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.

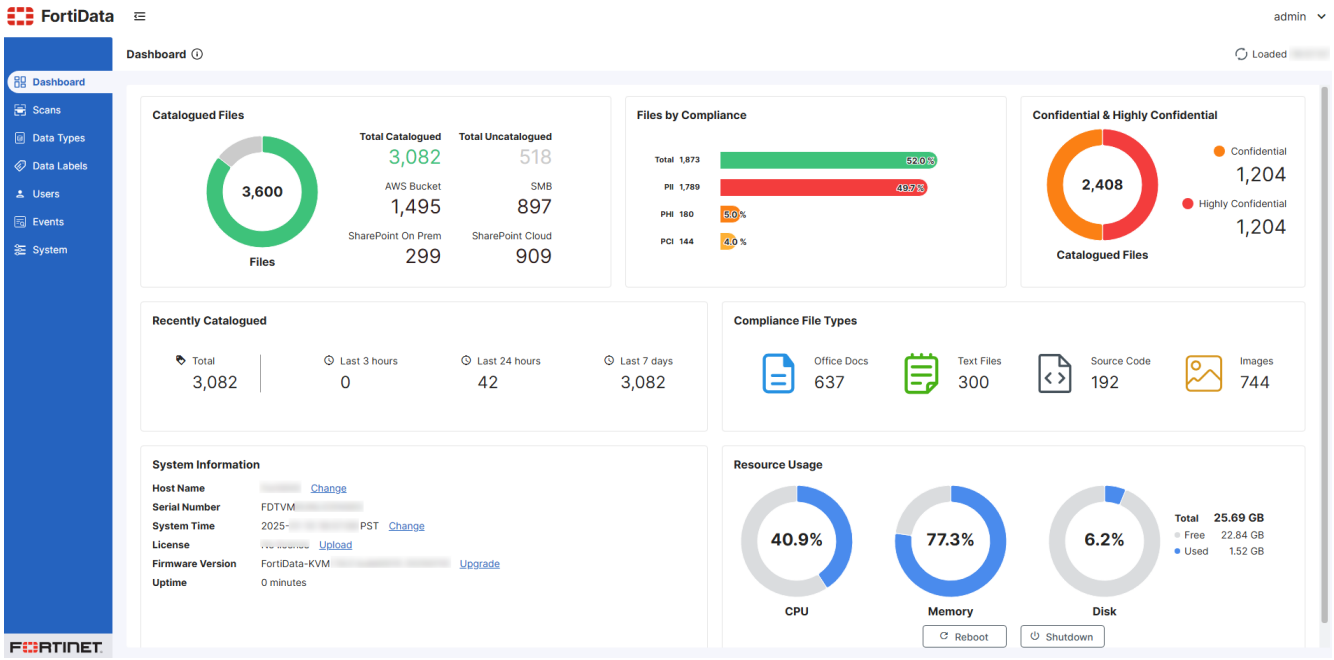
Getting started

Perform the following procedures to get started with FortiData:

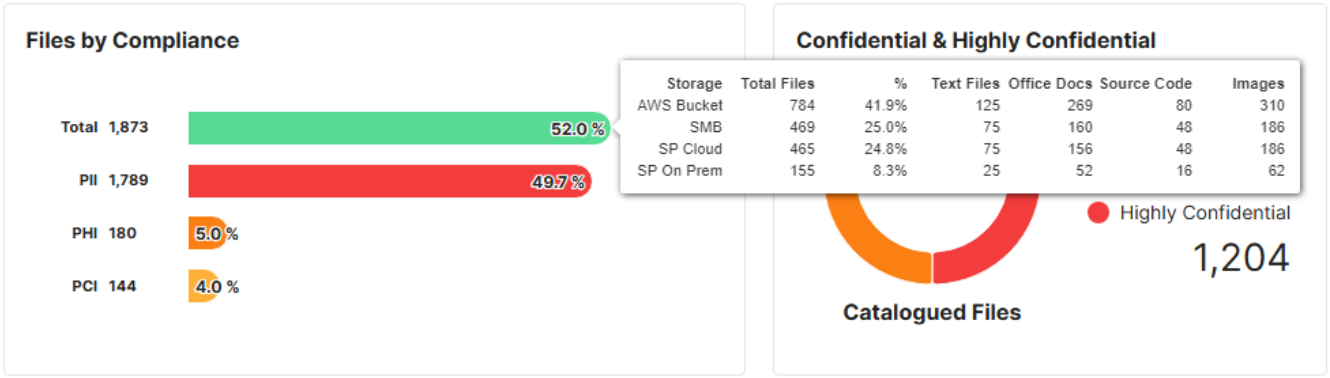
1. Configure interface and DNS settings. See Network on page 37
2. Configure timeout and system time. See Settings on page 39.
3. Configure HTTPS server certificate. See Certificates on page 41.
4. Create users of with different access scope to FortiData. See Users on page 32.
5. Create discovery policies 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).

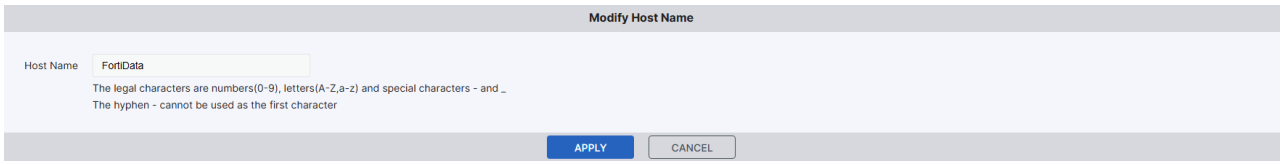


For the *Files by Compliance* and *Confidential & Highly Confidential* widgets, hover your mouse over each graph or chart to view more details about the data points.



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.



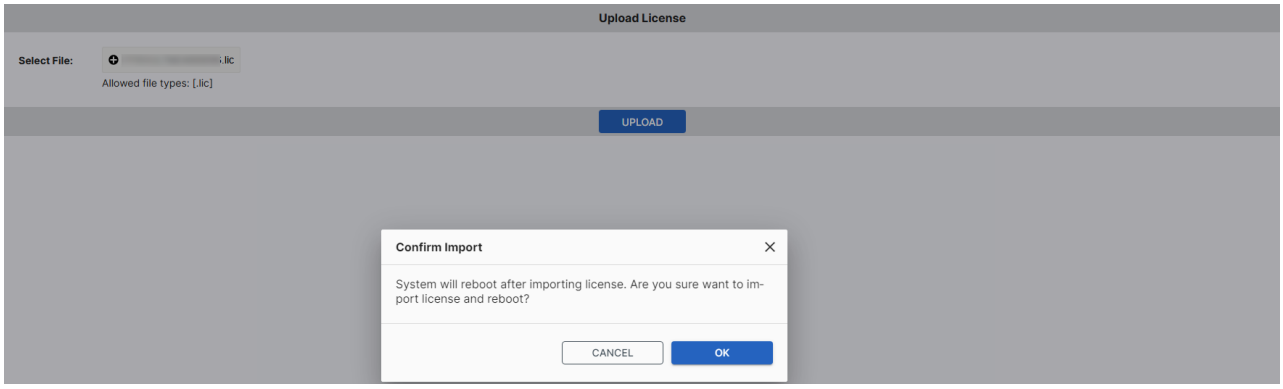
3. Specify the desired hostname and click *APPLY*.

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:

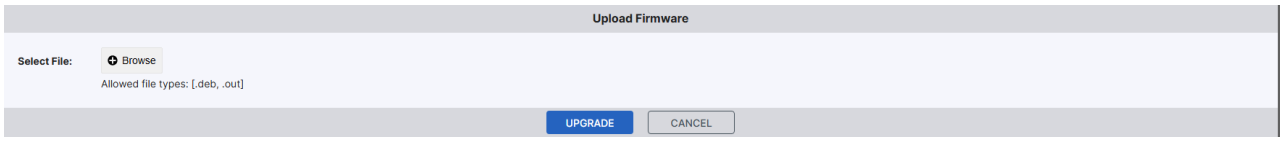
1. Go to the *Dashboard* > *System Information* widget.
2. Click *Upload* or *Upgrade* at the end of the *License* field.
3. Click *Browse* to locate the license file on your local disk.
4. Click *UPLOAD*.
5. Click *OK* when prompted.



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*.

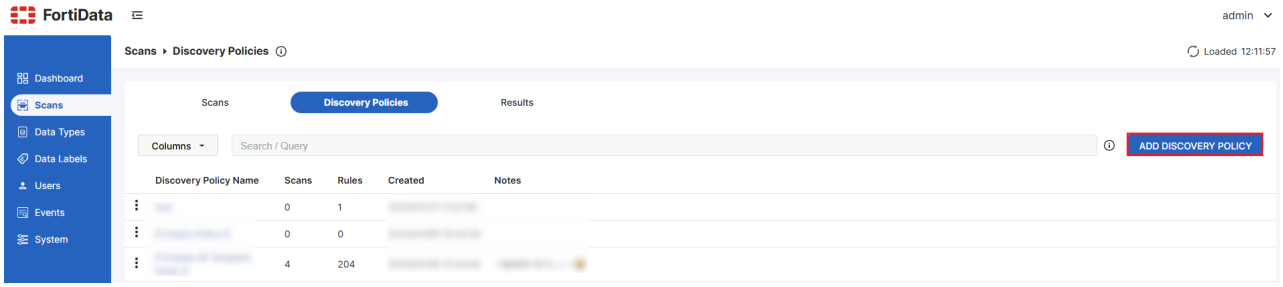
Alternatively, run the `execute shutdown` command via the CLI.

Scans

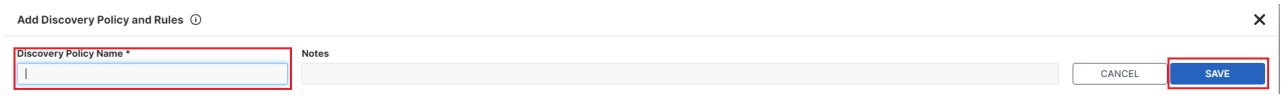
In the *Scans* page, you can create a data discovery policy to look for specific types of data (using data types) in files, such as financial transactions or health records, and add specific tags (using data labels) to files that meet the specified conditions. You can then define a scan to access and 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*.

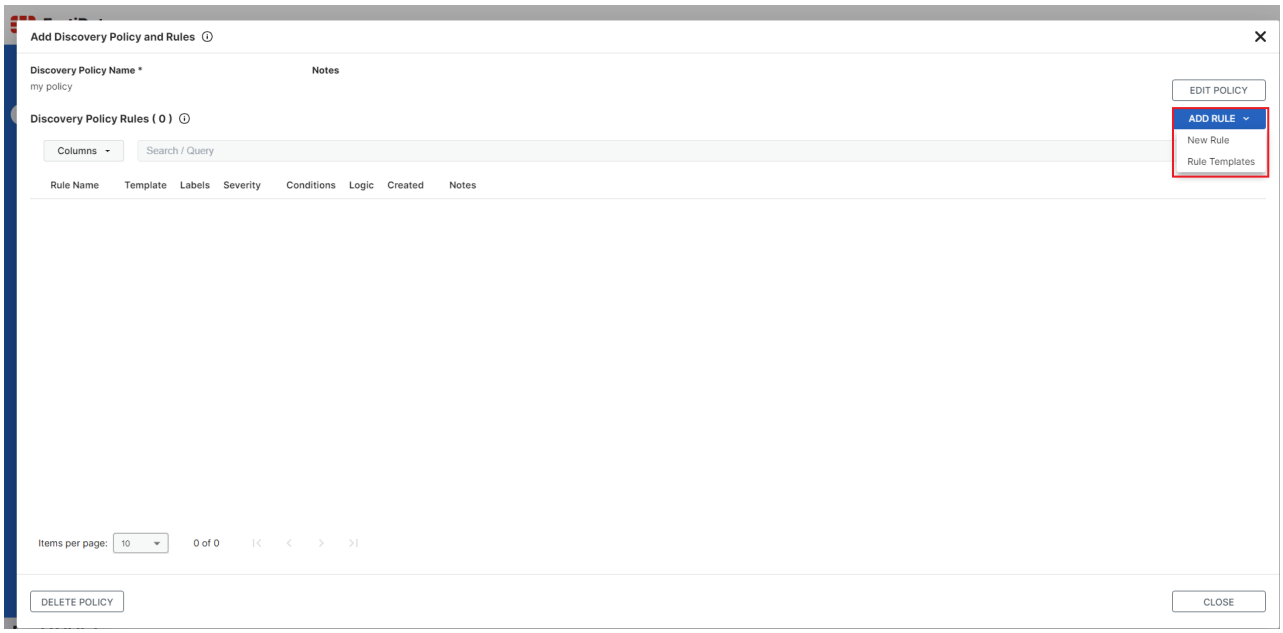


3. Specify the policy name and any notes, and then click *SAVE*.

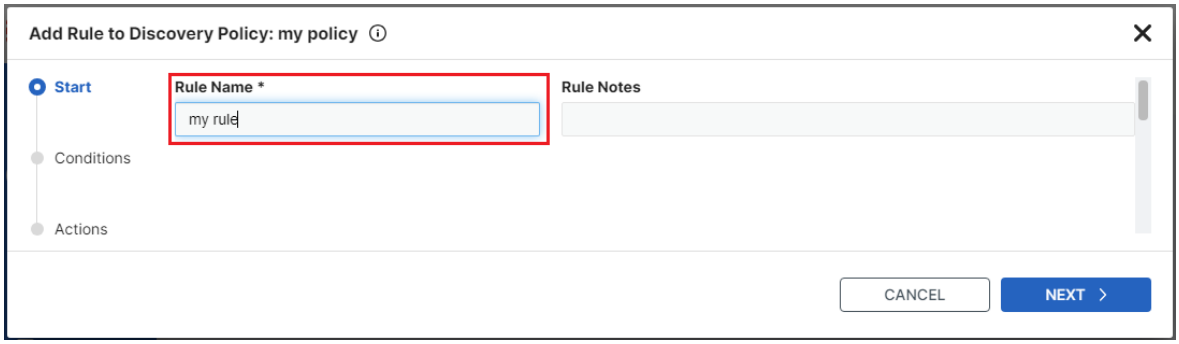


4. Click *ADD RULE* and select *New Rule* or *Rule Templates*, depending on whether you want to create your own data discovery rule or use a rule template predefined in FortiData.

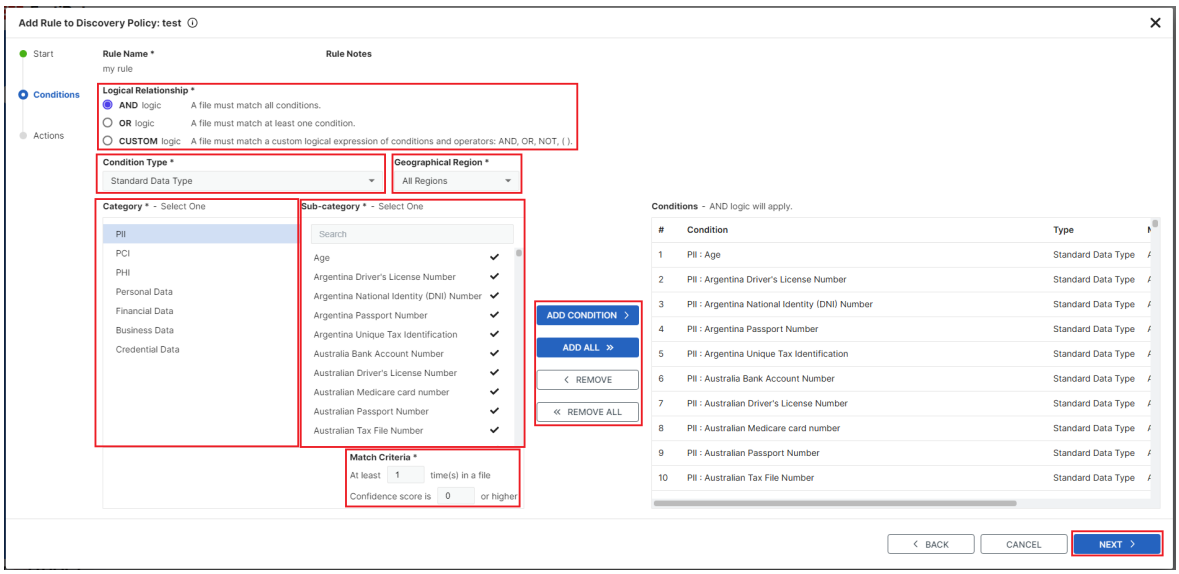
   A rule is a defined data pattern with a set of data types and logic conditions that a discovery policy maps to when recognizing patterns in files. You can view the full list of rule templates in the *Rule Templates* tab in the Data Types on page 22 page,



- 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
Logical Relationship	Select from the following logic options: • *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.

Condition Type	Select from the following condition types:
	 
	The full list of data types under each condition type (except for *File Type*) can be found in the corresponding tab in the Data Types on page 22 page.
	• *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.
	• *File Type*—Choose from the following file types:
	  • 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`.
	• *Machine Learning Document Classification Type*—List of data types that are created and dynamically updated by FortiData based on machine learning algorithms.

• *Category/Sub-category* • *Group Name/Data Type* **Note** - This option is specific to the *Custom Data Type Group* condition type.	• 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*.

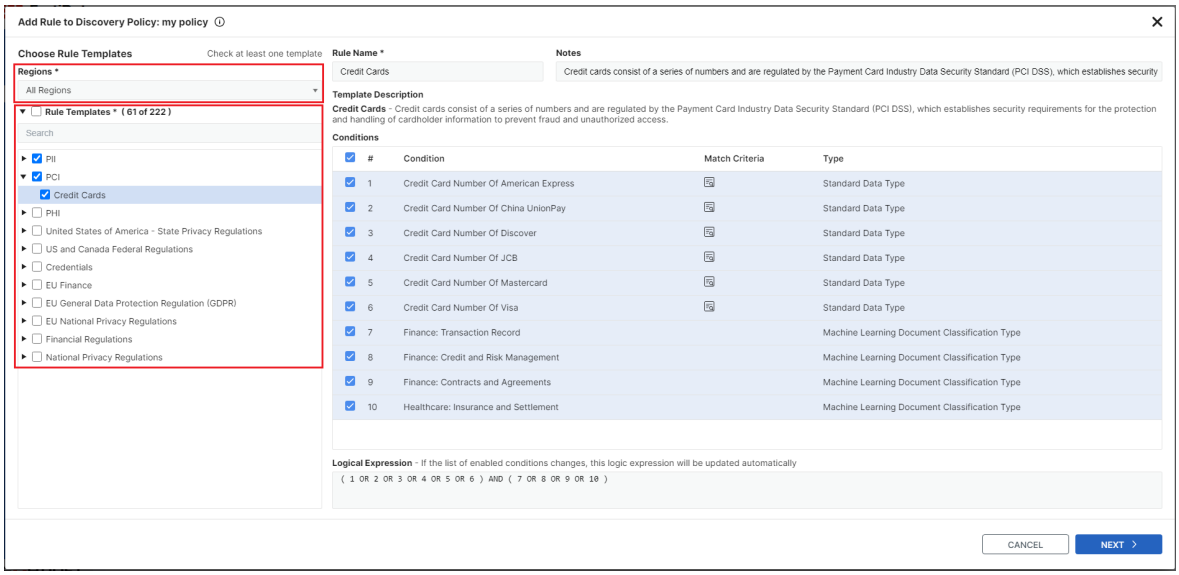
Option	Description
Match Criteria	For *Standard Data Type* and *Custom Data Type Group* condition types, you can configure the following thresholds: • The number of times the condition must match in the file in order to flag the file and perform the defined action. • The confidence score of the match. A result is considered a match only if the confidence score exceeds the specified threshold. For *File Type* and *Machine Learning Document Classification Type* condition types, the match criteria is always exact match.

iii. Add or remove conditions as needed.

iv. Click *NEXT*.

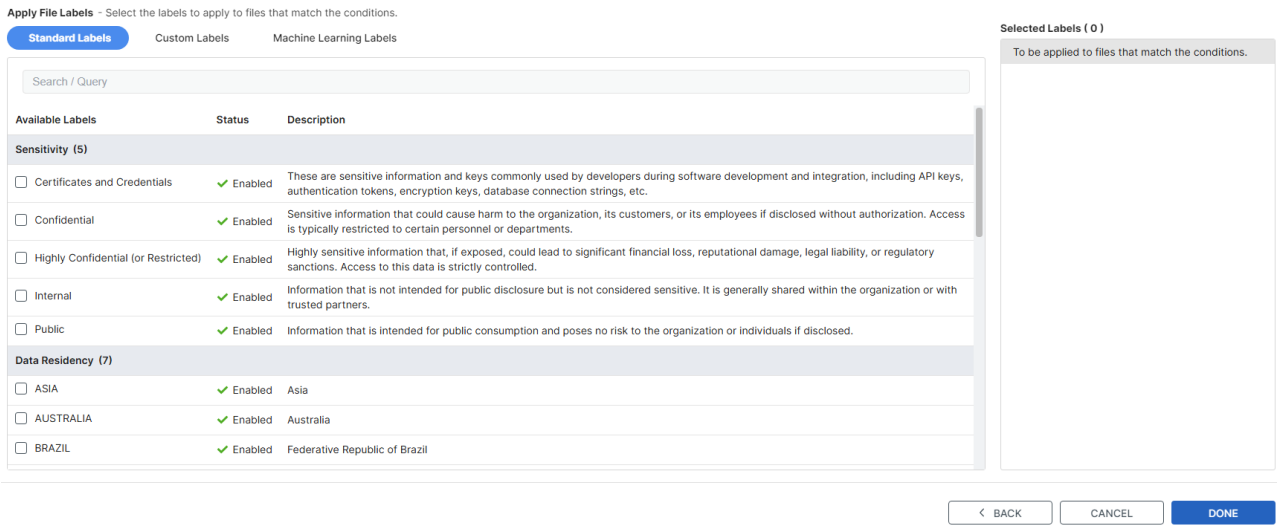
- To add a rule based on the FortiData templates:

i. Specify the region 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.

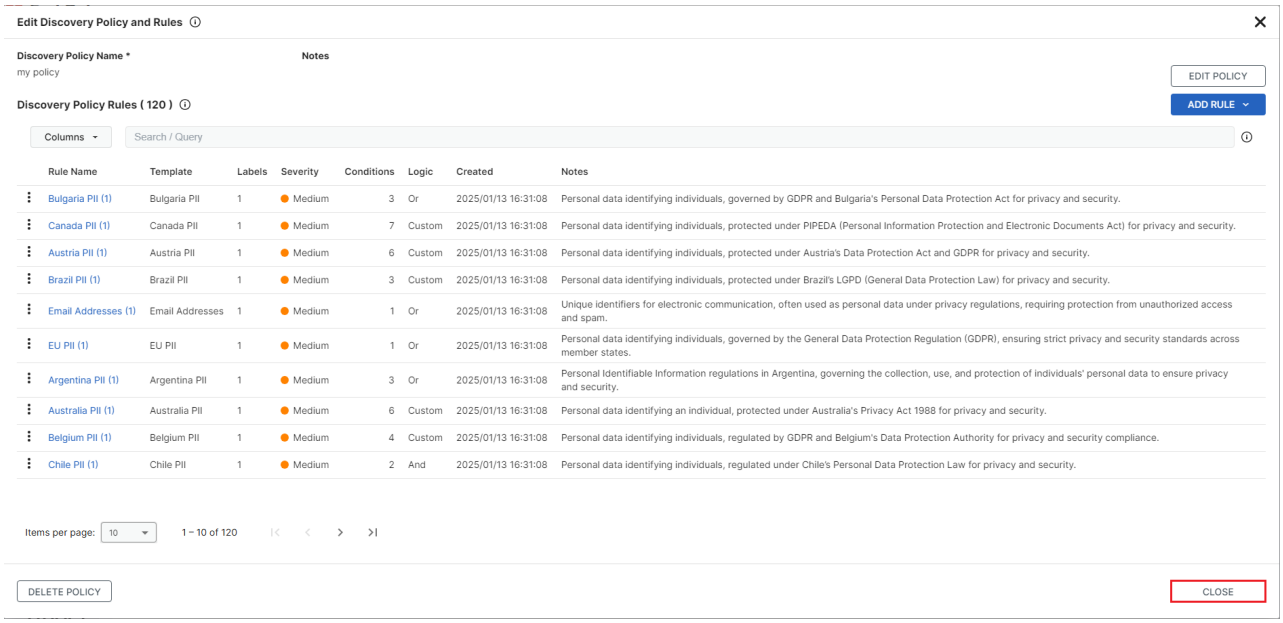


Choose from the following types and select labels under each type:

- 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
Standard Labels	Predefined labels by FortiData.
Custom Labels	Custom labels that you created.
Machine Learning Labels	Machine learning labels. You can select from the following modes: **Mode** / **Description** *Disable* — Do not apply machine learning labels to any matching files. *Automatic* — Automatically apply machine learning labels to matching files. *Manual* — Only apply selected machine learning labels to matching files. 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.

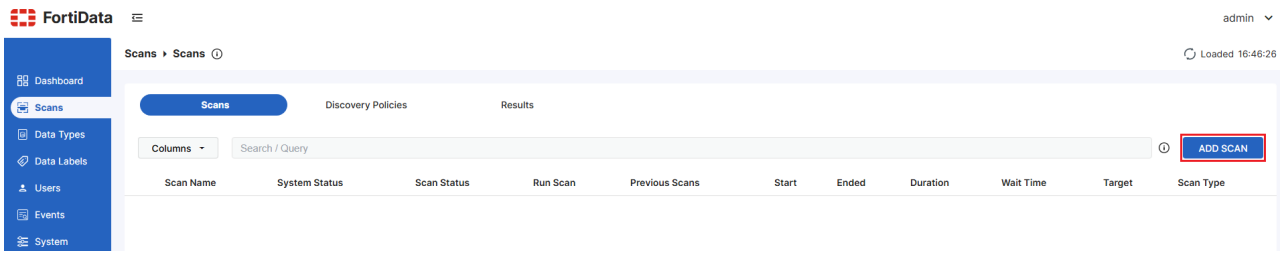
6. Click *DONE*.
7. Add more rules as needed by repeating steps 4 to 6.
8. Review the policy details and click *CLOSE*.



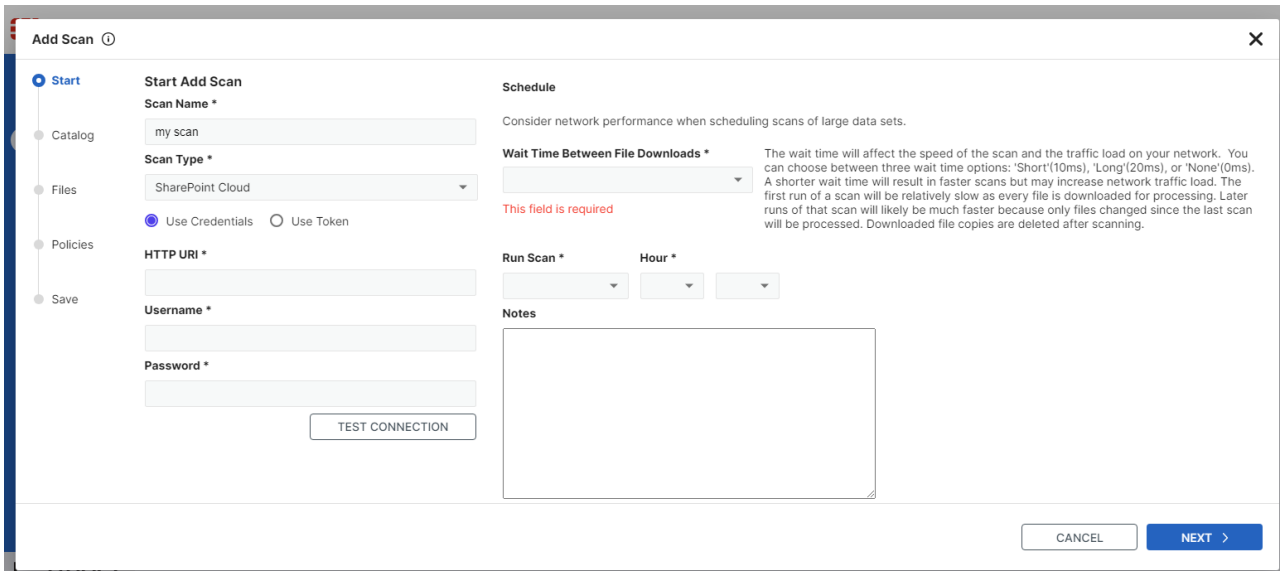
To create a scan:

You can create up to 16 scans.

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



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

Permission	Description
AuditLog.Read.All	Read all audit log data
BrowserSiteLists.Read.All	Read all browser site lists for your organization
Files.Read.All	Read files in all site collections
Files.SelectedOperations.Selected	Access selected Files without a signed in user.
Sites.Manage.All	Create, edit, and delete items and lists in all site collections
Sites.Read.All	Read items in all site collections

Scan Type	Required Permission(s)	
	Permission	**Description**
	Sites.Selected	Access selected site collections
	ActivityFeed.Read	Read activity data for your organization
	ServiceHealth.Read	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

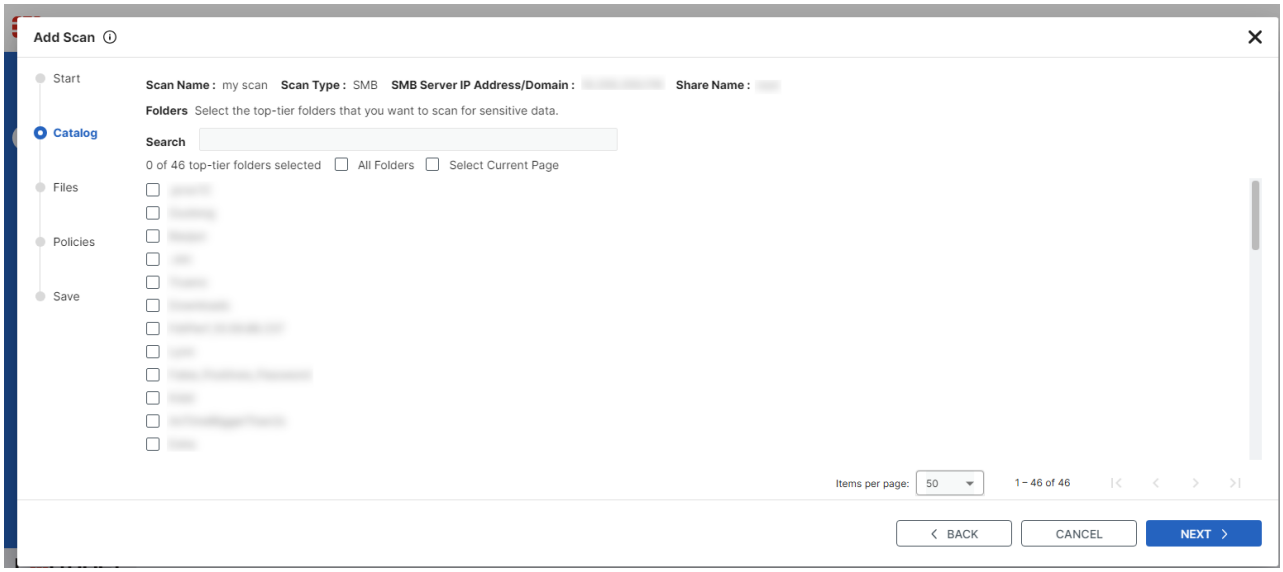
The wait time will affect the speed of the scan and the traffic load on your network. A shorter wait time will result in faster scans but may increase network traffic load. The first run of a scan will be relatively slow as every file is downloaded for processing. Subsequent runs of that scan will likely 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.

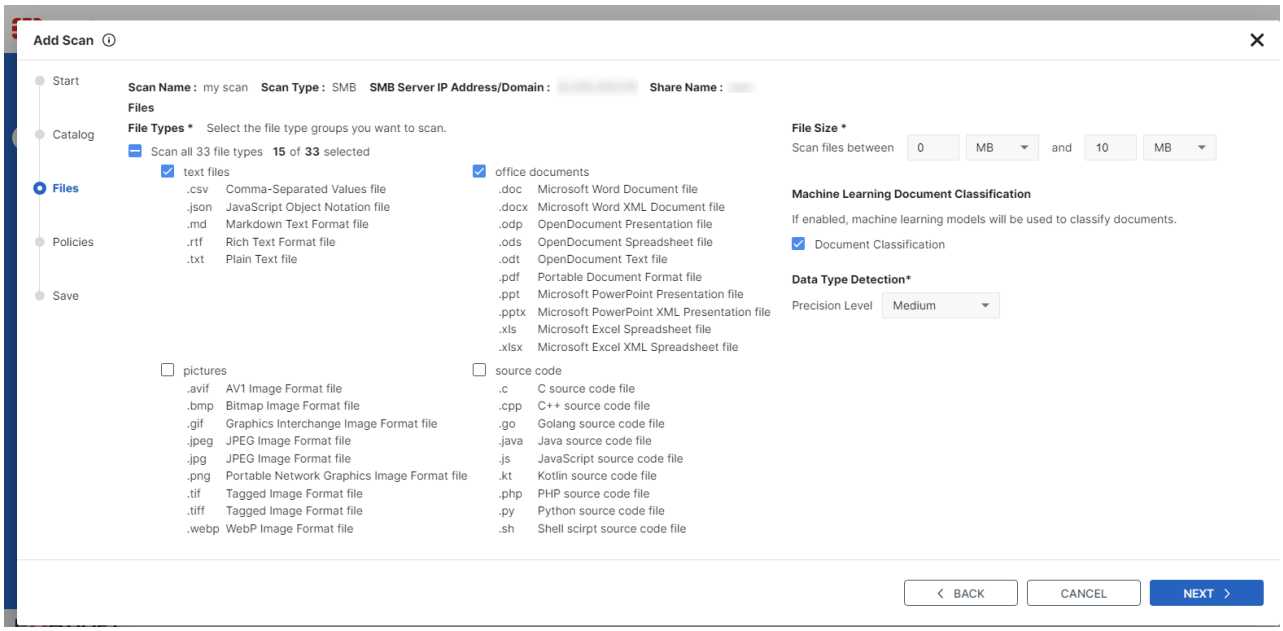
h. Click *NEXT*.

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

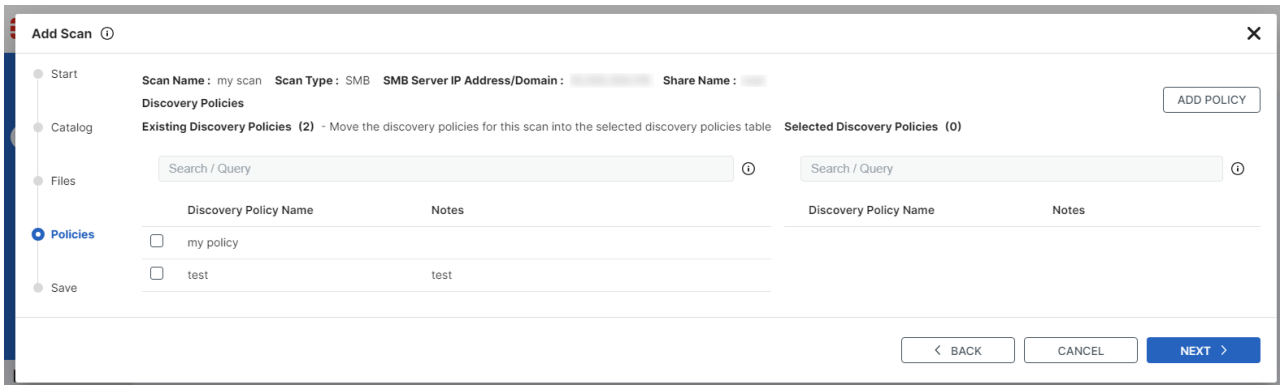


4. Configure the file types to scan, including file extensions, file size, machine learning document classification, and data type detection precision level.

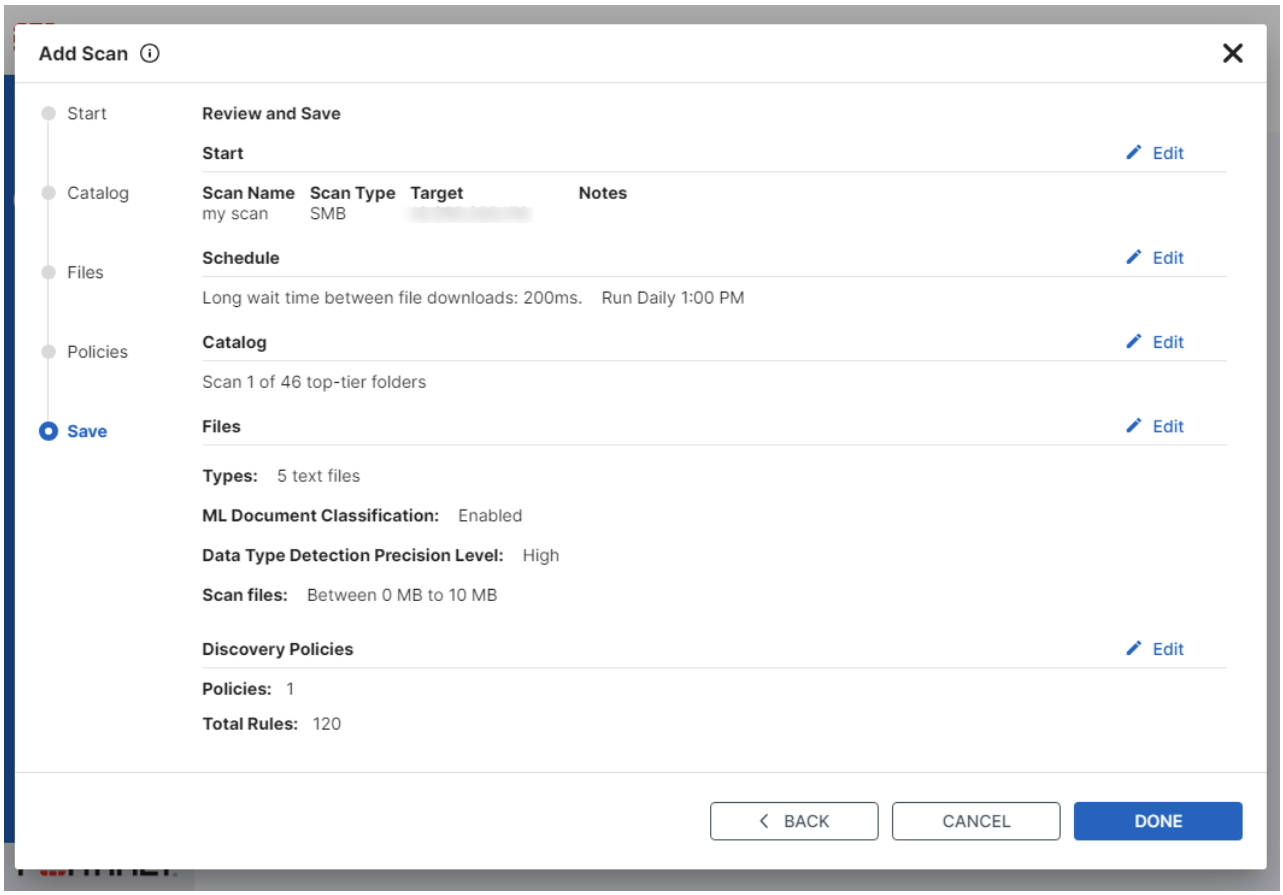
The precision level determines the threshold confidence level for data type detection. For example, if you select *High* in *Precision Level*, only data types with a confidence level of high (as predefined in FortiData) will be detected and displayed.



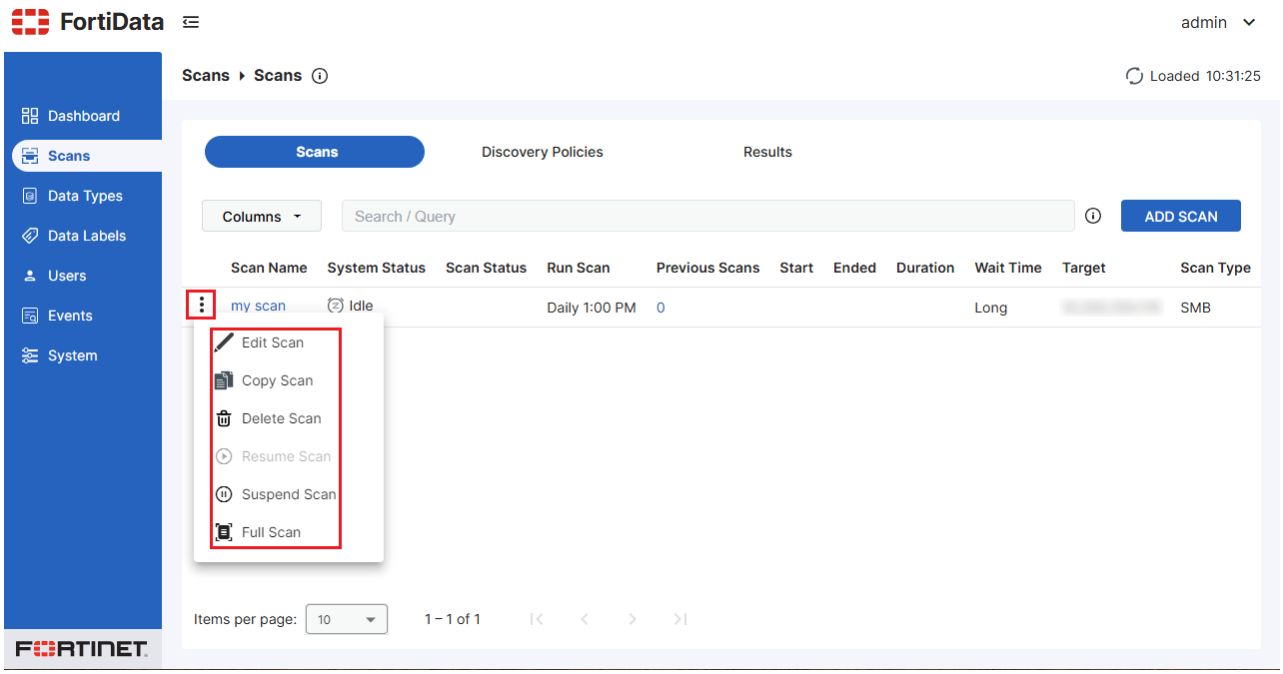
5. Click *NEXT*.
6. Select the discovery policies to apply to the scan and click *NEXT*.



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

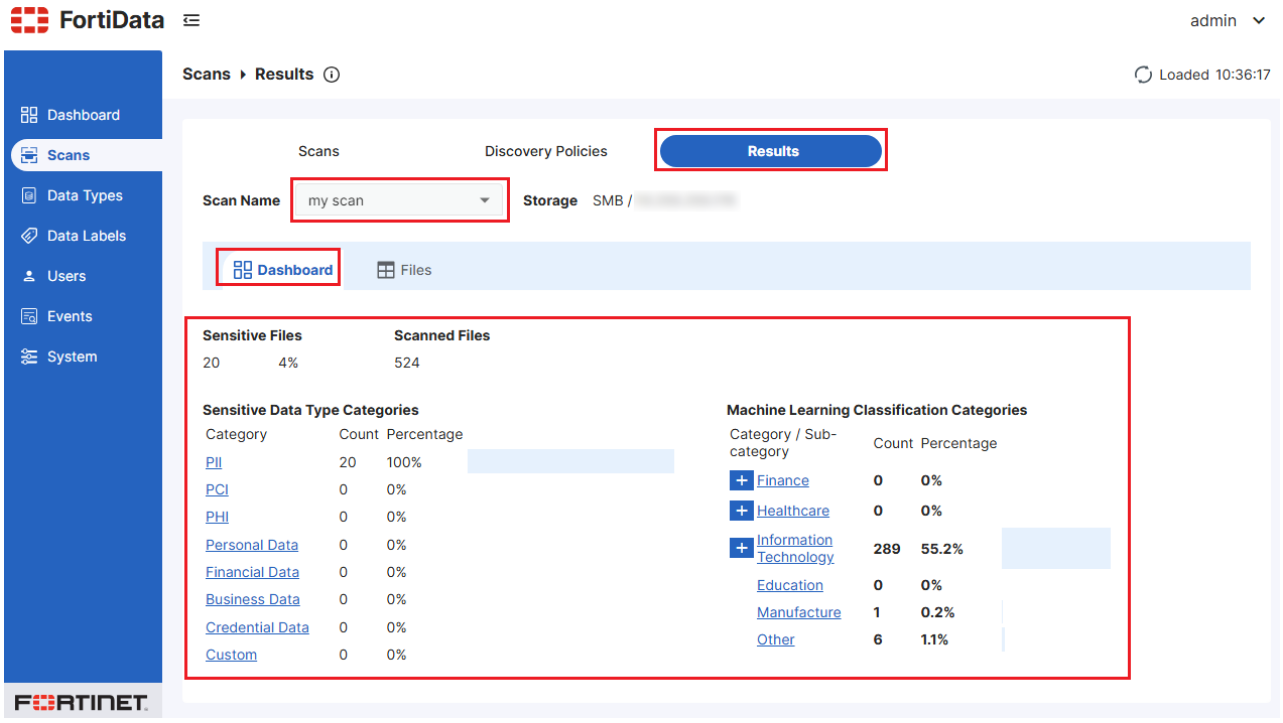


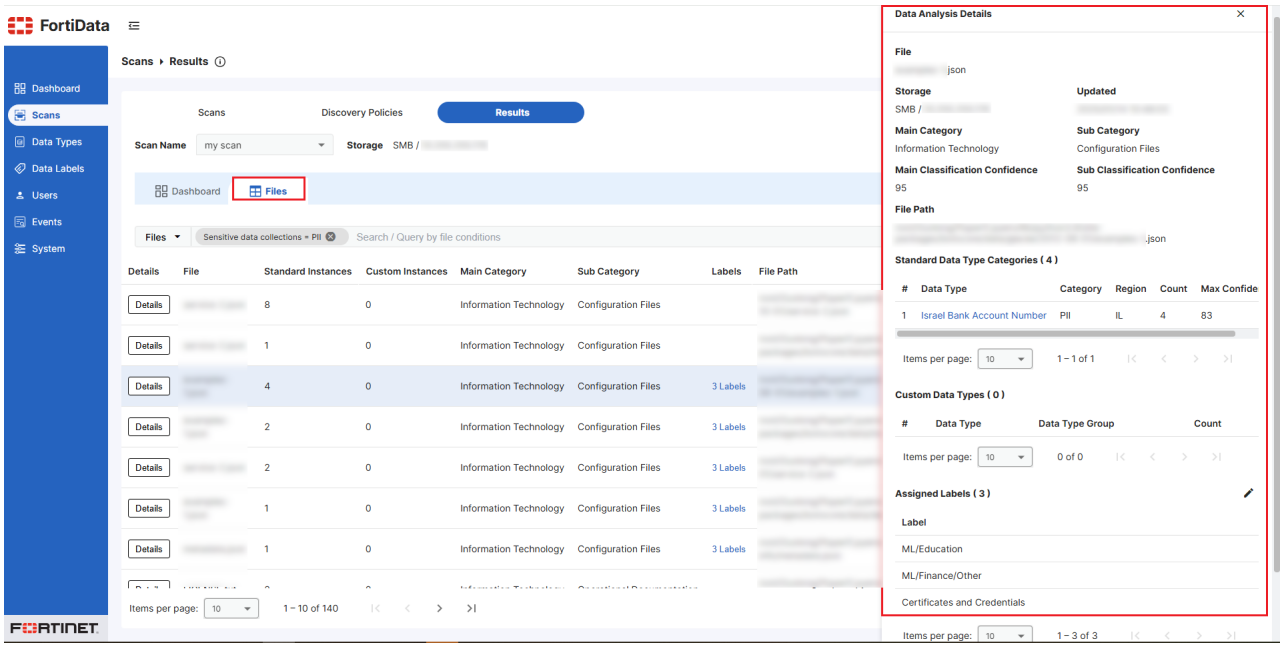
The scan is now configured to look for specific data in the target directory on the defined schedule and assign labels to files matching the conditions. You can perform the following operations on the scan by clicking the three dots at the beginning of the scan row and selecting an option from the list.



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.




FortiData
Dashboard
Scans
Data Types
Data Labels
Users
Events
System
Scans ▸ Results
Scans
Discovery Policies
Results
Scan Name
my scan
Storage
SMB /
Dashboard
Files
Files
Sensitive data collections = PII
Search / Query by file conditions
Details
File
Standard Instances
Custom Instances
Main Category
Sub Category
Labels
File Path
Information Technology
Configuration Files
3 Labels
Items per page:
1 – 10 of 140
Data Analysis Details
File
json
Storage
SMB /
Updated
Main Category
Information Technology
Sub Category
Configuration Files
Main Classification Confidence
95
Sub Classification Confidence
95
File Path
.json
Standard Data Type Categories (4)
Data Type Category Region Count Max Confide
1 Israel Bank Account Number PII IL 4 83
Items per page:
1 – 1 of 1
Custom Data Types (0)
Data Type Data Type Group Count
Items per page:
0 of 0
Assigned Labels (3)
Label
ML/Education
ML/Finance/Other
Certificates and Credentials
Items per page:
1 – 3 of 3

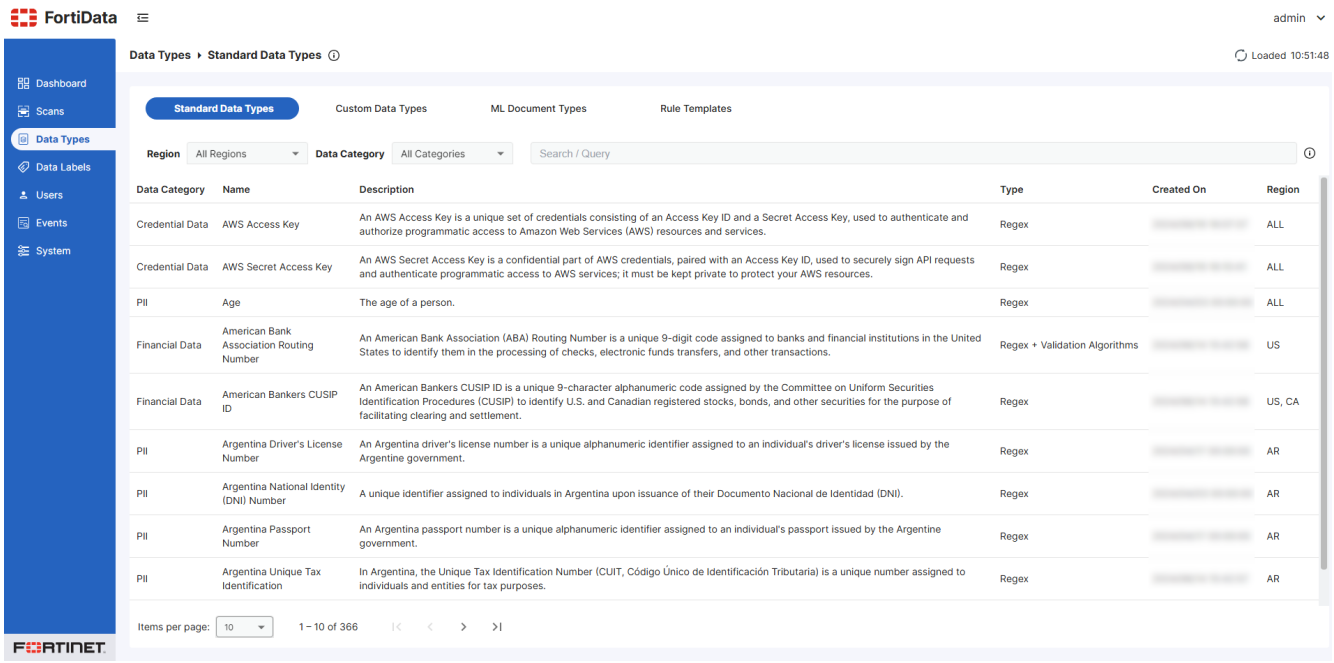
Data Types

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.

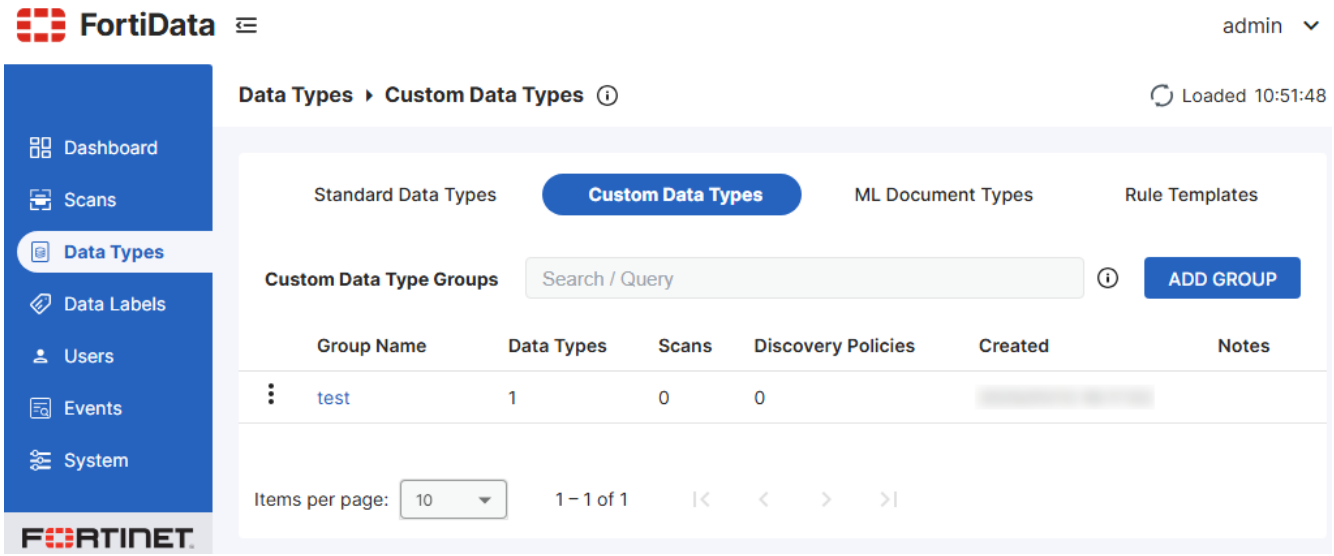
Standard Data Types

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.



Custom Data Types

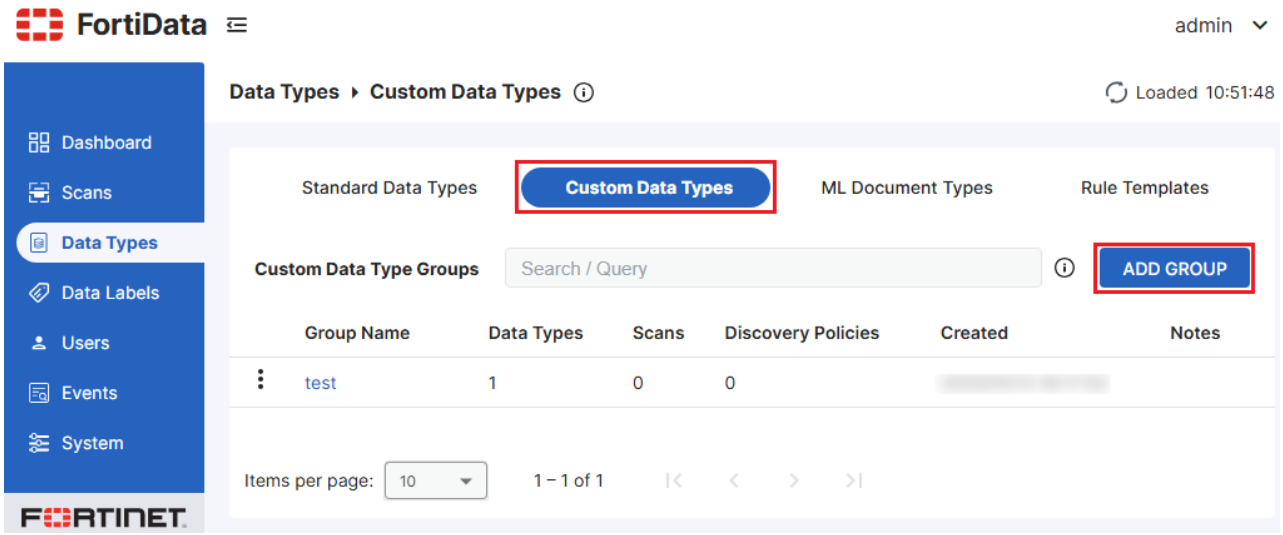
The *Custom Data Types* tab displays a list of custom data type groups that you defined in FortiData. You can search the custom data type groups by group name and/or notes.



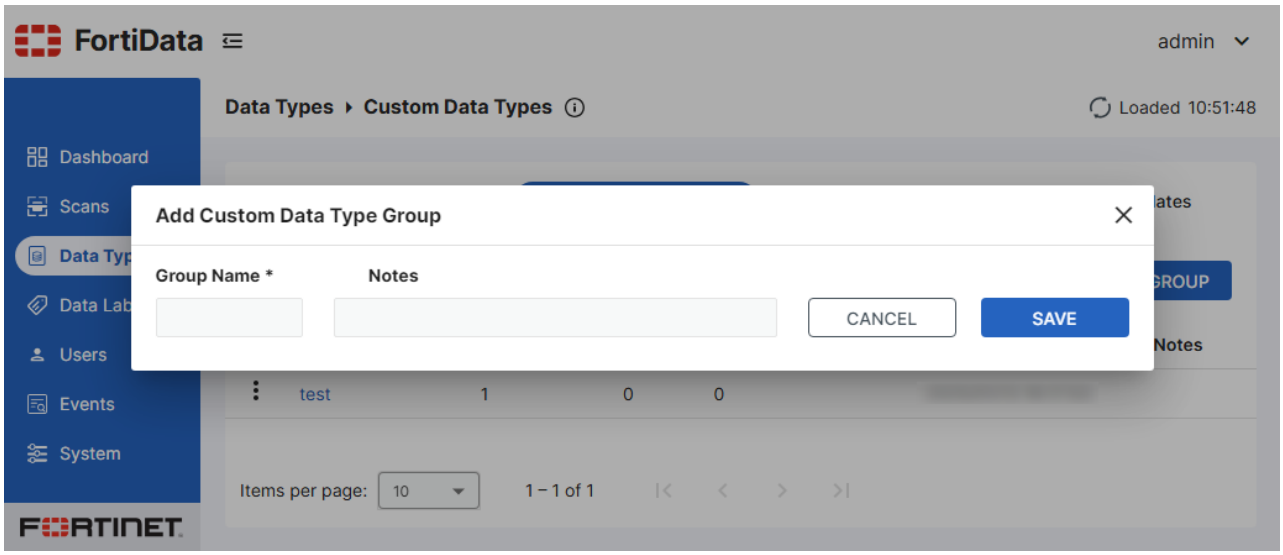
Custom data type groups are useful if the system's predefined data type do not meet your needs.

To create a custom data type group:

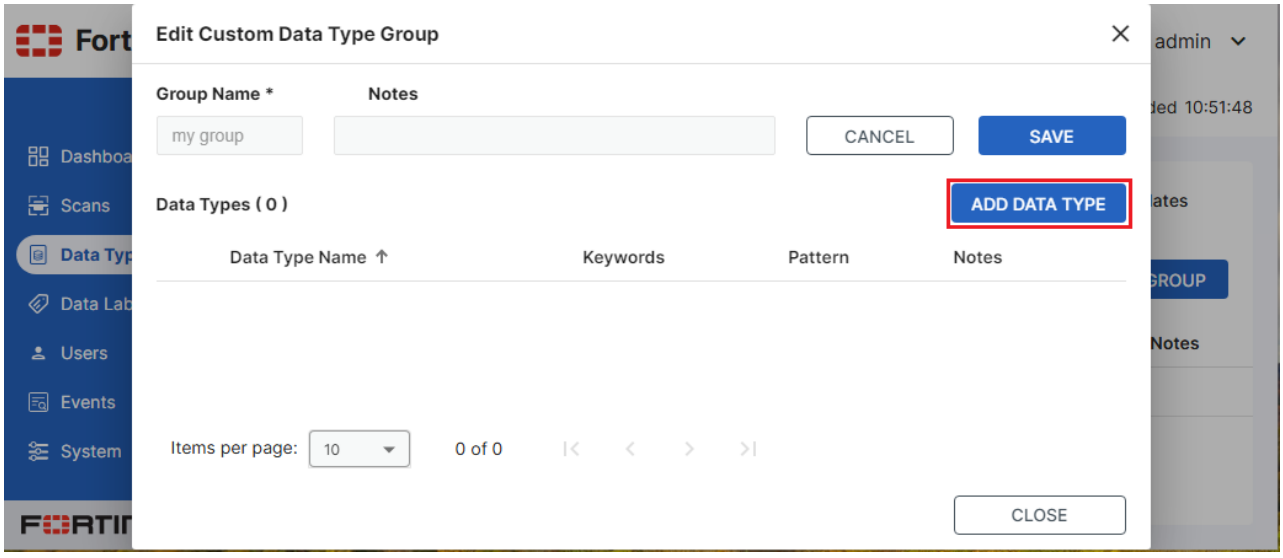
1. Go to *Data Types* > *Custom Data Types*.
2. Click *ADD GROUP*.



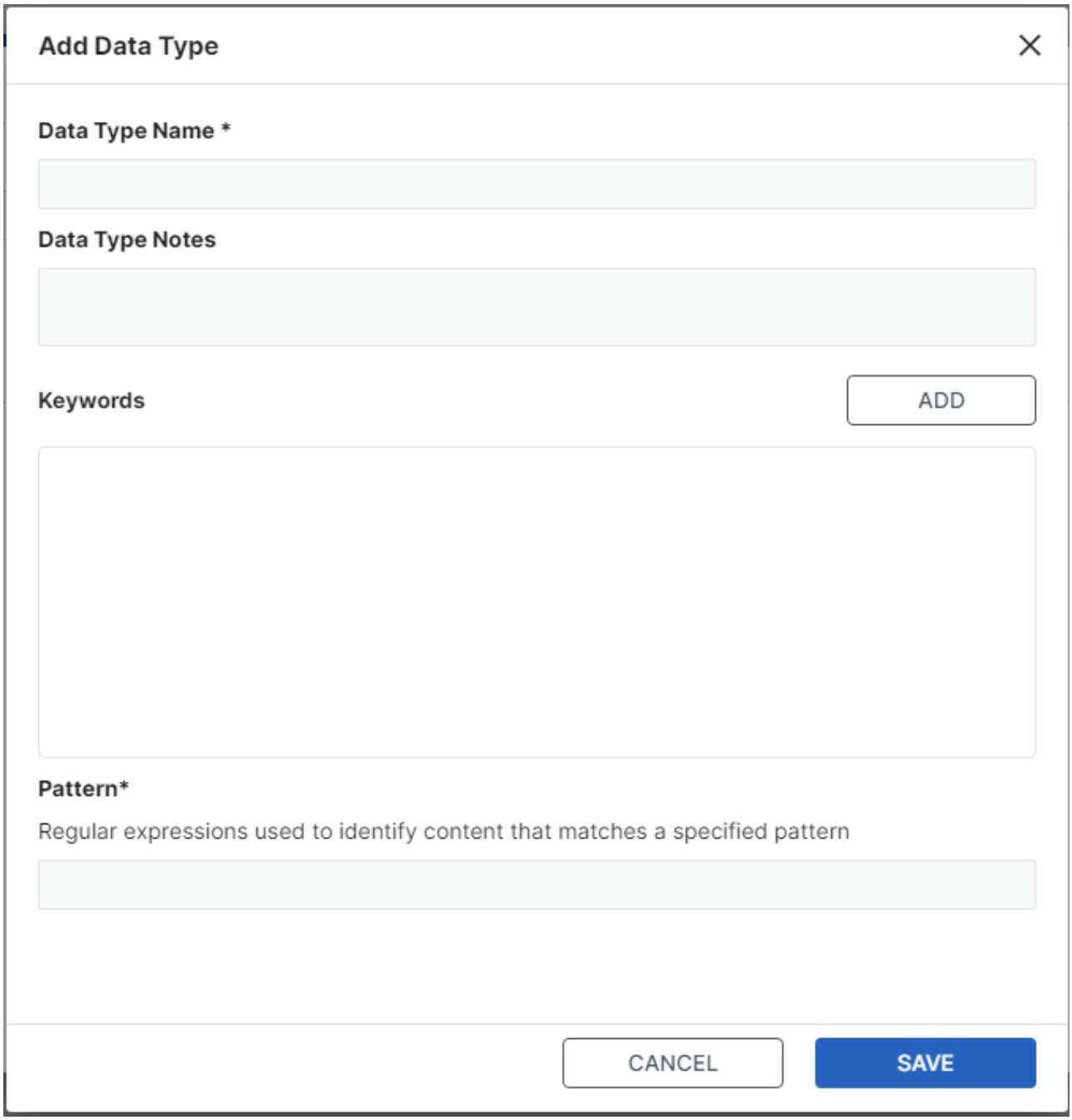
3. Specify the group name and notes, if needed.



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



6. Configure the data type with the following options:



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.

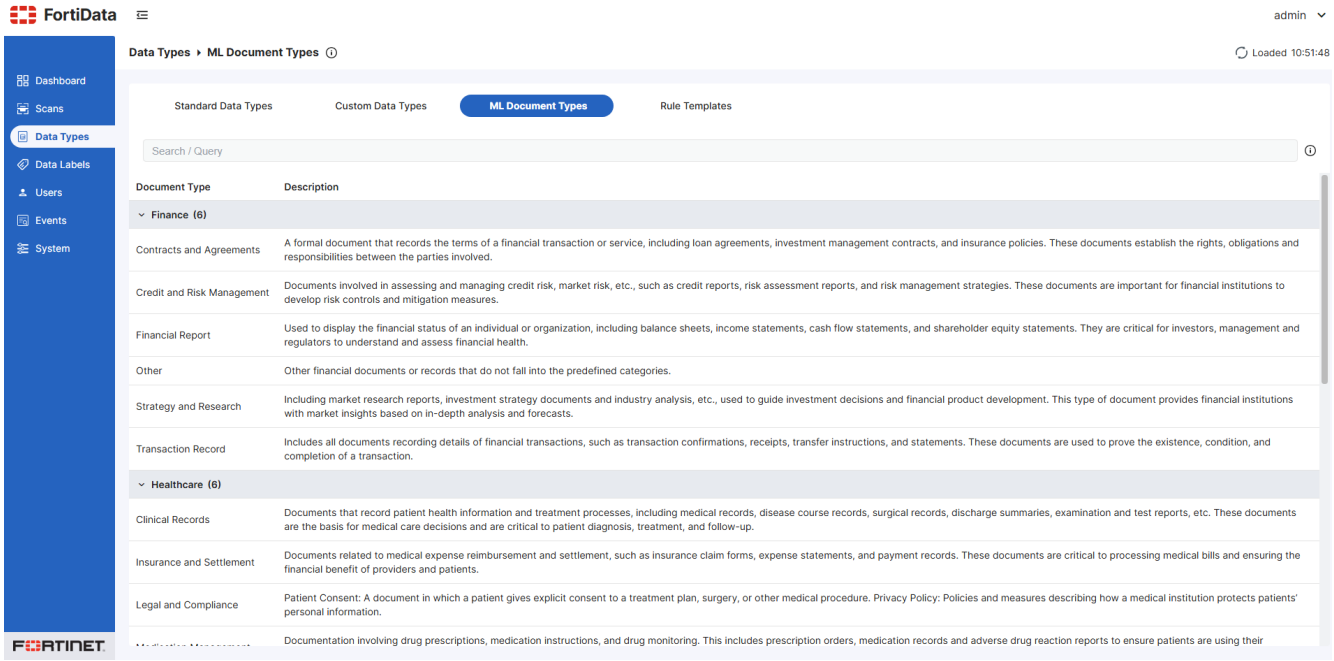
d. Click *SAVE*.

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

8. Click *CLOSE*.

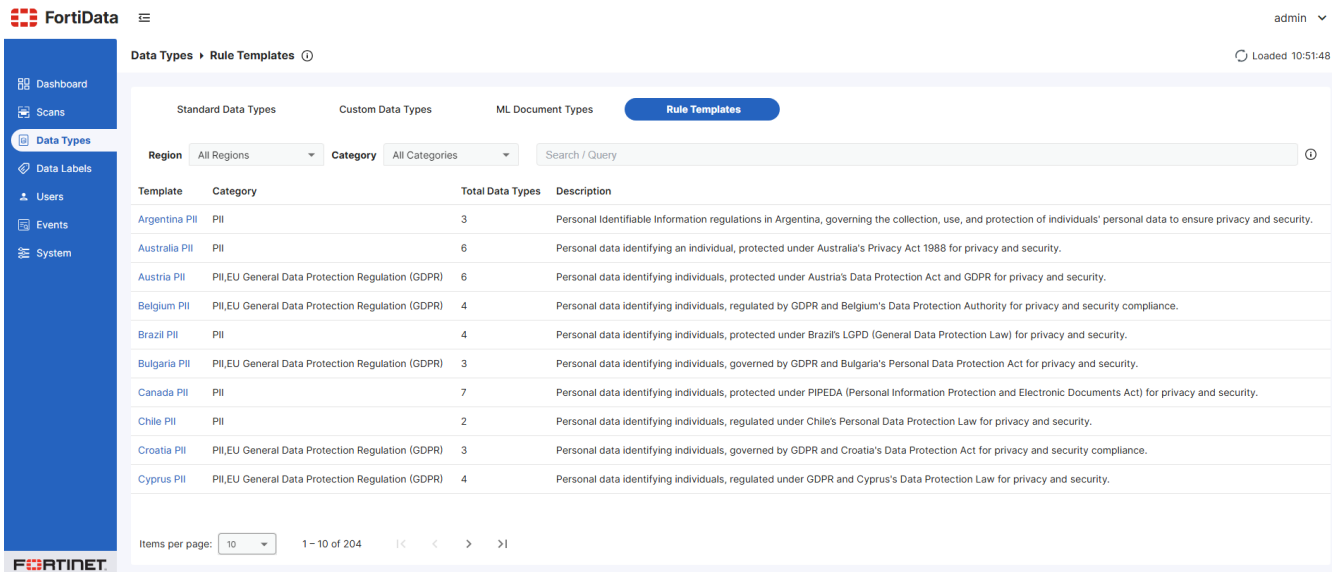
ML Document Types

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.



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
Dashboard
Scans
Data Types
Data Labels
Users
Events
System
Data Types ▸ Rule Templates
Loaded 10:51:48
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

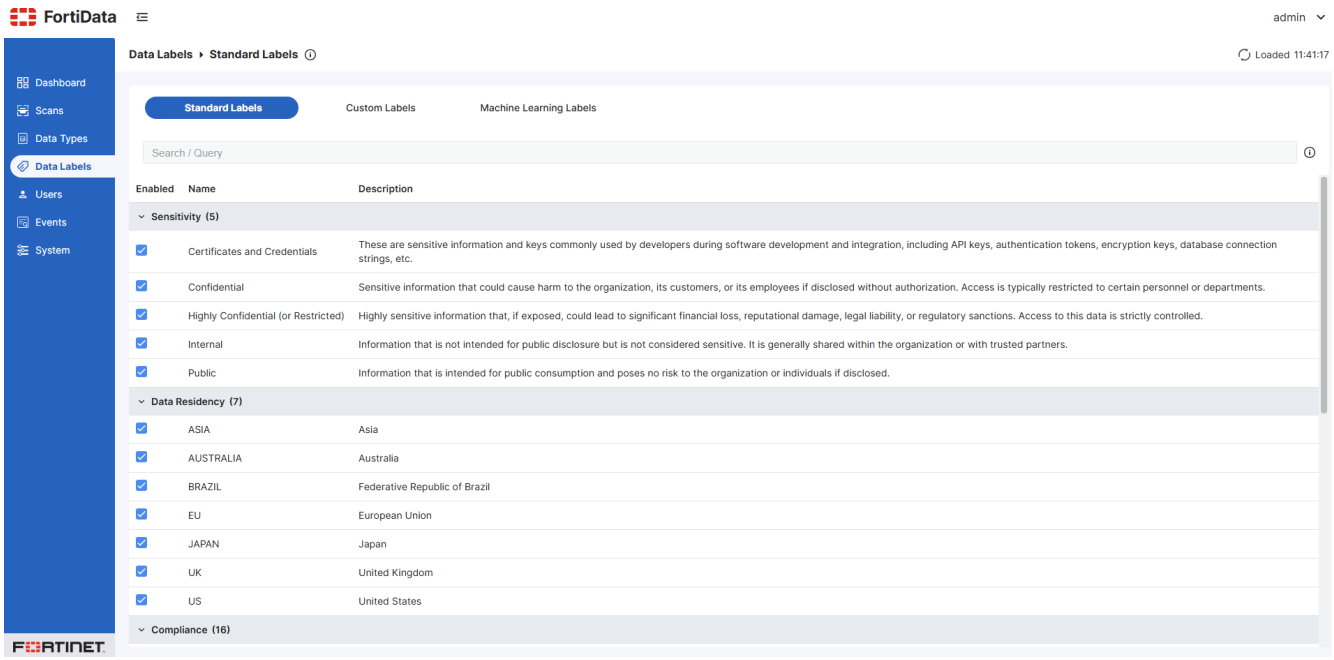
Data Labels

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

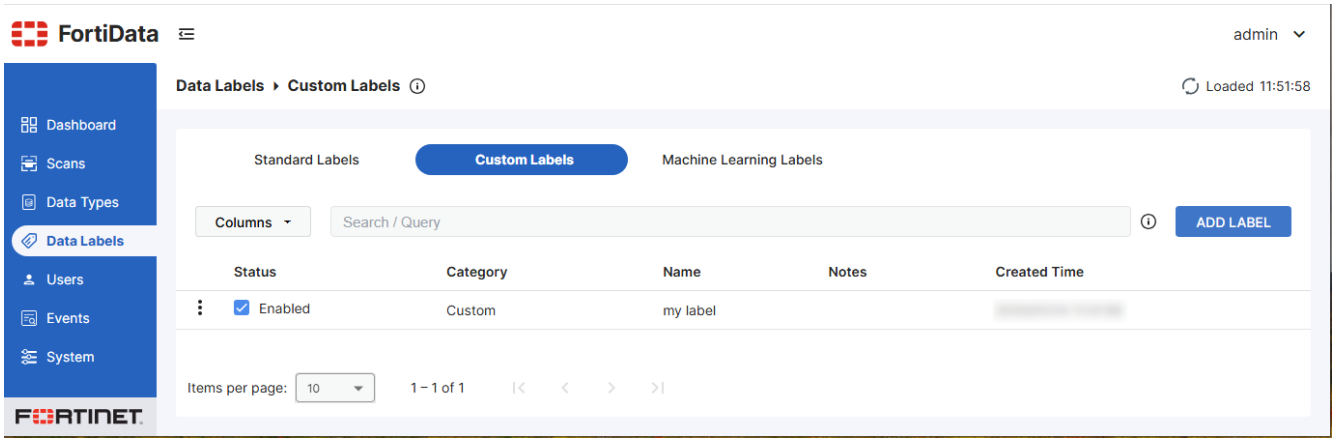
The *Standard Labels* tab displays a list of predefined data labels in FortiData. You can search the standard labels by name and/or description.



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:

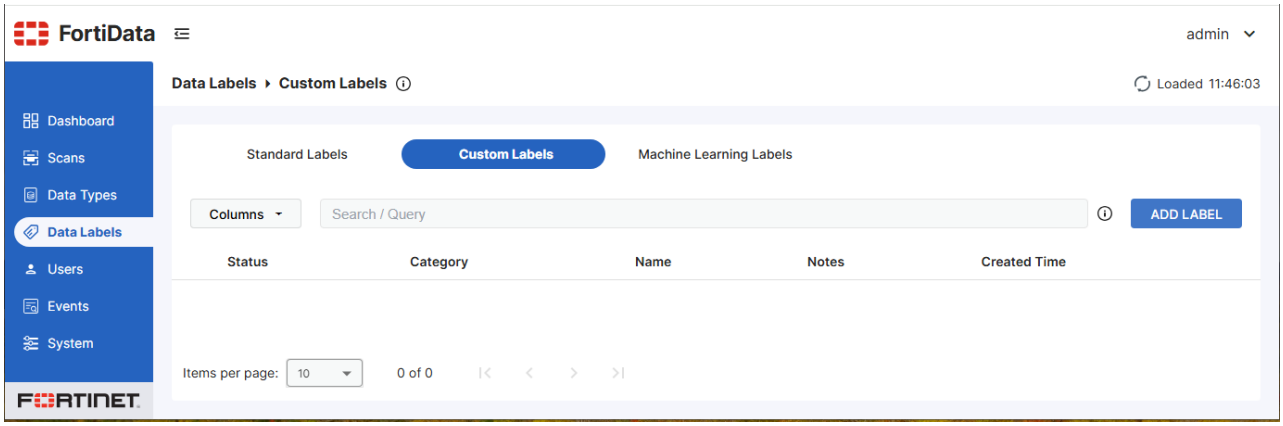
- ID
- Status
- Category
- Name
- Notes



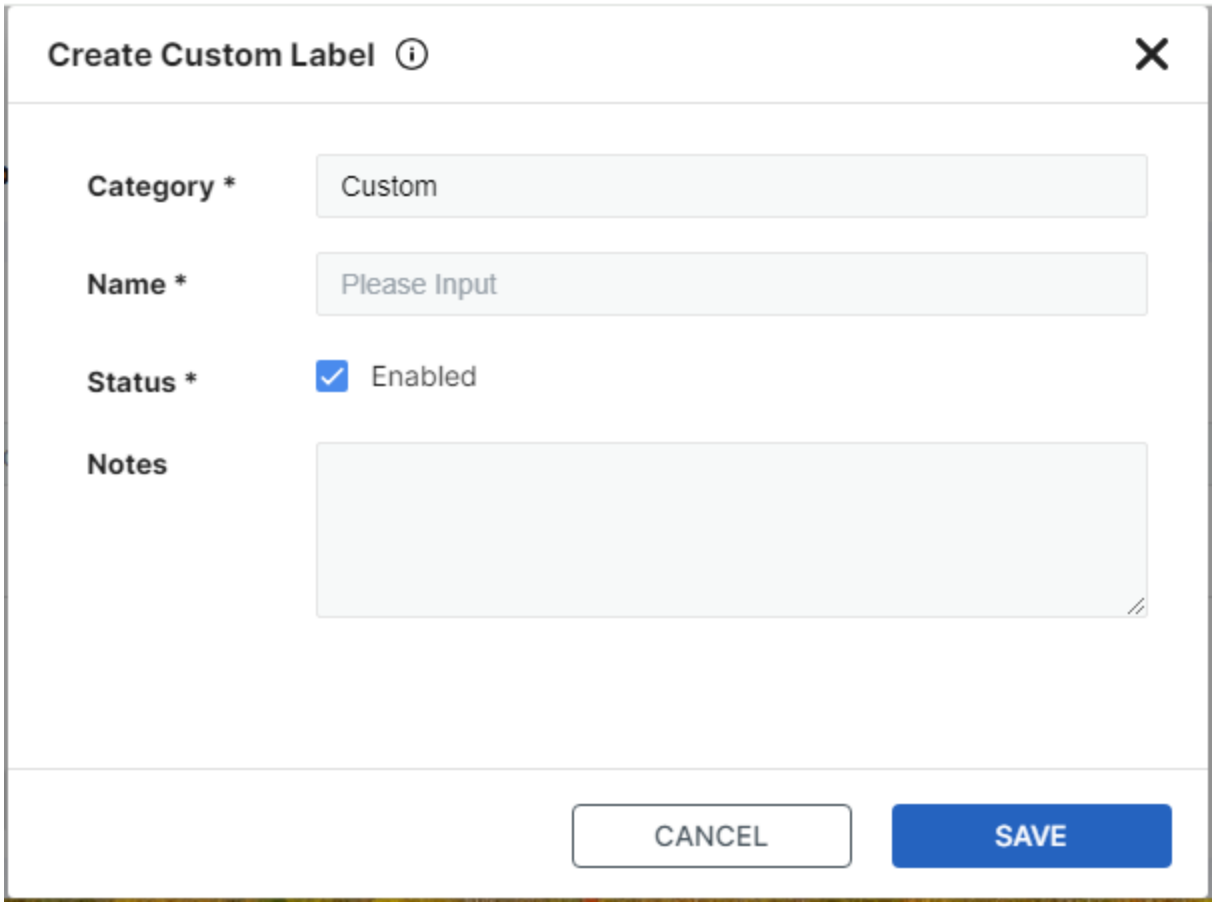
Custom data labels are useful if the system's predefined data labels do not meet your needs.

To create a custom data label:

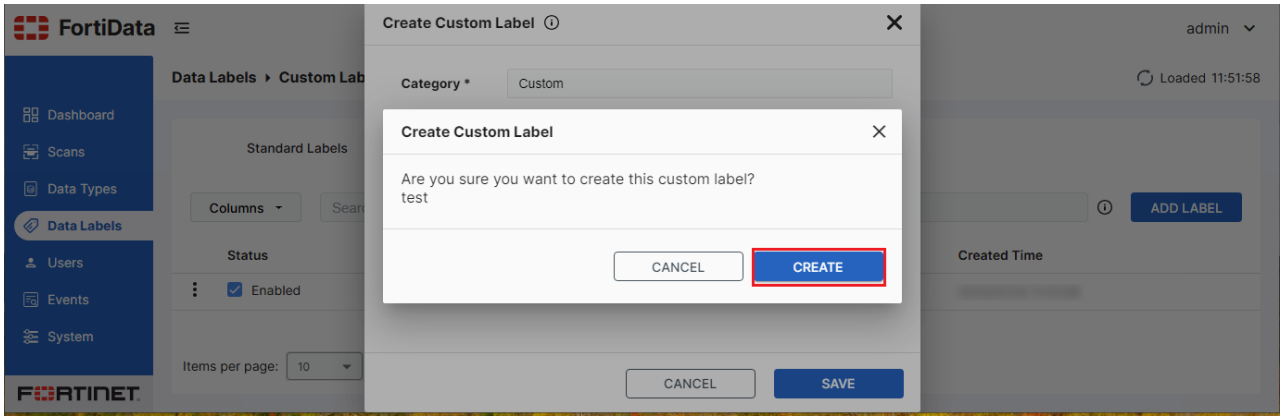
1. Go to *Data Labels > Custom Labels*.
2. Click *ADD LABEL*.



3. Specify the label name, configure the status of the label to be enabled or disabled, and add notes, if needed.

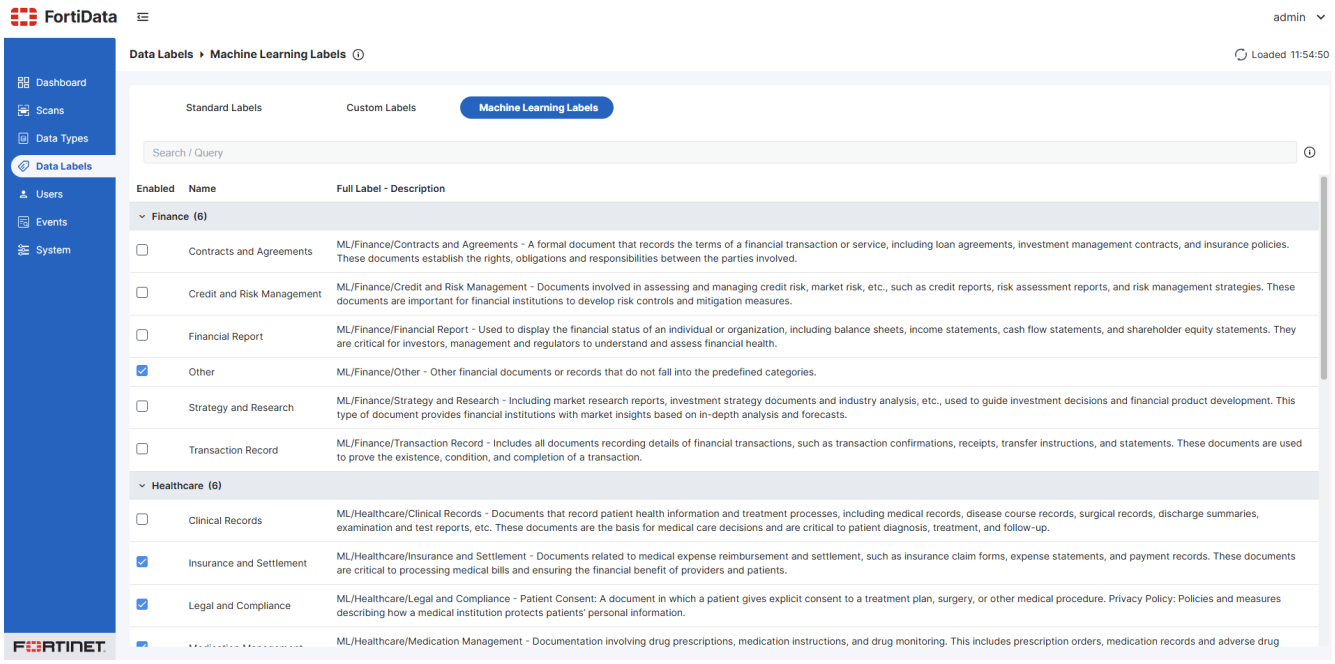


4. Click *SAVE*.
5. Click *CREATE* to confirm.



Machine Learning Labels

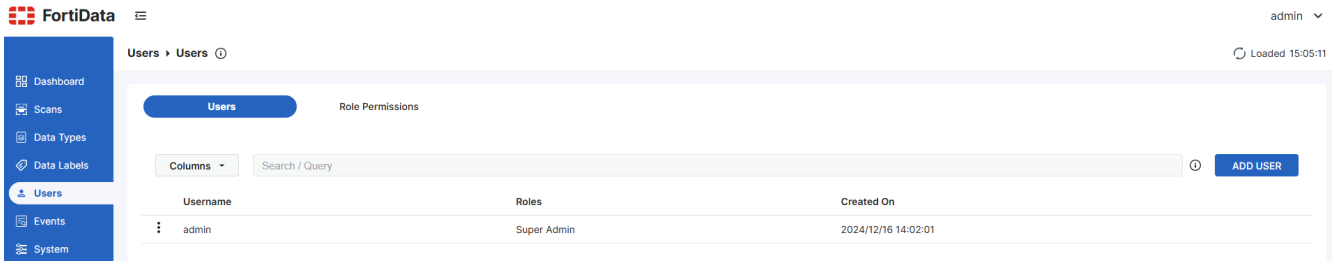
The *Machine Learning Labels* tab displays a list of data labels generated by FortiData machine learning. You can search the machine learning data labels by name.


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
Search / Query
Enabled
Name
Full Label - Description
Finance (6)
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.
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.
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.
Other
ML/Finance/Other - Other financial documents or records that do not fall into the predefined categories.
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.
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)
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.
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.
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.
ML/Healthcare/Medication Management - Documentation involving drug prescriptions, medication instructions, and drug monitoring. This includes prescription orders, medication records and adverse drug

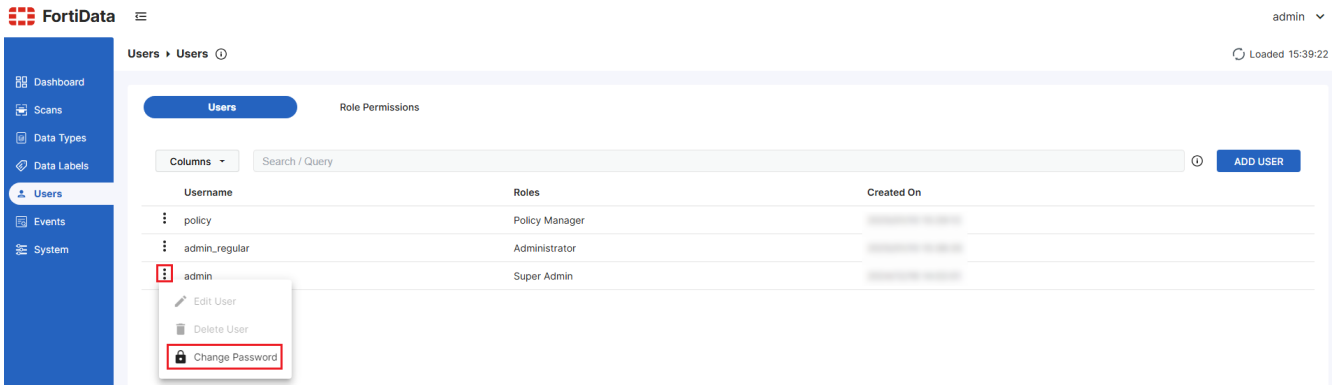
Users

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.



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*.



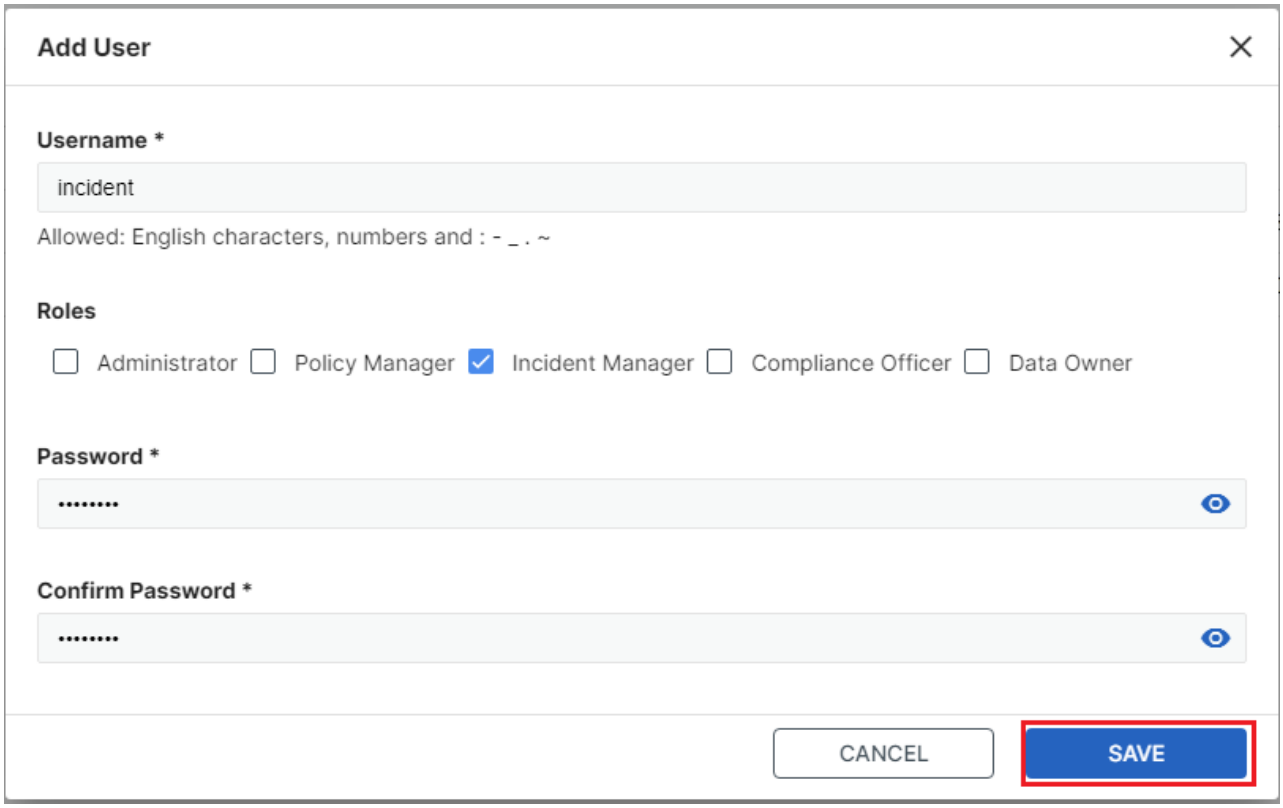
To create a user:

1. On *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.

4. Specify the password and confirm it.
5. Click *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:

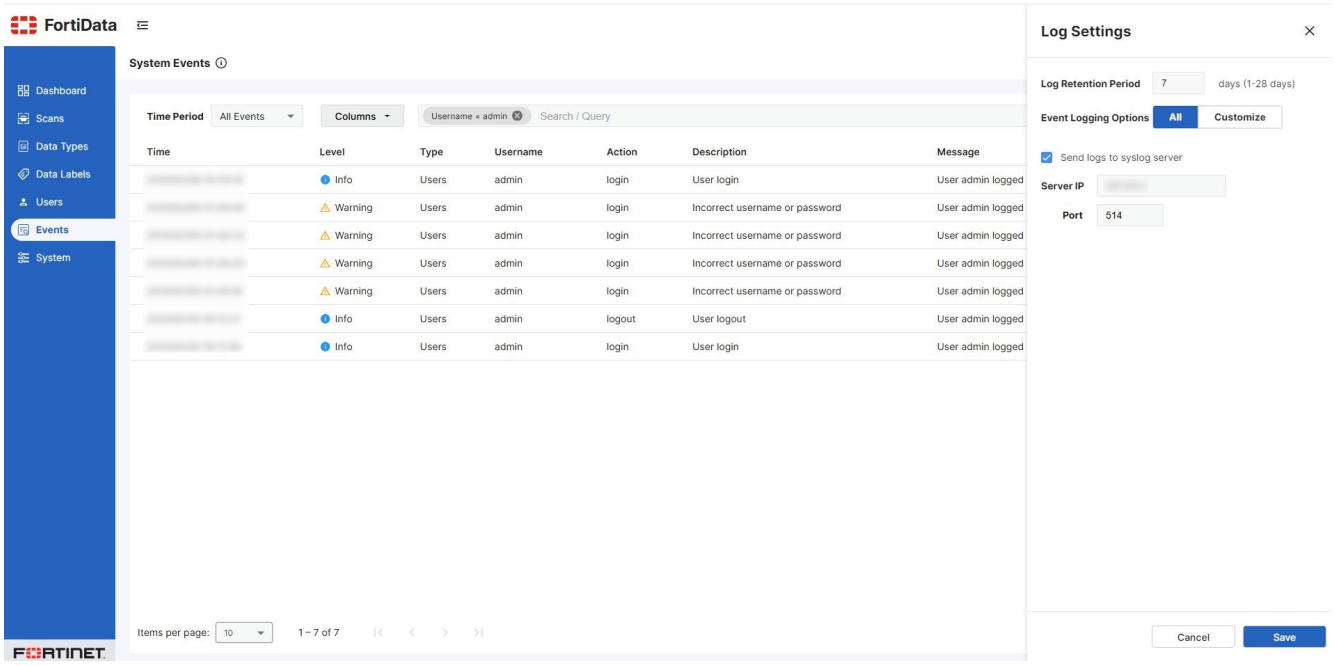
1. Click the three dots on the left of the row and select *Change Password*.
   Note that the password of the super admin can only be changed by the super admin.

Events

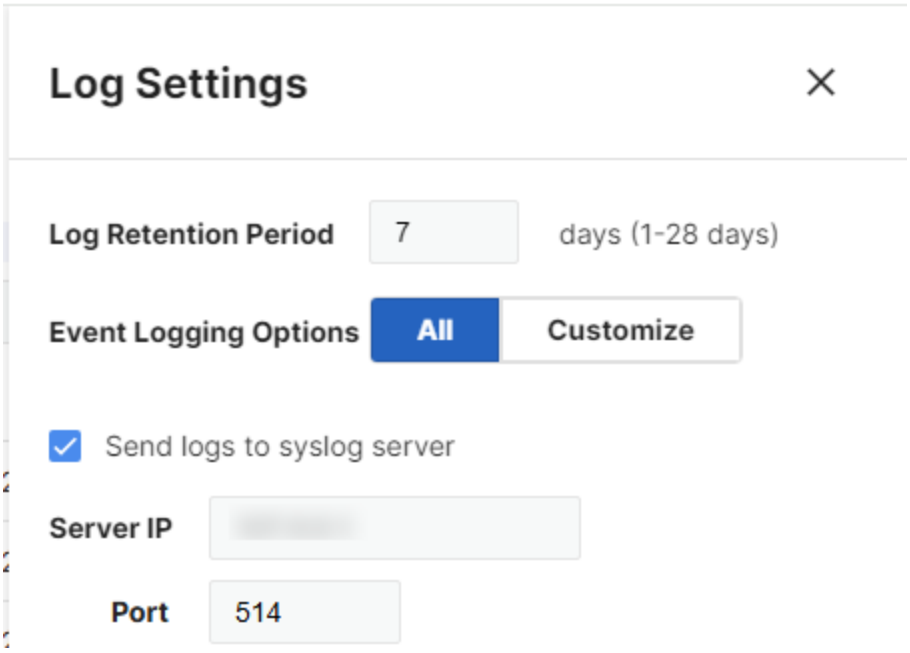
System events log data is available in the *Events* page. You can search the logs by different conditions and export the log as reports in JSON or CSV format.

Log Settings

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



You can configure the following options for logs:



Log Retention Period	Specify the number of days for which the log will be retained.
Event Logging Options	Select *All* to log all events. To customize the type of system events to log, select *Customize* and select from the following event types as needed: • 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

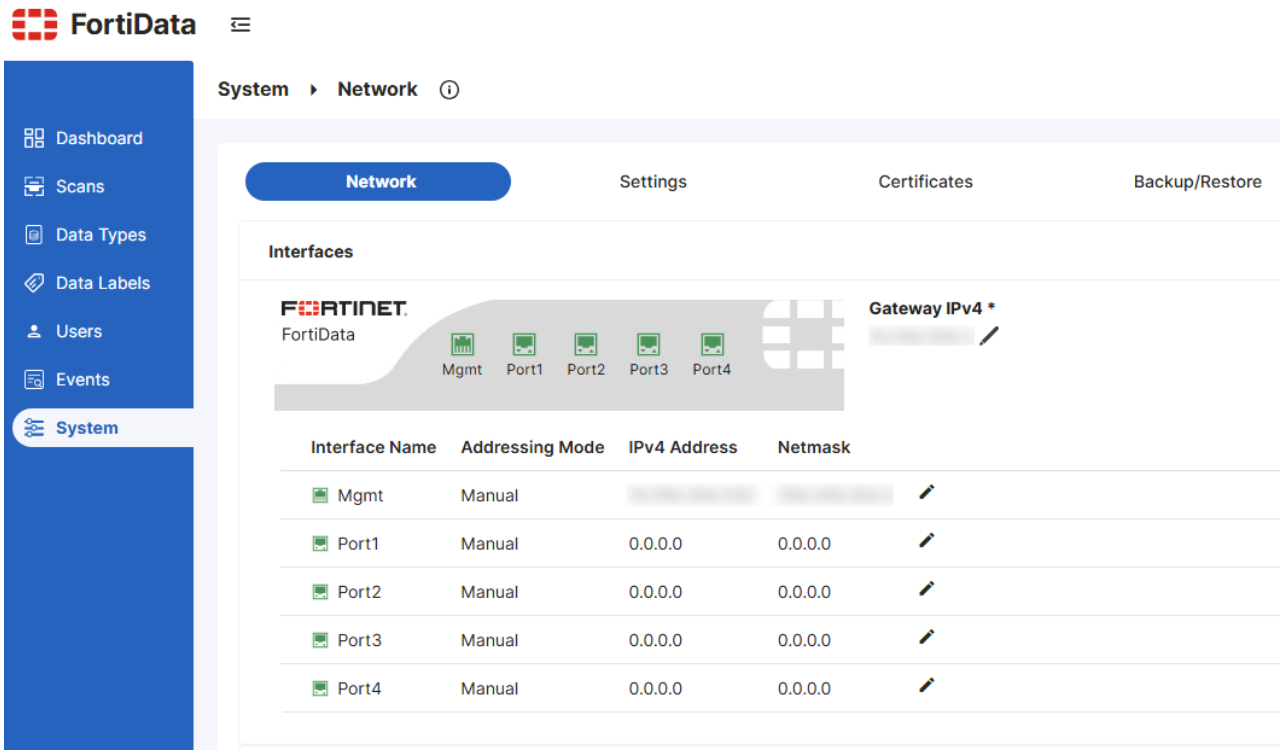
Configure the interfaces and DNS settings for FortiData in the *System* > *Network* tab.

Interfaces

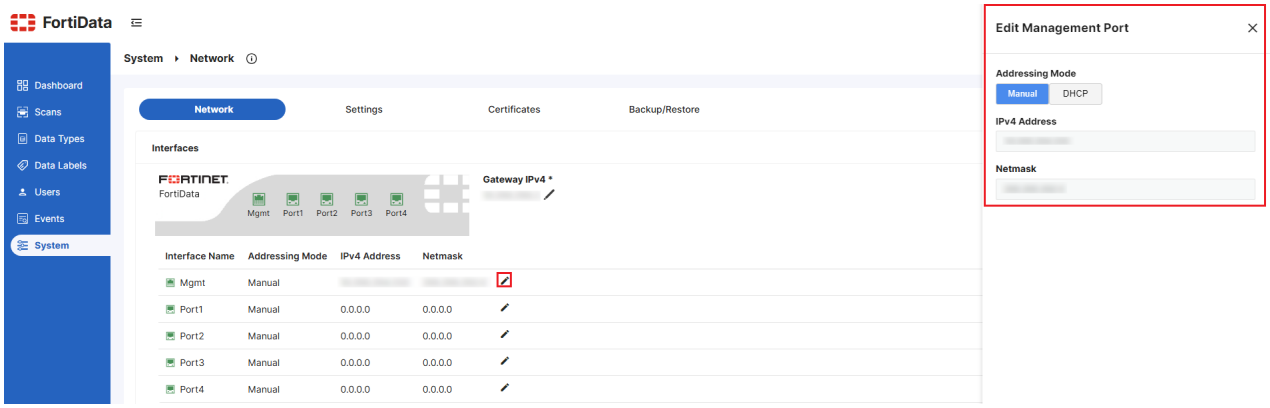
FortiData includes five interfaces: management and port 1 to 4.

To configure the interfaces:

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



2. Click the pencil icon for the default gateway or 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.
IPv4 Address	Enter the IP address.
Netmask	Enter the netmask.

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

DNS

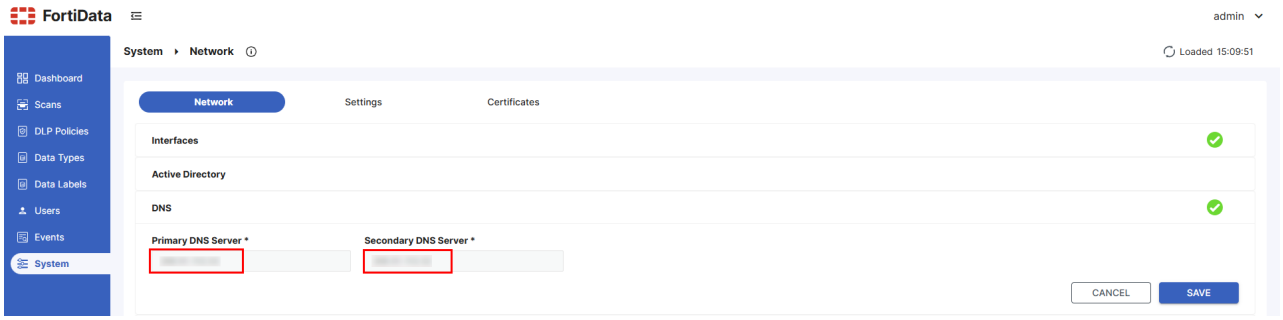
Like many other types of network devices, FortiData appliances require connectivity to DNS servers for DNS lookups.

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

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

To configure DNS settings via the web UI:

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

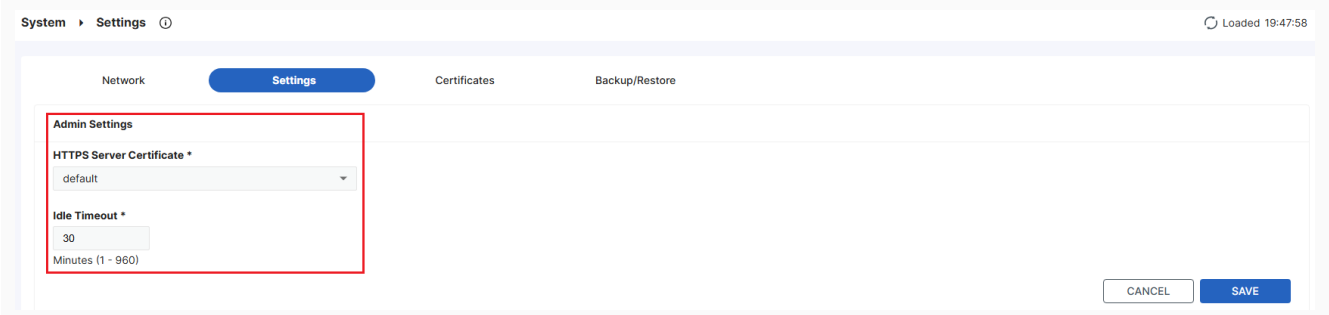


2. In *Primary DNS Server*, Enter the IP address of the primary DNS server.
3. In *Secondary DNS Server*, enter the IP address of the secondary DNS server.
4. Click *SAVE*.
   FortiData queries the DNS servers whenever it needs to resolve a domain name into an IP address, such as for NTP system time.

Settings

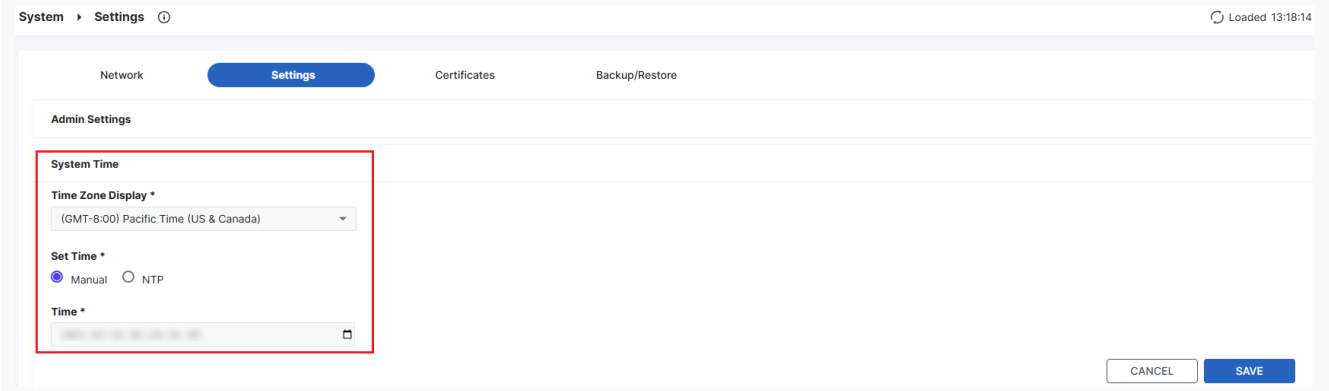
In this section, you can configure the following:

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



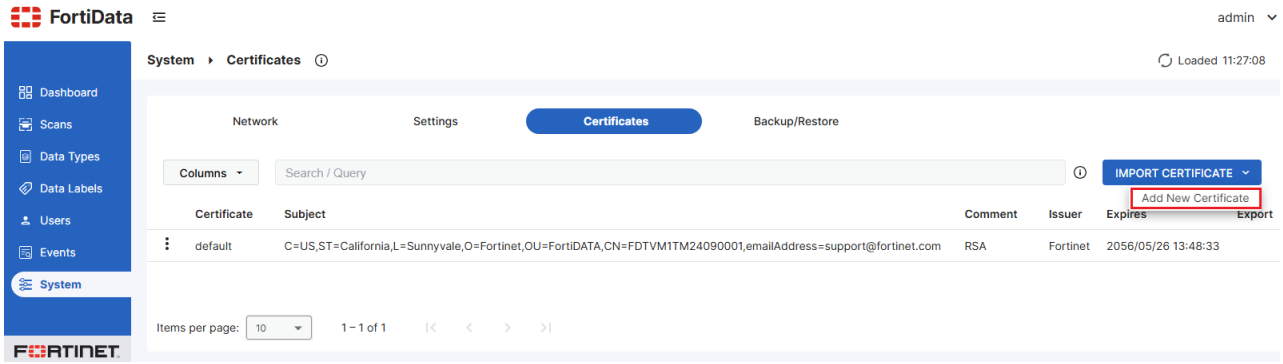
Time Zone Display	Select the time zone where the FortiData appliance is installed. The system will be updated according to the timezone, accounting for daylight savings time.
Set Time	Enter the current settings for the system date and time. You can change these manually. Use the calendar button to select 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*.

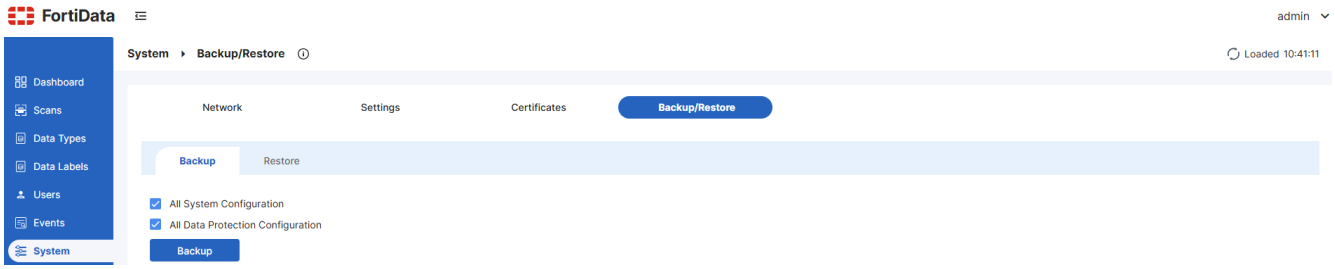


3. Click *BROWSE* to select the certificate file and key file respectively from your local directory.
4. **(Optional)** Specify a passphrase, if needed.
5. Click *IMPORT*.
6. Click *Close*.

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