Forcepoint

Forcepoint Data Classification

Powered by Getvisibility

CLI for Data Classification

Forcepoint

Report

Forcepoint
15 July, 2024

Table of Contents

Using Agent via command line interface (CLI) executable

Previously (versions prior to 3.0) it was possible to call the Agent executable with parameters to change classification/distribution/compliance of a file from command line.

Starting with version 3.0 we do ship a separate CLI executable with each Agent installation (**GVClient.CLI.Windows.exe**) that can be used to:

→ manually apply a given classification to a file.

→ manually apply a given distribution to a file.

→ manually apply a given compliance to a file.

→ apply classification/distribution/compliance as described in Expert Configuration, section **externalLabelMappings**.

NOTE: For the CLI functionality to work as expected in this document Agent version 3.5.9 is required.

What does it do?

By calling the CLI with parameters we run actions listed in previous paragraph and as a result **ADD** or **OVERWRITE** metadata of requested file.

What does it not do?

→ It is not possible to **REMOVE** any metadata from the file, you can only **ADD** or **OVERWRITE**.

→ It is not possible to add visual markings to the file (December 2023).

→ No machine learning capabilities - we need user to provide required classification/compliance/distribution as parameter.

Supported files

NOTE: This tool **DO NOT** currently support all Data Classification-supported files as per the document located here: Forcepoint Data Classification Powered by Getvisibility Synergy Supported File Types

It only supports files that have metadata. So, for example DOC/XLS/PPT files are **NOT SUPPORTED**.

Setup and functionality

Basic functionality and parameters

To classify a file using CLI and add PCI compliance you can run it as:

```
GVClient.CLI.Windows.exe filename.docx --silent --overwrite --save --tag e16409a7-1700-4153-9090-3955bc2f0ae8/Classification/Confidential --tag f14fc1f1-8950-40d5-8a29-45909da947d6/PCI/true
```

→ **--silent** - Optional. Silent executes the command in the background.

→ **--save** - Optional. A “Save” parameter is required to write changes to the files. W/o “save” the commands are executed in a “dry-run” mode

→ **--tag** - Optional. Tag parameter specifies what labels to write to a file.

→ **--map-external** - Optional. Map-external will use the mapping specified in the configuration under the "externalLabelMappings" stanza, as shown in the screenshot below. This parameter checks file's metadata with the regex specified in the configuration and applies a GV label specified in tagset and tag sections of the externalLabelMapping stanza of the configuration.

→ **--overwrite** - Optional. Overwrite means to disregard all existing GV tags inside of a file. For example, if we want to tag a file, and a file is already tagged by GV, then we will not overwrite GV tag if the overwrite option is specified.

Running CLI will result in logs being shown in the console. You can redirect the logs to a file or null device if you are running the CLI for multiple files.

Sample result:


```
C:\Users\Marcel>"C:\Program Files (x86)\GVClient\app-3.5.9\GVClient.CLI.Windows.exe" "C:\tools\bj\BJ Files\file-sample_1
MB.docx" --silent --overwrite --save --map-external
Got startup args: C:\tools\bj\BJ Files\file-sample_1MB.docx, --silent, --overwrite, --save, --map-external
Initializing application...
Performed classification: { "created": "2023-12-12T11:46:02.000307400Z", "originator": { "userName": "Marcel", "userDoma
inName": "W10W", "machineName": "W10W", "assemblyName": "CLI", "ipAddress": "100.112.66.43", "identityKind": "PLATFORM_I
DENTITY_KIND_CLI" }, "initialOrigin": { "userName": "Marcel", "userDomainName": "W10W", "machineName": "W10W", "assembly
Name": "CLI", "ipAddress": "100.112.66.43", "identityKind": "PLATFORM_IDENTITY_KIND_CLI" }, "clientSessionId": "10016d77
-ade5-4cf0-985e-15852a763294", "eventTime": "2023-12-12T11:46:02.000307400Z", "user": "Marcel", "agentId": "W10W/Marcel/
GVClient.CLI.Windows/100.112.66.43", "ipAddress": "100.112.66.43", "classificationEvent": { "classifiedFile": { "fileId"
: "bbd35e6c-6a69-5748-532c-c5f05eb98f7d", "path": "C:\\tools\\bj\\BJ Files\\file-sample_1MB.docx" }, "settings": { }, "c
lassificationValue": [ { "id": "ac4a810e-decf-4e3a-a9c2-88fcd6a56e1c", "tagset": { "name": "Classification", "id": "e164
09a7-1700-4153-9090-3955bc2f0ae8", "tags": [ { "name": "Classification", "id": "b7c4a4c1-0618-484d-be40-942991ff752e", "
tagType": "TAG_TYPE_CATEGORICAL", "defaultValue": { "type": "string", "value": "Public" }, "tagValues": [ { "type": "str
ing", "value": "Public" }, { "type": "string", "value": "Internal" }, { "type": "string", "value": "Confidential" }, { "
type": "string", "value": "Highly Confidential" } ] } ], "tagType": "TAG_TYPE_CATEGORICAL", "displayName": "CLASSIFICATI
ON" }, "created": "2023-12-12T11:46:02.406912700Z", "values": [ { "key": { "name": "Classification", "id": "b7c4a4c1-061
8-484d-be40-942991ff752e", "tagType": "TAG_TYPE_CATEGORICAL", "defaultValue": { "type": "string", "value": "Public" }, "
tagValues": [ { "type": "string", "value": "Public" }, { "type": "string", "value": "Internal" }, { "type": "string", "v
alue": "Confidential" }, { "type": "string", "value": "Highly Confidential" } ] }, "value": { "type": "string", "value":
 "Confidential" } } ], "confidences": [ { "key": { "name": "Classification", "id": "b7c4a4c1-0618-484d-be40-942991ff752e
", "tagType": "TAG_TYPE_CATEGORICAL", "defaultValue": { "type": "string", "value": "Public" }, "tagValues": [ { "type":
"string", "value": "Public" }, { "type": "string", "value": "Internal" }, { "type": "string", "value": "Confidential" },
 { "type": "string", "value": "Highly Confidential" } ] }, "value": 1 } ] } ] } }
```


figure 1.

Applying classification based on existing metadata content.

Other limitations

User under which the CLI is executed needs access/write rights to a file you are trying to modify. This may cause issues if CLI is executed under different user context.

This is specifically true for any DLP since it is not executing script in user context, rather SYSTEM.

Troubleshooting

NOTE: Verify customer is using Agent with at least version 3.5.9

→ Log files for CLI can be located at:

`%AppData%\Roaming\GVClient.CLI.Windows\Logs`

→ Example of log after running CLI with --map-external:

```
360     INFORMATION: Loading metadata from "C:\tools\bj\BJ Files\file-sample_1MB.docx" - 14 entries.
361     INFORMATION: Loading metadata from "GVClient.Common.Utils.Base64EncodedMetadataDictionary" - 1 entries.
362           DEBUG: Reading tagset e16409a7-1700-4153-9090-3955bc2f0ae8/Classification...
363           DEBUG: Reading value for tag Classification
364           DEBUG: Got property value Confidential
365           DEBUG: Property value is NOT equal to tagTemplate
366           DEBUG: Property value is NOT equal to tagTemplate
367           DEBUG: Property value is equal to tagTemplate
368           DEBUG: Property value is NOT equal to tagTemplate
369           DEBUG: Property value is NOT equal to tagTemplate
370           DEBUG: Some tagValues were found
371           DEBUG: ReadTagsetValue finished
372           DEBUG: WriteMetadataTagsetValues started
373           DEBUG: GetInternalMetadataAccessor started
374           DEBUG: GetInternalMetadataAccessor finished
375     INFORMATION: Loading metadata from "C:\tools\bj\BJ Files\file-sample_1MB.docx" - 14 entries.
376     INFORMATION: Loading metadata from "GVClient.Common.Utils.Base64EncodedMetadataDictionary" - 1 entries.
377           DEBUG: Writing tagset e16409a7-1700-4153-9090-3955bc2f0ae8/Classification...
378     INFORMATION: Saved metadata to "C:\tools\bj\BJ Files\file-sample_1MB.docx" - 14 entries.
379     INFORMATION: Saved metadata to "GVClient.Common.Utils.Base64EncodedMetadataDictionary" - 1 entries.
380           DEBUG: Updating Confidential -> Confidential
381     INFORMATION: Document saved.
382
```

figure 2.

Forcepoint

forcepoint.com/contact

About Forcepoint

Forcepoint is the leading user and data protection cybersecurity company, entrusted to safeguard organizations while driving digital transformation and growth. Forcepoint's humanly attuned solutions adapt in real-time to how people interact with data, providing secure access while enabling employees to create value. Based in Austin, Texas, Forcepoint creates safe, trusted environments for thousands of customers worldwide.

[Forcepoint Data Classification Powered by Getvisibility CLI for Data Classification]
[Status]15 Jul. 24