitted.

Workspace by country

A view of the different countries from which the devices connect. Since these are real-time data, date filtering is omitted.

Number of Workspaces per Operating system

This widget shows real-time data. Not filtered according to the date selector.

FlexxAgent version analysis

An analysis of the different versions of FlexxAgent used by the organization and selected operating system, so there is a widget for each supported operating system. This widget shows real-time data. Not filtered according to the date selector.

Top 5 sessions by average duration by user

Top 5 average session duration by user on the platform over time. This widget displays data filtered according to the date selector.

Current sessions capacity

Displays information about the number of sessions that can connect according to the current load in AVD (Azure Virtual Desktop) environments.

- Number of session hosts. Number of session hosts in the host pool.
- Users per host. Number of users that can accept each session host.
- **Total sessions.** Number of maximum sessions according with the number of session hosts and the configuration of each one.
- Available. Number of new sessions that can connect.
- Active. Current number of active sessions.
- Disconnected. Current number of disconnected sessions.
- Load. Current load percentage of the session host according with the current usage and availability. This widget shows real-time data. Not filtered according to the date selector.

Top 10 workspaces by current total used bandwidth

Top 10 devices with the highest currently used bandwidth in KB/s. This widget shows realtime data. Not filtered according to the date selector.

Current session host availability

Displays information about session host availability by host pool in AVD (Azure Virtual Desktop) environments.

- Session hosts. Number of session hosts.
- Available. How many session hosts are ready to accept new connections.
- %. Percentage of session hosts that are available.
- Sessions not allowed. Number of session hosts that are in drain mode and cannot accept new connections.

This widget shows real-time data. Not filtered according to the date selector.

Top 10 current most loaded pooled session hosts

Top 10 current most loaded pooled session hosts in AVD (Azure Virtual Desktop) environments. This widget shows real-time data. Not filtered according to the date selector.

Average logon duration per pool/catalog

Average logon duration of users in the group (Azure Virtual Desktop) or catalog (Citrix environments). This widget displays data filtered according to the date selector.

Top 10 workspaces by current total sessions

Top 10 devices sorted by the current number of sessions. This widget shows real-time data. Not filtered according to the date selector.

Average logon duration per operating system

Average logon duration per operating system. This widget displays data filtered according to the date selector.

Top 10 recent alerts

Top 10 most recent alerts, sorted by severity. This widget shows real-time data. Not filtered according to the date selector.

Top 10 workspaces by current total RAM used

Top 10 devices sorted by the currently used RAM in GB. This widget shows real-time data. Not filtered according to the date selector.

Current AVD resources

The number of devices, host groups, and application groups created in Azure Virtual Desktop. This widget shows real-time data. Not filtered according to the date selector.

Disconnected Sessions

Aggregated concurrent disconnected user sessions on the platform over time. This widget displays data filtered according to the date selector.

Workspaces per broker

Number of devices per agent, grouping by broker. This widget shows real-time data. Not filtered according to the date selector.

Workspace by city

A view of the different cities from which the devices connect. Since these are real-time data, date filtering is omitted.

Workspaces by wireless connection

A view of the different wireless connections in use by the devices. Since these are realtime data, date filtering is omitted.

Workspace by public ip address

A view of the different public IP addresses in use by the devices. Since these are real-time data, date filtering is omitted.

Workspaces per hypervisor

Number of devices per hypervisor. This widget shows real-time data. Not filtered according to the date selector.

Workspaces by operating system and build number

A ranking of operating system and build number combinations sorted by number of devices using each one. This widget displays data filtered according to the date selector.

Workspaces / Level 1 / Workspaces View

The 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.

rle <mark>x</mark>	× WORKSPACES	5				Al	ll tenants	-	2	Log Off
Level 1 V BB Dashboard UK	Workspaces			My Filters •	Filter by tag	Filte	r by workspa	ce group	Text to search	
Workspaces		o 🛛 🖉 🖉 🖓		₽ & > &	₽ ◊ 0 0	Ø	8	Export to	* Ope	rations +
Sections	Platforms	Machine †	Power state	Last user	Sessions	CPU	96 RAM U	ptime	Status	Connection
:= Connection logs	D 🚦 🗖		On		1	22 %	0 86 % 50	5 10h	⊘ ≫	ę
Da jože	D 👫 🗖		Non reporting	-	0	0 %	0 %			
	D 📑 🗖		On		1	3%	57 % 50	d 23h	⊘ ブ	÷
Alerta	D 📑 🗖		Non reporting		0	0 %	0 %			
Profile corage	🗆 🚦 🔶 🚳 🔺		off		0	0 %	0%		0	
Level 2 >	🗆 📑 🗖		On		1	3 %	82 % 2x	11h	⊘ ຯ	÷
смов > ф3 >	D 🚦 🗖		On		1	1 %	66 % 2x	d 8h	⊘ ኈ	ę
282	0 🚦 \ominus 🖪 🔺	1000	On		0	1 %	33 % 50	111h	\odot	9

Filtering

The information displayed on the screen can be customized by adding or removing columns of information and saving the filters used for future queries in the user's profile.

Header filtering options

The top menu concentrates tools, icons for each attribute, which filter the list based on the following criteria:

- Device technology filter:
 - Device type: physical or virtual.
 - Session broker used: Citrix, RDP or unknown.
 - Hypervisor: Hyper-V, Nutanix, vSphere, physical or unknown
- Device state filter:
 - The device has active notifications.

- The device is off.
- The device is in an unknown state for the broker.
- The device is in OK state.

Once a device is selected, or through multiple selection, the Operations button gives access to perform various tasks such as Power and Connection Actions or sending Notifications to users.

In My Filters there are also additional filtering options.

Filtering Options

To access the grouping and filtering options of the item list, right-click on the header of a column. Below, options will be shown according to the sorting, grouping, visibility, and filtering of the columns.

Column sorting

The options Sort Ascending and Sort Descending allow you to arrange the values of a column according to the letter or number they start with. For example, if the column % RAM is set to sort ascending, the column values will be arranged so that the first row corresponds to the device with the lowest percentage of RAM used and the last row with the highest percentage. Or if the column Status is set to sort descending, the first row will correspond to the device whose status is *Not reporting* and the last row will correspond to the device whose status is *Off*.

To reset the column sorting, click on Clear sorting.

Grouping by Column

The options Group by this column and Group panel allow creating a group of records for each value of the selected column field.

The difference between them is that Group by this column only considers the selected column for grouping the records, while Group panel allows selecting more than one column for grouping.

User	Start \downarrow	VM	Machine name	Device kind	Machine Type	Reconnection
					Workspace	~
				Ģ	Workspace	~
		eder Socialett			Workspace	✓

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.

			Export to 🔹	All	• Today	•
User	Start 👃	VM	Machine name	Device kind	Machine Type	Reconnection
	23/01/2024 8:11:10	85fae6fd-9341-41df-a411- fcc6e338cfca			Workspace	~
- construction of	23/01/2024 8:10:10	011dc01f-627d-4275-a75e- 2101b265c9e7	Contraction on the	Ģ	Workspace	~
	23/01/2024 8:05:10	93d98084-7a39-4885-8ec1- ede73d434e10			Workspace	~
	23/01/2024 8:04:27	efc56a04-ebb7-4fa8-bea1- 8bdde43ddc91			Workspace	
	23/01/2024 8:03:09	49e7e1a9-5ba0-4b73-9487- 457d3fa626af			Workspace	~
	23/01/2024 8:02:07	6a466231-d334-4609-aee1- 0decc99ce60a	Contact Service.com	Ģ	Workspace	₹

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.

			ort to 👻 🖌 All	•	Today -
Start	VM	Machine name	Device kind	Machine Type	Reconnection
23/01/2024 5:32:05	309b6a9c-f474-4322-96b8- c565bafadfa7		Ģ	Workspace	
22/01/2024 19:30:12	9a491ae9-32c1-49c0-8b83- c35997c92b6c		Ģ	Workspace	~
23/01/2024 8:02:07	6a466231-d334-4609-aee1- 0decc99ce60a		Ģ	Workspace	~
23/01/2024 7:37:17	3916b6e3-7358-45b6-ae5c- d24ac036469b			Workspace	
23/01/2024 8:03:09	49e7e1a9-5ba0-4b73-9487- 457d3fa626af	and the second sec		Workspace	~
22/01/2024 13:35:07	1589953c-3517-4ab3-be7f- c19ab0e3cf16	pest or weargo.		Workspace	
23/01/2024 4:23:10	4f35cff5-6d64-4ade-9d0c- c399aedc7cc8			Workspace	~
23/01/2024 7:58:46	37ab5ffd-891a-4012-899c- d53bd9e58563	OFERE TOP - THE MARK		Workspace	
23/01/2024 8:00:10	3916b6e3-7358-45b6-ae5c- d24ac036469b			Workspace	~

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 <u>here</u>.
- Filter by Organizational Unit (OU). Visible from the Workspaces view, filters by organizational unit.
- Filter by Operating System (OS). Visible from the Workspaces view, filters by operating system type.

• Filter by installed applications. Visible from the Workspaces view, filters by installed applications.

In the top menu, the icons allow:

- Set predefined filters.
- Reset the default list view.
- Export the list in *.csv or *.xlsx format.
- Depending on the view from which it is activated, the button >-, will give access to various microservices, such as clearing the browser cache or updating the operating system.
- Depending on the view from which the Operations button is activated, different actions will be accessible, such as shutting down devices or sending a notification.

Microservices execution

From the >- button, you can run any microservice enabled for the organization that has *System* as a configured context. This allows the execution of microservices with administrative permissions on the devices. The actions of enabling, creating, modifying, or deleting microservices are performed from the Portal.

Available operations

Depending on the view from which the Operations button is activated (list view or detail view), access to different actions will be provided.

Fle×		5						\Diamond	1	-		Log Off
Level 1 ~ Level 1 ~ UK Deshibberd	Workspaces	□ \$ 8	s 6 7 d 2		My Filters	Power off (not recommended)		Power and connection actio Tags FlexxAgent Maintenance (Drain mode) Refresh Workspace info	2015) 	to se		0
Sessions	Platforms	Machine †	RG Tenant	Power state On	Last user Ses	Log off Force log off Disconnect	i LANJ	Force check compliance Force update custom fields Remote administration	,	ĥ	Reset View Se	
John	0 🚦 🗖	 Married Married 		Not reporting	100000000000000000000000000000000000000	0.96	0.96	Remote assistance Notifications Change reporting group	•	2	Operations	,
Alerts				Not reporting		0 %	0 %	2d 8h	0	*	operations 	•
Profile Storage	□ 📲 🗇 🕺 🛆			On	100000000000000000000000000000000000000	3%		4d 20h	0	*	Ŷ	

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.

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

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.
- <u>Unattended</u>. 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.

- 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.

Workspaces / Level 1 / Workspaces / Detail view

Clicking on the name of a device in the Workspaces list view opens the device details. The interface is structured into four sections:

- Available actions
- General information
- Detailed information
- Tabbed information

Available actions

The detail view allows you to perform the same actions on the active device as in the list view, except for updating FlexxAgent, as well as other actions that are only available in this view.

Available actions:

- Microservices execution.
- Perform actions included in the Operations button.

Microservices execution

From the >- button, you can execute any microservice enabled for the organization that has System as configured context. This allows the execution of microservices with administrative permissions on the devices. The actions of enabling, creating, modifying, or deleting microservices are performed from the Portal.

Operations

From the detail view of a device you can perform the same Operations as in the list view, as well as Edit, Session Analyzer log tracking and OS Patching.
Edit

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

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

The Description field allows adding free text as a description or notes to the device.

When the code and/or description are defined, they will be visible in the general information block of the device, and it will be possible to filter by these fields in the list views.

Session Analyzer trace logging

FlexxAgent Analyzer logs can be configured to include or exclude information by criticality levels. From Operations -> Session Analyzer trace logging you can manage the log level change for FlexxAgent Analyzer.

rle <mark>×</mark>	WORKSPACES						• Q	Log O
Search Q Level 1 💙	Workspace \						Operations 👻 🔇	
K Deshboard	General						Power and connection actions Tags	,
C Sessions	Name	Summary status On	Power state On	FlexxAgent version 24.5.3.4	FlexxAgent status	FlexxAgent last repor 13/09/2024 12:41:1	Edit Maintenance (Drain mode) Refresh Workspace info	,
iii metion Lage	Connection	Subnet 192.168.1.0/24	MAC address 98-FC-84-E5-92-F4	Network changed			Force check compliance Force update custom fields Remote administration	
John L	Sessions 1	Last user	Connected from	Connection time 13/09/2024 1:16	Domain		Remote assistance Machine type	•
A. e Storage	Wireless network	Network signal 95 %	Code 🛈				Notifications	
eiz	Description ①					None Information	Session Analyzer trace logging Changgreporting group	•
els > } >	Tags					Warning Error Critical	OS Patching	•
	Extended					Trace Debug		

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

Operating system update

This option allows managing the update of the device that uses Windows as the operating system.

Flex	× WORKSPACES						• Q	Log Off
Level 1	Workspace \							
88 UK Dashboard						C 🗵 ·	Operations 👻	\geq
Workspaces	General						Power and connection actions Tags	•
Consistent Sensions	Name	Summary status On	Power state On	FlexxAgent version 24.5.3.4	FlexxAgent status	FlexxAgent last report (13/09/2024 12:31:05	Edit Maintenance (Drain mode)	,
∷⊒ Connection Lage	Connection	Subnet 192.168.1.0/24	MAC address 98-FC-84-E5-92-F4	Network changed			Refresh Workspace Info Force check compliance Force update custom fields	
	Sessions 1	Last user	Connected from	Connection time 13/09/2024 1:16	Domain		Remote administration Remote assistance	• •
Ners	Wireless network	Network signal 93 %	Code ①				Machine type Notifications	•
Level 2 >	Description (i)						Session Analyzer trace logging Change reporting group	,
Level 3 >	Tags					Get pending patches Get installed patches Patch OS now	OS Patching	•

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
- <u>Linux</u>
- macOS
- <u>ChromeOS</u>

• Android

Workspaces / Level 1 / Workspaces / Remote Assistance

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

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

Features

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

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.

Types of remote assistance

There are three types of remote assistance:

- Interactive remote assistance
- <u>Unattended remote assistance</u>
- 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.

Remote Assistance

Close



La sesión de Asistencia remota está lista para conectarse.

Contraseña: UgKPXUvDt211720102114_(: 🔲

Para iniciar la sesión de asistencia remota, descargar y abra el archivo de Flexxible Remote Assistance.

Nota: Es posible que deba autorizar la descarga en su navegador.

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.



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

() INFO

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

Dynamic remote assistance

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

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

() INFO

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

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

Although the reporting group to which the device belongs has been configured to receive **dynamic remote assistance**, Workspaces will display the three options to start remote assistance: <u>interactive</u>, <u>unattended</u>, and <u>dynamic</u>. 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 <u>https://ras.flexxible.com</u>, 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 <u>FlexxAgent</u> <u>Settings (Remote Assistance)</u> of its <u>reporting group</u>. From there, you can choose which type of remote assistance devices will have access to.

Edit FlexxAgent settings Environment FxxOne (FXXOne) Remote support Interactive

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 <u>dynamic</u>.

$\leftarrow \rightarrow$	c (west-eu-01.one.w	vorkspaces.flexxible.com/	ina ang sana ang san Ina ang sang sana ang sang sang sang sang			९ 🕁 🖬	। । य
	×w	ORKSPACES		west-eu-01.one.workspa Do you confirm this operation		ice	♀	Log Off
Level 1 🗸	Work	spaces			Aceptar	Cancelar	Filter by workspace group	Text to search
Workspaces						₽ ◊		Operations Power and connection actions
Genalora		Platforms	Machine †	Last user	Sessions	CPU	% RAM Uptime Code	Tags ,
:三 Connection logs					0	O 96	0.96	FlexxAgent , Maintenance (Drain mode) ,
					1	42.96	177 % 49m	Refresh Workspace info
		📑 📀 🚭		(constraint)	1	13.95	🕛 78 % 2d 5h	Force check compliance Force update custom fields
Aleta		.			1	4 96	🕕 78 % 13h 8m	Remote administration ,
Profile storage			0		0	0.96	Start remote assistance Start unattended remote assistance	Remote assistance
Level 2 >			() ====		1	2.96	Start dynamic remote assistance	Change reporting group
			resp.		0	0.96	0 %	
		Count=7						
	<	1 >						Page size 20 *

The remote assistance operation can be <u>activated</u> both from the <u>Sessions</u> view and from Workspaces.

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



Activation file download

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

File for devices with FlexxAgent installed

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

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

Flex				REMOTE ASSISTANCE DESKTOP	Close
Level 1 Level 1 Vertepase Sessors					
Sessions		Machine † RG Tenant	Power state	The remote assistance session is ready to connect.	
:= Connection logs				To start the remote assistance session, download and open the Flexxible Remote Assistance fil	e.
D jobs	o 📲 🗖			Note: You may need to authorize the download in your browser.	
				If you don't have FlexxAgent installed, instead of using .flxra version, you can download <u>.exe</u> versi	on
Aierts Profésitionage	< 1 >				
Level 2 >	Designed by Flexible	e [°] Version 24.10.2.9		1	

File for devices without FlexxAgent installed

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

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



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

Wait for the user's consent.



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

() INFO

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

Processes

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

- FlexxAgent.exe
- FlexxibleRA.exe

RE	Task Manager		Q	Type a name,	, publisher, or	PID to	search
≡		Details					
₽	Processes	Name	PID 20292	Status Running	User name SYSTEM	CPU 02	Memory (ac 117,860 K
4	Performance	FlexxibleRA.exe	20292	Running	3131 EIM	00	6,736 K

Behavior of remote assistance through proxy

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

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

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

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

Otherwise, the AnyDesk binary is launched with autodetect.

Flexxible Tools

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

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



These tools can be executed with the following administrative permissions:

- CMD
- PowerShell
- Registry editor
- Task Manager

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

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

() INFO

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

Workspaces / Level 1 / Sessions

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

Fle×	×w	ORKSPA	CES										\Diamond		Log Off
Search Q Level 1 💙	Text to sear	rch													
UK Dashboard										My Filters 🔹	Filter by	workspace g	roup	Text to search	Q
Workspaces.						Ģ (0	?			8) [f			• Opera	tions 👻
Sessions		Machine †	RG Tenant	Pool / Catalo Device Kind	Machine ty	pi User	Subscription	n. Session ty	pe Id	Connection	s Start Date	CPU	RAM	RTT	Status
		() [30000000] [300000000]	freedile Generation		Device			-	1	Active	10/10/2024 12:53:27	6 %	0,73 GB	0 ms	
eta ata			(maile (mail)		Device				1	Active	08/10/2024 14:55:38	1%	0,78 GB	0 ms	
L Alorts Profile Storage		Internet Internet Internet			Device	14000000		Name of Concession, Name o	1	Active	10/10/2024 22:36:28	15 %	1,66 GB	0 ms	

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 <u>Actions on devices</u>.

List filtering options

The filtering options for the list view are available at <u>filtering-options-in-listings</u>.

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

Notifications

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

() INFO

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

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

GENERAL					
User	Machine ①	Session type ① Workspace	Start Date ① 09/10/2024 8:57:36	Connected from ①	Connected ① Yes
Device kind ①	Session analyzer ① Running	Subscription/Broker ①	Pool / Catalog ①	Delivery group ①	
	e Logon info Notifications	Group Policy (GPO)	User logon his	story ®	
	e Logon info Notifications	s Start Layout init 1,9 s	User logon his 08-00-34.0857 08-00-34.2854 08-00-34.2814 08-00-34.1800 08-00-34.1810 08-00-34.1811	story [⊕]	

Available actions

From the device detail view, it's possible to perform the same actions as in the list view for the active device. This includes:

- Microservices execution.
- The actions included in the Operations button.

Microservices execution

Using the >- button, you can run any of the microservices enabled for the organization that have Session as the configured context. This allows the execution of microservices

under the user's identity. The actions of enabling, creating, modifying, or deleting microservices are performed from the Portal.

Operations

From the Operations button, you can execute the actions detailed in <u>Available Operations</u> for the active device.

General

The general information block of the device contains:

- User. Session user in domain\user format.
- Machine. Device hostname.
- Session Type. Session type, which can be Workspace or application for virtualized application sessions.
- Start Date. Date and time of session establishment.
- **Connected From.** When the selected device is a VDI or similar, it displays the name of the endpoint from which the virtual device is accessed.
- **Connected.** Indicates whether the user is actively connected to the session or if they have disconnected from it.
- Device Type. Virtual or physical.
- Session Analyzer. Indicates whether the FlexxAgent session analysis process is active or inactive.
- Subscription/Broker. If used, the Microsoft Azure or Citrix service that manages user connections to the workspace (e.g., Microsoft Azure Virtual Desktop (AVD), Citrix DaaS, Citrix On-premises).
- Group/Catalog. If used, a collection of machines that defines the specifications of the devices and how they are provisioned to users. e.g. host pools in Azure Virtual Desktop or machine catalogs in Citrix).
- **Delivery Group.** If used, a collection of machines selected from one or more machine catalogs. It specifies which users can use those machines, plus the applications and desktops available to those users.

Tabs

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

- <u>Connections</u>
- Performance
- Login information
- Notifications
- <u>Group Policy (GPO)</u>

Connections

Connection	Performance	Logon info	Notifications	Group Policy (GPO)			
						Today	•
Start	Ļ			End	Endpoint		Reconnection
10/1	0/2024 14:07:10			11/10/2024 0:07:10			×
Com	vt=1						

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

The session end date is only reported for disconnected or closed sessions; while the session remains active, the session end date will remain empty.

Performance

This tab	aroups	araphs	of the	main	performan	ce counters	for the	last two hours.
11110 0000	9.00000	9.001.00	01 0110		p 01 1 01 1 1 04 1	00 0000110010	101 0110	



Graphs are included for:

- **CPU.** Percentage of processor usage for the session, excluding resources used by other sessions or system processes.
- **Memory.** Amount of memory used, excluding resources used by other sessions or system processes.
- User Session Input Lag. The user's input lag refers to the time span between when a user performs an action, such as clicking a mouse button or pressing a key, and when the corresponding response is displayed on the screen or executed.
- Session Round-Trip Time (RTT). Time it takes for a data packet to travel from the user's device to a server or remote destination and then back to the user.

At the top of the tab, a link allows direct access to the diagnostic view for the active session in Analyzer.

Login information

This tab allows you to see detailed information about the user's login times. The view consists of two graphs:

- Duration of last login
- User login history

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

Notifications

Allows you to see if the session has any active notifications and their configuration data. When there are active notifications, a warning is shown at the top of the page.

Group Policy (GPO)

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

Connections Performance Logon info Notifications Group	Policy (GPO)	
Note: GPO info update interval is 10 minutes.		
Display name 1	Last application time	
Type: Machine (Count=18)		
	17/07/2024 17:16	
	17/07/2024 17:16	
	17/07/2024 17:16	

Workspaces / Level 1 / Connection Logs

The connection log allows you to view the historical session logs of users in the organization.

Search Q Level 1	Connection logs							
B글 UK Dashboard						My Filters 🔹	Filter by workspace group	ext to search P
Workspaces			□ Ģ		ß		All • To	oday -
C Sessions	User Start ↓	End	Machine name	Device kind	Machine type	Endpoint	Reconnection Subscription/Brol	ker Pool / Catalog
:= Connection Logs					Workspace		×	
D Jobs					Workspace		×	
Alerts	Contraction of the Contract of the	11/10/2024 12:00:13			Workspace		~	
		11/10/2024 11:55:08			Workspace		×	
Profile Storage	territory and the second second				Workspace			
Level 2 >			-	ø	Workspace	1.0.000	*	

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 <u>Filtering options</u> also available in the Sessions section.

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

rle <mark>×</mark>	×wor	RKSPACES				\Diamond	Log Off
Search Q Level 1	Jobs						
B급 UK Dashboard						My Filters 👻	Text to search ${\cal P}$
U Workspaces					Cana	cel job 🔹 🔹	Today -
C Sessions		Info	Status	Creation date 👃	Start time	End time	Owner
Connection Logs		Microservice on (LS_disk_cleanup) requested by 'Automatic operation trigger'	Completed	11/10/2024 12:03:00	11/10/2024 12:03:00	11/10/2024 12:03:05	Automatic operation trigger
,005							
1 Alerts		Microservice on (LS_disk_cleanup) requested by 'Automatic operation trigger'	/ 🕗 Completed	11/10/2024 11:57:58	11/10/2024 11:57:58	11/10/2024 11:58:03	Automatic operation trigger

The jobs view consists of the following elements:

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

Top options

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

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

Jobs list

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

Detail view

Flex		C Log Off			
Search Q Level 1	Jobs \ Microservice on	(LS_disk_cleanup) re	equested by 'Automatic operation trigg	er'	
88 UK Dashboard				Ø	Show Cmdlets
Workspecies	JOB INFORMATION				
Sessions := Connection Lags	100% Duration: 00:00:05	Name Microservice on (LS_disk_cle anup) requested by 'Automatic operation trigge r'	Status Completed	Start time 11/10/2024 12:03:00	End time 11/10/2024 12:03:05
Jobs Alerts		Owner Automatic operation trigger	Scheduled date 11/10/2024 12:02		

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.

- 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:

- <u>Logs</u>
- <u>Workspaces</u>

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 <u>Considerations about the code to use</u>.

Workspaces

The Workspaces tab allows you to easily see the information of the devices that executed the job, in case of multiple executions.

Job subscription

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

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

Workspaces / Level 2

This level of Workspaces groups functionalities to expand the range of available actions. Includes access to configuration functions that allow sending alerts externally, accessing the unified Windows event log, notifications management, and servers.



Functionalities available at this level:

- Event Logs
- Locations
- <u>Networks</u>
- Notifications
- <u>Reporting groups</u>
- <u>Servers</u>
- <u>Wifi networks</u>

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.

					All tenants - 🗘 Log Off				
Level 1 >	Events logs								
Level 2 Y					My Filters 👻 Text to search 🔎				
Alert notification profiles					C P X · Today ·				
Alert subscriptions	Event log data	Event log data collection is enabled. Event types: Error and Critical, Frequency: 10 minutes.							
	Event date 斗	Level	Source	Machine name	Message				
Locations ***** Networks Notifications	11/10/2024 11:59:48	Error	The support of the second	1000000000	[Thread][The execution request Notifications is not informed. Cause: System.ApplicationException: The execution request Notifications is not informed. at				
O O Reporting groups					Machine name: Process name: FlexxAgent (24.9.1.0)				
Servers	11/10/2024 7:06:33	! Error	Service Control Manager		The Servicio de Google Update (gupdate) service failed to start due to the following error: The service did not respond to the start or control request in a timely fashion.				

() INFO

Events are logged every 10 minutes, although this time can be manually configured from the Workspaces settings.

At the top of the interface, you will find the organization dropdown. If a user has access to more than one tenant, they can choose to view the event log for the selected tenant.



Filtering options

Event filtering allows you to view and select only the items that meet specific criteria, temporarily hiding the rest. The event list supports the same <u>filtering options</u> 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.

	My Filters 👻		Text to search ${\cal P}$		
	User filters	Þ	Filter Docs	h	
Ø	Save current filter		View all of my filters		
	Manage Filters				
	Clear filter				

Manage filters

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

Delete the filter

Allows you to delete the filters applied to the registered event list.

Temporary filter

In the top menu is the temporary filter, which by default shows the events recorded on the current day.



Available filters

- Today
- This week
- This month
- This quarter
- This year

() INFO

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

Detail view

The detail view contains detailed event information:

- Event date. Date of event logging in day and time format.
- Level. Severity of the event.
- Source. Source of the event.
- Event ID. Numeric identifier of the event.
- Log file. Event log file hosting the event.
- Machine name. Hostname of the device logging the error.
- Message. Content of the event message.

Event log information on a device

The detail view of a Windows device allows viewing of event logs for a specific device.

essions Per	formance Jobs	Alerts Event log Connecti	ion logs Wind	dows services Disks Boot history Notifications Security Compliance Group Policy (GPO) PnP Devices	Syste
				Today	•
Event log dat	a collection is enal	bled. Event types: Error and Critica	al, Event	(from agents with version >= 22.10.0.0), Frequency: 10 minutes.	
Date 🗍	Level	Source	Event ID	Message	
10/10/2024 22:07:29	Error	Microsoft Office 16 Alerts	300	Failed to parse element: VersionOverrides StoreId=(null) P1: Apps for Office P4: New Document	
10/10/2024 22:07:29	Error	Microsoft Office 16 Alerts	300	Failed to parse element: VersionOverrides StoreType=Unknown, StoreId=(null) P1: Apps for Office	

Additional event settings

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

Workspaces / Level 2 / Locations

Workspaces supports physical locations as a grouping entity for devices and networks, to which coordinates can be linked for geolocation.

List view

Fle>	WORKSPACES	C Log Off	
Level 1 > Level 2 ~ AD group operations	Locations		My Filters Text to search
Alert notification profiles	Name	Address	
Alert	The state in constant		
subscriptions Ei Event logs	Count=0		
Host pools (AVD)			
ှိပိုင် Networks			

Networks allow associating one or more wireless networks to them, and locations allow associating multiple networks.

Detail view

A location consists of the following information:

- Name. Friendly name of the location.
- Address. Postal address.
- Latitude. Numeric value of latitude.
- Longitude. Numeric value of longitude.

At the bottom, you can see the tabs:

- Networks. Networks identified by FlexxAgent included in this location; contains two options:
 - Link. Allows linking a new network to the policy.
 - Unlink. Allows unlinking a network from the policy.
- Workspaces. Devices included in the location
Workspaces / Level 2 / Networks

FlexxAgent collects multiple network information from devices. When more than five devices report the same network in the same organization, the network is automatically created in Workspaces. These help to automatically maintain an inventory of all networks detected in devices to get an accurate location mapping based on network data.

rle <mark>×</mark>		Q	Log Off			
Search Q Level 1 > Level 2 ~	Networks				My Filters -	
operations	Only networks in use by a minimur	n of 5 workspaces are displayed in th	is list.			
Alert subscriptions	Name	CIDR	Public IP	Gateway	VLAN	Location
Event logs				-	0	
Host pools (AVC)		10,000,000,000	Market Street		0	
Locations		100.000.000.000	0.02200.000	10020800001	0	
Networks			1000-001-000-0001	100.0000000	0	

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

	× WORKSPACES				C Log Off
Search Q Level 1 >	Network				
Level 2 💙					\mathcal{O} \langle \rangle
AD group operations	Name				
Alert notification profiles					
Alert	CIDR	Public IP	Gateway	VLAN	Location
Alert subscriptions	Construction and Constructions	100421120141	100404-004	0	
≣: Event logs					
Host pools (AVD)	Workspaces Wireless networks				
Host pools (AVD)					
-000 Networks	Machine name	Current Subnet	Public IP address	Current machine IP	Network changed
Networks	And the second se	No. 1997 at Realition (1998) Table		10.0011.00	Contraction of Contract

At the top block of the detailed view of a network, there is a list of collected fields:

- Name. Name of the network; by default the CIDR followed by the public IP. Allows customization.
- CIDR. Network CIDR.
- Public IP. The public IP used for internet access from the network.
- Gateway. IP address of the network gateway.
- VLAN. Identify VLAN, if any.
- Location. Location associated with the network. Preconfiguration required.

At the bottom of the interface, there are two tabs:

- Workspaces. Shows the list of devices connected to the network.
- Wireless networks. Displays the list of wireless networks linked to the network. It allows linking or unlinking wireless networks previously discovered by FlexxAgent on the devices with the link or unlink buttons at the top of the list.

Workspaces / Level 2 / Notifications

Notifications are a powerful tool for communicating directly, securely, and effectively with users. Due to their versatility, they are especially useful in service disruption scenarios as they allow communication with users effectively, even when the company's communication infrastructures and tools are not functional.

Notifications section

By default, the Notifications section displays information about active and scheduled notifications. To close them, you need to select the notifications you wish and press the Close notifications button.

As with all list views, you can filter the list content using the tools available in <u>filtering</u> <u>functionalities</u>.

Types of notifications

Workspaces includes two types of notifications that allow you to send different types of messages to users:

- <u>Pop-up Notifications</u>. Allows a pop-up window to be launched to the user with a message that the user can close with a click.
- Notifications. Designed for service disruption events where corporate communication channels might not be available. They are used when ensuring the message reaches users as quickly as possible to avoid a high volume of users trying to contact the support department.

Popup notifications

Sending notifications is available in the Sessions and Workspaces sections of Level 1. To send a popup notification, select the target sessions or devices and execute:

- Operations -> Notifications -> Send pop-up message.
- Specify the message and click 0k.

				All tenants	Ŧ	Ç	Log Off
Custom operations		Z_Host X · ⟨?⟩ (♡) (F	ilter by work:	space group Export to	Text to search	rations
	Last user	Sessions	CPU	% RAM	Uptime	Status	Connection
		1	4 %	. 78 %	4h 14m	⊘ 🛰 🙊	ê
		1	5 %	46 %	4h 53m	⊘ ≫ Ŗ	ø
		0	1 %	34 %	3d 11h	⊘ Ŗ	ģ
						Page size: 2	0 -

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

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



Notifications

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

While on screen, notifications reserve that space in such a way that the user can no longer occupy it with their applications. This is a mechanism to ensure that the user has the message visible.



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

To configure and launch a notification, the following is required:

- Define a time zone.
- Set start and end date and time.
- Choose between the three levels of severity:
 - Informative. Will generate a gray notification.
 - Maintenance. Will generate a yellow notification.
 - Technical Issue. Will generate a red notification.
- **Request Acceptance.** Enables a button to allow obtaining feedback from the user; once accepted, it closes for the user.
- Disable Minimize. Activated prevents users from minimizing the notification.
- Message 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.

Workspaces / Level 2 / Reporting groups from Workspaces

The Reporting Groups view from the Workspaces module allows you to see the status of the reporting groups created in the organization. It shows general information about the devices that make them up and offers the possibility to download FlexxAgent onto them.

List view

The list view shows a table with the listing of the report groups, according to their ID number, name, and corresponding organization.

At the top, there are a series of buttons that allow actions on the list of report groups.

- My filters. Allows managing filters to search for reporting groups.
- Text to search. Free search box to find groups matching the inserted term.
- Refresh. Used to reload the list of reporting groups after applying search filters.
- Reset all settings made for this view. Returns to the initial settings of the list.
- **Export all items.** Allows downloading the list of reporting groups in CSV and XLSX formats.
- **Download FlexxAgent.** FlexxAgent will be downloaded to the selected reporting groups.



Download FlexxAgent

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.

Flex	WORKSPACES		C Log Off
Search Q Level 1 > Level 2 ~ Alert notification profiles	Reporting groups		My Filters
Alect subscriptions	ld Id	Name †	Tenant
≣: Event logs		physical	rem://www.iii
		Second se	10000 (Dimension)
		200 E	(mergel/mergel)
Networks	Count=3		
Notifications			Page size 20 *

A window will open to download the FlexxAgent installer.

Download FlexxAgent Installer				OK Cancel
Download a .zip file to instal	l or repair FlexxAgent on machine	es comr	nunicating through this messaging s	ervice.
Target processor architecture	x64	*	Generate standalone installer (off	line)
Please refer to <u>http://5fbe84</u>	0348819.helpdocsonline.com for	r inform	ation on the FlexxAgent-Installer.exe	e command line arguments.

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

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

For other installation options, you can consult the <u>FlexxAgent</u> documentation.

Detail view

To obtain specific information about a report group, you need to select one in the list view table.

The detail view offers specific data about the selected report group: name, ID, FlexxDesktop license key, Portal update date, whether it has an Analyzer session enabled, client SID (security identifier), region, types of proxy and remote assistance enabled.

Fle <mark>x</mark>	WORKSPACES		Flexoible	• Q Log Off
Search Q Level 1 >	Reporting groups			
Level 2 ¥			C	Download FlexxAgent
profiles	Reporting Group			
Alert subscriptions	Name	ld	FlexxDesktop license key ①	Portal Update Date
≣:	(Ministration)			• 06/09/2024 ~
Event logs	Enable session analyzer	Customer SID	Region	
Locations	True ~		residential -	
Networks	Proxy type			
III Notifications	Sector prop official -			
~	Remote assistance			
Reporting groups	UNASSISTED			

Devices

The detail view of the report groups also presents specific information on three areas:

Devices

This is the list of devices that make up the report group being consulted. When it comes to a group that uses the fishing pattern to add devices, the configured RegEx term appears in a top box, as well as the id associated with the report group being queried.

25.6 / FXXOne Documentation / FXXOne

IP Notifications	Devices Devices history Users			
Power management policies (AVD)	Fishing pattern	^EquiposEstandar*	Fishing pattern scope	
Power management activity (AVD)				Image: Comparison of the second se
~	Name	User	St	atus 🕆
Reporting groups			Ur	nknown
Servers	Count=1			
(WiFinetworks	< 1 >			Page size 20 •

Devices history

It provides the name and the date of incorporation of the devices to the report group, also whether they have been assigned the group manually or automatically and the source and destination groups to which the devices have belonged.

Users

This is the list of users who belong to the report group. La tabla informa sobre el inquilino y rol que tienen asignados dentro de la organización

Workspaces / Level 2 / Servers

Flex								\Diamond		Log Off
Search Q Level 1 >	Servers									
Level 2 ¥						My Filters	• Filter by tag		Text to sea	rch P
AD group operations							3	x •	-	Operations 👻
Alert notification profiles	Server type †	Subscription	Name †	RG Tenant	Power state	CPU	% RAM	Code	Uptime	Connection
Alert	None			Constant Const	On	5 %	60 %		24d 11h	φ
subscriptions Ei Event logs	Count=1								Page size	20 -

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 perform the Machine Type->Server operation.

More information on how to include a device in this list.

List view

The list view contains all servers configured as such in Workspaces and allows the same actions with the devices listed in the Workspaces view.

Available operations

From the list view, at the top right of the interface, the following tools are included:

- Filtering Options
- <u>Microservices</u>
- <u>Operations</u>

Filtering options

This view allows the same *filtering functionalities* available in Workspaces.

Microservices

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

Operations

The Operations button allows executing the same <u>device management actions</u> as the Workspaces view.

Detail view

Flex	FIEXWORKSPACES									
Search Q Level 1 >	Servers	10. Texa (10. 10.								
Level 2 💙					0 2 •	Operations • <				
Alert notification profiles	General Name	Status On	Power state On	FlexxAgent version 24.9.1.1	FlexxAgent status	FlexxAgent last report ① 11/10/2024 13:30:06				
Alert subscriptions	Domain	Connection	Subnet	MAC address						
Ei Event logs	Code	a anna na								
Heat pools (AVD)	OU									
etvorks etvorks	8.									

The detail view of a server, in addition to the operations available at the top of the interface, contains the following sections:

- General information
- Extended information
- Specific information segmented into tabs at the bottom

General

The general information block of the device contains:

- Name. Device hostname.
- Status. Power status (on-off).
- FlexxAgent Version FlexxClient version number.
- FlexxAgent Status. Execution status of FlexxAgent (*Running* or *Stopped*)
- Last FlexxAgent Report Date. Date of last report received from FlexxAgent on the device.
- Domain. Domain to which the device belongs.
- Connection Type. Type of connection used by the device (*Ethernet* or *Wireless*)
- Subnet. Network addressing.
- MAC Address. MAC identifier.
- Code. Allows a string to be set as a code.
- **Network Changes.** Indicates if the device has changed its network configuration recently.
- Tags. Allows associating identifying tags.
- OU. Organizational unit of the domain where the device account resides.

Extended

The extended information block of the device contains:

- RAM. Total amount of RAM.
- Cores. Number of processor cores.
- IP Address. IP Address of the device.
- Windows Edition. Operating system edition.
- OS Build. Operating system build number.
- **Uptime.** Duration the device has been running since the last start or restart; note that if fastboot is enabled, the device only turns off when restarted.
- Fastboot. Indicates if the server has fastboot enabled.
- Last Windows Update. Date of last patch application.
- Last Boot Duration. Duration of the boot of the last start.
- Pending Restart. Determines if the device has a pending restart to apply updates.
- System Disk. Indicates the used space of the system disk.

- **Public IP and ISP.** If public IP data collection is enabled, it shows the public IP and provider.
- **Region.** If it is an Azure virtual machine, it will display the Azure region of the host.
- BIOS Manufacturer. Manufacturer of the BIOS.
- BIOS Version. Current BIOS version.
- SMBIOS Version. Current SMBIOS version.
- BIOS Serial Number. Unique identifier of the BIOS.
- Session Analyzer. Indicates the status of the FlexxAgent Analyzer process:
 - Not configured. FlexxAgent is configured not to start Session Analyzer.
 - **Disabled.** FlexxAgent does not start Session Analyzer because it has been disabled via the 'AvoidLaunchAnalyzer' registry key.
 - Configured. FlexxAgent is configured to start Session Analyzer in all user sessions.
 - **Installed.** FlexxAgent will not attempt to start Session Analyzer because Session Analyzer is already installed on the device.
 - Not compatible. FlexxAgent does not start Session Analyzer because it is not compatible with the device's operating system (e.g., a 32-bit version of Windows).

Tabs

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

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

Job

Sessions Performance Jobs	Alerts Event log Conn	ection logs Windows services Disk	s Boot history Notifications	Security Compliance G	Froup Policy (GPO) PnP Devices Syste
Info	Status	Creation date \downarrow	Start time 👃	End time	Owner
Mengan-Yakiranti Mengan-Yakiranti	 Completed 	25/09/2024 18:29:56	25/09/2024 18:29:56	25/09/2024 18:30:05	
and a second s	Completed	19/07/2024 10:38:47	19/07/2024 10:38:47	19/07/2024 10:38:57	the second second
angan balanca 'anga Salanca 'an anti'	Completed	19/07/2024 9:30:45	19/07/2024 9:30:45	19/07/2024 9:31:02	
Count=3					
$\langle \underline{1} \rangle$					Page size 20 *

All actions performed from servers on one or more devices are audited in the job queue. This tab allows you to check the jobs performed for the active device without having to go to the section.

Performance

In the performance tab, graphical information about CPU, memory, and bandwidth usage is displayed.

Alert

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.

	Image: Comparison of the second se
Active alerts: - [Critical] Low storage free space % for Workspace: Drive: C: Free space: 2 GB, Used Percentage: 98%	
General	

Event Logs

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

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

Disks

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

Boot history

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

Security (EDR)

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



Group Policy (GPO)

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

PnP Devices

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

Sessions	Performan	ce Jobs	Alerts	Event log	Connection logs	Windows services	Disks	Boot history	Notifications	Security	Compliance	Group Policy (GPO)	PnP Devices
Device m	nanager entri	es with err	or state										
	last PNP device 24 15:03:44	s update											
												D Ope	erations -
N	ame \downarrow					Dete	ction dat	e				Class	Device ID
	isco AnyConne	ect Virtual N	liniport /	Adapter for	Windows x64	27/1	/2023 13	3:51:47				Net	ROOT/NET/0000
c	lount=1												
< <u>1</u>	>												Page size 20 *
PnP ever	its												
	ction	Date \downarrow				User		Caption			(Device ID	
D PI	lugged in	17/07/202	4 16:01:	37				Generic PnP M	onitor		t	DISPLAY\CTX0466\2&1	23C1CA0&0&UID1
U	nplugged	17/07/202	4 14:40:	22				Generic PnP M	onitor		(DISPLAY\CTX0466\2&1	23C1CA08.08.UID1

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

Workspaces / Level 2 / Wireless networks

FlexxAgent collects multiple network information from devices. When FlexxAgent identifies the use of a wireless network, it is automatically created in Workspaces. These help maintain an inventory of all networks detected on devices to get an accurate location mapping based on network data. It is possible to associate it with <u>Networks</u> and <u>Locations</u> allowing to build a network inventory, the connected devices, the network operators in use, and much more.

List view

The list view allows you to see the relation of wireless networks discovered by the agent. You can search, filter, sort, show or hide columns, and more.

It also allows selecting a wireless network from the list and marking it as a trusted network; in that case, if FlexxAgent detects the network again in more than five devices, it will recreate it.

Detail view

Flex	WORKSPACES				\Diamond	Log Off
Level 1 >	WiFi network					
Level 2 💙						$[C] \langle \rangle$
AD group operations						
~	SSID	Public IP		Source device		
Alert notification profiles	10000000_0112_0000	NAMES OF T			Reliable	
Alert	ISP	City		Country	Network	
subscriptions	Conductors of Chargest 1994	Madrid		ES		
≣: Event logs						
Host pools (AVC)					ð	X · Operations ·
•	Machine name	U	lser name	Power	state	
Locations	No data to display					
one one Networks	Count=0					

At the top block of the detailed view of a network, there is a list of collected fields:

- **SSID.** Network name; by default, the CIDR followed by the public IP. Allows customization.
- Public IP. The public IP used for internet access from the network.
- Source Device. Name of the device that first declared the wireless network.
- Trusted. Indicates if this wireless network has been marked as trusted.
- ISP. Connectivity provider.
- **Population.** Indicates the population from where the internet connection is established.
- Country. Indicates the country from where the internet connection is established.
- Network. Allows associating this wireless network with a Network.

Connected devices to the network are displayed at the bottom.

Workspaces / Workspace Guides

Flex	×w	ORKSPACE	S						\Diamond		Log Off
Search Q Level 1	Work	spaces									
67 UK Deshboard						My Filters 🔹 Filt	er by tag	Filter by wor	kspace group	Text to searce	.h P
Workspaces			□ �	ø 6	?	▲ щ □ 2	D	P & > 3	₽- ◊	$\odot \odot$	Ø
D Sessions		Platforms	Machine †	RG Tenant	Power state	Last user Sessions	CPU	% RAM Uptime	Code	Status	Connection
i ionnection Logs				Translate Colors	On		26 %	🕛 96 % 15h 49m		⊘ ≫	Ŷ
D jobs			Internet	(manufacture)	Not reporting	Contraction and Co.	0 %	0 %		*	
L. Alerts				-	Not reporting		0 %	0 %		*	
A. Profile Storage				President and	On		11 %	62 % 2d 8h		⊘ 🛸	((•
Level 2 >		<mark></mark> 🖓 🖉	Internet in the second seco	(Teaching Comp	On		3 %	34 % 4d 20h		\otimes >	

This section offers resources designed to maximize the use of Workspaces. It includes detailed instructions on configuring and using functionalities, along with advanced settings that will allow you to tailor Workspaces to specific needs.

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

Workspaces / Guides / 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.

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

Flex	×wc	ORKSPACES							- 19	adder Contex	-	\mathbf{Q}		Log Of
Search Q Level 1	Work	spaces												
CC Deshboard						My Filters	•	Filter by tag		Filter by	workspace grou	IP Text to	search 🖇	ρ
Workspaces						Ģ ⊇		-C: 🗐	\odot	3	×		Operations	•
C Sessions		Platforms	Machine †	RG Tenant	Power state	Last user	Sessions	CPU	% RAM	Uptime	Code	Status	Connecti	ion
∷⊟ Connection Logs			(MARCE) (MARCE)	(Stradition Comp	Not reporting	100000000000		0 %	O 96					
D Jobs		Count=1												
Alers	< 1	>										Page si	ze 20 *	

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 0k to confirm the operation.
- 6. A floating panel will appear indicating that remote assistance is being prepared.

ASISTENCIA REMOTA	Cerrar
	Preparing

7. Once prepared, the information will appear.

ASISTENCIA REMOTA FLEXXIBLE\	Cerrar
The remote assistance session is ready to connect.	
Session Id:	
You can start the remote assistance session from your AnyDesk client, or download and execute the Flexxible Remote Assistar Note: You may need to authorize the download in your browser.	nce client.

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.



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

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



Workspaces / Guides / 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\DisableAu
tomaticRestartSignOn = 1 (DWORD)
```

Intune Policy

- Platform: Windows 10 and later
- Profile type: Administrative Templates

• Path: \Windows Components\Windows Logon Options

More information: <u>https://learn.microsoft.com/en-us/windows-server/identity/ad-</u> <u>ds/manage/component-updates/winlogon-automatic-restart-sign-on--arso-#policy-1</u>