

Administration Guide

FortiData 7.6.1



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



November 20, 2025

FortiData 7.6.1 Administration Guide

96-761-1109187-20251120

TABLE OF CONTENTS

Change log	4
Introduction	5
Getting started	6
Dashboard	7
Analytics	10
Summary	10
Files	11
Scan Incidents NEW	13
Discovery	16
Scans	16
Policies	23
Profiles NEW	29
Data Types	31
Standard	31
Custom	31
Documents	35
EDM NEW	40
IDM NEW	42
Templates	43
Data Labels	45
Standard Labels	45
Custom Labels	50
Users	52
Logs & Reports	54
Events	54
Reports NEW	55
Report Settings NEW	56
Log Settings	57
Log Servers	58
System	60
Network	60
Interfaces	60
DNS	62
Static Route NEW	62
Settings	64
FortiGuard NEW	65
Registering or renewing the service	65
Upgrading the package	65
Configuring FortiGuard server	65
Certificates	66
Backup/Restore	67

Change log

Date	Change Description
2025-07-03	Initial release.
2025-11-19	Updated Introduction on page 5.
2025-11-20	Updated Profiles NEW on page 29.

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 adding custom data types.

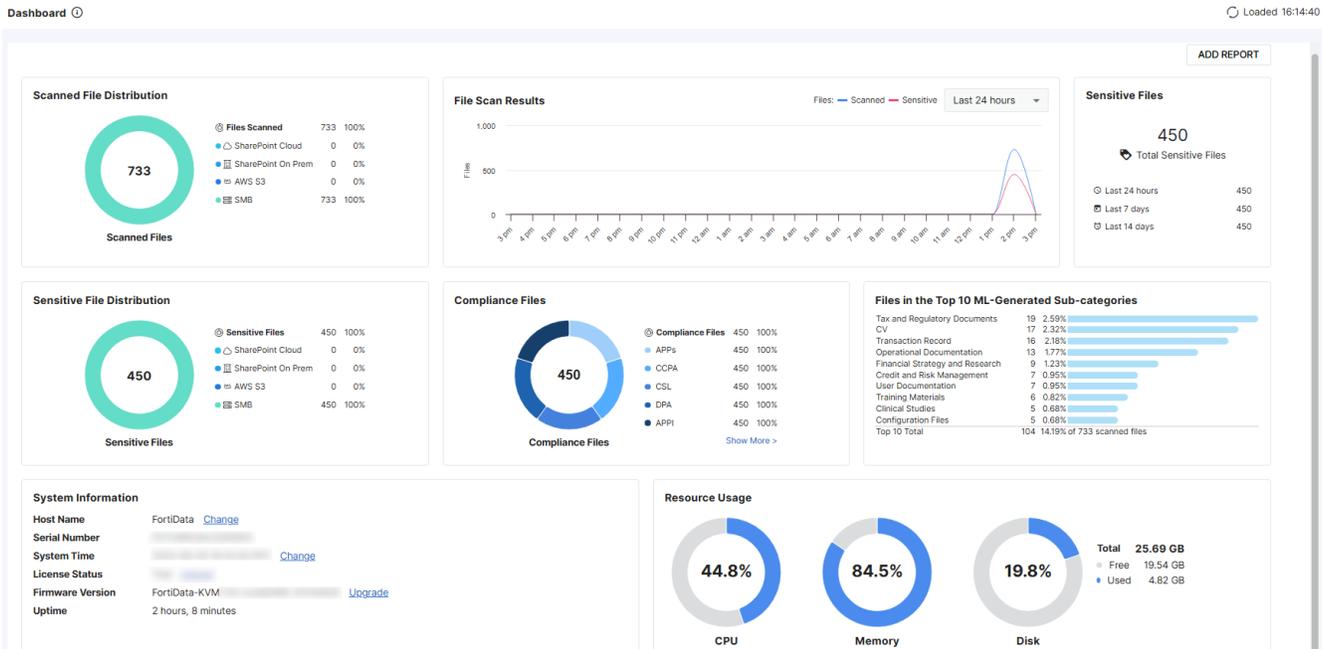
Getting started

Perform the following procedures to get started with FortiData:

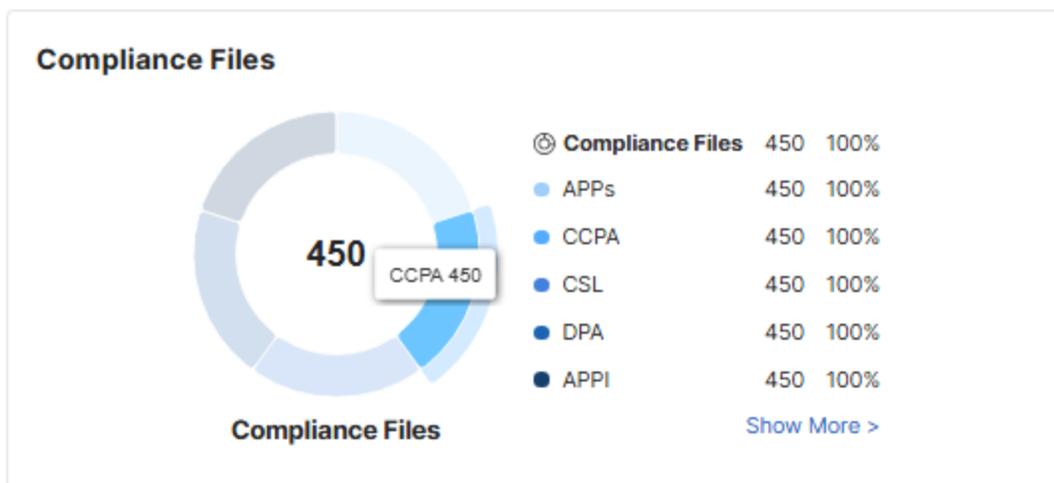
1. Configure interface and DNS settings. See [Network on page 60](#)
2. Configure timeout and system time. See [Settings on page 64](#).
3. Configure HTTPS server certificate. See [Certificates on page 66](#).
4. Create users of with different access scope to FortiData. See [Users on page 52](#).
5. Create discovery policies and scans to look for specific types of data in files of a specific location. See [Scans on page 16](#).

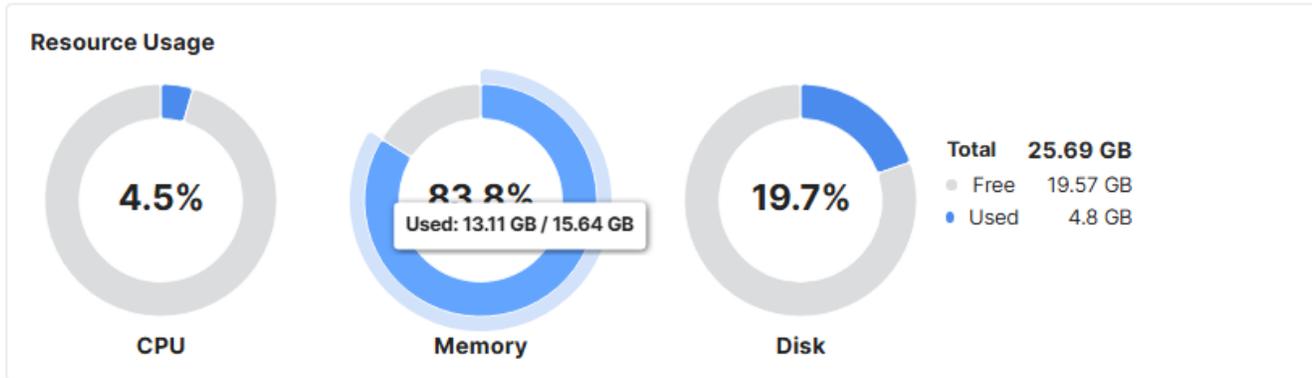
Dashboard

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 dashboard report using the *ADD REPORT* button on the top-right corner. The report will then be available in the *Logs & Reports > Reports NEW on page 55* page.



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





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.

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 64* 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.

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 67*.

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.



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.

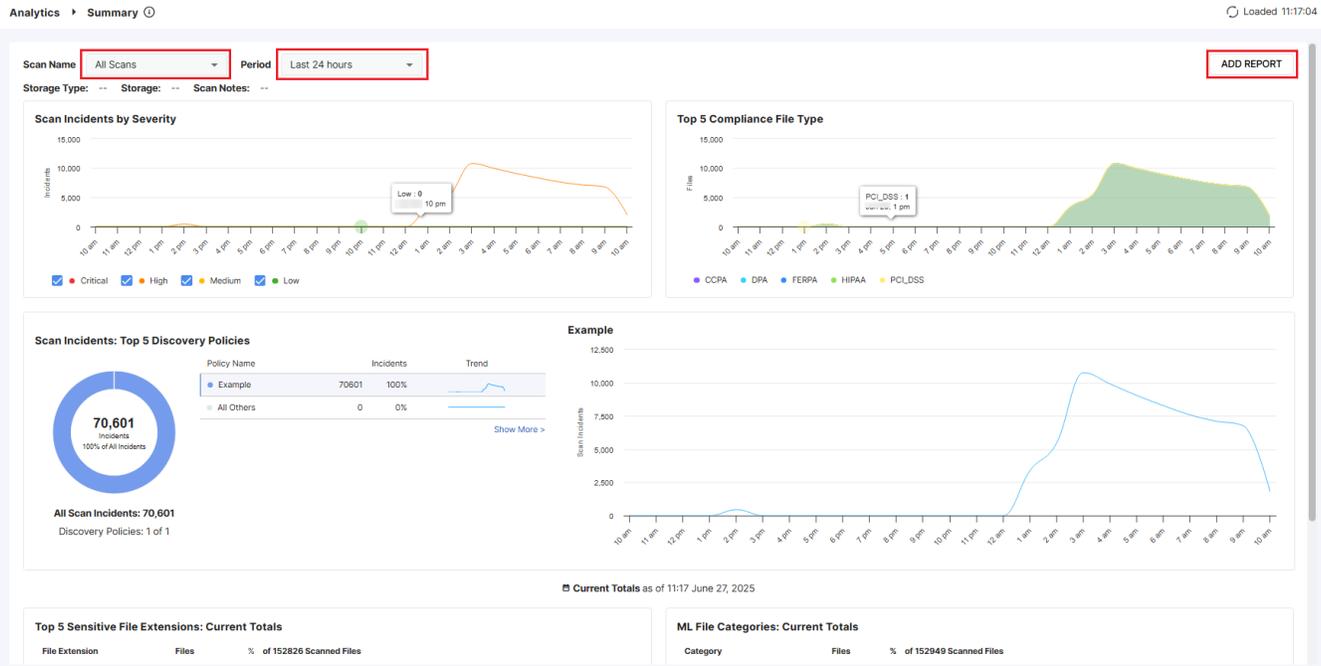
Analytics

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

- [Summary on page 10](#)
- [Files on page 11](#)
- [Scan Incidents NEW on page 13](#)

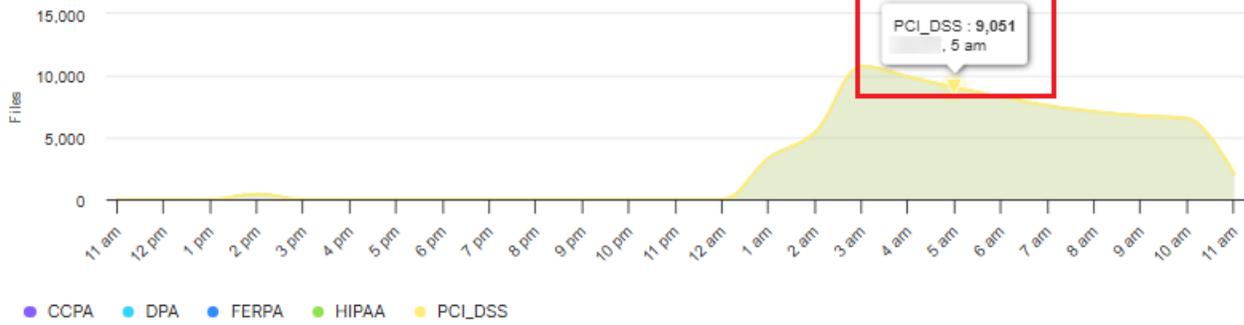
Summary

A summary of scan result is available in the *Analytics > Summary* page with interactive graphs and charts. You can filter the result by scan name and time period. You can also add an analytics summary report using the *ADD REPORT* button on the top-right corner. The report will then be available in the *Logs & Reports > Reports NEW on page 55* page.



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

Top 5 Compliance File Type



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

The screenshot shows the 'Sensitive Files by File Extension' modal window. The table below lists the file extensions and their corresponding counts and percentages of the 166,721 scanned files.

File Extension	Files	% of 166,721 Scanned Files
json	74,656	44.78%
py	1,379	0.83%
pdf	805	0.48%
jpg	117	0.07%
txt	107	0.06%
js	104	0.06%
png	69	0.04%
xlsx	28	0.02%
docx	21	0.01%
csv	20	0.01%
jpeg	12	0.01%
md	12	0.01%
webp	11	0.01%
c	7	0%
doc	6	0%
sh	6	0%

Files

A list of scanned files is available in the *Analytics > Files* 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*.

Analytics > Files ⊙ Loaded 11:23:37

Scanned Files (733) Scan Name Example ▼ Period Last 7 days ▼ EXPORT ▼

Storage Type: SMB Storage: Notes:

Actions ▼ Search / Query by file conditions ⊙

<input type="checkbox"/>	File Name	Standard Data Types	Custom Data Types	ML Category	ML Subcategory	Category Confidence	Labels	Quarantined	Copied	Extension	Size	Storage Type	Storage
<input type="checkbox"/>	...	1	0	Other		60	18 Labels			py	1 KB	SMB	
<input type="checkbox"/>	...	1	0	Other		60	18 Labels			md	1 KB	SMB	
<input type="checkbox"/>	...	1	0	Other		60	18 Labels			tif	293 KB	SMB	
<input type="checkbox"/>	...	1	0	Other		60	18 Labels			php	1 KB	SMB	
<input type="checkbox"/>	...	1	0	Other		60	18 Labels			go	1 KB	SMB	
<input type="checkbox"/>	...	1	0	Other		60	18 Labels			odp	1 KB	SMB	
<input type="checkbox"/>	...	1	0	Other		60	18 Labels			avif	4 KB	SMB	
<input type="checkbox"/>	...	1	0	Other		60	18 Labels			webp	4 KB	SMB	
<input type="checkbox"/>	...	1	0	Other		60	18 Labels			txt	1 KB	SMB	
<input type="checkbox"/>	...	1	0	Other		60	18 Labels			rtf	1 KB	SMB	
<input type="checkbox"/>	...	1	0	Other		60	18 Labels			gif	5 KB	SMB	
<input type="checkbox"/>	...	1	0	Other		60	18 Labels			png	6 KB	SMB	
<input type="checkbox"/>	...	1	0	Other		60	18 Labels			tiff	15 KB	SMB	
<input type="checkbox"/>	...	1	0	Other		60	18 Labels			java	1 KB	SMB	
<input type="checkbox"/>	...	1	0	Other		60	18 Labels			c++	1 KB	SMB	
<input type="checkbox"/>	...	1	0	Other		60	18 Labels			pdf	1 KB	SMB	
<input type="checkbox"/>	...	1	0	Other		60	18 Labels			inv	7 KB	SMB	

Items per page: 100 ▼ 1 - 100 of 733 < > 1 > >>

To see the assigned labels for a sensitive file, click the link in the *Labels* column.

Analytics > Files ⊙ Loaded 11:41:03

Scanned Files (733) Scan Name Example ▼ Period Last 7 days ▼ EXPORT ▼

Storage Type: SMB Storage: Notes:

Actions ▼ Search / Query by file conditions ⊙

<input type="checkbox"/>	File Name	Standard Data Types	Custom Data Types	ML Category	ML Subcategory	Category Confidence	Labels	Quarantined	Copied	Extension	Size	Storage Type	Storage
<input type="checkbox"/>	...	1	0	Other		60	18 Labels			py	1 KB	SMB	
<input type="checkbox"/>	...	1	0	Other		60	18 Labels			md	1 KB	SMB	
<input type="checkbox"/>	...	1	0	Other		60	18 Labels			tif	293 KB	SMB	

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.

Analytics > Files ⊙ Loaded 11:41:03

Scanned Files (733) Scan Name Example ▼ Period Last 7 days ▼ EXPORT ▼

Storage Type: SMB Storage: Notes:

Actions ▼ Search / Query by file conditions ⊙

<input type="checkbox"/>	File Name	Standard Data Types	Custom Data Types	ML Category	ML Subcategory	Category Confidence	Labels	Quarantined	Copied	Extension	Size	Storage Type	Storage
<input type="checkbox"/>	⋮ PCI_Visa_Card_Number.py	1	0	Other		60	18 Labels			py	1 KB	SMB	
<input type="checkbox"/>	⋮ View Details	1	0	Other		60	18 Labels			md	1 KB	SMB	
<input type="checkbox"/>	⋮ Quarantine File	1	0	Other		60	18 Labels			tif	293 KB	SMB	
<input type="checkbox"/>	⋮ Restore Quarantined File	1	0	Other		60	18 Labels			php	1 KB	SMB	

The screenshot shows the 'Analytics > Files' interface. At the top, there are filters for 'Scanned Files (733)', 'Scan Name' (Example), and 'Period' (Last 7 days). Below this is a table with columns: File Name, Standard Data Types, Custom Data Types, ML Category, ML Subcategory, Category Confidence, and Labels. A modal window titled 'File Details' is open on the right, showing information for a selected file, including File Name, Storage, Updated date, Main Category, Sub Category, Category Confidence, File Path, File Hash, and sections for Standard Data Type Categories and Custom Data Types.

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

This screenshot shows the 'Analytics > Files' interface with the 'Actions' button highlighted in a red box. The table below has additional columns: Quarantined, Copied, Extension, Size, Storage Type, and Storage. The 'Restore Quarantined Files' option is also highlighted in a red box. The top right shows 'Loaded 11:41:03' and an 'EXPORT' button.

Scan Incidents NEW

Scan incidents log data is available in the *Analytics > Scan Incidents* page. You can filter the logs by scan name, time period, and queries with various conditions. Retention period of scan incidents logs can be configured in *Logs & Reports > Log Settings on page 57*.

- 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 > Scan Incidents Loaded 10:47:50

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

Storage Type: SMB Storage: Notes:

Actions Search / Query

Time	File Name	Severity	Status	Mark As Ignored	False Positive	Labels
2025-10-27 10:47:50	...	High	New	No	No	18 Labels
2025-10-27 10:47:50	...	High	New	No	No	18 Labels
2025-10-27 10:47:50	...	High	New	No	No	18 Labels
2025-10-27 10:47:50	...	High	New	No	No	18 Labels
2025-10-27 10:47:50	...	High	New	No	No	18 Labels
2025-10-27 10:47:50	...	High	New	No	No	18 Labels
2025-10-27 10:47:50	...	High	New	No	No	18 Labels
2025-10-27 10:47:50	...	High	New	No	No	18 Labels
2025-10-27 10:47:50	...	High	New	No	No	18 Labels
2025-10-27 10:47:50	...	High	New	No	No	18 Labels
2025-10-27 10:47:50	...	High	New	No	No	18 Labels
2025-10-27 10:47:50	...	High	New	No	No	18 Labels
2025-10-27 10:47:50	...	High	New	No	No	18 Labels
2025-10-27 10:47:50	...	High	New	No	No	18 Labels
2025-10-27 10:47:50	...	High	New	No	No	18 Labels

Items per page: 100 1 - 100 of 73617

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

Analytics > Scan Incidents Loaded 10:47:50

Scan Incidents () Scan Name my scan Period Last 7 days EXPORT

Storage Type: SMB Storage: Notes:

Actions Search / Query

Time	File Name	Severity	Status	Labels
2025-10-27 10:47:50	...	High	New	18 Labels
2025-10-27 10:47:50	...	High	New	18 Labels
2025-10-27 10:47:50	...	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 () Scan Name my scan Period Last 7 days EXPORT

Storage Type: SMB Storage: Notes:

Actions Search / Query

Time	File Name	Severity	Status	Mark As Ignored	False Positive	Labels
2025-10-27 10:47:50	...	High	New	No	No	18 Labels
2025-10-27 10:47:50	...	High	New	No	No	18 Labels
2025-10-27 10:47:50	...	High	New	No	No	18 Labels

View Details

Delete

The screenshot displays the 'Analytics > Scan Incidents' page. At the top, there are filters for 'Scan Name' (my scan) and 'Period' (Last 7 days). Below this is a table of scan incidents with columns for 'Time', 'File Name', 'Severity', 'Status', 'Mark As Ignored', 'False Positive', and 'La'. A modal window titled 'Scan Incident Details' is open on the right, showing information for a specific incident. The modal includes fields for Time (2025), Severity (High), File Name, Data Source Type (SMB), File Path (root/), File Hash, File Size (1 KB), File Owner, Scan Name (my scan), Scan Create Time (2025), Discovery Policy Name (Example), and Discovery Rule Name (Example). It also lists 'Assigned Labels (18)' including APPI, CCPA, APPs, CSL, DPA, FERPA, FISMA, GLBA, GDPR, HIPAA, LGPD, NIST 800-53 and NIST 800-171, and PCLDSS. A 'CLOSE' button is at the bottom right of the modal.

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

This screenshot shows the same 'Analytics > Scan Incidents' page, but with the 'Actions' dropdown menu open. The menu options are: Delete, Change Severity, Change Status, Mark As Ignored, Unmark Ignored, Mark As False Positive, and Unmark False Positive. The table below the menu shows several incidents with a severity of 'High' and status of 'New'. The 'Actions' button is highlighted with a red box.

Discovery

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

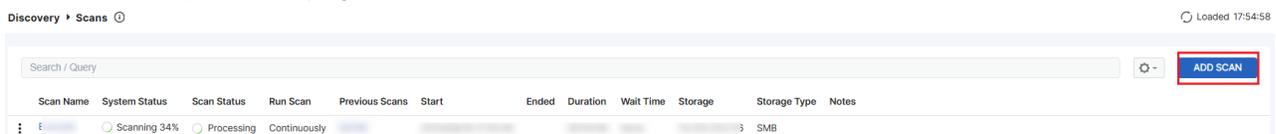
1. Create data discovery policies to look for specific types of data (using data types) in files and assign specific tags (using data labels) to files that meet the specified conditions. See [Policies on page 23](#).
2. Create data discovery profiles to copy or quarantine sensitive files to a specific local or remote folder. See [Profiles NEW on page 29](#).
3. 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. See [Scans on page 16](#).
4. View scan and classification results in the [Analytics on page 10](#) 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 10](#) pages. You can create up to 16 scans.

To create a scan:

1. In the *Discovery > Scans* page, click **ADD SCAN**.



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

Add Scan ⓘ
✕

- Start
- Catalog
- Files
- Policies
- Protection Profiles
- Save

Start Add Scan

Scan Name *

Storage Type *

Schedule

Consider network performance when scheduling scans of large data sets.

Wait Time Between File Downloads * ⓘ

Run Scan * Hour *

Notes

CANCEL
NEXT >

- a. Specify the scan name.
- b. Select the storage type from one of the following:
 - *AWS Bucket*
 - *SharePoint Cloud*
 - *SharePoint On Prem*
 - *SMB—Samba*
- c. Specify the authentication details for the target location. For the following scan types, the user or application must have all the required permissions.

Scan Type	Required Permission(s)	
<i>AWS Bucket</i>	<i>AmazonS3FullAccess</i>	
<i>SharePoint Cloud</i>	When using token authentication, the following permissions are required for FortiData to access the necessary APIs.	
Permission	Type	Description
Microsoft Graph		
<i>Application.Read.All</i>	Application	Read all applications.
<i>AuditLog.Read.All</i>	Application	Read all audit log data.
<i>Directory.Read.All</i>	Application	Read directory data.
<i>Files.ReadWrite.All</i>	Application	Read and write files in all site

Scan Type	Required Permission(s)		
	Permission	Type	Description
			collections.
	<i>Group.Read.All</i>	Application	Read all groups.
	<i>GroupMember.Read.All</i>	Application	Read all group memberships.
	<i>Organization.Read.All</i>	Application	Read organization information.
	<i>People.Read.All</i>	Application	Read all users' relevant people lists.
	<i>Reports.Read.All</i>	Application	Read all usage reports.
	<i>Sites.FullControl.All</i>	Application	Have full control of all site collections.
	<i>Sites.Manage.All</i>	Application	Create, edit, and delete items and lists in all site collections.
	<i>Sites.ReadWrite.All</i>	Application	Read and write items in all site collections.
	Office 365 Management APIs		
	<i>ActivityFeed.Read</i>	Application	Read activity data for your organization. This permission is required only if <i>Enable Monitor Audit Logs</i> is enabled.

- d. Click **TEST CONNECTION** to verify the connection is successful.
- e. 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.

- f. Configure the scan frequency to be daily or weekly or continuously. For daily and weekly scans, you can specify the hour or day when the scan is scheduled to run.
 - g. Add notes as needed.
 - h. Click **NEXT**.
3. Configure the scan folders and click **NEXT**.

Add Scan ? ✕

Scan Name: my scan **Storage Type:** SMB **Storage:** ██████████ **Share Name:** root

Folders Select the top-tier folders that you want to scan for sensitive data.

Search

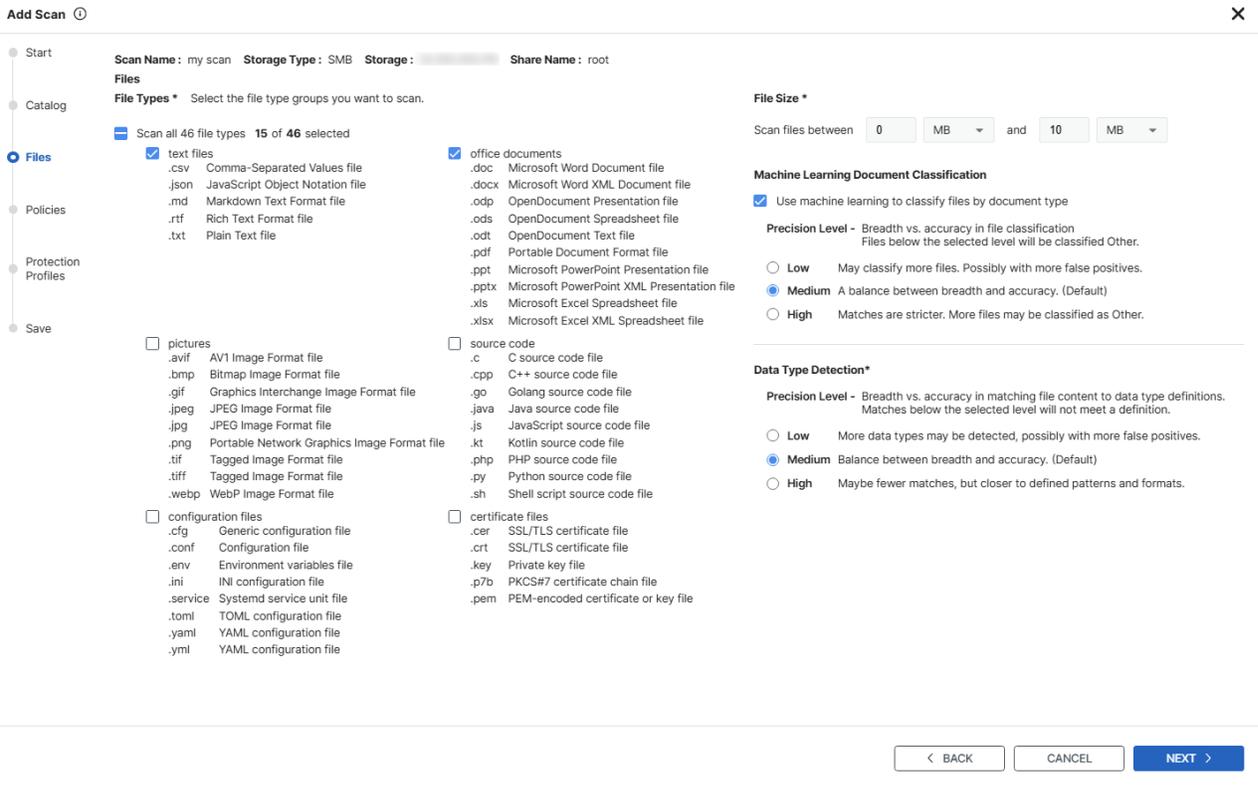
0 of 72 top-tier folders selected All Folders Select Current Page

- .cache
- .config
- .gnupg
- .local
- .mozilla
- .pcsc12
- .pki
- .ssh
- .thunderbird
- .vim
- AllFileTypes
- Baojun
- C.JL
- Copy File

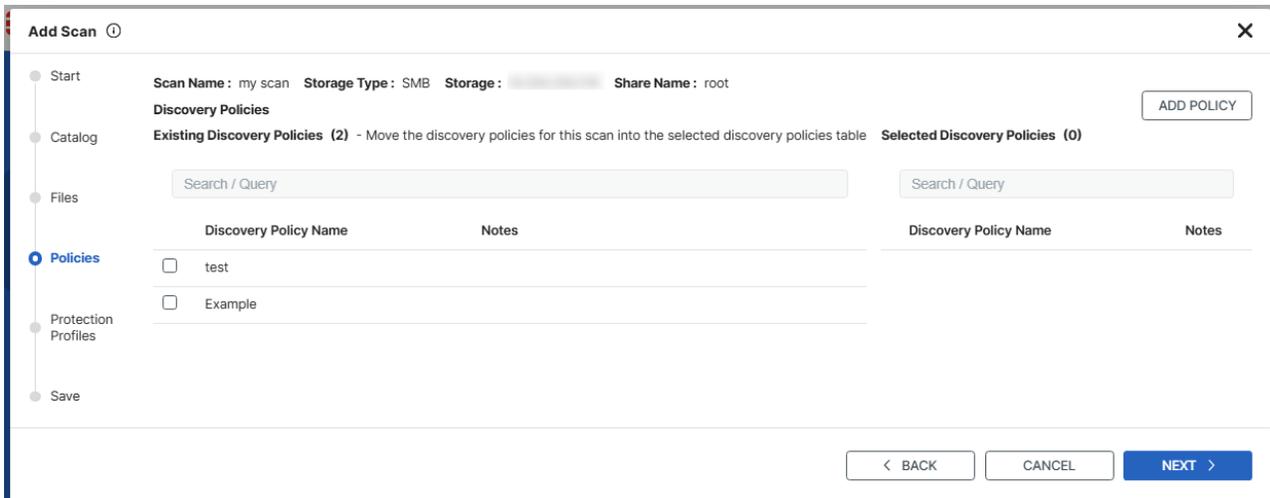
Items per page: 1 - 50 of 72 << < > >>

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.



5. Click **NEXT**.
6. Select the discovery policies to apply to the scan and click **NEXT**.



7. Select the copy and quarantine profile (see [Profiles NEW on page 29](#)) to handle sensitive files as needed and click **NEXT**.

Add Scan ⓘ

✕

- Start
- Catalog
- Files
- Policies
- Protection Profiles**
- Save

Scan Name : my scan **Storage Type :** SMB **Storage :** [REDACTED] **Share Name :** root

Protection Profiles

Copy Profile

Quarantine Profile

< BACK CANCEL NEXT >

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

Add Scan ⓘ
✕

- Start
- Catalog
- Files
- Policies
- Protection Profiles
- **Save**

Review and Save

Start ✎ Edit

Scan Name	Storage Type	Storage	Notes
my scan	SMB		

Schedule ✎ Edit

Short wait time between file downloads: 10ms. Run Daily 1:00 AM

Catalog ✎ Edit

Scan 72 of 72 top-tier folders

Files ✎ Edit

Types: 5 text files, 10 office documents, 9 source code

ML Document Classification: Enabled

Document Classification Precision Level: Medium

Data Type Detection Precision Level: Medium

Scan files: Between 0 MB to 10 MB

Discovery Policies ✎ Edit

Policies: 1

Total Rules: 1

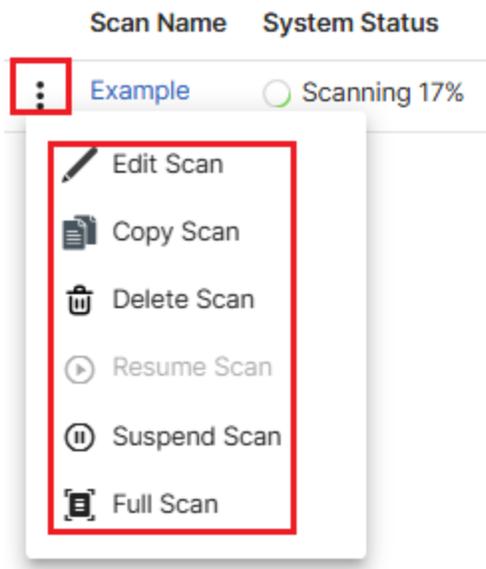
Protection Profiles ✎ Edit

Copy Profile: -

Quarantine Profile: -

< BACK
CANCEL
DONE

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 10](#).



- 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

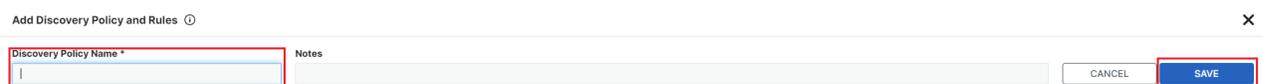
On the *Discovery > Policies* page, you can create data discovery policies to look for specific types of data (using [Data Types on page 31](#)) in files and assign specific tags (using [Data Labels on page 45](#)) to files that meet the specified conditions.

To create a discovery policy:

1. Go to *Discovery > Policies*.
2. Click **ADD DISCOVERY POLICY**.

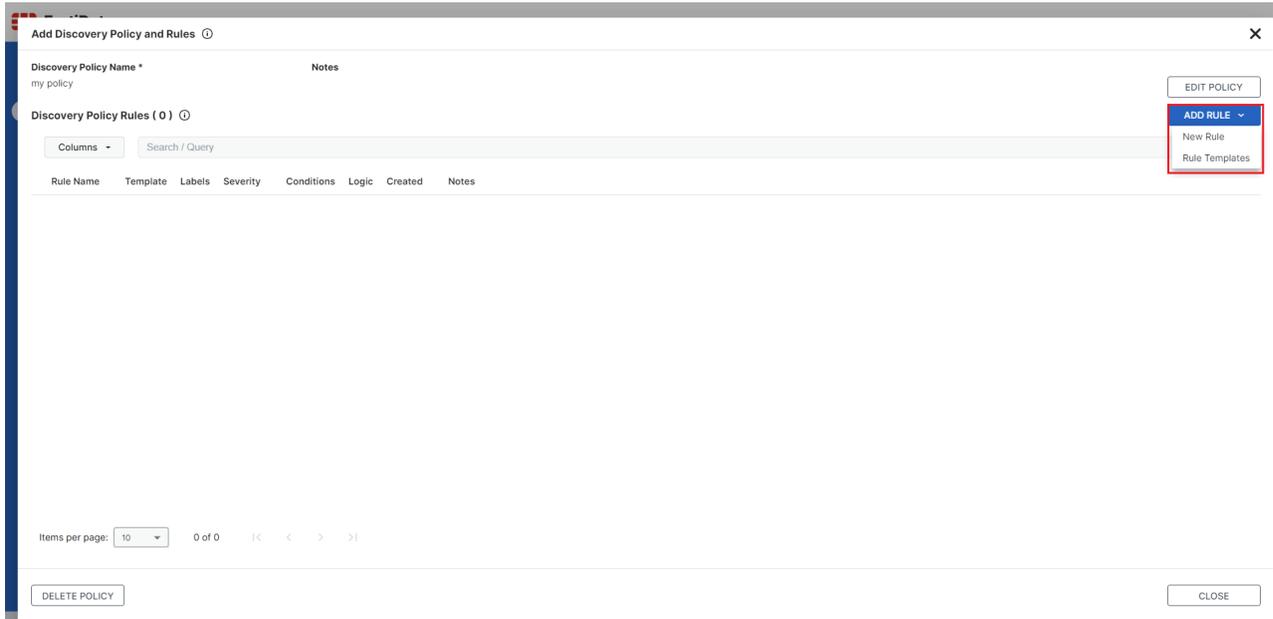


3. Specify the policy name and any notes, and then click **SAVE**.

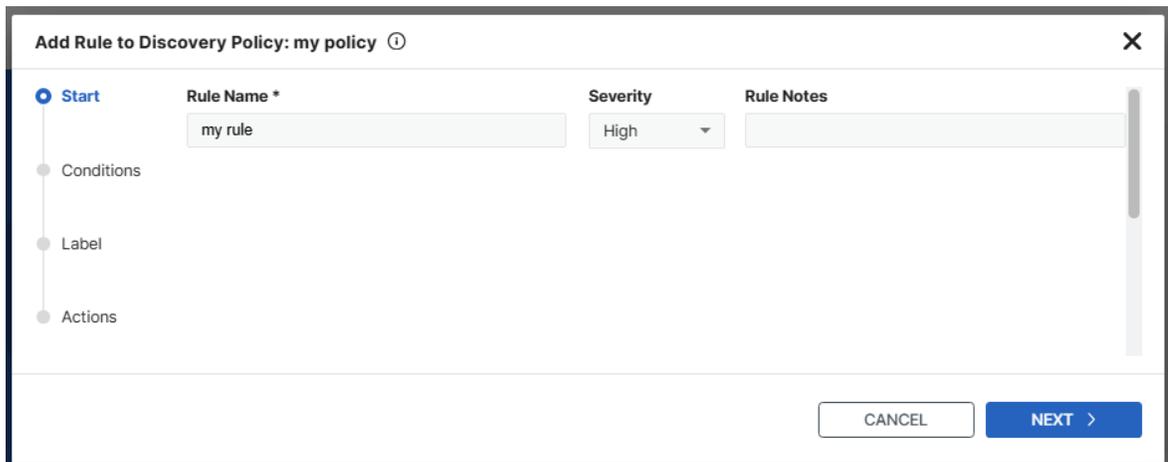


4. Click **ADD RULE** and select *New Rule* or *Rule Templates*, depending on whether you want to create your own data discovery rule or use a rule template predefined in FortiData.

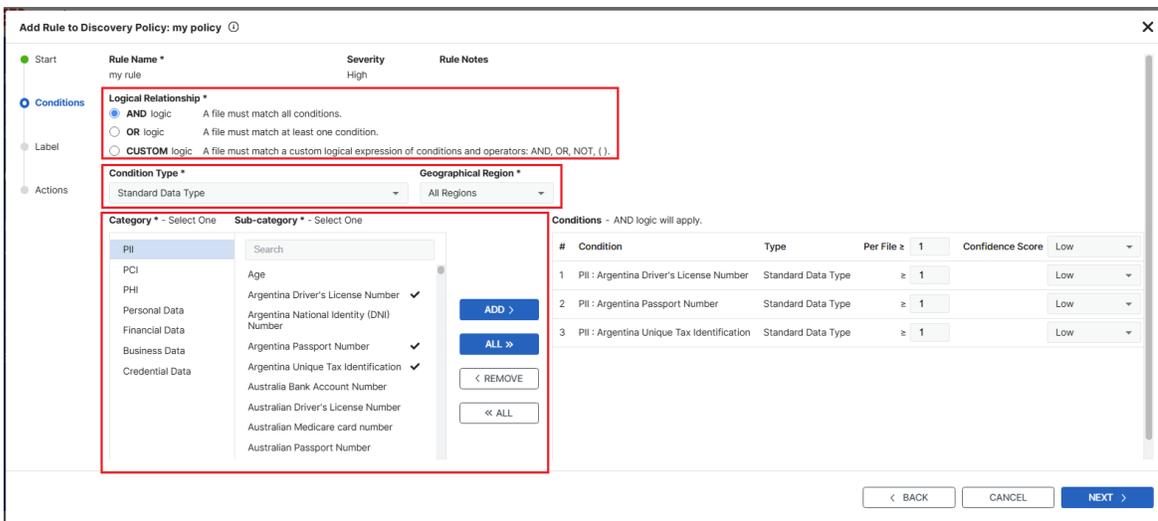
A rule is a defined data pattern with a set of data types and logic conditions that a discovery policy maps to when recognizing patterns in files. You can view the full list of rule templates in the *Rule Templates* tab in the [Data Types on page 31](#) page,



- To create a new rule:
 - i. Specify the rule name and severity. Add notes, if needed.



- ii. Configure the following options in the *Conditions* page:



Option	Description
<i>Logical Relationship</i>	<p>Select from the following logic options:</p> <ul style="list-style-type: none"> • AND—A file must match all conditions to be considered a match. • OR—A file must match at least one condition to be considered a match. • CUSTOM—A file must match a custom logical expression of conditions and operators: AND, OR, NOT, () to be considered a match.
<i>Condition Type</i>	<p>Select from the following condition types:</p> <hr/> <div style="display: flex; align-items: center;"> <p>The full list of data types under each condition type (except for <i>File Type</i>) can be found in the corresponding tab in the Data Types on page 31 page.</p> </div> <hr/> <ul style="list-style-type: none"> • Standard Data Type—The condition is based on standard data types predefined in FortiData, such as PII, PCI, and PHI. You can also further select the geographic region for the data types to narrow down the matching criteria. • Custom Data Type Group—Data type groups that you created. • ML Classified Document Type—List of data types that are created and dynamically updated by FortiData based on machine learning algorithms. • NEW Exact Data Match—EDM data types that you created. • NEW Indexed Document Match—IDM data types that you created. • NEW File Extension—Choose from the following file extensions:

Option	Description
	<ul style="list-style-type: none"> • Text Files—Select from the following file extensions: .csv, .json, .rtf, .txt. • Office Documents—Select from the following file extensions: .doc/.docx, .odp/ods/odt, .pdf, .ppt/pptx, .xls/xlsx. • Pictures—Select from the following file extensions: .avif, .bmp, .gif, .jpeg/jpg, .png, .tif/.tiff, .webp. • Source Code—Select from the following file extensions: .c/.cpp, .go, .java, .js, .kt, .php, .py, .sh. • Configuration files—Select from the following file extensions: .cfg, .conf, .env, .ini, .service, .toml, .yaml/.yml. • Certificate files—Select from the following file extensions: .cer, .crt, .key, .p7b, .pem. • File Type—Choose from the following file types: <ul style="list-style-type: none"> • Office Documents—Select from the following file types: .doc/.docx, .odp/ods/odt, .pdf, .ppt/pptx, .xls/xlsx. • Pictures—Select from the following file types: .avif, .bmp, .gif, .jpeg/jpg, .png, .tif/.tiff, .webp. • Text Files—Select from the following file types: .csv, .json, .md, .rtf, .txt. • Other—Select from the following file types: <ul style="list-style-type: none"> • Generic binary file with unknown or arbitrary content type • Plain text file with an ambiguous or unrecognized file extension
<ul style="list-style-type: none"> • <i>Category/Sub-category</i> • <i>Group Name/Data Type</i> <p>Note - This option is specific to the <i>Custom Data Type Group</i> condition type.</p>	<ul style="list-style-type: none"> • Select a category/group and then select any sub-categories/data types and click ADD CONDITION to add to the conditions list as matching criteria. • To add all subcategories/data types of a category or group, select the category or group and click ADD ALL. • You can also remove a specific condition by selecting it and clicking REMOVE. • To remove all added conditions, click REMOVE ALL.
<p><i>Match Criteria</i></p>	<p>For <i>Standard Data Type</i> and <i>Custom Data Type Group</i> condition types, you can configure the following thresholds:</p> <ul style="list-style-type: none"> • The number of times the condition must match in the file in order to flag the file and perform the defined action. • The confidence score of the match. A result is considered a match only if the confidence score exceeds the specified threshold.

Option	Description
	For <i>File Type</i> and <i>Machine Learning Document Classification Type</i> condition types, the match criteria is always exact match.

- iii. Add or remove conditions as needed.
 - iv. Click *NEXT*.
- To add a rule based on the FortiData templates:
 - i. Specify the region and severity for the rule template and select the categories and sub-categories from the rule template list, as needed.

Add Rule to Discovery Policy: my policy

Choose Rule Templates Check at least one template

Regions *
All Regions

Rule Name *
Argentina PII

Severity
Medium

Notes

Template Description
Argentina PII - Personal Identifiable Information regulations in Argentina, governing the collection, use, and protection of individuals' personal data to ensure privacy and security.

Conditions - Click to enable or disable a condition. Set the Per File and Confidence Score match criteria for each enabled condition.

#	Conditions (3 of 3)	Per File \geq	Confidence Score	Custom	\geq	Type
1	Argentina Driver's License Number	\geq 1	Custom	\geq 0	Standard Data Type	
2	Argentina National Identity (DNI) Number	\geq 1	Custom	\geq 0	Standard Data Type	
3	Argentina Passport Number	\geq 1	Custom	\geq 0	Standard Data Type	

Logical Expression - If the list of enabled conditions changes, this logic expression will be updated automatically
1 OR 2 OR 3

CANCEL NEXT

- ii. Click *NEXT*.

5. Define the labels to apply to files that match the selected conditions and click *NEXT*.

Add Rule to Discovery Policy: my policy

Start

Conditions

Label

Actions

Rule Name *
my rule

Severity
High

Rule Notes

Conditions
3

Logical Relationship
AND logic

Apply File Labels - Select the labels to apply to files that match the conditions.

Standard Labels Custom Labels

Automatically apply to files based on ML classification results *
Disable

Search / Query

Available Labels	Status	Description
Sensitivity (5)		
<input type="checkbox"/> Public	Enabled	Information that is intended for public consumption and poses no risk to the organization or individuals if disclosed.
<input type="checkbox"/> Internal	Enabled	Information that is not intended for public disclosure but is not considered sensitive. It is generally shared within the organization or with trusted partners.
<input type="checkbox"/> Confidential	Enabled	Sensitive information that could cause harm to the organization, its customers, or its employees if disclosed without authorization. Access is typically restricted to certain personnel or departments.
<input type="checkbox"/> Highly Confidential	Enabled	Highly sensitive information that, if exposed, could lead to significant financial loss, reputational damage, legal liability, or regulatory sanctions. Access to this data is strictly controlled.
<input type="checkbox"/> Restricted	Enabled	The most sensitive level of information, accessible only to explicitly authorized personnel. Unauthorized access or disclosure could lead to significant legal, financial, or operational consequences.

Selected Labels (0)
To be applied to files that match the conditions.

BACK CANCEL NEXT

Choose from the following types and select labels under each type:



- Use the *Search/Query* box to filter the results. A complete list of each label type is available in the [Data Labels on page 45](#) page.
- Before selecting any labels, make sure the label status is enabled. Otherwise, the label will not be applied to any files even if they match the selected conditions. To enable/disable a label, go to the corresponding tab of [Data Labels on page 45](#).

Label Type	Description
<i>Standard Labels</i>	<p>Predefined labels by FortiData, including machine learning labels. You can choose whether to apply machine learning labels to matching files using the following option.</p> <div style="border: 1px solid #ccc; padding: 5px;"> <p>Apply File Labels - Select the labels to apply to files that match the conditions.</p> <p> <input checked="" type="radio"/> Standard Labels <input type="radio"/> Custom Labels </p> <p>Automatically apply to files based on ML classification results Disable ▾</p> </div> <p>When enabled, ML labels are applied to files based on the FortiData machine learning model. The application of machine learning labels depends on the condition matching of this discovery policy. If there is condition match for a file, FortiData applies machine learning labels in addition to the standard and custom labels as selected by the administrator.</p>
<i>Custom Labels</i>	Custom labels that you created.

6. Apply copy/quarantine actions (defined in [Profiles NEW on page 29](#)) to sensitive files as needed and click *DONE*.

Add Rule to Discovery Policy: my policy ⓘ

- Start
- Conditions
- Label
- **Actions**

Rule Name *
my rule

Severity
High

Rule Notes

Conditions **Logical Relationship**

3 AND logic

Apply File Actions - Select the actions to apply to files that match the conditions.

Copy / Quarantine - Copy / Quarantine profile should be specified in Scan Policy

Enable File Copy / Quarantine

Copy file to a designated folder

Quarantine file to a designated folder

< BACK
CANCEL
DONE

7. Add more rules as needed by repeating steps 4 to 6.
8. Review the policy details and click *CLOSE*.

Edit Discovery Policy and Rules ⓘ
✕

Discovery Policy Name *

my policy

Notes

Discovery Policy Rules (1) ⓘ

Rule Name	Template	Labels	Severity	Conditions	Logic	Created	Notes
⋮ my rule	None	2	● High	3	And		

Items per page: 1 - 1 of 1

⏪
<

>
⏩

Profiles NEW

On the new *Discovery > Profiles* page, you can create a copy or quarantine profile to copy or move sensitive files to a specific directory for further investigation. You can then apply the profile to your scan (see [Scans on page 16](#)) and enable the copy/quarantine action in your discovery policy (see [Policies on page 23](#)).

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.

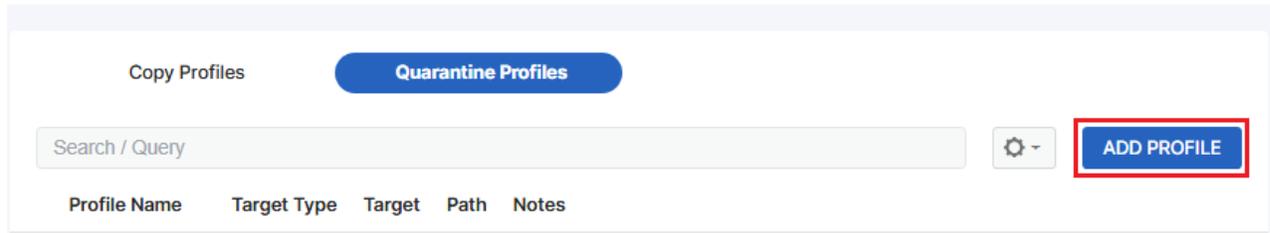


To ensure successful copy and quarantine operations, you must have the following permissions:

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

To create a copy or quarantine profile:

1. Go to *Discovery > Profiles*.
2. In the *Copy Profiles/Quarantine Profiles* tab, click **ADD PROFILE**.

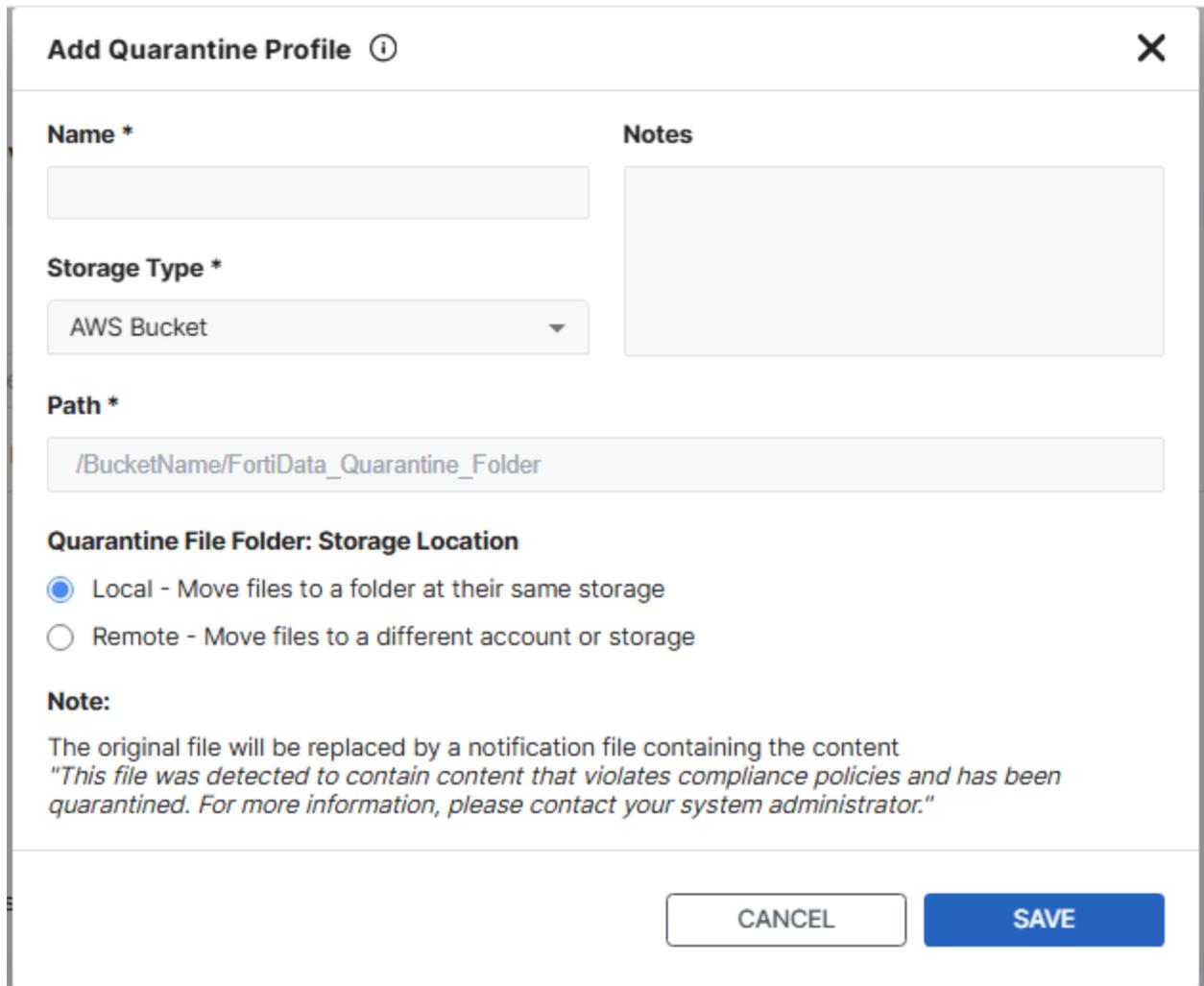


Copy Profiles **Quarantine Profiles**

Search / Query ⚙️ **ADD PROFILE**

Profile Name	Target Type	Target	Path	Notes
--------------	-------------	--------	------	-------

3. Specify the profile name, storage type, destination path, storage location, and any notes, and then click **SAVE**.



Add Quarantine Profile ⓘ ✕

Name * **Notes**

Storage Type *

AWS Bucket ▾

Path *

/BucketName/FortiData_Quarantine_Folder

Quarantine File Folder: Storage Location

Local - Move files to a folder at their same storage

Remote - Move files to a different account or storage

Note:

The original file will be replaced by a notification file containing the content
"This file was detected to contain content that violates compliance policies and has been quarantined. For more information, please contact your system administrator."

CANCEL **SAVE**

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). Use the *Data Types* page to view different categories of data types in FortiData. You can also see a list of predefined rule templates defined for specific data types and regions that meet specific industry needs.

The data types and rule templates can be referenced when you create discovery policies in the [Scans on page 16](#) page.

Standard

The *Standard* page displays a list of predefined data types in FortiData. You can filter the standard data types by region and/or category. You can search the standard data types by name and/or region.

Data Types ▶ Standard ⓘ

Loaded 12:04:00

Region	All Regions	Data Category	All Categories	Search / Query	
Data Category	Name	Description	Type	Created On	Region
Credential Data	ASP.NET Machine Key	The ASP.NET Machine Key is a configuration element used to specify the encryption and validation keys for securing data such as authentication tokens, view state, and cookies in ASP.NET applications.	Regex	2025/	ALL
Credential Data	AWS Access Key	An AWS Access Key is a unique set of credentials consisting of an Access Key ID and a Secret Access Key, used to authenticate and authorize programmatic access to Amazon Web Services (AWS) resources and services.	Regex	2024/	ALL
Credential Data	AWS Secret Access Key	An AWS Secret Access Key is a confidential part of AWS credentials, paired with an Access Key ID, used to securely sign API requests and authenticate programmatic access to AWS services; it must be kept private to protect	Regex	2024/	ALL

Items per page: 50 1 - 50 of 453 << < 1 > >>

Custom

The *Custom* page displays a list of custom data type groups that you defined in FortiData. You can search the custom data type groups by group name and/or notes.

Data Types ▶ Custom ⓘ

Loaded 12:02:34

Custom Data Type Groups  **ADD GROUP**

Group Name	Data Types	Scans	Discovery Policies	Created	Notes
⋮ test	0	0	0		

Items per page: 50 ▼ 1 - 1 of 1 |< < 1 ▼ > >|

Custom data type groups are useful if the system's predefined data type do not meet your needs.

To create a custom data type group:

1. Go to *Data Types > Custom*.
2. Click *ADD GROUP*.

Data Types ▶ Custom ⓘ

Loaded 12:02:34

Custom Data Type Groups  **ADD GROUP**

Group Name	Data Types	Scans	Discovery Policies	Created	Notes
⋮ test	0	0	0		

Items per page: 50 ▼ 1 - 1 of 1 |< < 1 ▼ > >|

3. Specify the group name and notes, if needed.

Add Custom Data Type Group ✕

Group Name *	Notes		
<input type="text"/>	<input type="text"/>	<input type="button" value="CANCEL"/>	<input type="button" value="SAVE"/>

4. Click *SAVE*.
5. Click *ADD DATA TYPE*.

Edit Custom Data Type Group ✕

Group Name * **Notes**

Data Types (0)

Data Type Name ↑	Keywords	Pattern	Notes
------------------	----------	---------	-------

Items per page: 0 of 0 |< < > >|

6. Configure the data type with the following options:

Add Data Type ✕

Data Type Name *

Data Type Notes

Keywords ADD

Pattern*

Regular expressions used to identify content that matches a specified pattern

CANCEL SAVE

- a. Specify the data type name and add notes as needed.
- b. Click *ADD* to define any keywords to look for during file scans.
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.
- c. 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.

d. Click **SAVE**.

7. Add more data types to the group by repeating steps 5-6.

8. Click **CLOSE**.

Documents

The *Documents* page displays a list of AI data types generated by FortiData machine learning. You can search the ML documents by document type.

Data Types ▶ ML Document ⓘ Loaded 12:07:22

Document Type	Description
▼ Finance (8)	
Audit and Assurance Documents	Documents generated during internal or external audit processes to assess financial accuracy, internal controls, and regulatory compliance. These reports provide independent assurance and are critical for corporate governance and risk management.
Credit and Risk Management	Documents involved in assessing and managing credit risk, market risk, etc., such as credit reports, risk assessment reports, and risk management strategies. These documents are important for financial institutions to develop risk controls and mitigation measures.
Expense and Reimbursement Records	Documents that support expense tracking and reimbursement processes. These typically include supporting evidence for employee expenses, management approvals, and payment confirmation. They are frequently used in both internal audits and operational controls.
Financial Report	Used to display the financial status of an individual or organization, including balance sheets, income statements, cash flow statements, and shareholder equity statements. They are critical for investors, management and regulators to understand and assess financial health.
Financial Strategy and Research	Including market research reports, investment strategy documents and industry analysis, etc., used to guide investment decisions and financial product development. This type of document provides financial institutions with market insights based on in-depth analysis and forecasts.
Loan and Financing Agreements	Documents outlining the terms and structure of loans, credit facilities, or other financial arrangements. These define obligations between borrowers and lenders, repayment conditions, interest rates, and covenants, and are central to debt and capital management.
Tax and Regulatory Documents	Documents prepared for tax reporting, compliance with government regulations, and financial oversight. These are critical for ensuring legal compliance and are often submitted to tax authorities or regulatory agencies.
Transaction Record	Includes all documents recording details of financial transactions, such as transaction confirmations, receipts, transfer instructions, and statements. These documents are used to prove the existence, condition, and completion of a transaction.
▼ Healthcare (5)	
Clinical Records	Documents that record patient health information and treatment processes, including medical records, disease course records, surgical records, discharge summaries, examination and test reports, etc. These documents are the basis for medical care decisions and are critical to patient diagnosis, treatment, and follow-up.
Clinical Studies	Clinical research report: records the design, implementation process and result analysis of the clinical trial.
Compliance and Risk Management	Patient Consent: A document in which a patient gives explicit consent to a treatment plan, surgery, or other medical procedure. Privacy Policy: Policies and measures describing how a medical institution protects patients' personal information.
Insurance and Settlement	Documents related to medical expense reimbursement and settlement, such as insurance claim forms, expense statements, and payment records. These documents are critical to processing medical bills and ensuring the financial benefit of providers and patients.
Medication Management	Documentation involving drug prescriptions, medication instructions, and drug monitoring. This includes prescription orders, medication records and adverse drug reaction reports to ensure patients are using their medications safely and effectively.

Main type and sub-types	Description
Finance (8)	
Audit and Assurance Documents	Documents generated during internal or external audit processes to assess financial accuracy, internal controls, and regulatory compliance. These reports provide independent assurance and are critical for corporate governance and risk management.
Credit and Risk Management	Documents involved in assessing and managing credit risk, market risk, etc., such as credit reports, risk assessment reports, and risk management strategies. These documents are important for financial institutions to develop risk controls and mitigation measures.
Expense and Reimbursement Records	Documents that support expense tracking and reimbursement processes. These typically include supporting evidence for employee

Main type and sub-types	Description
	expenses, management approvals, and payment confirmation. They are frequently used in both internal audits and operational controls.
Financial Report	Used to display the financial status of an individual or organization, including balance sheets, income statements, cash flow statements, and shareholder equity statements. They are critical for investors, management and regulators to understand and assess financial health.
Financial Strategy and Research	Including market research reports, investment strategy documents and industry analysis, etc., used to guide investment decisions and financial product development. This type of document provides financial institutions with market insights based on in-depth analysis and forecasts.
Loan and Financing Agreements	Documents outlining the terms and structure of loans, credit facilities, or other financial arrangements. These define obligations between borrowers and lenders, repayment conditions, interest rates, and covenants, and are central to debt and capital management.
Tax and Regulatory Documents	Documents prepared for tax reporting, compliance with government regulations, and financial oversight. These are critical for ensuring legal compliance and are often submitted to tax authorities or regulatory agencies.
Transaction Record	Includes all documents recording details of financial transactions, such as transaction confirmations, receipts, transfer instructions, and statements. These documents are used to prove the existence, condition, and completion of a transaction.
Healthcare (5)	
Clinical Records	Documents that record patient health information and treatment processes, including medical records, disease course records, surgical records, discharge summaries, examination and test reports, etc. These documents are the basis for medical care decisions and are critical to patient diagnosis, treatment, and follow-up.
Clinical Studies	Clinical research report: records the design, implementation process and result analysis of the clinical trial.
Compliance and Risk Management	Clinical research report: records the design, implementation process and result analysis of the clinical trial.
Insurance and Settlement	Documents related to medical expense reimbursement and settlement, such as insurance claim forms, expense statements, and payment records. These documents are critical to processing medical bills and ensuring the financial benefit of providers and patients.

Main type and sub-types	Description
Medication Management	Documentation involving drug prescriptions, medication instructions, and drug monitoring. This includes prescription orders, medication records and adverse drug reaction reports to ensure patients are using their medications safely and effectively.
HR (5)	
CV	Candidate CVs submitted during the recruitment process. It provides quick access to applicants' professional backgrounds, qualifications, and work experience, supporting informed hiring decisions and streamlined candidate evaluation.
Employee Record	Comprehensive records maintained for each employee throughout their lifecycle within the organization. Includes personal information, employment contracts, benefits enrollment, disciplinary records, training history, and separation documentation. These records ensure compliance with labor regulations and support HR operations, audits, and dispute resolution.
Performance Review	Documents related to employee performance evaluations. It helps track individual progress, identify areas for development, and support decisions related to promotions, training, or role adjustments. Consistent performance reviews contribute to employee growth and organizational success.
Recruitment	Documents related to the hiring process, including job requisitions, job descriptions, candidate applications, interview records, background checks, and offer letters. These documents are used to track recruitment activities, evaluate candidate qualifications, and ensure compliance with hiring policies. Proper management of recruitment documentation supports transparency, consistency, and alignment with organizational hiring standards.
Timesheet	Timesheet is used to record and track employee working hours, attendance, and time allocation across projects or tasks. Accurate timesheet documentation supports payroll processing, project management, and compliance with labor regulations.
Information Technology (7)	
Configuration Files	Configuration files containing structured information used to define system settings, application behaviors, or operational parameters. Includes JSON, XML, or YAML configuration files, environment variable definitions, and similar resources designed to facilitate system customization and operation.

Main type and sub-types	Description
Development Documentation	For software developers and project team members, it provides information such as product design, architecture, development specifications, and code samples. Development documentation supports the software development process and promotes effective communication within the team.
Log	Log is dedicated to recording detailed, time-stamped entries related to IT activities, system events, and operational workflows. It provides a chronological history of actions taken, system behavior, or incidents encountered, which is essential for auditing, troubleshooting, and maintaining system integrity.
Operational Documentation	Provides the guidance and processes system administrators and IT professionals need to manage and maintain IT systems. Includes system administration manuals, backup and recovery guides, security protocols and maintenance plans.
Test Documentation	Documentation that records software test plans, test cases, test results, and defect reports. Test documentation is critical to ensuring product quality and identifying and fixing defects.
Training Materials	Training course materials for users, developers, or system administrators designed to improve technical skills and product knowledge. Includes training manuals, online courses and instructional videos.
User Documentation	For end users, it provides detailed guidance on how to use a product or system. Includes user manual, quick start guide, FAQ (Frequently Asked Questions) and use cases. User documentation helps users understand product functionality and use the product effectively.
Legal (4)	
Contracts and Agreements	Formal documents that define the legally binding terms and conditions between two or more parties involved in a transaction or service relationship. This includes agreements such as loan contracts, investment management agreements, service contracts, and insurance policies. These documents specify each party's rights, obligations, responsibilities, and remedies in case of breach.
License Agreement	Legally enforceable contract that allows one party (the licensee) to use certain intellectual property owned by another party (the licensor), such as software, trademarks, patents, or copyrighted content. The agreement specifies terms such as usage scope, payment or royalties, duration, restrictions, and termination clauses, ensuring both parties' rights and responsibilities are clearly defined.

Main type and sub-types	Description
NDA Form	Legal document in which one or more parties agree to maintain the confidentiality of proprietary or sensitive information disclosed during a business or professional relationship. NDAs are designed to protect trade secrets, business plans, technical data, or personal information, and typically outline the scope of confidentiality, duration, and consequences of breach.
Patent	Official legal document granted by a governmental authority that confers exclusive rights to an inventor or applicant to make, use, sell, or license a specific invention for a fixed period (usually 20 years). A patent includes technical descriptions, claims, and drawings that define the scope of legal protection. It serves as a key instrument for protecting intellectual property and promoting innovation.
Source Code (9)	
C#	C# source files (.cs) define classes, methods, and application logic. They are compiled by the .NET runtime and are widely used in Windows applications, games (Unity), and enterprise systems.
C Language	The 'C Language' here refers collectively to both C and C++ source files. C provides low-level programming capabilities, while C++ builds on C with object-oriented features. Their source files typically use extensions such as .c, .cpp, and .h, and are compiled into machine code for high-performance applications.
Golang	Golang source files use the .go extension and start with a package declaration. They are compiled and used to build efficient, concurrent systems such as web servers, APIs, and CLI tools.
Java	Java source files use the .java extension, typically containing a public class matching the filename. They are compiled into bytecode and run on the Java Virtual Machine (JVM) for platform independence.
JavaScript	JavaScript files (.js, .mjs) contain code for browser or server environments. They define variables, functions, and modules, and are widely used for building interactive web applications.
Kotlin	Kotlin source files (.kt, .kts) define classes, functions, and scripts. Interoperable with Java, Kotlin is widely used in Android and backend development for its concise syntax and modern features.
PHP	PHP files (.php) embed code within HTML and are executed server-side. They handle logic, database access, and dynamic content generation for websites and web applications.
Python	Python source files (.py) contain readable, indented code used in scripting, data science, web development, and automation. They are interpreted by the Python runtime environment.

Main type and sub-types	Description
Shell	Python source files (.py) contain readable, indented code used in scripting, data science, web development, and automation. They are interpreted by the Python runtime environment.
Other (1)	
other	Other document

EDM NEW

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 *Data Types > EDM*.
2. Click **ADD DATASET**.



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

Add EDM Dataset and Rules ⓘ

Start

Dataset Name *

Enter Name

Notes

Enter Notes

Upload Data File *

File Requirements:

- Supported format: .csv
- File size limit: 512MB

+ Browse

CANCEL NEXT >

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
...csv

Notes
Check sensitive field names

Identify Sensitive Field Names (0 of 16)

Sensitive *	Field Name	Count	Data Types
<input type="checkbox"/>	SSN	30	
<input type="checkbox"/>	gender	30	
<input type="checkbox"/>	birthdate	30	
<input type="checkbox"/>	maiden name	30	
<input type="checkbox"/>	last name	30	
<input type="checkbox"/>	first name	30	
<input type="checkbox"/>	address	30	
<input type="checkbox"/>	city	30	
<input type="checkbox"/>	state	30	
<input type="checkbox"/>	zip	30	
<input type="checkbox"/>	phone	30	
<input type="checkbox"/>	email	30	
<input type="checkbox"/>	cc_type	30	
<input type="checkbox"/>	CCN	30	
<input type="checkbox"/>	cc_cvc	30	
<input type="checkbox"/>	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

< BACK CANCEL DONE

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

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

IDM NEW

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 indexed of templates using similarity, and determines a match if the similarity exceeds a predefined threshold.

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 *Data Types > 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.

Add IDM Index ⓘ ✕

Index Name *

Notes

Upload Data File *

File Requirements

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

README 2.txt ✓

Templates

The *Templates* page displays a list of predefined rule templates defined for specific data types and regions that meet specific industry needs. You can filter the rule templates by region and/or category. You can search the rule templates by template name.

Data Types

Data Types ▶ Rule Templates ⓘ

Loaded 12:08:34

Region	All Regions	Category	All Categories	Search / Query
Template	Category	Total Data Types	Description	
Argentina PII	PII	3	Personal Identifiable Information regulations in Argentina, governing the collection, use, and protection of individuals' personal data to ensure privacy and security.	
Australia PII	PII	6	Personal data identifying an individual, protected under Australia's Privacy Act 1988 for privacy and security.	
Austria PII	PII,EU General Data Protection Regulation (GDPR)	6	Personal data identifying individuals, protected under Austria's Data Protection Act and GDPR for privacy and security.	
Belgium PII	PII,EU General Data Protection Regulation (GDPR)	5	Personal data identifying individuals, regulated by GDPR and Belgium's Data Protection Authority for privacy and security compliance.	
Brazil PII	PII	4	Personal data identifying individuals, protected under Brazil's LGPD (General Data Protection Law) for privacy and security.	
Bulgaria PII	PII,EU General Data Protection Regulation (GDPR)	3	Personal data identifying individuals, governed by GDPR and Bulgaria's Personal Data Protection Act for privacy and security.	
Canada PII	PII	7	Personal data identifying individuals, protected under PIPEDA (Personal Information Protection and Electronic Documents Act) for privacy and security.	
Chile PII	PII	2	Personal data identifying individuals, regulated under Chile's Personal Data Protection Law for privacy and security.	
Croatia PII	PII,EU General Data Protection Regulation (GDPR)	3	Personal data identifying individuals, governed by GDPR and Croatia's Data Protection Act for privacy and security compliance.	
Cyprus PII	PII,EU General Data Protection Regulation (GDPR)	4	Personal data identifying individuals, regulated under GDPR and Cyprus's Data Protection Law for privacy and security.	
Czech PII	PII,EU General Data Protection Regulation (GDPR)	4	Personal data identifying individuals, protected under GDPR and the Czech Act on Personal Data Protection for privacy and security.	
Denmark PII	PII,EU General Data Protection Regulation (GDPR)	4	Personal data identifying individuals, governed by GDPR and the Danish Data Protection Act for privacy and security compliance.	
Estonia PII	PII	3	Personal data identifying individuals, regulated under GDPR and Estonia's Data Protection Act for privacy and security.	
Finland PII	PII,EU General Data Protection Regulation (GDPR)	5	Personal data identifying individuals, governed by GDPR and the Finnish Data Protection Act for privacy and security compliance.	

Items per page: 50 1 - 50 of 240 < < 1 > >

Data Labels

Data labels are markers for sensitive information and can be assigned to files that match specific conditions. Use the *Data Labels* page to view different categories of data labels in FortiData. You can also enable or disable a specific label by checking or unchecking the box for the row.

The data labels can be referenced when you create discovery policies (see [Policies on page 23](#)) so that the label will be assigned to files that match the defined conditions. Note that disabled labels will not be assigned to any matching files even if the label is selected in the discovery policy.

Standard Labels

The *Standard Labels* tab displays a list of predefined data labels in FortiData, including machine learning (ML) labels. You can search the standard labels by name and/or description.

Data Labels > Standard Labels ⓘ Loaded 15:58:15

Enabled	Name	Description
▼ Sensitivity (5)		
<input checked="" type="checkbox"/>	Public	Information that is intended for public consumption and poses no risk to the organization or individuals if disclosed.
<input checked="" type="checkbox"/>	Internal	Information that is not intended for public disclosure but is not considered sensitive. It is generally shared within the organization or with trusted partners.
<input checked="" type="checkbox"/>	Confidential	Sensitive information that could cause harm to the organization, its customers, or its employees if disclosed without authorization. Access is typically restricted to certain personnel or departments.
<input checked="" type="checkbox"/>	Highly Confidential	Highly sensitive information that, if exposed, could lead to significant financial loss, reputational damage, legal liability, or regulatory sanctions. Access to this data is strictly controlled.
<input checked="" type="checkbox"/>	Restricted	The most sensitive level of information, accessible only to explicitly authorized personnel. Unauthorized access or disclosure could lead to significant legal, financial, or operational consequences.
▼ Data Residency (7)		
<input checked="" type="checkbox"/>	US	United States
<input checked="" type="checkbox"/>	EU	European Union
<input checked="" type="checkbox"/>	UK	United Kingdom
<input checked="" type="checkbox"/>	ASIA	Asia
<input checked="" type="checkbox"/>	AUSTRALIA	Australia
<input checked="" type="checkbox"/>	BRAZIL	Federative Republic of Brazil
<input checked="" type="checkbox"/>	JAPAN	Japan
▼ Data Classification (48)		
<input checked="" type="checkbox"/>	PII	Personally Identifiable Information, such as names, addresses, SSNs, and phone numbers.
<input checked="" type="checkbox"/>	PHI	Protected Health Information, including medical records, prescriptions, and insurance details.
<input checked="" type="checkbox"/>	Payment Card Data	Payment Card Information, such as credit card numbers and billing details.

The following labels under *Data Classification* are machine learning (ML) labels:

ML label	Description
Finance	Finance-related document
Audit and Assurance Documents	Documents generated during internal or external audit processes to assess financial accuracy, internal controls, and regulatory compliance.

ML label	Description
	These reports provide independent assurance and are critical for corporate governance and risk management.
Credit and Risk Management	Documents involved in assessing and managing credit risk, market risk, etc., such as credit reports, risk assessment reports, and risk management strategies. These documents are important for financial institutions to develop risk controls and mitigation measures.
Expense and Reimbursement Records	Documents that support expense tracking and reimbursement processes. These typically include supporting evidence for employee expenses, management approvals, and payment confirmation. They are frequently used in both internal audits and operational controls.
Financial Report	Used to display the financial status of an individual or organization, including balance sheets, income statements, cash flow statements, and shareholder equity statements. They are critical for investors, management and regulators to understand and assess financial health.
Financial Strategy and Research	Including market research reports, investment strategy documents and industry analysis, etc., used to guide investment decisions and financial product development. This type of document provides financial institutions with market insights based on in-depth analysis and forecasts.
Loan and Financing Agreements	Documents outlining the terms and structure of loans, credit facilities, or other financial arrangements. These define obligations between borrowers and lenders, repayment conditions, interest rates, and covenants, and are central to debt and capital management.
Tax and Regulatory Documents	Documents prepared for tax reporting, compliance with government regulations, and financial oversight. These are critical for ensuring legal compliance and are often submitted to tax authorities or regulatory agencies.
Transaction Record	Includes all documents recording details of financial transactions, such as transaction confirmations, receipts, transfer instructions, and statements. These documents are used to prove the existence, condition, and completion of a transaction.
Healthcare	Healthcare-related document
Clinical Records	Documents that record patient health information and treatment processes, including medical records, disease course records, surgical records, discharge summaries, examination and test reports, etc. These documents are the basis for medical care decisions and are critical to patient diagnosis, treatment, and follow-up.
Clinical Studies	Clinical research report: records the design, implementation process and result analysis of the clinical trial.
Compliance and Risk Management	Clinical research report: records the design, implementation process and result analysis of the clinical trial.

ML label	Description
Insurance and Settlement	Documents related to medical expense reimbursement and settlement, such as insurance claim forms, expense statements, and payment records. These documents are critical to processing medical bills and ensuring the financial benefit of providers and patients.
Medication Management	Documentation involving drug prescriptions, medication instructions, and drug monitoring. This includes prescription orders, medication records and adverse drug reaction reports to ensure patients are using their medications safely and effectively.
HR	HR-related document
CV	Candidate CVs submitted during the recruitment process. It provides quick access to applicants' professional backgrounds, qualifications, and work experience, supporting informed hiring decisions and streamlined candidate evaluation.
Employee Record	Comprehensive records maintained for each employee throughout their lifecycle within the organization. Includes personal information, employment contracts, benefits enrollment, disciplinary records, training history, and separation documentation. These records ensure compliance with labor regulations and support HR operations, audits, and dispute resolution.
Performance Review	Documents related to employee performance evaluations. It helps track individual progress, identify areas for development, and support decisions related to promotions, training, or role adjustments. Consistent performance reviews contribute to employee growth and organizational success.
Recruitment	Documents related to the hiring process, including job requisitions, job descriptions, candidate applications, interview records, background checks, and offer letters. These documents are used to track recruitment activities, evaluate candidate qualifications, and ensure compliance with hiring policies. Proper management of recruitment documentation supports transparency, consistency, and alignment with organizational hiring standards.
Timesheet	Timesheet is used to record and track employee working hours, attendance, and time allocation across projects or tasks. Accurate timesheet documentation supports payroll processing, project management, and compliance with labor regulations.
Information Technology	Information Technology-related documents.
Configuration Files	Configuration files containing structured information used to define system settings, application behaviors, or operational parameters. Includes JSON, XML, or YAML configuration files, environment variable definitions, and similar resources designed to facilitate system customization and operation.

ML label	Description
Development Documentation	For software developers and project team members, it provides information such as product design, architecture, development specifications, and code samples. Development documentation supports the software development process and promotes effective communication within the team.
Log	Log is dedicated to recording detailed, time-stamped entries related to IT activities, system events, and operational workflows. It provides a chronological history of actions taken, system behavior, or incidents encountered, which is essential for auditing, troubleshooting, and maintaining system integrity.
Operational Documentation	Provides the guidance and processes system administrators and IT professionals need to manage and maintain IT systems. Includes system administration manuals, backup and recovery guides, security protocols and maintenance plans.
Test Documentation	Documentation that records software test plans, test cases, test results, and defect reports. Test documentation is critical to ensuring product quality and identifying and fixing defects.
Training Materials	Training course materials for users, developers, or system administrators designed to improve technical skills and product knowledge. Includes training manuals, online courses and instructional videos.
User Documentation	For end users, it provides detailed guidance on how to use a product or system. Includes user manual, quick start guide, FAQ (Frequently Asked Questions) and use cases. User documentation helps users understand product functionality and use the product effectively.
Legal	Legal-related document
Contracts and Agreements	Formal documents that define the legally binding terms and conditions between two or more parties involved in a transaction or service relationship. This includes agreements such as loan contracts, investment management agreements, service contracts, and insurance policies. These documents specify each party's rights, obligations, responsibilities, and remedies in case of breach.
License Agreement	Legally enforceable contract that allows one party (the licensee) to use certain intellectual property owned by another party (the licensor), such as software, trademarks, patents, or copyrighted content. The agreement specifies terms such as usage scope, payment or royalties, duration, restrictions, and termination clauses, ensuring both parties' rights and responsibilities are clearly defined.

ML label	Description
NDA Form	Legal document in which one or more parties agree to maintain the confidentiality of proprietary or sensitive information disclosed during a business or professional relationship. NDAs are designed to protect trade secrets, business plans, technical data, or personal information, and typically outline the scope of confidentiality, duration, and consequences of breach.
Patent	Official legal document granted by a governmental authority that confers exclusive rights to an inventor or applicant to make, use, sell, or license a specific invention for a fixed period (usually 20 years). A patent includes technical descriptions, claims, and drawings that define the scope of legal protection. It serves as a key instrument for protecting intellectual property and promoting innovation.
Source Code	Source code-related document
C#	C# source files (.cs) define classes, methods, and application logic. They are compiled by the .NET runtime and are widely used in Windows applications, games (Unity), and enterprise systems.
C Language	The 'C Language' here refers collectively to both C and C++ source files. C provides low-level programming capabilities, while C++ builds on C with object-oriented features. Their source files typically use extensions such as .c, .cpp, and .h, and are compiled into machine code for high-performance applications.
Golang	Golang source files use the .go extension and start with a package declaration. They are compiled and used to build efficient, concurrent systems such as web servers, APIs, and CLI tools.
Java	Java source files use the .java extension, typically containing a public class matching the filename. They are compiled into bytecode and run on the Java Virtual Machine (JVM) for platform independence.
JavaScript	JavaScript files (.js, .mjs) contain code for browser or server environments. They define variables, functions, and modules, and are widely used for building interactive web applications.
Kotlin	Kotlin source files (.kt, .kts) define classes, functions, and scripts. Interoperable with Java, Kotlin is widely used in Android and backend development for its concise syntax and modern features.
PHP	PHP files (.php) embed code within HTML and are executed server-side. They handle logic, database access, and dynamic content generation for websites and web applications.
Python	Python source files (.py) contain readable, indented code used in scripting, data science, web development, and automation. They are interpreted by the Python runtime environment.

ML label	Description
Shell	Python source files (.py) contain readable, indented code used in scripting, data science, web development, and automation. They are interpreted by the Python runtime environment.
other	Other document

Custom Labels

The *Custom Labels* tab displays a list of custom data labels that you defined in FortiData. You can search the custom data labels by the following criteria:

- ID
- Status
- Category
- Name
- Notes

Data Labels > Custom Labels ⓘ Loaded 16:08:29

Search / Query				
Status	Category	Name	Notes	Created Time
⋮ <input checked="" type="checkbox"/> Enabled	Custom	my label		2025/06/26 16:08:55

Custom data labels are useful if the system's predefined data labels do not meet your needs.

To create a custom data label:

1. Go to *Data Labels > Custom Labels*.
2. Click **ADD LABEL**.
3. Specify the label name, configure the status of the label to be enabled or disabled, and add notes, if needed.

Create Custom Label ⓘ

Category * Custom

Name * Please Input

Status * Enabled

Notes

CANCEL SAVE

4. Click *SAVE*.
5. Click *CREATE* to confirm.

Users

The *Users > Users* page is available to admin users only and displays a list of users in the FortiData system with their roles (see role definitions in the *Users > Role Permissions* page).

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



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*.



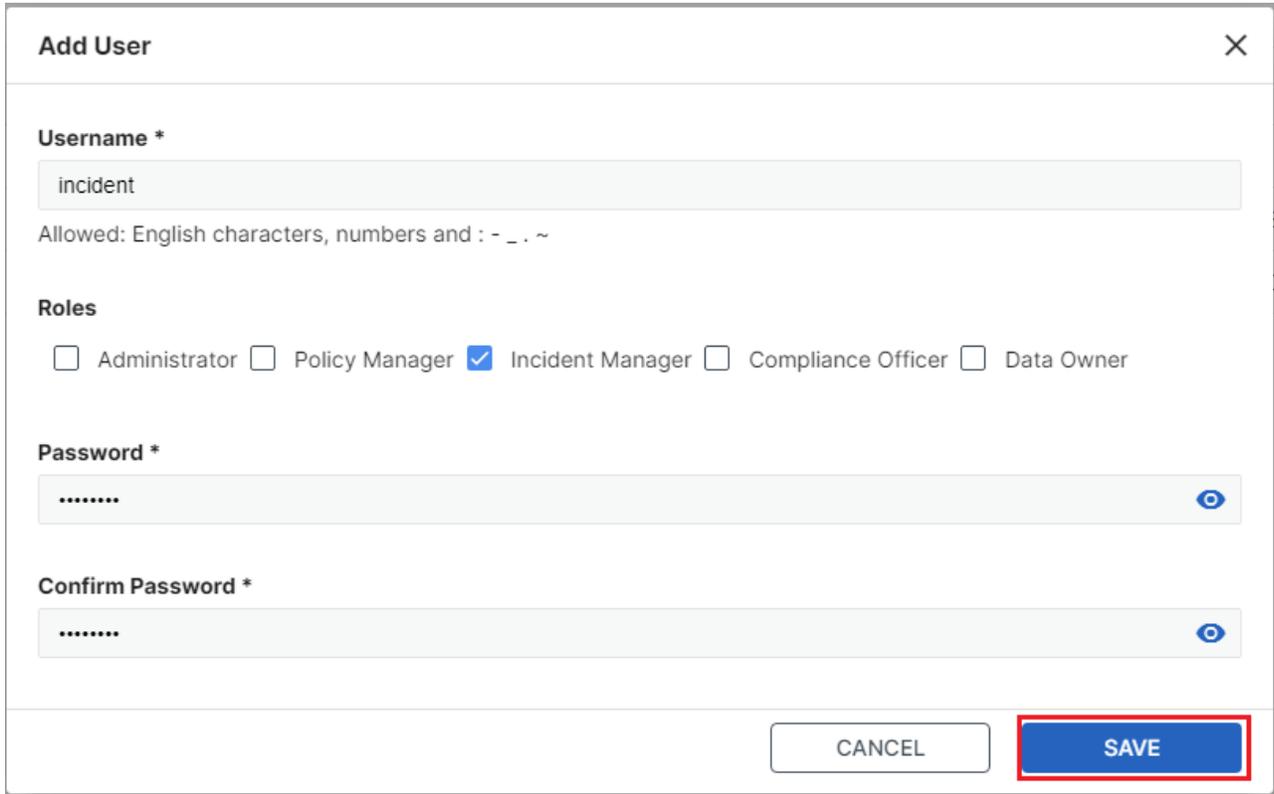
To create a user:

1. On the *Users > 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 a role. See role definitions below or in the *Users > Role Permissions* page.

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.

4. Specify the password and confirm it.

5. Click **SAVE**.



Add User [X]

Username *
incident
Allowed: English characters, numbers and : - _ . ~

Roles
 Administrator Policy Manager Incident Manager Compliance Officer Data Owner

Password *
..... [Eye icon]

Confirm Password *
..... [Eye icon]

CANCEL SAVE

6. 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.

Logs & Reports

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

- [Events on page 54](#)
- [Reports NEW on page 55](#)
- [Report Settings NEW on page 56](#)
- [Log Settings on page 57](#)
- [Log Servers on page 58](#)

Events

System events log data is available in the *Events* 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*.

Logs & Reports > Events ⓘ Loaded

Time Period

All Events

Username = admin
Search / Query

×

⚙️

EXPORT

Export JSON

Export CSV

Time ↓	Level	Type	Username	Action	Description	Message
	● Info	Users	admin	login	User login	User admin logged in successfully from [redacted]
	▲ Warning	Users	admin	login	Incorrect username or password	User admin logged in failed from 10.255.255.2
	● Info	System	admin	setup	Setup fabric	Fabric setup successfully
	● Info	Users	admin	login	User login	User admin logged in successfully from [redacted]
	● Info	Users	admin	login	User login	User admin logged in successfully from [redacted]
	● Info	System	admin	edit	https server config	Change the https server certificate to default, idle time to 960
	● Info	Users	admin	login	User login	User admin logged in successfully from [redacted]
	● Info	Users	admin	login	User login	User admin logged in successfully from [redacted]
	● Info	Users	admin	login	User login	User admin logged in successfully from [redacted]
	● Info	Users	admin	login	User login	User admin logged in successfully from [redacted]
	● Info	Users	admin	login	User login	User admin logged in successfully from [redacted]
	● Info	Data Types	admin	create	Create new custom data type group	Create custom data type group test
	● Info	Users	admin	login	User login	User admin logged in successfully from [redacted]
	● Info	Discovery Policies	admin	create	Add discovery policy	Add a new discovery policy test
	● Info	Users	admin	login	User login	User admin logged in successfully from [redacted]
	● Info	System	admin	create	Add API key	Added API key test
	● Info	Users	admin	login	User login	User admin logged in successfully from [redacted]

Items per page: 100
1 - 27 of 27

<<
<
1
>
>>

FortiData 7.6.1 Administration Guide
Fortinet Inc.

54

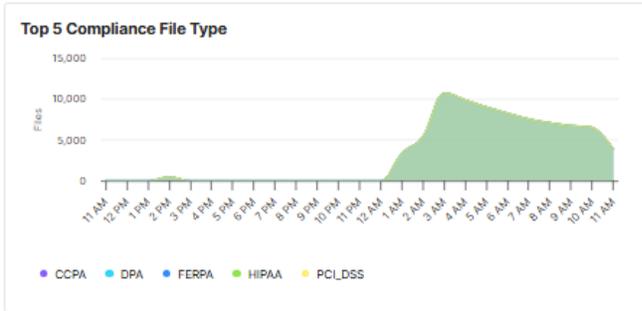
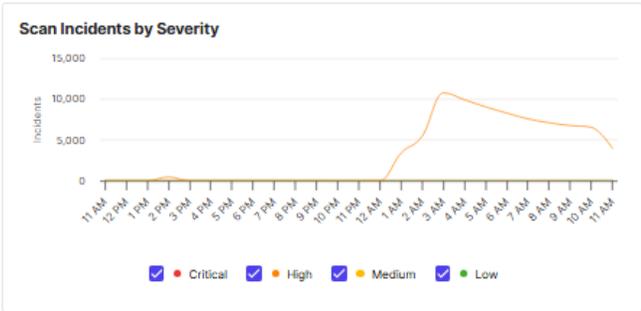
Reports NEW

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 [Summary on page 10](#) reports (in HTML or PDF format) for a specific time period. The last report can be downloaded by clicking the file icon in the *Last Report* column.

Sample report:

FortiData Report for Analytics Summary

Report Name: report Period: Last 24 hours
 Timestamp: Schedule: Once on 2025- PDT
 Scan Name: All Scans Storage: All
 Created by: admin
 Notes:



Top 5 Sensitive File Extensions: Current Totals

File Extension	Files	% of 170292 Scanned Files
.JSON	76,317	44.82%
.PY	1,379	0.81%
.PDF	805	0.47%
.JPG	117	0.07%
.TXT	107	0.06%
Top 5 Totals	79,092	46.45%

[Show More >](#)

ML File Categories: Current Totals

Category	Files	% of 170352 Scanned Files
Information Technology	66,861	39.25%
Source Code	9,516	5.59%
Finance	100	0.06%
Legal	95	0.06%
HR	94	0.06%
Healthcare	87	0.05%
Other	92,762	54.45%
Total Categorized Files	169,515	99.51%

[Show More >](#)

Scan Incidents: Top 5 Discovery Policies

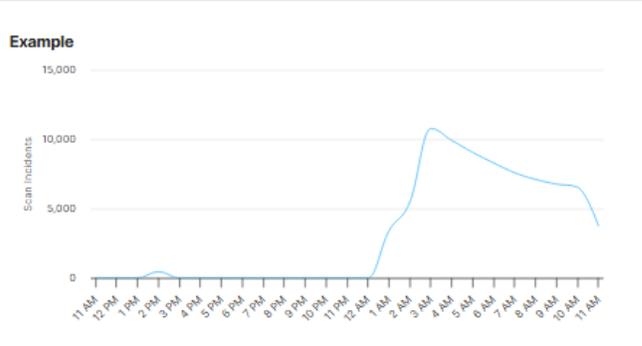


79,092
Incidents
100.00% of All Incidents

Policy Name	Incidents	Trend
Example	79092 100.00%	
All Others	0 0.00%	

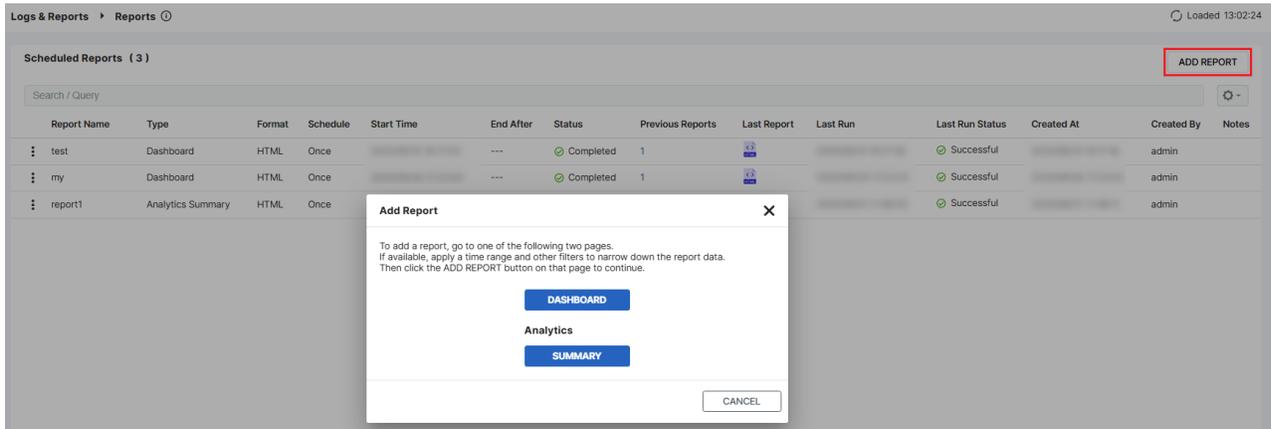
[Show More >](#)

All Scan Incidents: 79,092
Discovery Policies: 1 of 1



To create a report:

1. On the *Logs & Reports > Reports* page, click **ADD REPORT**.



2. Click *Dashboard* or *Summary*, depending on the type of report you are creating.
3. Specify the report name, running frequency, start time, format (HTML or PDF), scan period, and notes (if needed).
4. For analytics summary reports, select the scan from the list as well.
5. Click **SAVE**.
The report appears in the list.
6. **(Optional)** Configure the retention period for the reports in the [Report Settings NEW](#) on page 56 page as needed. The default is 30 days for all report types.

Report Settings **NEW**

In the *Logs & Reports > Report Settings* page, you can configure the retention period for dashboard and analytics summary reports. See [Reports NEW](#) on page 55.

Report Retention Period

Reports Retention Period

Customize

Once Report	<input type="text" value="30"/>	days (1-365 days)
Daily Report	<input type="text" value="30"/>	days (1-365 days)
Weekly Report	<input type="text" value="30"/>	days (1-365 days)
Monthly Report	<input type="text" value="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.

Log Settings

In the *Logs & Reports > Log Settings* page, you can configure the following options:

Event Log

Log Retention Period days (1-90 days)

Event Logging Options All Customize

Cancel
Save

Scan Incidents

Log Retention Period days (1-90 days)

Cancel
Save

Event Log	
<i>Log Retention Period</i>	Specify the number of days(1-90) for which the event logs will be retained. The default is 7 days.
<i>Event Logging Options</i>	Select <i>All</i> to log all events. To customize the type of system events to log, select <i>Customize</i> and select from the event types as needed.
Scan Incidents	
<i>Log Retention Period</i>	Specify the number of days(1-90) for which the Scan Incidents NEW on page 13 logs will be retained. The default is 7 days.

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 *

Server Type *

Server Address *

Protocol *

Port *

Connection Status

Notes

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, for example, Syslog.
Server Address	Specify the IP address of the log server. Click <i>Test Connection</i> to verify the connection is successful.
Protocol	Specify the 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 scan incidents. You can also further define the scope of logs to send to the log server using the <i>Log Level</i> and <i>Severity</i> dropdown filter.

System

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

- [Network on page 60](#)
- [Settings on page 64](#)
- [Certificates on page 66](#)
- [Backup/Restore on page 67](#)

Network

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

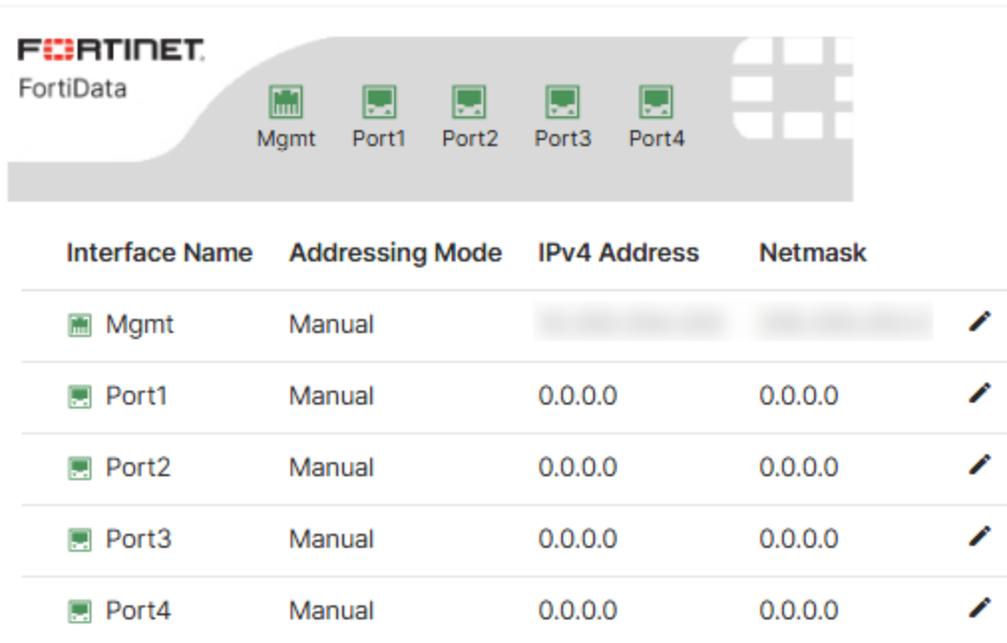
Interfaces

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

To configure the interfaces:

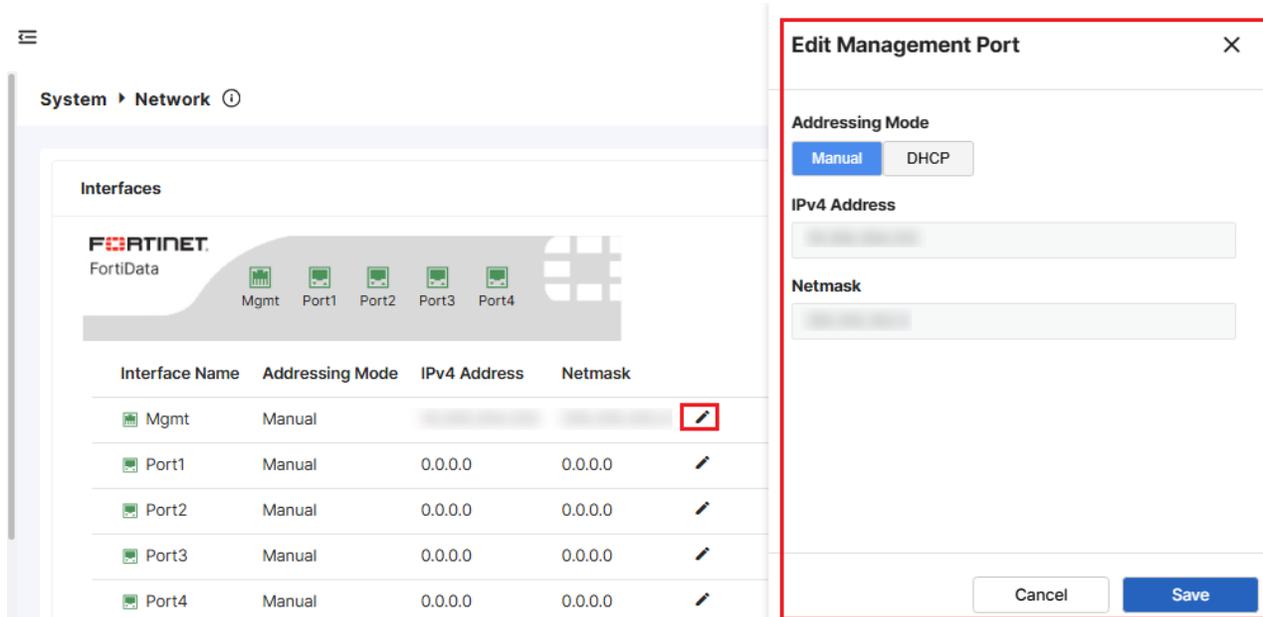
1. In the *System > Network* tab, click *Interfaces* to display the interfaces setting.

Interfaces



Interface Name	Addressing Mode	IPv4 Address	Netmask
Mgmt	Manual		
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.



Setting

Description

Addressing Mode

Specify whether FortiData acquires an IPv4 address for this network interface manually or using DHCP.

Setting	Description
IPv4 Address	Enter the IP address.
Netmask	Enter the netmask.

- Click *Save* to complete the interface configuration.
- 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.

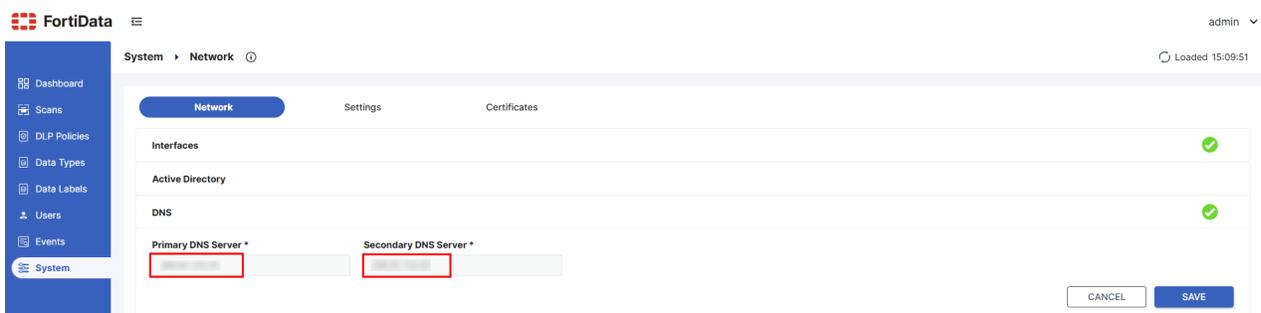
Your Internet service provider (ISP) may supply IP addresses of DNS servers, or you may want to use the IP addresses of your own DNS servers. You must provide unicast, non-local addresses for your DNS servers. Localhost and broadcast addresses will not be accepted.



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:

- Go to *System > Network > DNS*.



- In *Primary DNS Server*, Enter the IP address of the primary DNS server.
- In *Secondary DNS Server*, enter the IP address of the secondary DNS server.
- 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 NEW

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 > Network > Static Route* and click **ADD**.

The screenshot shows the 'Static Route' configuration page. At the top right, there is a blue 'ADD' button highlighted with a red rectangular box. Below the header, there are three columns: 'Destination IP/Mask (IPv4)', 'Gateway (IPv4)', and 'Interface'. The 'Destination IP/Mask (IPv4)' column contains the value '0.0.0.0/0'. The 'Gateway (IPv4)' and 'Interface' columns are currently empty.

2. Enter the following information:

The screenshot shows a 'New Static Route' dialog box with a close button (X) in the top right corner. It contains three input fields:

- Destination IP/Mask (IPv4)**: A text input field containing '0.0.0.0/0'.
- Gateway (IPv4) ***: An empty text input field.
- Interface ***: A dropdown menu that is currently empty.

 At the bottom of the dialog, there are two buttons: 'CANCEL' and 'SAVE'.

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**.

Settings

In this section, you can configure the following:

Admin Settings

System > Settings ⓘ Loaded 18:28:33

Admin Settings

HTTPS Server Certificate *

default ▼

Idle Timeout *

30 Minutes (1 - 960)

HTTPS Server Certificate	Select the TLS certificates uploaded in <i>System > Certificates on page 66</i> .
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 > Settings ⓘ Loaded 18:28:33

Admin Settings

System Time

Time Zone Display *

(GMT-8:00) Pacific Time (US & Canada) ▼

Set Time *

Manual NTP

Time *

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.

FortiGuard **NEW**

FortiData uses the following FortiGuard packages:

- **ML 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 the package

Follow steps below to upgrade the package:

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*.

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:

- Go to *System > FortiGuard*.
- Enable *Use Explicit Proxy for FortiGuard Server*.
- Configure these settings

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.

- Click *Apply*.

Certificates

You can import the following types of certificates in the *System > 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.

To import a new CA certificate:

- Go to *System > Certificates*.
- Click *IMPORT CERTIFICATE > Add New CA Certificate*.

System > Certificates ⓘ Loaded 18:01:52

⚙️ IMPORT CERTIFICATE

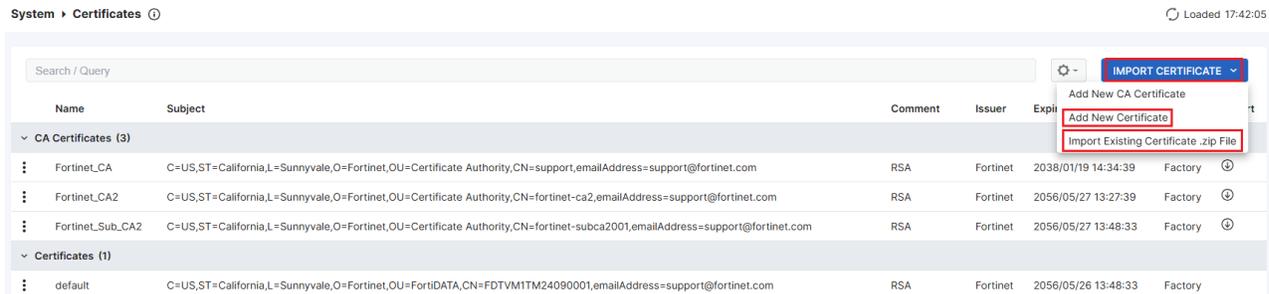
Name	Subject	Comment	Issuer	Expire	Factory
CA Certificates (3)					
Fortinet_CA	C=US,ST=California,L=Sunnyvale,O=Fortinet,OU=Certificate Authority,CN=support,emailAddress=support@fortinet.com	RSA	Fortinet	2038/01/19 14:34:39	Factory ⓘ
Fortinet_CA2	C=US,ST=California,L=Sunnyvale,O=Fortinet,OU=Certificate 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

Add New CA Certificate
Add New Certificate
Import Existing Certificate .zip File

3. Click *BROWSE* to select the certificate file from your local directory.
4. **(Optional)** Specify a passphrase, if needed.
5. Click *IMPORT*.
6. Click *Close*.

To import a customized TLS certificate:

1. Go to *System > Certificates*.
2. Click *IMPORT CERTIFICATE* and select one of the following options:



- *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 on page 64* tab.

Backup/Restore

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

System ▶ **Backup & Restore** ⓘ

Backup

- All System Configuration
- All Data Protection Configuration

Backup

Restore

Select Configuration file

Allowed file types: [.zip]

Restore

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. 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. Click *Restore*.



www.fortinet.com

Copyright© 2025 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. 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.