Forcepoint

Forcepoint Data Visibility

Powered by GetVisibility

Admin Guide

Forcepoint

Report

Forcepoint
4 November 2023
Forcepoint Proprietary

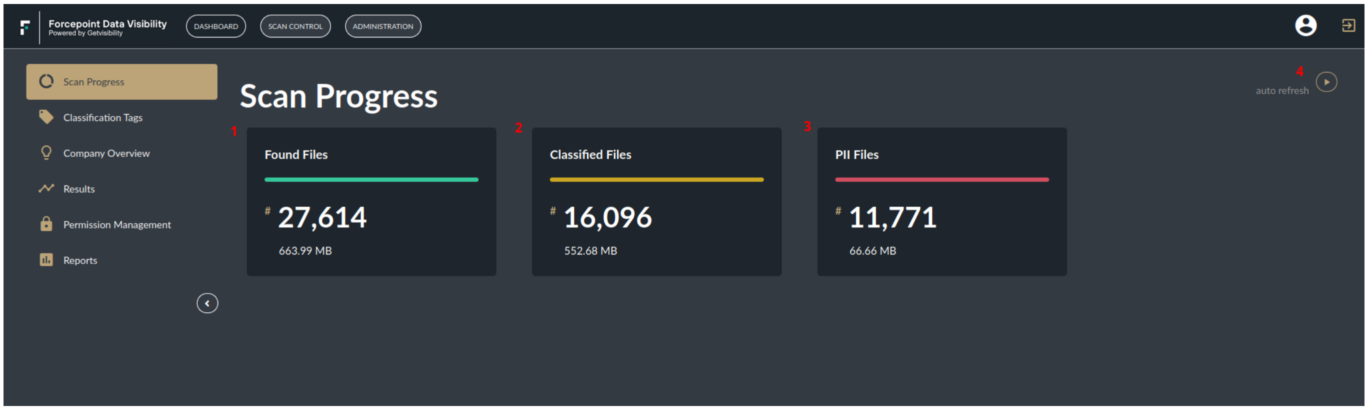
forcepoint.com

Table of Contents

DASHBOARD > SCAN PROGRESS.....2
DASHBOARD > CLASSIFICATION TAGS.....2
DASHBOARD > COMPANY OVERVIEW.....3
DASHBOARD > RESULTS.....4
DASHBOARD > PERMISSION MANAGEMENT.....5
DASHBOARD > REPORTS.....5
SCAN CONTROL > DISCOVER.....6
SCAN CONTROL > SCAN.....6
ADMINISTRATION > CONNECTIONS > CIFS/LDAP.....7
ADMINISTRATION > CONNECTIONS > SHAREPOINT.....8
ADMINISTRATION > SCREENS > RESULTS SCREEN.....9
ADMINISTRATION > PATTERN MATCHING.....10
Filters.....*10*
Pattern Table.....*11*
ADMINISTRATION > USER MANAGEMENT.....12

A screen-by-screen guide to the platform

Dashboard > Scan Progress



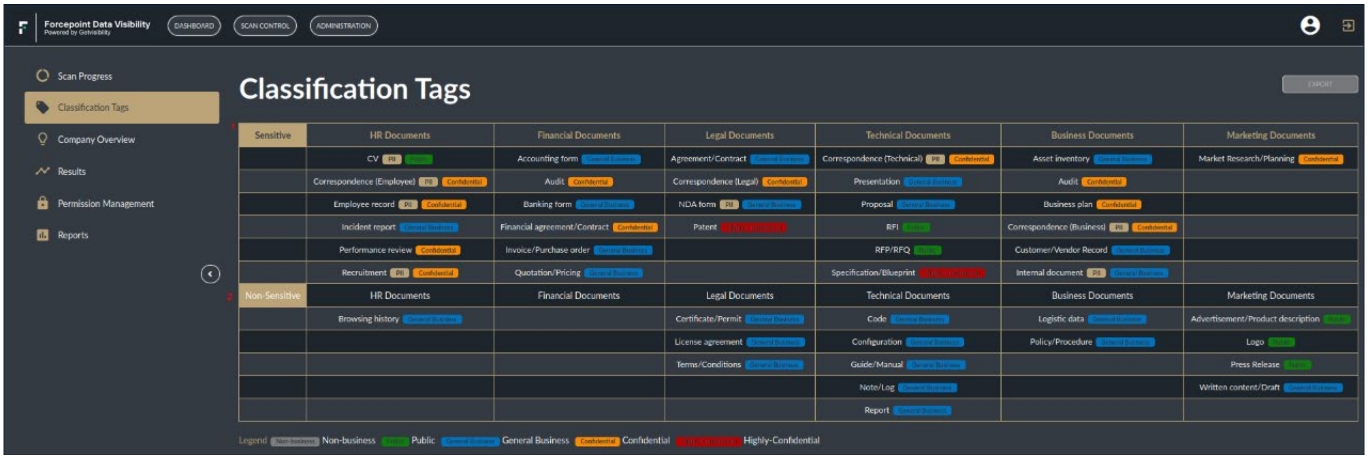
Scan Progress

Found Files	Classified Files	PII Files
# 27,614	# 16,096	# 11,771
663.99 MB	552.68 MB	66.66 MB

Figure 1: Scan Progress page

1. All files found during all scans carried out.
2. All files successfully classified by AI/ML.
3. All files containing Personal Identifiable Information.
4. Set to refresh the results automatically.

Dashboard > Classification Tags



Classification Tags

Sensitive	HR Documents	Financial Documents	Legal Documents	Technical Documents	Business Documents	Marketing Documents
	CV PII Public	Accounting form General Business	Agreement/Contract General Business	Correspondence (Technical) PII Confidential	Asset inventory General Business	Market Research/Planning Confidential
	Correspondence (Employee) PII Confidential	Audit Confidential	Correspondence (Legal) Confidential	Presentation General Business	Audit Confidential	
	Employee record PII Confidential	Banking form General Business	NDA form PII General Business	Proposal General Business	Business plan Confidential	
	Incident report General Business	Financial agreement/Contract Confidential	Patent Highly-Confidential	RFI Public	Correspondence (Business) PII Confidential	
	Performance review Confidential	Invoice/Purchase order General Business		RFP/RFQ Public	Customer/Vendor Record General Business	
	Recruitment PII Confidential	Quotation/Pricing General Business		Specification/Blueprint Highly-Confidential	Internal document PII General Business	
Non-Sensitive	**HR Documents**	**Financial Documents**	**Legal Documents**	**Technical Documents**	**Business Documents**	**Marketing Documents**
	Browsing history General Business		Certificate/Permit General Business	Code General Business	Logistic data General Business	Advertisement/Product description Public
			License agreement General Business	Configuration General Business	Policy/Procedure General Business	Logo Public
			Terms/Conditions General Business	Guide/Manual General Business		Press Release Public
				Note/Log General Business		Written content/Draft General Business
				Report General Business		

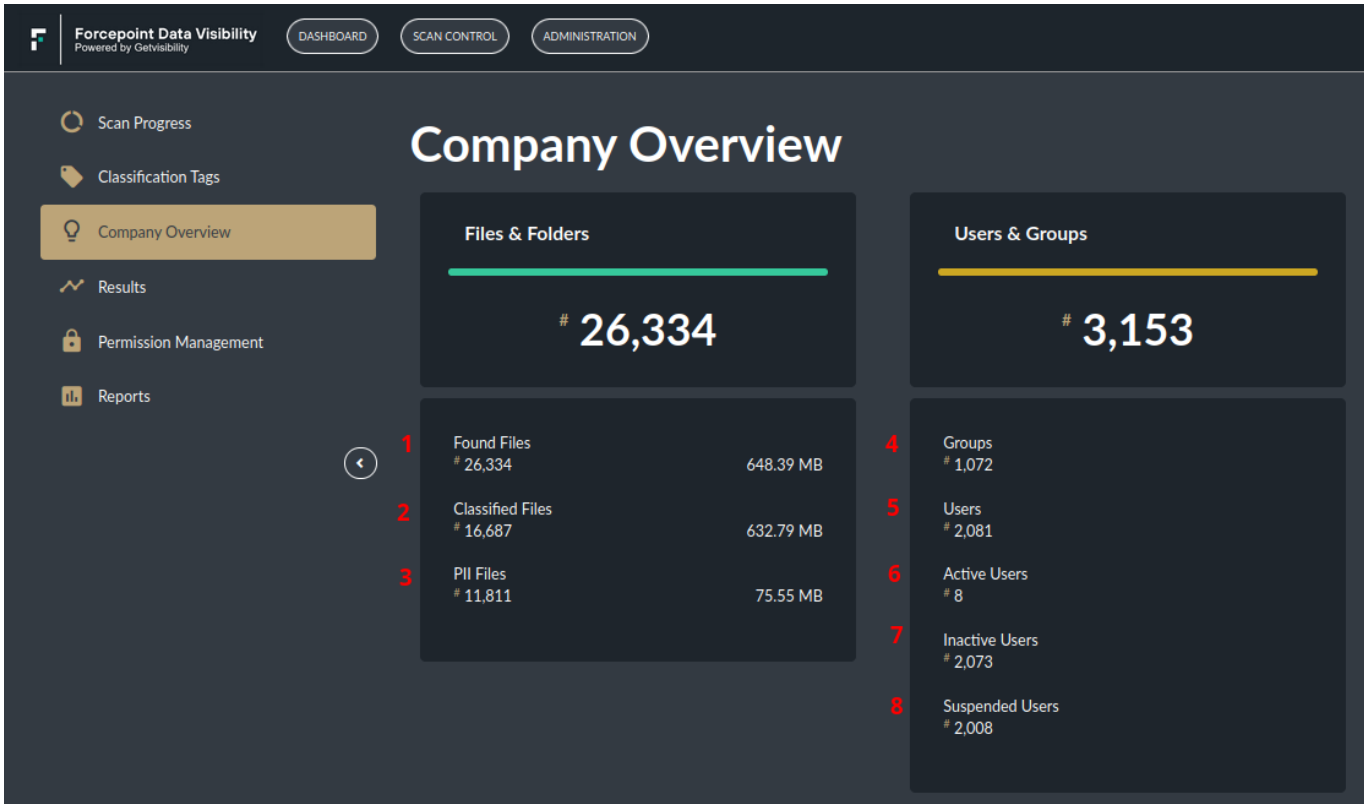
Legend: Non-business Non-business, Public Public, General Business General Business, Confidential Confidential, Highly-Confidential Highly-Confidential

Figure 2: Classification Tags page

Details of the classification taxonomy used to categorize and classify files:

1. The **Sensitive** grouping identifies files that the organization deems to have a critical impact on their operations.
2. The **Non-Sensitive** grouping identifies files that do not fit into the above group but should be classified and categorized, nonetheless.

Dashboard > Company Overview



Company Overview

Files & Folders

26,334

Users & Groups

3,153

Found Files
26,334 648.39 MB

Classified Files
16,687 632.79 MB

PII Files
11,811 75.55 MB

Groups
1,072

Users
2,081

Active Users
8

Inactive Users
2,073

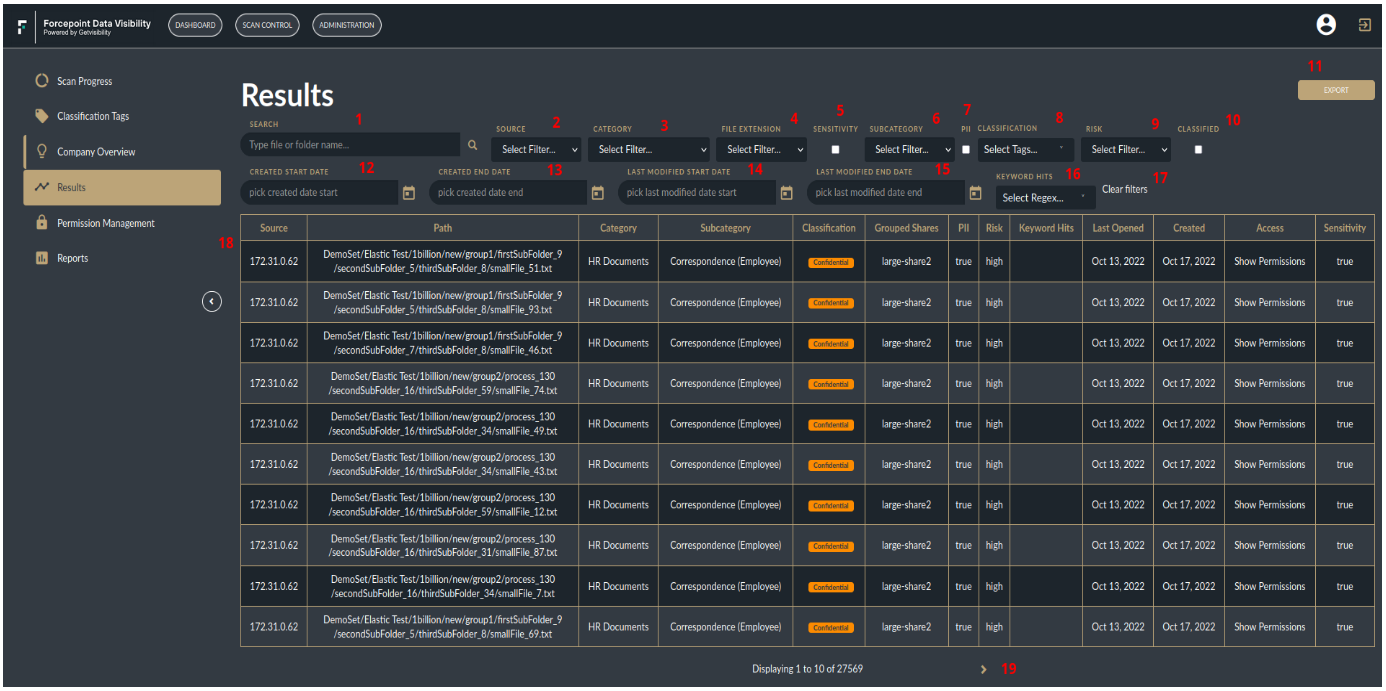
Suspended Users
2,008

Figure 3: Company Overview page

An overall look at the file and access landscape of the organization/company:

1. All files found during all scans carried out.
2. All files successfully classified by AI/ML.
3. All files containing Personal Identifiable Information.
4. The number of Active Directory groups found.
5. The number of Active Directory users found.
6. The number of users who have logged-in in the last 90 days.
7. The number of users who have not logged-in in the last 90 days.
8. The number of users whose access has been paused/suspended.

Dashboard > Results



Source	Path	Category	Subcategory	Classification	Grouped Shares	PII	Risk	Keyword Hits	Last Opened	Created	Access	Sensitivity
172.31.0.62	DemoSet/Elastic Test/1billion/new/group1/firstSubFolder_9/secondSubFolder_5/thirdSubFolder_8/smallFile_51.txt	HR Documents	Correspondence (Employee)	Confidential	large-share2	true	high		Oct 13, 2022	Oct 17, 2022	Show Permissions	true
172.31.0.62	DemoSet/Elastic Test/1billion/new/group1/firstSubFolder_9/secondSubFolder_5/thirdSubFolder_8/smallFile_93.txt	HR Documents	Correspondence (Employee)	Confidential	large-share2	true	high		Oct 13, 2022	Oct 17, 2022	Show Permissions	true
172.31.0.62	DemoSet/Elastic Test/1billion/new/group1/firstSubFolder_9/secondSubFolder_7/thirdSubFolder_8/smallFile_46.txt	HR Documents	Correspondence (Employee)	Confidential	large-share2	true	high		Oct 13, 2022	Oct 17, 2022	Show Permissions	true
172.31.0.62	DemoSet/Elastic Test/1billion/new/group2/process_130/secondSubFolder_16/thirdSubFolder_59/smallFile_74.txt	HR Documents	Correspondence (Employee)	Confidential	large-share2	true	high		Oct 13, 2022	Oct 17, 2022	Show Permissions	true
172.31.0.62	DemoSet/Elastic Test/1billion/new/group2/process_130/secondSubFolder_16/thirdSubFolder_34/smallFile_49.txt	HR Documents	Correspondence (Employee)	Confidential	large-share2	true	high		Oct 13, 2022	Oct 17, 2022	Show Permissions	true
172.31.0.62	DemoSet/Elastic Test/1billion/new/group2/process_130/secondSubFolder_16/thirdSubFolder_34/smallFile_43.txt	HR Documents	Correspondence (Employee)	Confidential	large-share2	true	high		Oct 13, 2022	Oct 17, 2022	Show Permissions	true
172.31.0.62	DemoSet/Elastic Test/1billion/new/group2/process_130/secondSubFolder_16/thirdSubFolder_59/smallFile_12.txt	HR Documents	Correspondence (Employee)	Confidential	large-share2	true	high		Oct 13, 2022	Oct 17, 2022	Show Permissions	true
172.31.0.62	DemoSet/Elastic Test/1billion/new/group2/process_130/secondSubFolder_16/thirdSubFolder_31/smallFile_87.txt	HR Documents	Correspondence (Employee)	Confidential	large-share2	true	high		Oct 13, 2022	Oct 17, 2022	Show Permissions	true
172.31.0.62	DemoSet/Elastic Test/1billion/new/group2/process_130/secondSubFolder_16/thirdSubFolder_34/smallFile_7.txt	HR Documents	Correspondence (Employee)	Confidential	large-share2	true	high		Oct 13, 2022	Oct 17, 2022	Show Permissions	true
172.31.0.62	DemoSet/Elastic Test/1billion/new/group1/firstSubFolder_9/secondSubFolder_5/thirdSubFolder_8/smallFile_69.txt	HR Documents	Correspondence (Employee)	Confidential	large-share2	true	high		Oct 13, 2022	Oct 17, 2022	Show Permissions	true

Displaying 1 to 10 of 27569

Figure 4: Results page

1. Search for files or folders using their path.
2. Select/filter by the source of the files, for example: SMB, Sharepoint.
3. Filter by Categorization of files. Linked to their functionality, for example: HR and Finance.
4. Filter by file extension, for example: docx, jpg, and pdf.
5. Filter by sensitivity. These are files that have been deemed to contain critical organizational information.
6. Filter by Subcategorization of files. This identifies their usage, for example: contract, code, and sales agreement.
7. Filter by PII. Files that contain Personal Identifiable Information (PII).
8. Filter by Classification tags. These are security tags put on files, for example: Internal and Confidential.
9. Filter by Risk level. Associates critical data with user access. Low, medium, and high based on the share of users that have access to that file. Higher level more users have access.
10. Filter on files that were successfully classified or not. Folder have included her as non-classified.
11. Export data from the current filters to a CSV.
12. Filter on files created on or after this date.
13. Filter on files created on or before this date.
14. Filter on files modified on or after this date.
15. Filter on files modified on or before this date.
16. Select Keywords/Patterns/RegEx. Multiple can be selected and their counts will be visible.
17. Clear all previously set filters.
18. The file results based on the filters used.

19. Navigate to next set of 10 displayed files using the filters.

Dashboard > Permission Management

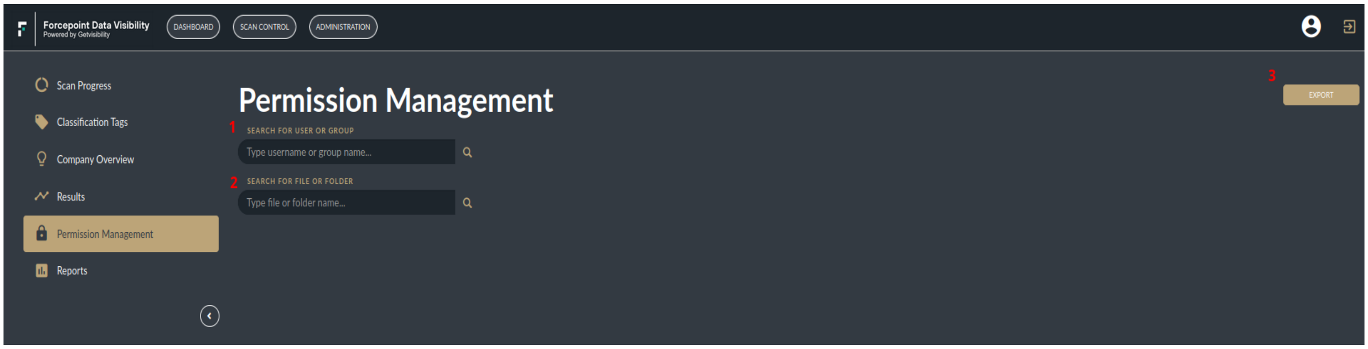


Figure 5: Permission Management page

To investigate files and users/groups based on access or permissions.

1. Enter to know user or group name.
2. Enter to known file or folder name.
3. Export results of search to CSV.

Dashboard > Reports

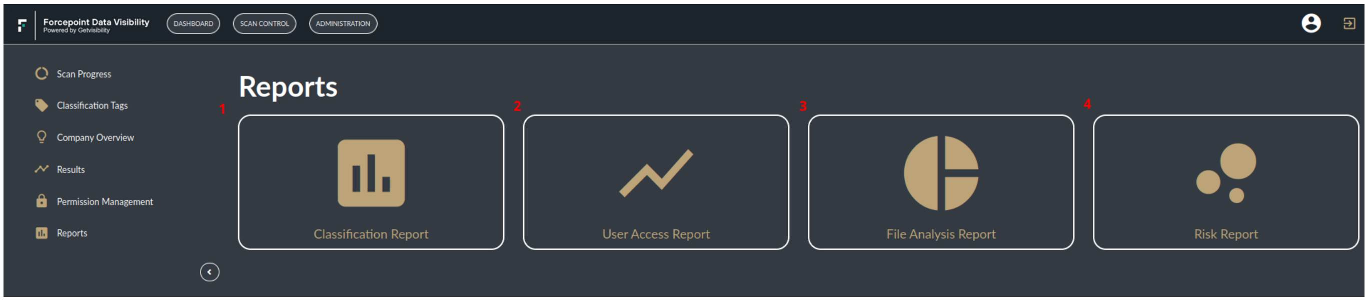
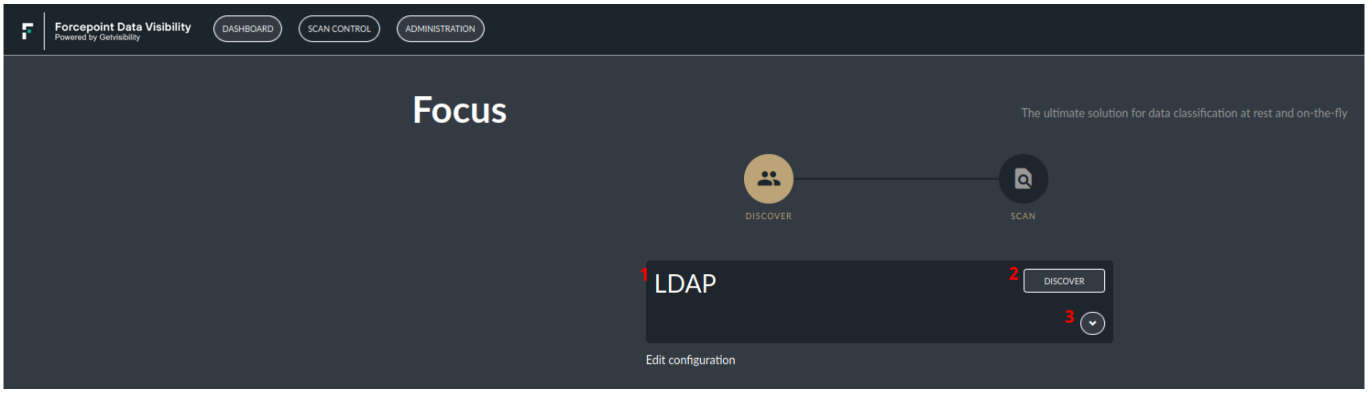


Figure 6: Reports page

Generate preconfigured PDF reports. Select the icons to download the report:

1. Detailed report on the classification and categorization of files scanned.
2. Details of Active Directory users from a security perspective.
3. Tailored to help in regulatory analysis, this report details files that fall under regulatory regimes such as GDPR.
4. Detailing the areas where data risk is most severe. Risk scoring helps allocate remediation resources.

Scan Control > Discover

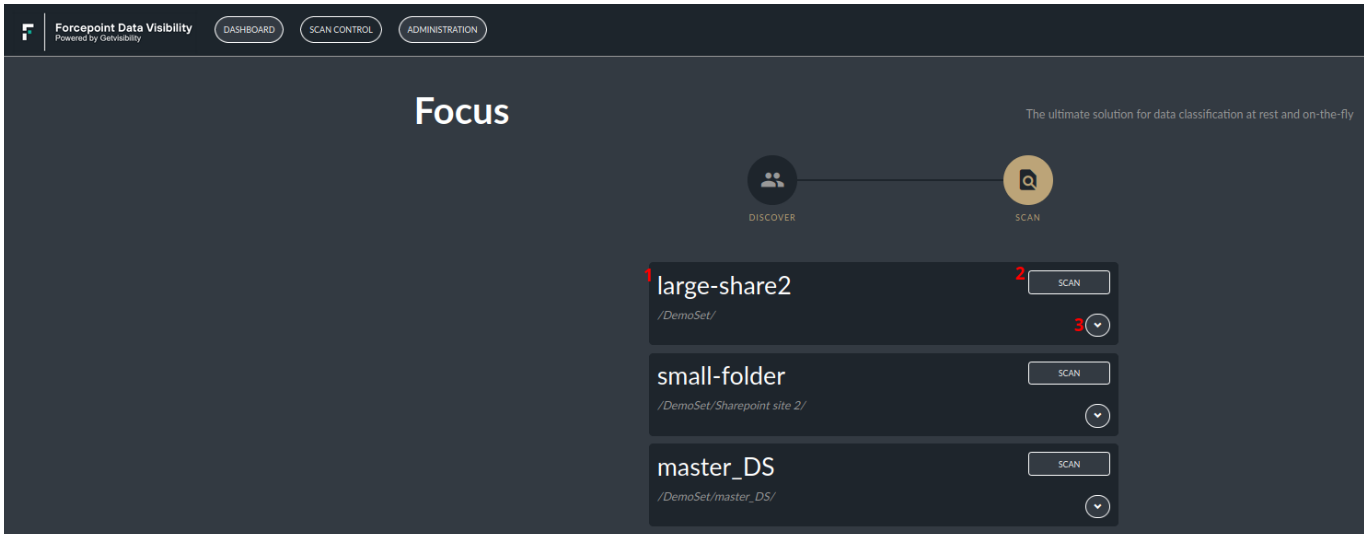


The ultimate solution for data classification at rest and on-the-fly

Figure 7: Discover page

1. Configured LDAP scan name.
2. Kick of the scan of users and groups.
3. View connection details.

Scan Control > Scan

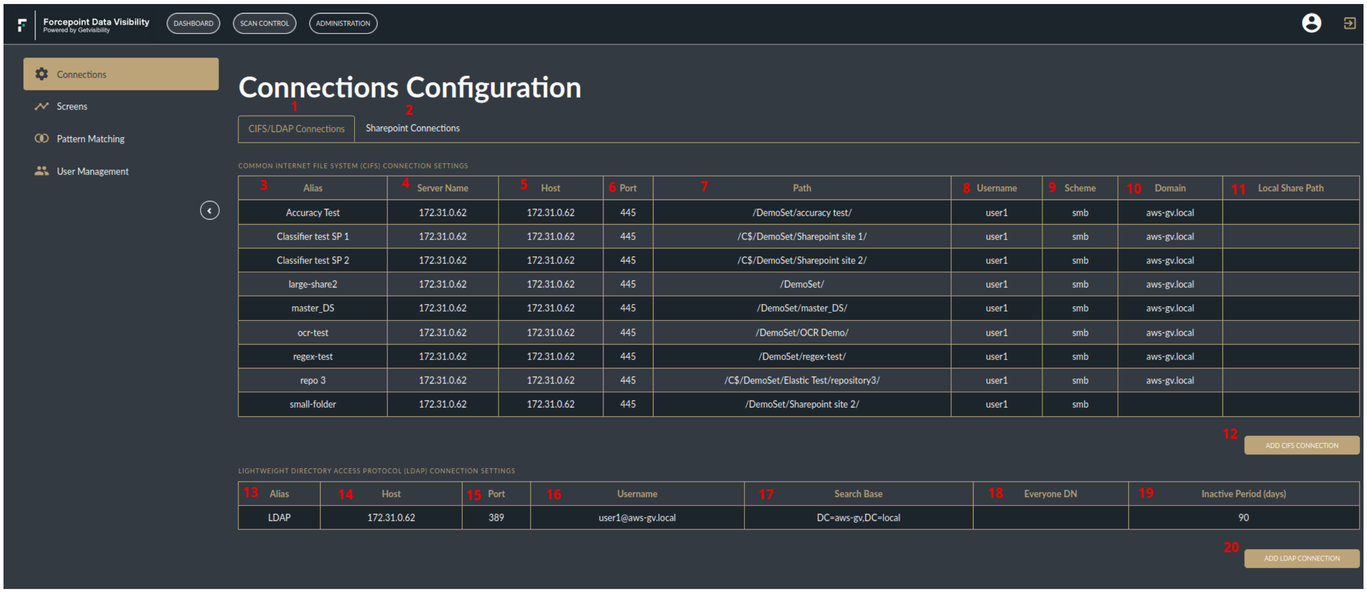


The ultimate solution for data classification at rest and on-the-fly

Figure 8: Scan page

1. Configured SMB scan name.
2. Kick off the file scan.
3. View SMB connection details.

Administration > Connections > CIFS/LDAP



Connections Configuration

CIFS/LDAP Connections | Sharepoint Connections

COMMON INTERNET FILE SYSTEM (CIFS) CONNECTION SETTINGS

Alias	Server Name	Host	Port	Path	Username	Scheme	Domain	Local Share Path
Accuracy Test	172.31.0.62	172.31.0.62	445	/DemoSet/accuracy test/	user1	smb	aws-gv.local	
Classifier test SP 1	172.31.0.62	172.31.0.62	445	/C$/DemoSet/Sharepoint site 1/	user1	smb	aws-gv.local	
Classifier test SP 2	172.31.0.62	172.31.0.62	445	/C$/DemoSet/Sharepoint site 2/	user1	smb	aws-gv.local	
large-share2	172.31.0.62	172.31.0.62	445	/DemoSet/	user1	smb	aws-gv.local	
master_DS	172.31.0.62	172.31.0.62	445	/DemoSet/master_DS/	user1	smb	aws-gv.local	
ocr-test	172.31.0.62	172.31.0.62	445	/DemoSet/OCR Demo/	user1	smb	aws-gv.local	
regex-test	172.31.0.62	172.31.0.62	445	/DemoSet/regex-test/	user1	smb	aws-gv.local	
repo 3	172.31.0.62	172.31.0.62	445	/C$/DemoSet/Elastic Test/repository3/	user1	smb	aws-gv.local	
small-folder	172.31.0.62	172.31.0.62	445	/DemoSet/Sharepoint site 2/	user1	smb		

LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL (LDAP) CONNECTION SETTINGS

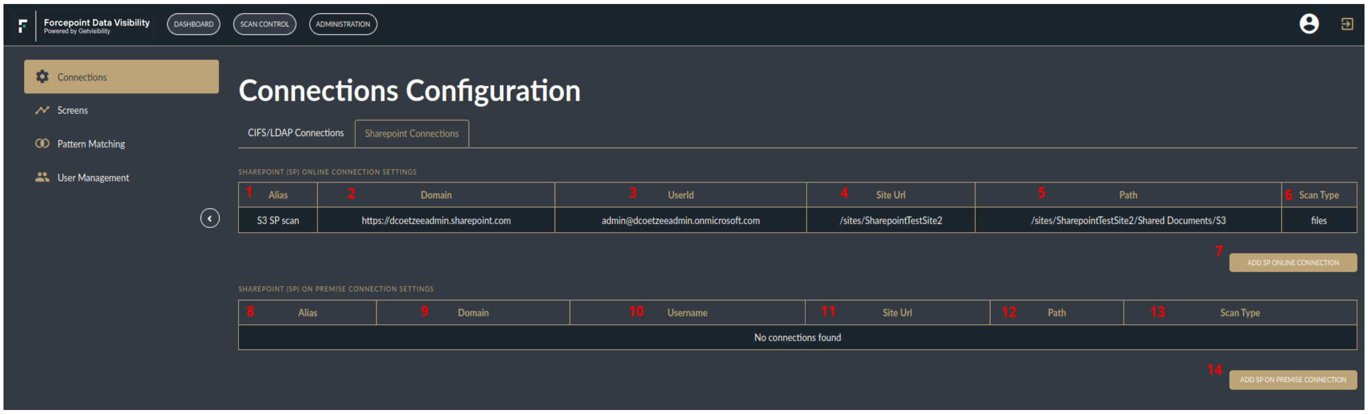
Alias	Host	Port	Username	Search Base	Everyone DN	Inactive Period (days)
LDAP	172.31.0.62	389	user1@aws-gv.local	DC=aws-gv,DC=local		90

Figure 9: CIFS/LDAP Connections page

Configure various file and user scans:

1. Tab to setup CIFS file-based connections and LDAP user-based connections.
2. Tab to setup Sharepoint Online and On-Prem connections.
3. The name used to identify the connections.
4. The name of the server/machine to be scanned.
5. The IP address of the server/machine to be scanned.
6. The port used to access the server.
7. The path of the root directory to begin scanning from.
8. The username that grants access to these files.
9. The protocol used to view the files.
10. The domain in which the files are located.
11. If the files are a local share, this is the path used to begin scanning.
12. Opens the CIFS connection wizard to setup a new connection.
13. The name used to identify the configured LDAP scanning.
14. The host where the Active Directory (AD) is located.
15. The port used to access the AD.
16. The username that grants access to all AD data.
17. The LDAP base to begin the scan.
18. The alias, if applicable of the Everyone/World grouping.
19. Inactivity period of users. Used to identify users who have not logged-in in that time.
20. Open the LDAP connection wizard to setup a new scanning.

Administration > Connections > Sharepoint



Connections Configuration

SHAREPOINT (SP) ONLINE CONNECTION SETTINGS

1 Alias	2 Domain	3 UserId	4 Site Url	5 Path	6 Scan Type
S3 SP scan	https://dcoetzeeadmin.sharepoint.com	admin@dcoetzeeadmin.onmicrosoft.com	/sites/SharepointTestSite2	/sites/SharepointTestSite2/Shared Documents/S3	files

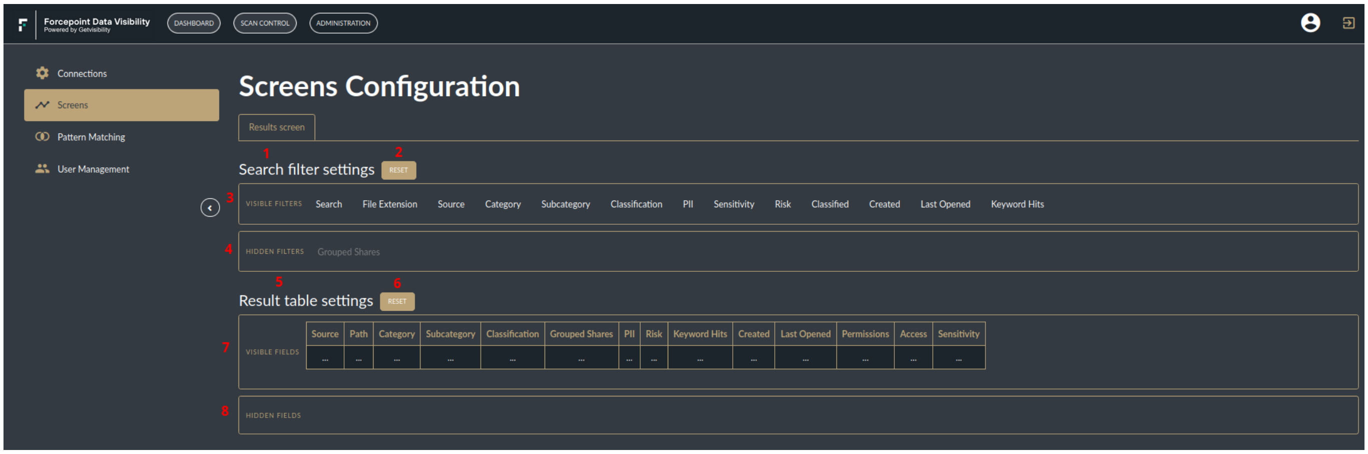
SHAREPOINT (SP) ON PREMISE CONNECTION SETTINGS

8 Alias	9 Domain	10 Username	11 Site Url	12 Path	13 Scan Type
No connections found					

Figure 10: Sharepoint Connection page

1. Name used to identify the configured Sharepoint connection.
2. The Domain address of the Sharepoint server.
3. The user that grants access to the files to be scanned.
4. The URL to the files.
5. The path at which the scan will begin.
6. The type of entities to be scanned (files/users).
7. Open Sharepoint Online Connection wizard.
8. Name used to identify the configured Sharepoint connection.
9. The Domain address of the Sharepoint server.
10. The user that grants access to the files to be scanned.
11. The URL to the files.
12. The path at which the scan will begin.
13. The type of entities to be scanned (files/users).
14. Open Sharepoint On-Prem Connection wizard.

Administration > Screens > Results screen



Source	Path	Category	Subcategory	Classification	Grouped Shares	PII	Risk	Keyword Hits	Created	Last Opened	Permissions	Access	Sensitivity
...	...	...	...	...	...	...	...	...	...	...	...	...	...

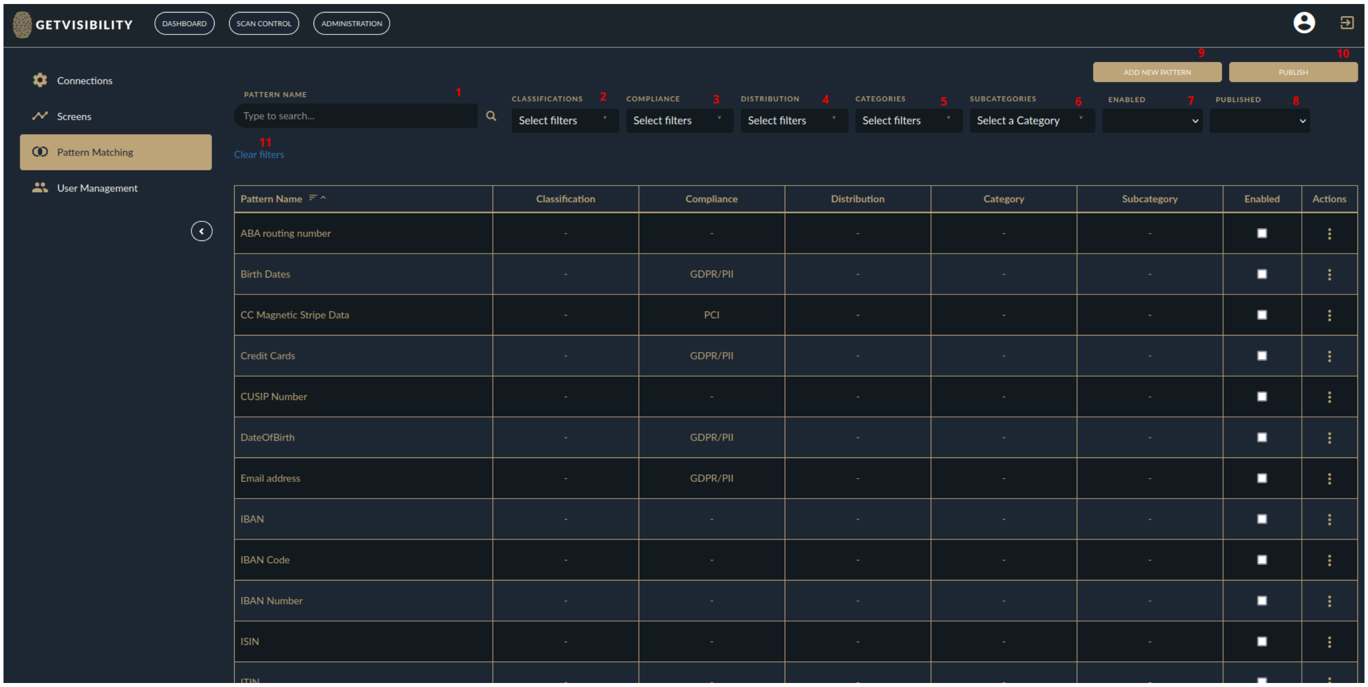
Figure 11: Screens page

Edit the way results are filtered and presented on the **Dashboard > Results screen**.

1. The filter setting used to search files.
2. Reset any previous configuration to the default below.
3. List of filters that will be seen on the **Results screen**.
4. List of filters that will not be seen on the **Results screen**.
5. The file attributes that will be visible on the **Results screen**.
6. Reset any previous configuration to the default below.
7. The file attribute and other fields visible on the **Results screen** files table.

Administration > Pattern Matching

Filters

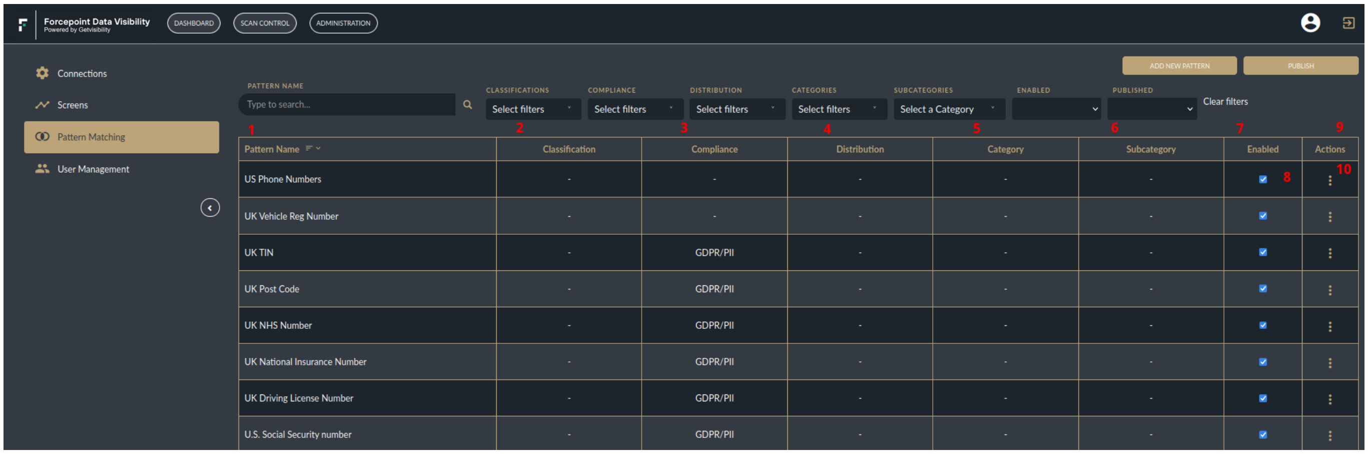


Pattern Name	Classification	Compliance	Distribution	Category	Subcategory	Enabled	Actions
ABA routing number	-	-	-	-	-	☐	⋮
Birth Dates	-	GDPR/PII	-	-	-	☐	⋮
CC Magnetic Stripe Data	-	PCI	-	-	-	☐	⋮
Credit Cards	-	GDPR/PII	-	-	-	☐	⋮
CUSIP Number	-	-	-	-	-	☐	⋮
DateOfBirth	-	GDPR/PII	-	-	-	☐	⋮
Email address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

Figure 12: Filters 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.

Pattern Table



Pattern Name	Classification	Compliance	Distribution	Category	Subcategory	Enabled	Actions
US Phone Numbers	-	-	-	-	-	☑	⋮
UK Vehicle Reg Number	-	-	-	-	-	☑	⋮
UK TIN	-	GDPR/PII	-	-	-	☑	⋮
UK Post Code	-	GDPR/PII	-	-	-	☑	⋮
UK NHS Number	-	GDPR/PII	-	-	-	☑	⋮
UK National Insurance Number	-	GDPR/PII	-	-	-	☑	⋮
UK Driving License Number	-	GDPR/PII	-	-	-	☑	⋮
U.S. Social Security number	-	GDPR/PII	-	-	-	☑	⋮

Figure 13: Pattern table

1. Sort patterns by name.
2. Sort patterns by Classification tag.
3. Sort patterns by Compliance tag.
4. Sort patterns by Distribution tag.
5. Sort patterns by Category.
6. Sort patterns by Subcategory.
7. Sort patterns on whether they are enabled or not.
8. Switch to enable or disable a pattern.
9. Actions column.
10. Select to view.

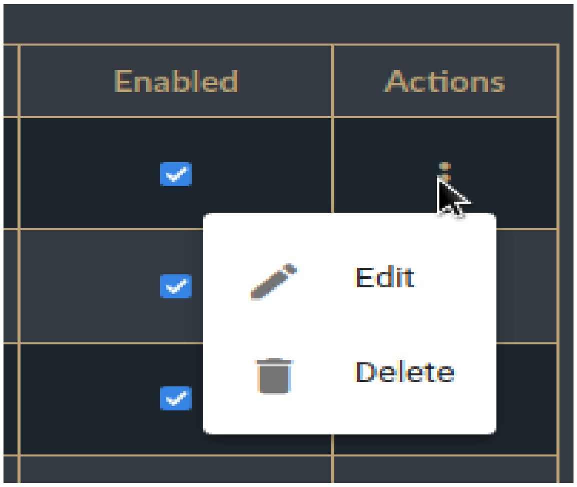


Figure 14: View options

11. Select edit to edit pattern contents.
12. Select delete to remove the pattern.

Administration > User Management

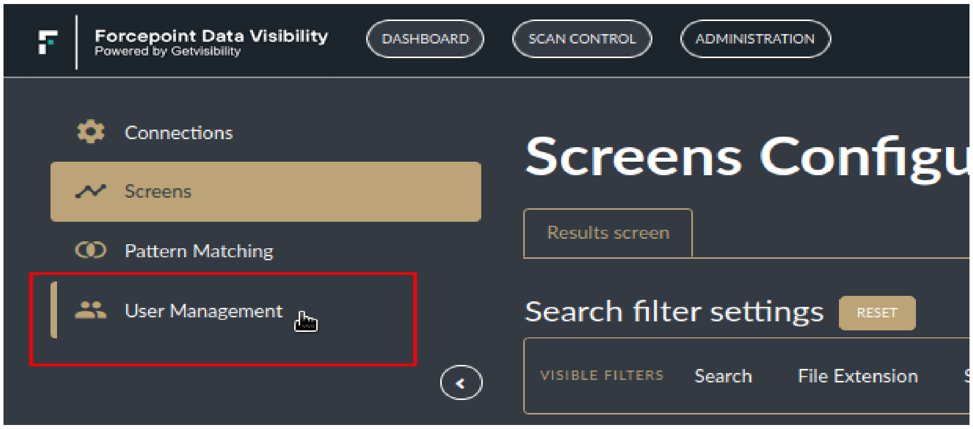


Figure 15: User Management tab

This screen will bring the user to the Keycloak dashboard.

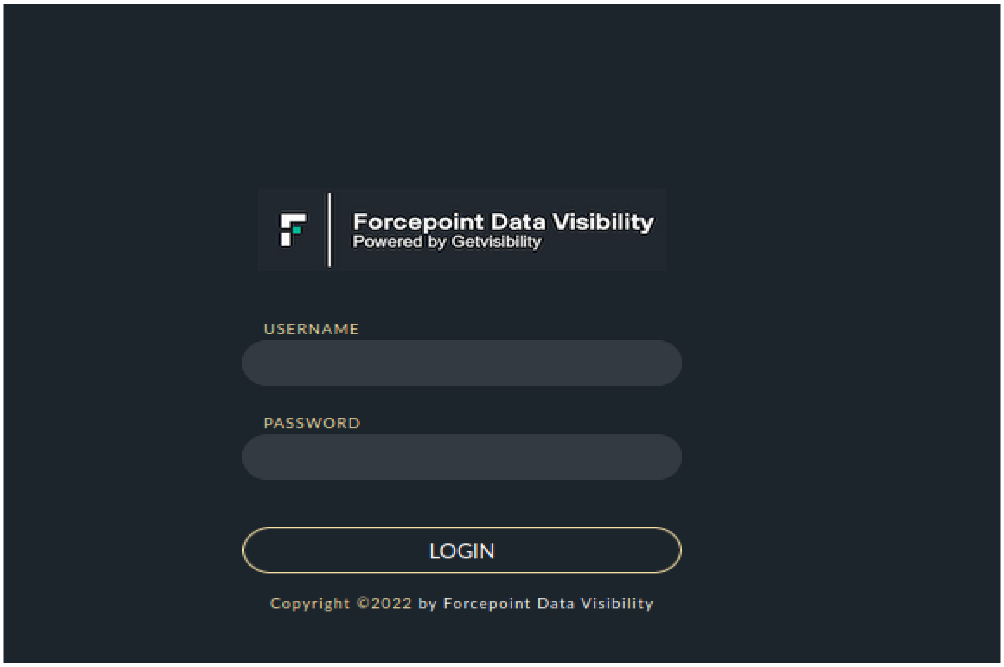
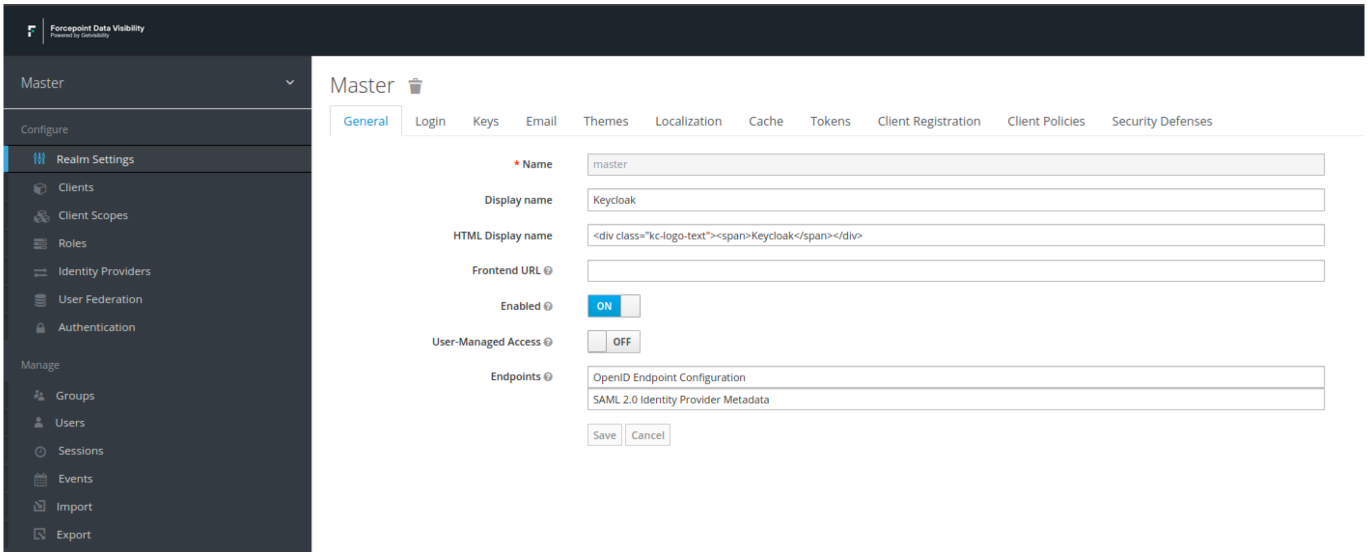

Forcepoint Data Visibility
Powered by Getvisibility
USERNAME
PASSWORD
LOGIN
Copyright ©2022 by Forcepoint Data Visibility

Figure 16: Forcepoint Data Visibility login page

Here, login, credentials, users, and access details can be configured.



* Name	master
Display name	Keycloak
HTML Display name	<div class="kc-logo-text"><span>Keycloak</span></div>
Frontend URL	
Enabled	ON
User-Managed Access	OFF
Endpoints	OpenID Endpoint Configuration SAML 2.0 Identity Provider Metadata

Figure 17: General page

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.