

Administration Guide

FortiData 7.6.0



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



June 27, 2025

FortiData 7.6.0 Administration Guide

96-760-1109187-20250627

TABLE OF CONTENTS

Change log	4
Introduction	5
Getting started	6
Dashboard	7
Scans	10
Data Types	22
Standard Data Types	22
Custom Data Types	23
ML Document Types	26
Rule Templates	26
Data Labels	28
Standard Labels	28
Custom Labels	28
Machine Learning Labels	30
Users	32
Events	35
Log Settings	35
System	37
Network	37
Interfaces	37
DNS	39
Settings	39
Certificates	41
Backup/Restore	41

Change log

Date	Change Description
2025-02-24	Initial release.
2025-03-10	Updated Data Types on page 22.
2025-04-24	Updated Scans on page 10.

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 Microsoft SharePoint (both on-premise and cloud), AWS, and Samba (SMB) environments 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.



Integration with Fortinet security fabric is currently unavailable but is coming soon with planned integration with FortiGate, FortiAnalyzer, and FortiClient. 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.

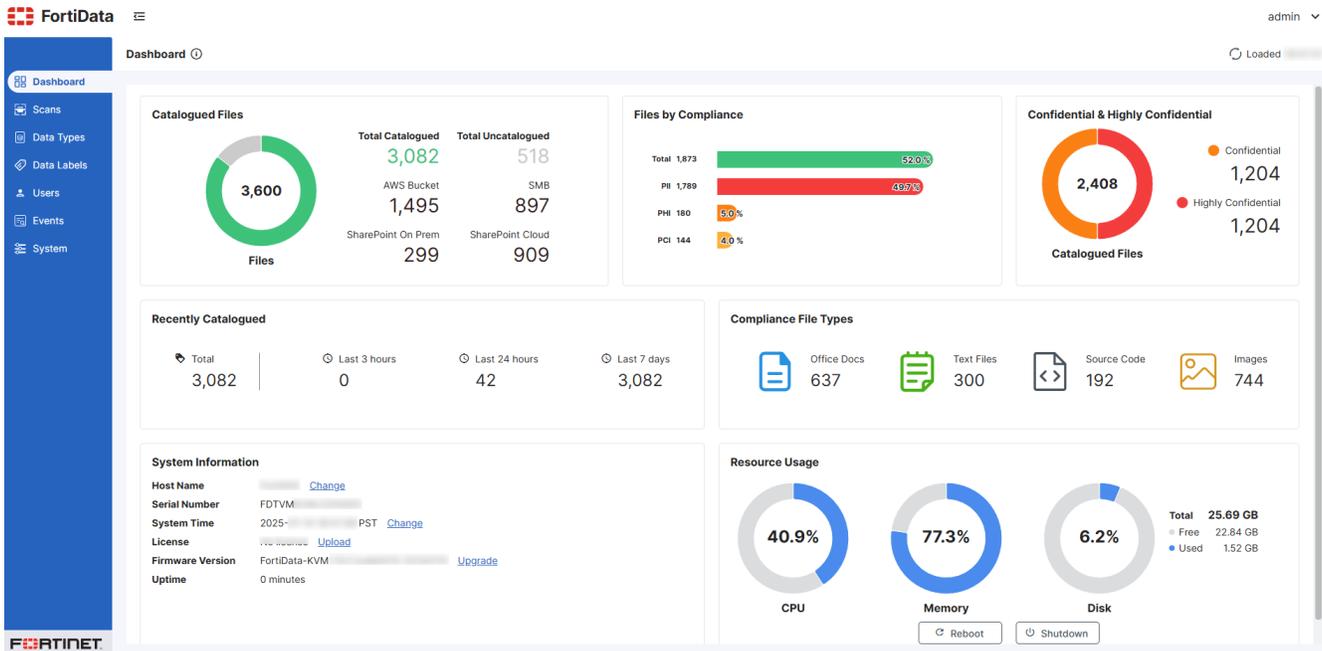
Getting started

Perform the following procedures to get started with FortiData:

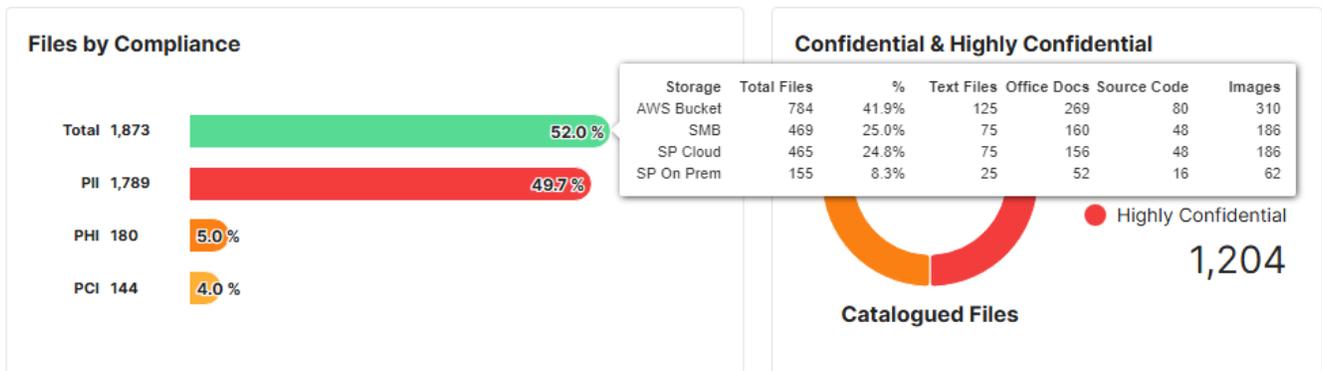
1. Configure interface and DNS settings. See [Network on page 37](#)
2. Configure timeout and system time. See [Settings on page 39](#).
3. Configure HTTPS server certificate. See [Certificates on page 41](#).
4. Create users of with different access scope to FortiData. See [Users on page 32](#).
5. Create discovery policies and scans to look for specific types of data in files of a specific location. See [Scans on page 10](#).

Dashboard

Use the *Dashboard* to view information of the system, such as the number of catalogued files by platform, file compliance and confidentiality information, resource usage, and system information (hostname, serial number, system time, license status, firmware version).

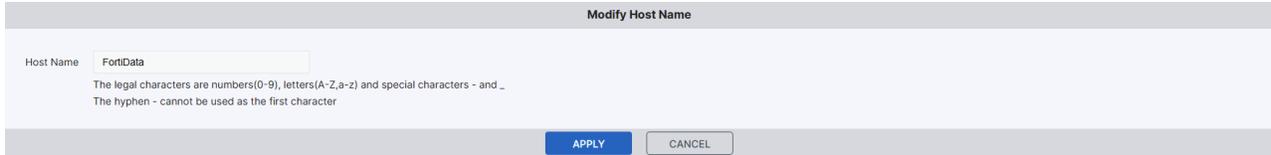


For the *Files by Compliance* and *Confidential & Highly Confidential* widgets, hover your mouse over each graph or chart to view more details about the data points.



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.



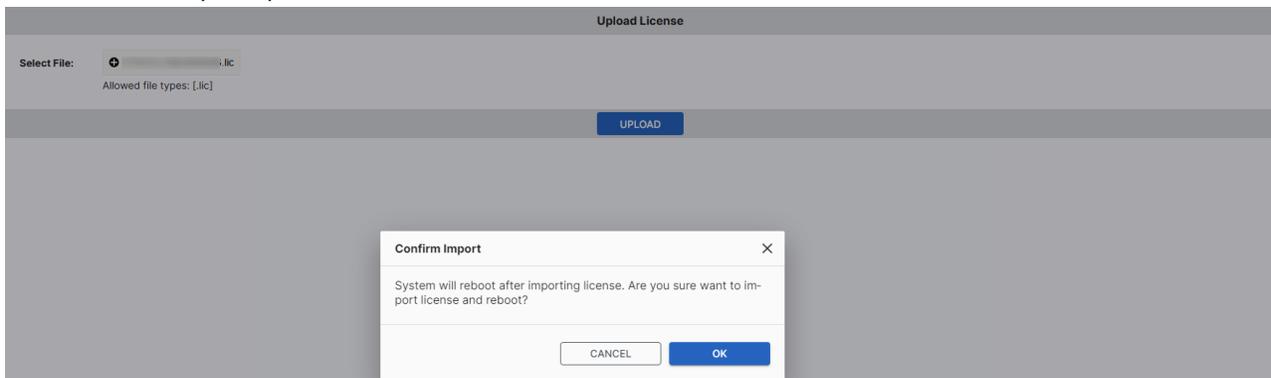
3. Specify the desired hostname and click *APPLY*.

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 39* 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 41*.

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 > Resource Usage* widget.
2. Click *Reboot*.

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

To shut down the system:

1. Go to *Dashboard > Resource Usage*.
2. Click *Shutdown*.

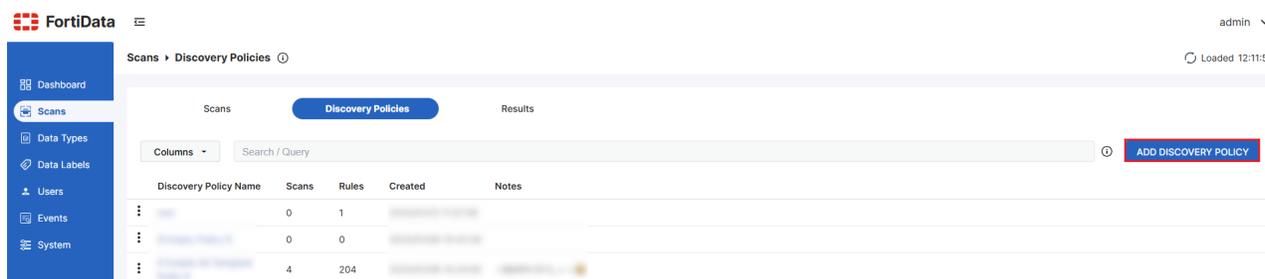
Alternatively, run the `execute shutdown` command via the CLI.

Scans

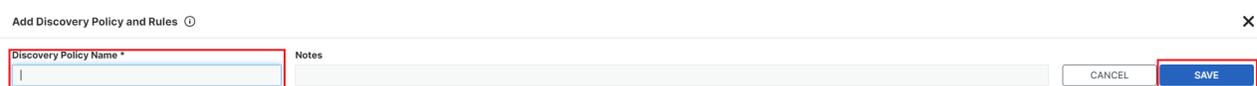
In the *Scans* page, you can create a data discovery policy to look for specific types of data (using data types) in files, such as financial transactions or health records, and add specific tags (using data labels) to files that meet the specified conditions. You can then define a scan to access and analyze files in a target location (for a storage type) using the conditions and actions defined in the discovery policy with a proper schedule. Scan and classification results can then be viewed in the *Results* tab.

To create a discovery policy:

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

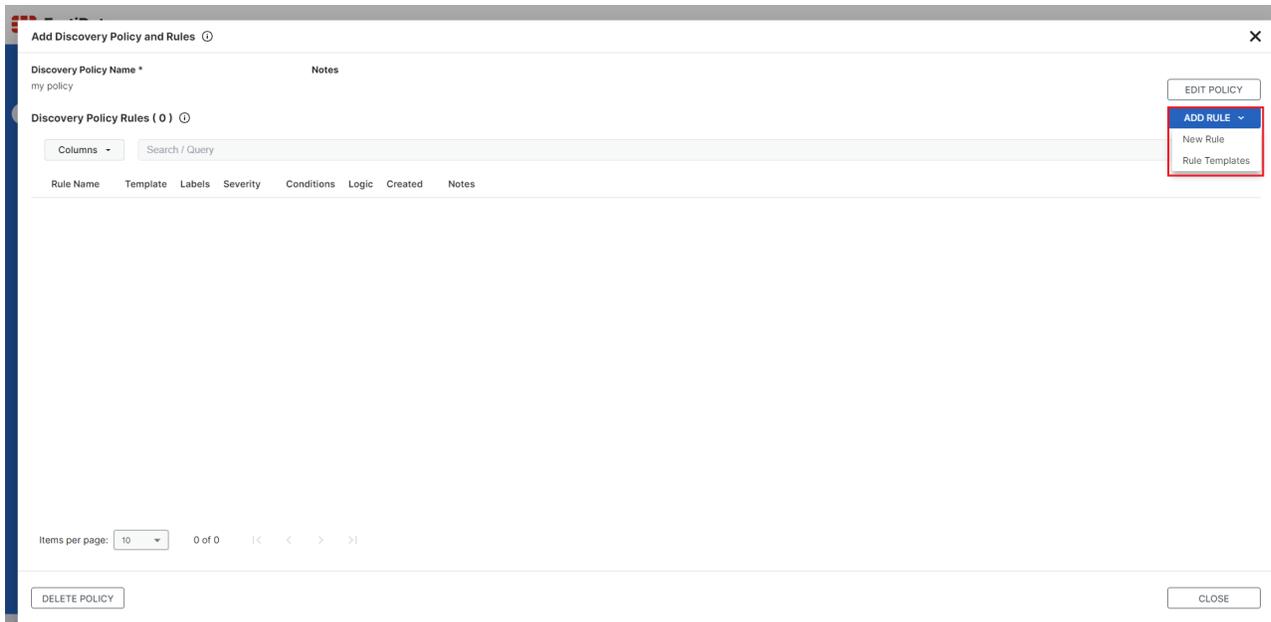


3. Specify the policy name and any notes, and then click **SAVE**.

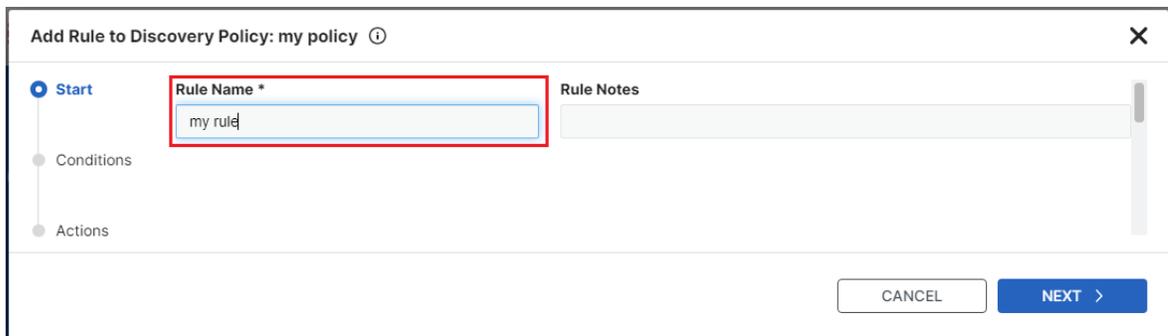


4. Click **ADD RULE** and select *New Rule* or *Rule Templates*, depending on whether you want to create your own data discovery rule or use a rule template predefined in FortiData.

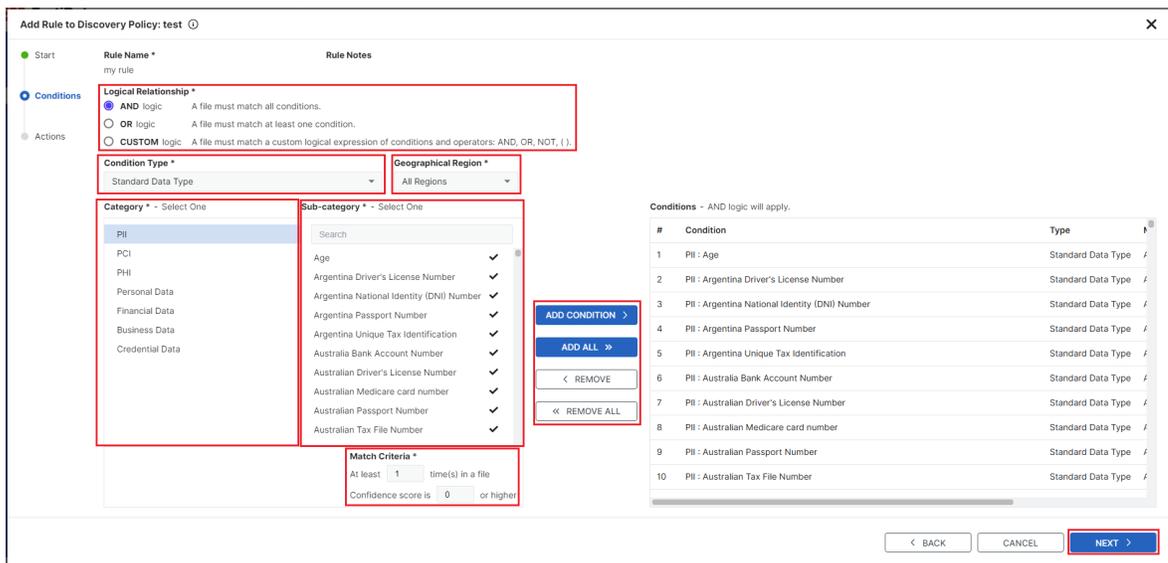
A rule is a defined data pattern with a set of data types and logic conditions that a discovery policy maps to when recognizing patterns in files. You can view the full list of rule templates in the *Rule Templates* tab in the [Data Types on page 22](#) page,



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



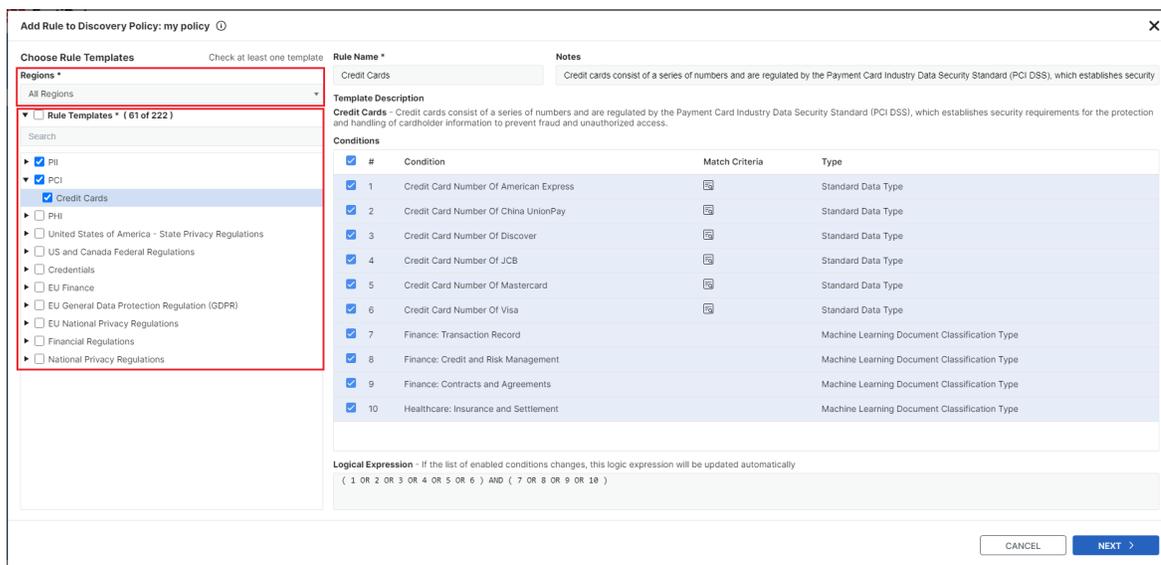
- ii. Configure the following options in the *Conditions* page:



Option	Description
<i>Logical Relationship</i>	<p>Select from the following logic options:</p> <ul style="list-style-type: none"> • <i>AND</i>—A file must match all conditions to be considered a match. • <i>OR</i>—A file must match at least one condition to be considered a match. • <i>CUSTOM</i>—A file must match a custom logical expression of conditions and operators: AND, OR, NOT, () to be considered a match.
<p><i>Condition Type</i></p>	<p>Select from the following condition types:</p> <hr/> <div data-bbox="683 632 764 737" style="display: inline-block; vertical-align: middle;">  </div> <div data-bbox="802 625 1406 758" style="display: inline-block; vertical-align: middle; margin-left: 10px;"> <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 22 page.</p> </div> <hr/> <ul style="list-style-type: none"> • <i>Standard Data Type</i>—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. • <i>Custom Data Type Group</i>—Data type groups that you created. • <i>File Type</i>—Choose from the following file types: <ul style="list-style-type: none"> • Text Files—Select from the following file extensions: .csv, .json, .md, .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. • <i>Machine Learning Document Classification Type</i>—List of data types that are created and dynamically updated by FortiData based on machine learning algorithms. <hr/> <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 <i>ADD CONDITION</i> 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 <i>ADD ALL</i>. • You can also remove a specific condition by selecting it and clicking <i>REMOVE</i>. • To remove all added conditions, click <i>REMOVE ALL</i>.

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

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



- ii. Click *NEXT*.
- 5. Define the labels to apply to files that match the selected conditions.

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

Standard Labels Custom Labels Machine Learning Labels

Search / Query

Available Labels	Status	Description
Sensitivity (5)		
<input type="checkbox"/> Certificates and Credentials	✓ Enabled	These are sensitive information and keys commonly used by developers during software development and integration, including API keys, authentication tokens, encryption keys, database connection strings, etc.
<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 (or Restricted)	✓ 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"/> 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"/> Public	✓ Enabled	Information that is intended for public consumption and poses no risk to the organization or individuals if disclosed.
Data Residency (7)		
<input type="checkbox"/> ASIA	✓ Enabled	Asia
<input type="checkbox"/> AUSTRALIA	✓ Enabled	Australia
<input type="checkbox"/> BRAZIL	✓ Enabled	Federative Republic of Brazil

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

< BACK CANCEL DONE

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 28](#) 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 28](#).

Label Type	Description								
<i>Standard Labels</i>	Predefined labels by FortiData.								
<i>Custom Labels</i>	Custom labels that you created.								
<i>Machine Learning Labels</i>	Machine learning labels. You can select from the following modes: <table border="1" style="margin-top: 10px;"> <thead> <tr> <th>Mode</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>Disable</i></td> <td>Do not apply machine learning labels to any matching files.</td> </tr> <tr> <td><i>Automatic</i></td> <td>Automatically apply machine learning labels to matching files.</td> </tr> <tr> <td><i>Manual</i></td> <td>Only apply selected machine learning labels to matching files.</td> </tr> </tbody> </table> <p>When enabled, ML labels are applied to files based on the FortiData ML model. The application of ML labels depends on the condition matching of this discovery policy. If there is condition match for a file, FortiData applies ML labels in addition to the standard and custom labels as selected by the administrator.</p>	Mode	Description	<i>Disable</i>	Do not apply machine learning labels to any matching files.	<i>Automatic</i>	Automatically apply machine learning labels to matching files.	<i>Manual</i>	Only apply selected machine learning labels to matching files.
Mode	Description								
<i>Disable</i>	Do not apply machine learning labels to any matching files.								
<i>Automatic</i>	Automatically apply machine learning labels to matching files.								
<i>Manual</i>	Only apply selected machine learning labels to matching files.								

6. Click *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 * Notes

my policy [EDIT POLICY](#)

Discovery Policy Rules (120) [ADD RULE](#)

Columns - Search / Query 🔍

Rule Name	Template	Labels	Severity	Conditions	Logic	Created	Notes
⋮ Bulgaria PII (1)	Bulgaria PII	1	● Medium	3	Or	2025/01/13 16:31:08	Personal data identifying individuals, governed by GDPR and Bulgaria's Personal Data Protection Act for privacy and security.
⋮ Canada PII (1)	Canada PII	1	● Medium	7	Custom	2025/01/13 16:31:08	Personal data identifying individuals, protected under PIPEDA (Personal Information Protection and Electronic Documents Act) for privacy and security.
⋮ Austria PII (1)	Austria PII	1	● Medium	6	Custom	2025/01/13 16:31:08	Personal data identifying individuals, protected under Austria's Data Protection Act and GDPR for privacy and security.
⋮ Brazil PII (1)	Brazil PII	1	● Medium	3	Custom	2025/01/13 16:31:08	Personal data identifying individuals, protected under Brazil's LGPD (General Data Protection Law) for privacy and security.
⋮ Email Addresses (1)	Email Addresses	1	● Medium	1	Or	2025/01/13 16:31:08	Unique identifiers for electronic communication, often used as personal data under privacy regulations, requiring protection from unauthorized access and spam.
⋮ EU PII (1)	EU PII	1	● Medium	1	Or	2025/01/13 16:31:08	Personal data identifying individuals, governed by the General Data Protection Regulation (GDPR), ensuring strict privacy and security standards across member states.
⋮ Argentina PII (1)	Argentina PII	1	● Medium	3	Or	2025/01/13 16:31:08	Personal identifiable information regulations in Argentina, governing the collection, use, and protection of individuals' personal data to ensure privacy and security.
⋮ Australia PII (1)	Australia PII	1	● Medium	6	Custom	2025/01/13 16:31:08	Personal data identifying an individual, protected under Australia's Privacy Act 1988 for privacy and security.
⋮ Belgium PII (1)	Belgium PII	1	● Medium	4	Custom	2025/01/13 16:31:08	Personal data identifying individuals, regulated by GDPR and Belgium's Data Protection Authority for privacy and security compliance.
⋮ Chile PII (1)	Chile PII	1	● Medium	2	And	2025/01/13 16:31:08	Personal data identifying individuals, regulated under Chile's Personal Data Protection Law for privacy and security.

Items per page: 10 1 - 10 of 120 ⏪ ⏩

[DELETE POLICY](#) [CLOSE](#)

To create a scan:



You can create up to 16 scans.

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

FortiData admin

Scans > Scans Loaded 16:46:26

Scans Discovery Policies Results

Columns - Search / Query [ADD SCAN](#)

Scan Name	System Status	Scan Status	Run Scan	Previous Scans	Start	Ended	Duration	Wait Time	Target	Scan Type
-----------	---------------	-------------	----------	----------------	-------	-------	----------	-----------	--------	-----------

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

- a. Specify the scan name.
- b. Select the scan 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.														
	<table border="1"> <thead> <tr> <th>Permission</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>AuditLog.Read.All</i></td> <td>Read all audit log data</td> </tr> <tr> <td><i>BrowserSiteLists.Read.All</i></td> <td>Read all browser site lists for your organization</td> </tr> <tr> <td><i>Files.Read.All</i></td> <td>Read files in all site collections</td> </tr> <tr> <td><i>Files.SelectedOperations.Selected</i></td> <td>Access selected Files without a signed in user.</td> </tr> <tr> <td><i>Sites.Manage.All</i></td> <td>Create, edit, and delete items and lists in all site collections</td> </tr> <tr> <td><i>Sites.Read.All</i></td> <td>Read items in all site collections</td> </tr> </tbody> </table>	Permission	Description	<i>AuditLog.Read.All</i>	Read all audit log data	<i>BrowserSiteLists.Read.All</i>	Read all browser site lists for your organization	<i>Files.Read.All</i>	Read files in all site collections	<i>Files.SelectedOperations.Selected</i>	Access selected Files without a signed in user.	<i>Sites.Manage.All</i>	Create, edit, and delete items and lists in all site collections	<i>Sites.Read.All</i>	Read items in all site collections
Permission	Description														
<i>AuditLog.Read.All</i>	Read all audit log data														
<i>BrowserSiteLists.Read.All</i>	Read all browser site lists for your organization														
<i>Files.Read.All</i>	Read files in all site collections														
<i>Files.SelectedOperations.Selected</i>	Access selected Files without a signed in user.														
<i>Sites.Manage.All</i>	Create, edit, and delete items and lists in all site collections														
<i>Sites.Read.All</i>	Read items in all site collections														

Scan Type	Required Permission(s)								
	<table border="1"> <thead> <tr> <th>Permission</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>Sites.Selected</i></td> <td>Access selected site collections</td> </tr> <tr> <td><i>ActivityFeed.Read</i></td> <td>Read activity data for your organization</td> </tr> <tr> <td><i>ServiceHealth.Read</i></td> <td>Read service health information for your organization</td> </tr> </tbody> </table>	Permission	Description	<i>Sites.Selected</i>	Access selected site collections	<i>ActivityFeed.Read</i>	Read activity data for your organization	<i>ServiceHealth.Read</i>	Read service health information for your organization
Permission	Description								
<i>Sites.Selected</i>	Access selected site collections								
<i>ActivityFeed.Read</i>	Read activity data for your organization								
<i>ServiceHealth.Read</i>	Read service health information for your organization								

- 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*.

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

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

Add Scan ⓘ

Start

Scan Name: my scan Scan Type: SMB SMB Server IP Address/Domain: Share Name:

Catalog

Files

File Types * Select the file type groups you want to scan.

Scan all 33 file types 15 of 33 selected

text files

- .csv Comma-Separated Values file
- .json JavaScript Object Notation file
- .md Markdown Text Format file
- .rtf Rich Text Format file
- .txt Plain Text file

office documents

- .doc Microsoft Word Document file
- .docx Microsoft Word XML Document file
- .odp OpenDocument Presentation file
- .ods OpenDocument Spreadsheet file
- .odt OpenDocument Text file
- .pdf Portable Document Format file
- .ppt Microsoft PowerPoint Presentation file
- .pptx Microsoft PowerPoint XML Presentation file
- .xls Microsoft Excel Spreadsheet file
- .xlsx Microsoft Excel XML Spreadsheet file

pictures

- .avif AV1 Image Format file
- .bmp Bitmap Image Format file
- .gif Graphics Interchange Image Format file
- .jpeg JPEG Image Format file
- .jpg JPEG Image Format file
- .png Portable Network Graphics Image Format file
- .tif Tagged Image Format file
- .tiff Tagged Image Format file
- .webp WebP Image Format file

source code

- .c C source code file
- .cpp C++ source code file
- .go Golang source code file
- .java Java source code file
- .js JavaScript source code file
- .kt Kotlin source code file
- .php PHP source code file
- .py Python source code file
- .sh Shell script source code file

File Size *
Scan files between 0 MB and 10 MB

Machine Learning Document Classification
If enabled, machine learning models will be used to classify documents.
 Document Classification

Data Type Detection*
Precision Level Medium

< BACK CANCEL NEXT >

5. Click *NEXT*.

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

Add Scan ⓘ

Start

Scan Name: my scan Scan Type: SMB SMB Server IP Address/Domain: Share Name:

Discovery Policies

Existing Discovery Policies (2) - Move the discovery policies for this scan into the selected discovery policies table

Selected Discovery Policies (0)

Search / Query ⓘ

Discovery Policy Name	Notes
<input type="checkbox"/> my policy	
<input type="checkbox"/> test	test

Search / Query ⓘ

Discovery Policy Name	Notes
-----------------------	-------

< BACK CANCEL NEXT >

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

Add Scan ⓘ

- Start
- Catalog
- Files
- Policies
- Save**

Review and Save

Start [Edit](#)

Scan Name	Scan Type	Target	Notes
my scan	SMB		

Schedule [Edit](#)

Long wait time between file downloads: 200ms. Run Daily 1:00 PM

Catalog [Edit](#)

Scan 1 of 46 top-tier folders

Files [Edit](#)

Types: 5 text files

ML Document Classification: Enabled

Data Type Detection Precision Level: High

Scan files: Between 0 MB to 10 MB

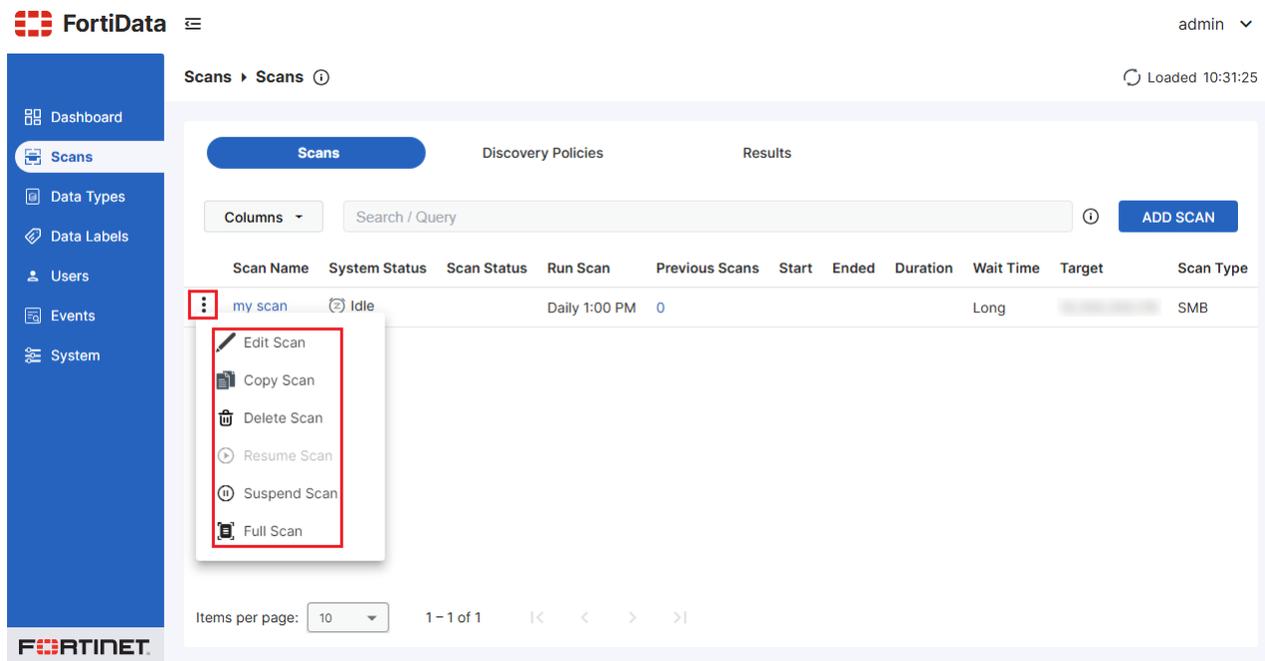
Discovery Policies [Edit](#)

Policies: 1

Total Rules: 120

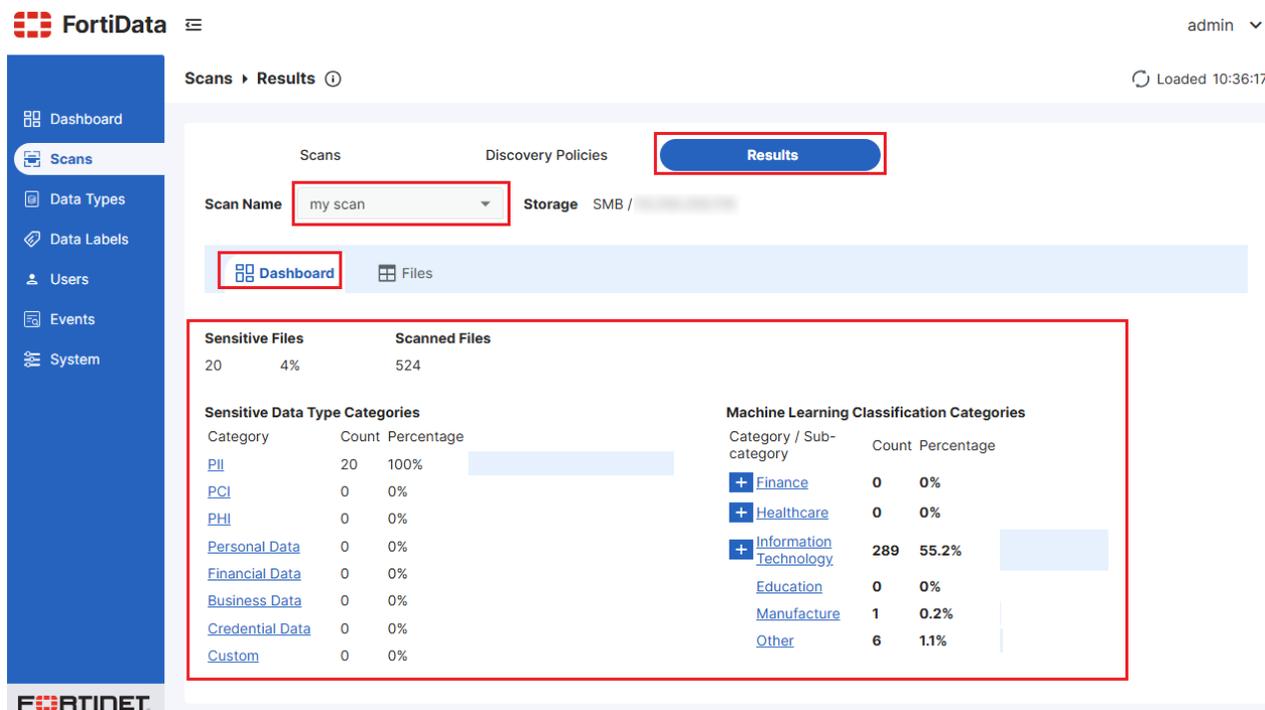
< BACK CANCEL **DONE**

The scan is now configured to look for specific data in the target directory on the defined schedule and assign labels to files matching the conditions. 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 check scan results:

1. Go to *Scans > Results*.
2. Filter the results by scan name and view the results in dashboard view or file list view with scan details about each file.



The screenshot shows the FortiData interface for scanning results. The main area displays a table of scan results with columns for File, Standard Instances, Custom Instances, Main Category, Sub Category, Labels, and File Path. A sidebar titled 'Data Analysis Details' is open on the right, providing a breakdown of the selected file's data types and labels.

Scans Results Table:

Details	File	Standard Instances	Custom Instances	Main Category	Sub Category	Labels	File Path
[Details]	[Redacted]	8	0	Information Technology	Configuration Files		[Redacted]
[Details]	[Redacted]	1	0	Information Technology	Configuration Files		[Redacted]
[Details]	[Redacted]	4	0	Information Technology	Configuration Files	3 Labels	[Redacted]
[Details]	[Redacted]	2	0	Information Technology	Configuration Files	3 Labels	[Redacted]
[Details]	[Redacted]	2	0	Information Technology	Configuration Files	3 Labels	[Redacted]
[Details]	[Redacted]	1	0	Information Technology	Configuration Files	3 Labels	[Redacted]
[Details]	[Redacted]	1	0	Information Technology	Configuration Files	3 Labels	[Redacted]

Data Analysis Details Sidebar:

- File:** [Redacted].json
- Storage:** SMB / [Redacted]
- Updated:** [Redacted]
- Main Category:** Information Technology
- Sub Category:** Configuration Files
- Main Classification Confidence:** 95
- Sub Classification Confidence:** 95
- File Path:** [Redacted].json
- Standard Data Type Categories (4):**

#	Data Type	Category	Region	Count	Max Confide
1	Israel Bank Account Number	PII	IL	4	83
- Custom Data Types (0):** (Empty table)
- Assigned Labels (3):**
 - Label: ML/Education
 - Label: ML/Finance/Other
 - Label: Certificates and Credentials

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 10](#) page.

Standard Data Types

The *Standard Data Types* tab 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.

The screenshot shows the FortiData interface for the 'Standard Data Types' tab. The page includes a navigation sidebar on the left with options like Dashboard, Scans, Data Types, Data Labels, Users, Events, and System. The main content area displays a table of predefined data types. The table has columns for Data Category, Name, Description, Type, Created On, and Region. The data is filtered by 'All Regions' and 'All Categories'. A search bar is available for filtering by name or region. The table lists 10 data types, including AWS Access Key, AWS Secret Access Key, Age, American Bank Association Routing Number, American Bankers CUSIP ID, Argentina Driver's License Number, Argentina National Identity (DNI) Number, Argentina Passport Number, and Argentina Unique Tax Identification. The page also shows pagination information: 'Items per page: 10' and '1 - 10 of 366'.

Data Category	Name	Description	Type	Created On	Region
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		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 your AWS resources.	Regex		ALL
PII	Age	The age of a person.	Regex		ALL
Financial Data	American Bank Association Routing Number	An American Bank Association (ABA) Routing Number is a unique 9-digit code assigned to banks and financial institutions in the United States to identify them in the processing of checks, electronic funds transfers, and other transactions.	Regex + Validation Algorithms		US
Financial Data	American Bankers CUSIP ID	An American Bankers CUSIP ID is a unique 9-character alphanumeric code assigned by the Committee on Uniform Securities Identification Procedures (CUSIP) to identify U.S. and Canadian registered stocks, bonds, and other securities for the purpose of facilitating clearing and settlement.	Regex		US, CA
PII	Argentina Driver's License Number	An Argentina driver's license number is a unique alphanumeric identifier assigned to an individual's driver's license issued by the Argentine government.	Regex		AR
PII	Argentina National Identity (DNI) Number	A unique identifier assigned to individuals in Argentina upon issuance of their Documento Nacional de Identidad (DNI).	Regex		AR
PII	Argentina Passport Number	An Argentina passport number is a unique alphanumeric identifier assigned to an individual's passport issued by the Argentine government.	Regex		AR
PII	Argentina Unique Tax Identification	In Argentina, the Unique Tax Identification Number (CUIT, Código Único de Identificación Tributaria) is a unique number assigned to individuals and entities for tax purposes.	Regex		AR

Custom Data Types

The *Custom Data Types* tab 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.

The screenshot shows the FortiData interface with the 'Custom Data Types' tab selected. The sidebar on the left contains navigation links: Dashboard, Scans, Data Types (highlighted), Data Labels, Users, Events, and System. The main content area displays a table of Custom Data Type Groups. The table has the following columns: Group Name, Data Types, Scans, Discovery Policies, Created, and Notes. A single row is visible with the group name 'test', 1 Data Type, 0 Scans, and 0 Discovery Policies. Above the table is a search bar labeled 'Search / Query' and an 'ADD GROUP' button. The breadcrumb path is 'Data Types > Custom Data Types'. The user 'admin' is logged in, and the page was loaded at 10:51:48.

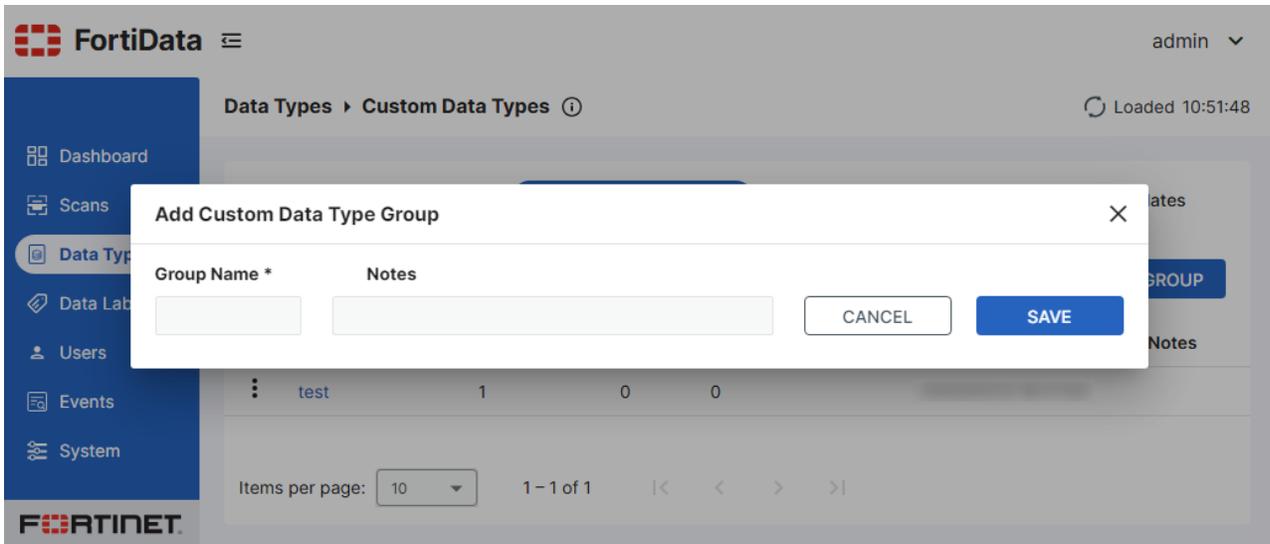
Custom data type groups are useful if the system's predefined data type do not meet your needs.

To create a custom data type group:

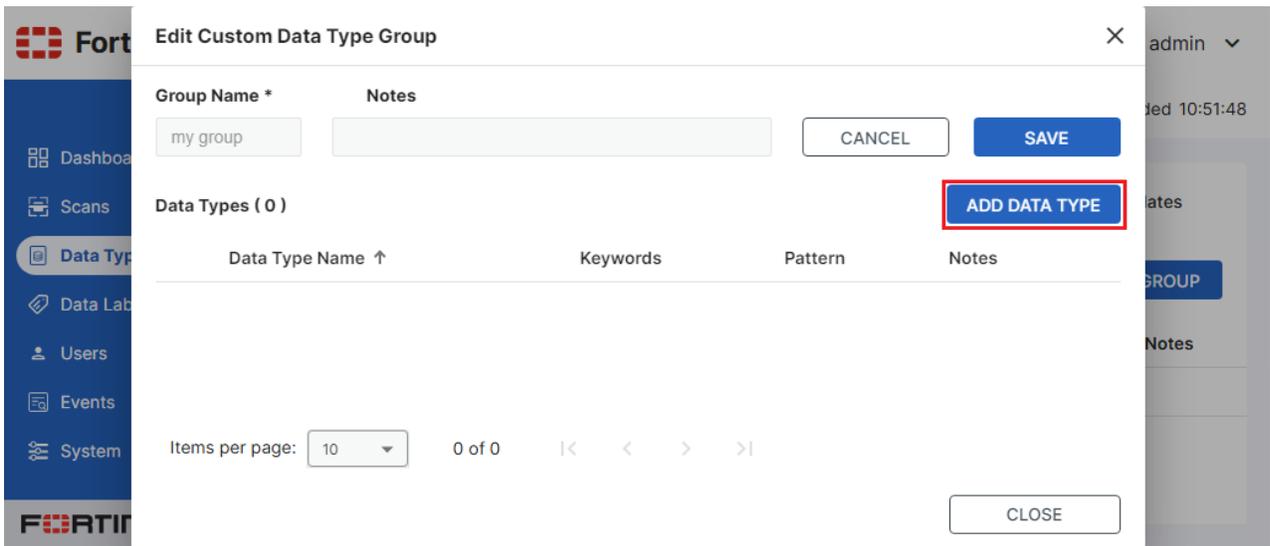
1. Go to *Data Types > Custom Data Types*.
2. Click *ADD GROUP*.

This screenshot is identical to the previous one, but with red boxes highlighting the 'Custom Data Types' tab in the breadcrumb path and the 'ADD GROUP' button, indicating the next step in the process.

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



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



6. Configure the data type with the following options:

Add Data Type [X]

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*.

ML Document Types

The *ML Document Types* tab displays a list of data types generated by FortiData machine learning. You can search the ML document types by document type.

The screenshot shows the FortiData interface for ML Document Types. The sidebar on the left contains navigation links: Dashboard, Scans, Data Types (selected), Data Labels, Users, Events, and System. The main content area is titled "Data Types > ML Document Types" and includes a search bar and a table of document types. The table is organized into two main categories: Finance (6) and Healthcare (6). The Finance category includes: Contracts and Agreements, Credit and Risk Management, Financial Report, Other, Strategy and Research, and Transaction Record. The Healthcare category includes: Clinical Records, Insurance and Settlement, Legal and Compliance, and Documentation involving drug prescriptions. The Fortinet logo is visible in the bottom left corner of the interface.

Document Type	Description
Finance (6)	
Contracts and Agreements	A formal document that records the terms of a financial transaction or service, including loan agreements, investment management contracts, and insurance policies. These documents establish the rights, obligations and responsibilities between the parties involved.
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.
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.
Other	Other financial documents or records that do not fall into the predefined categories.
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.
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 (6)	
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.
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.
Legal and Compliance	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.
Documentation involving drug prescriptions	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

Rule Templates

The *Rule Templates* tab 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.

FortiData

admin

Data Types > Rule Templates

Standard Data Types Custom Data Types ML Document Types Rule Templates

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)	4	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.

Items per page: 10 1 - 10 of 204

FORTINET

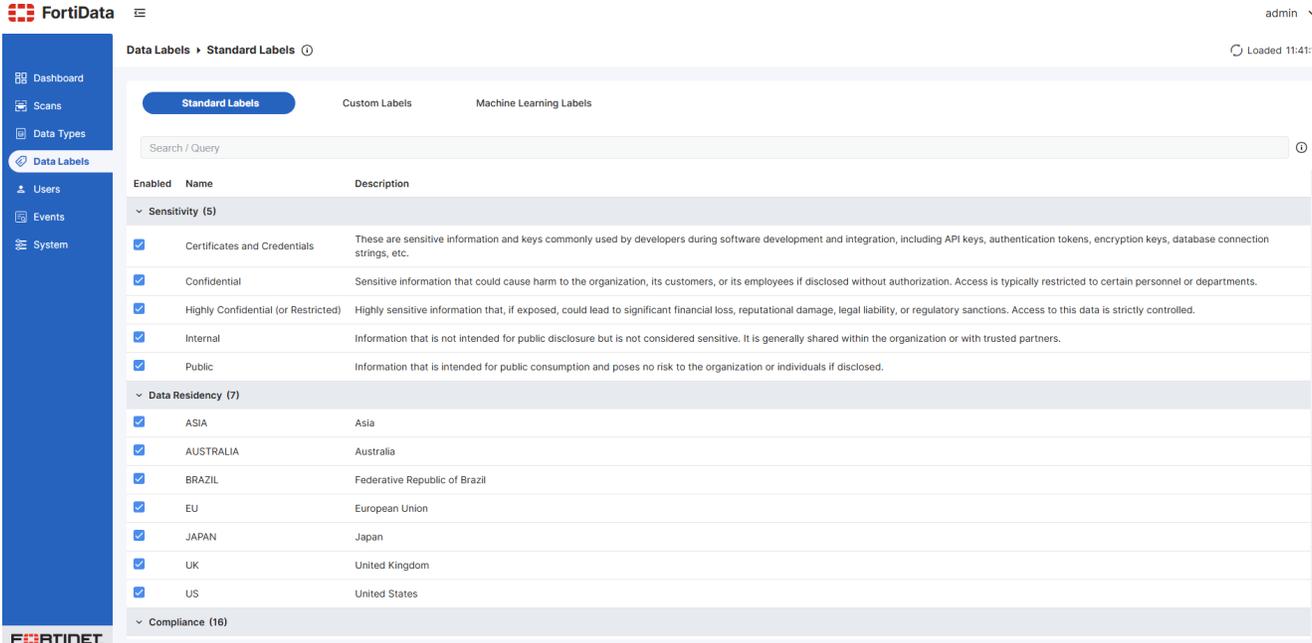
Data Labels

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 in the [Scans on page 10](#) page 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. You can search the standard labels by name and/or description.



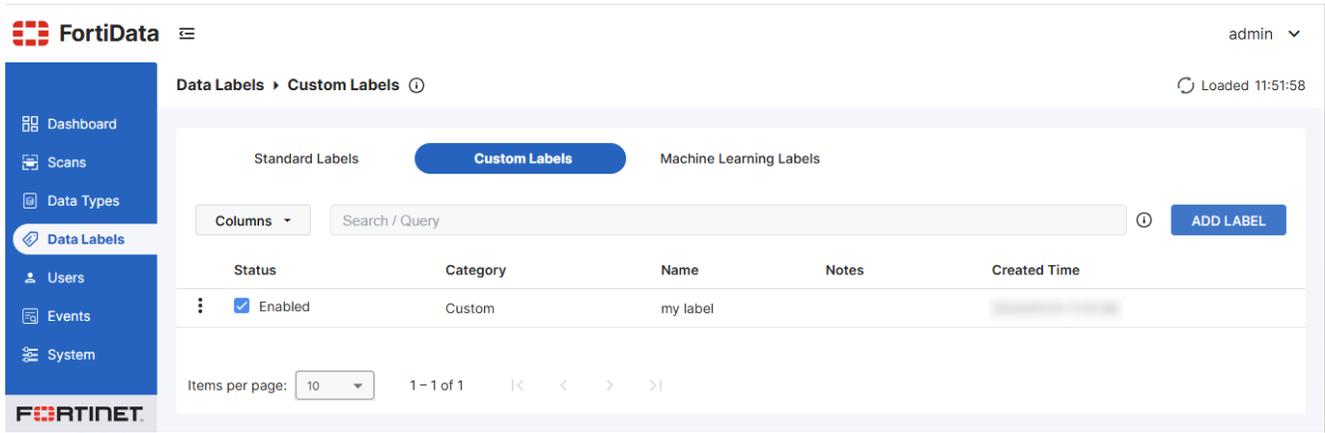
The screenshot shows the FortiData interface for Standard Labels. The page is titled "Data Labels > Standard Labels" and includes a search bar and three tabs: "Standard Labels", "Custom Labels", and "Machine Learning Labels". The "Standard Labels" tab is active, displaying a table of predefined labels.

Enabled	Name	Description
Sensitivity (5)		
<input checked="" type="checkbox"/>	Certificates and Credentials	These are sensitive information and keys commonly used by developers during software development and integration, including API keys, authentication tokens, encryption keys, database connection strings, etc.
<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 (or Restricted)	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"/>	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"/>	Public	Information that is intended for public consumption and poses no risk to the organization or individuals if disclosed.
Data Residency (7)		
<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"/>	EU	European Union
<input checked="" type="checkbox"/>	JAPAN	Japan
<input checked="" type="checkbox"/>	UK	United Kingdom
<input checked="" type="checkbox"/>	US	United States
Compliance (16)		

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:

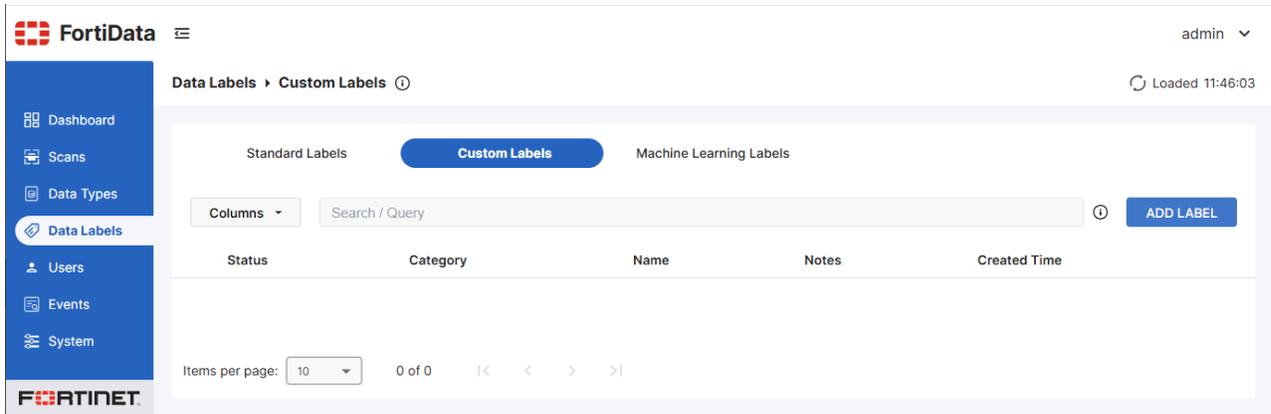
- ID
- Status
- Category
- Name
- Notes



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

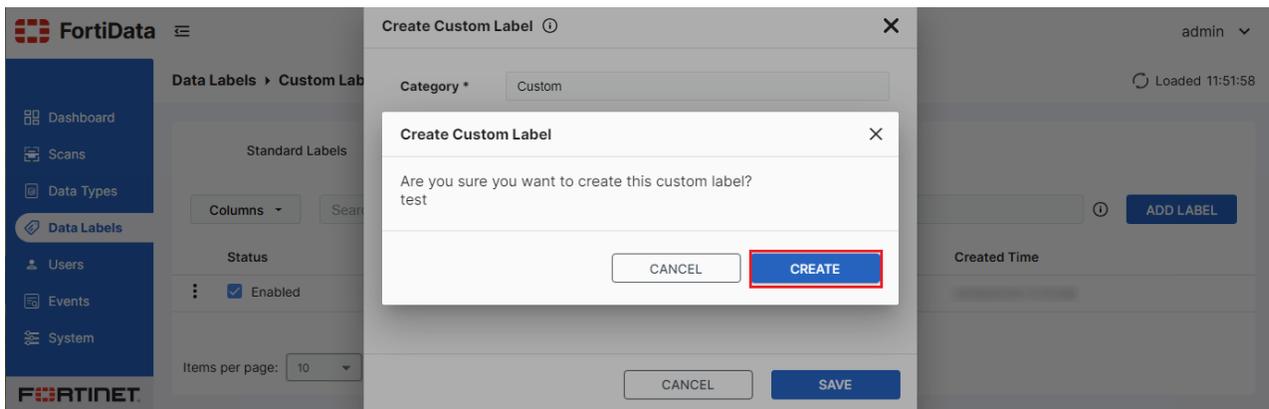
Name * Please Input

Status * Enabled

Notes

CANCEL SAVE

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



Machine Learning Labels

The *Machine Learning Labels* tab displays a list of data labels generated by FortiData machine learning. You can search the machine learning data labels by name.

FortiData
admin

- Dashboard
- Scans
- Data Types
- Data Labels
- Users
- Events
- System

Data Labels > Machine Learning Labels
Loaded 11:54:50

Standard Labels
Custom Labels
Machine Learning Labels

Enabled	Name	Full Label - Description
Finance (6)		
<input type="checkbox"/>	Contracts and Agreements	ML/Finance/Contracts and Agreements - A formal document that records the terms of a financial transaction or service, including loan agreements, investment management contracts, and insurance policies. These documents establish the rights, obligations and responsibilities between the parties involved.
<input type="checkbox"/>	Credit and Risk Management	ML/Finance/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.
<input type="checkbox"/>	Financial Report	ML/Finance/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.
<input checked="" type="checkbox"/>	Other	ML/Finance/Other - Other financial documents or records that do not fall into the predefined categories.
<input type="checkbox"/>	Strategy and Research	ML/Finance/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.
<input type="checkbox"/>	Transaction Record	ML/Finance/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 (6)		
<input type="checkbox"/>	Clinical Records	ML/Healthcare/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.
<input checked="" type="checkbox"/>	Insurance and Settlement	ML/Healthcare/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.
<input checked="" type="checkbox"/>	Legal and Compliance	ML/Healthcare/Legal and Compliance - 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.
<input checked="" type="checkbox"/>	Medication Management	ML/Healthcare/Medication Management - Documentation involving drug prescriptions, medication instructions, and drug monitoring. This includes prescription orders, medication records and adverse drug

Users



The *Users* page is available to admin users only.

The FortiData system has one default administrative account named "admin", which is a super administrator with the highest privileges, including creating or deleting admin users.

The screenshot shows the FortiData interface with the 'Users' tab selected. The user list contains one entry:

Username	Roles	Created On
admin	Super Admin	2024/12/16 14:02:01

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*.

The screenshot shows the FortiData interface with the 'Users' tab selected. The user list contains three entries:

Username	Roles	Created On
policy	Policy Manager	
admin_regular	Administrator	
admin	Super Admin	

A context menu is open for the 'admin' user, showing options: Edit User, Delete User, and Change Password (highlighted with a red box).

To create a user:

1. On *User* 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 *Role Permissions* tab.

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.

Name	Permissions
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.

- Specify the password and confirm it.
- Click *SAVE*.

Add User
✕

Username *

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

Roles

Administrator
 Policy Manager
 Incident Manager
 Compliance Officer
 Data Owner

Password *

Confirm Password *

- Click *YES* to confirm.

To change the role of a user:

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

To delete a user:

- 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.

Events

System events log data is available in the *Events* page. You can search the logs by different conditions and export the log as reports in JSON or CSV format.

Log Settings

Click *LOG SETTINGS* to open the *Log Settings* window:

The screenshot shows the FortiData interface. On the left is a navigation menu with options: Dashboard, Scans, Data Types, Data Labels, Users, Events (selected), and System. The main area displays 'System Events' with a table of logs. The table has columns: Time, Level, Type, Username, Action, Description, and Message. The logs show a mix of 'Info' and 'Warning' levels for 'Users' type, with actions like 'login' and 'logout'. A search bar at the top of the table is set to 'Username = admin'. At the bottom of the table, it shows 'Items per page: 10' and '1 - 7 of 7'. On the right, the 'Log Settings' window is open, showing:

- Log Retention Period: 7 days (1-28 days)
- Event Logging Options: All (selected), Customize
- Send logs to syslog server
- Server IP: [Redacted]
- Port: 514
- Buttons: Cancel, Save

You can configure the following options for logs:

Log Settings ×

Log Retention Period days (1-28 days)

Event Logging Options All Customize

Send logs to syslog server

Server IP

Port

Log Retention Period	Specify the number of days for which the log will be retained.
Event Logging Options	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 following event types as needed: <ul style="list-style-type: none">• Dashboard• Data Labels• Data Types• Discovery Policies• Scans• System• Users
Send logs to syslog	Enable to send the log to the syslog server when saving logs. You can then specify the IP and port of the syslog server.

System

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

- [Network on page 37](#)
- [Settings on page 39](#)
- [Certificates on page 41](#)
- [Backup/Restore on page 41](#)

Network

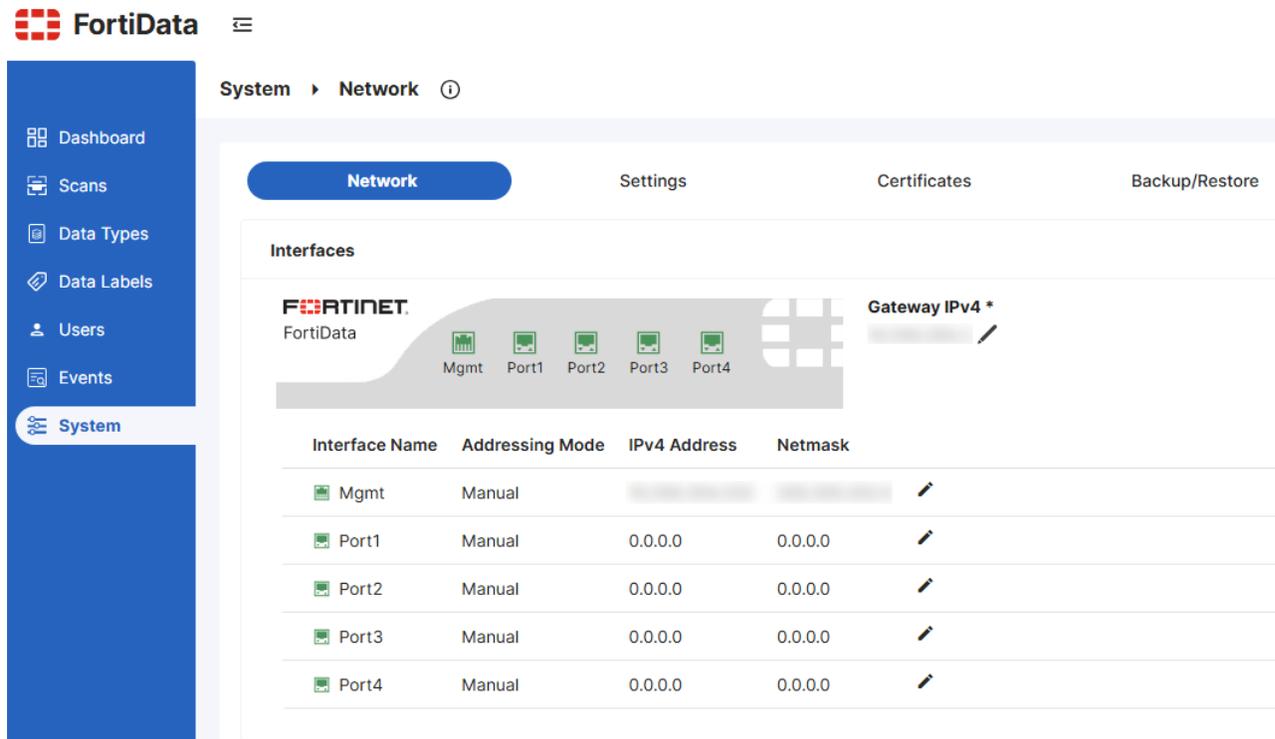
Configure the interfaces and DNS settings for FortiData in the *System > Network* tab.

Interfaces

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

To configure the interfaces:

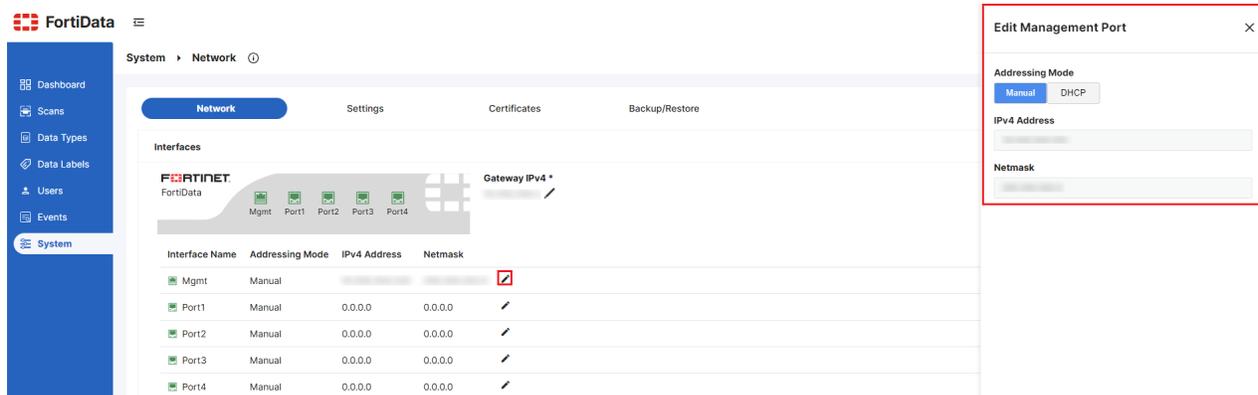
1. In the *System > Network* tab, click *Interfaces* to display the interfaces setting.



The screenshot shows the FortiData web interface. The left sidebar contains navigation options: Dashboard, Scans, Data Types, Data Labels, Users, Events, and System (selected). The main content area is titled 'System > Network' and has tabs for Network, Settings, Certificates, and Backup/Restore. The 'Network' tab is active, displaying the 'Interfaces' section. At the top, there is a visual representation of the device with icons for Mgmt, Port1, Port2, Port3, and Port4. Below this is a table with the following columns: Interface Name, Addressing Mode, IPv4 Address, and Netmask. The table contains five rows: Mgmt, Port1, Port2, Port3, and Port4. Each row has a pencil icon in the Netmask column, indicating that the settings can be edited.

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 the default gateway or an interface to edit the settings.



This screenshot shows the same interface as the previous one, but with the 'Edit Management Port' dialog box open. The dialog box has a title bar with a close button (X) and contains three fields: 'Addressing Mode' with radio buttons for 'Manual' (selected) and 'DHCP'; 'IPv4 Address' with a text input field; and 'Netmask' with a text input field. A red box highlights the dialog box.

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

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

DNS

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

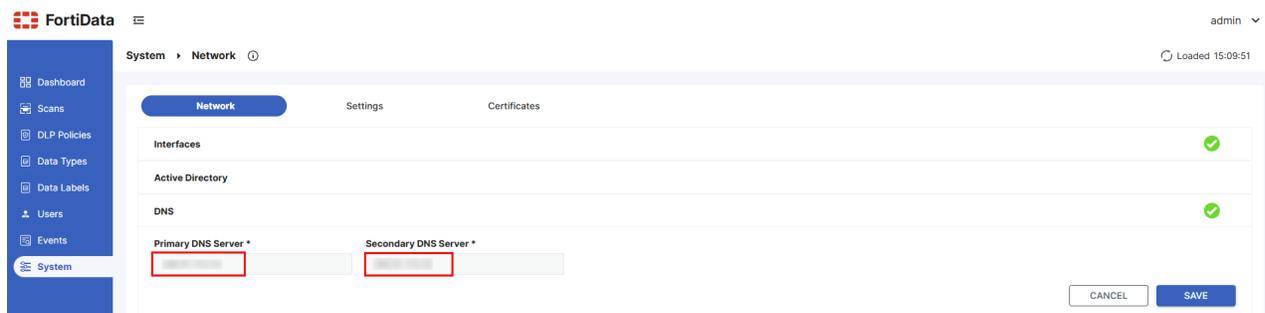
Your Internet service provider (ISP) may supply IP addresses of DNS servers, or you may want to use the IP addresses of your own DNS servers. You must provide unicast, non-local addresses for your DNS servers. Localhost and broadcast addresses will not be accepted.



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

To configure DNS settings via the web UI:

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



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

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

Settings

In this section, you can configure the following:

Admin Settings

HTTPS Server Certificate

Select the TLS certificates uploaded in *System > Certificates on page 41*.

You must reboot the appliance after changing the HTTPS server certificate.

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
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

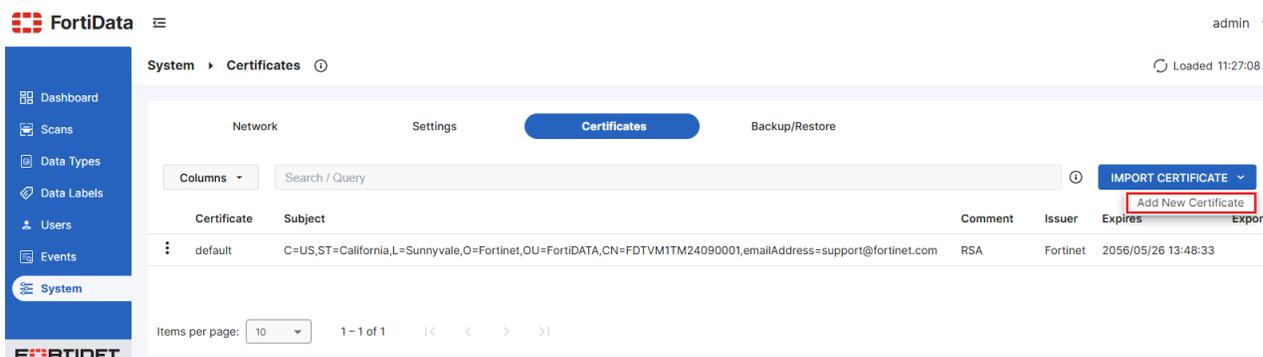
Enter the interval, in minutes, at which the system time is synchronized with the NTP server. The default is 60.

Certificates

You can upload customized TLS certificates for HTTPS access to FortiData's GUI in the *System > Certificates* tab and then apply the certificate in the *System > Settings on page 39* tab,

To import a certificate using certificate file and key file:

1. Go to *System > Certificates*.
2. Click *IMPORT CERTIFICATE > Add New Certificate*.

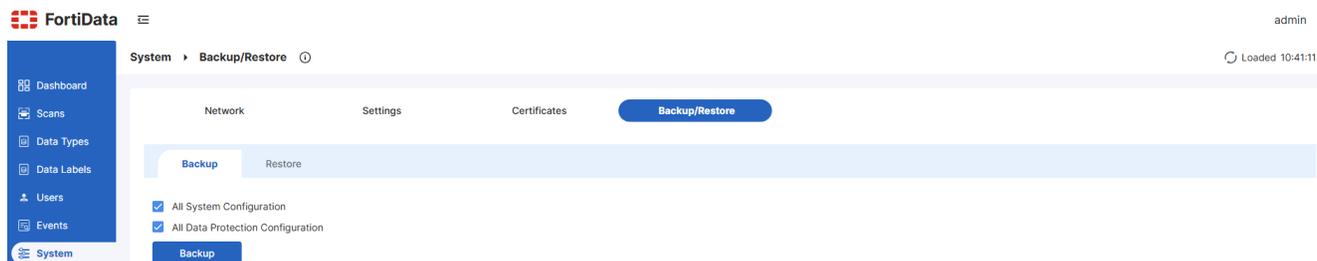


3. Click *BROWSE* to select the certificate file and key file respectively from your local directory.
4. **(Optional)** Specify a passphrase, if needed.
5. Click *IMPORT*.
6. Click *Close*.

To apply the certificate, go to the *System > Settings on page 39* tab.

Backup/Restore

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



To back up the FortiData configurations:

1. In the *Backup* tab, 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* tab, 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.