SPIRION

Spirion Extensions

Configuring Forcepoint DLP to Assign Actions to Classification Tags Created by Spirion

Introduction

Forcepoint DLP users need to identify the classification tags created by Spirion and assign actions (e.g., block, move, copy, allow) to specific Spirion classification and protection tags in Forcepoint DLP.

Spirion applies visual and non-visual markings on files (e.g., .docx, .xlsx, .ppt, .pdf etc.) based on your organizational policy. If a file contains sensitive content, it may be marked as *Private* or *Sensitive* by the user in a Microsoft Office product or automatically marked based on rules created by an Spirion administrator using workflow rules.

Spirion consistently adds the classification tag to the same metadata location within each file. In Forcepoint DLP, you may configure a custom policy's **Analyzed Fields** to search specifically through the file metadata. This limits the scope of the scan to the metadata created by Spirion, allowing better and more accurate detection of the classification tags.

In Forcepoint DLP, you can detect Spirion labels on a file's metadata using the **File Labeling** classifier.

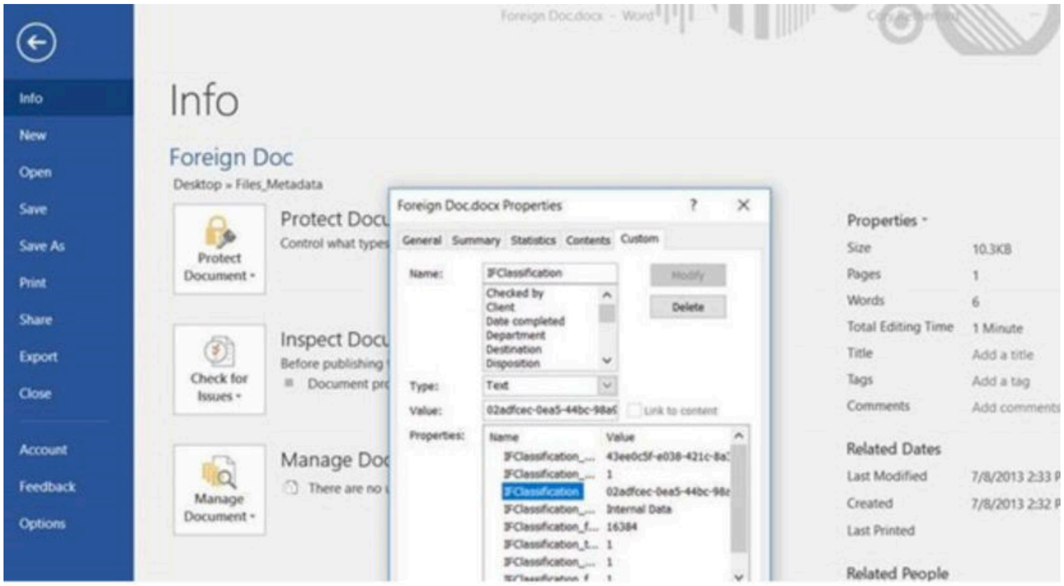
To assign actions to specific Spirion classification tags, you must create a custom DLP policy that contains a rule for the unique classification tag.entioned.

Requirements

Products: Forcepoint DLP, Forcepoint DLP Endpoint
Version: 8.6, 8.5, 8.4

Before creating the custom DLP policy, you must know the unique classification tags.

- For Microsoft Office documents, the classification tag is included in the or example, the classification tag is located in a Microsoft Word document's Properties under Tags. The Spirion Data Classification process embeds a friendly name, associated GUIDS, and other tags. You can view this directly through the metadata properties of the files (such as Word) as highlighted in the Doc properties. The GUID attribute Ifclassification stores the unique classification tags.



Foreign Doc

Desktop » Files_Metadata

Foreign Doc.docx Properties

Name: IFClassification

Checked by
Client
Date completed
Department
Destination
Disposition

Type: Text

Value: 02adfcec-0ea5-44bc-98a6

□ Link to content

Properties:

Name	Value
IFClassification_...	43ee0c5f-e038-421c-8a
IFClassification_...	1
IFClassification	02adfcec-0ea5-44bc-98
IFClassification_...	Internal Data
IFClassification_f...	16384
IFClassification_t...	1
IFClassification_...	1
IFClassification_f	1

Properties ▾

Size	10.3KB
Pages	1
Words	6
Total Editing Time	1 Minute
Title	Add a title
Tags	Add a tag
Comments	Add comments

Related Dates

Last Modified	7/8/2013 2:33 P
Created	7/8/2013 2:32 P
Last Printed	

Related People

- As a best practice, Forcepoint recommends that you create custom classification tags that a user would not type into their file. If the document ontains text that matches the classification tag, the file may inadvertently be assigned an incorrect action.

Creating a custom DLP policy for a Spirion Classfication and Protection tags

For more information on creating a custom DLP policy, see Creating Custom DLP Policies in the Forcepoint DLP Administrator Help.

1. In the Forcepoint Security Manager, select **Policy Management** from the left side menu, then click **DLP Policies** > **Manage Policies.**
2. Click **Add** > **Custom Policy**.
3. Under the **General** tab:

   a. Enter the **Policy name:** This name should relate to the classification tag's name.
   b. Check the **Enabled** checkbox.
   c. Leave the **Description:** field empty, or add descriptive information (optional).
   d. Enter None into the **Policy owners:** field.
   e. Select **Use the policy name for the rule name.**
4. Click **Next.**
5. Under the Condition tab:

   a. From the two drop-down menus, select **specific** data and **all parts of the transaction as a whole**. The full sentence should now read: "This rule monitors: **specific data** in: **all parts of the transaction as a whole.**"
   b. At the bottom of the window, click **Add** > **Patterns and Phrases** > **New** > **Key Phrase**, then enter the following:

   - **Name**: a name based on the unique identifier associated with the Spirion classification tag.
   - **Description**: leave blank, or add descriptive information (optional).
   - **Phrase to search**: the unique identifier associated with the Spirion classification tag that is visible in the document's Tag metadata, or in an email's x-header.

   c. Click **OK** to add the key phrase.
6. Review the **Select a Content Classifier** window's **General** tab and make sure that the displayed information is correct.
7. Review the **Select a Content Classifier** window's **Properties** tab. Under **Analyzed Fields**, you may either search all available fields, or target the search to only specific fields.

   a. For documents, select the **File metadata** field.
   b. For emails, select the **Other header (may be user-defined)** field. Additionally, you may also select **User-defined header** and enter the classification
   tag into the field.
8. Click **OK.**
9. Click **Next** to complete the Condition.
10. Under the **Severity & Action** tab:

    a. Leave the default **Create an incident for every matched condition** selected.
    b. Select **High** and the appropriate action from the drop-down menus. The sentence would read "When the condition is matched, severity is: **High** and the action plan is: **Block All.**" if you chose to Block.
11. Click **Next.**

12. Under the **Source** tab, leave the defaults:

    a. **Specify the sources of data that apply to this rule**: All
    b. **Machine type**: All machines
    c. **Network location**: Anywhere

13. Click **Next.**
14. Under the **Destination** tab, enable all that apply:

    a. Network email: add the user, group, or everyone who will be affected.
    b. Web: include all.
    c. Mobile Email
    d. Endpoint Printing
    e. Endpoint Applications
    f. Endpoint Removable Media
    g. Endpoint LAN

15. Click **Next.**
16. Review the information under the **Finish** tab.
17. If the information is correct, click the **Finish** button.
18. In the **Deployment Needed** window, click **Yes**.
19. On the **Deployment Process** screen, the policy has been deployed once all rows in the **Status** column display **Success.**
20. Open the Forcepoint DLP Endpoint client and click the **Update** button. The **Last scan ended** status will update to reflect the latest date and time.

To test the policy, create a file containing the Spirion classification tag in the file's metadata. If you selected a Block action, then the file would be blocked from being copied to a specified location.

Legal Disclaimer

This solution shown herein is based on a standard system configuration, which may be different from the system in your computing environment. Additional customization of your system may be required. Please contact Spirion Support for assistance.

There is no guarantee or warranty of any kind that this solution will perform as documented herein in your environment.