Administration Guide

FortiData 7.6.2

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO LIBRARY
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

March 20, 2026
FortiData 7.6.2 Administration Guide
96-762-1109187-20260320

TABLE OF CONTENTS

Change log

Date	Change Description
2026-02-12	Initial document release.
2026-03-20	Updated Data Types on page 32 and Data Fingerprinting on page 34.

Introduction

For most security and IT teams, visibility into data is fractured across multiple cloud and on-premise data stores and locations, resulting in fragmented data security coverage and low visibility into the current state of the organization’s data security posture.

Leveraging AI machine learning, FortiData provides a centralized view of the sprawl of sensitive data across your on-premise SMB/CIFS file systems by discovering, classifying, and labeling sensitive data using its advanced data recognition and customizable data types. You can also configure scans to access and analyze files in a target location with a proper schedule.

FortiData supports integration with the following Fortinet security fabric products:

- FortiGate (7.6.4 or later)
- FortiClient (7.4.4 or later)

FortiData aims to strengthen data security in Fortinet security fabric and ensure that sensitive data is adequately protected at the endpoint, edge, on-premise, and in the cloud, whether the data is in transit or at rest.

This guide intends to help you navigate and leverage the features of FortiData and guide you through the process of creating scan tasks, configuring scan policies, and analyzing scan results using reports.

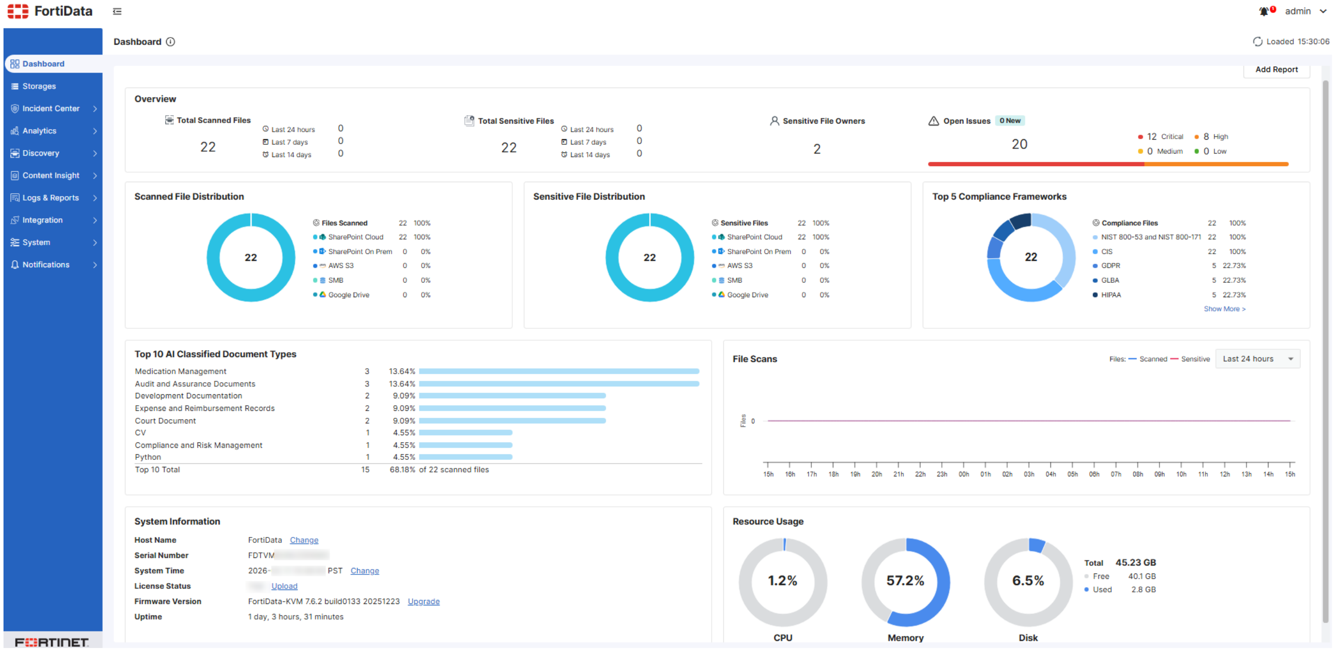
Getting started

The following is a high-level workflow of using FortiData:

1. Configure interface and DNS settings. See Network on page 53
2. Configure timeout and system time. See Settings on page 51.
3. Configure HTTPS server certificate. See Certificates on page 56.
4. Create users of with different access scope to FortiData. See User Management on page 45.
5. Configure data types and data classifiers to identify the data patterns to look for in files. See Content Insight on page 32.
6. Create a storage location to scan for sensitive date and labeling. See Storages on page 10.
7. Create discovery policies and scans to look for specific types of data in files in the target storage. See Discovery on page 21.
8. Configure email notifications for data issues using built-in email templates. See Notifications on page 62.
9. View aggregated scan results and reports in Dashboard on page 7 and Logs & Reports on page 40.
10. View the security posture of your files in Analytics on page 16.

Dashboard

Use the *Dashboard* to view information of the system, such as scanned or sensitive file distribution by platform, file compliance and sensitivity information, resource usage, and system information (hostname, serial number, system time, license status, firmware version). You can also add a *Risk Overview* report using the *Add Report* button on the top-right corner. The report will then be available in the *Logs & Reports > Reports on page 42* page.



Overview

Total Scanned Files		
22	Last 24 hours	0
	Last 7 days	0
	Last 14 days	0

Total Sensitive Files		
22	Last 24 hours	0
	Last 7 days	0
	Last 14 days	0

Sensitive File Owners: 2

Open Issues 0 New: 20 — 12 Critical, 8 High, 0 Medium, 0 Low

Scanned File Distribution (22)

Files Scanned	22	100%
SharePoint Cloud	22	100%
SharePoint On Prem	0	0%
AWS S3	0	0%
SMB	0	0%
Google Drive	0	0%

Sensitive File Distribution (22)

Sensitive Files	22	100%
SharePoint Cloud	22	100%
SharePoint On Prem	0	0%
AWS S3	0	0%
SMB	0	0%
Google Drive	0	0%

Top 5 Compliance Frameworks (22)

Compliance Files	22	100%
NIST 800-53 and NIST 800-171	22	100%
CIS	22	100%
GDPR	5	22.73%
GLBA	5	22.73%
HIPAA	5	22.73%

Show More >

Top 10 AI Classified Document Types

Medication Management	3	13.64%
Audit and Assurance Documents	3	13.64%
Development Documentation	2	9.09%
Expense and Reimbursement Records	2	9.09%
Court Document	2	9.09%
CV	1	4.55%
Compliance and Risk Management	1	4.55%
Python	1	4.55%
Top 10 Total	15	68.18% of 22 scanned files

File Scans

Files: — Scanned — Sensitive Last 24 hours

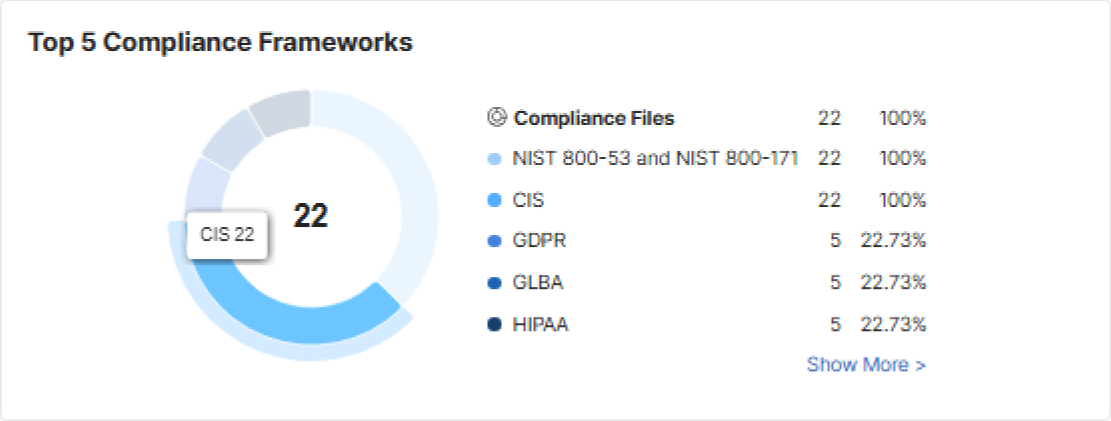
System Information

Host Name	FortiData Change
Serial Number	FDTVM[redacted]
System Time	2026-[redacted] PST Change
License Status	[redacted] Upload
Firmware Version	FortiData-KVM 7.6.2 build0133 20251223 Upgrade
Uptime	1 day, 3 hours, 31 minutes

Resource Usage

Total	45.23 GB
Free	40.1 GB
Used	2.8 GB

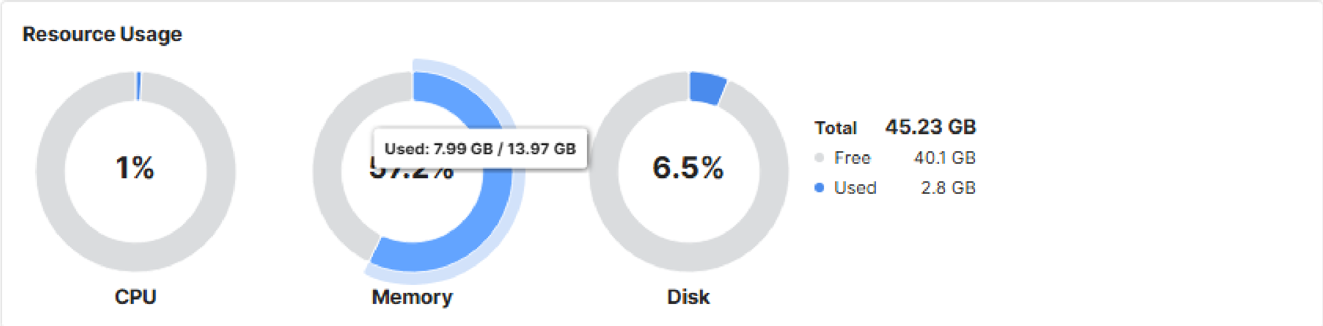
Hover your mouse over a graph or chart to view more details about the data points.



Top 5 Compliance Frameworks

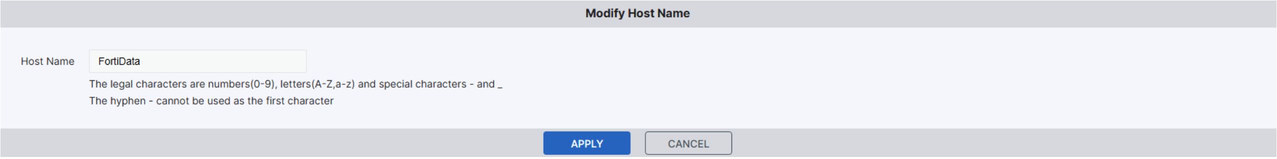
Compliance Files	22	100%
NIST 800-53 and NIST 800-171	22	100%
CIS	22	100%
GDPR	5	22.73%
GLBA	5	22.73%
HIPAA	5	22.73%

Show More >



To change the hostname:

1. Go to the *Dashboard* > *System Information* widget.
2. Click *Change* at the end of the *Host Name* field. The following page appears.



Modify Host Name

Host Name: FortiData

The legal characters are numbers(0-9), letters(A-Z,a-z) and special characters - and _
The hyphen - cannot be used as the first character

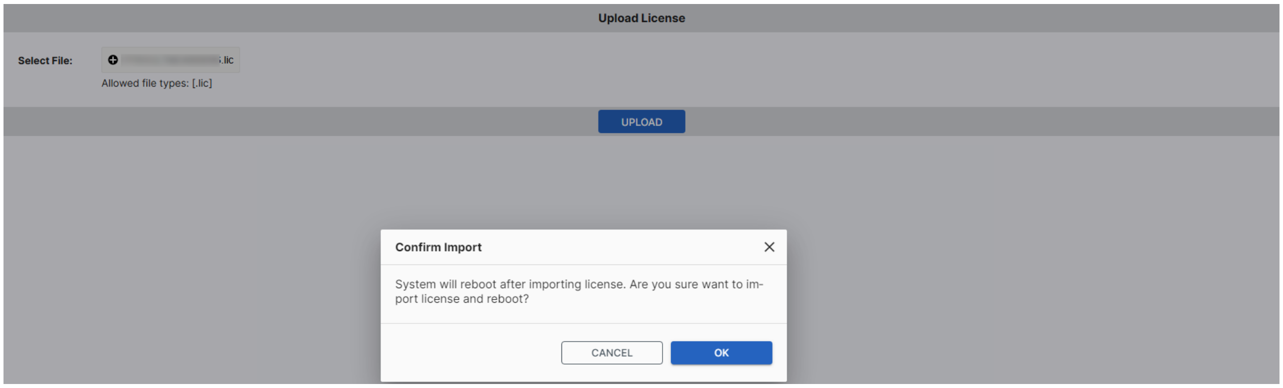
3. Specify the desired hostname and click *APPLY*.

To change the system time:

1. Go to the *Dashboard* > *System Information* widget.
2. Click *Change* at the end of the *System Time* field.
3. Configure the system time in the *System* > *Settings on page 51* tab.

To upload or change the license:

1. Go to the *Dashboard* > *System Information* widget.
2. Click *Upload* or *Upgrade* at the end of the *License* field.
3. Click *Browse* to locate the license file on your local disk.
4. Click *UPLOAD*.
5. Click *OK* when prompted.



Upload License

Select File: [redacted].lic

Allowed file types: [.lic]

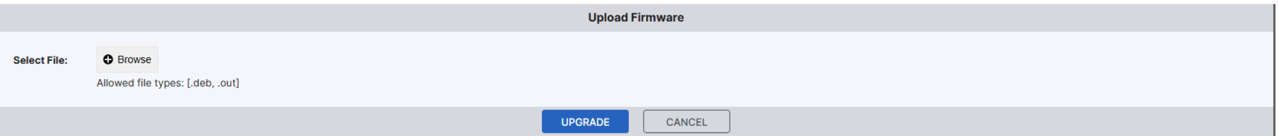
Confirm Import

System will reboot after importing license. Are you sure want to import license and reboot?

To upgrade the firmware:

FortiData does not support downgrading to previous firmware versions. You can back up configurations before upgrade or restore older firmware and configurations in *System* > *Backup & Restore on page 60*.

1. Download the firmware file from the Fortinet support website. See the FortiData KVM or ESXi guide for more details.
2. Go to *Dashboard* > *System Information*.
3. Click *Upgrade* at the end of *Firmware Version*. The following window displays.



Allowed file types: [.deb, .out]

4. Click *Browse* to select the downloaded firmware.
5. Click *UPGRADE*.
6. Wait for the upgrade to complete, which might take a few minutes.

The system replaces the firmware on the active partition and reboots.

To reboot the system:

1. Go to the *Dashboard* .
2. On the top-right corner, click *admin* > *Reboot*.

Alternatively, run the `execute reboot` command via the CLI.

To shut down the system:

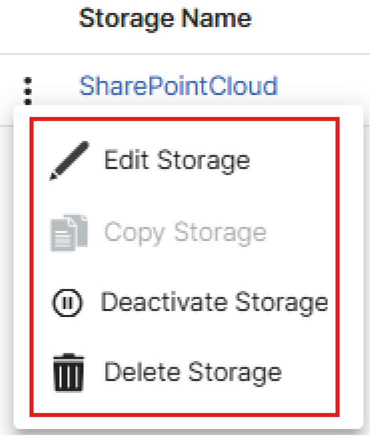
1. Go to the *Dashboard* .
2. On the top-right corner, click *admin* > *Shutdown*.

Alternatively, run the `execute shutdown` command via the CLI.

Storages

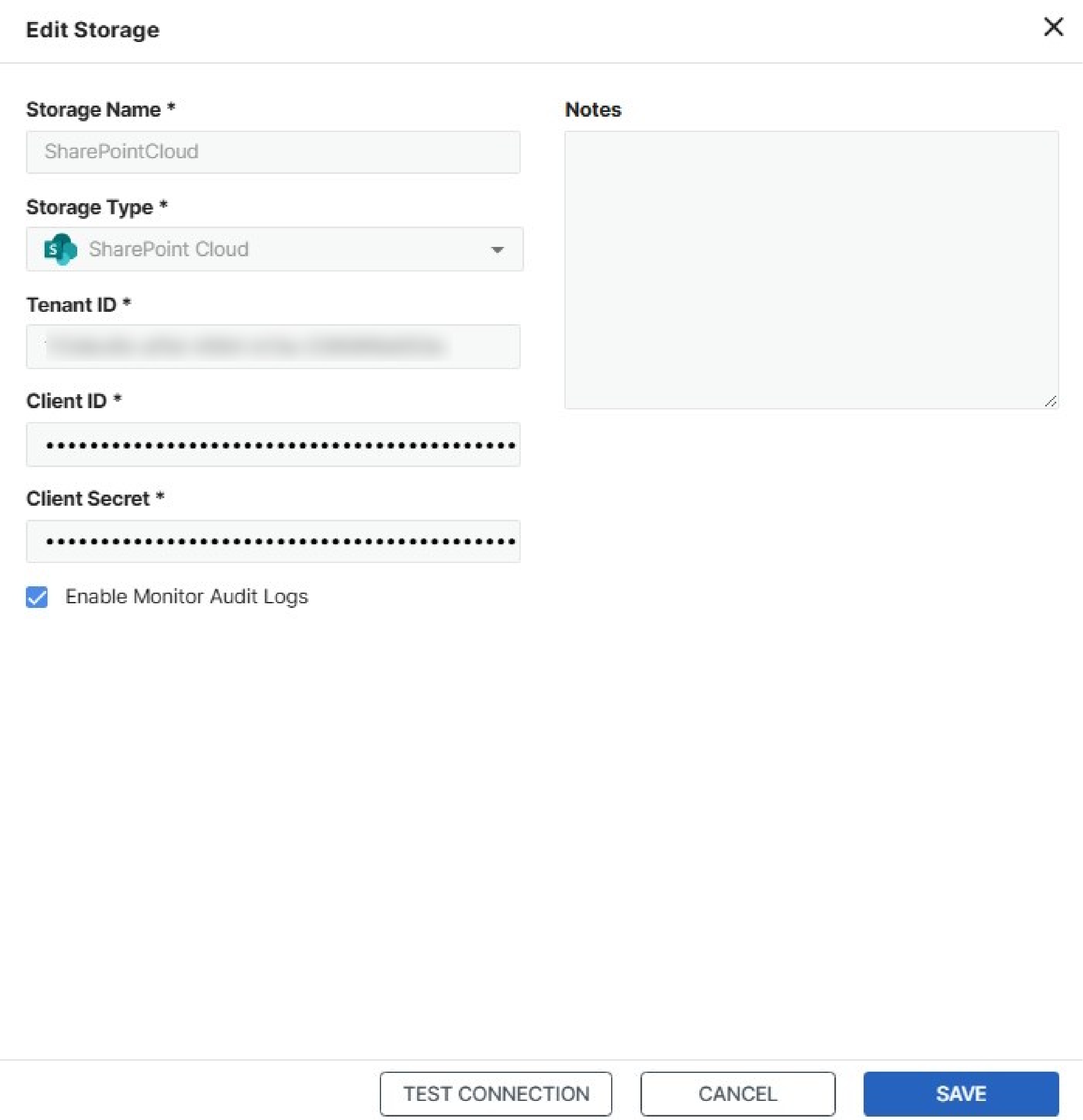
The *Storages* page lists all storage locations you have configured in FortiData, which you can reference in Scans on page 21. You can search the storages by queries with various conditions.

- To customize the columns to display in the table, use the *Configure* button on the top-right.
- To edit, copy, activate/deactivate a storage, click the eclipsis in front of the storage name and select from the following options:



To add a storage:

1. Click *Add Storage*.
2. specify the storage name and select the storage type from one of the following.
   - *AWS Bucket*
   - *SharePoint Cloud*
   - *SharePoint On Prem*
   - *SMB*—Samba
   - *Google Drive*



Edit Storage

Storage Name * SharePointCloud

Storage Type * SharePoint Cloud

Tenant ID * [redacted]

Client ID * ••

Client Secret * ••

☑ Enable Monitor Audit Logs

Notes

3. Specify the authentication details for the target location. For the following storage types, the user or application must have all the required permissions.

Storage Type	Required Permission(s)
AWS Bucket	*AmazonS3FullAccess*
SharePoint Cloud	When using token authentication, the following permissions are required for FortiData to access the necessary APIs.

Storage Type	Required Permission(s)		
	Permission	**Type**	**Description**
	Microsoft Graph		
	Application.Read.All	Application	Read all applications.
	AuditLog.Read.All	Application	Read all audit log data.
	Directory.Read.All	Application	Read directory data.
	Files.ReadWrite.All	Application	Read and write files in all site collections.
	Group.Read.All	Application	Read all groups.
	GroupMember.Read.All	Application	Read all group memberships.
	Organization.Read.All	Application	Read organization information.
	People.Read.All	Application	Read all users' relevant people lists.
	Reports.Read.All	Application	Read all usage reports.
	Sites.FullControl.All	Application	Have full control of all site collections.
	Sites.Manage.All	Application	Create, edit, and delete items and lists in all site collections.
	Sites.ReadWrite.All	Application	Read and write items in all site collections.
	Office 365 Management APIs		
	ActivityFeed.Read	Application	Read activity data for your organization. This permission is required only if *Enable Monitor Audit Logs* is enabled.

4. Select *Enable Monitor Audit Logs* as needed.
5. Added notes as needed.
6. Click *TEST CONNECTION* to verify the connection is successful.
7. Click *SAVE*.

Incident Center

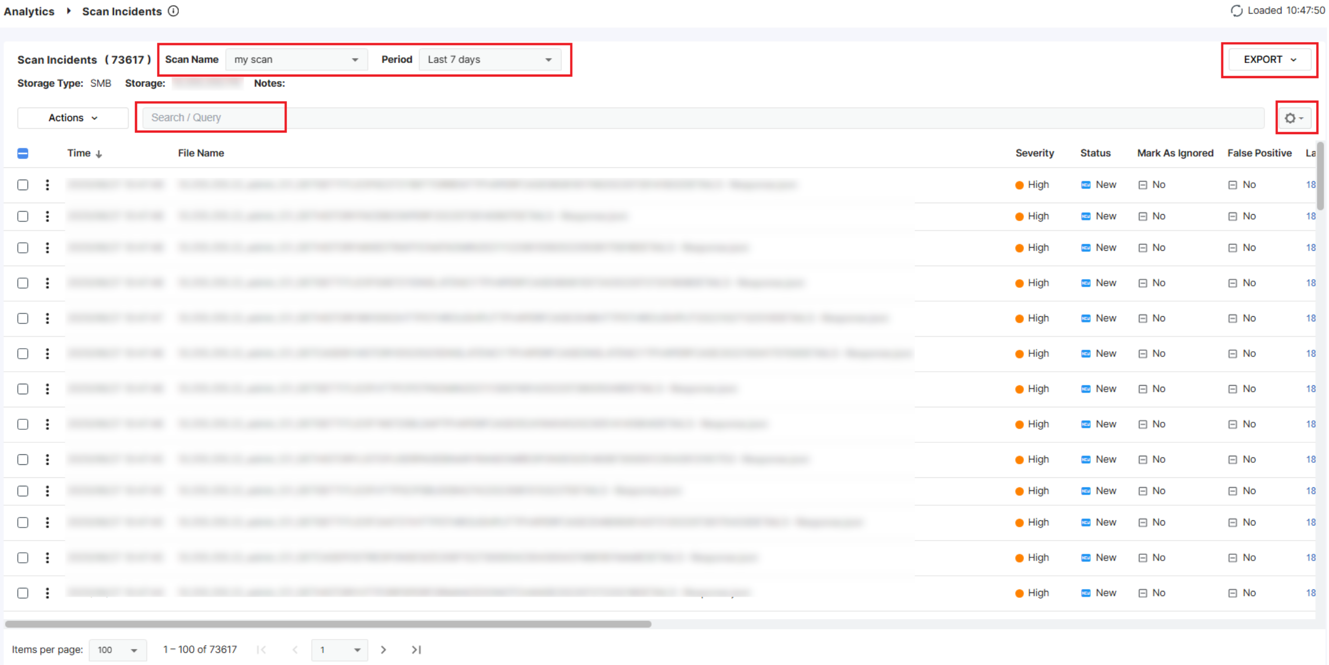
Go to the *Incident Center* page to view scan-based and integration-based incidents.

- Issues on page 13
- Integration Events on page 15

Issues

The *Incident Center> Issues* page lists scan-based incidents in an aggregated dynamic view. You can filter the logs by storage name, time period, and queries with various conditions. Retention period of scan incidents logs is 30 days

- To customize the columns to display in the table, use the *Configure* button on the top-right.
- To export the logs, click *EXPORT > Export JSON/CSV*.



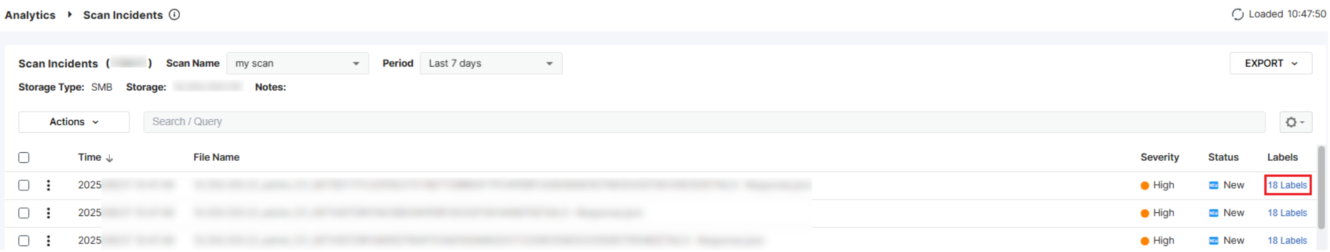
Scan Incidents (73617) Scan Name: my scan Period: Last 7 days

Storage Type: SMB Storage: [redacted] Notes:

☐		Time ↓	File Name	Severity	Status	Mark As Ignored	False Positive	La
☐	⋮	[redacted]	[redacted]	● High	New	⊟ No	⊟ No	18
☐	⋮	[redacted]	[redacted]	● High	New	⊟ No	⊟ No	18
☐	⋮	[redacted]	[redacted]	● High	New	⊟ No	⊟ No	18
☐	⋮	[redacted]	[redacted]	● High	New	⊟ No	⊟ No	18
☐	⋮	[redacted]	[redacted]	● High	New	⊟ No	⊟ No	18
☐	⋮	[redacted]	[redacted]	● High	New	⊟ No	⊟ No	18
☐	⋮	[redacted]	[redacted]	● High	New	⊟ No	⊟ No	18
☐	⋮	[redacted]	[redacted]	● High	New	⊟ No	⊟ No	18
☐	⋮	[redacted]	[redacted]	● High	New	⊟ No	⊟ No	18
☐	⋮	[redacted]	[redacted]	● High	New	⊟ No	⊟ No	18
☐	⋮	[redacted]	[redacted]	● High	New	⊟ No	⊟ No	18
☐	⋮	[redacted]	[redacted]	● High	New	⊟ No	⊟ No	18
☐	⋮	[redacted]	[redacted]	● High	New	⊟ No	⊟ No	18

Items per page: 100 1 – 100 of 73617 |< < 1 > >|

To see the assigned labels for an incident, click the link in the *Labels* column.



Analytics ▸ Scan Incidents ⓘ — Loaded 10:47:50

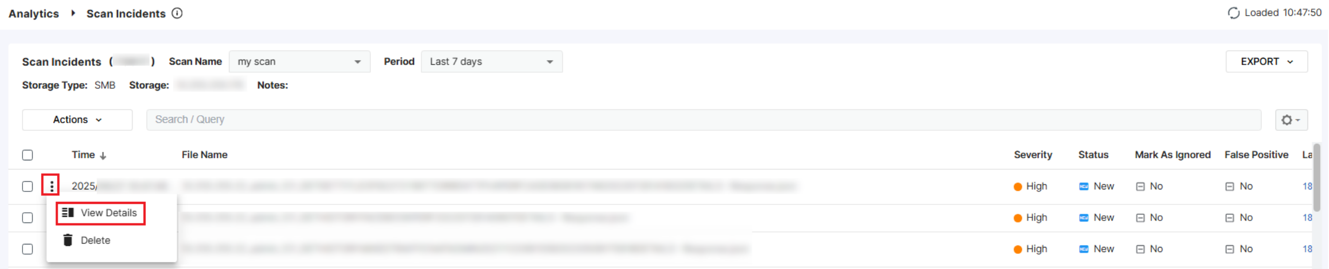
Scan Incidents ([redacted]) Scan Name: my scan Period: Last 7 days EXPORT

Storage Type: SMB Storage: [redacted] Notes:

Actions — Search / Query

☐	Time ↓	File Name	Severity	Status	Labels
☐	2025[redacted]	[redacted]	● High	New	18 Labels
☐	2025[redacted]	[redacted]	● High	New	18 Labels
☐	2025[redacted]	[redacted]	● High	New	18 Labels

To view more details of an incident, click the three dots at the front of the row and select *View Details*. The *Scan Incident Details* pane appears on the right.



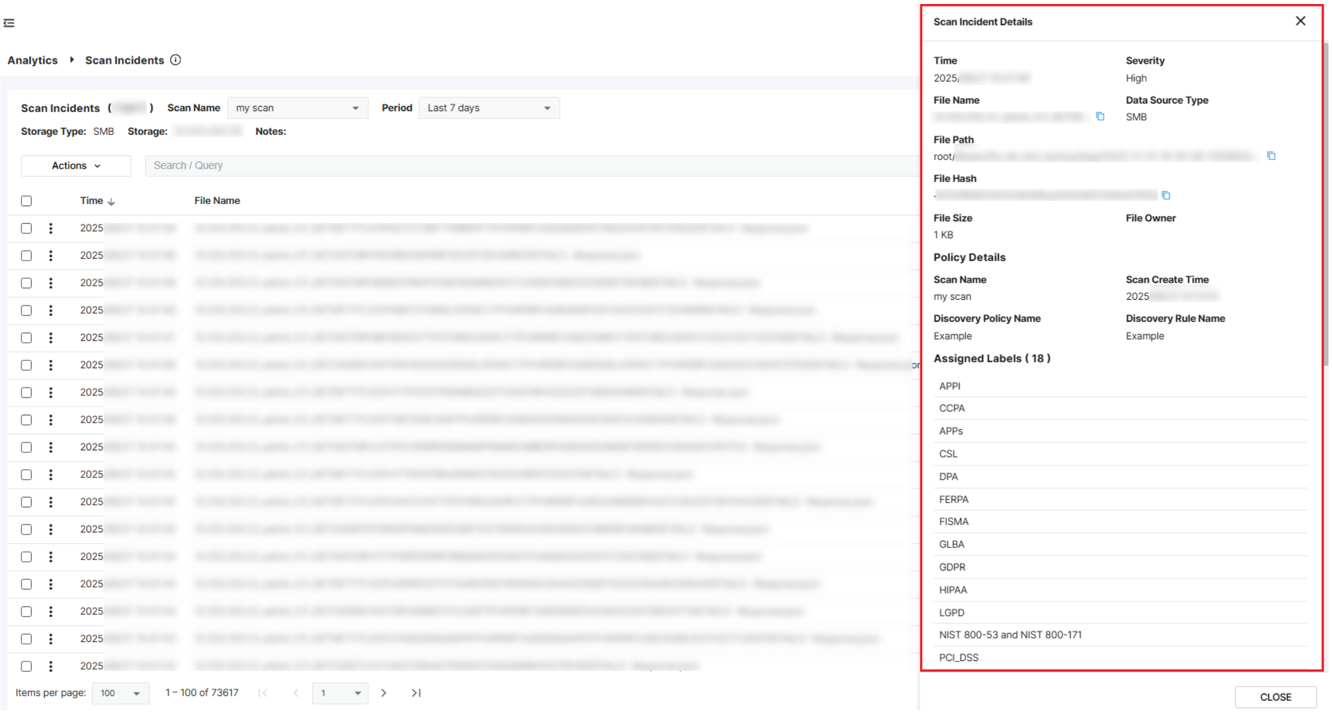
Analytics ▸ Scan Incidents ⓘ — Loaded 10:47:50

Scan Incidents ([redacted]) Scan Name: my scan Period: Last 7 days EXPORT

Storage Type: SMB Storage: [redacted] Notes:

Actions — Search / Query

☐	Time ↓	File Name	Severity	Status	Mark As Ignored	False Positive	La
☐	2025/[redacted]	[redacted]	● High	New	No	No	18
☐		[redacted]	● High	New	No	No	18
☐		[redacted]	● High	New	No	No	18



Analytics ▸ Scan Incidents ⓘ

Scan Incidents ([redacted]) Scan Name: my scan Period: Last 7 days

Storage Type: SMB Storage: [redacted] Notes:

Actions — Search / Query

☐	Time ↓	File Name
☐	2025[redacted]	[redacted]

Items per page: 100 1 – 100 of 73617 1

Scan Incident Details

Time 2025/[redacted]	Severity High
File Name [redacted]	Data Source Type SMB
File Path root/[redacted]	
File Hash [redacted]	
File Size 1 KB	File Owner

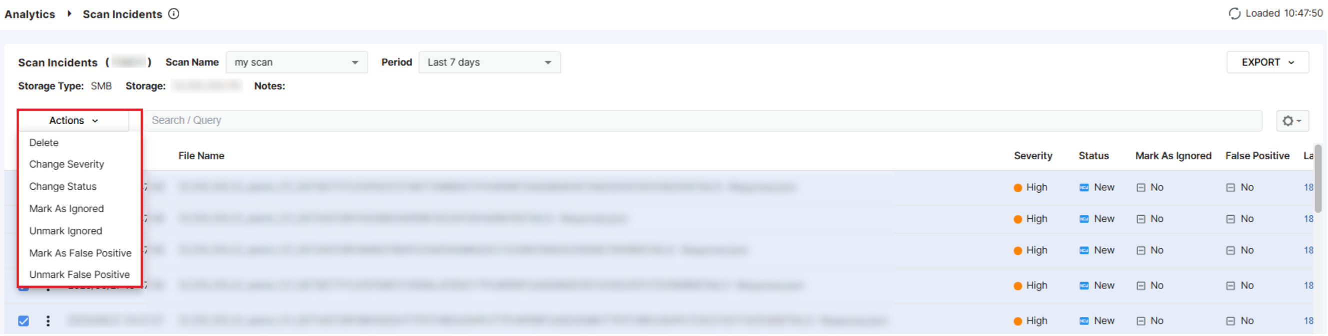
Policy Details

Scan Name my scan	Scan Create Time 2025[redacted]
Discovery Policy Name Example	Discovery Rule Name Example

Assigned Labels (18)

APPI
CCPA
APPs
CSL
DPA
FERPA
FISMA
GLBA
GDPR
HIPAA
LGPD
NIST 800-53 and NIST 800-171
PCI_DSS

Select one or more incidents and click the *Actions* button to perform the following operations:



Analytics ▸ Scan Incidents ⓘ

Loaded 10:47:50

Scan Incidents ([redacted]) Scan Name: my scan Period: Last 7 days

Storage Type: SMB Storage: [redacted] Notes:

File Name	Severity	Status	Mark As Ignored	False Positive	La
[redacted]	● High	New	⊟ No	⊟ No	18
[redacted]	● High	New	⊟ No	⊟ No	18
[redacted]	● High	New	⊟ No	⊟ No	18
[redacted]	● High	New	⊟ No	⊟ No	18
[redacted]	● High	New	⊟ No	⊟ No	18

Integration Events

The *Incident Center> Integration Events* page lists scan incidents for files uploaded by FortiClient (see Integration with FortiClient). You can filter the logs by time period and queries with various conditions. Retention period of integration events logs is 30 days.

- To customize the columns to display in the table, use the *Configure* button on the top-right.
- To export the logs, click *Export > Export JSON/CSV*.

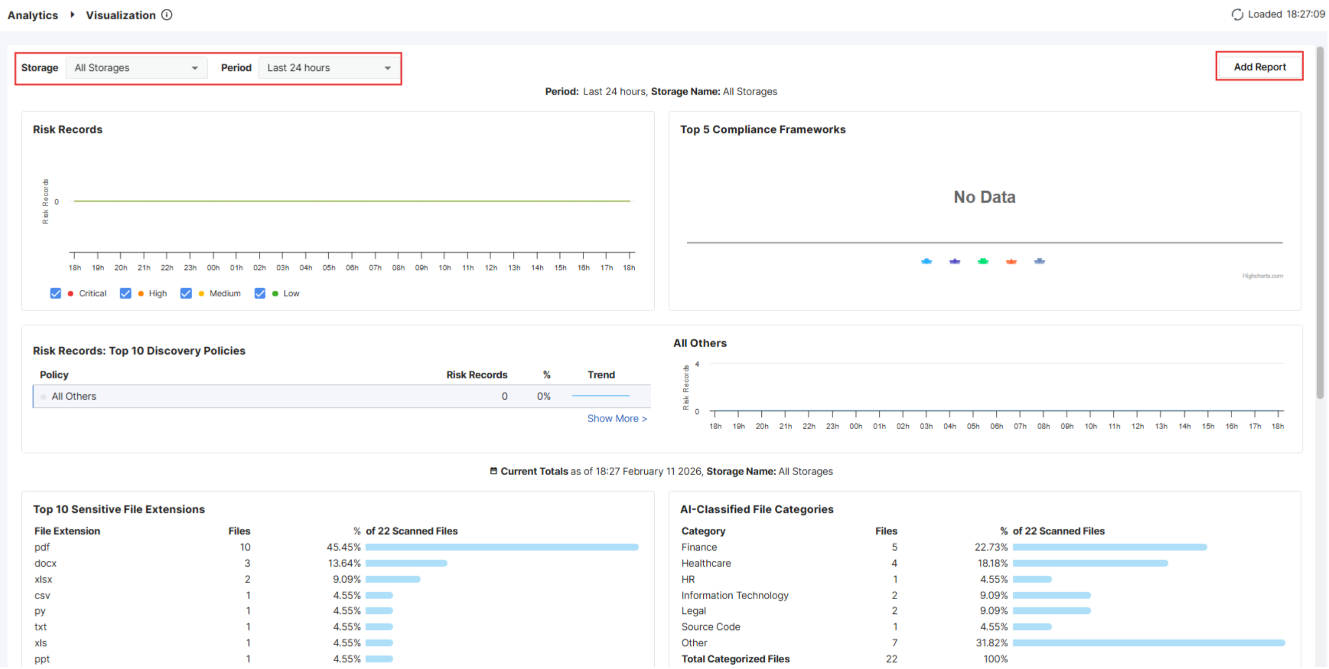
Analytics

Go to the *Analytics* page to view a visualized summary of the scan results and a list of scanned files.

- Visualization on page 16
- Data on page 17
- Identities on page 19

Visualization

A summary of scan result is available in the *Analytics* > *Visualization* page with interactive graphs and charts. You can filter the result by storage name and time period. You can also add a *Sensitive Data Landscape* report using the *Add Report* button on the top-right corner. The report will then be available in the *Logs & Reports* > *Reports on page 42* page.



Storage: All Storages
Period: Last 24 hours

Period: Last 24 hours, **Storage Name:** All Storages

Risk Records: Top 10 Discovery Policies

Policy	Risk Records	%	Trend
All Others	0	0%	

Current Totals as of 18:27 February 11 2026, **Storage Name:** All Storages

Top 10 Sensitive File Extensions

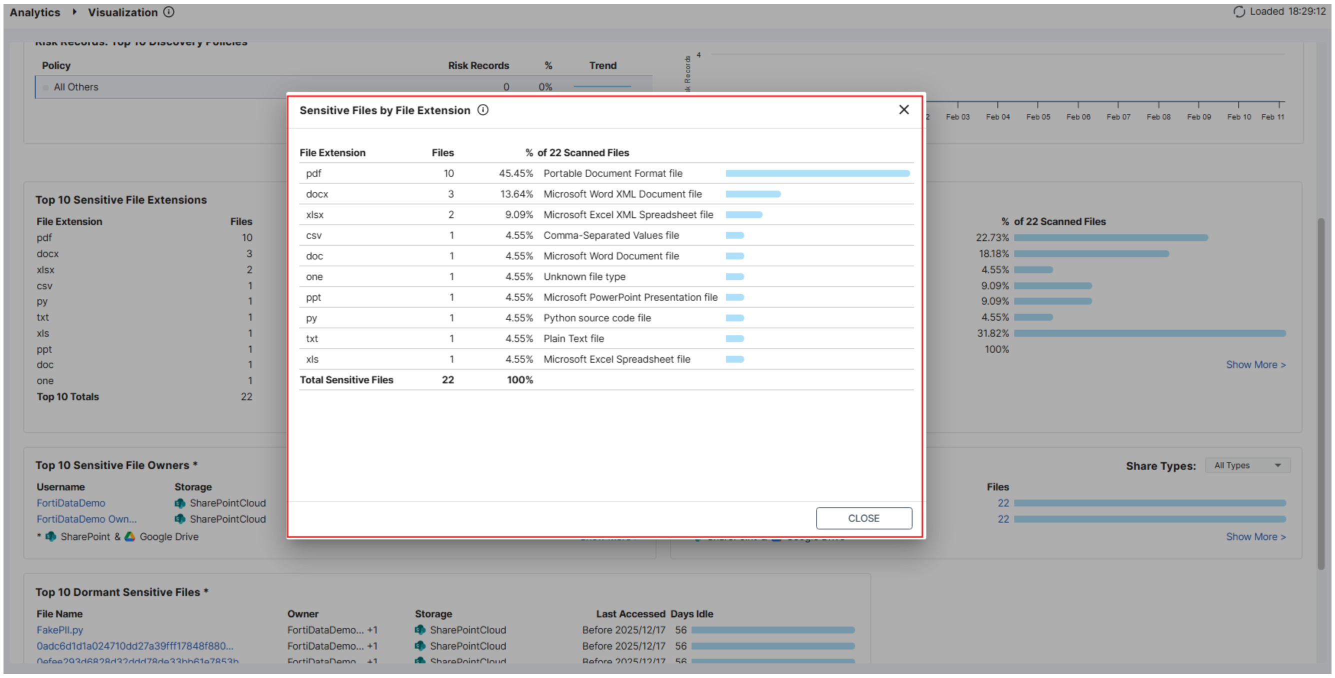
File Extension	Files	% of 22 Scanned Files
pdf	10	45.45%
docx	3	13.64%
xlsx	2	9.09%
csv	1	4.55%
py	1	4.55%
txt	1	4.55%
xls	1	4.55%
ppt	1	4.55%

AI-Classified File Categories

Category	Files	% of 22 Scanned Files
Finance	5	22.73%
Healthcare	4	18.18%
HR	1	4.55%
Information Technology	2	9.09%
Legal	2	9.09%
Source Code	1	4.55%
Other	7	31.82%
Total Categorized Files	22	100%

Hover your mouse over a graph or chart to view more details about the data points.

Click *Show More* to view more details about the data points.



Sensitive Files by File Extension ⓘ

File Extension	Files	% of 22 Scanned Files	
pdf	10	45.45%	Portable Document Format file
docx	3	13.64%	Microsoft Word XML Document file
xlsx	2	9.09%	Microsoft Excel XML Spreadsheet file
csv	1	4.55%	Comma-Separated Values file
doc	1	4.55%	Microsoft Word Document file
one	1	4.55%	Unknown file type
ppt	1	4.55%	Microsoft PowerPoint Presentation file
py	1	4.55%	Python source code file
txt	1	4.55%	Plain Text file
xls	1	4.55%	Microsoft Excel Spreadsheet file
Total Sensitive Files	**22**	**100%**	

Policy	Risk Records	%	Trend
All Others	0	0%	

Top 10 Sensitive File Extensions

File Extension	Files
pdf	10
docx	3
xlsx	2
csv	1
py	1
txt	1
xls	1
ppt	1
doc	1
one	1
Top 10 Totals	22

Top 10 Sensitive File Owners *

Username	Storage
FortiDataDemo	SharePointCloud
FortiDataDemo Own...	SharePointCloud

* SharePoint & Google Drive

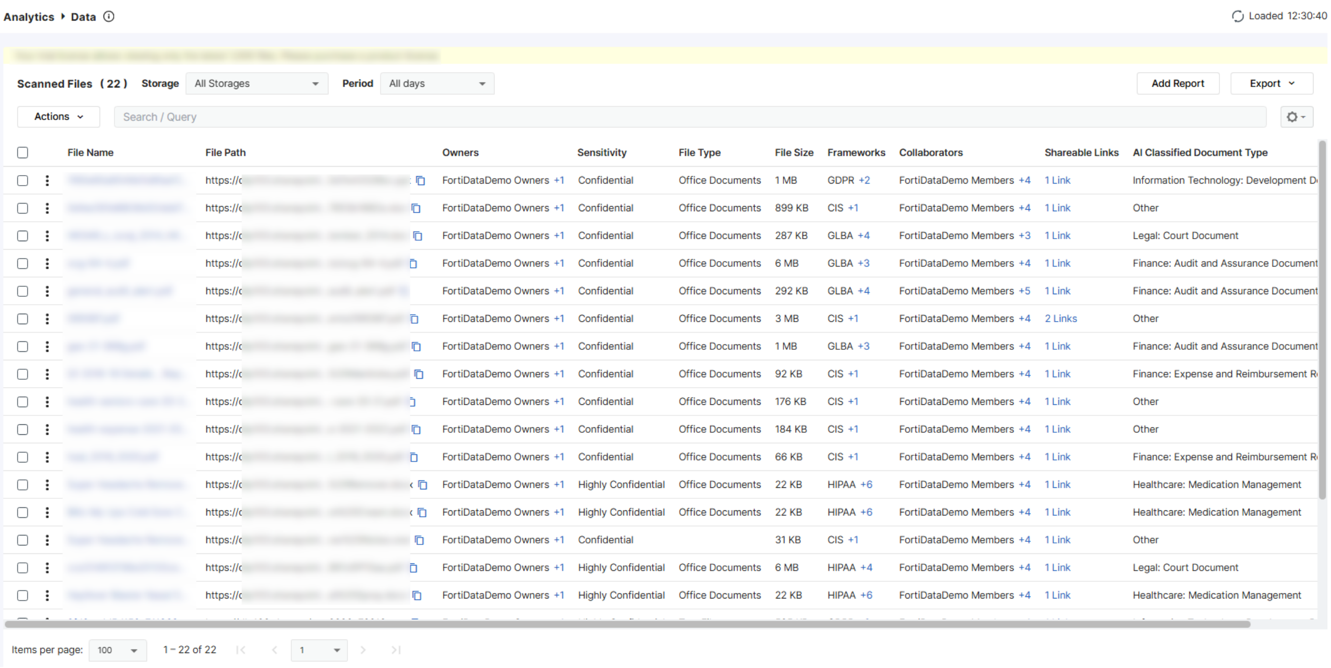
Top 10 Dormant Sensitive Files *

File Name	Owner	Storage	Last Accessed	Days Idle
FakePII.py	FortiDataDemo... +1	SharePointCloud	Before 2025/12/17	56
0adc6d1d1a024710dd27a39fff17848f880...	FortiDataDemo... +1	SharePointCloud	Before 2025/12/17	56
0efee293d6828d32ddd78de33bb61e7853b	FortiDataDemo... +1	SharePointCloud	Before 2025/12/17	56

Data

A list of scanned files is available in the *Analytics > Data* page. You can filter the files by scan name, time period, and queries with various conditions.

- To customize the columns to display in the table, use the *Configure* button on the top-right.
- To export the scanned file list, click *Export > Export JSON/CSV*.
- To create a *Data Inventory* report, click *Add Report*. The report will appear in *Logs & Reports > Reports on page 42*.

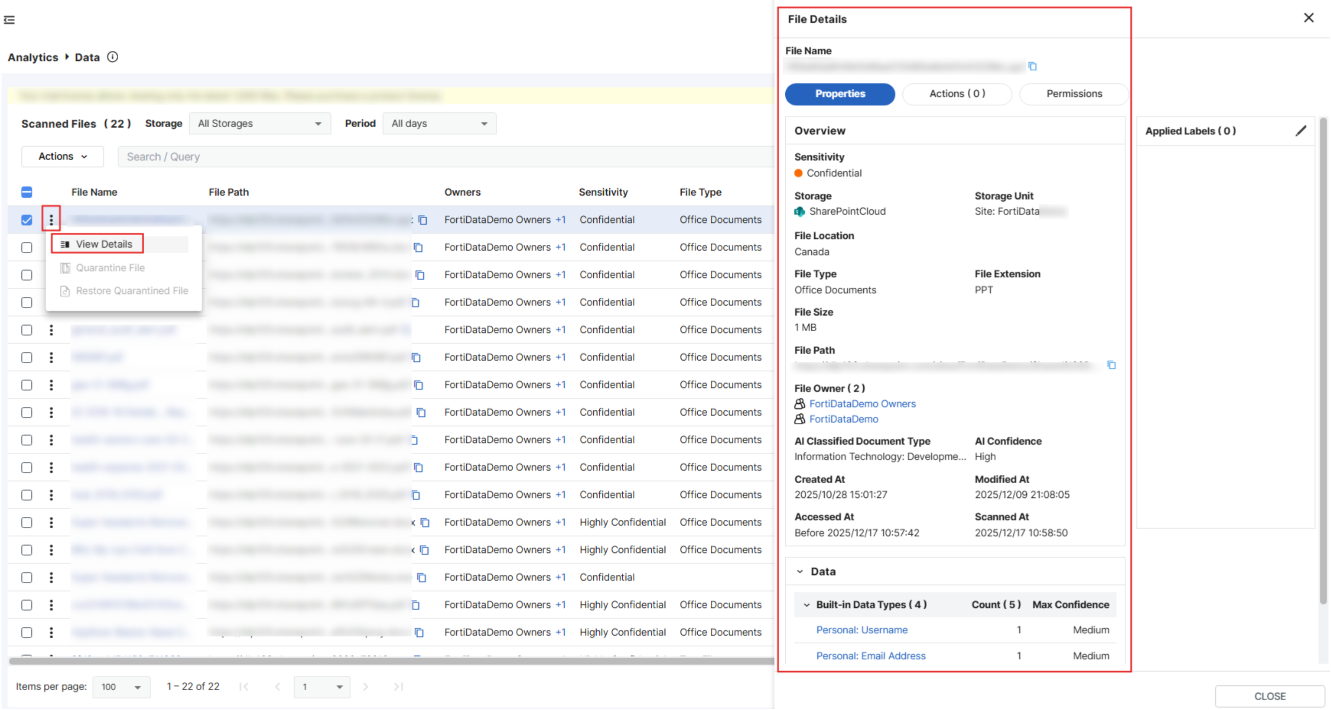


Scanned Files (22) Storage: All Storages Period: All days

□		File Name	File Path	Owners	Sensitivity	File Type	File Size	Frameworks	Collaborators	Shareable Links	AI Classified Document Type
□	⋮	[redacted]	https://c[redacted]	FortiDataDemo Owners +1	Confidential	Office Documents	1 MB	GDPR +2	FortiDataDemo Members +4	1 Link	Information Technology: Development D
□	⋮	[redacted]	https://c[redacted]	FortiDataDemo Owners +1	Confidential	Office Documents	899 KB	CIS +1	FortiDataDemo Members +4	1 Link	Other
□	⋮	[redacted]	https://c[redacted]	FortiDataDemo Owners +1	Confidential	Office Documents	287 KB	GLBA +4	FortiDataDemo Members +3	1 Link	Legal: Court Document
□	⋮	[redacted]	https://c[redacted]	FortiDataDemo Owners +1	Confidential	Office Documents	6 MB	GLBA +3	FortiDataDemo Members +4	1 Link	Finance: Audit and Assurance Document
□	⋮	[redacted]	https://c[redacted]	FortiDataDemo Owners +1	Confidential	Office Documents	292 KB	GLBA +4	FortiDataDemo Members +5	1 Link	Finance: Audit and Assurance Document
□	⋮	[redacted]	https://c[redacted]	FortiDataDemo Owners +1	Confidential	Office Documents	3 MB	CIS +1	FortiDataDemo Members +4	2 Links	Other
□	⋮	[redacted]	https://c[redacted]	FortiDataDemo Owners +1	Confidential	Office Documents	1 MB	GLBA +3	FortiDataDemo Members +4	1 Link	Finance: Audit and Assurance Document
□	⋮	[redacted]	https://c[redacted]	FortiDataDemo Owners +1	Confidential	Office Documents	92 KB	CIS +1	FortiDataDemo Members +4	1 Link	Finance: Expense and Reimbursement R
□	⋮	[redacted]	https://c[redacted]	FortiDataDemo Owners +1	Confidential	Office Documents	176 KB	CIS +1	FortiDataDemo Members +4	1 Link	Other
□	⋮	[redacted]	https://c[redacted]	FortiDataDemo Owners +1	Confidential	Office Documents	184 KB	CIS +1	FortiDataDemo Members +4	1 Link	Other
□	⋮	[redacted]	https://c[redacted]	FortiDataDemo Owners +1	Confidential	Office Documents	66 KB	CIS +1	FortiDataDemo Members +4	1 Link	Finance: Expense and Reimbursement R
□	⋮	[redacted]	https://c[redacted]	FortiDataDemo Owners +1	Highly Confidential	Office Documents	22 KB	HIPAA +6	FortiDataDemo Members +4	1 Link	Healthcare: Medication Management
□	⋮	[redacted]	https://c[redacted]	FortiDataDemo Owners +1	Highly Confidential	Office Documents	22 KB	HIPAA +6	FortiDataDemo Members +4	1 Link	Healthcare: Medication Management
□	⋮	[redacted]	https://c[redacted]	FortiDataDemo Owners +1	Confidential		31 KB	CIS +1	FortiDataDemo Members +4	1 Link	Other
□	⋮	[redacted]	https://c[redacted]	FortiDataDemo Owners +1	Highly Confidential	Office Documents	6 MB	HIPAA +4	FortiDataDemo Members +4	1 Link	Legal: Court Document
□	⋮	[redacted]	https://c[redacted]	FortiDataDemo Owners +1	Highly Confidential	Office Documents	22 KB	HIPAA +6	FortiDataDemo Members +4	1 Link	Healthcare: Medication Management

Items per page: 100 1 – 22 of 22 1

To view more details of a scanned file, click the three dots at the front of the row and select *View Details*. The *File Details* pane appears on the right.



File Details

File Name
[redacted]

Overview

Sensitivity
● Confidential

Storage: SharePointCloud
Storage Unit: Site: FortiData[redacted]

File Location
Canada

File Type: Office Documents
File Extension: PPT

File Size
1 MB

File Path
[redacted]

File Owner (2)
FortiDataDemo Owners
FortiDataDemo

AI Classified Document Type: Information Technology: Developme...
AI Confidence: High

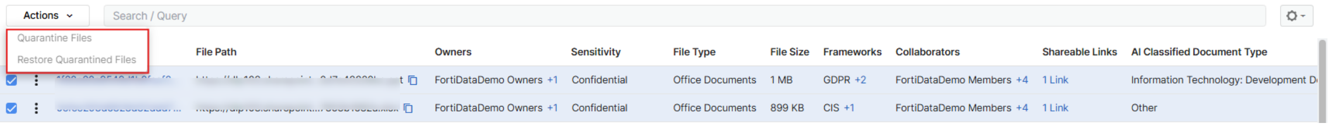
Created At: 2025/10/28 15:01:27
Modified At: 2025/12/09 21:08:05

Accessed At: Before 2025/12/17 10:57:42
Scanned At: 2025/12/17 10:58:50

Data

Built-in Data Types (4)	Count (5)	Max Confidence
Personal: Username	1	Medium
Personal: Email Address	1	Medium

Select one or more scanned files and click the *Actions* button to perform the following operations:

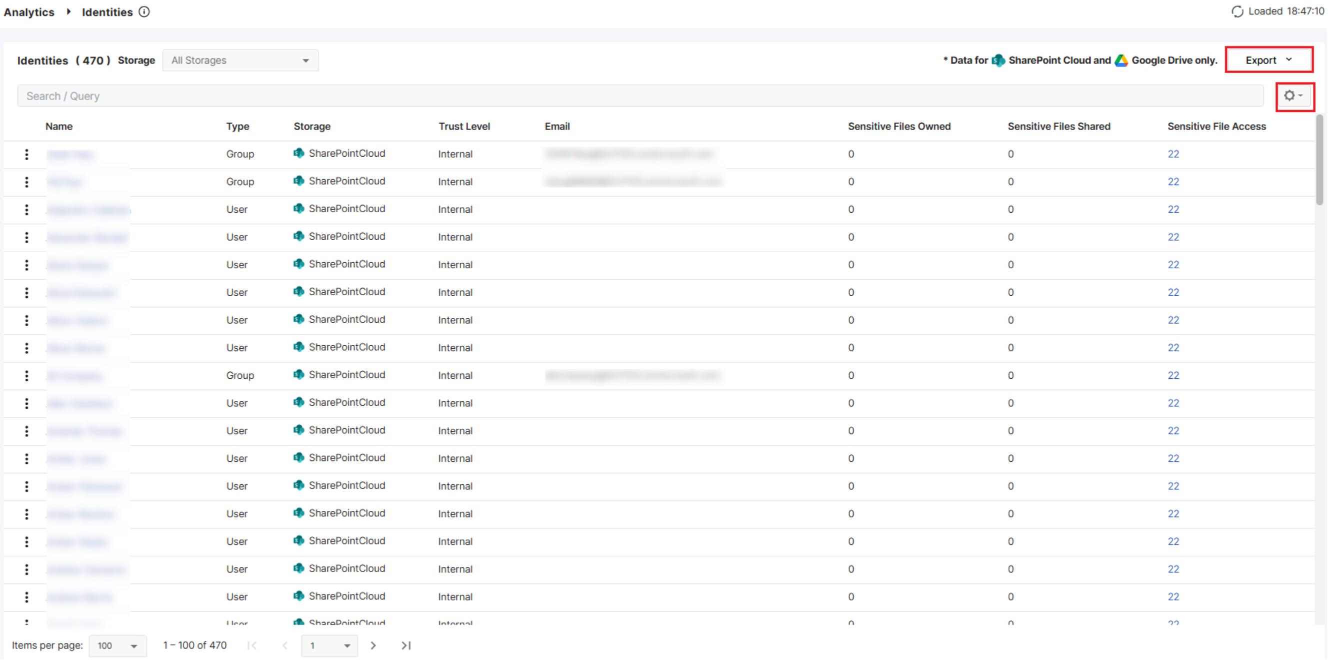


		File Name	File Path	Owners	Sensitivity	File Type	File Size	Frameworks	Collaborators	Shareable Links	AI Classified Document Type
☑	⋮	[redacted]	[redacted]	FortiDataDemo Owners +1	Confidential	Office Documents	1 MB	GDPR +2	FortiDataDemo Members +4	1 Link	Information Technology: Development D
☑	⋮	[redacted]	[redacted]	FortiDataDemo Owners +1	Confidential	Office Documents	899 KB	CIS +1	FortiDataDemo Members +4	1 Link	Other

Identities

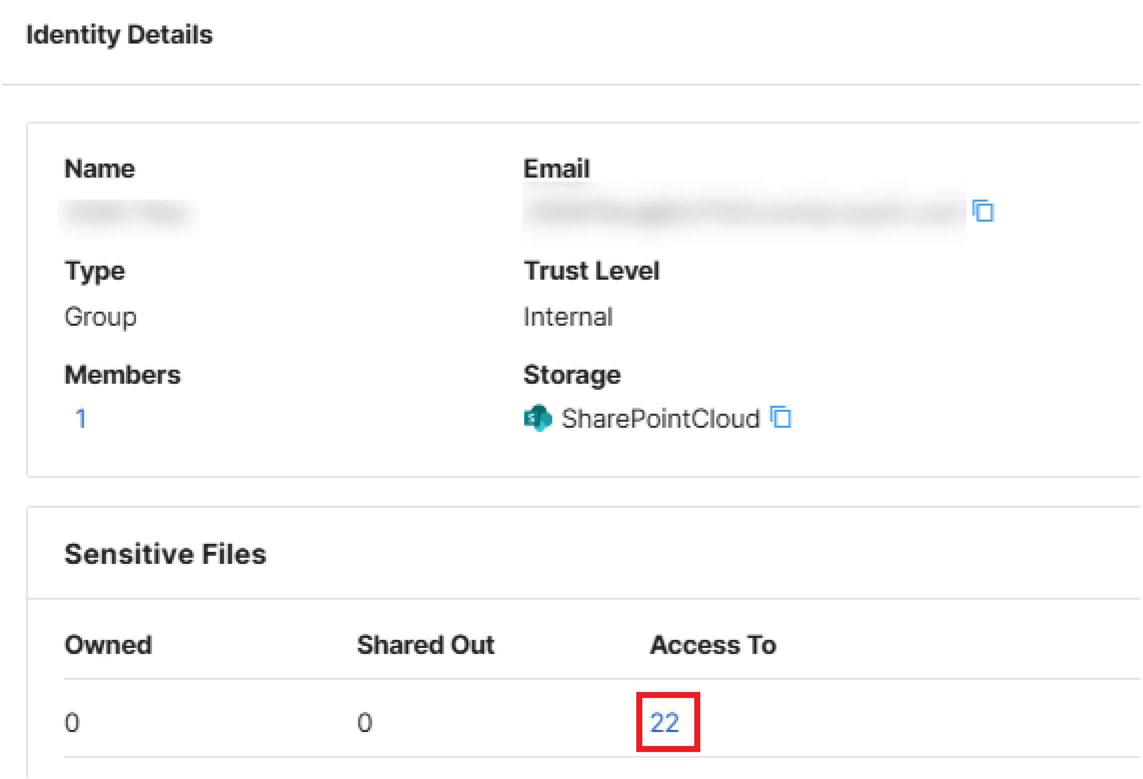
The *Analytics > Identities* page lists the users and groups fetched from cloud storage systems. You can filter the users/groups by storage name and queries with various conditions.

- To customize the columns to display in the table, use the *Configure* button on the top-right.
- To export the users and groups list, click *Export > Export JSON/CSV*.



Name	Type	Storage	Trust Level	Email	Sensitive Files Owned	Sensitive Files Shared	Sensitive File Access
[redacted]	Group	SharePointCloud	Internal	[redacted]	0	0	22
[redacted]	Group	SharePointCloud	Internal	[redacted]	0	0	22
[redacted]	User	SharePointCloud	Internal		0	0	22
[redacted]	User	SharePointCloud	Internal		0	0	22
[redacted]	User	SharePointCloud	Internal		0	0	22
[redacted]	User	SharePointCloud	Internal		0	0	22
[redacted]	User	SharePointCloud	Internal		0	0	22
[redacted]	User	SharePointCloud	Internal		0	0	22
[redacted]	Group	SharePointCloud	Internal	[redacted]	0	0	22
[redacted]	User	SharePointCloud	Internal		0	0	22
[redacted]	User	SharePointCloud	Internal		0	0	22
[redacted]	User	SharePointCloud	Internal		0	0	22
[redacted]	User	SharePointCloud	Internal		0	0	22
[redacted]	User	SharePointCloud	Internal		0	0	22
[redacted]	User	SharePointCloud	Internal		0	0	22
[redacted]	User	SharePointCloud	Internal		0	0	22
[redacted]	User	SharePointCloud	Internal		0	0	22
[redacted]	User	SharePointCloud	Internal		0	0	22

Click the name to view details about the user or group. You can then view the filtered list of sensitive files associated with the user or group by clicking the link.

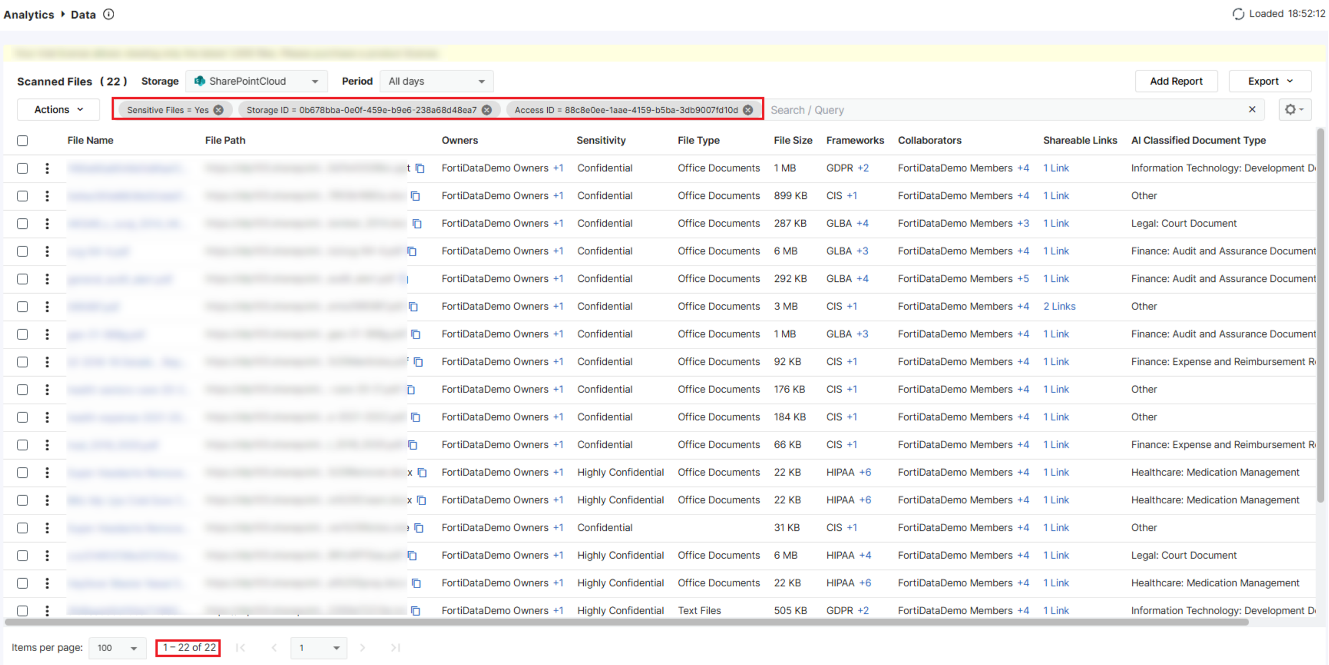


Identity Details

Name [redacted]	**Email** [redacted]
Type Group	**Trust Level** Internal
Members 1	**Storage** SharePointCloud

Sensitive Files

Owned	Shared Out	Access To
0	0	22



Analytics ▸ Data ⓘ

Loaded 18:52:12

Scanned Files (22) Storage: SharePointCloud Period: All days

Sensitive Files = Yes ⊗ Storage ID = 0b678bba-0e0f-459e-b9e6-238a68d48ea7 ⊗ Access ID = 88c8e0ee-1aae-4159-b5ba-3db9007fd10d ⊗

Search / Query

☐	File Name	File Path	Owners	Sensitivity	File Type	File Size	Frameworks	Collaborators	Shareable Links	AI Classified Document Type
☐	[redacted]	[redacted]	FortiDataDemo Owners +1	Confidential	Office Documents	1 MB	GDPR +2	FortiDataDemo Members +4	1 Link	Information Technology: Development D
☐	[redacted]	[redacted]	FortiDataDemo Owners +1	Confidential	Office Documents	899 KB	CIS +1	FortiDataDemo Members +4	1 Link	Other
☐	[redacted]	[redacted]	FortiDataDemo Owners +1	Confidential	Office Documents	287 KB	GLBA +4	FortiDataDemo Members +3	1 Link	Legal: Court Document
☐	[redacted]	[redacted]	FortiDataDemo Owners +1	Confidential	Office Documents	6 MB	GLBA +3	FortiDataDemo Members +4	1 Link	Finance: Audit and Assurance Document
☐	[redacted]	[redacted]	FortiDataDemo Owners +1	Confidential	Office Documents	292 KB	GLBA +4	FortiDataDemo Members +5	1 Link	Finance: Audit and Assurance Document
☐	[redacted]	[redacted]	FortiDataDemo Owners +1	Confidential	Office Documents	3 MB	CIS +1	FortiDataDemo Members +4	2 Links	Other
☐	[redacted]	[redacted]	FortiDataDemo Owners +1	Confidential	Office Documents	1 MB	GLBA +3	FortiDataDemo Members +4	1 Link	Finance: Audit and Assurance Document
☐	[redacted]	[redacted]	FortiDataDemo Owners +1	Confidential	Office Documents	92 KB	CIS +1	FortiDataDemo Members +4	1 Link	Finance: Expense and Reimbursement R
☐	[redacted]	[redacted]	FortiDataDemo Owners +1	Confidential	Office Documents	176 KB	CIS +1	FortiDataDemo Members +4	1 Link	Other
☐	[redacted]	[redacted]	FortiDataDemo Owners +1	Confidential	Office Documents	184 KB	CIS +1	FortiDataDemo Members +4	1 Link	Other
☐	[redacted]	[redacted]	FortiDataDemo Owners +1	Confidential	Office Documents	66 KB	CIS +1	FortiDataDemo Members +4	1 Link	Finance: Expense and Reimbursement R
☐	[redacted]	[redacted]	FortiDataDemo Owners +1	Highly Confidential	Office Documents	22 KB	HIPAA +6	FortiDataDemo Members +4	1 Link	Healthcare: Medication Management
☐	[redacted]	[redacted]	FortiDataDemo Owners +1	Highly Confidential	Office Documents	22 KB	HIPAA +6	FortiDataDemo Members +4	1 Link	Healthcare: Medication Management
☐	[redacted]	[redacted]	FortiDataDemo Owners +1	Confidential		31 KB	CIS +1	FortiDataDemo Members +4	1 Link	Other
☐	[redacted]	[redacted]	FortiDataDemo Owners +1	Highly Confidential	Office Documents	6 MB	HIPAA +4	FortiDataDemo Members +4	1 Link	Legal: Court Document
☐	[redacted]	[redacted]	FortiDataDemo Owners +1	Highly Confidential	Office Documents	22 KB	HIPAA +6	FortiDataDemo Members +4	1 Link	Healthcare: Medication Management
☐	[redacted]	[redacted]	FortiDataDemo Owners +1	Highly Confidential	Text Files	505 KB	GDPR +2	FortiDataDemo Members +4	1 Link	Information Technology: Development D

Items per page: 100 1 – 22 of 22 1

Discovery

The *Discovery* menu allows you to configure policies, rules, profiles, and schedules to scan for sensitive files. Follow the configuration steps below:

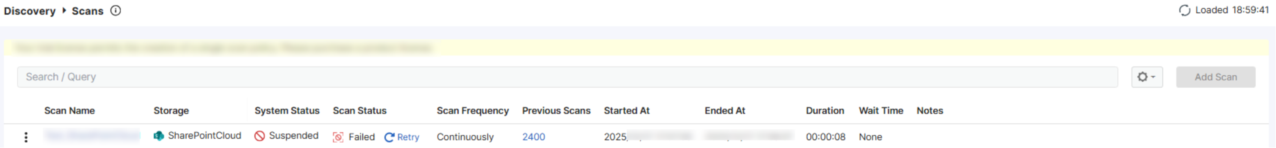
1. Create data discovery policies to look for specific types of data (using Data Classifiers on page 37) in files and assign specific labels to files that meet the specified context conditions. See Policies on page 27.
2. Define a scan to access and analyze files in a target location (for a storage type) using the conditions and actions defined in the discovery policy with a proper schedule. See Scans on page 21.
3. View file scan and classification results in the *Analytics on page 16* pages.

Scans

On the *Discovery* > *Scans* page, you can define a scan to access and analyze files in a target location (for a storage type) using the conditions and actions defined in the discovery policy with a proper schedule and apply a profile as needed. Scan and classification results can then be viewed in the *Analytics on page 16* pages. You can create up to 16 scans.

To create a scan:

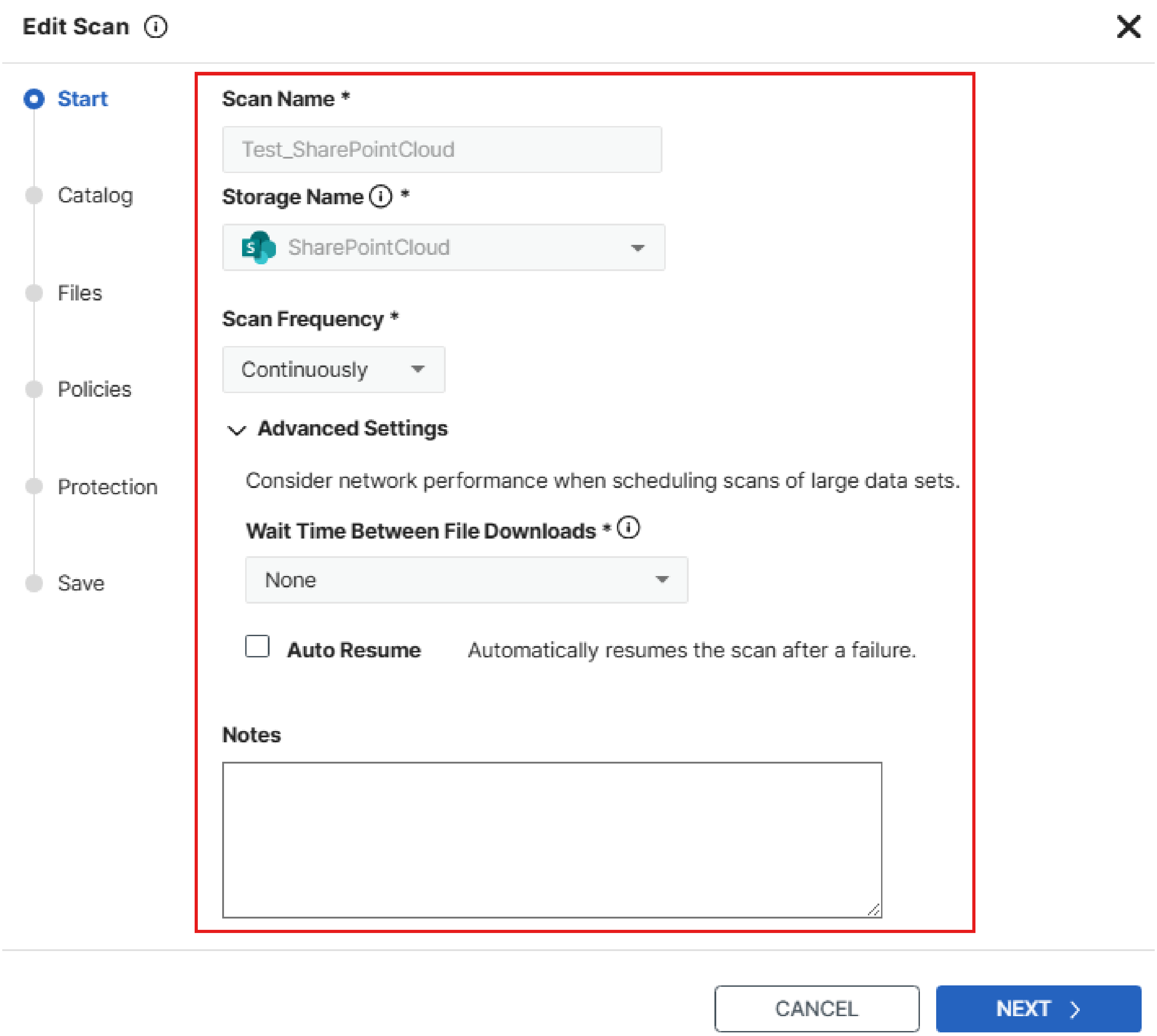
1. In the *Discovery* > *Scans* page, click *Add Scan*.



[redacted]

	Scan Name	Storage	System Status	Scan Status	Scan Frequency	Previous Scans	Started At	Ended At	Duration	Wait Time	Notes
⋮	[redacted]	SharePointCloud	⃠ Suspended	Failed ↻ Retry	Continuously	2400	2025, [redacted]	[redacted]	00:00:08	None	

2. Configure the scan storage and schedule by specifying the following options:



Edit Scan ⓘ

Scan Name *

Test_SharePointCloud

Storage Name ⓘ *

SharePointCloud

Scan Frequency *

Continuously

Advanced Settings

Consider network performance when scheduling scans of large data sets.

Wait Time Between File Downloads * ⓘ

None

□ Auto Resume Automatically resumes the scan after a failure.

Notes

a. Specify the scan name.

b. Select a storage (defined in Storages on page 10) to scan. The following storage types are supported:

- *AWS Bucket*
- *SharePoint Cloud*
- *SharePoint On Prem*
- *SMB*—Samba
- *Google Drive*

- Only active storages are listed. To activate an inactive storage, go to Storages on page 10, click the options icon in front of the storage name, and click *Activate*.
- A storage can be used by only one scan. You cannot select a storage that has been referenced in another scan already.

c. Configure the scan frequency to be daily, weekly, or continuously. For daily and weekly scans, you can specify the hour or day when the scan is scheduled to run.

d. Under *Advanced Settings*, select one of the following for *Wait Time Between File Downloads*:
   - *Short*—10 ms
   - *Long*—20 ms
   - *None*—0 ms

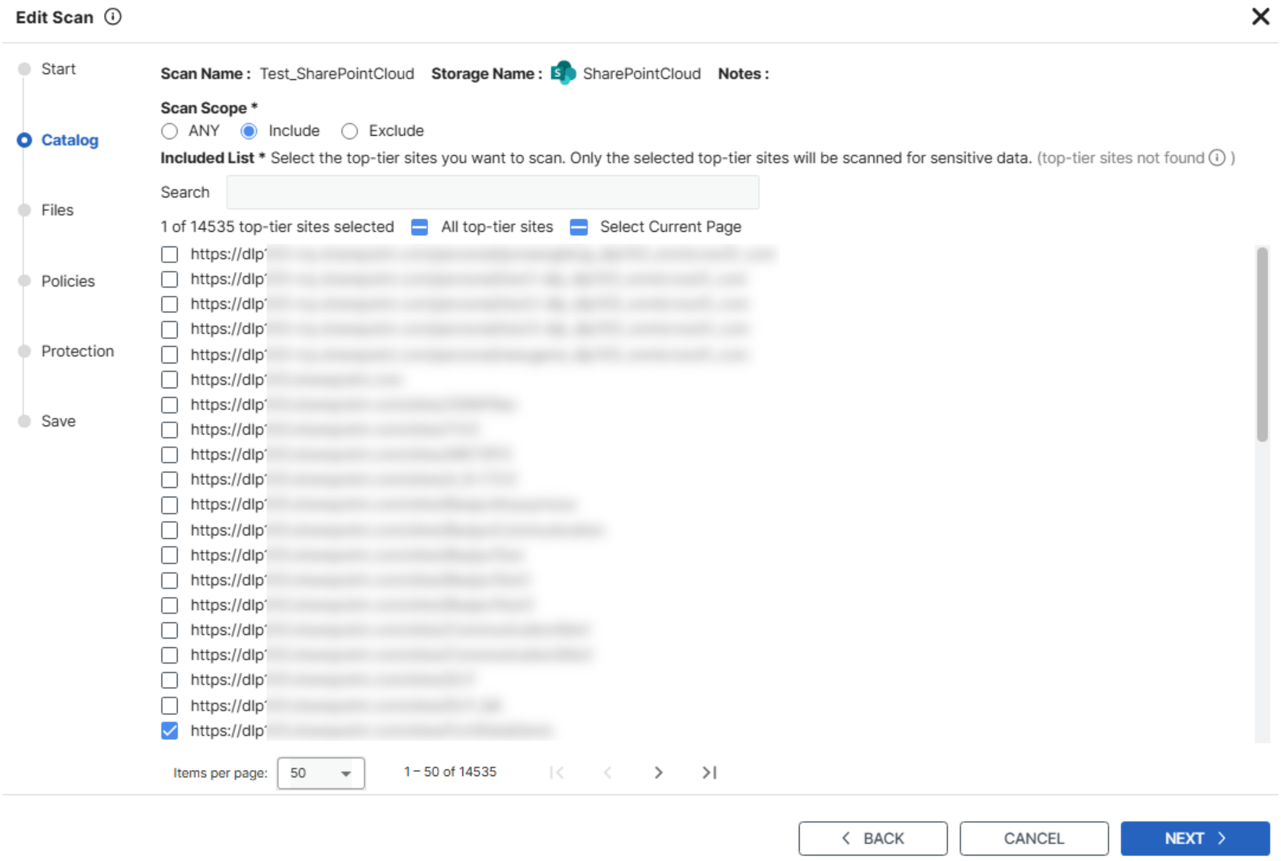
The wait time will affect the speed of the scan and the traffic load on your network. A shorter wait time will result in faster scans but may increase network traffic load. The first run of a scan will be relatively slow as every file is downloaded for processing. Subsequent runs of that scan will likely be much faster because only files changed since the last scan will be processed. Downloaded file copies are deleted after scanning.

e. Optionally, enable *Auto Resume* to automatically resume the scan after a failure.

f. Add notes as needed.

g. Click *NEXT*.

3. Configure the scan scope and click *NEXT*.



Edit Scan ⓘ ✕

Scan Name : Test_SharePointCloud **Storage Name :** SharePointCloud **Notes :**

Scan Scope *

○ ANY ● Include ○ Exclude

Included List * Select the top-tier sites you want to scan. Only the selected top-tier sites will be scanned for sensitive data. (top-tier sites not found ⓘ)

Search

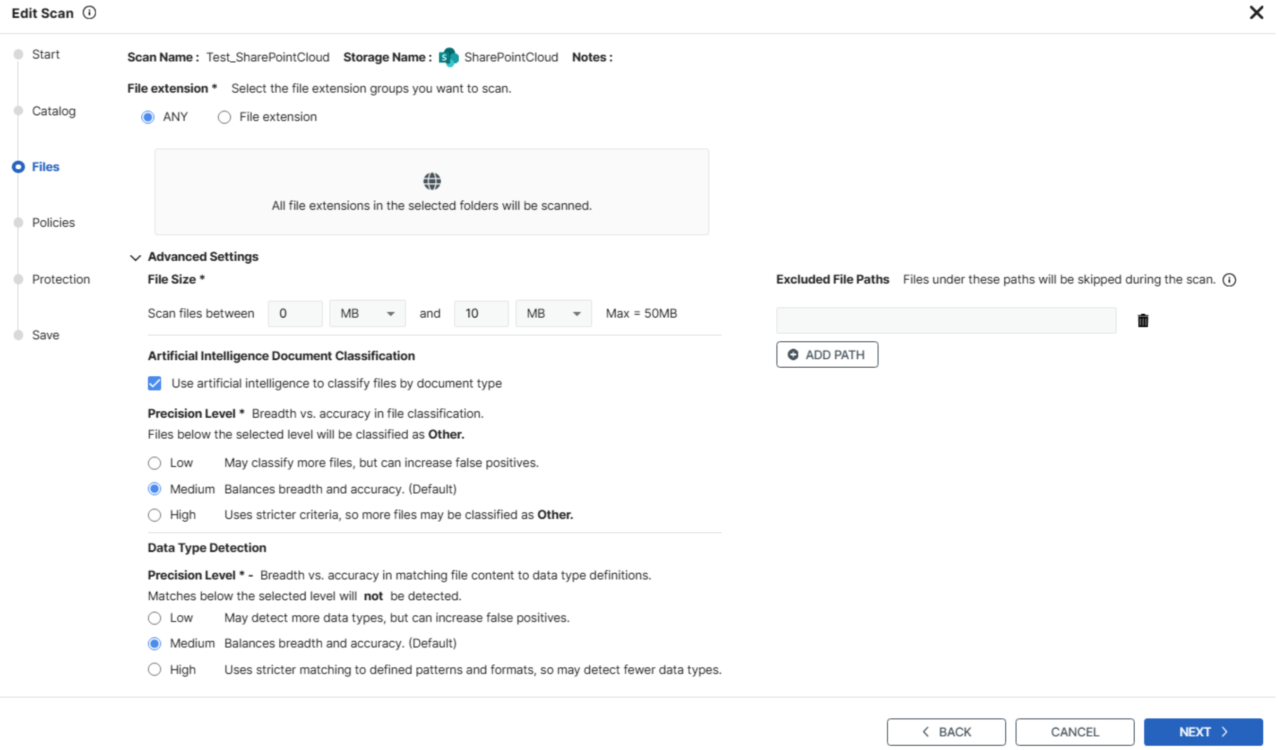
1 of 14535 top-tier sites selected ▬ All top-tier sites ▬ Select Current Page

☐ https://dlp[redacted]
☐ https://dlp[redacted]
☐ https://dlp[redacted]
☐ https://dlp[redacted]
☐ https://dlp[redacted]
☐ https://dlp[redacted]
☐ https://dlp[redacted]
☐ https://dlp[redacted]
☐ https://dlp[redacted]
☐ https://dlp[redacted]
☐ https://dlp[redacted]
☐ https://dlp[redacted]
☐ https://dlp[redacted]
☐ https://dlp[redacted]
☐ https://dlp[redacted]
☐ https://dlp[redacted]
☐ https://dlp[redacted]
☐ https://dlp[redacted]
☐ https://dlp[redacted]
☑ https://dlp[redacted]

Items per page: 50 1 – 50 of 14535

4. Configure the file types to scan, including file extensions, file size, machine learning document classification, and precision level.

The precision level determines the threshold confidence level for ML file classification and data type detection. For example, if you select *High* in *Precision Level* under *Data Type Detection*, only data types with a confidence level of high (as predefined in FortiData) will be detected and displayed.



Edit Scan ⓘ

Scan Name : Test_SharePointCloud **Storage Name :** SharePointCloud **Notes :**

File extension * Select the file extension groups you want to scan.

● ANY ○ File extension

All file extensions in the selected folders will be scanned.

Advanced Settings

File Size *

Scan files between 0 MB and 10 MB Max = 50MB

Excluded File Paths Files under these paths will be skipped during the scan. ⓘ

Artificial Intelligence Document Classification

☑ Use artificial intelligence to classify files by document type

Precision Level * Breadth vs. accuracy in file classification.
Files below the selected level will be classified as **Other.**

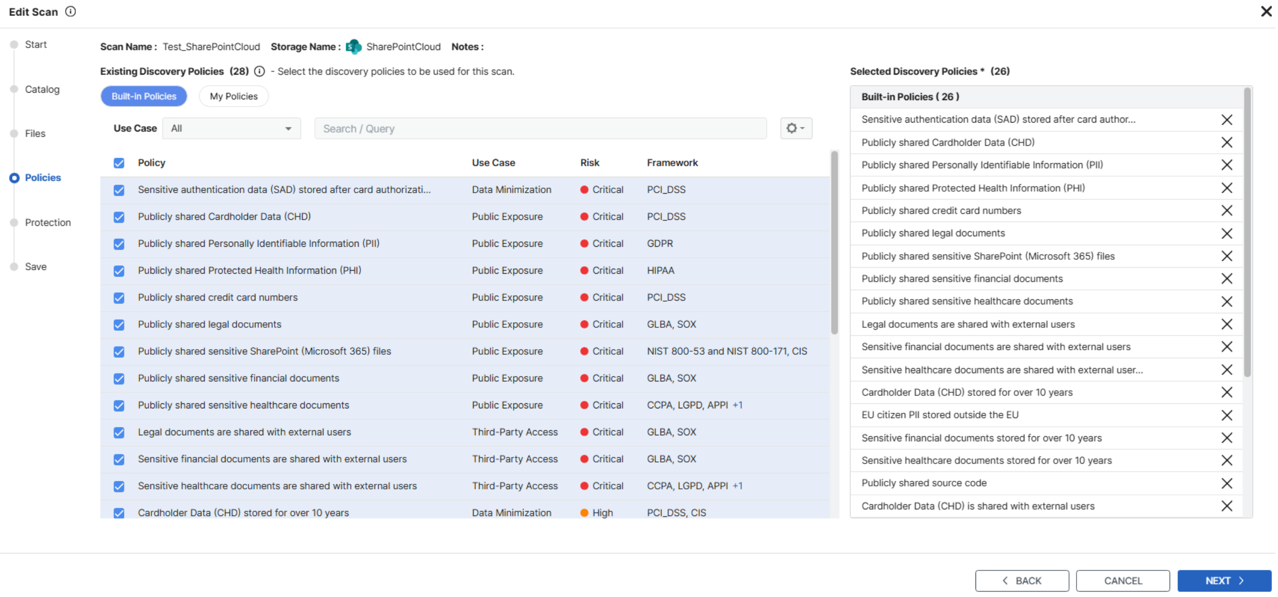
○ Low May classify more files, but can increase false positives.
● Medium Balances breadth and accuracy. (Default)
○ High Uses stricter criteria, so more files may be classified as **Other.**

Data Type Detection

Precision Level * - Breadth vs. accuracy in matching file content to data type definitions.
Matches below the selected level will **not** be detected.

○ Low May detect more data types, but can increase false positives.
● Medium Balances breadth and accuracy. (Default)
○ High Uses stricter matching to defined patterns and formats, so may detect fewer data types.

5. Click *NEXT*.
6. Select the discovery policies (see Policies on page 27) to apply to the scan and click *NEXT*.



Edit Scan ⓘ

Scan Name : Test_SharePointCloud **Storage Name :** SharePointCloud **Notes :**

Existing Discovery Policies (28) ⓘ - Select the discovery policies to be used for this scan.

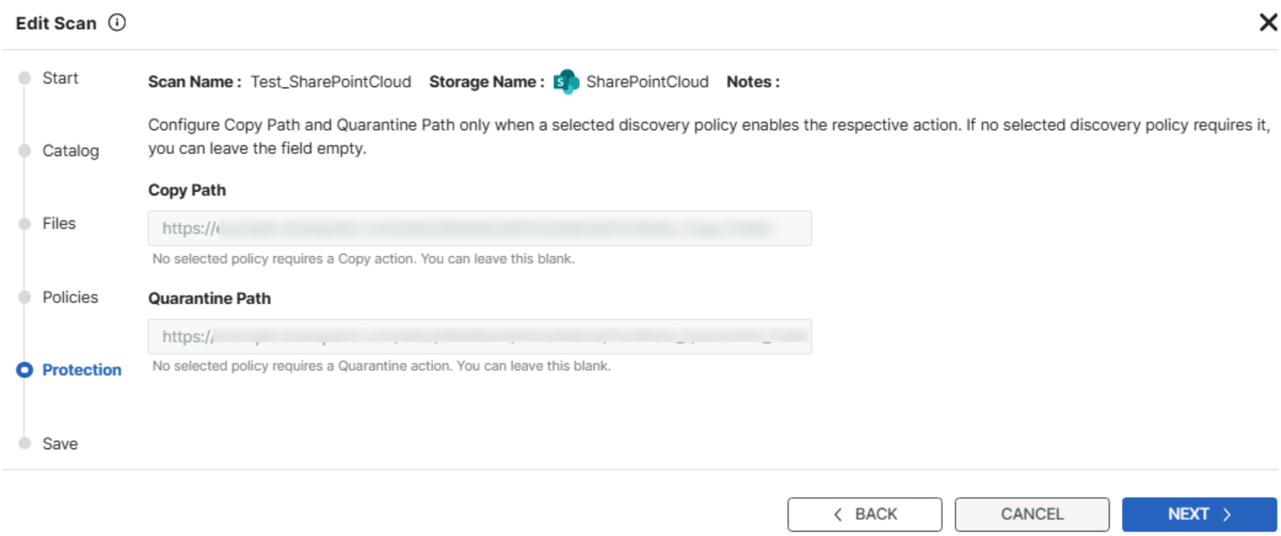
Use Case All Search / Query

☑	Policy	Use Case	Risk	Framework
☑	Sensitive authentication data (SAD) stored after card authorizati...	Data Minimization	● Critical	PCI_DSS
☑	Publicly shared Cardholder Data (CHD)	Public Exposure	● Critical	PCI_DSS
☑	Publicly shared Personally Identifiable Information (PII)	Public Exposure	● Critical	GDPR
☑	Publicly shared Protected Health Information (PHI)	Public Exposure	● Critical	HIPAA
☑	Publicly shared credit card numbers	Public Exposure	● Critical	PCI_DSS
☑	Publicly shared legal documents	Public Exposure	● Critical	GLBA, SOX
☑	Publicly shared sensitive SharePoint (Microsoft 365) files	Public Exposure	● Critical	NIST 800-53 and NIST 800-171, CIS
☑	Publicly shared sensitive financial documents	Public Exposure	● Critical	GLBA, SOX
☑	Publicly shared sensitive healthcare documents	Public Exposure	● Critical	CCPA, LGPD, APPI +1
☑	Legal documents are shared with external users	Third-Party Access	● Critical	GLBA, SOX
☑	Sensitive financial documents are shared with external users	Third-Party Access	● Critical	GLBA, SOX
☑	Sensitive healthcare documents are shared with external users	Third-Party Access	● Critical	CCPA, LGPD, APPI +1
☑	Cardholder Data (CHD) stored for over 10 years	Data Minimization	● High	PCI_DSS, CIS

Selected Discovery Policies * (26)

Built-in Policies (26)	
Sensitive authentication data (SAD) stored after card author...	✕
Publicly shared Cardholder Data (CHD)	✕
Publicly shared Personally Identifiable Information (PII)	✕
Publicly shared Protected Health Information (PHI)	✕
Publicly shared credit card numbers	✕
Publicly shared legal documents	✕
Publicly shared sensitive SharePoint (Microsoft 365) files	✕
Publicly shared sensitive financial documents	✕
Publicly shared sensitive healthcare documents	✕
Legal documents are shared with external users	✕
Sensitive financial documents are shared with external users	✕
Sensitive healthcare documents are shared with external user...	✕
Cardholder Data (CHD) stored for over 10 years	✕
EU citizen PII stored outside the EU	✕
Sensitive financial documents stored for over 10 years	✕
Sensitive healthcare documents stored for over 10 years	✕
Publicly shared source code	✕
Cardholder Data (CHD) is shared with external users	✕

7. If any of the selected policies require copying or quarantining sensitive files for further investigation, specify the directory to copy or move sensitive files to.



Edit Scan

Scan Name : Test_SharePointCloud Storage Name : SharePointCloud Notes :

Configure Copy Path and Quarantine Path only when a selected discovery policy enables the respective action. If no selected discovery policy requires it, you can leave the field empty.

Copy Path

https://[redacted]

No selected policy requires a Copy action. You can leave this blank.

Quarantine Path

https://[redacted]

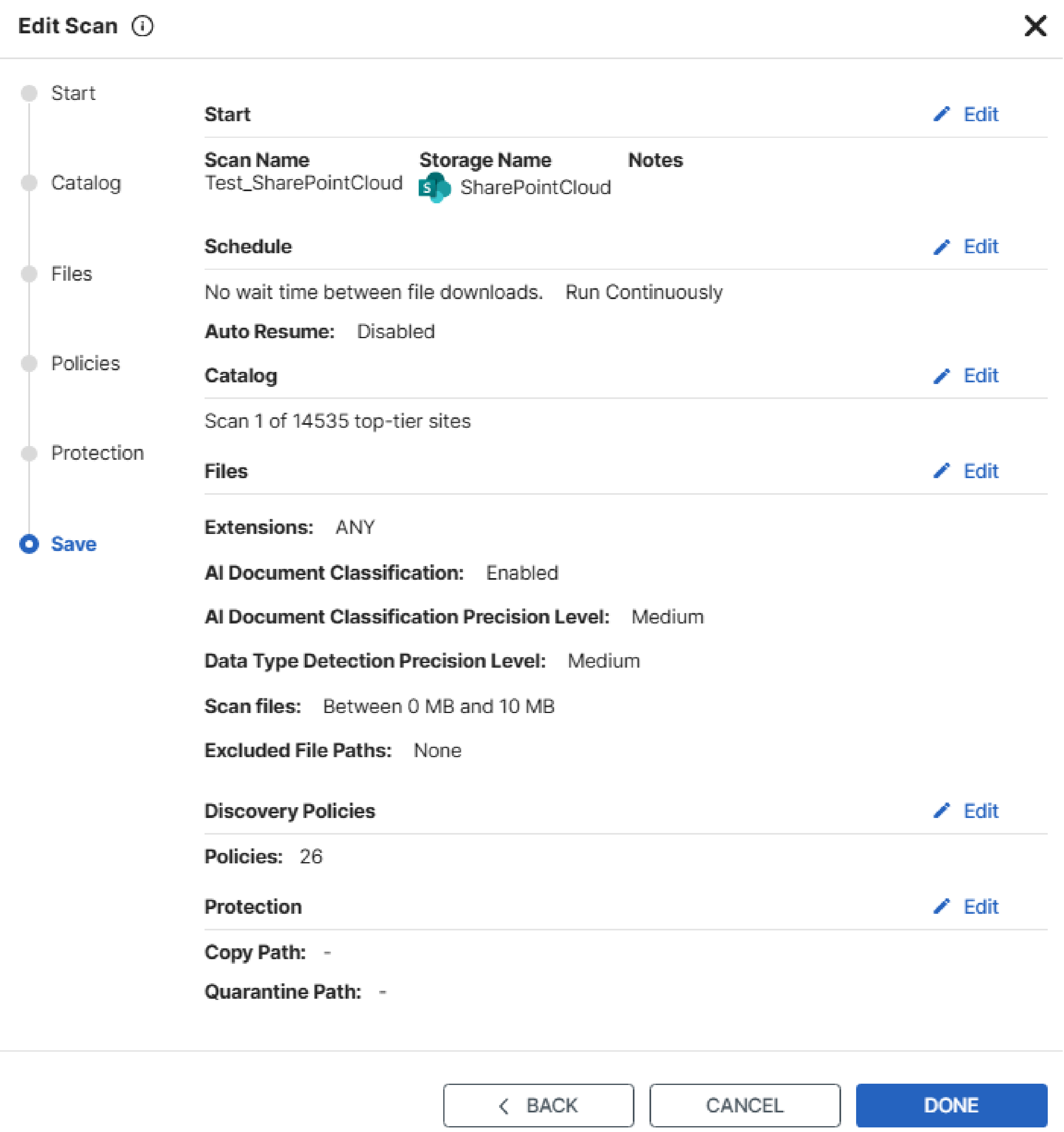
No selected policy requires a Quarantine action. You can leave this blank.

Before quarantining a sensitive file for further investigation, FortiData creates a placeholder TXT file notifying you that the original file violated compliance policies and has been quarantined. A CSV metadata file is also generated to record information about the original file before it is quarantined.

To ensure successful copy and quarantine operations, you must have the following permissions:

- **Copy**—Read/write permission of the destination folder
- **Quarantine**—Read/write permission of both the original files and destination folder

8. Review the details for the scan, edit any details as needed, and click *DONE*.



Edit Scan ⓘ ✕

Start ✎ Edit

Scan Name	Storage Name	Notes
Test_SharePointCloud	SharePointCloud	

Schedule ✎ Edit

No wait time between file downloads. Run Continuously

Auto Resume: Disabled

Catalog ✎ Edit

Scan 1 of 14535 top-tier sites

Files ✎ Edit

Extensions: ANY

AI Document Classification: Enabled

AI Document Classification Precision Level: Medium

Data Type Detection Precision Level: Medium

Scan files: Between 0 MB and 10 MB

Excluded File Paths: None

Discovery Policies ✎ Edit

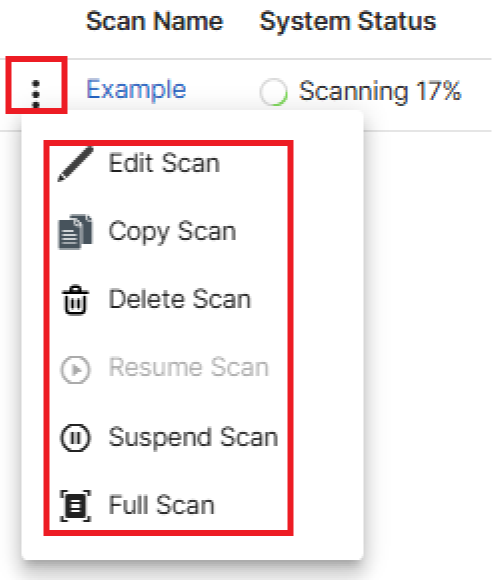
Policies: 26

Protection ✎ Edit

Copy Path: -

Quarantine Path: -

The scan is now configured to look for specific data in the target directory on the defined schedule, assign labels to files matching the conditions, and copy or quarantine sensitive files as needed. You can perform the following operations on the scan by clicking the three dots at the beginning of the scan row and selecting an option from the list. To view scan results, go to *Analytics on page 16*.



	Scan Name	System Status
⋮	Example	○ Scanning 17%

- A full scan re-scans all files and deletes all existing scan results.
- After editing a scan, you can choose to re-run the scan after saving the configurations, in which case a full scan will be performed and all existing scan results will be deleted.

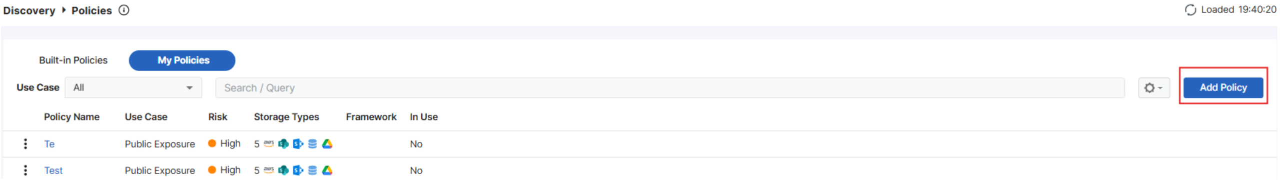
Policies

A policy looks for specific types of data (using Data Classifiers on page 37) in files and assigns specific labels to files that meet the specified context conditions. You can also configure the policy to copy or quarantine matching files to a specific directory for further investigation.

The *Discovery > Policies* page lists built-in policies and custom policies that you created. You can filter the policies by use case and queries with various conditions. To customize the columns to display in the table, use the *Configure* button on the top-right.

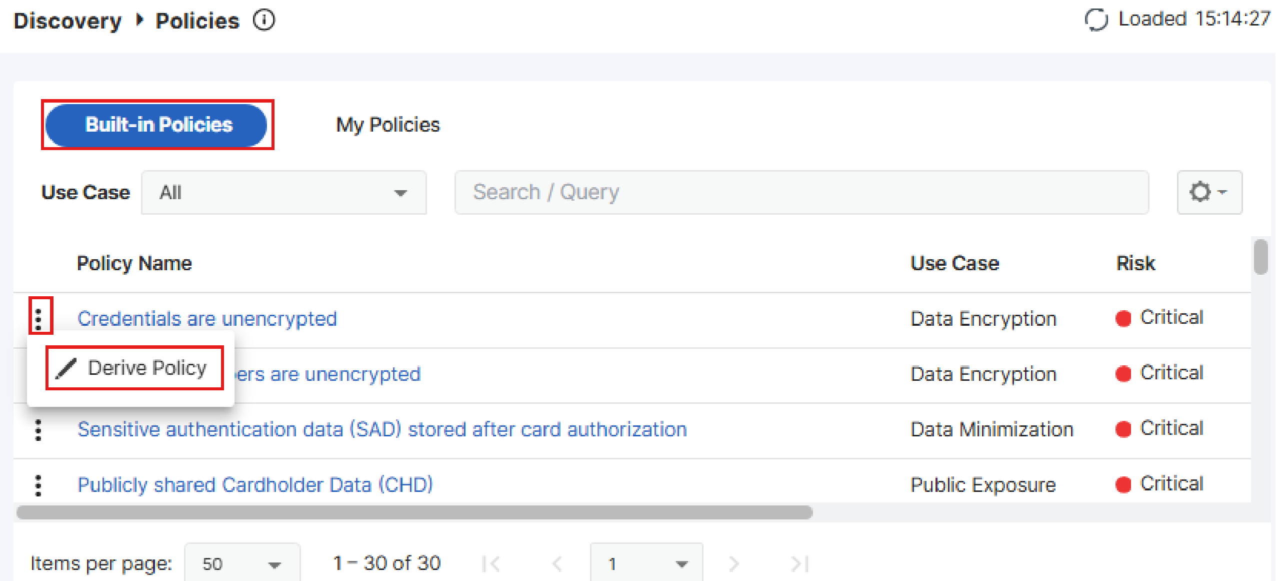
To create a policy:

1. Go to *Discovery > Policies > My Policies*.
2. To create a policy from scratch, click *Add Policy*.



	Policy Name	Use Case	Risk	Storage Types	Framework	In Use
⋮	Te	Public Exposure	● High	5		No
⋮	Test	Public Exposure	● High	5		No

To build from an existing policy, click the eclipsis in front of the policy name and select *Derive Policy* (for built-in policies) or *Copy Policy* (for custom policies).



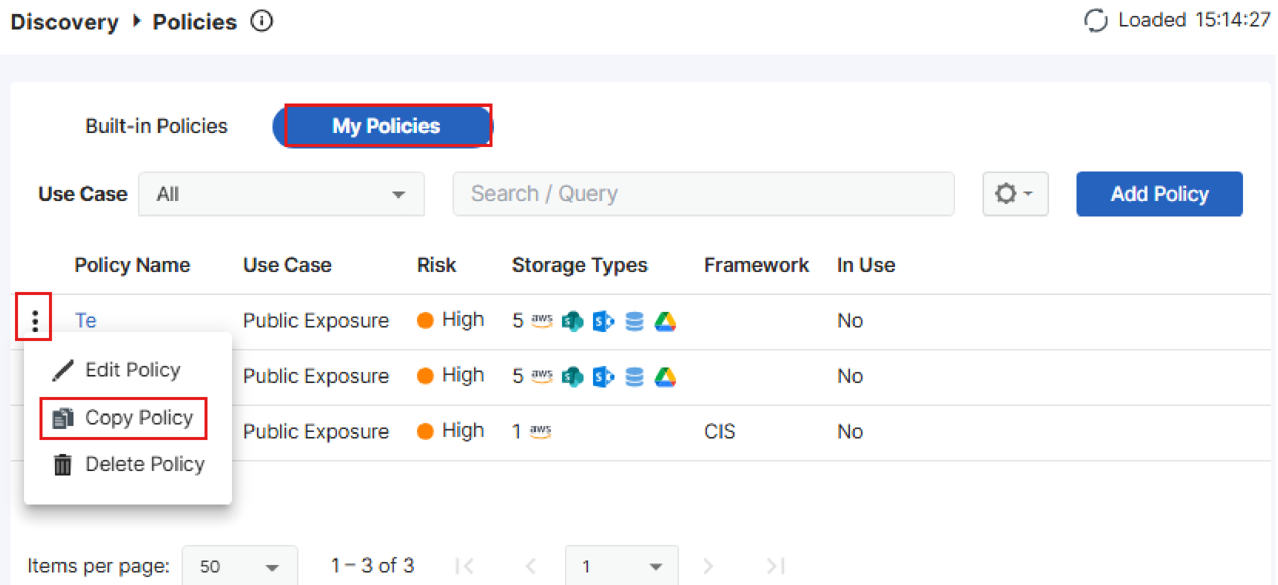
Discovery ▸ Policies ⓘ Loaded 15:14:27

Built-in Policies | My Policies

Use Case: All | Search / Query

	Policy Name	Use Case	Risk
⋮	Credentials are unencrypted	Data Encryption	● Critical
Derive Policy	…ers are unencrypted	Data Encryption	● Critical
⋮	Sensitive authentication data (SAD) stored after card authorization	Data Minimization	● Critical
⋮	Publicly shared Cardholder Data (CHD)	Public Exposure	● Critical

Items per page: 50 1 – 30 of 30 1



Discovery ▸ Policies ⓘ Loaded 15:14:27

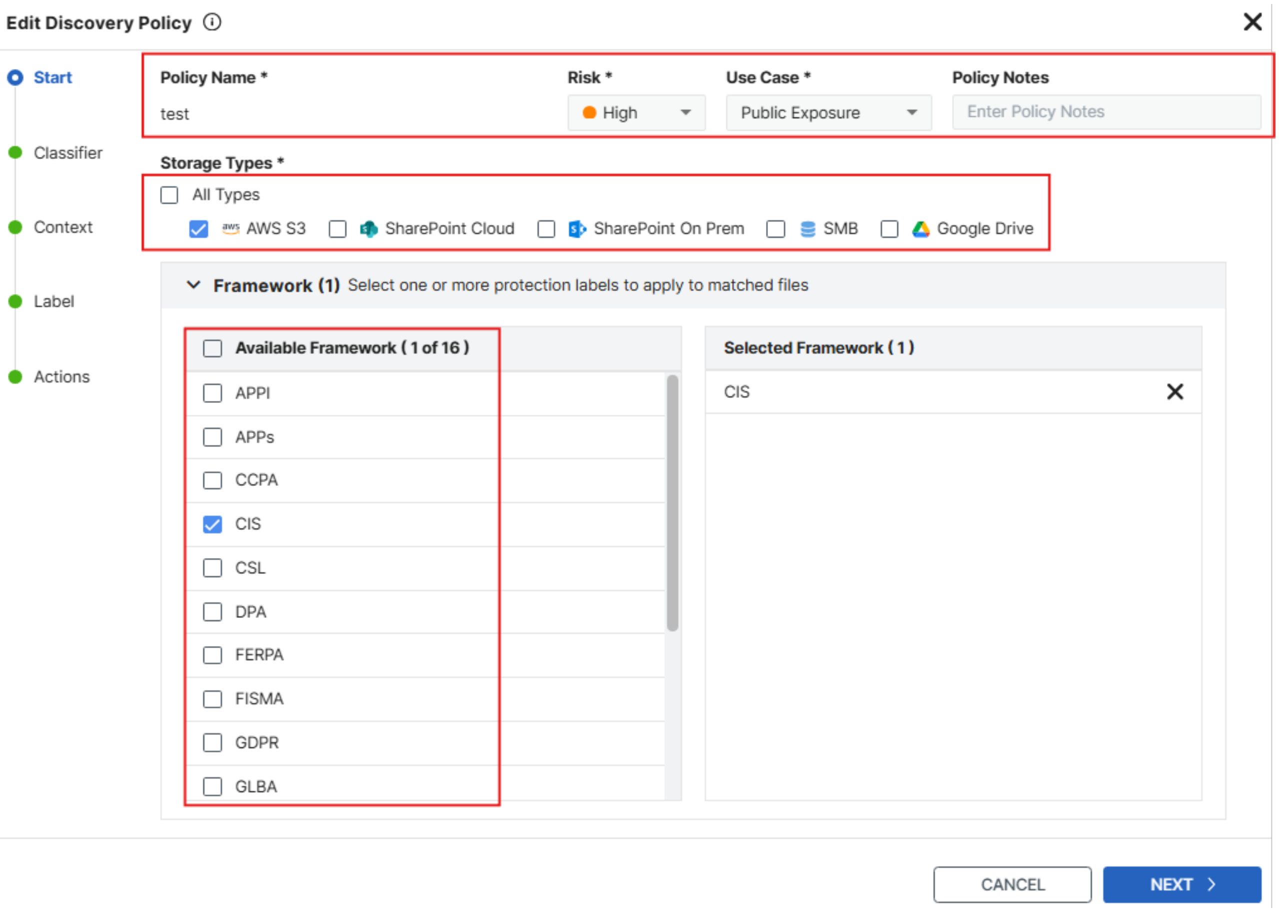
Built-in Policies | My Policies

Use Case: All | Search / Query | Add Policy

	Policy Name	Use Case	Risk	Storage Types	Framework	In Use
⋮	Te	Public Exposure	● High	5		No
Edit Policy		Public Exposure	● High	5		No
Copy Policy		Public Exposure	● High	1	CIS	No
Delete Policy						

Items per page: 50 1 – 3 of 3 1

3. Specify the policy name, risk, use case, and add any notes.



Edit Discovery Policy ⓘ

- Start
- Classifier
- Context
- Label
- Actions

Policy Name *	Risk *	Use Case *	Policy Notes
test	● High	Public Exposure	Enter Policy Notes

Storage Types *

□ All Types

☑ AWS S3 □ SharePoint Cloud □ SharePoint On Prem □ SMB □ Google Drive

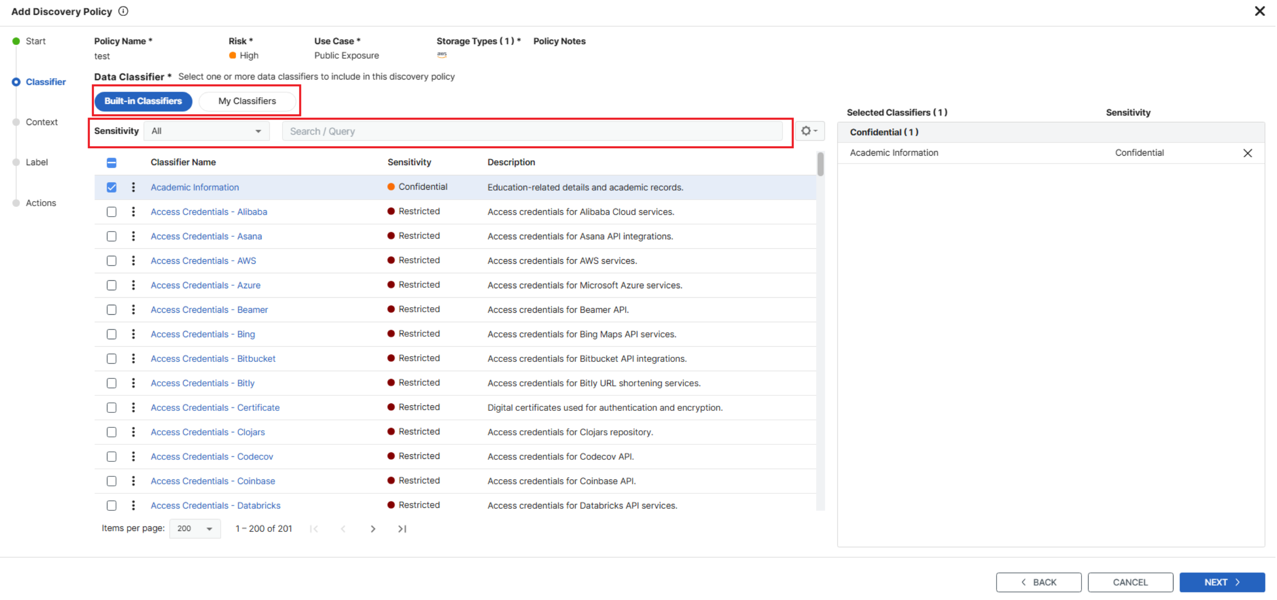
Framework (1) Select one or more protection labels to apply to matched files

□ Available Framework (1 of 16)
□ APPI
□ APPs
□ CCPA
☑ CIS
□ CSL
□ DPA
□ FERPA
□ FISMA
□ GDPR
□ GLBA

Selected Framework (1)
CIS ✕

4. Select the storage type(s) and frameworks (which can be used for assigning labels to matching files in later steps). Click *NEXT*.

5. Select one or more Data Classifiers on page 37 to include in the policy. You can choose built-in classifiers (predefined in FortiData) or custom classifiers based on your needs. Use the *Sensitivity* filter and *Search/Query* box to filter the results.



Add Discovery Policy ⓘ

- Start
- Classifier
- Context
- Label
- Actions

Policy Name *	Risk *	Use Case *	Storage Types (1) *	Policy Notes
test	● High	Public Exposure	aws	

Data Classifier * Select one or more data classifiers to include in this discovery policy

Sensitivity: All

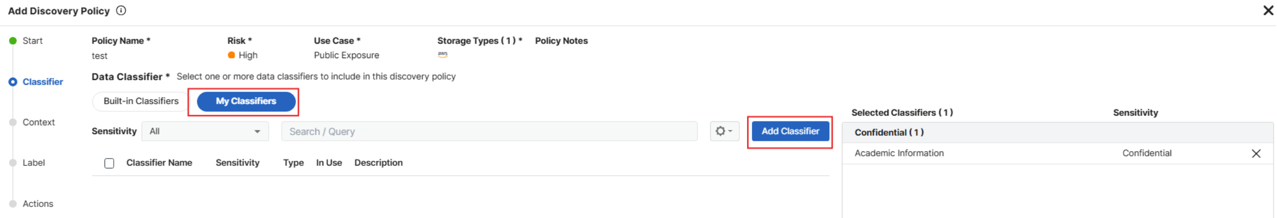
Search / Query

☐	Classifier Name	Sensitivity	Description
☑	Academic Information	● Confidential	Education-related details and academic records.
□	Access Credentials - Alibaba	● Restricted	Access credentials for Alibaba Cloud services.
□	Access Credentials - Asana	● Restricted	Access credentials for Asana API integrations.
□	Access Credentials - AWS	● Restricted	Access credentials for AWS services.
□	Access Credentials - Azure	● Restricted	Access credentials for Microsoft Azure services.
□	Access Credentials - Beamer	● Restricted	Access credentials for Beamer API.
□	Access Credentials - Bing	● Restricted	Access credentials for Bing Maps API services.
□	Access Credentials - Bitbucket	● Restricted	Access credentials for Bitbucket API integrations.
□	Access Credentials - Bitly	● Restricted	Access credentials for Bitly URL shortening services.
□	Access Credentials - Certificate	● Restricted	Digital certificates used for authentication and encryption.
□	Access Credentials - Clojars	● Restricted	Access credentials for Clojars repository.
□	Access Credentials - Codecov	● Restricted	Access credentials for Codecov API.
□	Access Credentials - Coinbase	● Restricted	Access credentials for Coinbase API.
□	Access Credentials - Databricks	● Restricted	Access credentials for Databricks API services.

Items per page: 200 1 – 200 of 201

Selected Classifiers (1)	Sensitivity	
Confidential (1)		
Academic Information	Confidential	✕

You can also create a new custom classifier by clicking *Add Classifier* in the *My Classifiers* tab. See Data Classifiers on page 37.



Add Discovery Policy

Policy Name *: test
Risk *: High
Use Case *: Public Exposure
Storage Types (1) *
Policy Notes

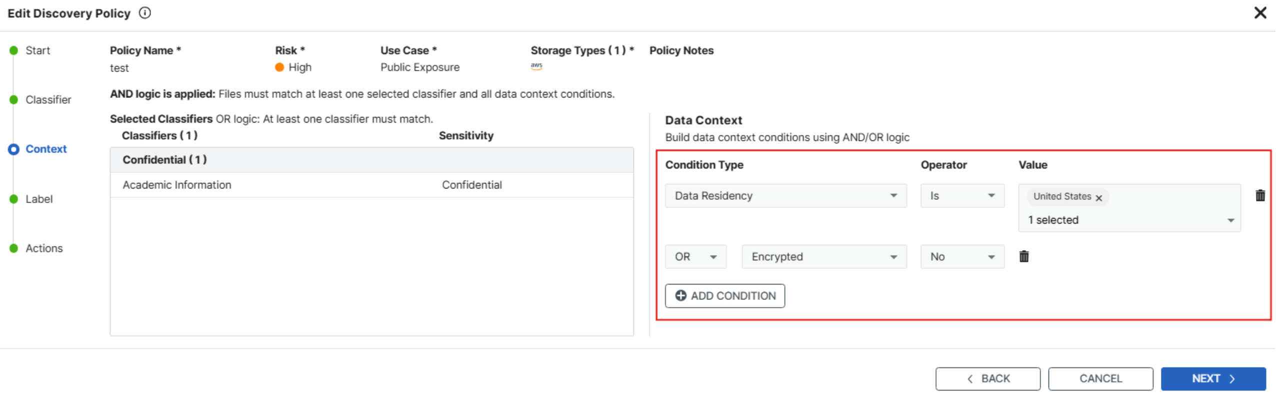
Data Classifier * Select one or more data classifiers to include in this discovery policy

Sensitivity: All

☐	Classifier Name	Sensitivity	Type	In Use	Description

Selected Classifiers (1)	Sensitivity
Confidential (1)	
Academic Information	Confidential

6. Click *NEXT*.
7. Add data context conditions using AND/OR logic and click *NEXT*.



Edit Discovery Policy

Policy Name *: test
Risk *: High
Use Case *: Public Exposure
Storage Types (1) *
Policy Notes

AND logic is applied: Files must match at least one selected classifier and all data context conditions.

Selected Classifiers OR logic: At least one classifier must match.

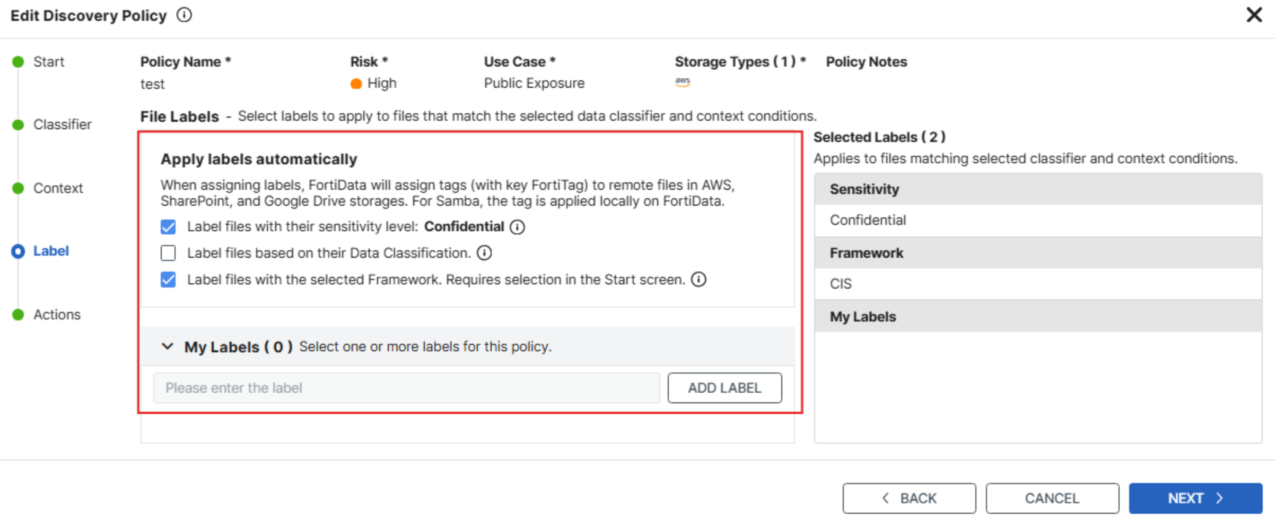
Classifiers (1)	Sensitivity
Confidential (1)	
Academic Information	Confidential

Data Context
Build data context conditions using AND/OR logic

	Condition Type	Operator	Value
	Data Residency	Is	United States 1 selected
OR	Encrypted	No	

8. Select the labels (markers for sensitive information) to apply to files that match the selected data classifier and context conditions. Click *NEXT*.

   You can choose to allow FortiData to apply labels to files automatically using the sensitivity level (defined in the matching data classifier), data classification (performed by AI engine, see FortiGuard on page 58), or selected framework (that you defined in step 4). You can also add custom labels under *My Labels* by entering the label in the text box and clicking *ADD LABEL*.



Edit Discovery Policy

Policy Name *: test
Risk *: High
Use Case *: Public Exposure
Storage Types (1) *
Policy Notes

File Labels - Select labels to apply to files that match the selected data classifier and context conditions.

Apply labels automatically

When assigning labels, FortiData will assign tags (with key FortiTag) to remote files in AWS, SharePoint, and Google Drive storages. For Samba, the tag is applied locally on FortiData.

☑ Label files with their sensitivity level: **Confidential**
☐ Label files based on their Data Classification.
☑ Label files with the selected Framework. Requires selection in the Start screen.

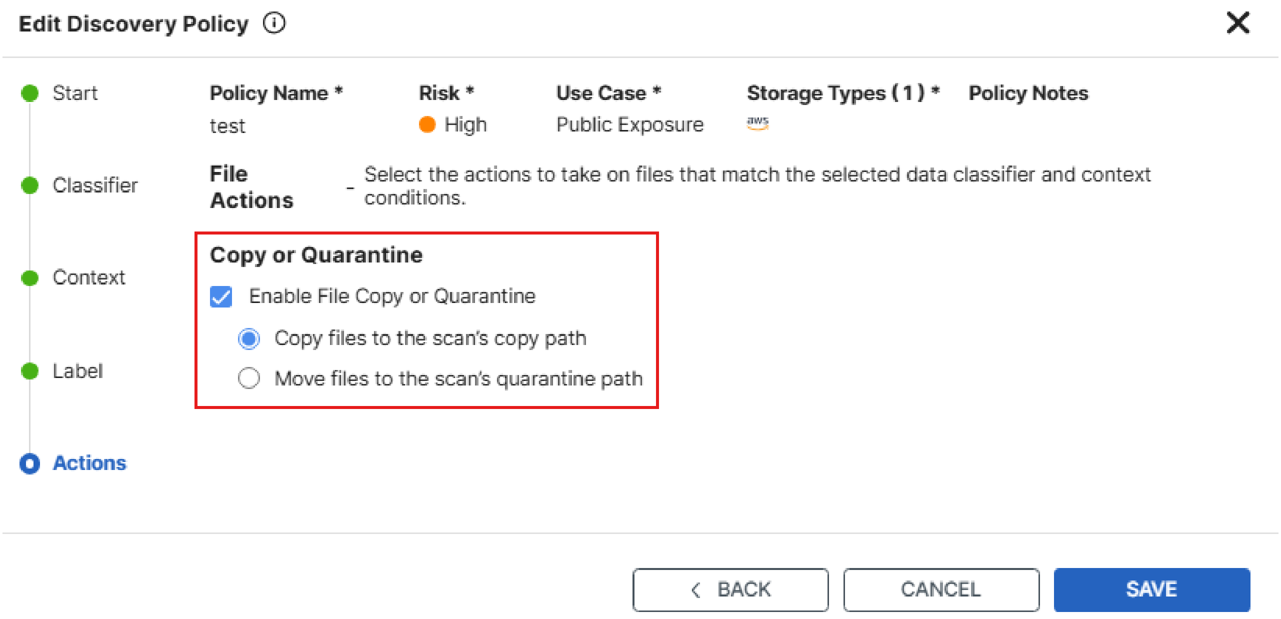
My Labels (0) Select one or more labels for this policy.

Please enter the label

Selected Labels (2)
Applies to files matching selected classifier and context conditions.

Sensitivity
Confidential
Framework
CIS
My Labels

9. Optionally, select *Enable File Copy or Quarantine* to allow copying or quarantining sensitive files to the directory defined in Scans on page 21. Click *SAVE*.



Edit Discovery Policy ⓘ ✕

- Start
- Classifier
- Context
- Label
- **Actions**

Policy Name *	Risk *	Use Case *	Storage Types (1) *	Policy Notes
test	● High	Public Exposure	aws	

File Actions - Select the actions to take on files that match the selected data classifier and context conditions.

Copy or Quarantine

☑ Enable File Copy or Quarantine

● Copy files to the scan's copy path

○ Move files to the scan's quarantine path

Content Insight

The *Content Insight* menu allows you to configure data types and fingerprinting (IDM and EDM) for data classification. You can then configure data classifiers (using data types and fingerprinting) for file matching and labeling.

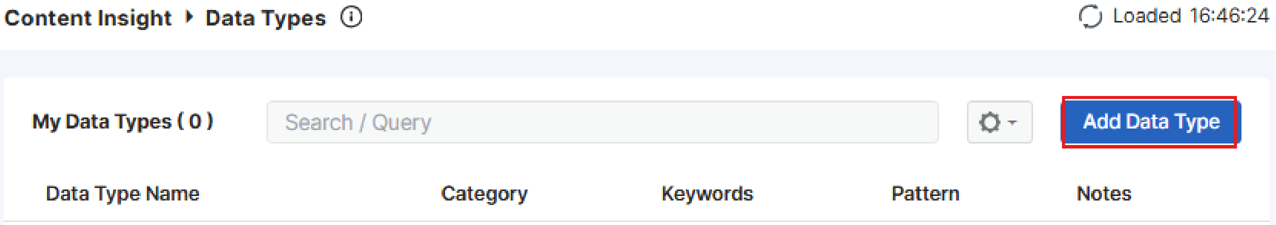
- Data Types on page 32
- Data Fingerprinting on page 34
- Data Classifiers on page 37

Data Types

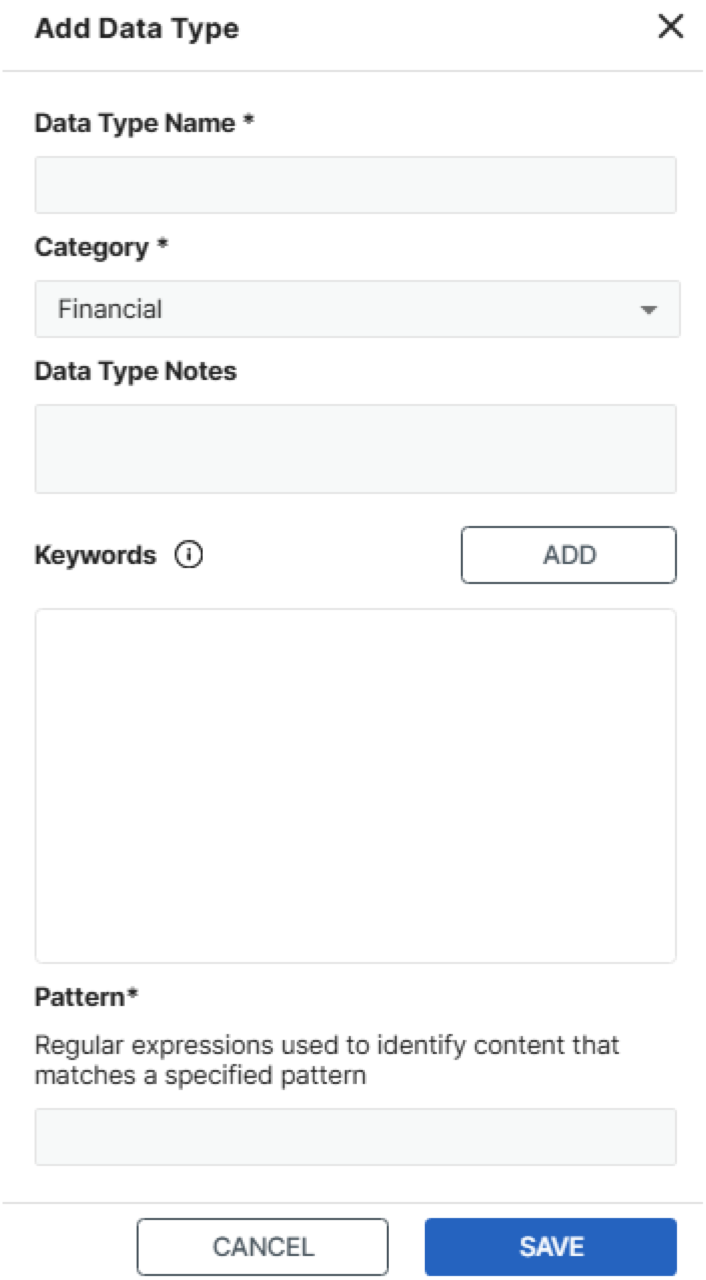
In a DLP system, data types are categories of sensitive information that the system can detect and protect. Common data types include PII (Personally Identifiable Information), PHI (Protected Health Information), and PCI (Payment Card Information). The *Content Insight > Data Types* page displays a list of data types (of different categories) that you defined, which can then be referenced when you create Data Classifiers on page 37.. You can search the custom data type groups by various dimensions.

To define a data type:

1. In the *Content Insight > Data Types* page, click *Add Data Type*.



2. Configure the data type with the following options:



Category * Financial

Regular expressions used to identify content that matches a specified pattern

a. Specify the data type name.

b. Select the category, which can be one of the following:
   - Financial
   - Health
   - Credential
   - Personal
   - Business

c. Add notes as needed.

d. Click *ADD* to define any keywords to look for during file scans. Keyword matching is case-insensitive.

For example, you can configure the keywords `Driver License` and `DLN` to look for files that include `Driver License` or `DLN`. If a file includes any of the keywords, FortiData proceeds to evaluate the file against any regular expressions as defined in the next step.

e. Specify the regular expressions with the content pattern to look for in files that match any of the keywords defined in the previous step.

For example, for files that match the keyword `Driver License` or `DLN`, you can specify the regular expression `[A-Z]\d{7}` that looks for the content pattern of a leading capital letter followed by seven digits. With this definition of the data type, a file that includes a driver license number T16700185 will be considered a match.

f. Add more keywords to the data type by repeating steps d and e.

3. Click *SAVE*.

Data Fingerprinting

You can define data fingerprinting using IDM (Indexed Document Matching) and EDM (exact data match) data types and use them in Data Classifiers on page 37.

IDM

IDM (Indexed Document Matching) is a fast, interpretable, and accurate document matching approach, ideal for recognizing structured documents based on predefined formats or templates. It is especially effective in high-security, compliance-driven environments such as finance, government, and enterprise data protection.

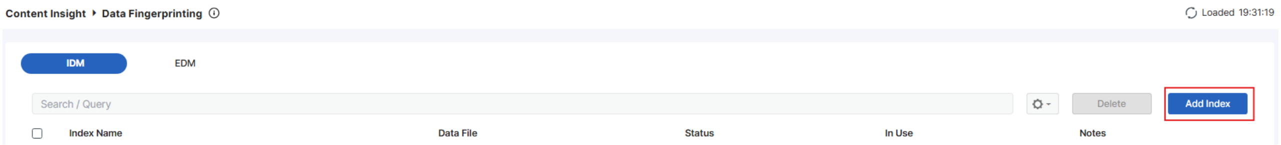
FortiData builds the index by processing uploaded documents, extracting key features such as text content, and storing them as searchable templates for future matching. FortiData then parses the scanned files to extract key structural features, compares them against the indexes of templates using similarity by comparing the text content of files with the IDM data file, and determines a match if the similarity exceeds a predefined threshold (a percentage value from 0 - 100):

Threshold	Similarity Value
High	80 or higher
Medium	70-79
Low	60-69
Note You can also define a custom threshold for the IDM when creating Data Classifiers on page 37.	

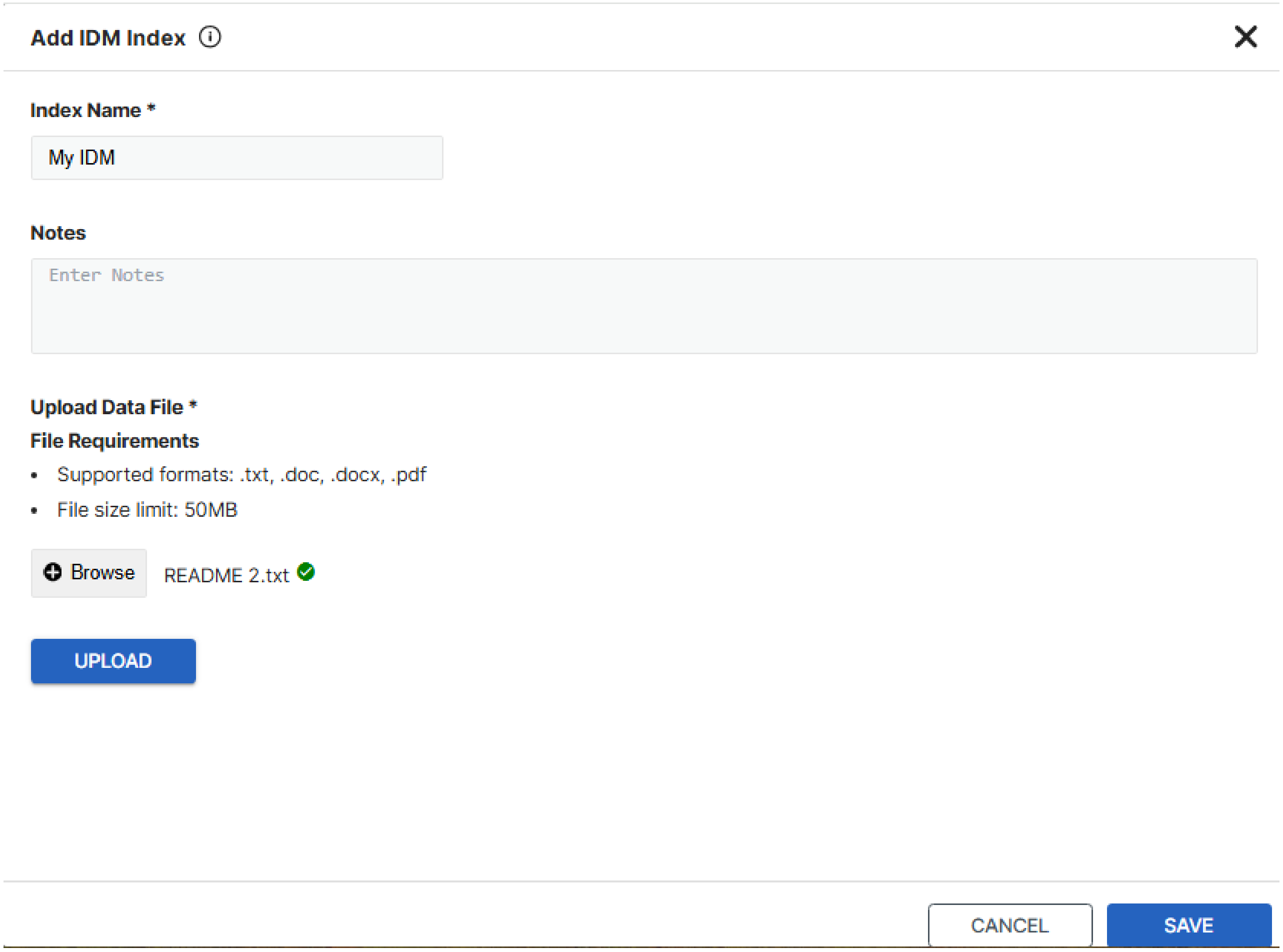
The *IDM* page displays a list of IDM data types that you defined in FortiData. You can search the IDM data type by index name, data file name, and notes.

To create an IDM data type:

1. Go to *Content Insight > Data Fingerprinting > IDM*.
2. Click *Add Index*.



3. Specify the index name and notes (as needed), upload the data file (`.txt`, `.doc`, `.docx`, `.pdf`), and click *SAVE*.



Index Name *

My IDM

Notes

Enter Notes

Upload Data File *

File Requirements

- Supported formats: .txt, .doc, .docx, .pdf
- File size limit: 50MB

README 2.txt ✓

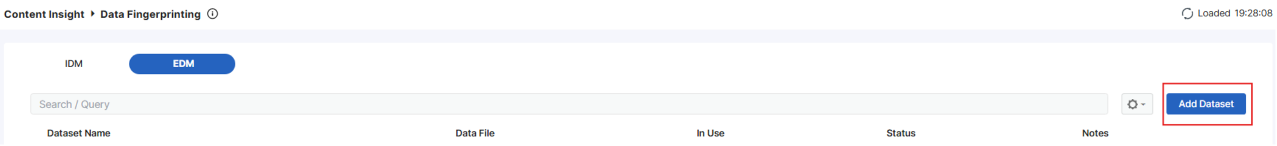
EDM

EDM (exact data match) is a DLP technique that identifies particular data values within an indexed data source that require safeguarding.

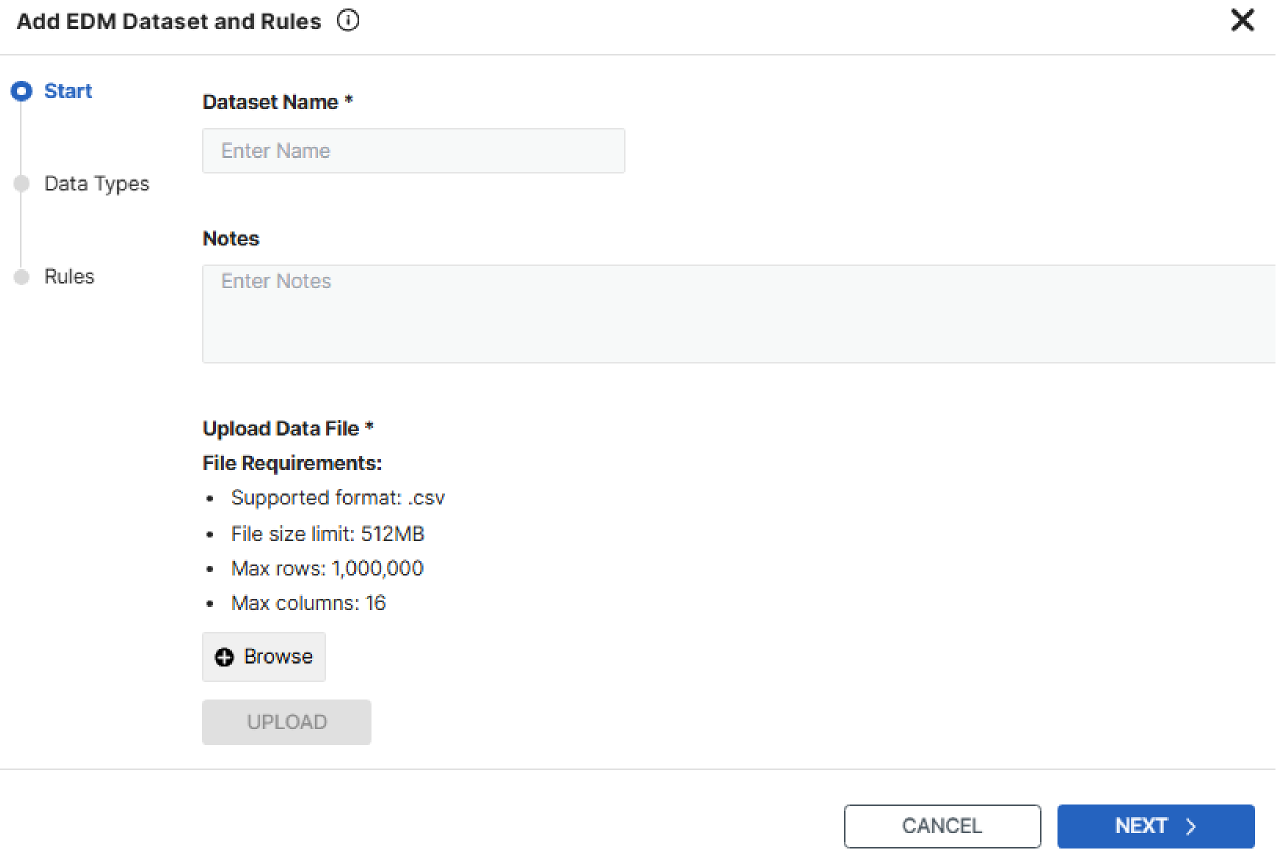
The *EDM* page displays a list of EDM data types that you defined in FortiData. You can search the EDM data type by dataset value, creation or update time, and notes.

To create an EDM data type:

1. Go to *Content Insight > Data Fingerprinting > EDM*.
2. Click *Add Dataset*.



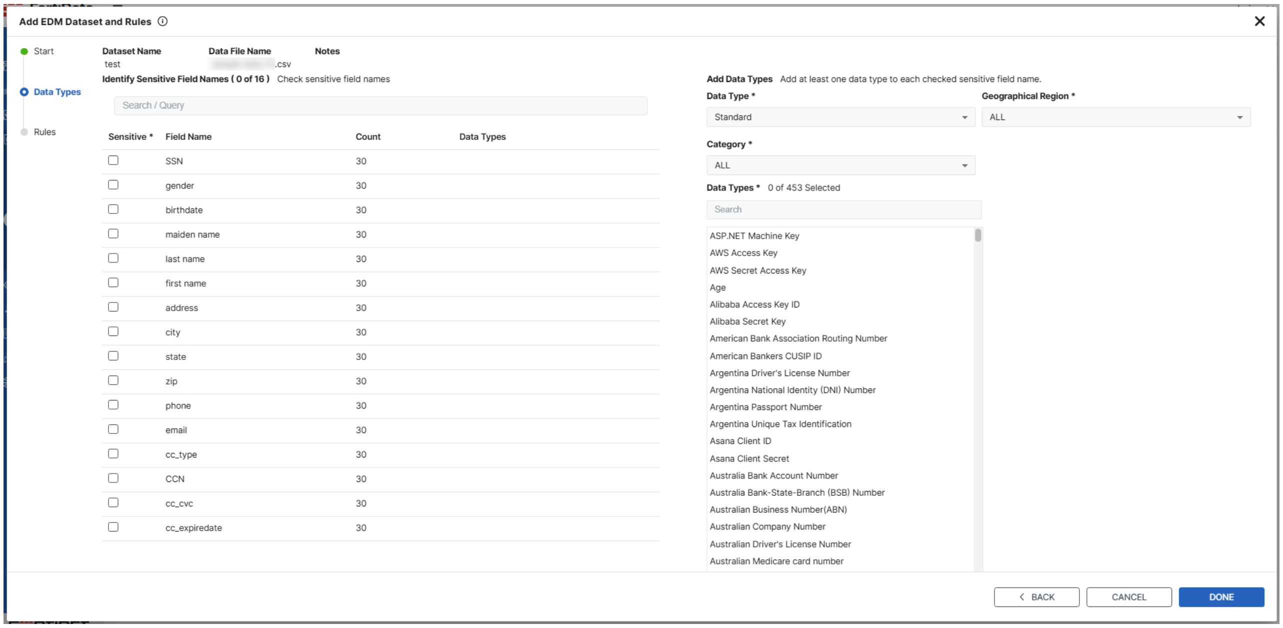
3. Specify the dataset name and notes (as needed), upload the data file (`.csv`), and click *NEXT*.



File Requirements:

- Supported format: .csv
- File size limit: 512MB
- Max rows: 1,000,000
- Max columns: 16

4. Select the sensitive fields to look for and add data types for the fields and click *DONE*.



Add EDM Dataset and Rules ⓘ ✕

- ● Start
- ○ **Data Types**
- ● Rules

Dataset Name: test
Data File Name: [redacted].csv
Notes

Identify Sensitive Field Names (0 of 16) Check sensitive field names

Search / Query

Sensitive *	Field Name	Count	Data Types
□	SSN	30	
□	gender	30	
□	birthdate	30	
□	maiden name	30	
□	last name	30	
□	first name	30	
□	address	30	
□	city	30	
□	state	30	
□	zip	30	
□	phone	30	
□	email	30	
□	cc_type	30	
□	CCN	30	
□	cc_cvc	30	
□	cc_expiredate	30	

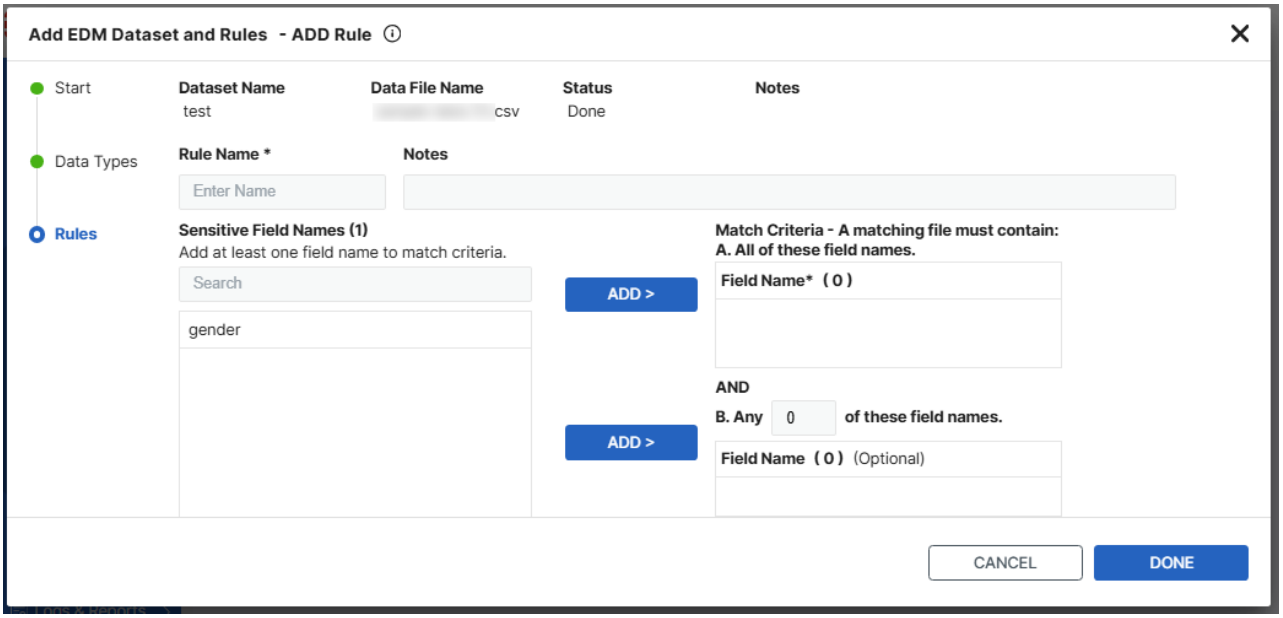
Add Data Types Add at least one data type to each checked sensitive field name.

Data Type *: Standard
Geographical Region *: ALL
Category *: ALL
Data Types * 0 of 453 Selected

Search

ASP.NET Machine Key
AWS Access Key
AWS Secret Access Key
Age
Alibaba Access Key ID
Alibaba Secret Key
American Bank Association Routing Number
American Bankers CUSIP ID
Argentina Driver's License Number
Argentina National Identity (DNI) Number
Argentina Passport Number
Argentina Unique Tax Identification
Asana Client ID
Asana Client Secret
Australia Bank Account Number
Australia Bank-State-Branch (BSB) Number
Australian Business Number(ABN)
Australian Company Number
Australian Driver's License Number
Australian Medicare card number

5. Click *ADD RULE* to create a rule for the EDM data type as needed and click *DONE*.



Add EDM Dataset and Rules - ADD Rule ⓘ ✕

- ● Start
- ● Data Types
- ○ **Rules**

Dataset Name: test
Data File Name: [redacted]csv
Status: Done
Notes

Rule Name *: Enter Name
Notes

Sensitive Field Names (1)
Add at least one field name to match criteria.

Search

gender

Match Criteria - A matching file must contain:
A. All of these field names.

Field Name* (0)

AND

B. Any 0 **of these field names.**

Field Name (0) (Optional)

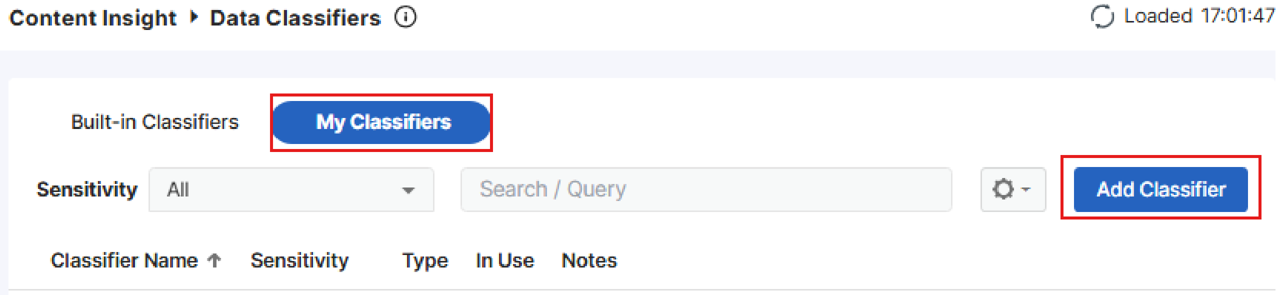
6. Add more rules as needed and click *DONE*.

Data Classifiers

A data classifier is a defined data pattern with a set of data types and logic conditions that a policy (see Policies on page 27) maps to when recognizing patterns in files. FortiData provides built-in data classifiers defined for specific data types and regions that meet specific industry needs. You can also create a new data classifier from scratch or copy from an existing data classifier.

To create a new data classifier:

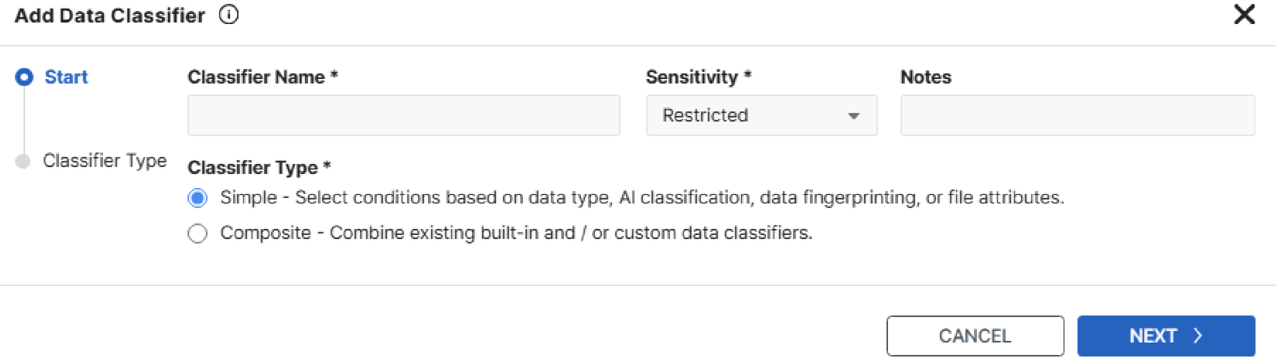
1. To create a data classifier from scratch, click *Add Classifier*.



Sensitivity: All

To build from an existing data classifier, click the eclipsis in front of the data classifier name and select *Derive Classifier* (for built-in classifiers) or *Copy Classifier* (for custom classifiers).

2. Specify the classifier name and select the sensitivity.



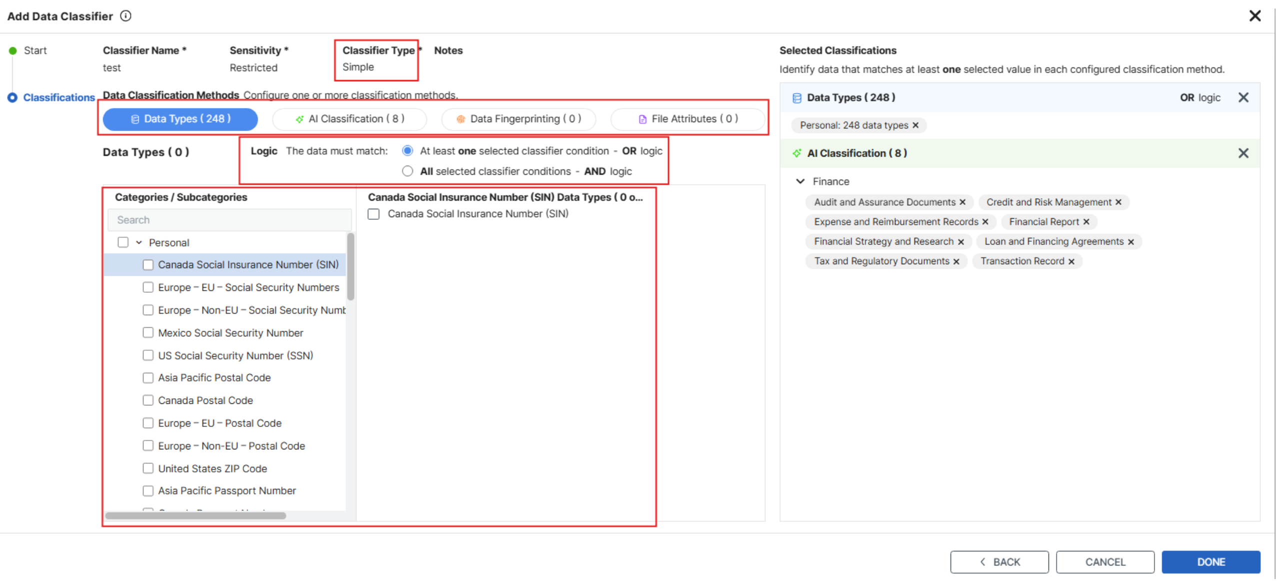
Sensitivity *: Restricted

Classifier Type *

● Simple - Select conditions based on data type, AI classification, data fingerprinting, or file attributes.

○ Composite - Combine existing built-in and / or custom data classifiers.

3. Add notes, if needed.
4. Select the classifier type, which can be the following:
   - **Simple**—Select conditions based on data type, AI classification, data fingerprinting, or file attributes.
   - **Composite**—Combine existing built-in and / or custom data classifiers.
5. For simple classifiers, select the data classification method(s), logic relationships, and the data types for each method.



Add Data Classifier

Start | Classifier Name * test | Sensitivity * Restricted | Classifier Type * Simple | Notes

Classifications

Data Classification Methods Configure one or more classification methods.

Data Types (248) | AI Classification (8) | Data Fingerprinting (0) | File Attributes (0)

Data Types (0)

Logic The data must match: ● At least **one** selected classifier condition - **OR** logic ○ **All** selected classifier conditions - **AND** logic

Categories / Subcategories

- □ Personal
  - □ Canada Social Insurance Number (SIN)
  - □ Europe – EU – Social Security Numbers
  - □ Europe – Non-EU – Social Security Numt
  - □ Mexico Social Security Number
  - □ US Social Security Number (SSN)
  - □ Asia Pacific Postal Code
  - □ Canada Postal Code
  - □ Europe – EU – Postal Code
  - □ Europe – Non-EU – Postal Code
  - □ United States ZIP Code
  - □ Asia Pacific Passport Number

Canada Social Insurance Number (SIN) Data Types (0 o...

□ Canada Social Insurance Number (SIN)

Selected Classifications

Identify data that matches at least **one** selected value in each configured classification method.

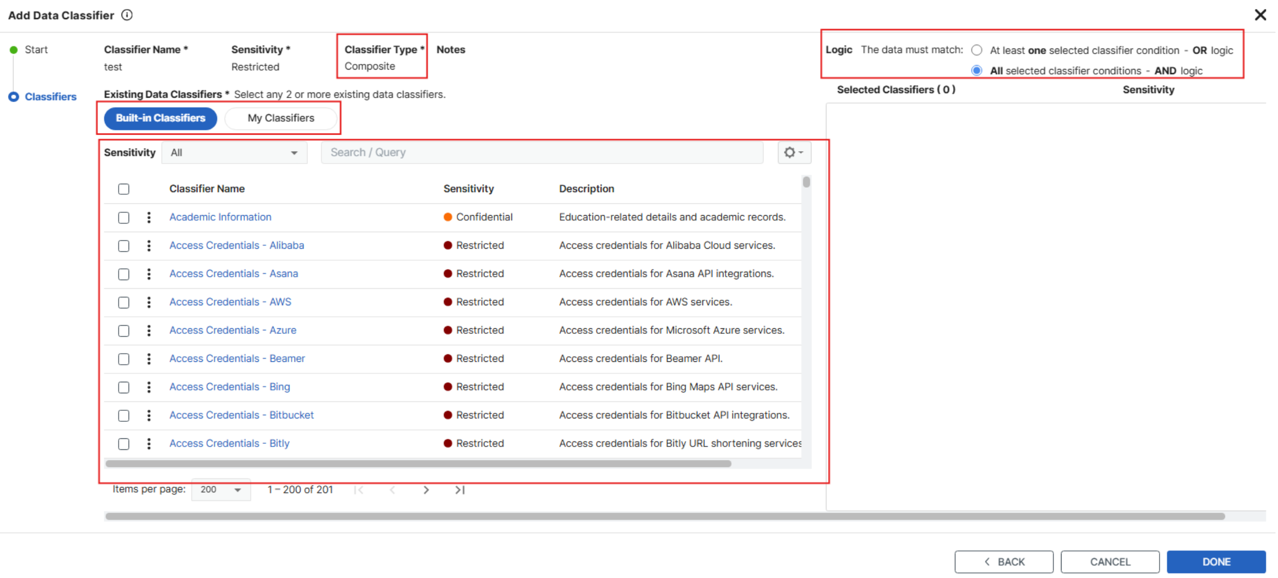
Data Types (248) **OR** logic

Personal: 248 data types ×

AI Classification (8)

Finance: Audit and Assurance Documents × Credit and Risk Management × Expense and Reimbursement Records × Financial Report × Financial Strategy and Research × Loan and Financing Agreements × Tax and Regulatory Documents × Transaction Record ×

For composite classifiers, select the data classifier type(s) and the classifiers for each type. Select the logic to apply to the classifiers.



Add Data Classifier

Start | Classifier Name * test | Sensitivity * Restricted | Classifier Type * Composite | Notes

Classifiers

Existing Data Classifiers * Select any 2 or more existing data classifiers.

Built-in Classifiers | My Classifiers

Sensitivity All

Logic The data must match: ○ At least **one** selected classifier condition - **OR** logic ● **All** selected classifier conditions - **AND** logic

Selected Classifiers (0) Sensitivity

	Classifier Name	Sensitivity	Description
□	Academic Information	● Confidential	Education-related details and academic records.
□	Access Credentials - Alibaba	● Restricted	Access credentials for Alibaba Cloud services.
□	Access Credentials - Asana	● Restricted	Access credentials for Asana API integrations.
□	Access Credentials - AWS	● Restricted	Access credentials for AWS services.
□	Access Credentials - Azure	● Restricted	Access credentials for Microsoft Azure services.
□	Access Credentials - Beamer	● Restricted	Access credentials for Beamer API.
□	Access Credentials - Bing	● Restricted	Access credentials for Bing Maps API services.
□	Access Credentials - Bitbucket	● Restricted	Access credentials for Bitbucket API integrations.
□	Access Credentials - Bitly	● Restricted	Access credentials for Bitly URL shortening services

Items per page: 200 1 – 200 of 201

- *AND*—The data must match all selected classifier conditions to be considered a match.
- *OR*—The data must match at least one selected classifier condition to be considered a match.

6. Add or remove classifiers as needed.
7. Click *DONE*.

Logs & Reports

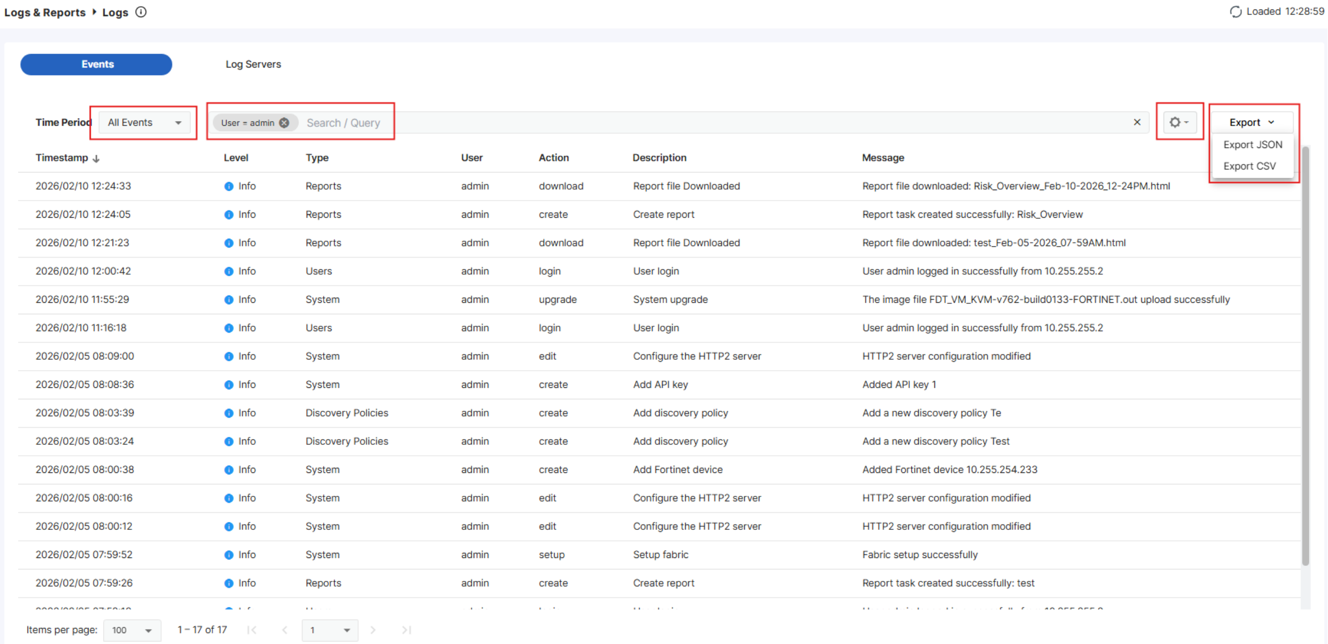
Go to the *Logs & Reports* page to view logs and reports. You can also configure log servers and report settings.

- Logs on page 40
  - Log Servers on page 40
- Reports on page 42
  - Report Settings on page 43

Logs

System events log data is available in the *Logs & Reports > Logs* page. By default, all event logs are displayed. You can filter the logs by time period and queries with various conditions.

- To customize the columns to display in the table, use the *Configure* button on the top-right.
- To export the logs, click *EXPORT > Export JSON/CSV*.



Time Period: All Events

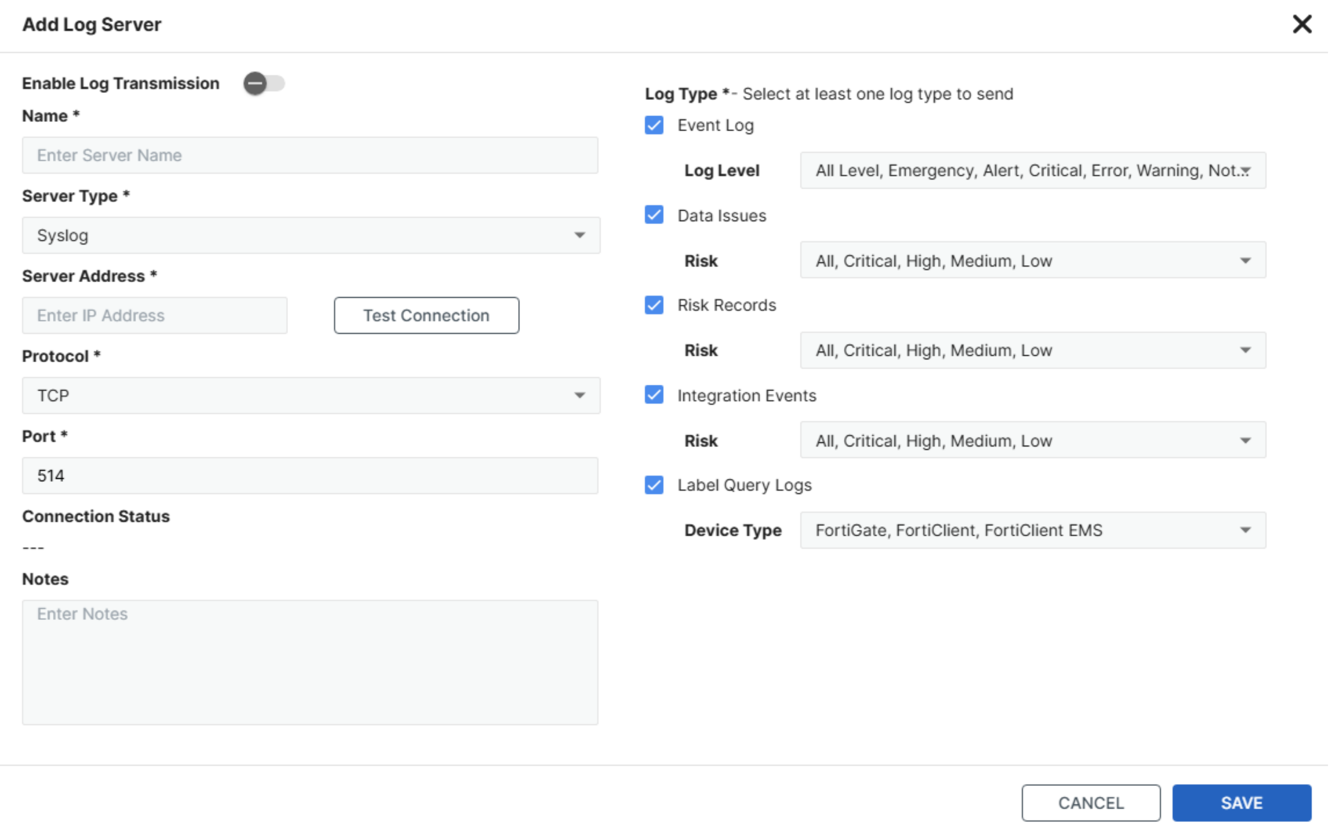
User = admin

Timestamp ↓	Level	Type	User	Action	Description	Message
2026/02/10 12:24:33	Info	Reports	admin	download	Report file Downloaded	Report file downloaded: Risk_Overview_Feb-10-2026_12-24PM.html
2026/02/10 12:24:05	Info	Reports	admin	create	Create report	Report task created successfully: Risk_Overview
2026/02/10 12:21:23	Info	Reports	admin	download	Report file Downloaded	Report file downloaded: test_Feb-05-2026_07-59AM.html
2026/02/10 12:00:42	Info	Users	admin	login	User login	User admin logged in successfully from 10.255.255.2
2026/02/10 11:55:29	Info	System	admin	upgrade	System upgrade	The image file FDT_VM_KVM-v762-build0133-FORTINET.out upload successfully
2026/02/10 11:16:18	Info	Users	admin	login	User login	User admin logged in successfully from 10.255.255.2
2026/02/05 08:09:00	Info	System	admin	edit	Configure the HTTP2 server	HTTP2 server configuration modified
2026/02/05 08:08:36	Info	System	admin	create	Add API key	Added API key 1
2026/02/05 08:03:39	Info	Discovery Policies	admin	create	Add discovery policy	Add a new discovery policy Te
2026/02/05 08:03:24	Info	Discovery Policies	admin	create	Add discovery policy	Add a new discovery policy Test
2026/02/05 08:00:38	Info	System	admin	create	Add Fortinet device	Added Fortinet device 10.255.254.233
2026/02/05 08:00:16	Info	System	admin	edit	Configure the HTTP2 server	HTTP2 server configuration modified
2026/02/05 08:00:12	Info	System	admin	edit	Configure the HTTP2 server	HTTP2 server configuration modified
2026/02/05 07:59:52	Info	System	admin	setup	Setup fabric	Fabric setup successfully
2026/02/05 07:59:26	Info	Reports	admin	create	Create report	Report task created successfully: test

Items per page: 100   1 – 17 of 17   1

Log Servers

Configure log servers to send the logs. Click *Add Log Server* and configure the following options.



Add Log Server

Enable Log Transmission

Name *

Enter Server Name

Server Type *

Syslog

Server Address *

Enter IP Address

Test Connection

Protocol *

TCP

Port *

514

Connection Status

Notes

Enter Notes

Log Type *- Select at least one log type to send

☑ Event Log

Log Level: All Level, Emergency, Alert, Critical, Error, Warning, Not...

☑ Data Issues

Risk: All, Critical, High, Medium, Low

☑ Risk Records

Risk: All, Critical, High, Medium, Low

☑ Integration Events

Risk: All, Critical, High, Medium, Low

☑ Label Query Logs

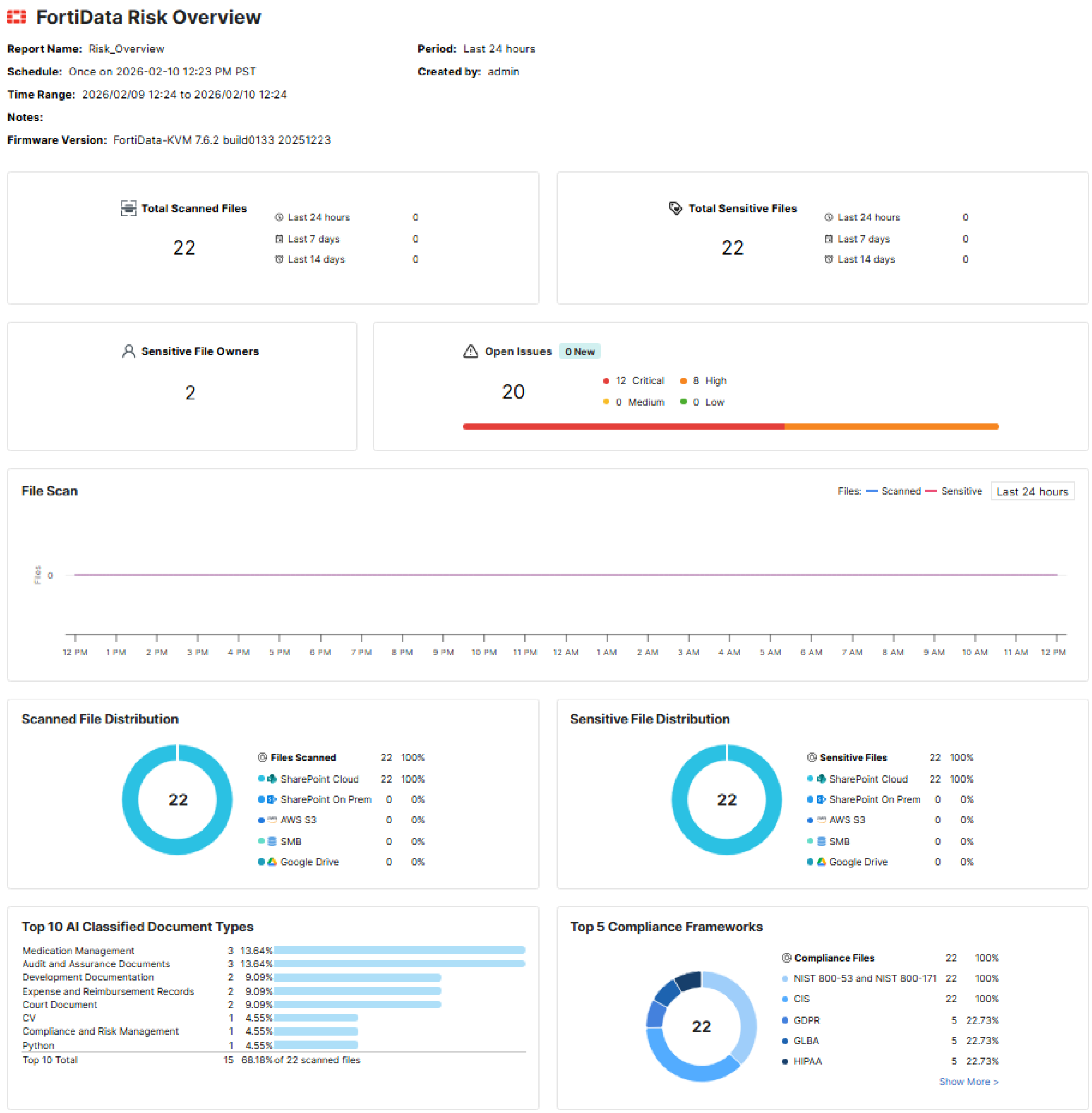
Device Type: FortiGate, FortiClient, FortiClient EMS

Enable Log Transmission	Enable to send logs to this server.
Name	Specify the name of the log server.
Server Type	Specify the type of the server: • Syslog • FortiAnalyzer
Server Address	Specify the IP address of the log server. Click *Test Connection* to verify the connection is successful.
Protocol	Specify the syslog server protocol, which can be TCP or UDP.
Port	Specify the port of the log server.
Notes	Specify any comments about this log server.
Log Type	Specify the types of logs to send to the log server, such as event log and data issues. You can also further define the scope of logs to send to the log server using the dropdown filters.

Reports

The *Logs & Reports > Reports* page displays a list of configured reports and the running history and status. You can create one-time or recurring Dashboard on page 7 and analytics Visualization on page 16 reports (in HTML or PDF format) for a specific time period. The last report can be downloaded by clicking the file icon in the *Download* column.

Sample report:



FortiData Risk Overview

Report Name: Risk_Overview
Schedule: Once on 2026-02-10 12:23 PM PST
Time Range: 2026/02/09 12:24 to 2026/02/10 12:24
Notes:
Firmware Version: FortiData-KVM 7.6.2 build0133 20251223

Period: Last 24 hours
Created by: admin

Total Scanned Files 22

Last 24 hours	0
Last 7 days	0
Last 14 days	0

Total Sensitive Files 22

Last 24 hours	0
Last 7 days	0
Last 14 days	0

Sensitive File Owners 2

Open Issues 0 New

20

● 12 Critical ● 8 High
● 0 Medium ● 0 Low

File Scan

Scanned File Distribution

Files Scanned	22	100%
SharePoint Cloud	22	100%
SharePoint On Prem	0	0%
AWS S3	0	0%
SMB	0	0%
Google Drive	0	0%

Sensitive File Distribution

Sensitive Files	22	100%
SharePoint Cloud	22	100%
SharePoint On Prem	0	0%
AWS S3	0	0%
SMB	0	0%
Google Drive	0	0%

Top 10 AI Classified Document Types

Medication Management	3	13.64%
Audit and Assurance Documents	3	13.64%
Development Documentation	2	9.09%
Expense and Reimbursement Records	2	9.09%
Court Document	2	9.09%
CV	1	4.55%
Compliance and Risk Management	1	4.55%
Python	1	4.55%
Top 10 Total	15	68.18% of 22 scanned files

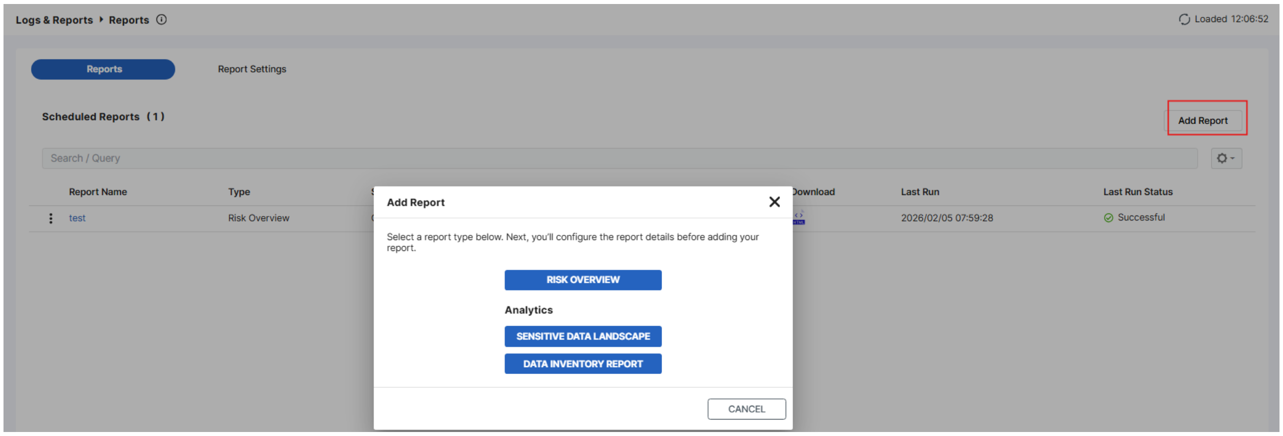
Top 5 Compliance Frameworks

Compliance Files	22	100%
NIST 800-53 and NIST 800-171	22	100%
CIS	22	100%
GDPR	5	22.73%
GLBA	5	22.73%
HIPAA	5	22.73%

Show More >

To create a report:

1. On the *Logs & Reports > Reports* page, click *Add Report*.



Report Name	Type	Last Run	Last Run Status
test	Risk Overview	2026/02/05 07:59:28	✓ Successful

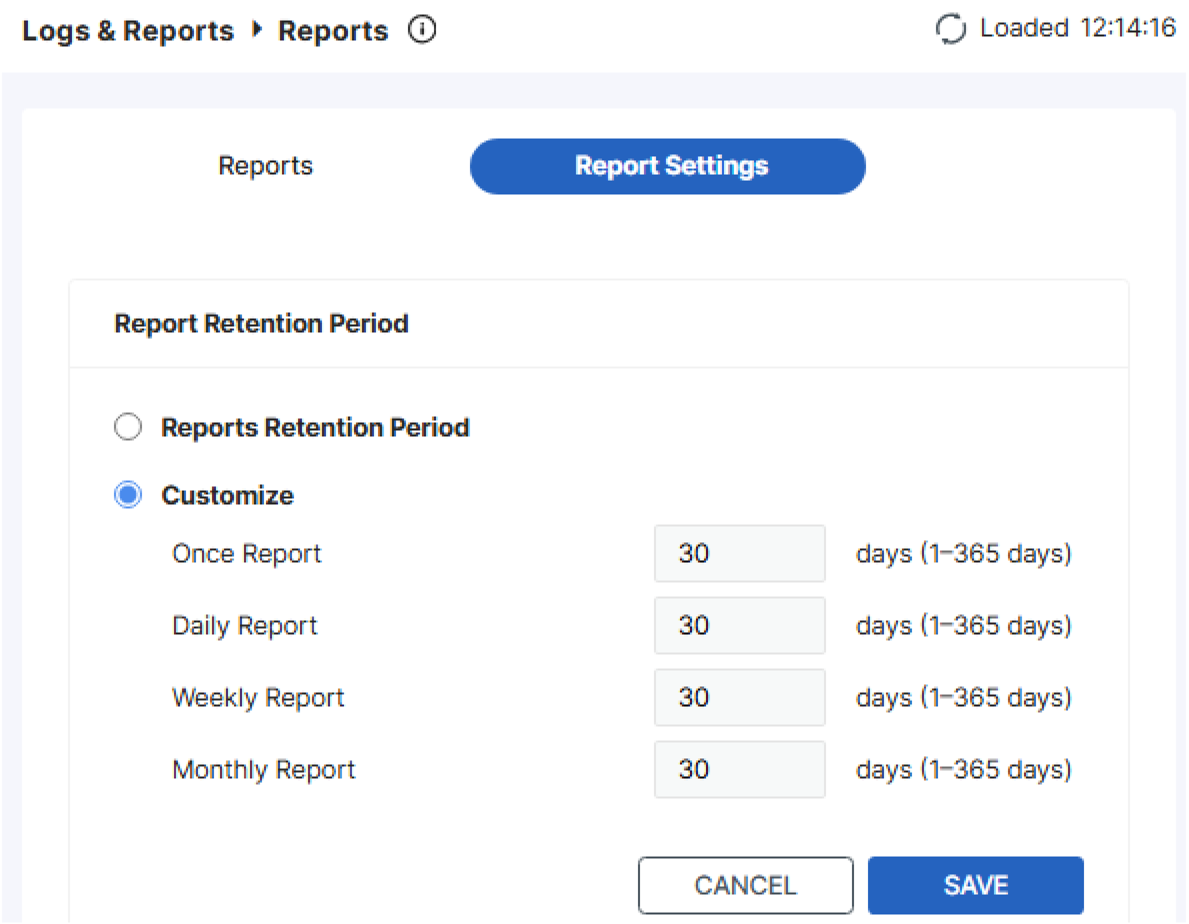
Select a report type below. Next, you'll configure the report details before adding your report.

2. Select a report type depending on your needs.
3. Specify the report name, running frequency, start time, format (HTML or PDF), storage, scan period, notification email template (HTML or plain), and notes (if needed).
4. For *Sensitive Data Landscape* and *Data Inventory* reports, select the storage from the list as well. By default, all storage locations are selected
5. Click *SAVE*.

   The report appears in the list.
6. **(Optional)** Configure the retention period for the reports in the Report Settings on page 43 page as needed. The default is 30 days for all report types.

Report Settings

In the *Logs & Reports > Reports > Report Settings* page, you can configure the retention period for reports. See Reports on page 42.



Report Retention Period

○ Reports Retention Period

● Customize

Once Report	30	days (1–365 days)
Daily Report	30	days (1–365 days)
Weekly Report	30	days (1–365 days)
Monthly Report	30	days (1–365 days)

Report Retention Period	Specify the number of days (1-90) for which the reports will be retained. The default is 30 days.
Customize	Configure the number of days (1-365) for which each report type will be retained. The default is 30 days for all report types.

System

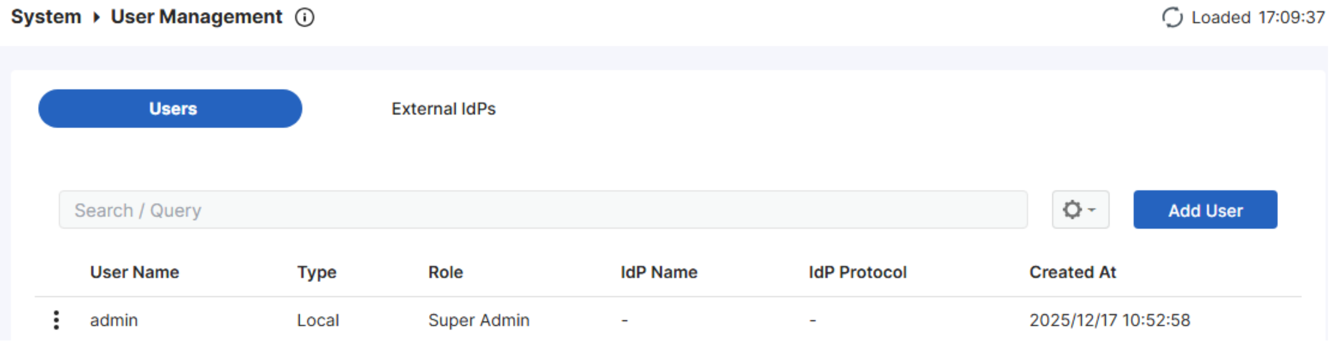
Go to the *System* page to view system related information, and manage system settings.

- User Management on page 45
- Settings on page 51
- FortiGuard on page 58
- Backup & Restore on page 60

User Management

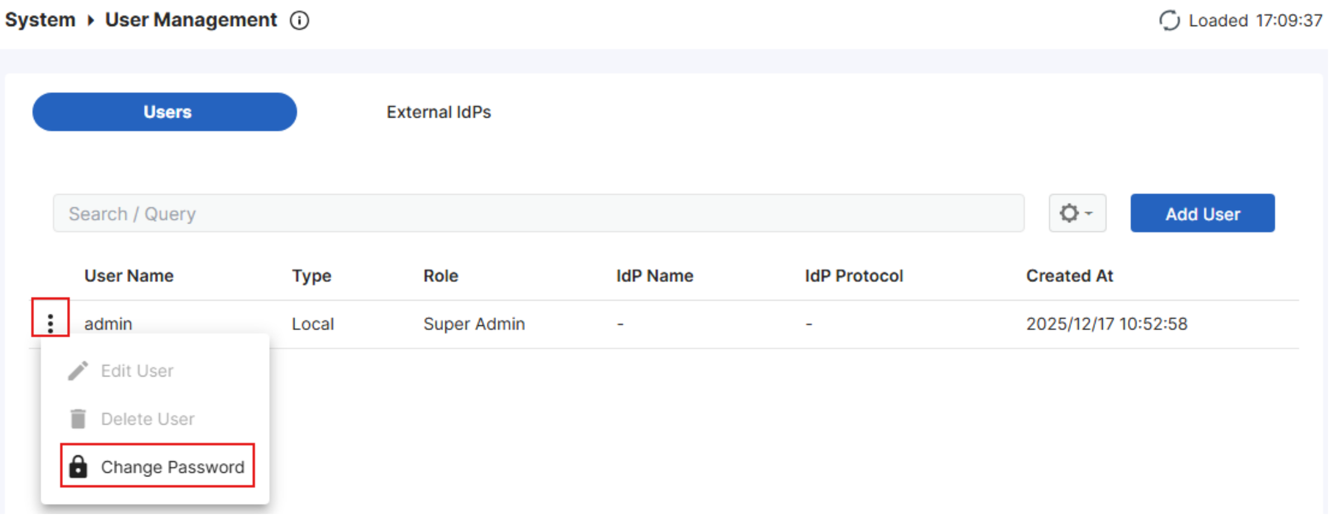
The *System* > *User Management* > *Users* page is available to admin users only and displays a list of users in the FortiData system with their roles.

A default administrative account named "admin" is created, which is a super administrator with the highest privileges, including creating or deleting admin users.



	User Name	Type	Role	IdP Name	IdP Protocol	Created At
⋮	admin	Local	Super Admin	-	-	2025/12/17 10:52:58

This user cannot be deleted or edited. However, you can change the password by clicking the three dots on the left of the row and select *Change Password*.



System ▸ User Management ⓘ   Loaded 17:09:37

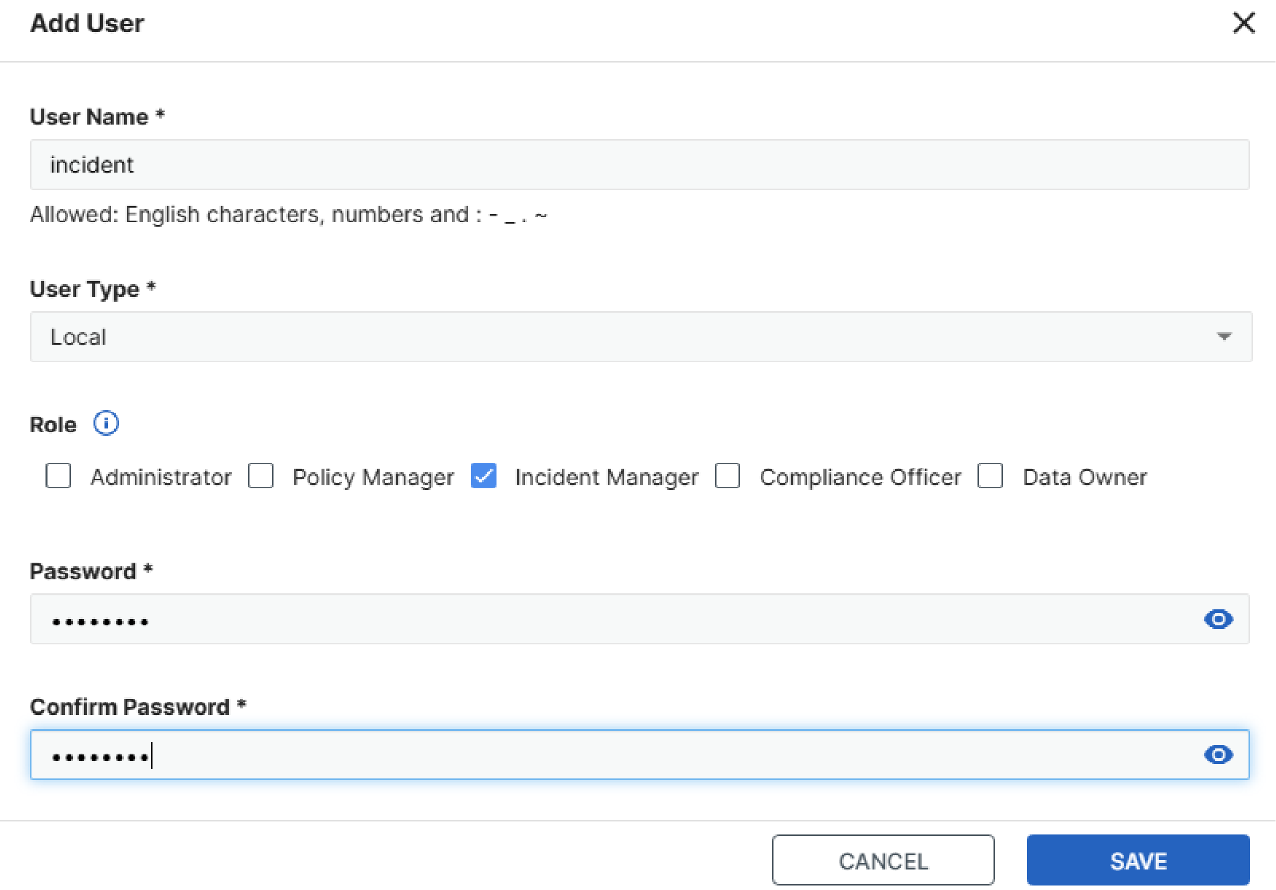
User Name	Type	Role	IdP Name	IdP Protocol	Created At
admin	Local	Super Admin	-	-	2025/12/17 10:52:58

To create a user:

1. On the *System* > *User Management* > *Users* page, click *Add User*.
2. Specify the username. Only alphabetical letters, numbers, and the following special characters are allowed in a username: : - _ . ~
3. Select the user type:
   - To create a local user, select *Local*.
   - To add a user from a remote IdP server (see External IdPs on page 49), select *Remote (Match a user on a remote server)* or *Remote + Wildcard (Match all users on a remote server)*.
4. Select a role. See role definitions below.

Name	Permissions
Administrator	Full administrative access, including creating administrative or user accounts and deleting user accounts. Compared with the default super admin user, administrators cannot delete administrative account.
Policy Manager	Create, modify, and delete policies and rules.
Incident Manager	Access to incident logs and data security dashboard alerts.
Compliance Officer	Read-only access to policies, logs, and audit reports.
Data Owner	Review access to specific data scanning rules, DLP rules and incidents.

5. For local users, specify the password and confirm it.



Add User

User Name *

incident

Allowed: English characters, numbers and : - _ . ~

User Type *

Local

Role

□ Administrator □ Policy Manager ☑ Incident Manager □ Compliance Officer □ Data Owner

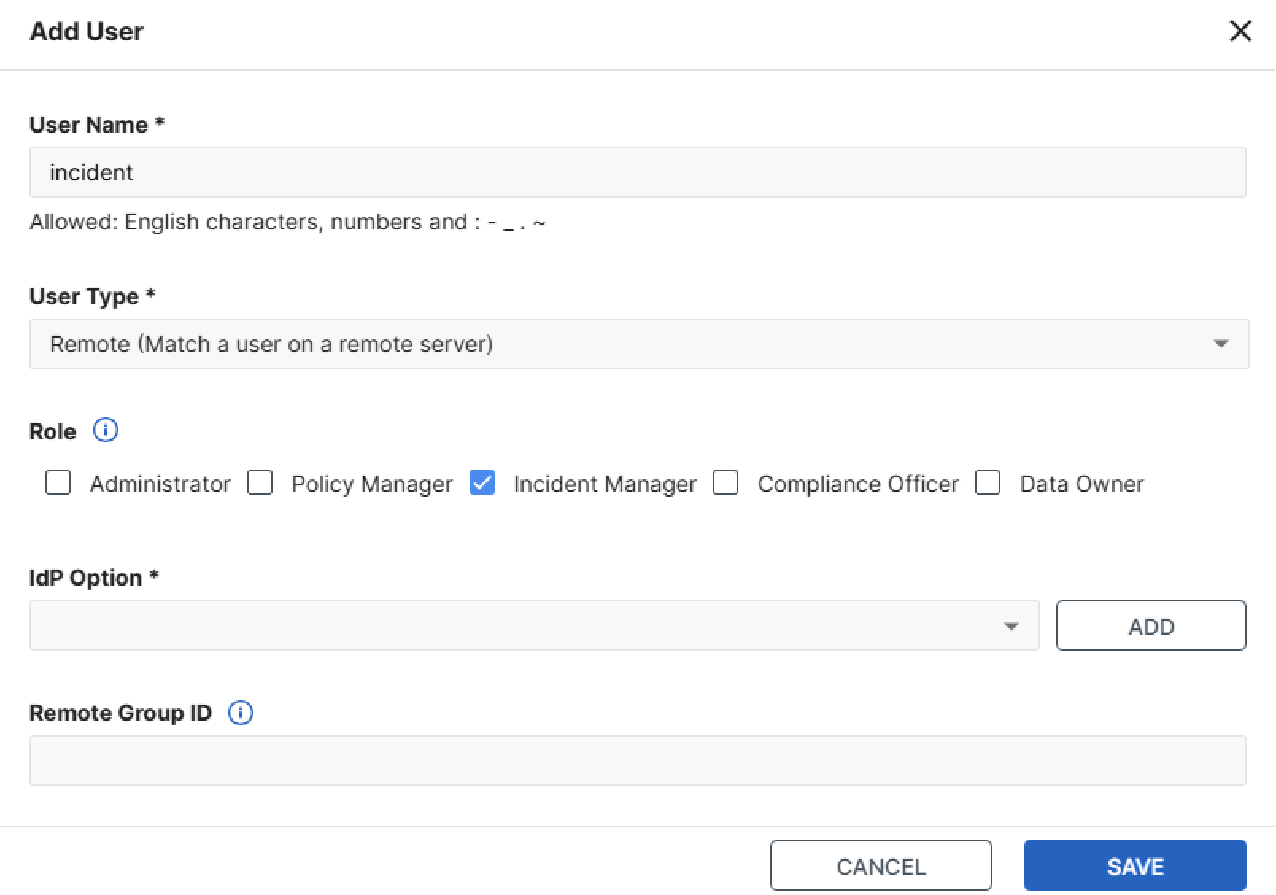
Password *

•••••••••

Confirm Password *

•••••••••

6. For remote users, select the IdP or add a new one (see External IdPs on page 49) and specify the remote group ID.



Add User

User Name *

incident

Allowed: English characters, numbers and : - _ . ~

User Type *

Remote (Match a user on a remote server)

Role

☐ Administrator ☐ Policy Manager ☑ Incident Manager ☐ Compliance Officer ☐ Data Owner

IdP Option *

Remote Group ID

7. Click *SAVE*.
8. Click *YES* to confirm.

To change the role of a user:

1. Click the three dots on the left of the row and select *Edit User*.

To delete a user:

1. Click the three dots on the left of the row and select *Delete User*.
   Note that admin users can only be deleted by the super admin.

To change the password of a user:

1. Click the three dots on the left of the row and select *Change Password*.
   Note that the password of the super admin can only be changed by the super admin.

External IdPs

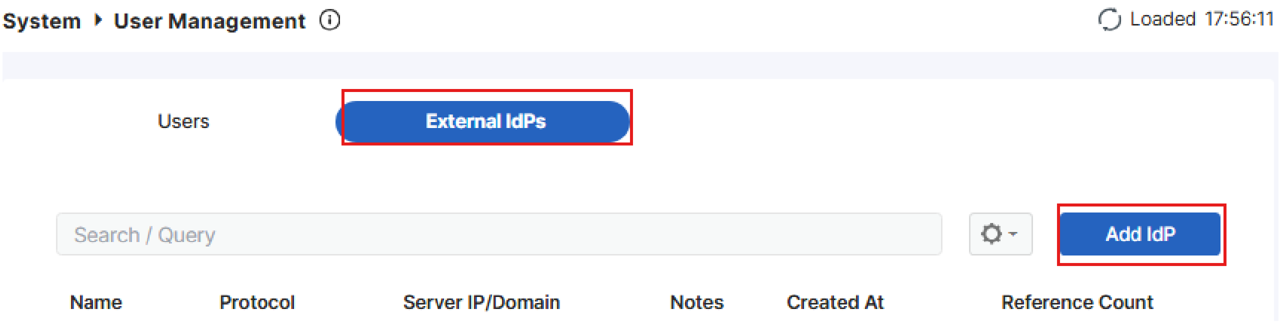
Use the *System* > *User Management* > *External IdPs* page to configure external IdPs for remote users. You can then add the remote users to the users list (see User Management on page 45).

The following external IdP types are supported:

- LDAP
- Kerberos
- SAML 2.0

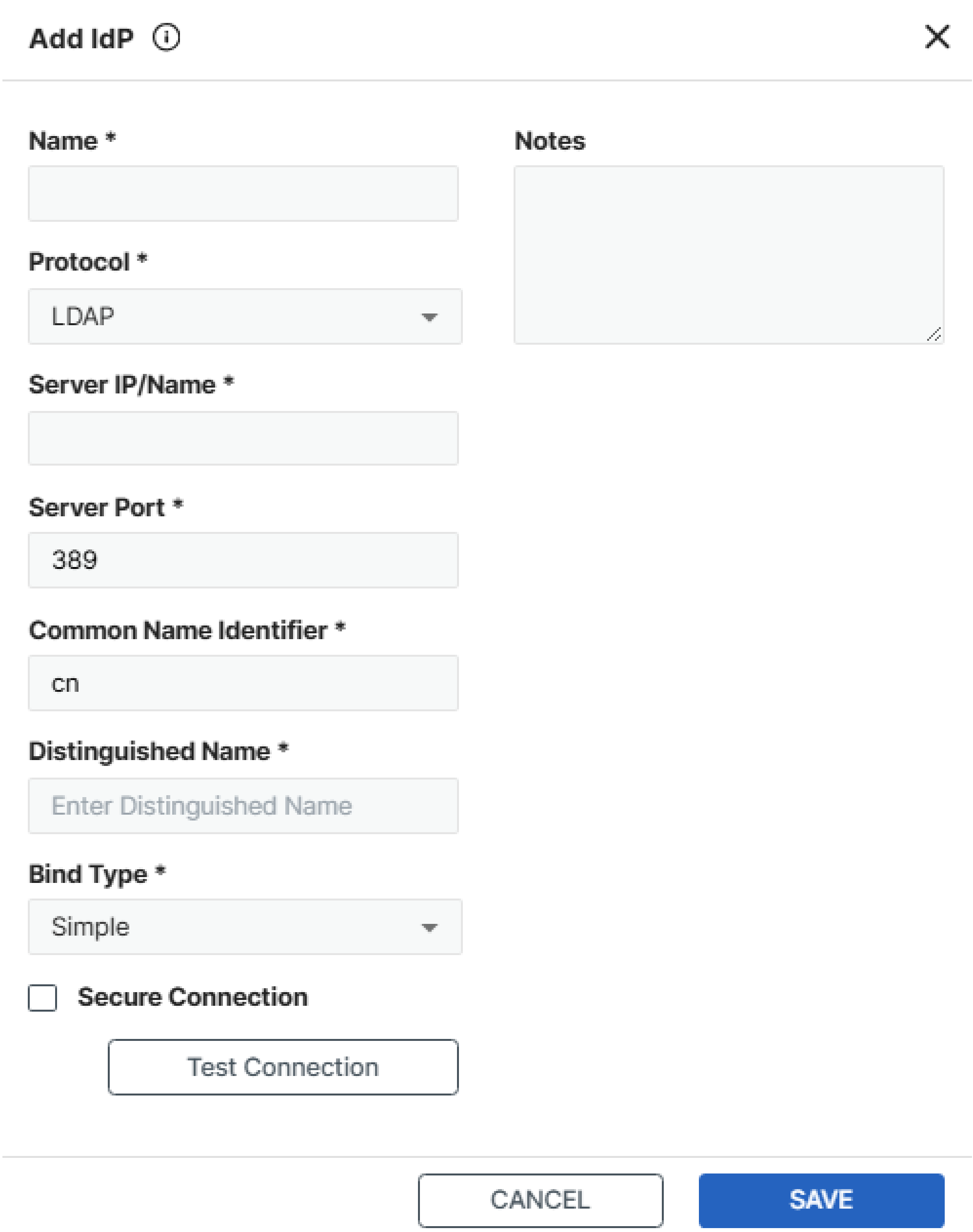
To add an IdP server:

1. On the *System* > *User Management* > *External IdPs* page, click *Add IdP*.



Name	Protocol	Server IP/Domain	Notes	Created At	Reference Count

2. Specify the name.



Add IdP

Name *

Notes

Protocol * LDAP

Server IP/Name *

Server Port * 389

Common Name Identifier * cn

Distinguished Name * Enter Distinguished Name

Bind Type * Simple

☐ Secure Connection

3. Select the protocol and configure the following options:

Protocol	Configuration options	
LDAP	*Server IP/Name*	IP or FQDN of the LDAP server.
	Server Port	Port of the LDAP server.
	Common Name Identifier	Common name identifier of the LDAP server.
	Distinguished Name	Distinguished name of the LDAP server.
	Bind Type	Select from the following:

Protocol	Configuration options	
		• Simple • Anonymous • Regular
	Secure Connection	Select to enable HTTPS connection for better security. You can then further select the *STARTTLS* or *LDAPS* protocol and CA/client certificate.
	Test Connection	Click to verify if the server connection is successful.
Kerberos	*Delegated Realm*	Specify the delegated realm.
	Port	Specify the port of the Kerberos server.
	KDC Host	Specify the KDC host. If left empty, FortiData uses delegated realm as KDC host instead.
	Test Connection	Click to verify if the server connection is successful.
SAML 2.0	*Address*	URL of the service provider.
	Entity ID	Entity ID of the service provider.
	Assertion consumer service URL	Assertion consumer service URL of the service provider.
	Signal logout service URL	Signal logout service URL of the service provider.
	IdP entity ID	Entity ID of the IdP.
	IdP single sign-on URL	Single sign-on URL of the IdP.
	IdP single logout URL	Single logout URL of the IdP.
	Certificate	Select a remote certificate from the list or add a new one. See Certificates on page 56.
	Attribute used to identity users	Specify the attribute used to identity users.
	Attribute used to identity groups	Specify the attribute used to identity groups.

4. Click *SAVE*.

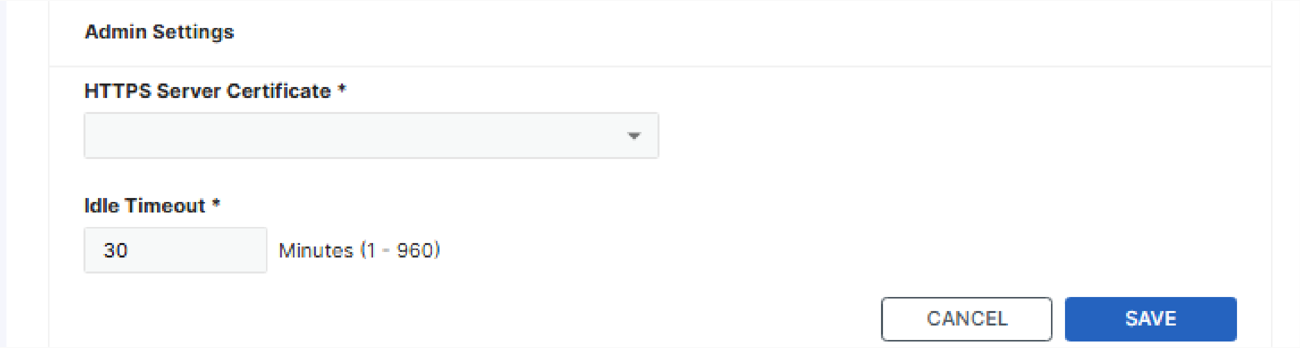
Settings

The *System* > *Settings* page includes the following tabs:

General

In the *System* > *Settings* > *General* tab, you can configure the following:

Admin Settings



Admin Settings

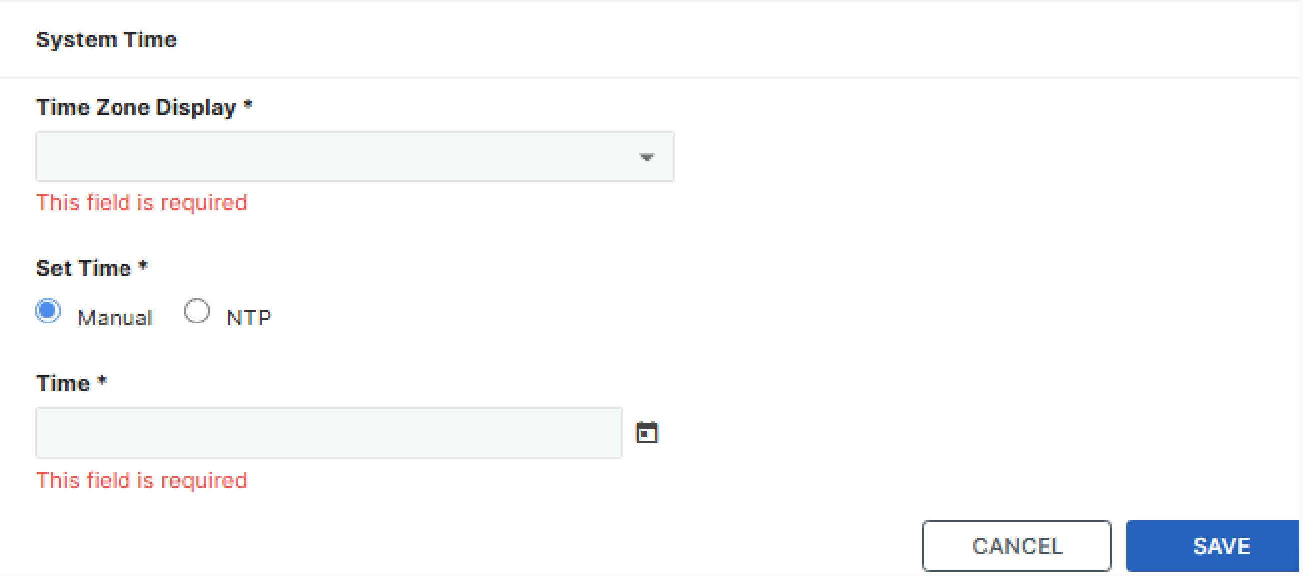
HTTPS Server Certificate *

Idle Timeout *

30 Minutes (1 - 960)

HTTPS Server Certificate	Select the TLS certificates uploaded in *System* > *Certificates on page 56*.
Idle Timeout	Define the idle timeout period (within the range of 1-960 minutes) to expire a FortiData GUI session. The default is 30 minutes,

System Time



System Time

Time Zone Display *

This field is required

Set Time *

● Manual ○ NTP

Time *

This field is required

Time Zone Display	Select the time zone where the FortiData appliance is installed. The system will be updated according to the timezone, accounting for daylight savings time.

Set Time	Enter the current settings for the system date and time. You can change these manually. Use the calendar button to select the date and time from a calendar.
NTP Server	Enter the IP address or domain name of an NTP server. To find an NTP server that you can use, see http://www.ntp.org.
Sync Interval	Enter the interval, in minutes, at which the system time is synchronized with the NTP server. The default is 60.

Network

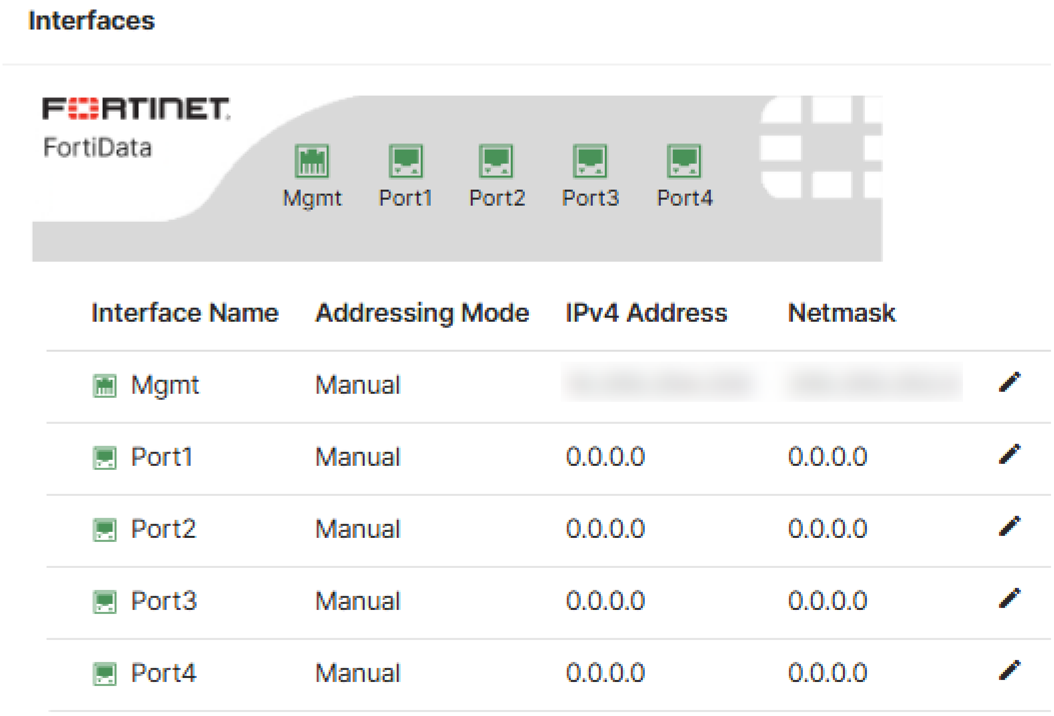
Configure the interfaces and DNS settings for FortiData in the *System* > *Settings* > *Network* tab.

Interfaces

FortiData includes five interfaces: management and port 1 to 4.

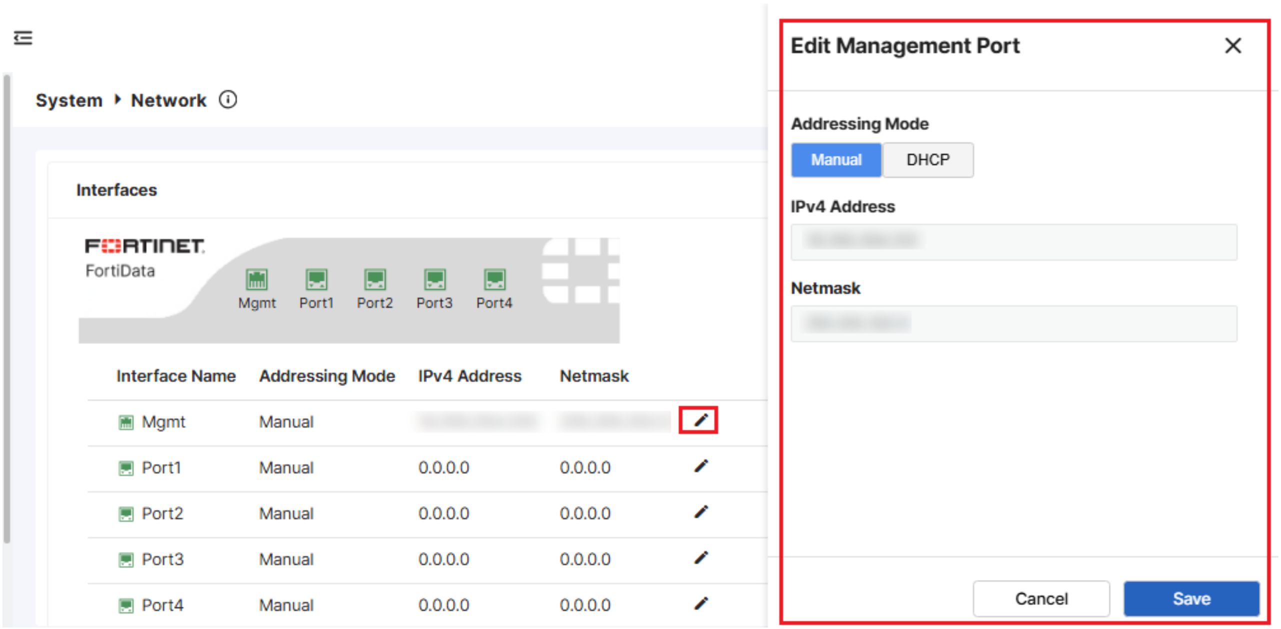
To configure the interfaces:

1. In the *System* > *Settings* > *Network* tab, click *Interfaces* to display the interfaces setting.



Interface Name	Addressing Mode	IPv4 Address	Netmask	
Mgmt	Manual	[redacted]	[redacted]	✎
Port1	Manual	0.0.0.0	0.0.0.0	✎
Port2	Manual	0.0.0.0	0.0.0.0	✎
Port3	Manual	0.0.0.0	0.0.0.0	✎
Port4	Manual	0.0.0.0	0.0.0.0	✎

2. Click the pencil icon for an interface to edit the settings.



Interface Name	Addressing Mode	IPv4 Address	Netmask
Mgmt	Manual	[redacted]	[redacted]
Port1	Manual	0.0.0.0	0.0.0.0
Port2	Manual	0.0.0.0	0.0.0.0
Port3	Manual	0.0.0.0	0.0.0.0
Port4	Manual	0.0.0.0	0.0.0.0

Edit Management Port

Addressing Mode: Manual | DHCP

IPv4 Address: [redacted]

Netmask: [redacted]

Setting	Description
Addressing Mode	Specify whether FortiData acquires an IPv4 address for this network interface manually or using DHCP.
IPv4 Address	Enter the IP address.
Netmask	Enter the netmask.

3. Click *Save* to complete the interface configuration.
4. Repeat the steps above for each interface you want to configure.

DNS

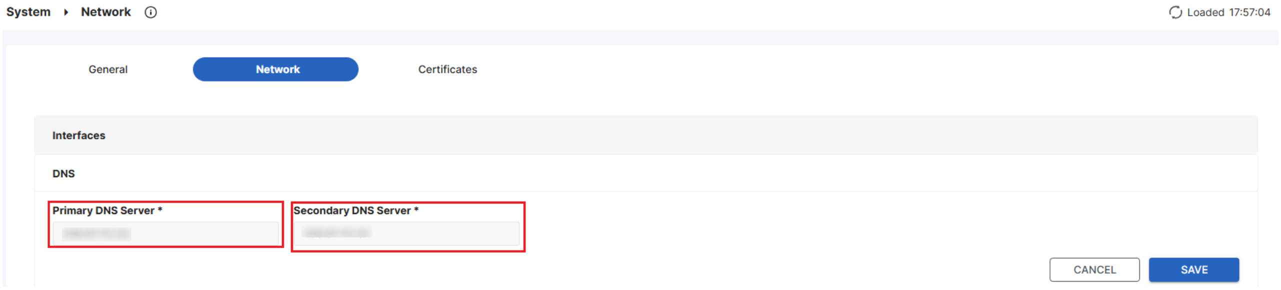
Like many other types of network devices, FortiData appliances require connectivity to DNS servers for DNS lookups.

Your Internet service provider (ISP) may supply IP addresses of DNS servers, or you may want to use the IP addresses of your own DNS servers. You must provide unicast, non-local addresses for your DNS servers. Localhost and broadcast addresses will not be accepted.

Incorrect DNS settings or unreliable DNS connectivity can cause issues with some features, such as NTP system time.

To configure DNS settings via the web UI:

1. Go to *System* > *Settings* > *Network* > *DNS*.



Primary DNS Server * [redacted]

Secondary DNS Server * [redacted]

2. In *Primary DNS Server*, Enter the IP address of the primary DNS server.
3. In *Secondary DNS Server*, enter the IP address of the secondary DNS server.
4. Click *SAVE*.

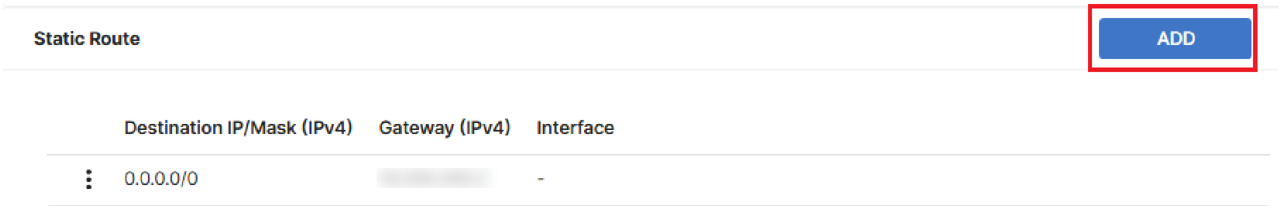
   FortiData queries the DNS servers whenever it needs to resolve a domain name into an IP address, such as for NTP system time.

Static Route

The default route has a destination of 0.0.0.0/0.0.0.0, representing the least specific route in the routing table.

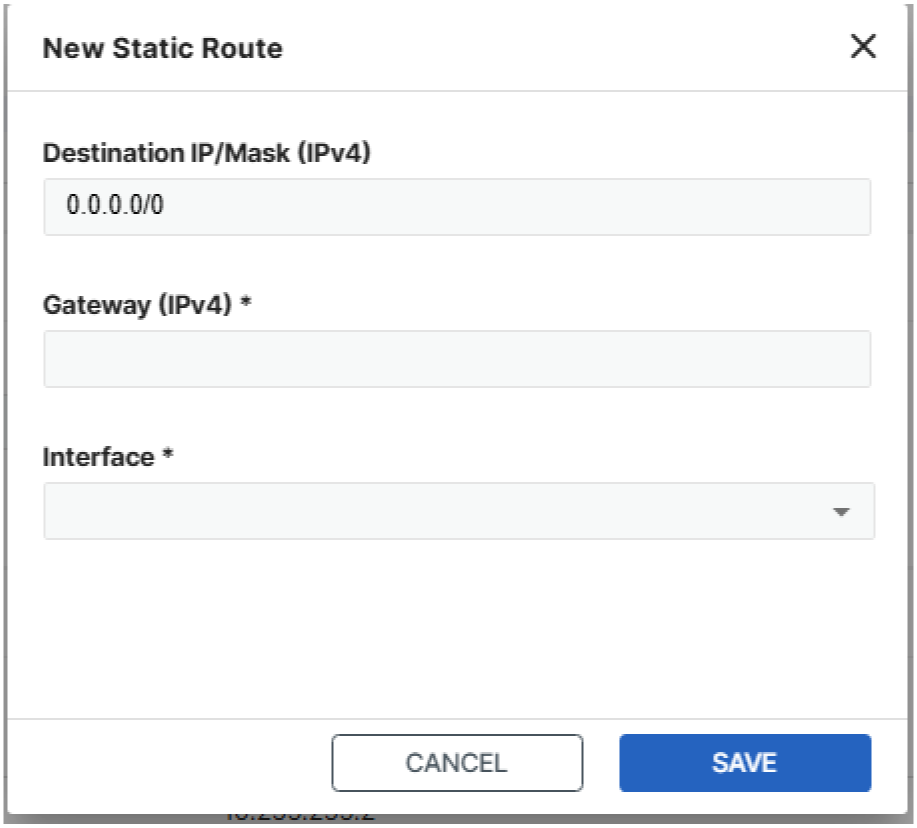
To add a static route in the GUI:

1. Go to *System* > *Settings* > *Network* > *Static Route* and click *Add*.



	Destination IP/Mask (IPv4)	Gateway (IPv4)	Interface
⋮	0.0.0.0/0	[redacted]	-

2. Enter the following information:



New Static Route

Destination IP/Mask (IPv4): 0.0.0.0/0

Gateway (IPv4) *

Interface *

Destination IP/Mask (IPv4)	Enter the destination IP address and netmask. A value of `0.0.0.0/0.0.0.0` creates a default route.
Gateway (IPv4)	Enter the gateway IP address.
Interface	Select the name of the interface that the static route will connect through.

3. Click *SAVE*.

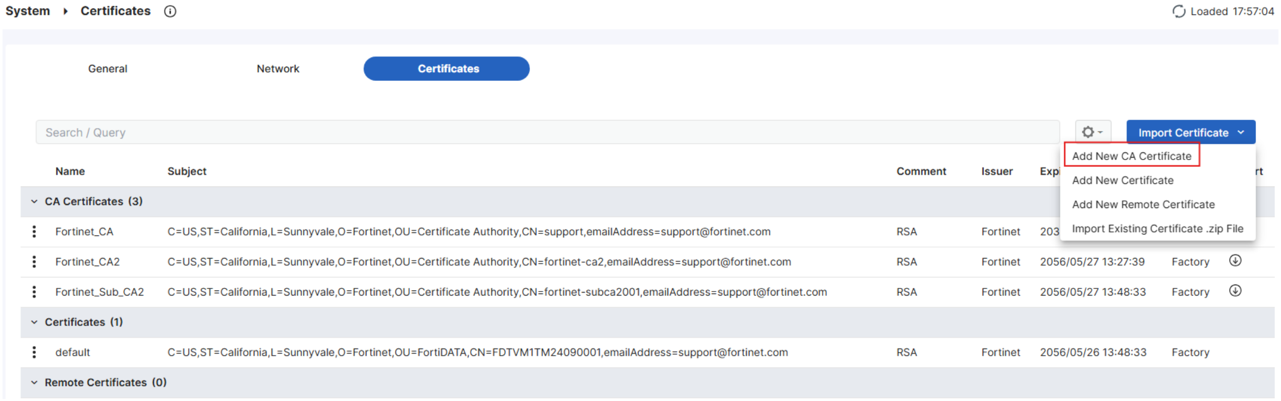
Certificates

You can import the following types of certificates in the *System > Settings > Certificates* tab:

- **CA certificates**—Use this option to import private or well-known CA certificates to the FortiData so that certificates signed by this CA are trusted by the FortiData.
- **Customized TLS certificates**—Use this option to import customized TLS certificates for HTTPS access to FortiData's GUI.
- **Remote certificates**—Use this option to import remote certificates to the FortiData. For example, you may want to add SAML certificates for External IdPs on page 49.

To import a new CA certificate:

1. Go to *System > Settings > Certificates*.
2. Click *Import Certificate > Add New CA Certificate*.



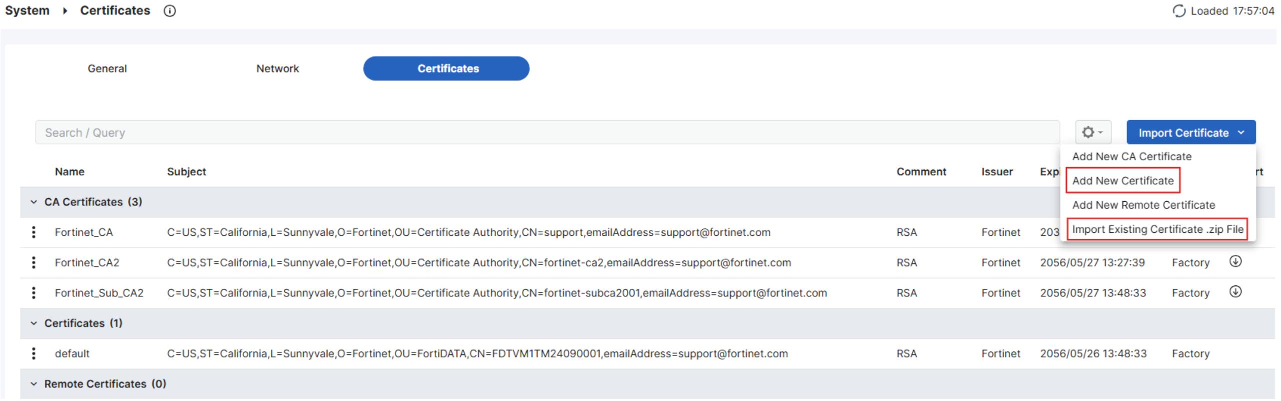
System ▸ Certificates ⓘ — Loaded 17:57:04

	Name	Subject	Comment	Issuer	Exp	rt	
˅ CA Certificates (3)							
⋮	Fortinet_CA	C=US,ST=California,L=Sunnyvale,O=Fortinet,OU=Certificate Authority,CN=support,emailAddress=support@fortinet.com	RSA	Fortinet	203		
⋮	Fortinet_CA2	C=US,ST=California,L=Sunnyvale,O=Fortinet,OU=Certificate Authority,CN=fortinet-ca2,emailAddress=support@fortinet.com	RSA	Fortinet	2056/05/27 13:27:39	Factory	⊕
⋮	Fortinet_Sub_CA2	C=US,ST=California,L=Sunnyvale,O=Fortinet,OU=Certificate Authority,CN=fortinet-subca2001,emailAddress=support@fortinet.com	RSA	Fortinet	2056/05/27 13:48:33	Factory	⊕
˅ Certificates (1)							
⋮	default	C=US,ST=California,L=Sunnyvale,O=Fortinet,OU=FortiDATA,CN=FDTVM1TM24090001,emailAddress=support@fortinet.com	RSA	Fortinet	2056/05/26 13:48:33	Factory	
˅ Remote Certificates (0)							

3. Click *BROWSE* to select the Base64(PEM) certificate file (`.cer` or `.crt`) from your local directory. The first character cannot be "." or "-".
4. Click *IMPORT*.
5. Click *Close*.

To import a customized TLS certificate:

1. Go to *System > Settings > Certificates*.
2. Click *Import Certificate* and select one of the following options:



System ▸ Certificates ⓘ — Loaded 17:57:04

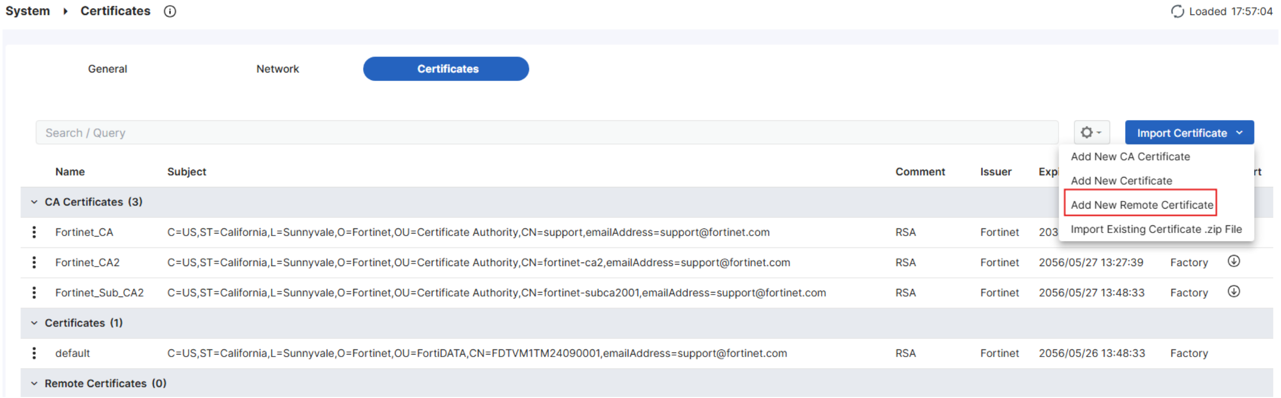
	Name	Subject	Comment	Issuer	Exp	rt	
˅ CA Certificates (3)							
⋮	Fortinet_CA	C=US,ST=California,L=Sunnyvale,O=Fortinet,OU=Certificate Authority,CN=support,emailAddress=support@fortinet.com	RSA	Fortinet	203		
⋮	Fortinet_CA2	C=US,ST=California,L=Sunnyvale,O=Fortinet,OU=Certificate Authority,CN=fortinet-ca2,emailAddress=support@fortinet.com	RSA	Fortinet	2056/05/27 13:27:39	Factory	⊕
⋮	Fortinet_Sub_CA2	C=US,ST=California,L=Sunnyvale,O=Fortinet,OU=Certificate Authority,CN=fortinet-subca2001,emailAddress=support@fortinet.com	RSA	Fortinet	2056/05/27 13:48:33	Factory	⊕
˅ Certificates (1)							
⋮	default	C=US,ST=California,L=Sunnyvale,O=Fortinet,OU=FortiDATA,CN=FDTVM1TM24090001,emailAddress=support@fortinet.com	RSA	Fortinet	2056/05/26 13:48:33	Factory	
˅ Remote Certificates (0)							

   - *Add New Certificate*—Import a certificate using certificate file and key file
   - *Import Existing Certificate .zip File*—Import an existing certificate .zip file
3. Click *BROWSE* to select the certificate file and key file or the certificate `.zip` file from your local directory.
4. **(Optional)** Specify a passphrase, if needed.
5. Click *IMPORT*.
6. Click *Close*.

To apply the customized TLS certificate, go to the *System > Settings > General on page 52* tab.

To import a new remote certificate:

1. Go to *System > Settings > Certificates*.
2. Click *Import Certificate > Add New Remote Certificate*.



	Name	Subject	Comment	Issuer	Expi		rt
CA Certificates (3)							
⋮	Fortinet_CA	C=US,ST=California,L=Sunnyvale,O=Fortinet,OU=Certificate Authority,CN=support,emailAddress=support@fortinet.com	RSA	Fortinet	203		
⋮	Fortinet_CA2	C=US,ST=California,L=Sunnyvale,O=Fortinet,OU=Certificate Authority,CN=fortinet-ca2,emailAddress=support@fortinet.com	RSA	Fortinet	2056/05/27 13:27:39	Factory	⊕
⋮	Fortinet_Sub_CA2	C=US,ST=California,L=Sunnyvale,O=Fortinet,OU=Certificate Authority,CN=fortinet-subca2001,emailAddress=support@fortinet.com	RSA	Fortinet	2056/05/27 13:48:33	Factory	⊕
Certificates (1)							
⋮	default	C=US,ST=California,L=Sunnyvale,O=Fortinet,OU=FortiDATA,CN=FDTVM1TM24090001,emailAddress=support@fortinet.com	RSA	Fortinet	2056/05/26 13:48:33	Factory	
Remote Certificates (0)							

3. Click *BROWSE* to select the Base64(PEM) certificate file (`.cer` or `.crt`) from your local directory. The first character cannot be "." or "-".
4. Click *IMPORT*.
5. Click *Close*.

FortiGuard

FortiData uses the following FortiGuard packages:

- **AI Classification Model**—For machine learning classification of the documents.
- **NLP Model**— For recognizing data types from the target files.
- **Data Type Database**—For data type definition, including keyword, regex patterns, predefined rule templates and other related attributes.

You must have the corresponding license to upgrade these packages..

Services could be renewed via Fortinet authorised partners and distributors.

Registering or renewing the service

Upon purchasing services from your reseller, you will receive the service registration document by email, which includes the service title and summary, such as the contractor registration code. Then follow steps below:

1. Log into Fortinet Support at *support.fortinet.com*.
2. Click *Register/Renew*.
   If you have not registered your FortiData account, enter the serial number to register it. If you have registered your FortiData account, you can see the information from *System > FortiGuard Information*.
3. Enter your Contract Registration Code (find the code from the Service Entitlement Summary).

Upgrading FortiGuard packages

To manually upgrade the FortiGuard packages:

1. Obtain the package files from Fortinet Support.
2. In the *System > FortiGuard Information* page, click *Upgrade*。
3. Click *Browse* to select the package file and click *Upload*.
4. Click *Apply*.

To automatically upgrade the FortiGuard packages:

1. In the *System > FortiGuard Information > FortiData Model & Data Type Database Updates* section, enable *Schedule Updates*.
2. Configure the update schedule as needed.
3. Click *Apply*.

You can also manually do it using the *Update AI Classification, NLP and Data Type Definitions* button.

Configuring FortiGuard server

The FortiGuard server is used for license validation. You can customize the FortiGuard server in the following ways:

- Override the FortiGuard server by selecting the *Override FortiGuard Server* option and specifying a custom FortiGuard server.
- Configure FortiData to connect through an explicit (non-transparent) web proxy server to the FortiGuard Distribution Network (FDN) if you cannot connect to it directly. The FortiData will then connect to the proxy using the HTTP CONNECT method, as described in RFC 2616 (http://tools.ietf.org/rfc/rfc2616.txt).

To use explicit proxy for FortiGuard server:

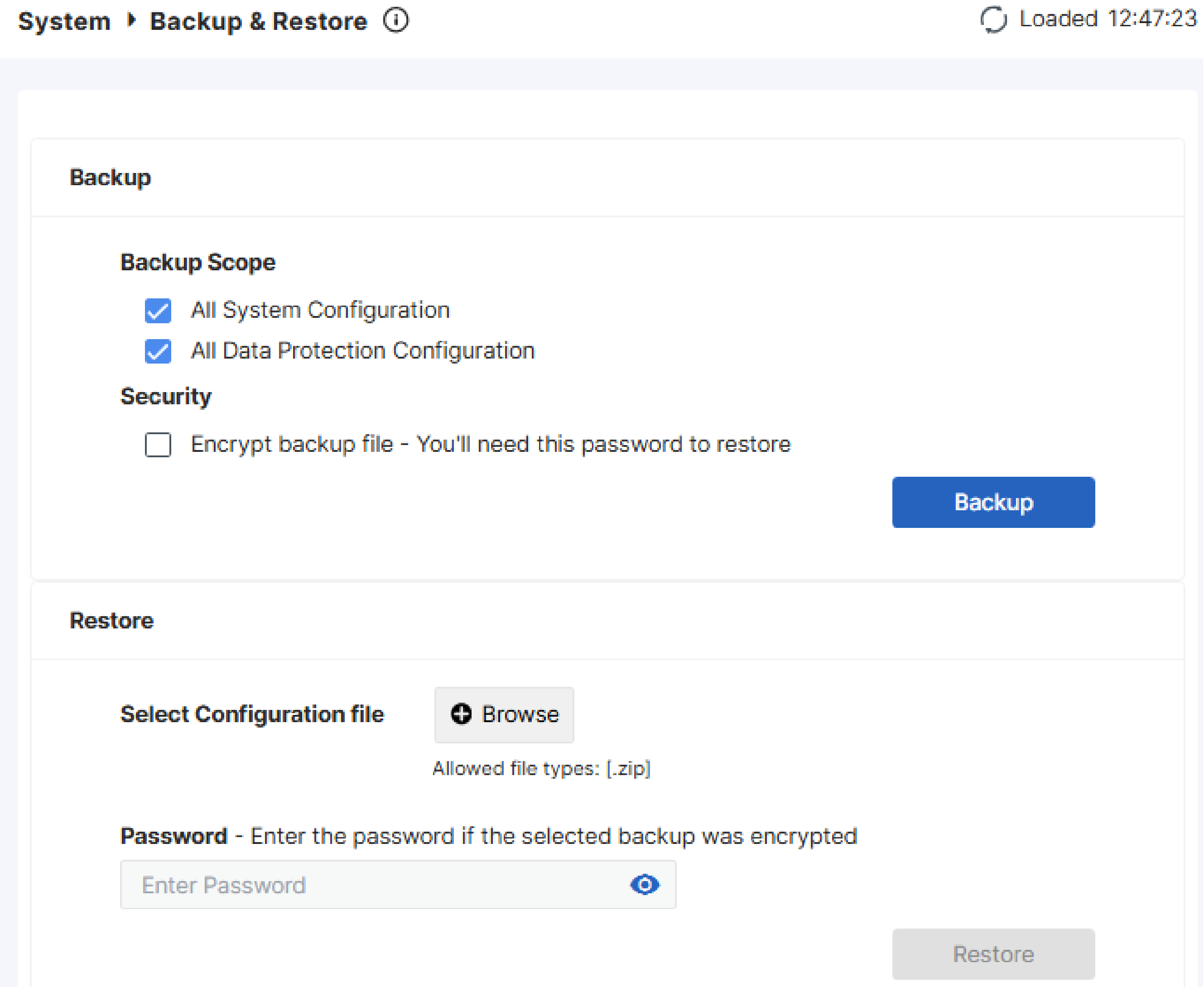
a. Go to *System > FortiGuard*.
b. Enable *Use Explicit Proxy for FortiGuard Server*.
c. Configure the following options:

Proxy Address	Enter either the IP address or fully qualified domain name (FQDN) of the web proxy.
Proxy Port	Enter the port number on which the web proxy listens for connections.
Username	If the proxy requires authentication, enter the FortiData's login name on the web proxy.
Password	If the proxy requires authentication, enter the password for the FortiData's login name on the web proxy.

d. Click *Apply*.

Backup & Restore

Use the *System > Backup & Restore* tab to back up or restore the FortiData configurations.



System ▸ Backup & Restore ⓘ

Loaded 12:47:23

Backup

Backup Scope

☑ All System Configuration

☑ All Data Protection Configuration

Security

□ Encrypt backup file - You'll need this password to restore

Restore

Select Configuration file

Allowed file types: [.zip]

Password - Enter the password if the selected backup was encrypted

To back up the FortiData configurations:

1. In the *Backup* section, select *All System Configuration* and/or *All Data Protection Configuration* (including scans and schedules, policies, data types, and data labels, which are related to data protection).
2. Optionally, enable *Encrypt backup file* to add a password to the backup file. The password is required to restore the system.
3. Click *Backup*.

To restore a saved FortiData configuration:

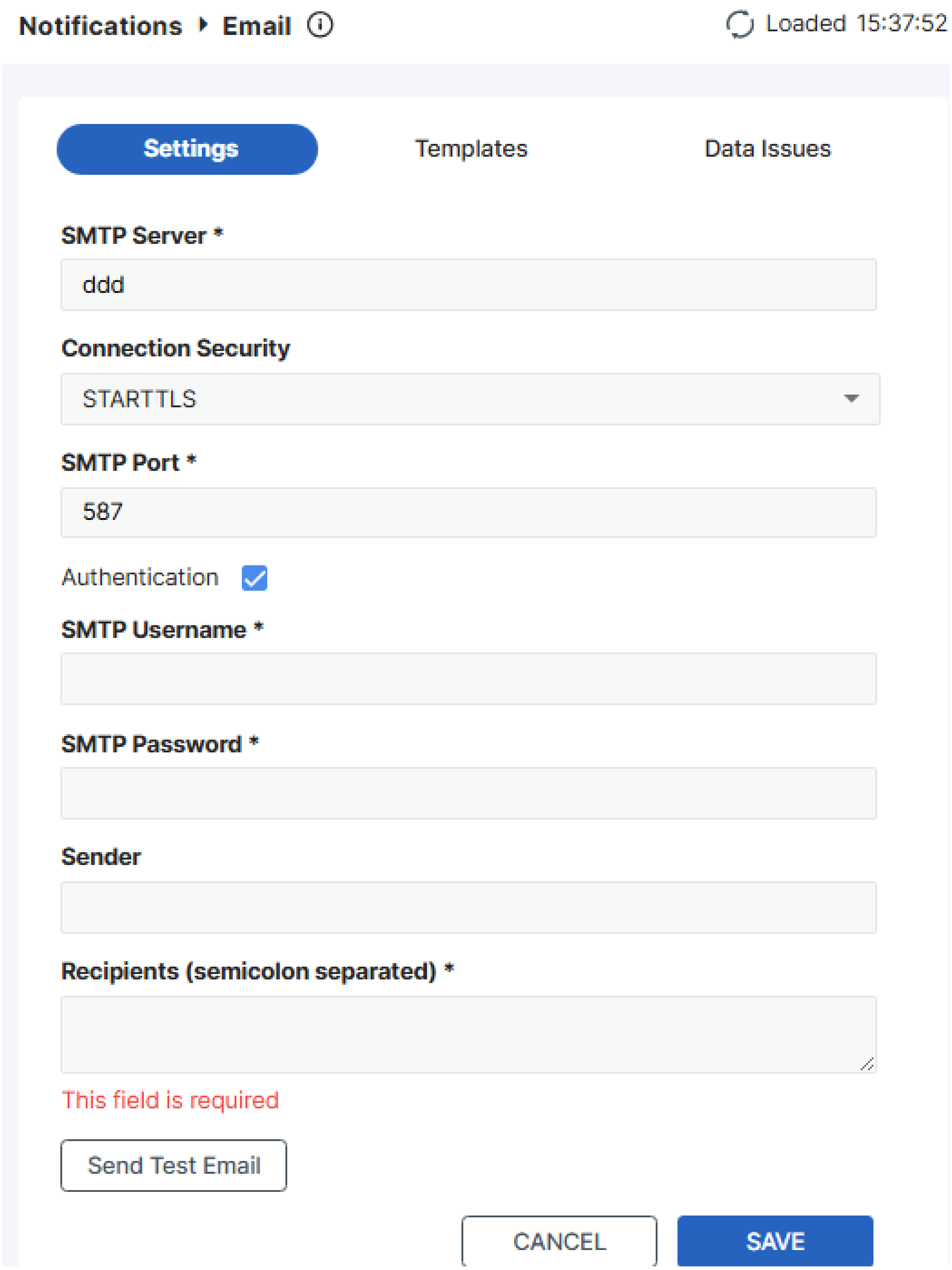
1. In the *Restore* section, click *Browse* to locate and select the saved configuration file (`.zip`).
2. Enter the password if the selected backup was encrypted.
3. Click *Restore*.

Notifications

Use the *Notifications > Email* page to configure email notifications, such as setting up SMTP servers and enabling email notification for data issues using built-in email templates.

To configure an SMTP server:

1. Go to *Notifications > Email > Settings*.
2. Configure the following options:



Notifications ▸ Email ⓘ

Loaded 15:37:52

SMTP Server *

ddd

Connection Security

STARTTLS

SMTP Port *

587

Authentication ☑

SMTP Username *

SMTP Password *

Sender

Recipients (semicolon separated) *

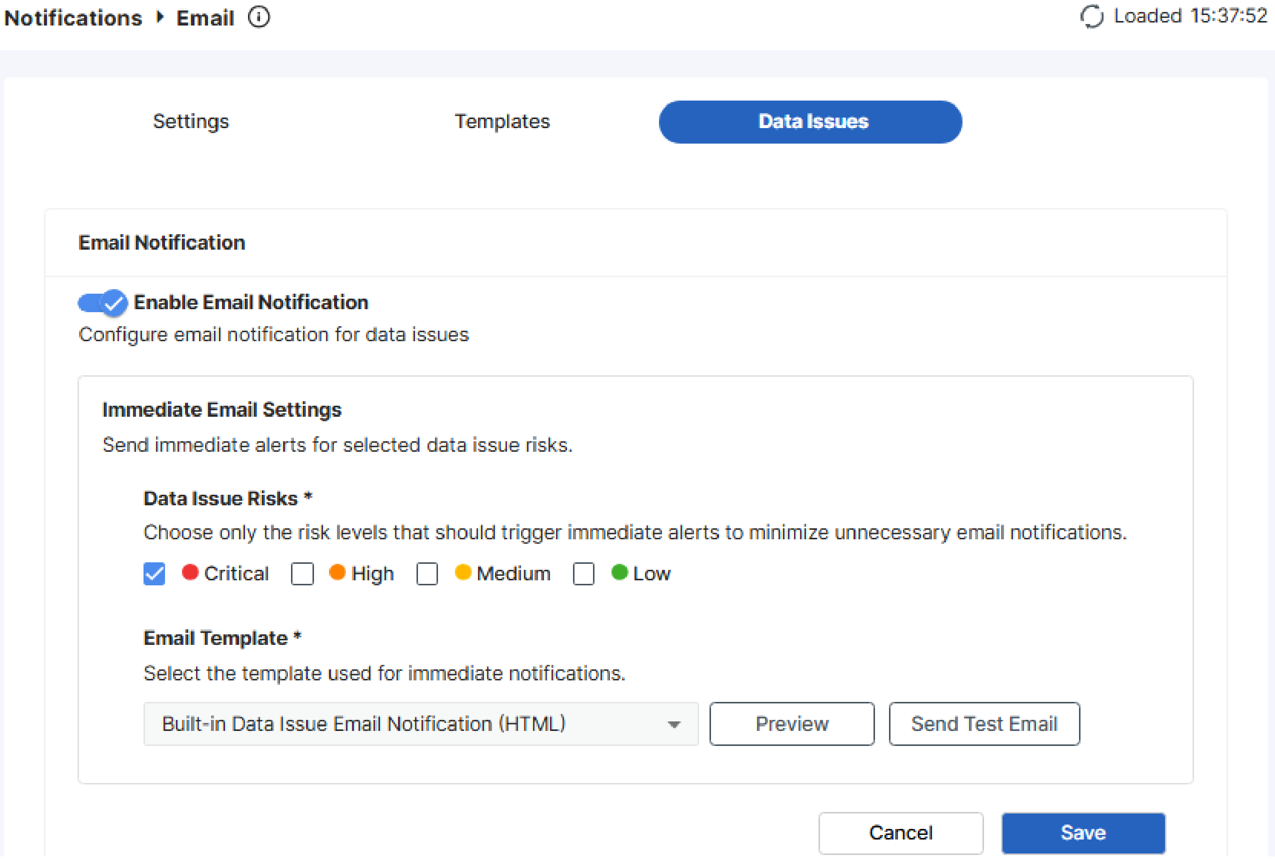
This field is required

SMTP Server	Enter either the IP address or fully qualified domain name (FQDN) of the SMTP server.
Connection Security	Select one of the following: • *None*—Do not use secure connection. • *SMTPS*—Use SMTPS to secure connection. • *STARTTLS*—Use STARTTLS to secure connection.

SMTP Port	Enter the port number on which the SMTP server listens for connections. The default is 587.
Authentication	Enable to require authentication for the SMTP server. You must specify the SMTP username and password.
Sender	Enter the email address of the sender.
Recipients	Enter the email address of recipients. Use semicolons to separate multiple recipients.

3. Click *Send Test Email* to verify that the SMTP server configuration is successful.
4. Click *SAVE*.

To enable email notifications for data issues:

1. Go to *Notifications > Email > Data Issues*.
2. Toggle on *Enable Email Notifications* and configure the following options:
3. 

Notifications ▸ Email ⓘ

Loaded 15:37:52

Settings | Templates | **Data Issues**

Email Notification

☑ **Enable Email Notification**

Configure email notification for data issues

Immediate Email Settings

Send immediate alerts for selected data issue risks.

Data Issue Risks *

Choose only the risk levels that should trigger immediate alerts to minimize unnecessary email notifications.

☑ ● Critical □ ● High □ ● Medium □ ● Low

Email Template *

Select the template used for immediate notifications.

Built-in Data Issue Email Notification (HTML) ▾ | Preview | Send Test Email

Cancel | Save

4. Select the risk level(s) of data issues to trigger email notifications.
5. Select an email template from the list. You can preview to see if it meets your needs. A full list of email templates are also available in the *Notifications > Email > Templates* tab.
6. Click *Send Test Email* to verify that the configuration is successful.
7. Click *Save*.

www.fortinet.com

Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.