Forcepoint

Forcepoint Data Visibility

Powered by GetVisibility

Ex-ID (Pattern Matching UI)

Forcepoint

Report

Forcepoint
4 November 2023
Forcepoint Proprietary

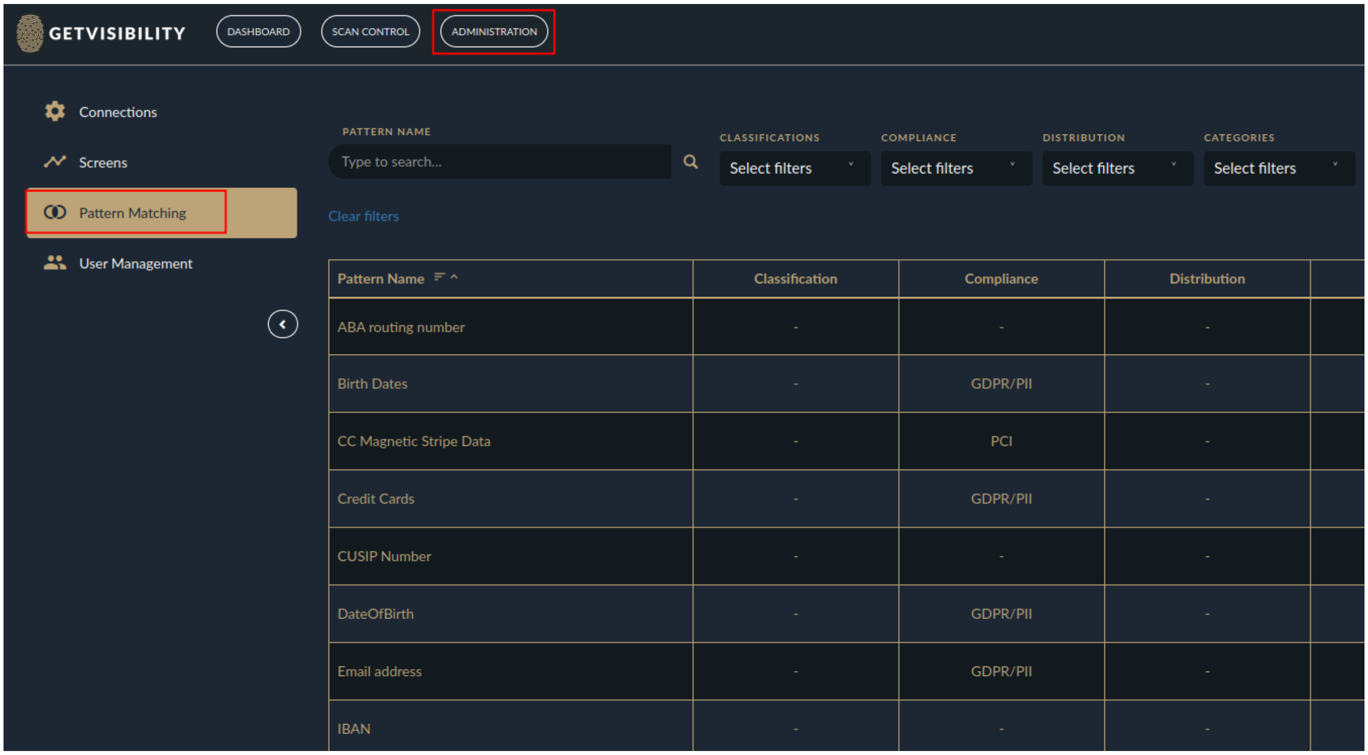
forcepoint.com

Table of Contents

Introduction

The pattern matching functionality allows users to identify pieces of information in a document. A pattern is considered as a RegEx that will be matched and the rules that may or may not apply once detected.

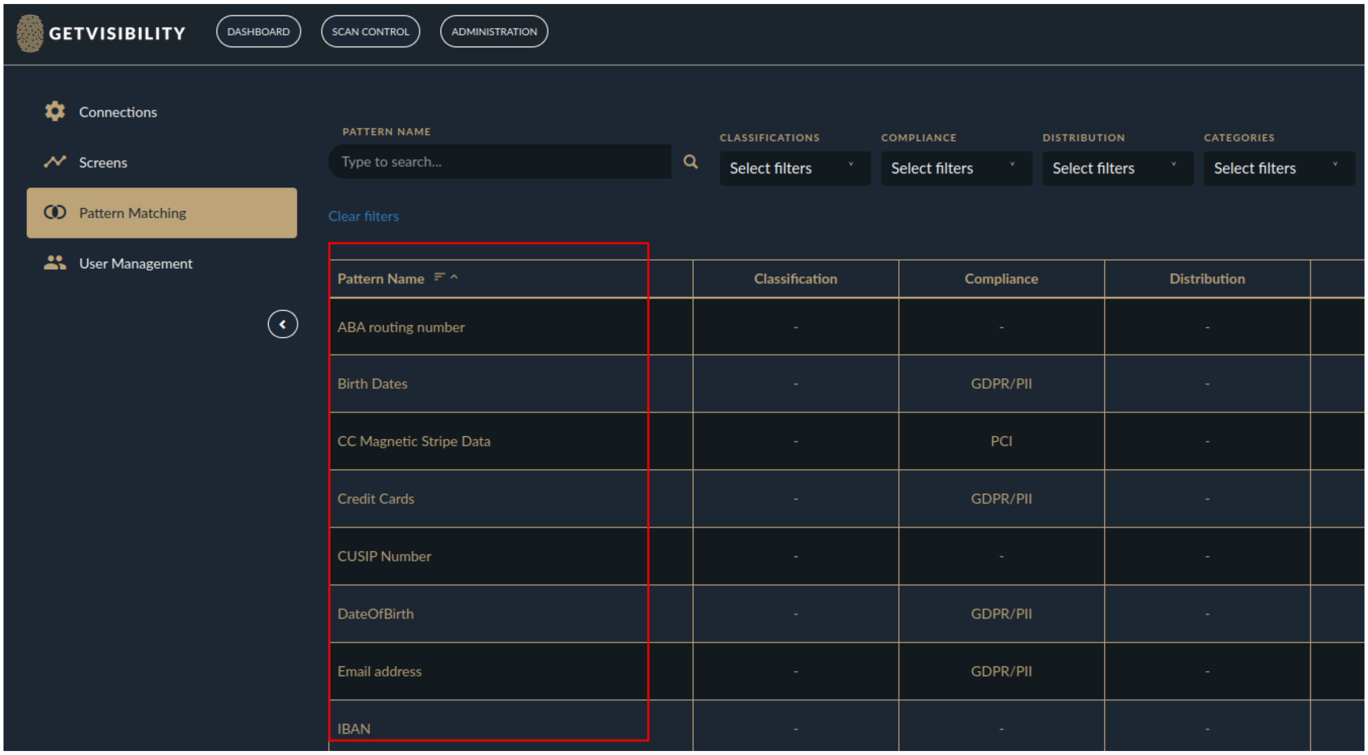
1. Navigate to **Administration > Pattern Matching**.



Pattern Name	Classification	Compliance	Distribution
ABA routing number	-	-	-
Birth Dates	-	GDPR/PII	-
CC Magnetic Stripe Data	-	PCI	-
Credit Cards	-	GDPR/PII	-
CUSIP Number	-	-	-
DateOfBirth	-	GDPR/PII	-
Email address	-	GDPR/PII	-
IBAN	-	-	-

Figure 1: Pattern Matching page

2. Display the list of pre-configured patterns available.



PATTERN NAME: Type to search...

CLASSIFICATIONS: Select filters

COMPLIANCE: Select filters

DISTRIBUTION: Select filters

CATEGORIES: Select filters

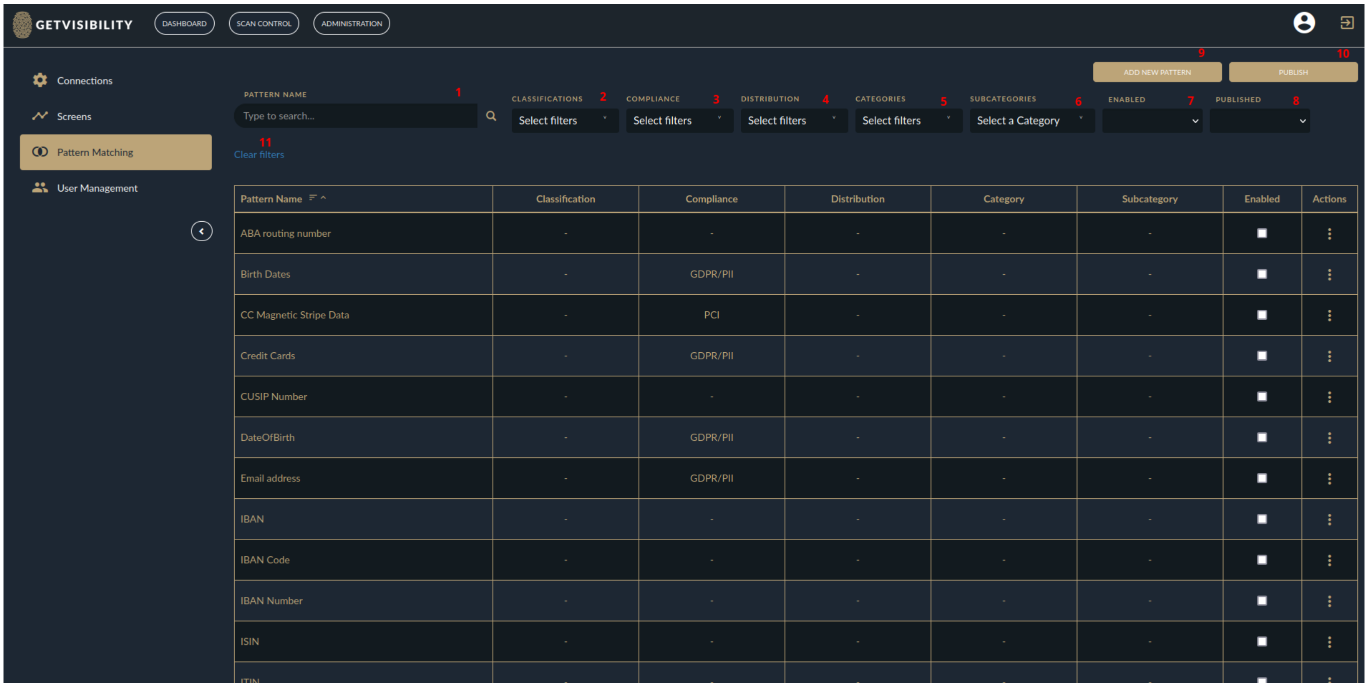
Clear filters

Pattern Name	Classification	Compliance	Distribution
ABA routing number	-	-	-
Birth Dates	-	GDPR/PII	-
CC Magnetic Stripe Data	-	PCI	-
Credit Cards	-	GDPR/PII	-
CUSIP Number	-	-	-
DateOfBirth	-	GDPR/PII	-
Email address	-	GDPR/PII	-
IBAN	-	-	-

Figure 2: Pattern Name list

3. If these patterns are detected during a scan they will be presented using the **Pattern Name** to the user.

Filters and Options



PATTERN NAME: Type to search...

CLASSIFICATIONS: Select filters

COMPLIANCE: Select filters

DISTRIBUTION: Select filters

CATEGORIES: Select filters

SUBCATEGORIES: Select a Category

ENABLED:

PUBLISHED:

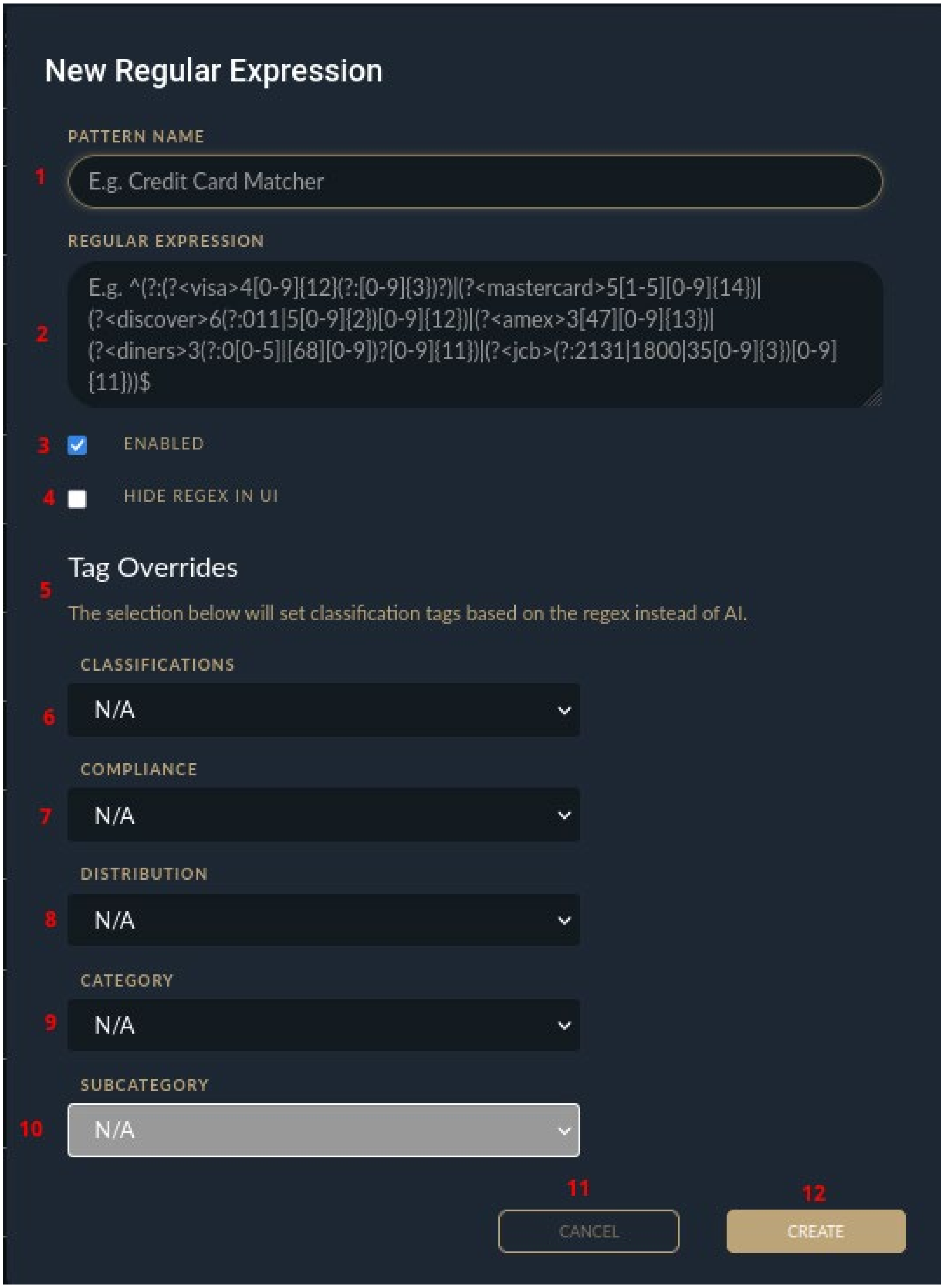
Clear filters

Pattern Name	Classification	Compliance	Distribution	Category	Subcategory	Enabled	Actions
ABA routing number	-	-	-	-	-	□	⋮
Birth Dates	-	GDPR/PII	-	-	-	□	⋮
CC Magnetic Stripe Data	-	PCI	-	-	-	□	⋮
Credit Cards	-	GDPR/PII	-	-	-	□	⋮
CUSIP Number	-	-	-	-	-	□	⋮
DateOfBirth	-	GDPR/PII	-	-	-	□	⋮
Email address	-	GDPR/PII	-	-	-	□	⋮
IBAN	-	-	-	-	-	□	⋮
IBAN Code	-	-	-	-	-	□	⋮
IBAN Number	-	-	-	-	-	□	⋮
ISIN	-	-	-	-	-	□	⋮
ITIN	-	-	-	-	-	□	⋮

Figure 3: Pattern Matching page

1. **Search:** Enter text here to filter patterns based in name.
2. **Classification:** Filter by classification tags associated with patterns.
3. **Compliance:** Filter by compliance tags associated with patterns.
4. **Distribution:** Filter by distribution tags associated with patterns.
5. **Categories:** Filter by file categories associated with patterns.
6. **Subcategories:** Filter by file subcategories associated with patterns.
7. **Enabled:** Filter by patterns that have been enabled or disabled.
8. **Published:** Filter by patterns that have been published or unpublished.
9. **Add New Pattern:** Create a custom pattern.
10. **Publish:** Push changes to the pattern matching system for start using.
11. **Clear filters:** Remove all previously selected filters.

Create a New Pattern



New Regular Expression

PATTERN NAME

E.g. Credit Card Matcher

REGULAR EXPRESSION

```
E.g. ^(?:(?<visa>4[0-9]{12}(?:[0-9]{3})?)|(?<mastercard>5[1-5][0-9]{14})|
(?<discover>6(?:011|5[0-9]{2})[0-9]{12})|(?<amex>3[47][0-9]{13})|
(?<diners>3(?:0[0-5]|[68][0-9])?[0-9]{11})|(?<jcb>(?:2131|1800|35[0-9]{3})[0-9]
{11}))$
```

☑ ENABLED

□ HIDE REGEX IN UI

Tag Overrides

The selection below will set classification tags based on the regex instead of AI.

CLASSIFICATIONS: N/A

COMPLIANCE: N/A

DISTRIBUTION: N/A

CATEGORY: N/A

SUBCATEGORY: N/A

Figure 4: New Regular Expression pane

1. **Pattern Name:** Identifies the RegEx when it is found by the software.
2. **Regular Expression:** The sequence to be matched.

3. **Enabled:** Whether the pattern will be searched for by the software.
4. **Hide RegEx in UI:** Obfuscates the regular expression.
5. **Tag Overrides:** When the RegEx is found these tags will be written to the file.
6. **Classifications:** Security levels.
7. **Compliance:** Regulations that apply to data.
8. **Distribution:** Policies on how data should distribute.
9. **Category:** Data grouping.
10. **Subcategory:** Data subgrouping.
11. **Cancel:** Exit without saving.
12. **Create:** Save pattern information and exit.

Glossary of terms

1. **RegEx:** Regular Expression, a sequence or pattern that is searched for in text. Ex-ID uses Java RegEx notation.
2. **Rules:** Instructions for Ex-ID about what to do when a RegEx is detected in a file.
3. **Pattern:** The RegEx and rules associated with its detection.
4. **Pattern Name:** Used to identify the pattern when it is detected.
5. **Classification:** Tags that help secure documents and other files. For example: Public, Internal, and Confidential.
6. **Compliance:** Tags that help organizations conform to certain regulatory regimes. By applying compliance tags such as GDPR/PII to RegEx such as Social Security number, organizations can identify all related documents.
7. **Distribution:** Tags that specify how a file should be moved either within or outside an organization.
8. **Category:** From GetVisibility ML model. These are groupings of information based on their use. For example: Finance, HR, or Technical Documents.
9. **Subcategory:** From GetVisibility ML model. These are sub-groupings of information based on their particular use. For example:. CV (resume), Code, or Sales Agreement.
10. **Publish:** The action of pushing the enabled patterns to be used. As some parts of the system need to be restarted to take on a new pattern matching configuration, we allow users to choose when to enact the configuration so as not to impact the workflow of others.
11. **Unpublished:** A pattern that has been created, changed, or edited but has not been pushed to the pattern matching system.
12. **Published:** A pattern that is currently part of the pattern matching configuration.
13. **Disabled:** A pattern that is currently part of the pattern matching configuration but is not to be detected.
14. **Enabled:** An active pattern. One that is part of the configuration and will be used by the pattern matching system.
15. **Hide RegEx:** Ex-ID allows for RegEx notations to be obfuscated for security and intellectual property reasons.

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.