Forcepoint Data Security Posture Management

Powered by Getvisibility

GV Troubleshooting Training

Forcepoint

Report

Forcepoint
April 23, 2024

Table of Contents

AGENDA **2**

DEPLOY THROUGH THE LICENSE PORTAL 2
K3s Cheat-Sheet 5
Agent-Edge not Working - Symptoms 5
Agent-Edge not Working - Troubleshoot 6
flink-jobmanager Service Enters crashloopback State - Symptoms 6
flink-jobmanagerservice enters crashloopback State - Troubleshoot 6
Cluster Paused/Unpaused 6
Labels 7
Labels Issues - Symptoms 7
Labels Issues – Symptoms – Fix 8
traefikpatch not Applied – Symptoms 8
traefikpatch not Applied – Troubleshooting 9
traefikpatch not Applied – Fix 9
KEYCLOAK ISSUES 11
Keycloakadmin site ok but UI not -symptoms 11
Keycloak Admin Site ok but UI not -Fix 12
Reset Admin Password 12
AGENT ISSUES 12
Installation Fails 12
Generate Installation Logs Command 13
Agent not Connected to Server / Configuration not Available. 14
Agent Icon not Appearing in Taskbar 14
Plugins not Loading / Classification Ribbon not Visible 15
Agent ribbon is greyed out 16
Platform Hub is not Running 17
Logs Directories 18

Agenda

1. Deploy through the license portal.
    - Full registration command.
2. Rancher/K3s issues
    - k3s cheat-sheet
    - agent-edge not working.
    - flink-jobmanagerservice crashing.
    - Cluster paused/unpaused.
    - Labels
    - traefikpatch not applied.
    - support-tools chart.
3. Keycloak issues
    - Keycloak admin site ok but UI not
    - Reset admin password.
4. Agent issues
    - Installation fails.
    - Generate installation logs.
    - Agent not connected to server.
    - Agent icon not appearing in taskbar.
    - Plugin not loading/Classification ribbon not visible.
    - Agent ribbon greyed out.
    - “Unexpected error when updating document.”
    - Platform Hub is not running.
    - Logs directories

Deploy through the License Portal

Portal URL: https://license-management.master.k3s.getvisibility.com/#/license-management/register

- CUSTOMER
- REGION
- LICENCE TYPE
- SEATS
- EXPIRATION DATE
- EVALUATION LICENCE

- ORDER PROCESSOR EMAIL ADDRESS(ES)
- CC EMAIL ADDRESS(ES)
- CUSTOMER EMAIL (OPTIONAL)

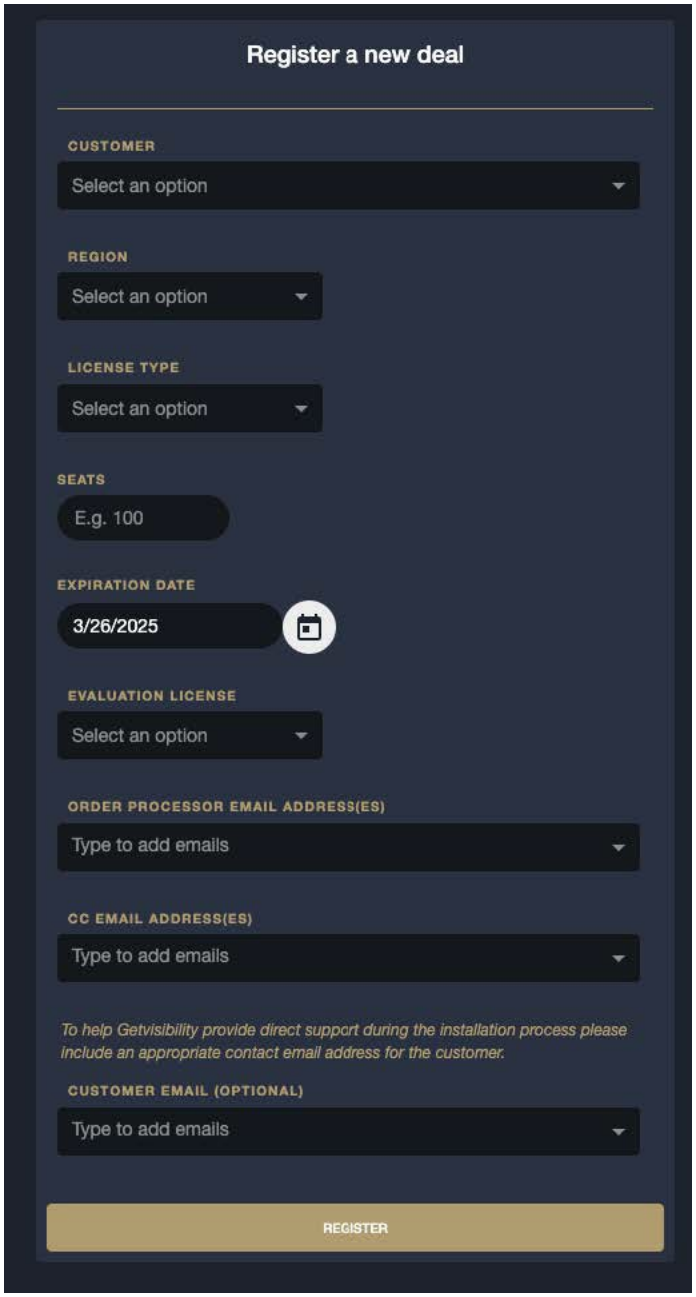
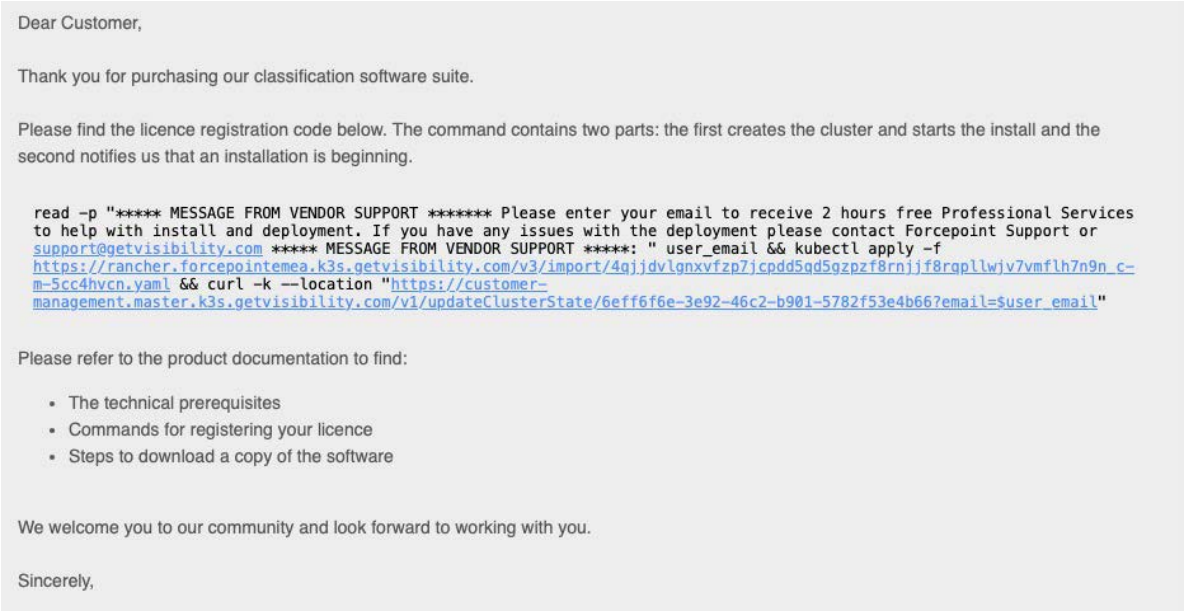


Figure 1.

Confirmation Email



Dear Customer,

Thank you for purchasing our classification software suite.

Please find the licence registration code below. The command contains two parts: the first creates the cluster and starts the install and the second notifies us that an installation is beginning.

```
read -p "***** MESSAGE FROM VENDOR SUPPORT ******* Please enter your email to receive 2 hours free Professional Services
to help with install and deployment. If you have any issues with the deployment please contact Forcepoint Support or
support@getvisibility.com ***** MESSAGE FROM VENDOR SUPPORT *****: " user_email && kubectl apply -f
https://rancher.forcepointemea.k3s.getvisibility.com/v3/import/4gjjdvlgnxvfzp7jcpdd5qd5gzpzf8rnjjf8rqpllwjv7vmflh7n9n_c-
m-5cc4hvcn.yaml && curl -k --location "https://customer-
management.master.k3s.getvisibility.com/v1/updateClusterState/6eff6f6e-3e92-46c2-b901-5782f53e4b66?email=$user_email"
```

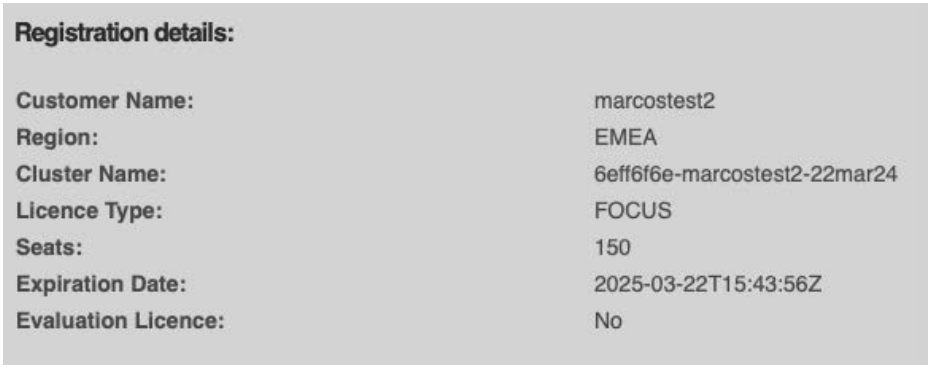
Please refer to the product documentation to find:

- The technical prerequisites
- Commands for registering your licence
- Steps to download a copy of the software

We welcome you to our community and look forward to working with you.

Sincerely,

Figure 2.



Registration details:

Customer Name:	marcostest2
Region:	EMEA
Cluster Name:	6eff6f6e-marcostest2-22mar24
Licence Type:	FOCUS
Seats:	150
Expiration Date:	2025-03-22T15:43:56Z
Evaluation Licence:	No

Figure 3.

Applying Registration Command

Prompt for email.

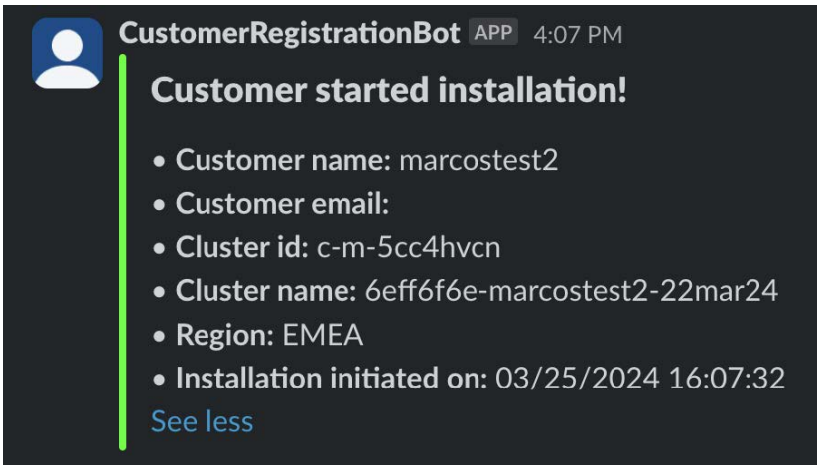


Figure 4.

K3s Cheat-Sheet

- `Kubectl` get pods -A →retrieve information about all pods in all namespaces (local, default, cattle-system, etc.)
- `Kubectl` get events -A →retrieve information about events from all name spaces.
- `Kubectl` describes nodes →receive detailed information about each node in the cluster.
- `Kubectl` logs pod/$POD_NAME -n $NAMESPACE_NAME →retrieve logs from a specific pod.
- `journalctl-u k3s --since "7 days ago" --no-tail > /tmp/k3s.log` →logs from k3s service. Information about startupof k3s service, errorsor warningsduring operation, events related to Kubernetes components and other relevant system messages.

Pods, events, and logs can be retrieved from Rancher as well. Let's see how!

Agent-Edge not Working - Symptoms

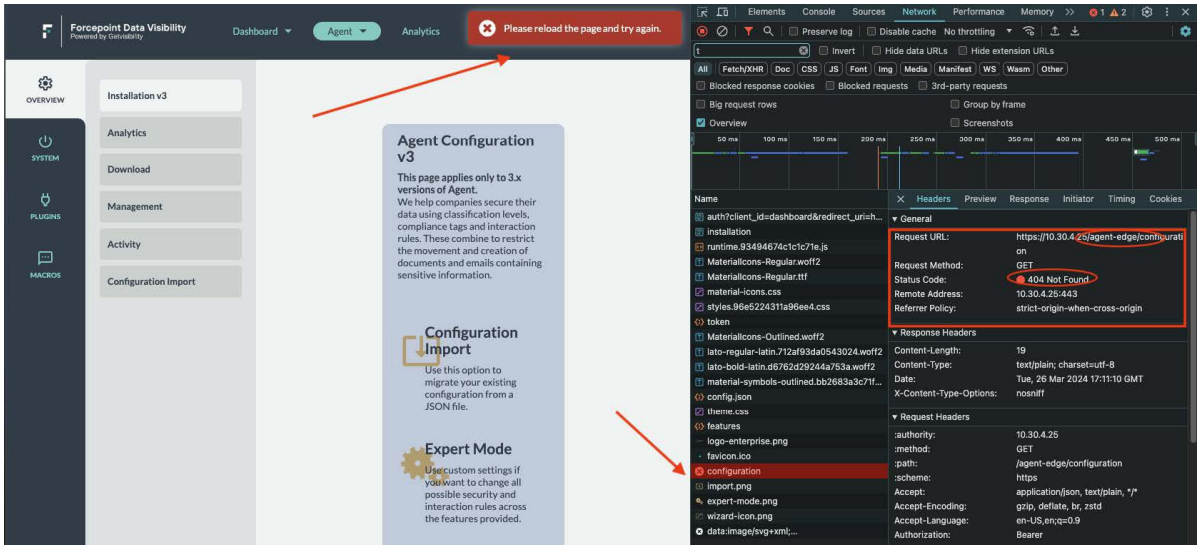


Figure 5.

Relevant PlatformHublogs (Agent's perspective):

03/26/2024 17:21:02.601 [T10\AgentEdgeConnectivityManager.HandleConnectionAbortion] [OfficeVersionNumber: 16.0.17328.20184, OfficeVersionName: O365ProPlusRetail] [CpuCores: 4] [TotalMemory: 15.65GB] INFORMATION: Connection was aborted: Grpc.Core.RpcException: Status(`StatusCode="Unimplemented", Detail="Bad gRPCresponse. HTTP status code: 404"`)

Agent-Edge not Working - Troubleshoot

Rancher

- Check deployment
- Check pod logs

Collect info and create a ticket with GV Support.

flink-jobmanager Service Enters crashloopback State - Symptoms

- Agent doesn't receive suggestions
- Platform Hub logs (agent point of view)
    - 03/26/2024 17:35:58.523 [T3\ConfigurationListener.Start] [OfficeVersionNumber: 16.0.17328.20184, OfficeVersionName: O365ProPlusRetail] [CpuCores: 4] [TotalMemory: 15.65GB] WARNING: Error occuredin ConfigurationListener: Grpc.Core.RpcException: Status(StatusCode="Unknown", Detail="Application error processing RPC")
    - At Grpc.Net.Client.Internal.HttpContentClientStreamReader`2.MoveNextCore(CancellationTokencancellationToken)
    - at GVClient.Application.Hub.AgentsEdge.Components.ConfigurationListener.Start(CancellationTokencancellationToken, CallInvokercallInvoker) in D:\a\office-classifier\office-classifier\GVClient\3.Application\GVClient.Application.Hub\AgentsEdge\Components\ConfigurationListener.cs:line42
    - 03/26/2024 17:35:58.523 [T3\ConfigurationListener.Start] [OfficeVersionNumber: 16.0.17328.20184, OfficeVersionName: O365ProPlusRetail] [CpuCores: 4] [TotalMemory: 15.65GB] INFORMATION: Waiting some time before restarting configuration listener...

flink-jobmanagerservice enters crashloopback State - Troubleshoot

Rancher

- Check deployment
- Check pod logs

Collect info and create a ticket with GV Support.

Cluster Paused/Unpaused

Rancher →Hamburger menu →Continuous delivery →Clusters →cluster_name

A paused cluster will essentially not receive updates when GV releases them. GV releases updates (new versions of

the product) every 1 or 2 weeks that can affect several deployments (pods).

In this process, what usually happens is that the affected deployment deploys a new pod(s), and after this(these) is(are) completed and running healthy, the old ones are terminated.

All other functionalities are still there.

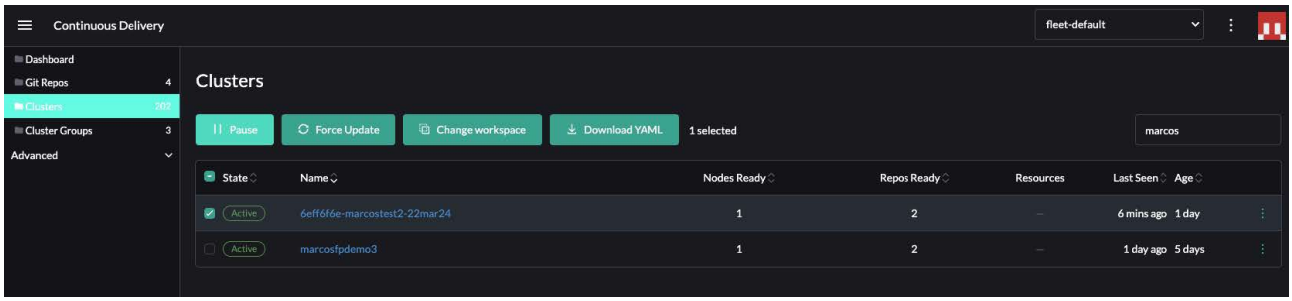


Figure 6.

Labels

Rancher →Hamburger menu →Continuous delivery →Clusters →cluster_name→three dots →Edit Config

If the deployment was deployed correctly, all labels should be fine. But sometimes there could be spelling mistakes for the manually entered ones or the product type needs to be changed.

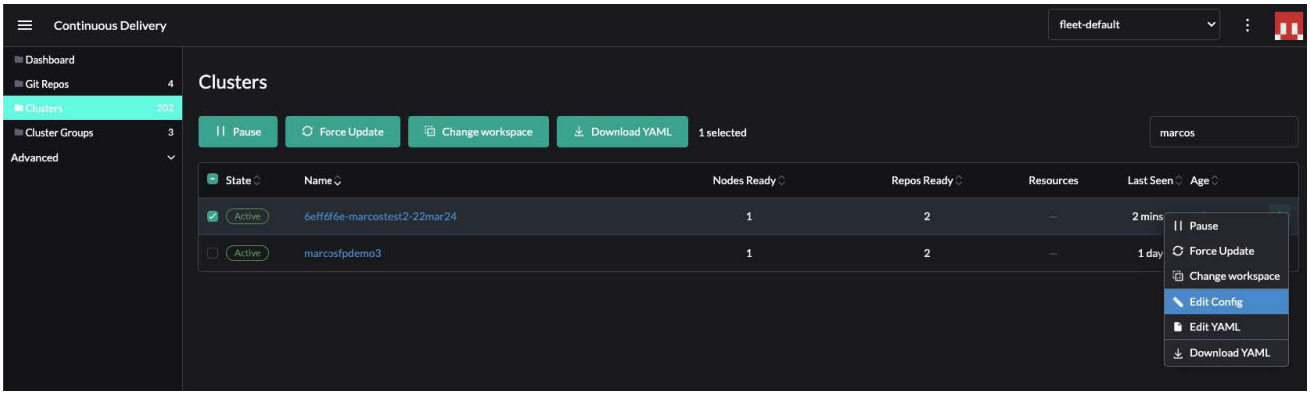


Figure 7.

Labels Issues - Symptoms

- Several deployments missing. Normally an enterprise deployment has ~75 pods, an error in label could show ~40 pods in Ranceror kubectlget pods A
- 404 on dashboard AND keycloakadmin page
- Agent not connecting to the backend

Relevant missing deployments:

- agent-edge (hence the 404 in dashboard)

- classification-tags
- classifier-focus
- classifier-synergy
- connector-generic (and others)
- dashboard (hence 404 as well)
- fleet-agent
- flink(both)
- scan-data-manager
- scan-manager
- And more!

Labels Issues – Symptoms – Fix

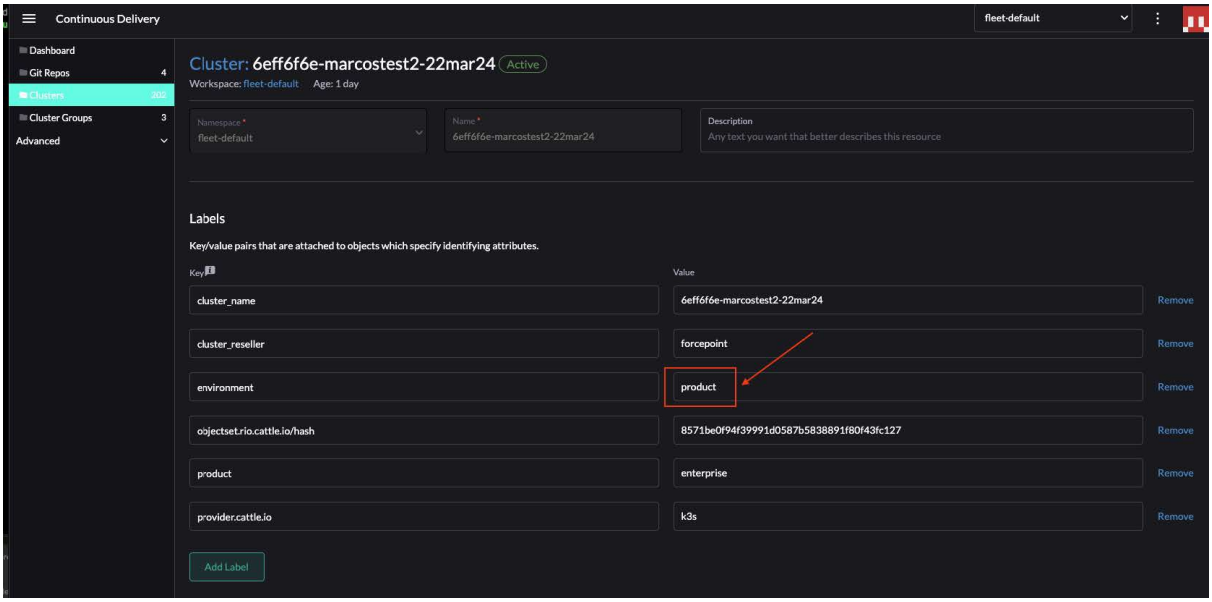


Figure 8.

traefikpatch not Applied – Symptoms

- 404 on keycloakadmin site

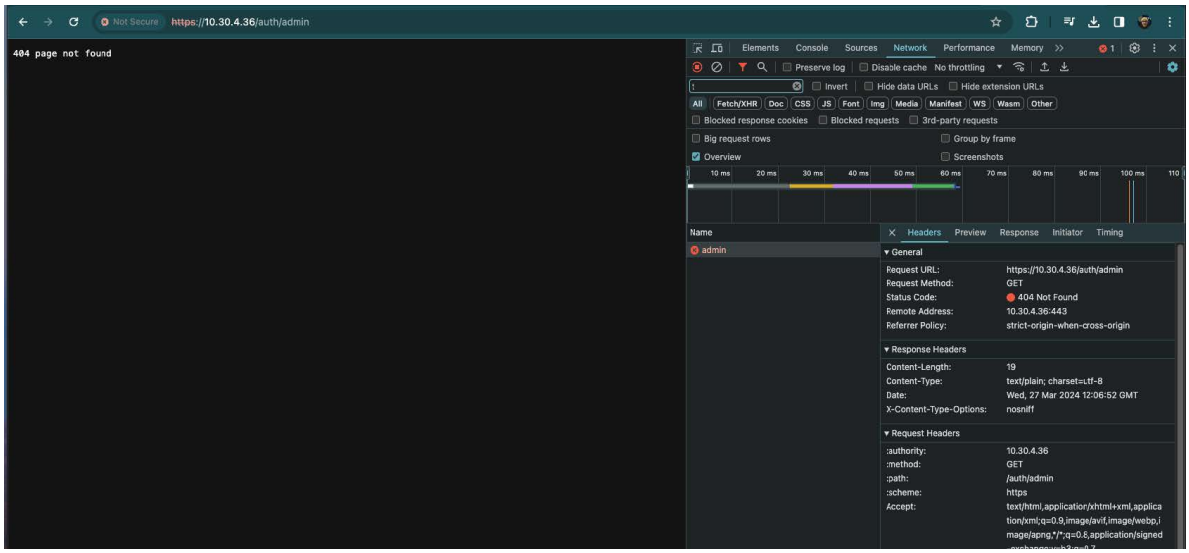


Figure 9.

traefikpatch not Applied – Troubleshooting

- Check traefiklogs (search for ingress)

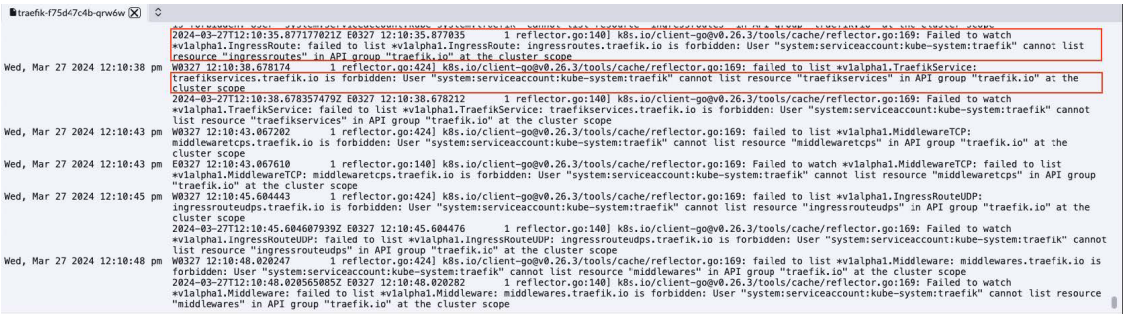


Figure 10.

traefikpatch not Applied – Fix

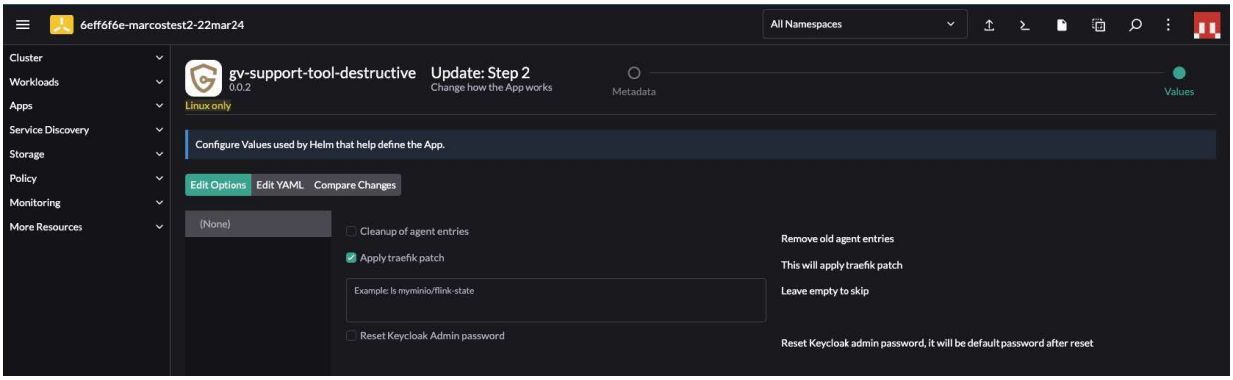


Figure 11.

- Or create a ticket with GV support
- traefik logs after applying the patch
- And keycloak site becomes accessible

traefik-6f9c5c49f6-8kfx8

```
Wed, Mar 27 2024 12:16:21 pm  time="2024-03-27T12:16:21Z" level=info msg="Configuration loaded from flags."
```

Figure 12.

Support Tools

- Support tools is a chart that provides quick access to troubleshooting tools
- It can be installed from Apps →Charts and filtering for it
- Upon installation we will be able to choose from a series of predefined checks
- The most common ones are (from the Default tab, the rest of the tabs are more advanced and out of scope for this training):
- Run generic system checks: it will give a summary of cpu/storage/inodes/memory/os-version
- Run kubectlget pods -A
- Run kubectlget events -A
- Retrieve v3 agent config from Consul
- Retrieve v4 agent config from ES
- After installation, two jobs will be created and to access the retrieved information. The information will be in the logs of the job from default namespace.

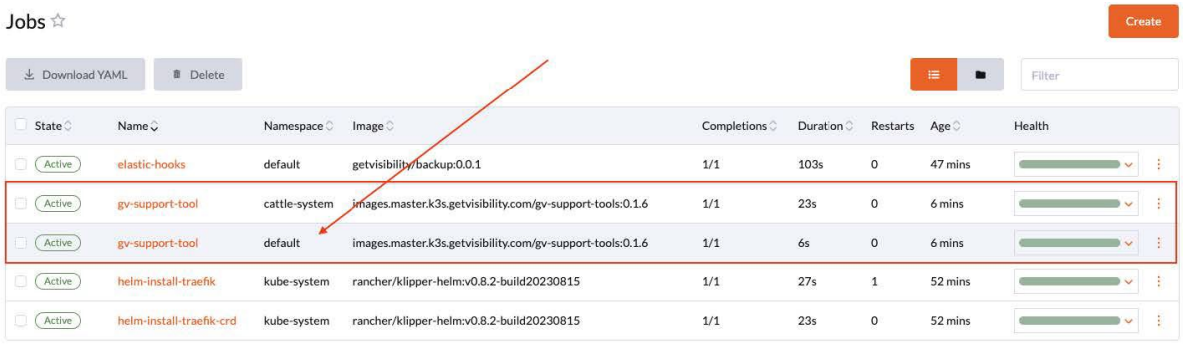


Figure 13.

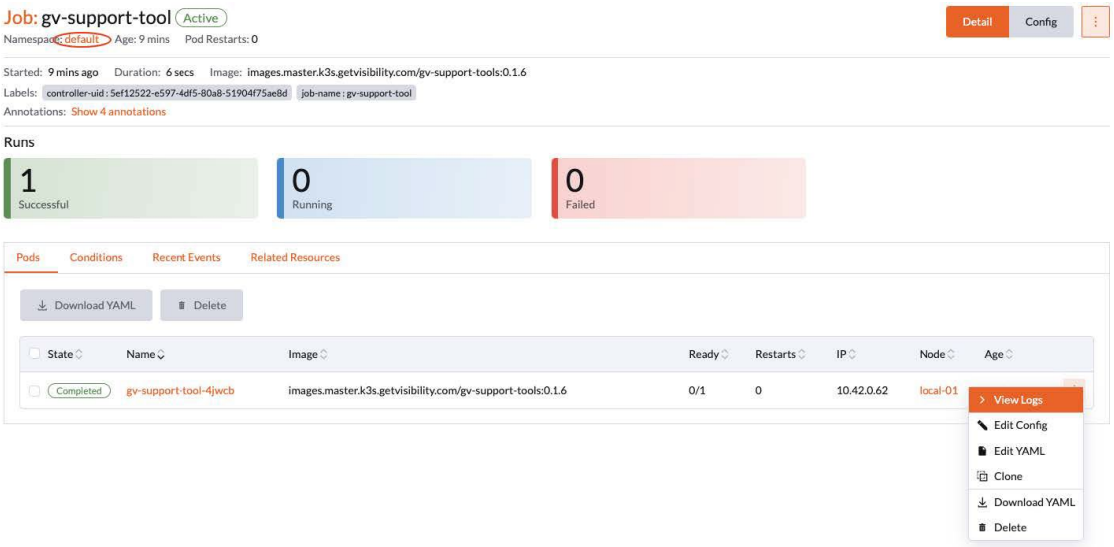


Figure 14.

Keycloak issues

Keycloakadmin site ok but UI not -symptoms

When accessing https://server-ip/ui, an 'Invalid parameter: `redirect_uri`' appears

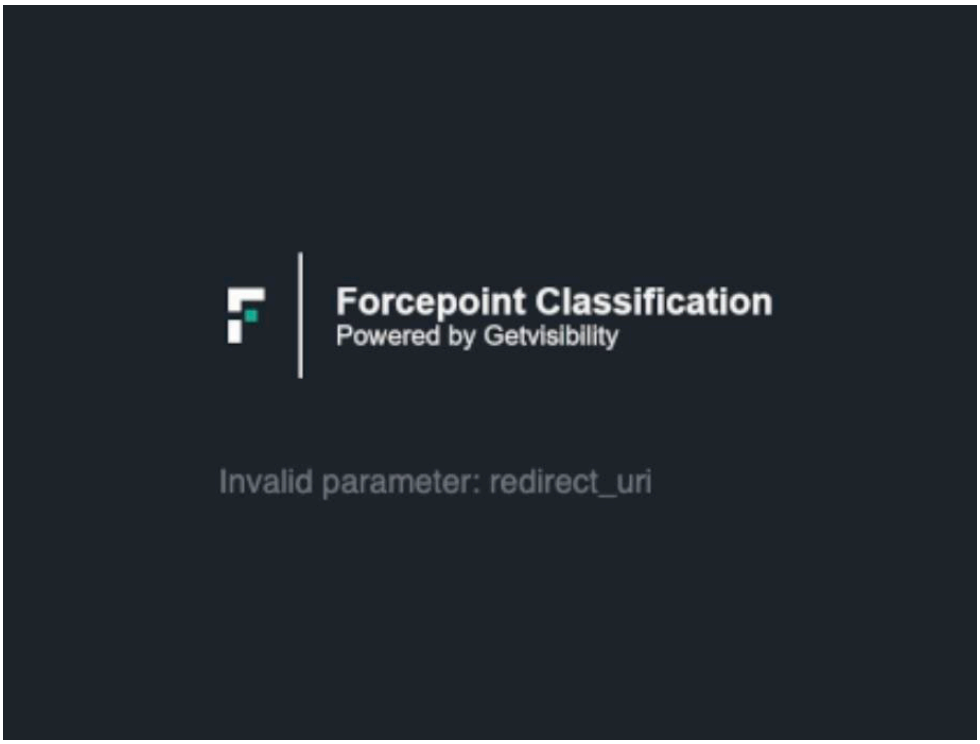


Figure 15.

Keycloak Admin Site ok but UI not -Fix

Add https://server-ip/* in **Keycloak→gvrealm →Clients →Valid redirect URIs**

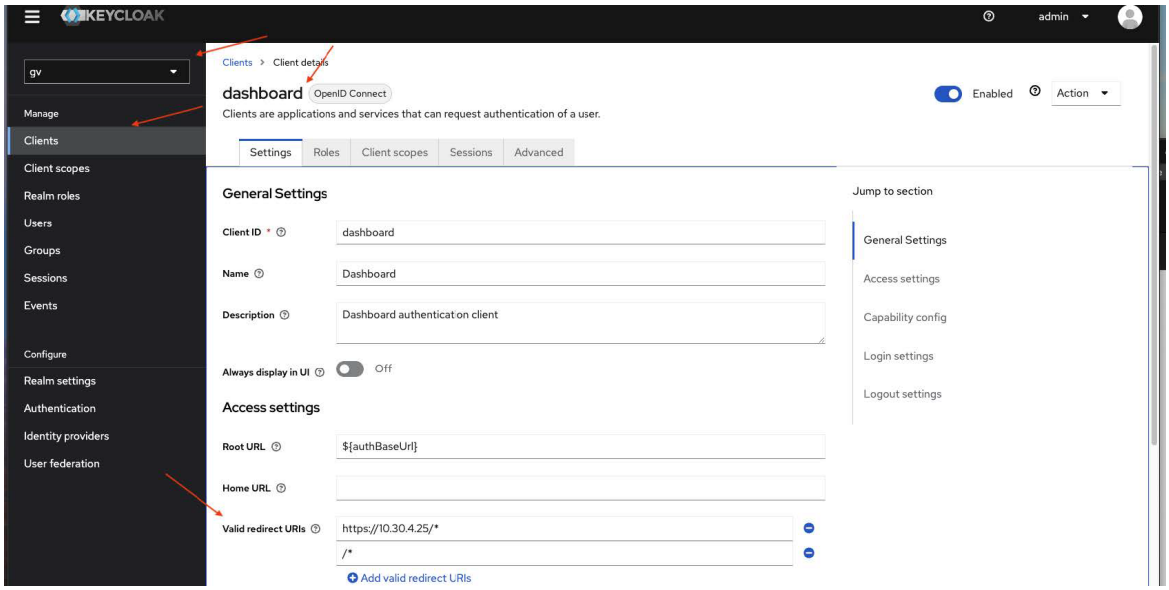


Figure 16.

Reset Admin Password

Rancher →Apps →Charts →GV - Support Tool Destructive

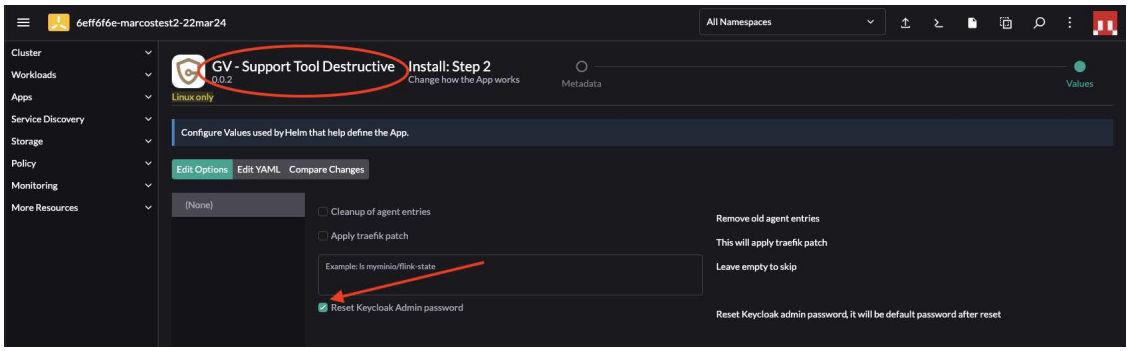


Figure 17.

Or create a ticket with GV support.

Agent Issues

Installation Fails

If the installation of the agent fails abruptly, please check the following points:

- InstallerConfig.json has a typo
- Make sure there are no left overs from previous installations under C:\Program Files (x86)\GVClient\
- Try to restart the process explorer.exe

- Reboot after previous versions were removed
- Make sure the file installerConfig.json is not blocked->right-click -> Properties -> Unblock

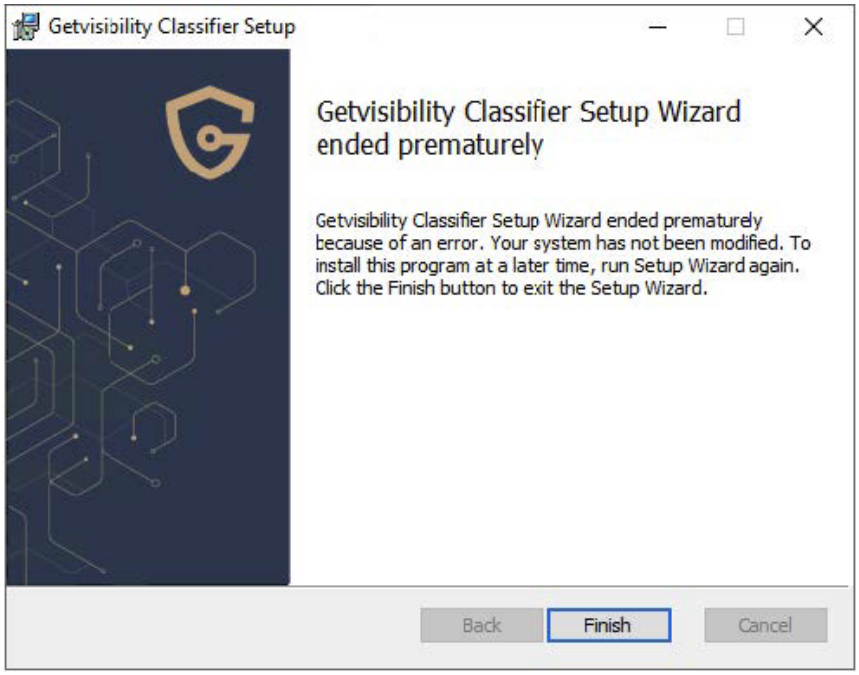


Figure 18.

Generate Installation Logs Command

```
AgentClassifier.4.0.5-Forcepoint-windows.msi /lv c:\install.log
```

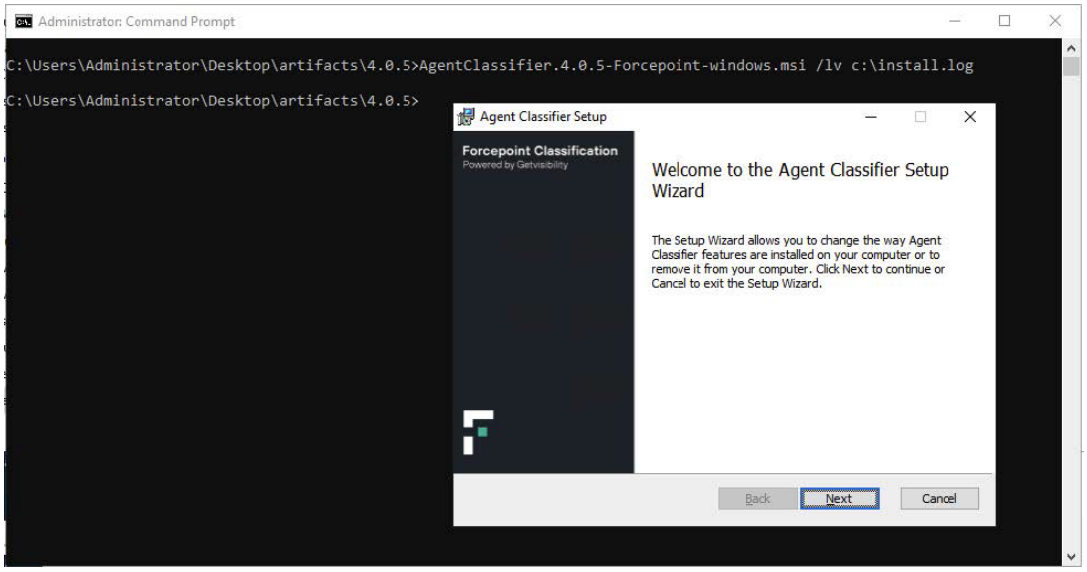


Figure 19.

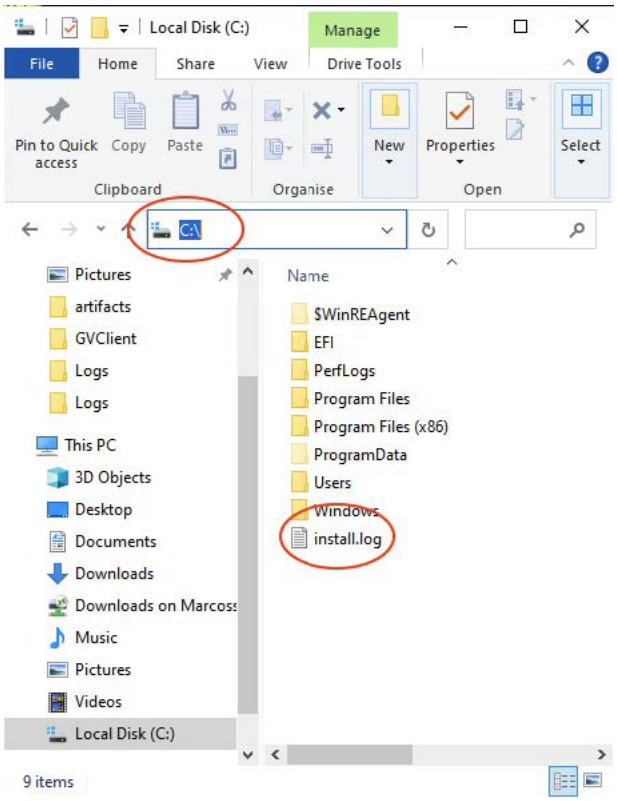


Figure 20.

Agent not Connected to Server / Configuration not Available.

- Symptoms: ribbon greyed out; not receive suggestions; not receive config changes from the UI

Main reasons:

- Wrong IP in the configuration →search PlatformHublogs for `AgentEdgeConnectivityManager`
- agent default user not configured in Keycloak → search PlatformHublogs for Grpc.Core.RpcException: Status(StatusCode="Unauthenticated", Detail="JWT Token is null or malformed")
- agent-edge failing
- Network issues (endpoint doesn't reach the server)
- No communication through port 443 →check with telnet

Agent Icon not Appearing in Taskbar

- Missing icon in taskbar is usually an indicator that the AgentUIprocess is not running at all.
- Symptoms: no pop upwindows at all.
- Main reasons: AgentUIprocess crashed →run manually from C:\Program Files (x86)\GVClient\app-4.0.5\AgentUI\GVClient.AgentUI.exe

Plugins not Loading / Classification Ribbon not Visible

Main reasons:

- Ribbon suppressed in Agent Config
- Plugin is disabled under COM Add-ins

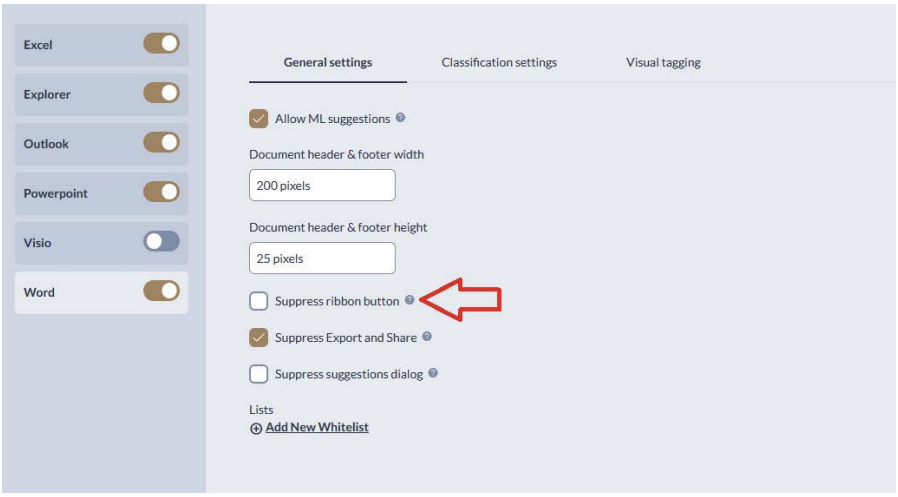


Figure 21.

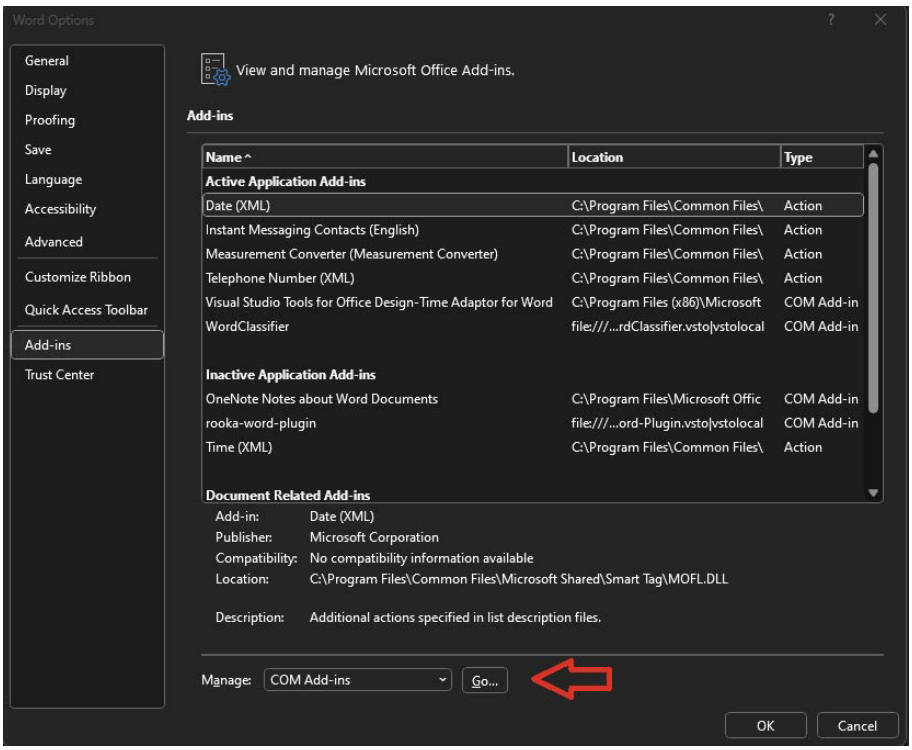


Figure 22.

Agent ribbon is greyed out

A greyed-out button is an indication that the plugin is loaded but classification is not available.

Main reasons:

- Plugin is disabled in Agent Config
- Platform Hub is not running/Agent Configuration not available.

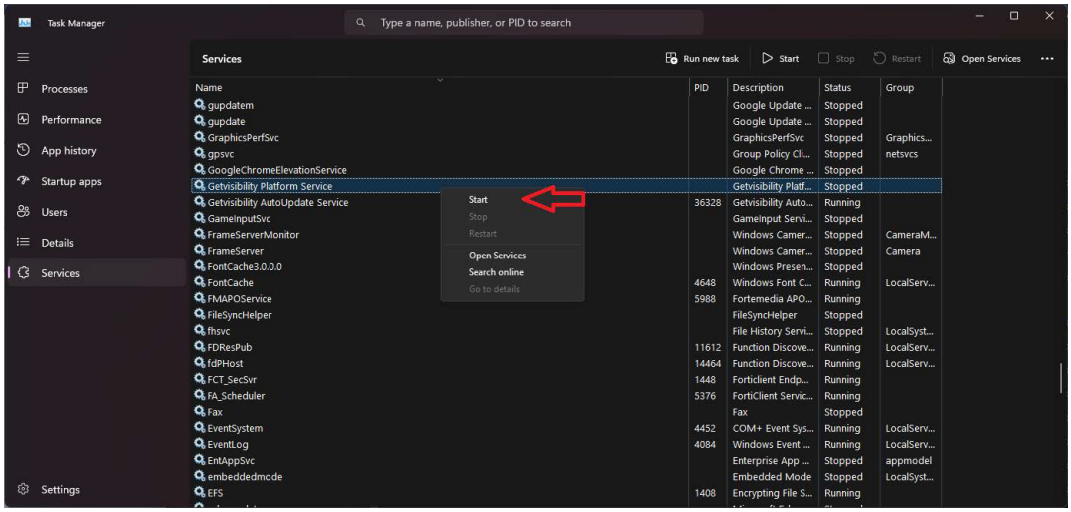


Figure 23.

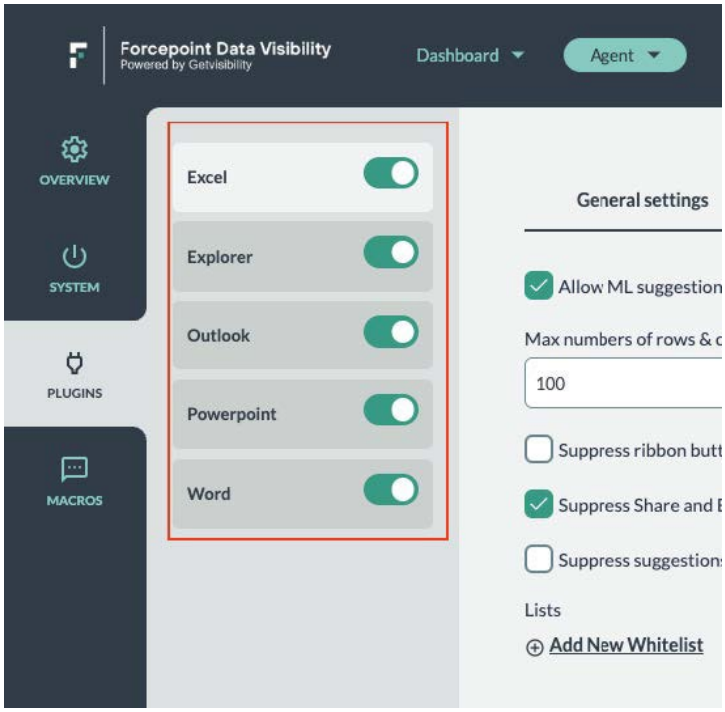


Figure 24.

“Unexpected error when updating document. Please contact support.”

When the Office Plugin (Word, Excel, Outlook, or PowerPoint) encounters an unexpected error while trying to update the document, a generic error message will be shown to the user.

This will occur when there is a new, unhandled bug that has previously not been seen.

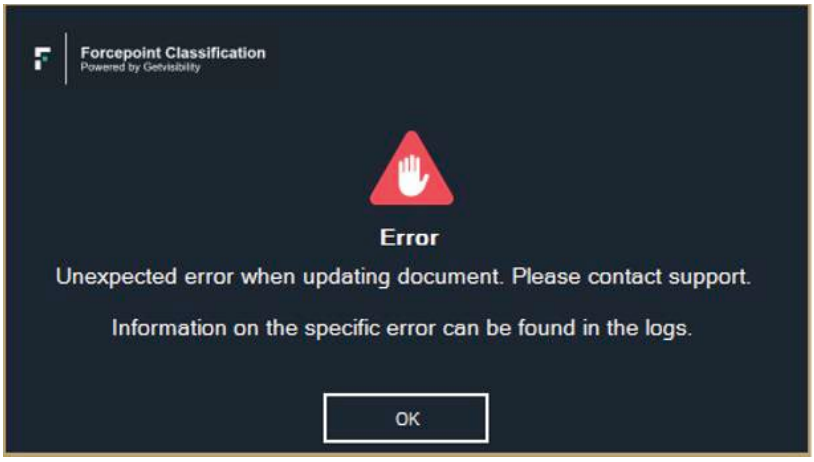


Figure 25.

Troubleshooting:

Search the log file for the relevant plugin (Word, Excel, Outlook, or PowerPoint) for either FATAL and/or Unhandled exception when updating document to find the correct entry.

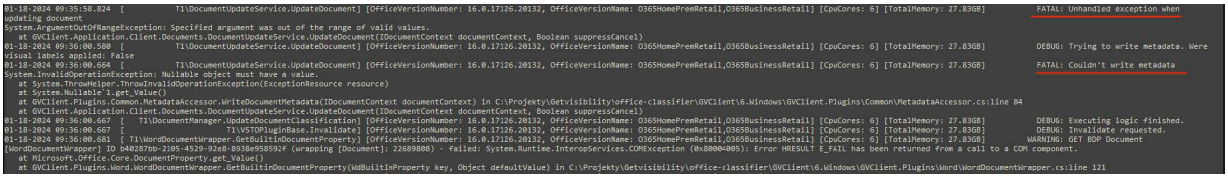


Figure 26.

Platform Hub is not Running

The Platform Hub is essential for the agent's functionality; without it, the entire product cannot operate properly.

Main reasons:

- .NET Framework not installed. It’s essential that the machine has the following frameworks installed:
- .NET Framework 4.7.2 or higher
- .NET 6.x.x

Note: look for ‘runtime’ versions (no SDK or Desktop Runtime)

Service Startup Type is misconfigured →set to Automatic (Delayed Start) or Automatic

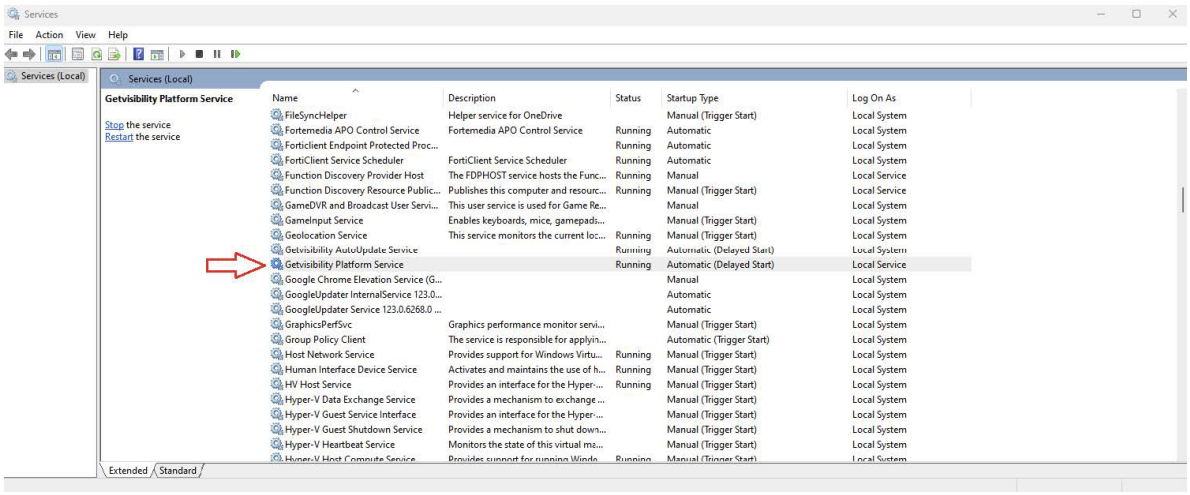


Figure 27.

Logs Directories

Platform Hub logs:
`C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\GVClient.PlatformHub.Windows\Logs`

Plugin logs:

- `%appdata%\OutlookClassifier\Logs`
- `%appdata%\ExcelClassifier\Logs`
- `%appdata%\GVClient.Powerpoint\Logs`
- `%appdata%\WordClassifier\Logs`

Auto update logs:
`C:\Windows\SysWOW64\config\systemprofile\AppData\Roaming\GVClient.AutoUpdateService.Windows\Logs`

Forcepoint

forcepoint.com/contact

About Forcepoint

Forcepoint simplifies security for global businesses and governments. Forcepoint's all-in-one, truly cloud-native platform makes it easy to adopt Zero Trust and prevent the theft or loss of sensitive data and intellectual property no matter where people are working. Based in Austin, Texas, Forcepoint creates safe, trusted environments for customers and their employees in more than 150 countries. Engage with Forcepoint on www.forcepoint.com, Twitter and LinkedIn.

[Forcepoint Data Security Posture Management Powered by GetVisibility GV Troubleshooting Training] [Status]23 Apr. 24