

Forcepoint

Forcepoint Data Classification

Powered by Getvisibility

Admin Guide Agent v4



Report

Table of Contents

OVERVIEW	2
ANALYTICS.....	2
DOWNLOAD.....	3
MANAGEMENT.....	3
ACTIVITY	3
CONFIGURATION IMPORT	4
<i>Select a configuration file to import.....</i>	4
<i>Download current configuration</i>	5
SYSTEM.....	5
GLOBAL	5
<i>Enable auto-update.....</i>	5
<i>Enable beta version update</i>	6
<i>Machine names for receiving beta version.....</i>	6
<i>Heartbeat frequency.....</i>	6
<i>Supported languages.....</i>	6
<i>Agent suggestion frequency rate.....</i>	6
<i>Minimum confidence threshold.....</i>	6
<i>Agent: Disable Configuration Menu.....</i>	7
<i>Block Server Address edit.....</i>	7
<i>Help URL.....</i>	7
<i>Ribbon title.....</i>	8
<i>Order tag from top to bottom.....</i>	8
PLUGINS.....	10
SHARED CONFIGURATIONS.....	10
<i>General Settings.....</i>	10
<i>Classification settings.....</i>	14
<i>Visual Tagging.....</i>	19
<i>Show header/footer/watermark (and title/subtitle for PPT).....</i>	23
EXCLUSIVE CONFIGURATIONS	24
<i>Explorer.....</i>	24
<i>General settings</i>	24
<i>Classification settings.....</i>	28
<i>Visual tagging settings</i>	33
CUSTOM RULES	33

Overview

Under **Agent** we have all the options related with Agent (both v3 and v4) configurations. In this article we will focus on v4 configurations.

The most left column has four big buttons: **Overview**, **System**, **Plugins** and **Custom Rules**.

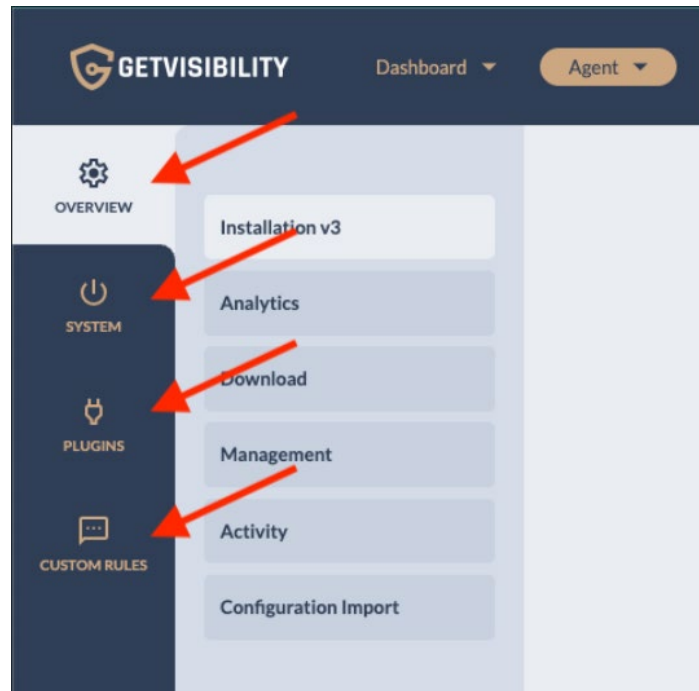


figure 1.

Analytics

This page gives an overview idea of the various agents in the organization. The page has different visual representation of the following:

- Top 10 users by activity
- Endpoint Distribution by OS
- Agent Incidents per Day
- Agent Incidents by Incident type
- Incident Distribution by User
- Latest Agent Incidents.

The admin can also the details in CSV file or JSON file format.

Download

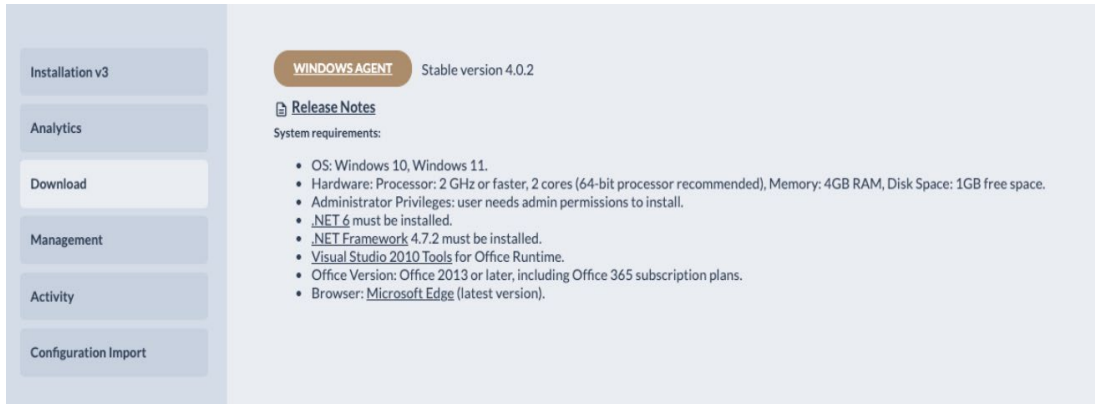


figure 2.

The Download button (if configured) enables the user to download the latest stable version of the agent and includes its minimum system requirements for proper operation.

Management

This page gives the user a high-level status of all the agents installed. Details like Name of agent, the IP address and When was the agent last seen is shown on this dashboard. User can also see if the agent is Online or not. It also has another field like Agent version, Operating System of Agent, and which department the agent belongs to. The admin can sort and export the details and also use the advance GQL query to filter out details.

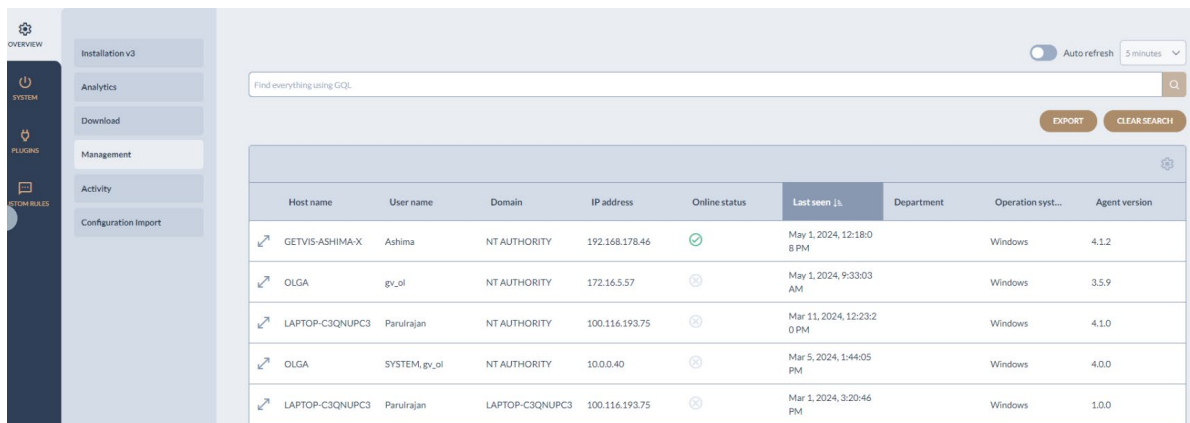


figure 3.

Activity

This page is for Admins that want a detail of the users' events using agents in MS Office and Outlook. Extensive tables detailing classification and email events are provided with various columns to display. The admin can sort and export the details and also use the advance GQL query to filter out details.

The various columns available on the activity page are:

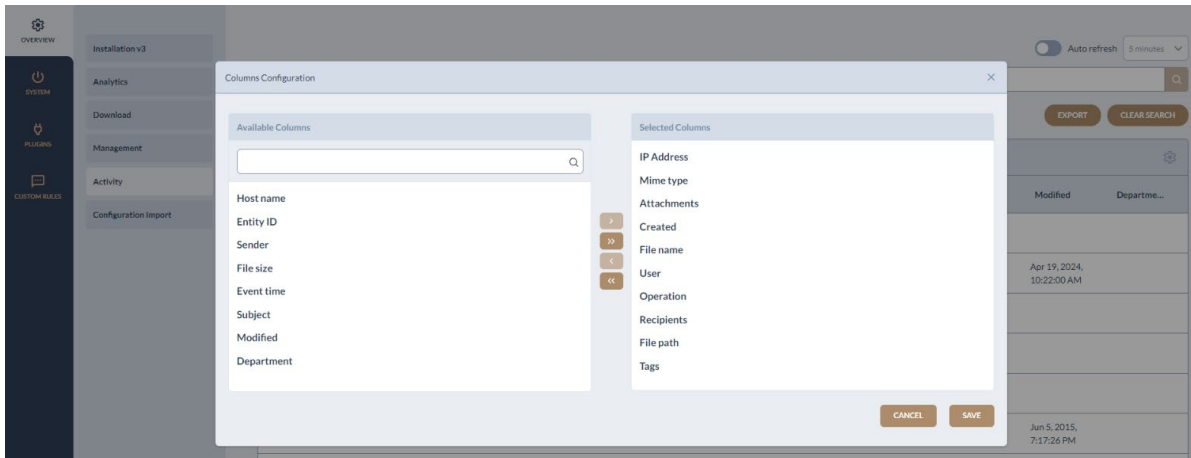


figure 4.

Details of the columns will be displayed with Export and GQL functions.

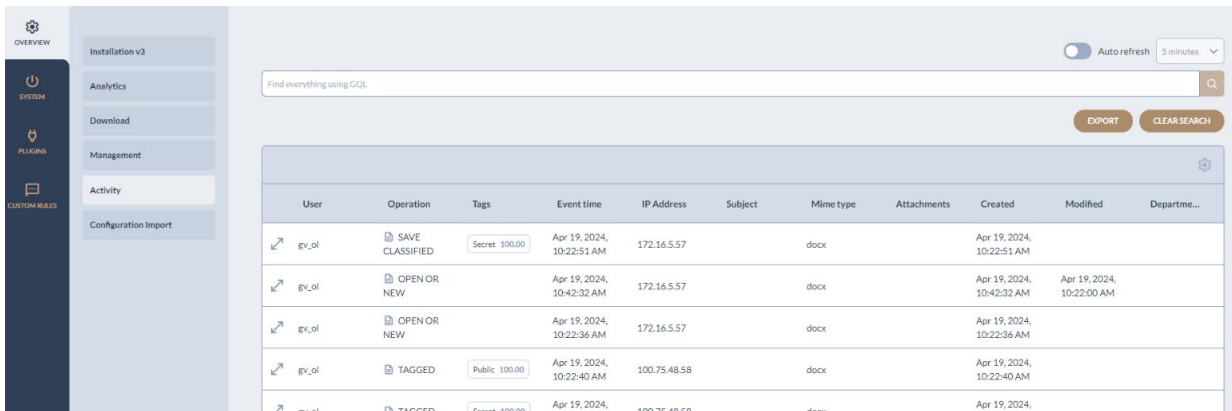


figure 5.

Configuration import

This section allows the user to import or download **agent v4** configurations in the form of .json files.

Select a configuration file to import

Once the user has chosen a JSON file, it will undergo a swift validation check. If the formatting is correct, the file will be displayed for comparison with the existing one.

A check-box will appear in order to approve import and click **Replace Configuration** down right.

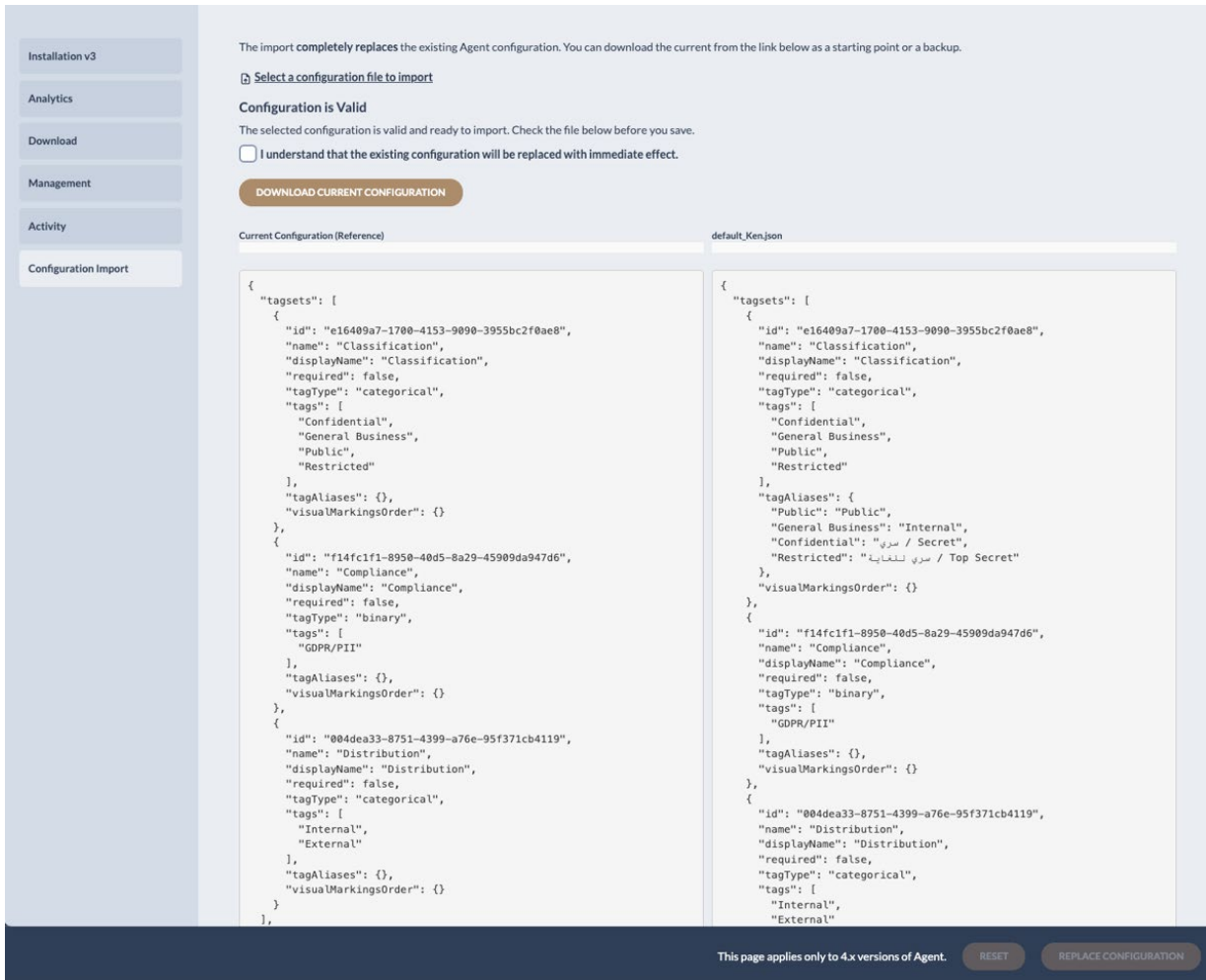


figure 6.

Download current configuration

This will download the latest configuration set, also, in the form of .json file. The file will have this kind of naming format “getvisibility-agent-configuration-20240402154432.json”

System

The System section provides general agent v4 configuration.

Global

Enable auto-update

This option will allow the agent to monitor for new stable releases and install them if available.

Auto-update: server URL or path → by **default**, the agent will look in for new artifacts to update from. If the user would like to use a specific URL or path to look for the artifacts, it should be configured here. The formatting should be as follows:

URL: https://path/to/web/server/containing/binaries/

Path: C:\path\to\artifacts\folder\

Auto-update: regex for agent packages to include → by default, the agent will use a regex pattern to look for artifacts that meet the same naming (`(\d+\.\d+\.\d+|\.)zip`) (e.g. `AgentClassifier.4.0.5-Forcepoint-windows.msi` will continue to look for Forcepoint-flavoured installers, whereas `GVClient.4.0.5-Getvisibility-windows.msi` will continue to look for Getvisibility-flavoured installers). The formatting should be as follows:

```
(flavour)\d+\.\d+\.\d+|\.)zip
```

Auto-update: check for updates frequency rate → this configures how often the agent will look for newer versions on the entered server auto-update server URL/path. Valid values should be 1 or higher, expressed in minutes.

Enable beta version update

This option will allow the agent to monitor for new beta releases and install them if available.

Machine names for receiving beta version

If no machine name is added here, no one will receive the beta updates.

Heartbeat frequency

This determines how often the agent will send a ping to the backend to report it's alive.

Supported languages

Languages set here will appear as options to select from the configuration section on the agent's tray bar icon

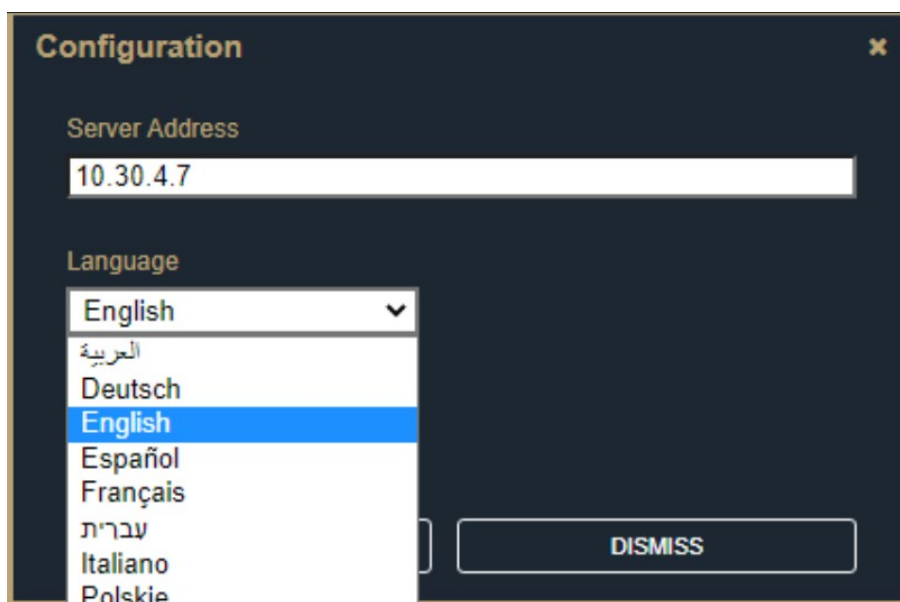


figure 7.

Agent suggestion frequency rate

Determines how frequently the agent sends text to the backend for analysis and feedback. It is expressed in seconds, with valid values starting from 1. The default value is 15.

Note that lower values may lead to performance issues, while extremely high values (e.g., 300) could result in no suggestions being received.

Minimum confidence threshold

ML suggestions always come with a confidence value. If the confidence value of the suggestion is higher than the threshold, it will be displayed.

If the confidence value of the suggestion is lower than the threshold, no suggestion will be displayed.

Agent: Disable Configuration Menu

If this option is checked, the **Configuration** menu will not be displayed when right-clicking on the agent's tray bar icon.

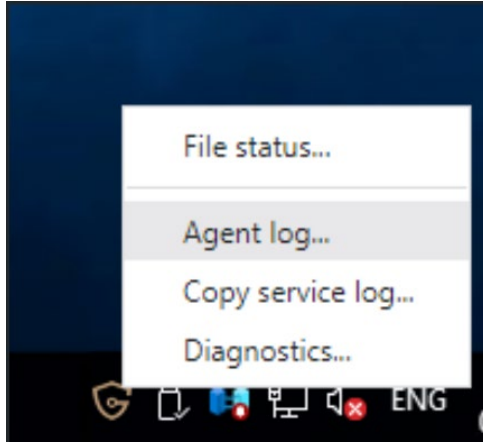


figure 8.

Block Server Address edit

If selected, the **Server Address** field will be grayed out, rendering it non-editable.

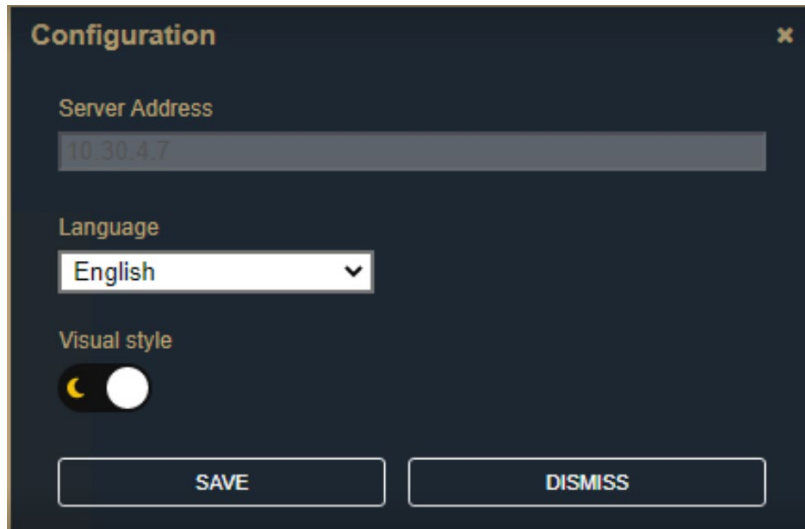


figure 9.

Help URL

Adds a link to the configured URL on the agent pop up window.

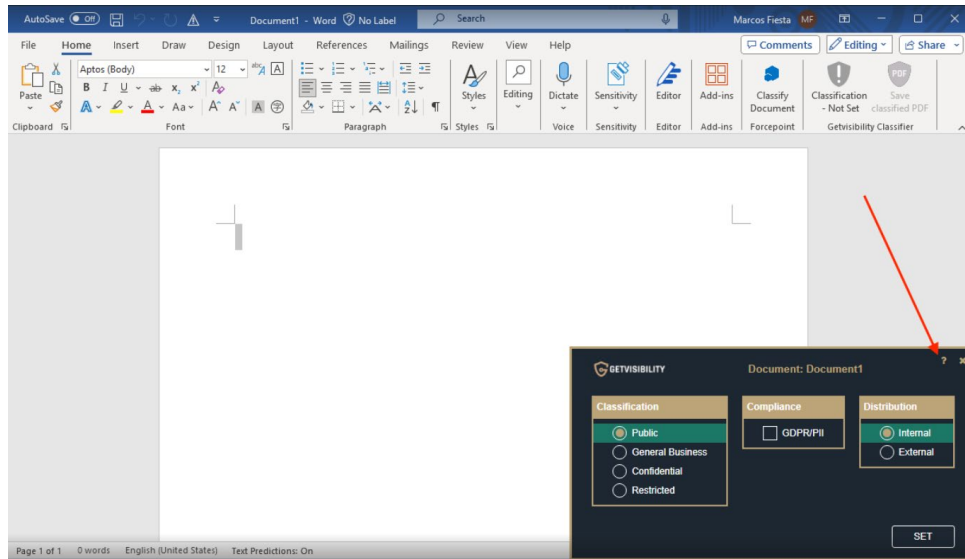


figure 10.

Ribbon title

Changes default **Classification** title.

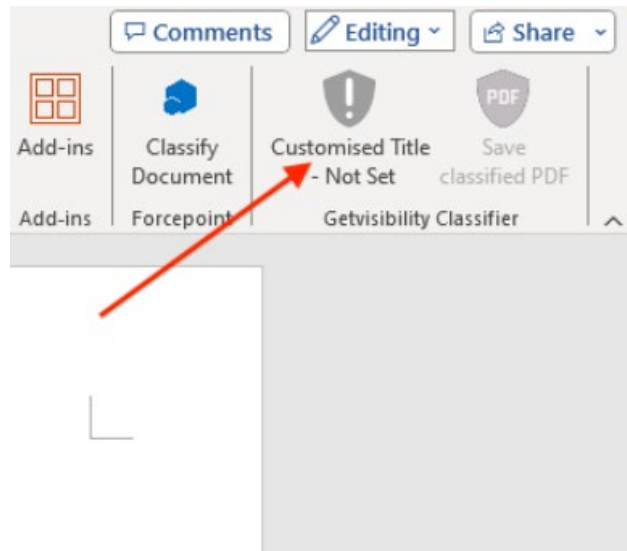


figure 11.

Order tag from top to bottom

Allows to order tags according to one of these criteria (for examples, **Public**, **General Business**, **Confidential**, **Restricted** were used):

- Most to least severe
- Least to most severe

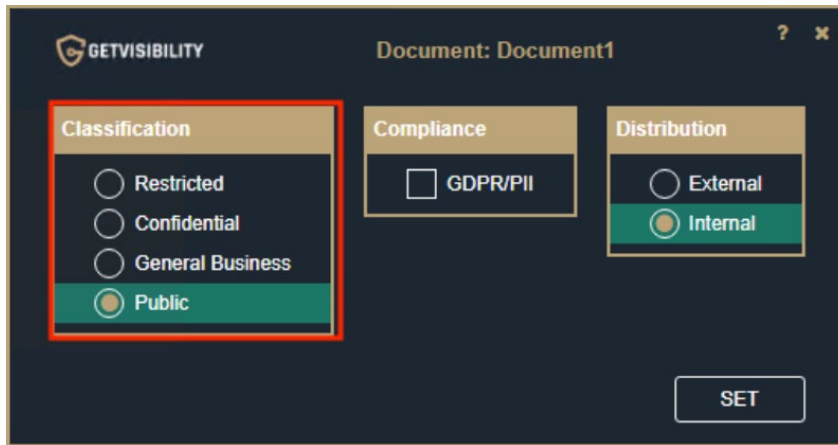


figure 12.

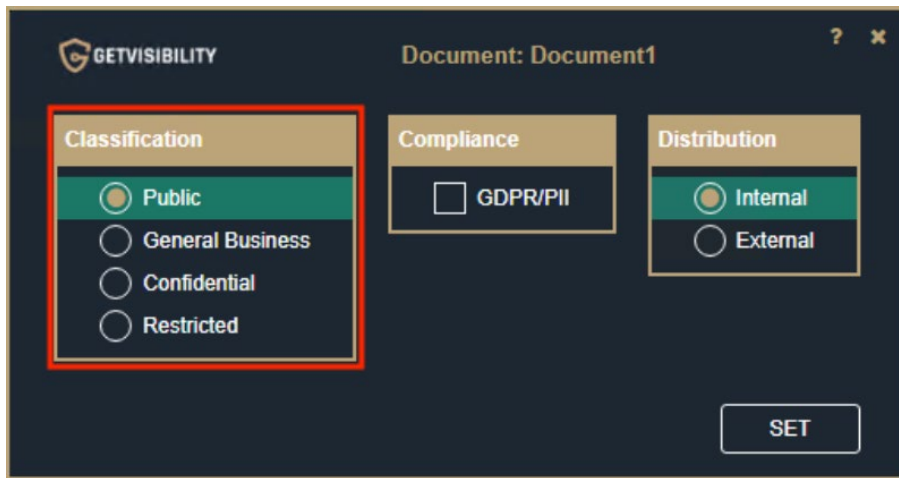


figure 13.

NOTE: The order in which the tagsets are defined (currently only by editing the .json file) is significant. For instance, in a three-level classification taxonomy (e.g., Public, Internal, Confidential), if these are defined as (Internal, Confidential, Public), Internal will be considered the lowest level and Public the highest.

```
"tagsets": [
  {
    "id": "e16409a7-1700-4153-9090-3955bc2f0ae8",
    "name": "Classification",
    "displayName": "Classification",
    "required": false,
    "tagType": "categorical",
```

```

"tags": [
  "Internal",
  "Confidential",
  "Public"
],
"tagAliases": {},
"visualMarkingsOrder": {}
},

```

Plugins

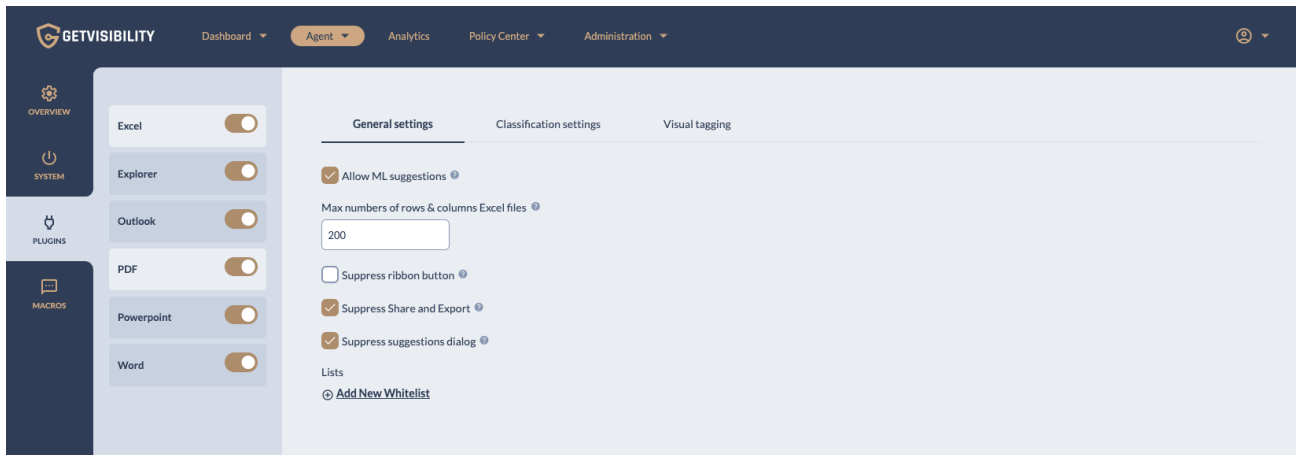


figure 14.

This section enables users to easily activate or deactivate the **Excel**, **Explorer**, **Outlook**, **PDF**, **PowerPoint**, and **Word** plugins.

When a plugin is deactivated, its corresponding Ribbon will appear grayed out when opening the application, and no actions from the classifier will be executed.

Word, **Excel**, **PowerPoint**, and **Outlook** plugin configurations are quite similar and share several commonalities. However, there are also specific configurations that apply uniquely to each of them.

Firstly, we will address the **Shared Configurations** across all apps before delving into the specifics for each one.

Shared Configurations

General Settings

Allow ML suggestions

This option will enable/disable sending text to the backend in order to generate suggestions based on an ML model. If enabled, agent will receive suggestions.

Suppress ribbon button

This option will hide the ribbon button on selected app.

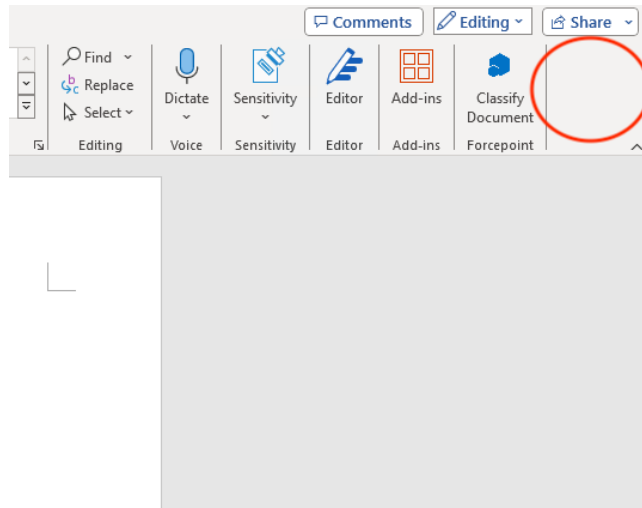


figure 15.

Suppress Export and Share

This option will remove **Export** and **Share** buttons from the **File** menu on the selected app.

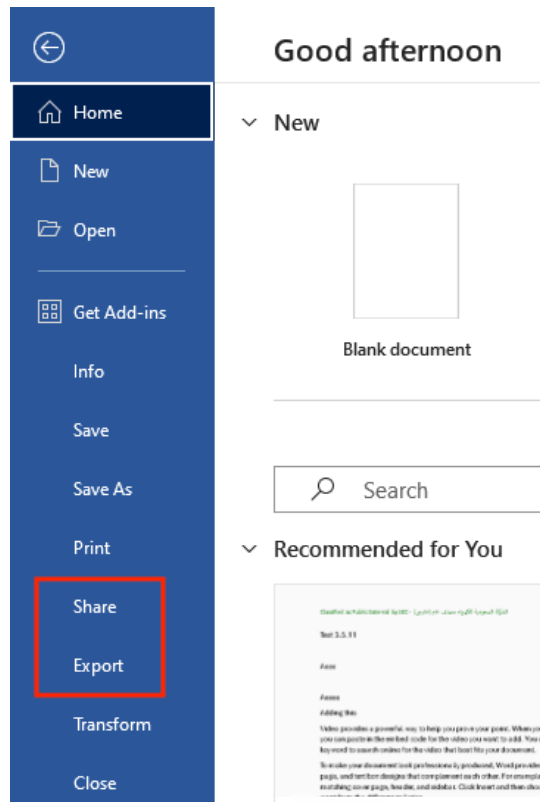


figure 16.

Suppress suggestions dialog

Enabling this option will prevent suggestion pop-ups from appearing. Suggestions will be visible when you click on the **Classification** button.

NOTE: Please make sure to check **Allow ML suggestions** to receive suggestions.

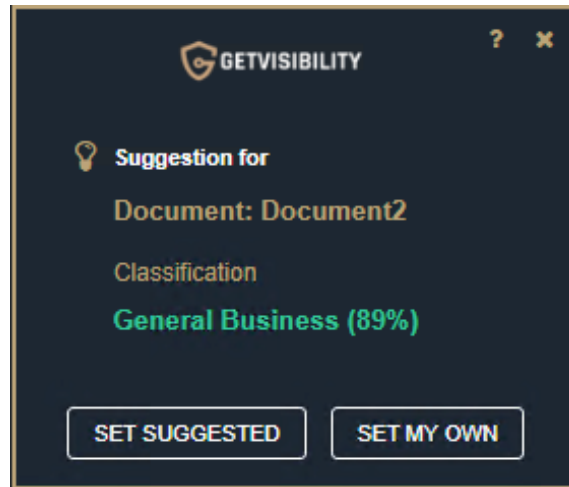


figure 17.

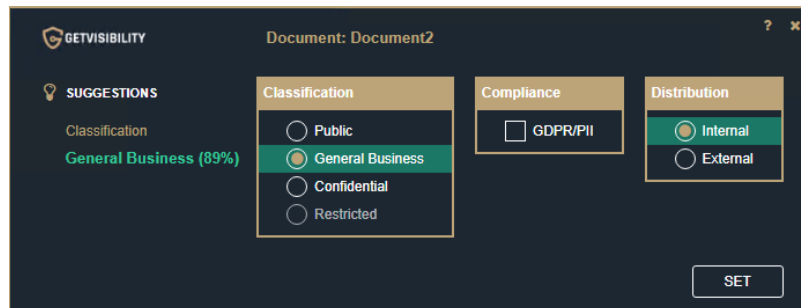


figure 18.

Add New Whitelist

This option will allow a certain user or domain to classify with selected classification. Whitelists can be created for Classification, Distribution or Compliance. Once created, if no one is whitelisted, no one will access selected tagset.

For example, if `mycompany.domain.com` is whitelisted for `Restricted` tagset, a user not belonging to it will see the selected tagset grayed-out (see screenshot above).

Notice that the field legend says, 'You can use both users (`user@domain.com`) or domains (`domain.com`) when adding new items to this list'. To get this information, you can go to the Command Prompt and run `"whoami."` This command will return the `machinename\username` value.

```
C:\> Administrator: Command Prompt

Microsoft Windows [Version 10.0.20348.2031]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator>whoami
marcos3\administrator

C:\Users\Administrator>
```

figure 19.

Then, you can simply right-click on **This PC** and select **Properties**. Under the **Full device name**, you will find the domain to which the machine belongs.

Device specifications	
Device name	marcos3
Full device name	marcos3.JIRIS-AD.local
Processor	AMD EPYC 7R13 Processor 2.65 GHz
Installed RAM	16.0 GB (15.6 GB usable)
Device ID	5226B783-C86C-48B8-824D-0C243D94D7A7
Product ID	00454-60000-00001-AA088
System type	64-bit operating system, x64-based processor
Pen and touch	No pen or touch input is available for this display

figure 20.

Lastly, we can enter `username@domain` or `domain` to whitelist.

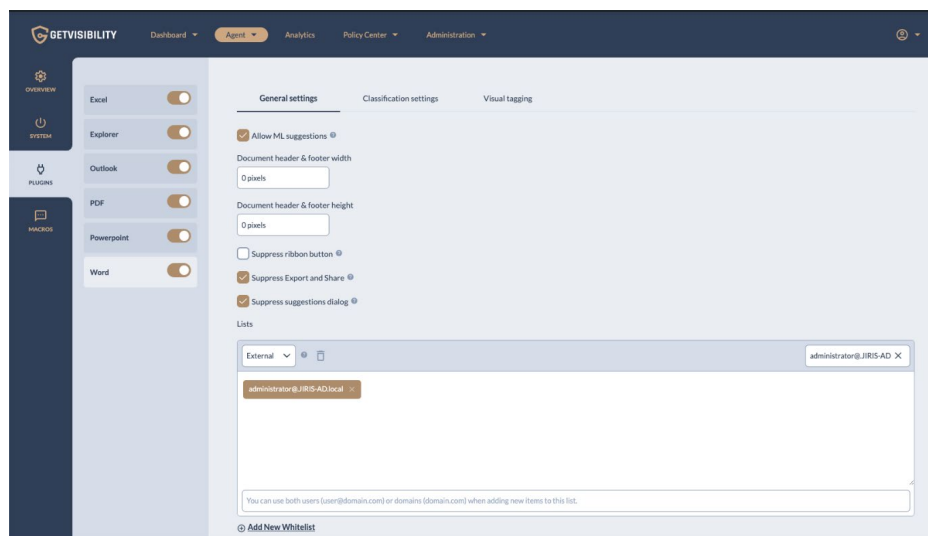


figure 21.

NOTE: you can also use Office's login user/domain to achieve the same results.

Classification settings

Allow lowering the level of Classification

This option enables re-classifying files with a lower level of **classification**. The process involves opening a file, making edits, classifying it, saving the changes, and then closing it.

Upon reopening the file, lower levels of classification will be enabled or grayed out if checked or unchecked, respectively.

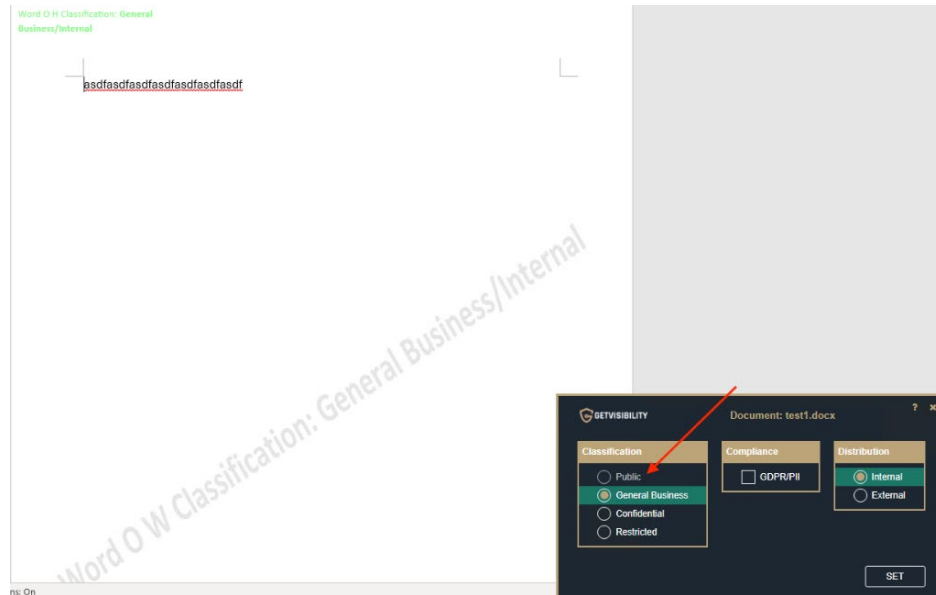


figure 22.

Allow lowering the level of Distribution

Similarly, as the one before, this option enables re-classifying files with a lower level of **distribution**. The process involves opening a file, making edits, classifying it, saving the changes, and then closing it.

Upon reopening the file, lower levels of distribution will be enabled or grayed out if checked or unchecked, respectively.

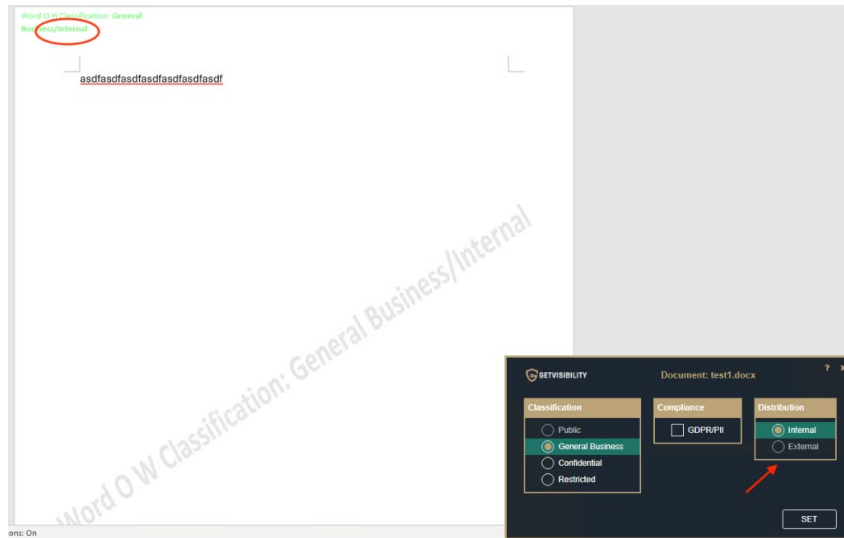


figure 23.

Default Classification

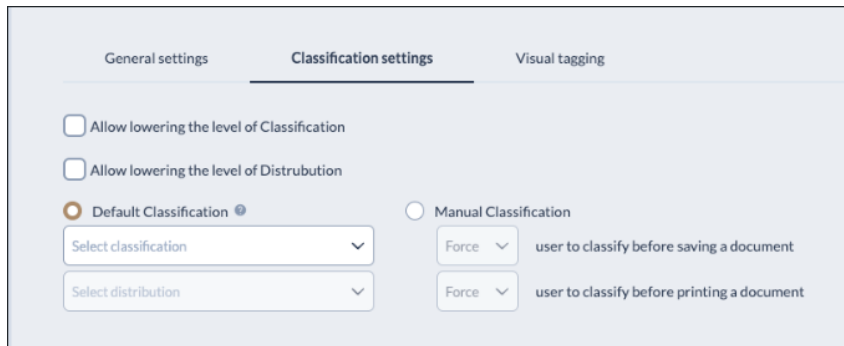


figure 24.

Here, users have the option to set default values for Classification and/or Distribution. This allows the desired set tagsets to be automatically applied upon **Saving** or **Printing**.

It is important to note that the triggers for automatic application are limited to **Saving** and/or **Printing**, so simply editing the file will not result in classification (or distribution) tags being applied.

Manual Classification

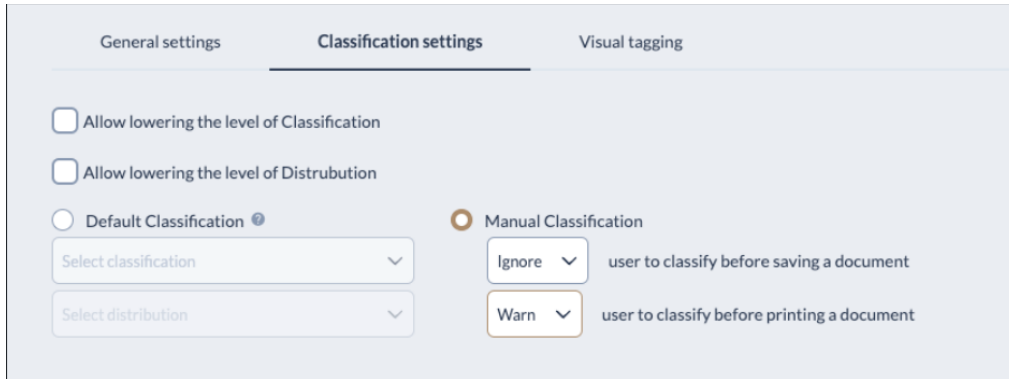


figure 25.

As opposed to **Default Classification**, manual intervention is required here. The agent's behavior on the two triggers offers three options:

- **Ignore**: If the user does not classify the file, there will be no pop-up upon saving (or printing), only logging activity will occur.
- **Warn**: When the user does not classify the file and attempts to save (or print), a warning pop-up will appear. It provides them with the choice to classify (**SET MY OWN**) or proceed without classifying (**SAVE ANYWAY**).

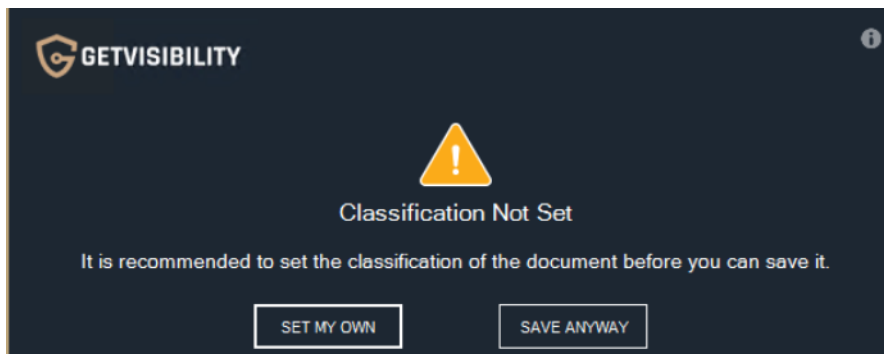


figure 26.

NOTE: For printing the warning pop up is quite similar.

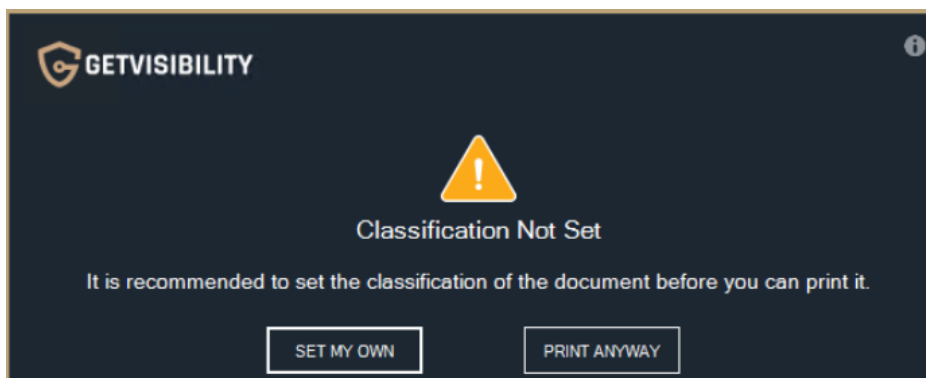


figure 27.

- **Force:** if the user does not classify the file, upon saving (or printing) a pop up will be shown, forcing them to classify (**SET MY OWN**).

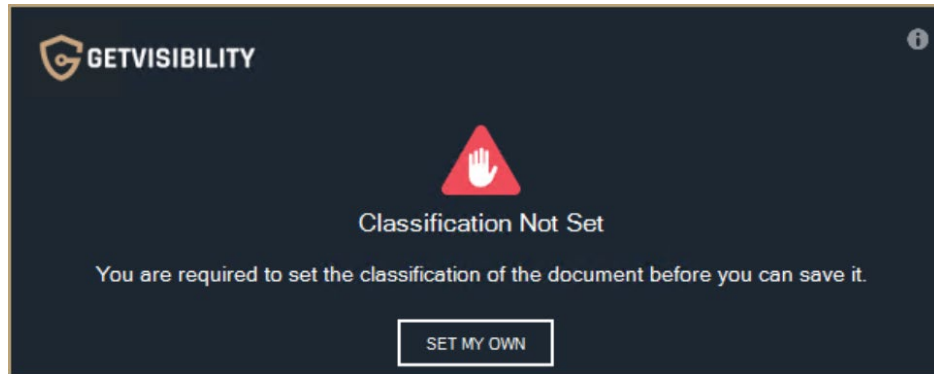


figure 28.

NOTE: For printing the force pop up is quite similar.

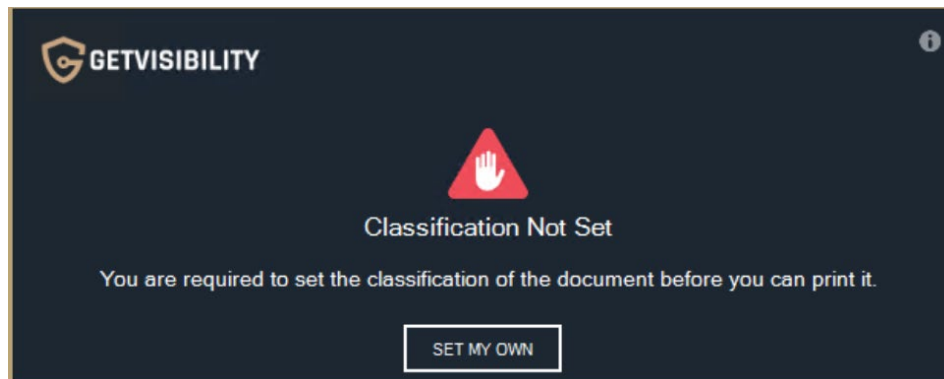


figure 29.

Machine learning accuracy classification threshold (%)

As it was mentioned before, ML suggestions always come with a confidence value. This option allows the agent to **ignore**, **warn** or **force** user to select the suggested classification tag or a higher one.

Notice that the pop-up windows (in the event of selecting 'warn') will only appear when you **SAVE**. If you perform regular document editing or manual classification, the pop-up will NOT be displayed.

- **Ignore:** when receiving a suggestion, users will have the option to select a lower classification tag than the suggested one.
- **Warn:** when receiving a suggestion, users will be warned when selecting a lower classification tag than the suggested one.

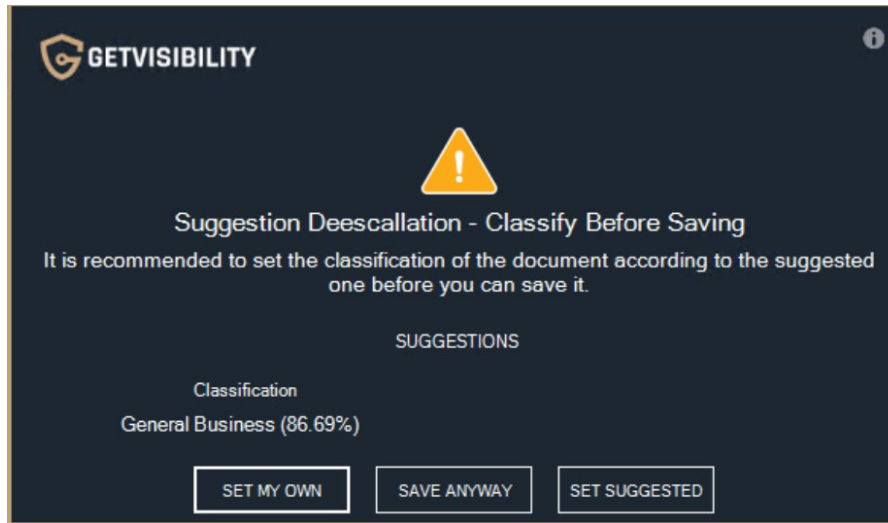


figure 30.

→ **Force:** when receiving a suggestion, users will be forced to select the suggested classification tag or higher.

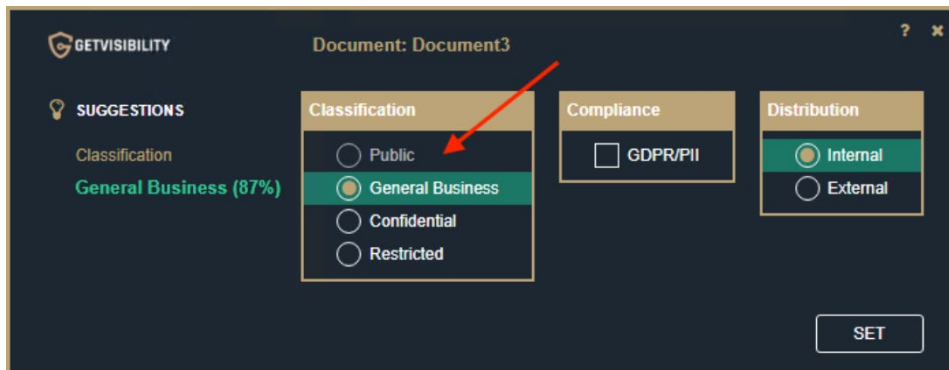


figure 31.

The threshold percentage indicates the minimum confidence required for these triggers. This means that if the ML suggestion's confidence level is lower than the set threshold, no warning or enforcement will occur.

Auto Classification Configuration

This feature enables users to automatically classify items based on machine learning (ML) suggestions. When the confidence level of an ML suggestion exceeds the chosen threshold, the selected classification, distribution, or compliance will be applied without manual intervention.

NOTE: A new configuration can be added with the 'Add new auto-classification configuration' button, to apply a different category, and select a different threshold as well.

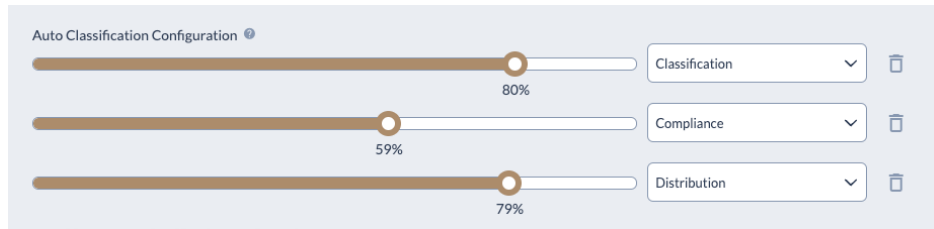


figure 32.

Visual Tagging

Always show visual tags configuration popup

If checked, the user will see the **Visual Label Options** popup window and will be able to configure them on each **SAVE** or **PRINT** trigger.

If un-checked, visual markings will be applied to all pages. Pop-ups will only be shown in the cases where user input is required to decide on ambiguity between the config and the current document.

The popup is slightly different depending on if Word, Excel, or PowerPoint is being used.

Notice there are no pop-ups in Outlook as there is no concept of title pages or different header/footer types (floating/fixed).

Word

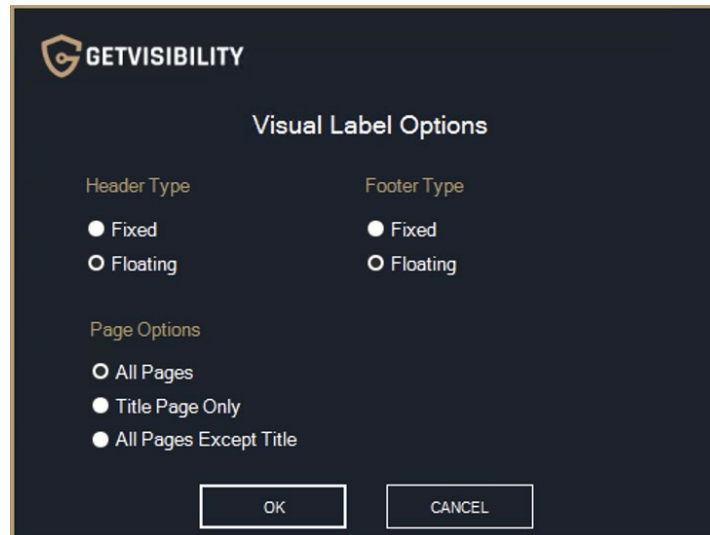


figure 33.

Header/Footer Type: Here, the user can choose the type of header and footer they wish to apply. The options for are:

- **Fixed** - Adds the header/footer text to the standard text area.
- **Floating** - Creates a text box within the header/footer area. This avoids any conflicts with existing headers/footers and allows for more flexible placement (i.e. typically to place the marking at the very top/bottom of the page).

NOTE: The actual alignment (left corner, right corner, centre) is determined by the text-align style attribute from the header/footer configuration.

Page Options - 3 choices: **Title Page Only**, **All Pages**, **All Pages Except Title Page**

Threshold: If the number of pages in the document is greater than or equal to the threshold only then visual labels will be applied to the **Title Page Only** or **All Pages Except Title Page**.

Excel

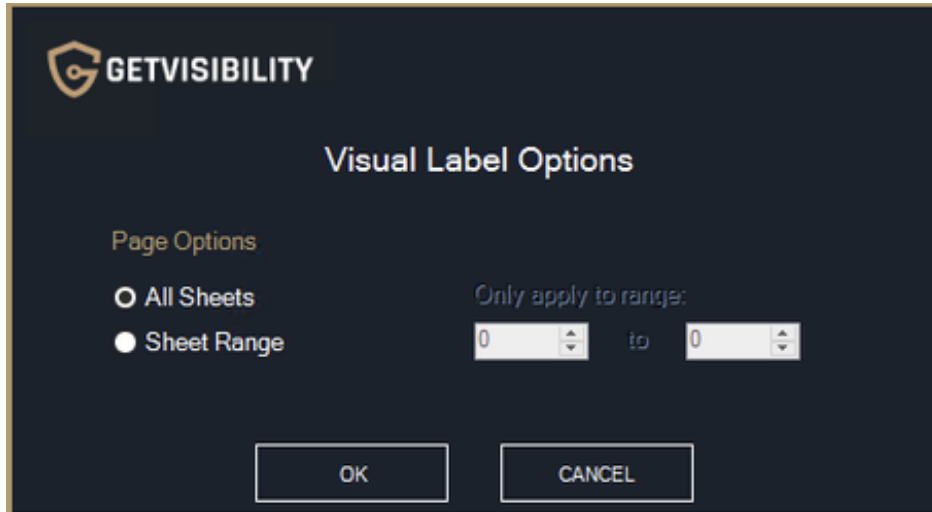


figure 34.

PowerPoint

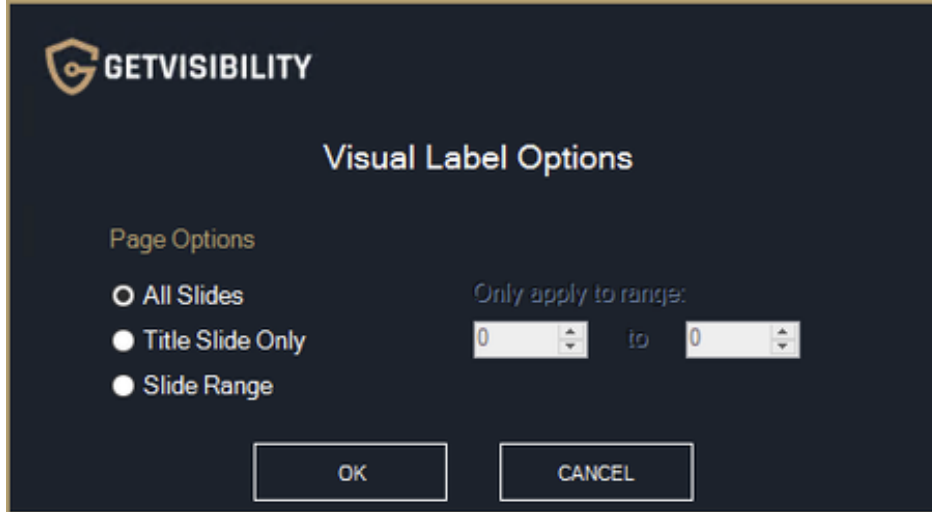


figure 35.

Enforce page layout option

This will set the chosen option by default without prompting the **Visual Label Options** pop-up.

Again, the options are slightly different depending on if **Word**, **Excel**, or **PowerPoint** is being used.

Word

Page Options - 3 choices: **Title Page Only, All Pages, All Pages Except Title Page**

Threshold: If the number of pages in the document is greater than or equal to the threshold only then visual labels will be applied to the Title Page Only or All Pages Except Title Page.

Excel

Page Options - 2 choices: All Sheets, Sheet range.

NOTE: The chosen numbers do not refer to the names of the sheets in Excel (“Sheet1”, “Sheet3”, etc) as these are re-nameable placeholder names. They refer to sheets counting from left to right.

To use this, please use the `fromSheet` and/or `toSheet` fields in Excel configuration. If excluded from config or both set to 0, markings will be applied to all sheets.

PowerPoint

Page Options - 3 choices: **All Slides, Title slide only, Slide range**

Threshold: If the number of pages in the document is greater than or equal to the threshold only then visual labels will be applied to the Title Page Only or All Pages Except Title Page.

Enforce Header and Footer type

If this option is selected it will apply the chosen option on **Headers** and **Footers**.

As explained before, there are two options here:

→ **Floating:** creates a text box within the header/footer area. It looks like this:

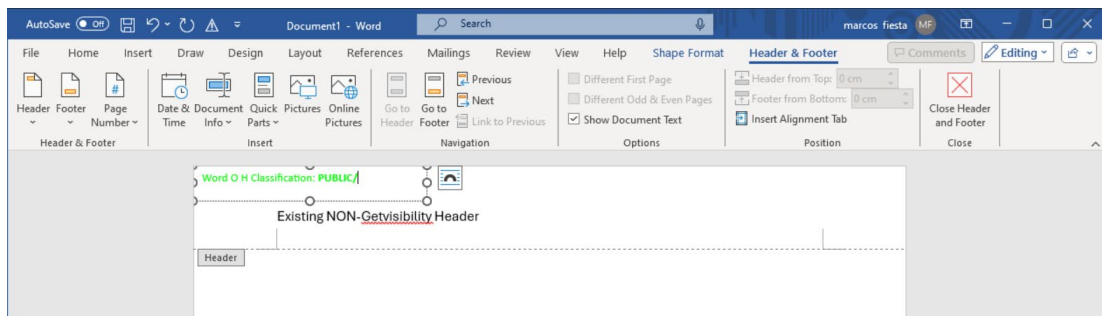


figure 36.

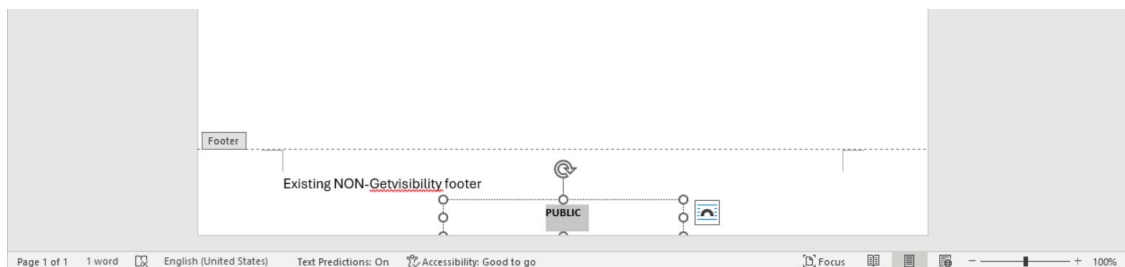


figure 37.

→ **Fixed:** adds the header/footer text to the standard text area. It looks like this:

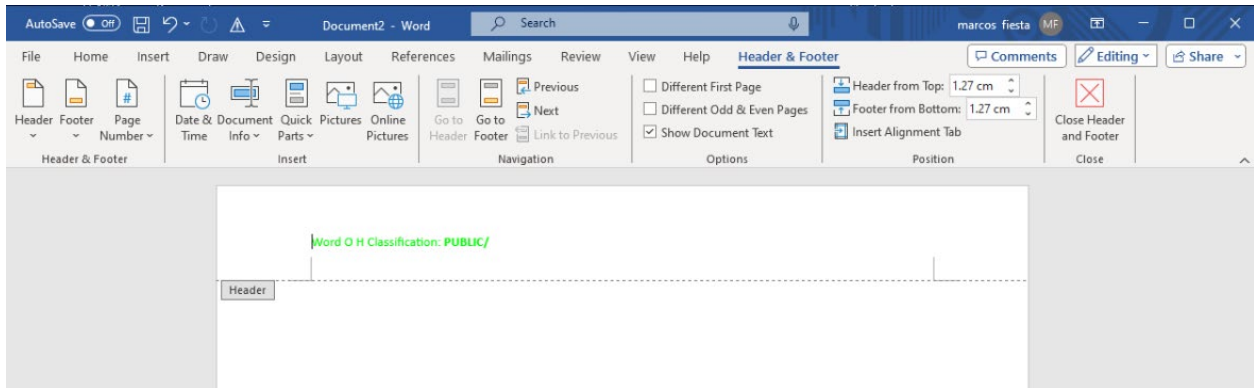


figure 38.



figure 39.

Enforce overwrite option

If this option is selected it will apply the chosen option on **Headers** and **Footers**.

Before going through the available options, a clarification on what this implies. This option will act over the visual markings on the selected header/footer type (refer to the 'Enforce Header and Footer type' section).

Available options are:

- **Overwrite:** the existing header or footer will be deleted, and the new one will be written.
- **Append:** the new header or footer will be added after the existing one.

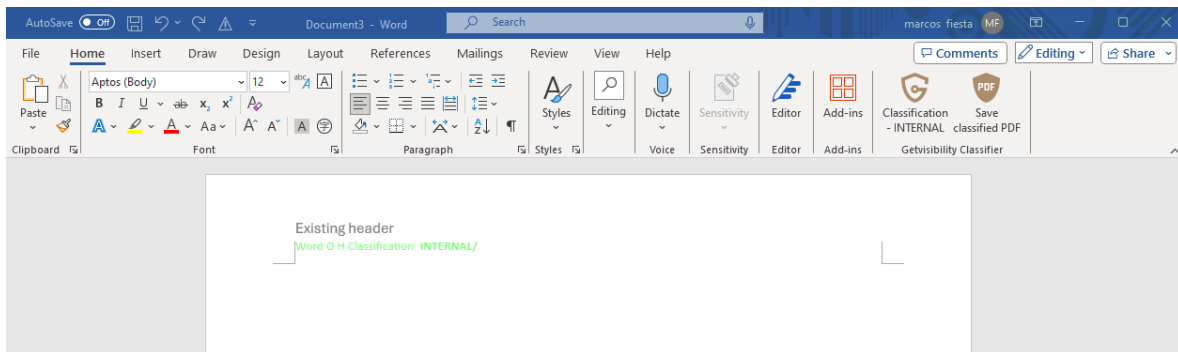


figure 40.



figure 41.

NOTE: For **FIXED** visual markings, If there is an existing **Header/Footer** prior to classifying and **Overwrite** option is selected, upon manual classification or trigger (print/save), existing visual marking will be overwritten.

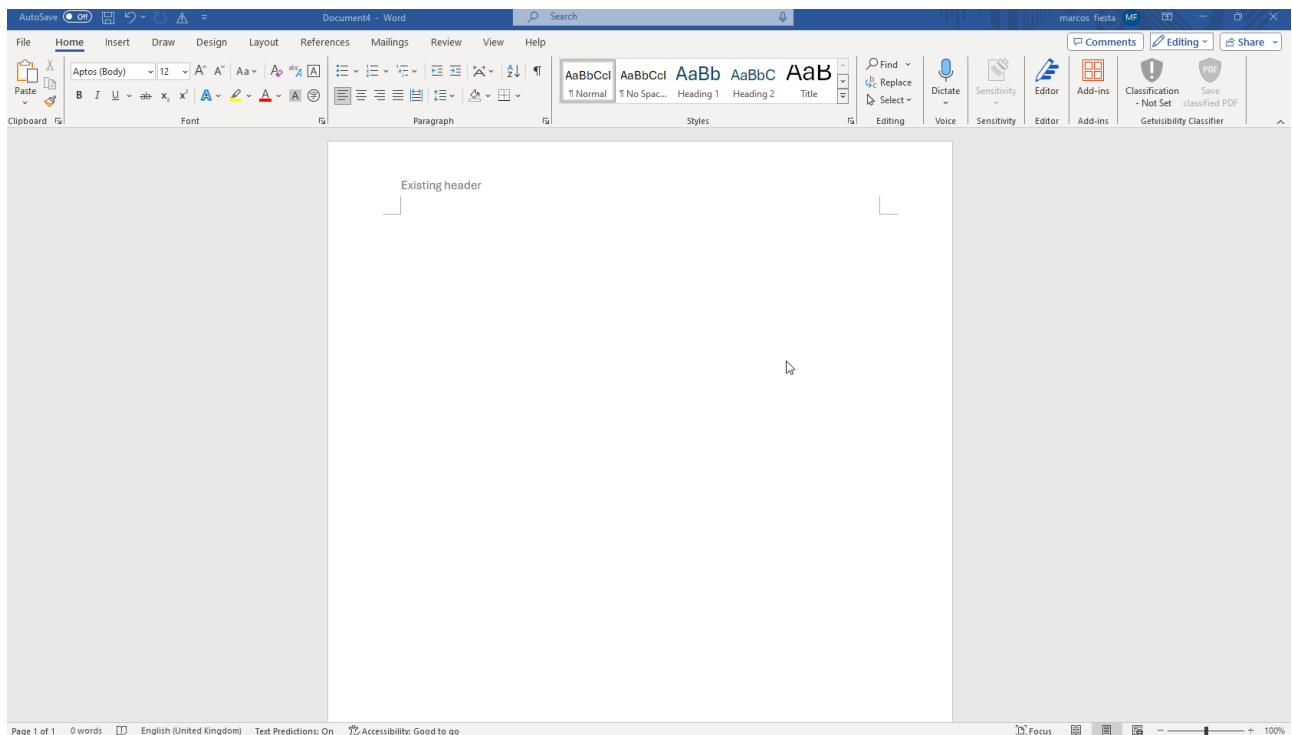


figure 42.

If this option is unchecked (no enforce), and in the case where the document already has a “fixed” header/footer and the user chooses this option in the **Visual Label Options** pop up, they will be asked if they wish to append the marking to the existing text or overwrite it. This is not shown if selected “Floating” is selected.

Show header/footer/watermark (and title/subtitle for PPT)

In this section the user can insert the content of visual markings. Text should be written in HTML language, please refer to this article for more information.

Forcepoint Data Classification Powered by Getvisibility Agent Guide for Writing Visual Labels

Variables

As highlighted in the article, a 'classification' variable is utilized. Additionally, there are several others that can also be employed. Here is a list of these variables:

- classification - shows classification output including aliases
- classification_raw - shows classification output, does not include aliases
- classification_guid - unique id generated based on tagset id and tag name
- distribution - shows distribution output including aliases
- distribution_raw - shows distribution output, does not include aliases
- distribution_guid - unique id generated based on tagset id and tag name
- compliance - shows compliance output including aliases
- compliance_raw - shows compliance output, does not include aliases
- compliance_guid - unique id generated based on tagset id and tag name
- datetime - timestamp for classification, with this format "yyyy-MM-dd\\THH:mm:ss\\Z"
- email
- user - current user name
- machineid - device name
- fileid - Getvisibility id assigned for the classified file

This is an HTML header or footer example that uses all of them

```
<span>classification - {classification} | classification_raw {classification_raw} |
classification_guid {classification_guid} | distribution {distribution} | distribution_raw
{distribution_raw} | distribution_guid {distribution_guid} | compliance {compliance} |
compliance_raw {compliance_raw} | compliance_guid {compliance_guid} | datetime {datetime} |
email {email} | user {user} | machineid {machineid} | fileid {fileid}</span>
```

And this is the output for a default configuration, Public - GDPR/PII - Internal classification:

```
classification - Public | classification_raw Public | classification_guid 13d38db9-2856-70ed-
377c-2844870099bd | distribution Internal | distribution_raw Internal | distribution_guid
623852d7-e653-49e5-892a-1a607b4e6c4a | compliance GDPR/PII | compliance_raw GDPR/PII |
compliance_guid d6046d4c-e562-c94a-a2e1-0665cd09a654 | datetime 2024-04-10T10:59:53Z | email |
user Administrator | machineid MARCOS3 | fileid dd8543fc-0a77-4374-887d-5cc03054030a
```

NOTE: These variables can also be utilized to write metadata. Currently, this can only be edited in the .json file and not through the UI.

Exclusive Configurations

Explorer

Explorer plugin refers to right-clicking over a file in order to classify, for supported files other from **Word, Excel, PowerPoint, and Outlook**. For this, user only has the option to:

Allow lowering the level of Classification

Classification can be changed to a lower level. For example, a file classified as **Confidential** is then classified as **Public**.

Allow lowering the level of Distribution

Distribution can be changed to a lower level. For example, a file which distribution is set as **External** is changed to **Internal**.

General settings

Excel

Max numbers of rows & columns Excel files

This setting determines the maximum number of rows and columns that the agent will scan to extract text and send it to the backend for additional analysis.

It is important to note that this process occurs for every sheet, which can consume significant resources. To enhance performance, consider reducing this value.

Outlook

Specify maximum number of recipients

This value specifies how many recipients can be added when sending an email.

When including more recipients than the value set, a pop-up message will appear. If 0 is set, unlimited recipients can be added.

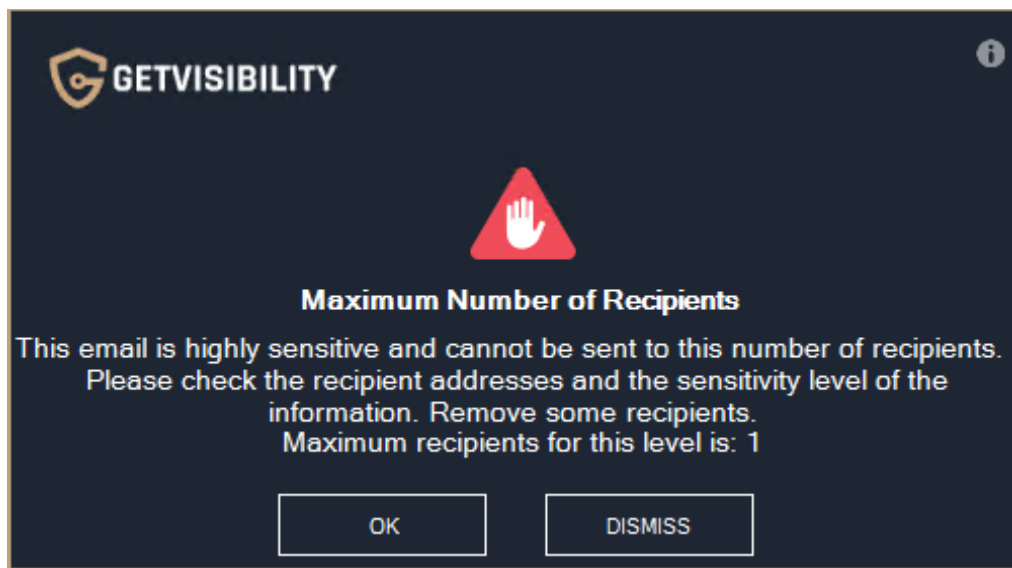


figure 43.

File extension to exclude

This section enables the user to specify the images, audio & video, or other file types from attached files that will not be checked for tags.

Allow

Specific group of users or domains allowed as **recipients**. Any user or domain not included in this list will be unable to be sent emails.

This option is not restrictive, meaning that if left empty, all users or domains **recipients** are considered allowed.

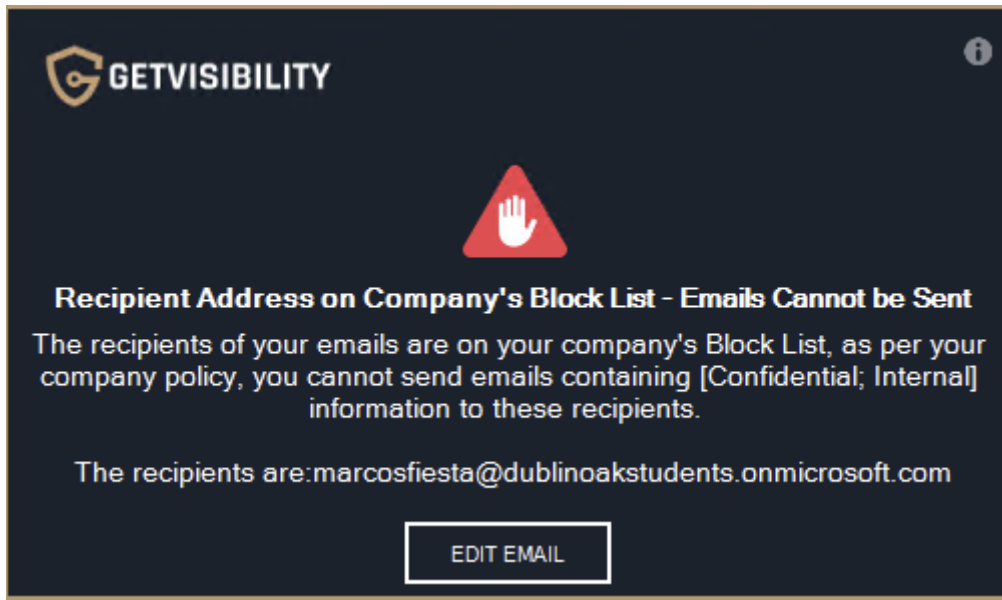


figure 44.

Permission to send

Specific group of users or domains allowed as **sender**. Any user or domain not included in this list will be unable to send emails.

This option is not restrictive, meaning that if left empty, all users or domains **senders** are considered allowed.

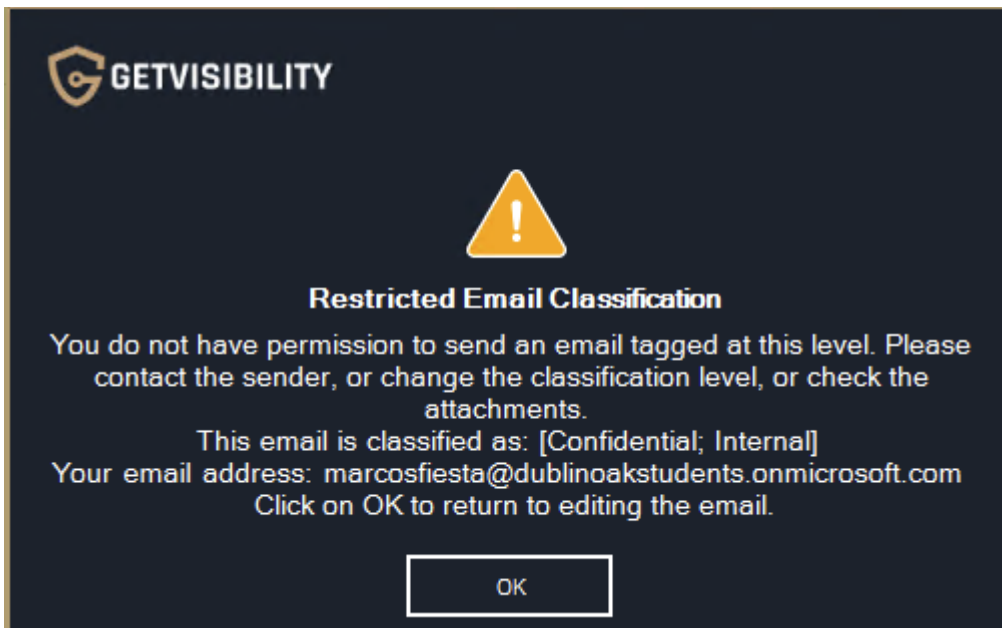


figure 45.

Block

Specific group of users or domains blocked as **recipients**. Emails to any user or domain included in this list will be blocked upon sending.

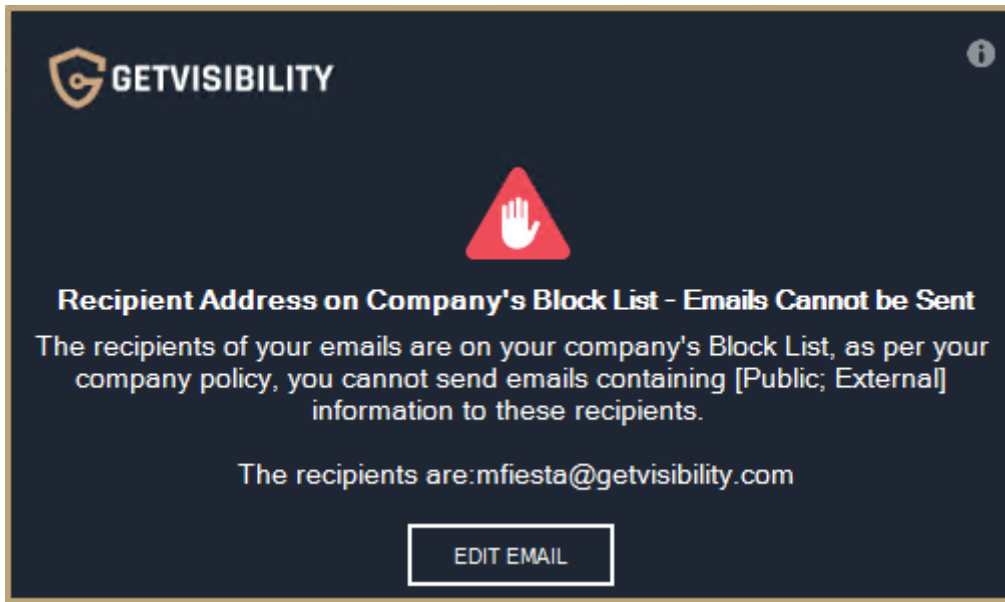


figure 46.

Warn

Specific group of users or domains blocked as **recipients**. Emails to any user or domain included in this list will be warned upon sending.

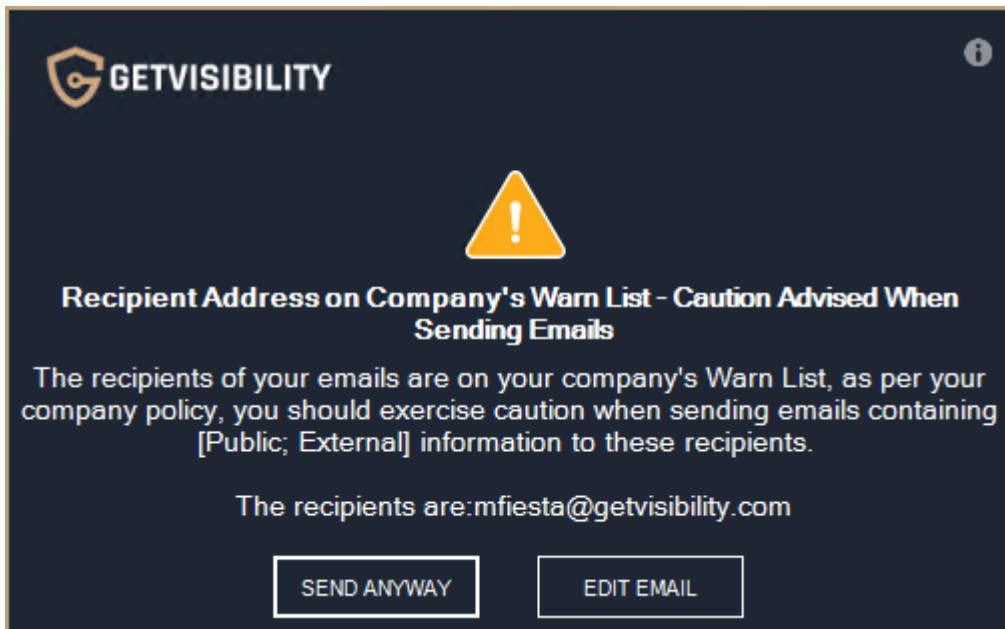


figure 47.

Powerpoint

All settings already covered in the **Shared Configuration** section.

Word & PDF

Document header & footer width

This value applies to the default width for floating headers and footers.

Document header & footer height

This value applies to the default height for floating headers and footers.

Classification settings

Excel

All settings already covered in the **Shared Configuration** section.

Outlook

Default email policy

This option gives the user the ability to **Allow (Ignore)**, **Warn (Warn)**, or **Block (Force)** emails by default. It is designed to complement the **Allow**, **Permission to Send**, **Warn**, and **Block** domains found in the '**General settings**' section.

For example, abc@domain.com is in the **Allow** list. If default email policy is set to '**Force**' and the user sends a **classified** email to another domain, they will get a **Block** sign like this

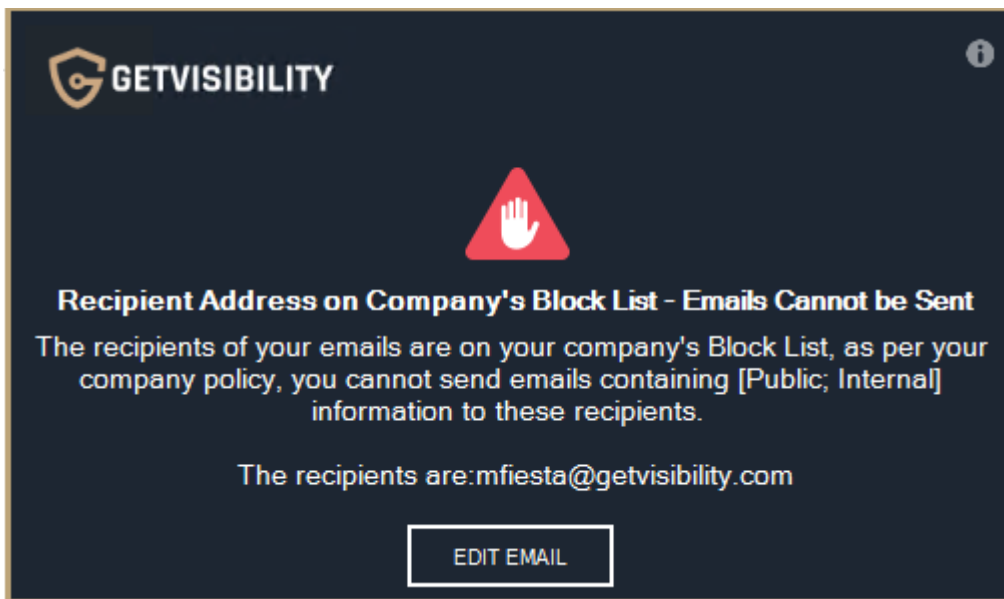


figure 48.

The **Default** email policy operates with **classified emails** in conjunction with the allowed, permitted to send, warned, or blocked domains. If none are set, this email policy will not trigger.

Continuing with the same example, if **Default Classification** is chosen, **Default** email policy will trigger.

General settings **Classification settings** Visual tagging

Default email policy
Force ▾

Attachment Classification lower than email policy
Ignore ▾

Unclassified attachments policy
Ignore ▾

Allow lowering the level of Classification

Allow lowering the level of Distrubution

Auto classify on reply/forward

Classify emails same as attachments

Classify attachments same as emails

Show prefix classification on email subject ?

Show suffix classification on email subject ?

Default Classification ? Manual Classification

Public ▾ Warn ▾ user to classify before sending an email

Internal ▾ Warn ▾ user to classify before printing an email

figure 49.

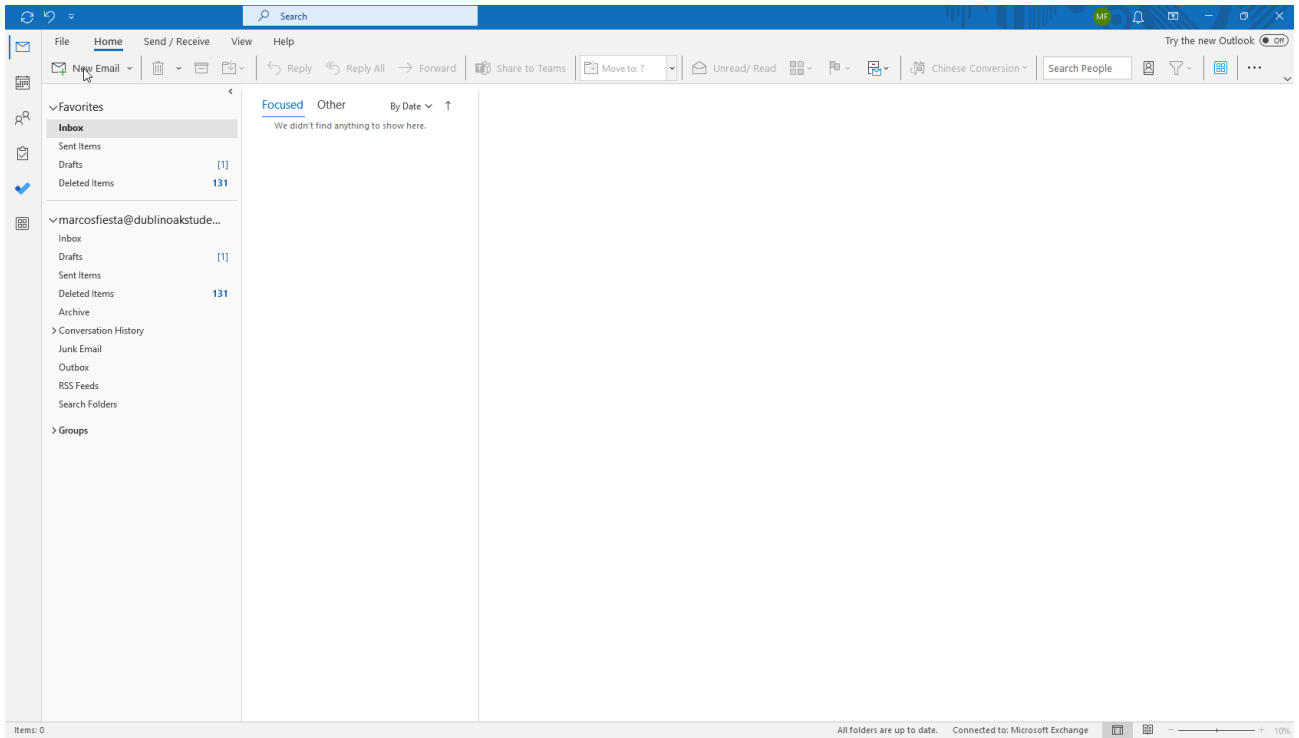


figure 50.

NOTE: If the email is sent without classification (or a warning is set to continue), Default email policy will not trigger as Default email policy is bypassed by Manual classification).

Attachment Classification lower than email policy

Here the user can choose to **Ignore**, **Warn**, or **Force**, if attachment's classification is **higher** than email's classification.

NOTE: There is a discrepancy between the title and the actual behavior. The condition will be triggered (ignore, warn, or force) if the attachment's classification is **HIGHER** than that of the document.

Unclassified attachments policy

This option enables users to choose whether to ignore, receive a warning, or be required to classify attachments when an unclassified one is attached.

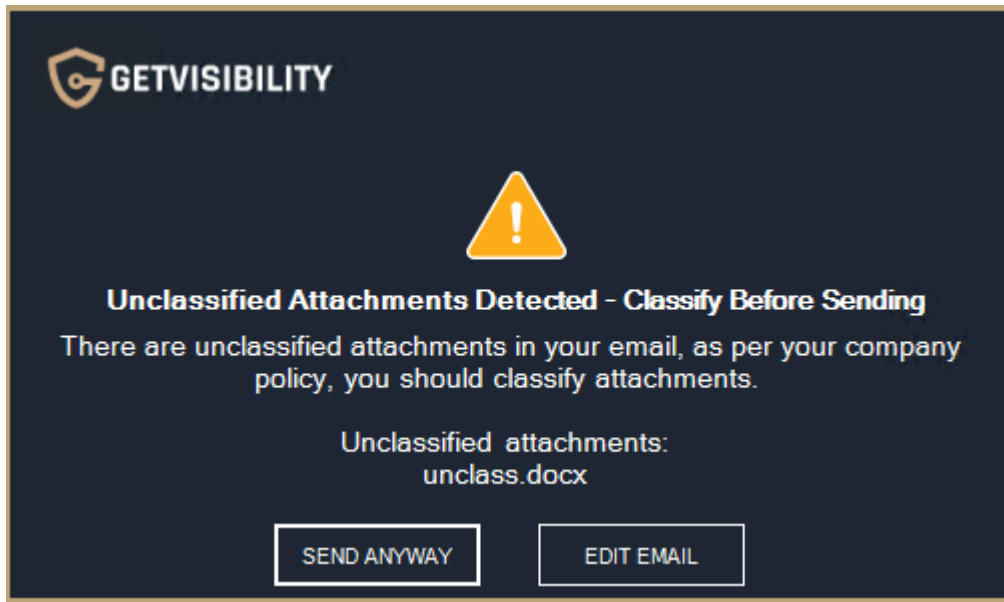


figure 51.

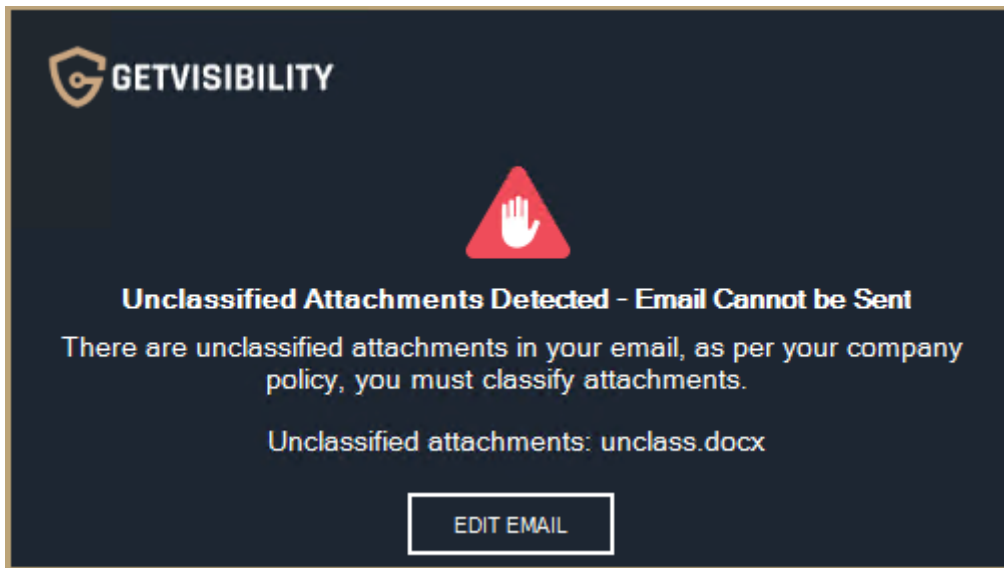


figure 52.

NOTE: if 'Classify attachments same as emails' option (described below) is enabled, and attachment classification is lower than the email classification, the attachment will be classified automatically, not triggering this warning.

The same will happen if **Default Classification** for emails is set.

Auto classify on reply/forward

This option enables users to inherit the original email classification when replying, replying all, or forwarding an email.

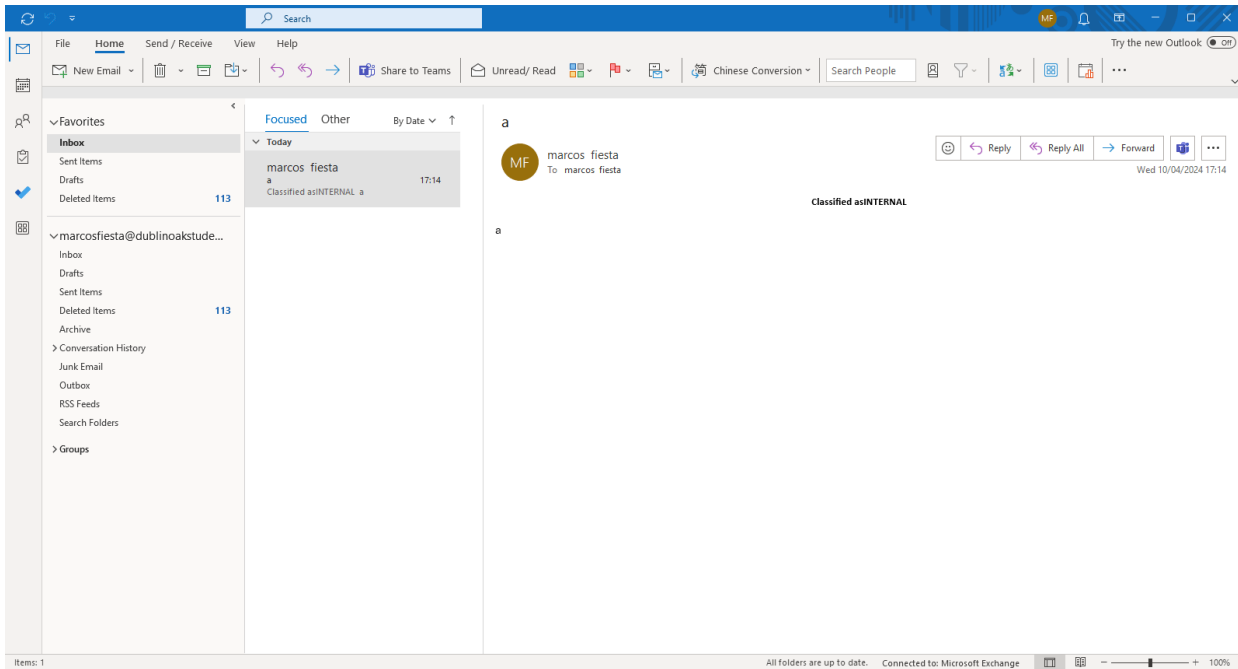


figure 53.

Classify emails same as attachments

This option enables users to inherit classification from attachments if no classification is manually chosen. If there are attachments with various levels of classification, it will inherit the higher one.

Classify attachments same as emails

This option enables users to classify **unclassified** attachments with the same classification as email.

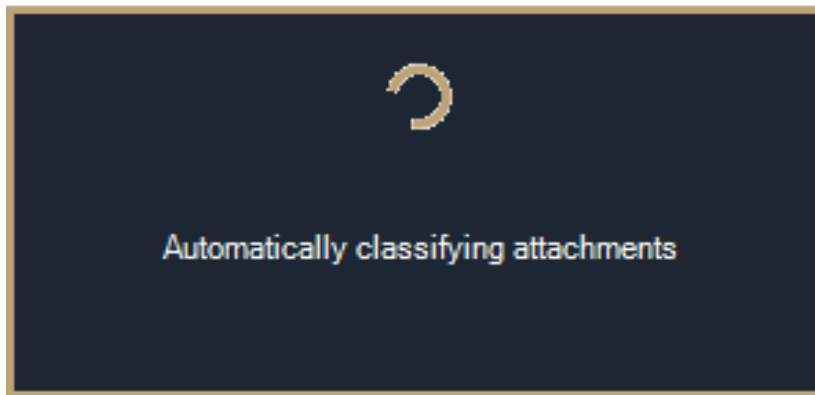


figure 54.

Show prefix classification on email subject

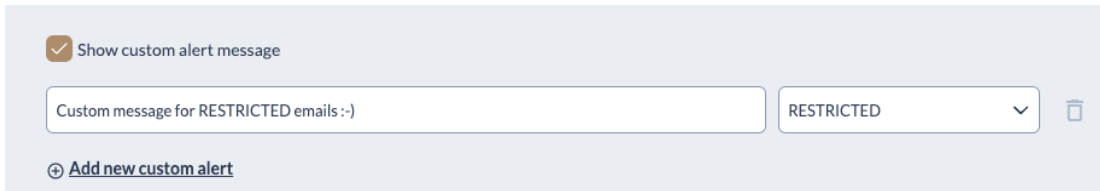
This option allows the user to prepend the classification tag to the email subject.

Show suffix classification on email subject

This option allows the user to append the classification tag to the email subject.

Show custom alert message

This option allows the user to set a custom message for the chosen classification level.



The screenshot shows a configuration panel for custom alert messages. At the top, there is a checked checkbox labeled 'Show custom alert message'. Below this is a text input field containing the message 'Custom message for RESTRICTED emails :-)' and a dropdown menu currently set to 'RESTRICTED'. A trash icon is visible to the right of the dropdown. At the bottom of the panel, there is a link with a plus icon labeled 'Add new custom alert'.

figure 55.

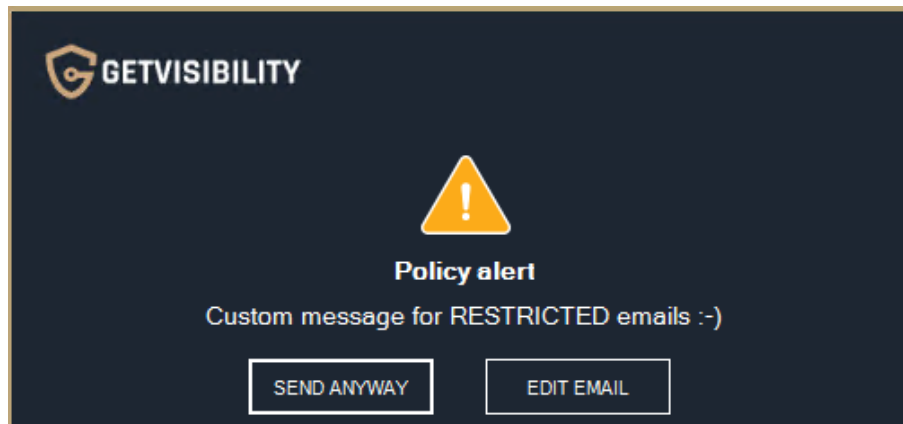


figure 56.

Powerpoint

All settings already covered in the **Shared Configuration** section.

Word

All settings already covered in the **Shared Configuration** section.

Visual tagging settings

Excel

All settings already covered in the **Shared Configuration** section.

Outlook

All settings already covered in the **Shared Configuration** section.

Powerpoint

All settings already covered in the **Shared Configuration** section.

Word

All settings already covered in the **Shared Configuration** section.

Custom Rules

Custom Rules are the v4 equivalent of v3's Overrides (previously called 'Macros' in v4). They consist of configurations that apply to

the selected **Target** when the chosen **Trigger** is activated and will override any **default** configuration related to that selected trigger and target, as set up in the **Plugins** section.

- Depending on the existing taxonomy, a **Custom Rule** may be activated by either **Classification, Compliance, or Distribution**.
- Each **Custom Rule** is designed to target only one Application (Excel, Outlook, PowerPoint, or Word).
- **Custom Rules** can be individually toggled on or off based on the user's specific needs. It can also be edited, deleted, and copied.

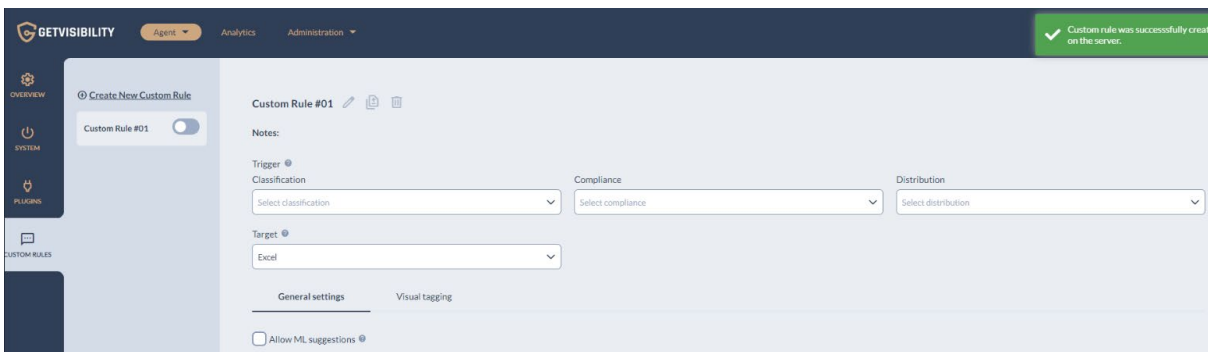


figure 57.

The **General settings, Classification settings, and Visual tagging configurations** are the same as the ones described in the **Plugins** section.



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.