Administration Guide

FortiData 7.6.1

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

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

FORTINET BLOG
https://blog.fortinet.com

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

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

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

FORTIGUARD LABS
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

November 20, 2025
FortiData 7.6.1 Administration Guide
96-761-1109187-20251120

TABLE OF CONTENTS

Change log

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

Introduction

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

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

FortiData supports integration with the following Fortinet security fabric products:

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

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

This guide intends to help you navigate and leverage the features of FortiData and guide you through the process of creating scan tasks, configuring scan policies, and adding custom data types.

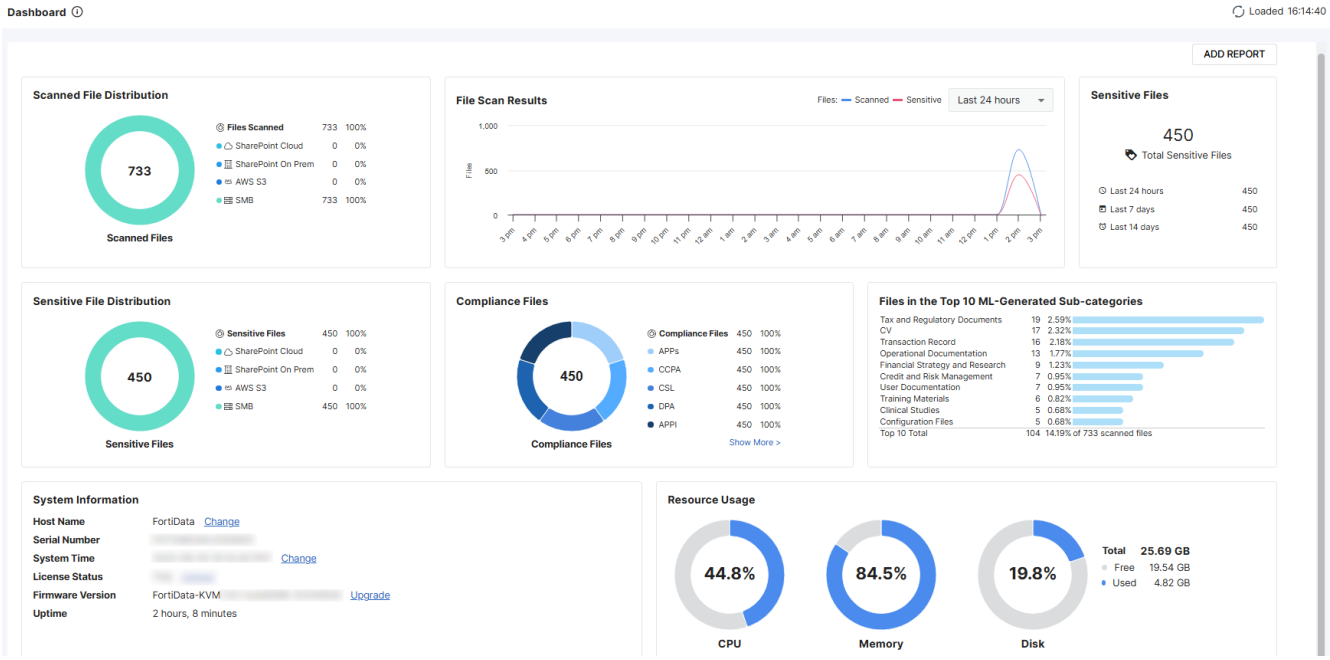
Getting started

Perform the following procedures to get started with FortiData:

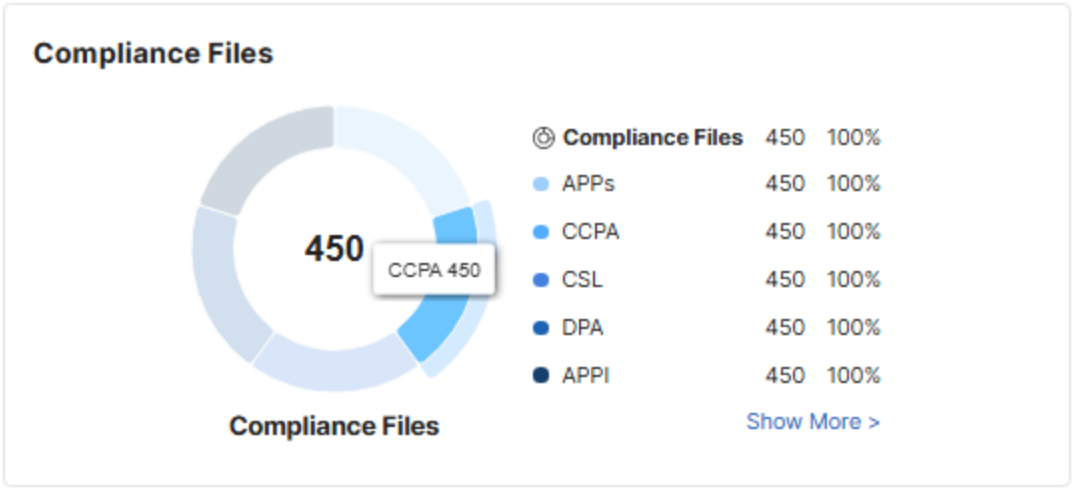
1. Configure interface and DNS settings. See Network on page 60
2. Configure timeout and system time. See Settings on page 64.
3. Configure HTTPS server certificate. See Certificates on page 66.
4. Create users of with different access scope to FortiData. See Users on page 52.
5. Create discovery policies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

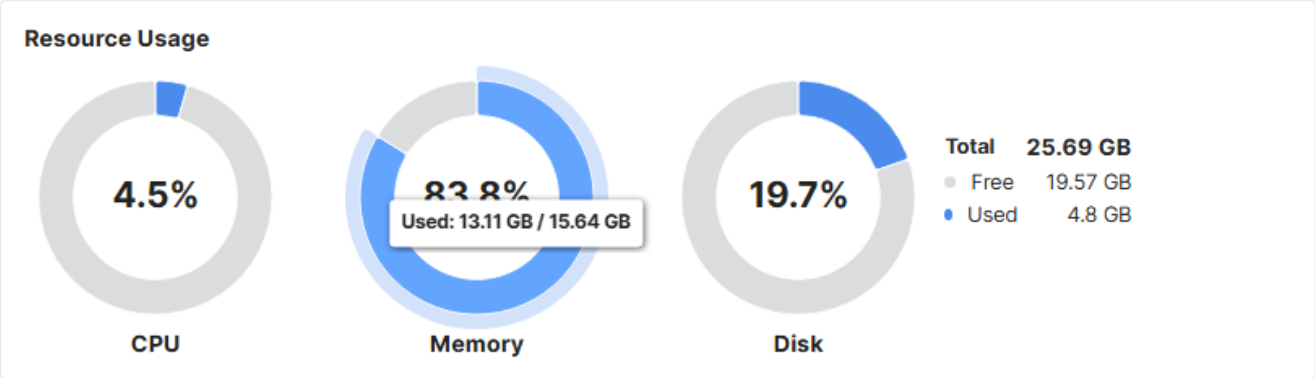
Dashboard

Use the *Dashboard* to view information of the system, such as scanned or sensitive file distribution by platform, file compliance and sensitivity information, resource usage, and system information (hostname, serial number, system time, license status, firmware version). You can also add a dashboard report using the *ADD REPORT* button on the top-right corner. The report will then be available in the *Logs & Reports* > *Reports NEW on page 55* page.



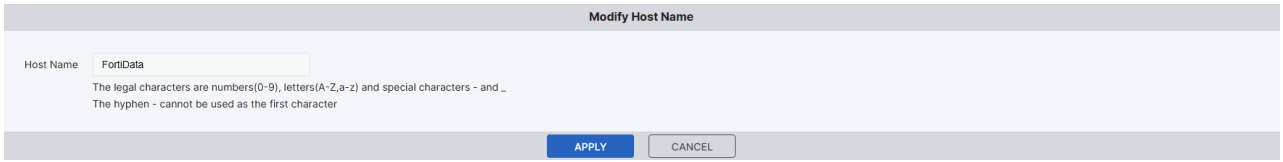
Hover your mouse over a graph or chart to view more details about the data points.





To change the hostname:

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



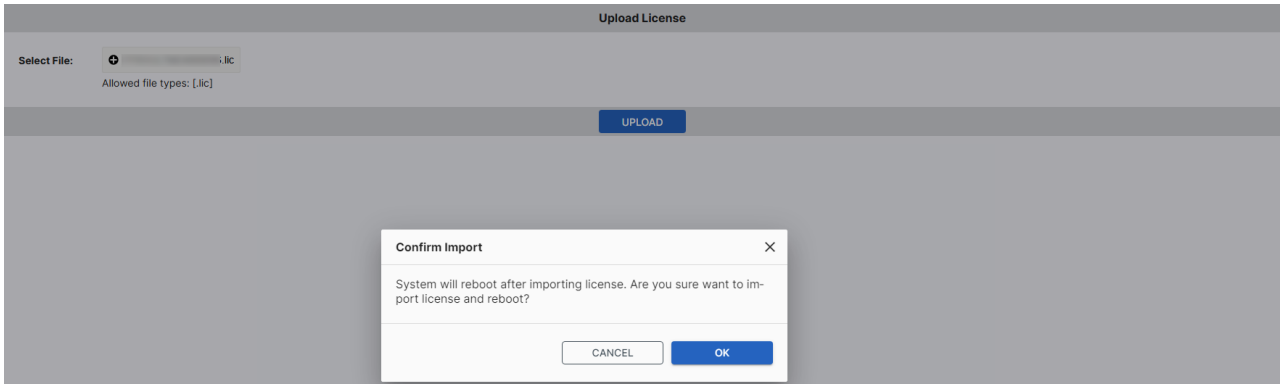
3. Specify the desired hostname and click *APPLY*.

To change the system time:

1. Go to the *Dashboard* > *System Information* widget.
2. Click *Change* at the end of the *System Time* field.
3. Configure the system time in the *System* > *Settings on page 64* tab.

To upload or change the license:

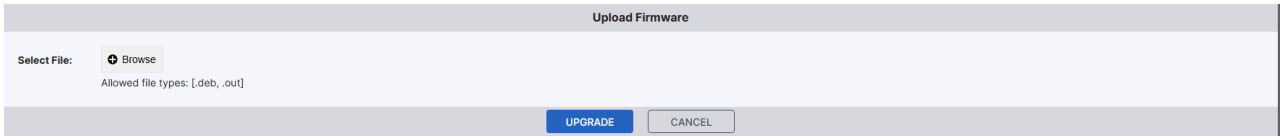
1. Go to the *Dashboard* > *System Information* widget.
2. Click *Upload* or *Upgrade* at the end of the *License* field.
3. Click *Browse* to locate the license file on your local disk.
4. Click *UPLOAD*.
5. Click *OK* when prompted.



To upgrade the firmware:

FortiData does not support downgrading to previous firmware versions. You can back up configurations before upgrade or restore older firmware and configurations in *System* > *Backup/Restore on page 67*.

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



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

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

To reboot the system:

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

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

To shut down the system:

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

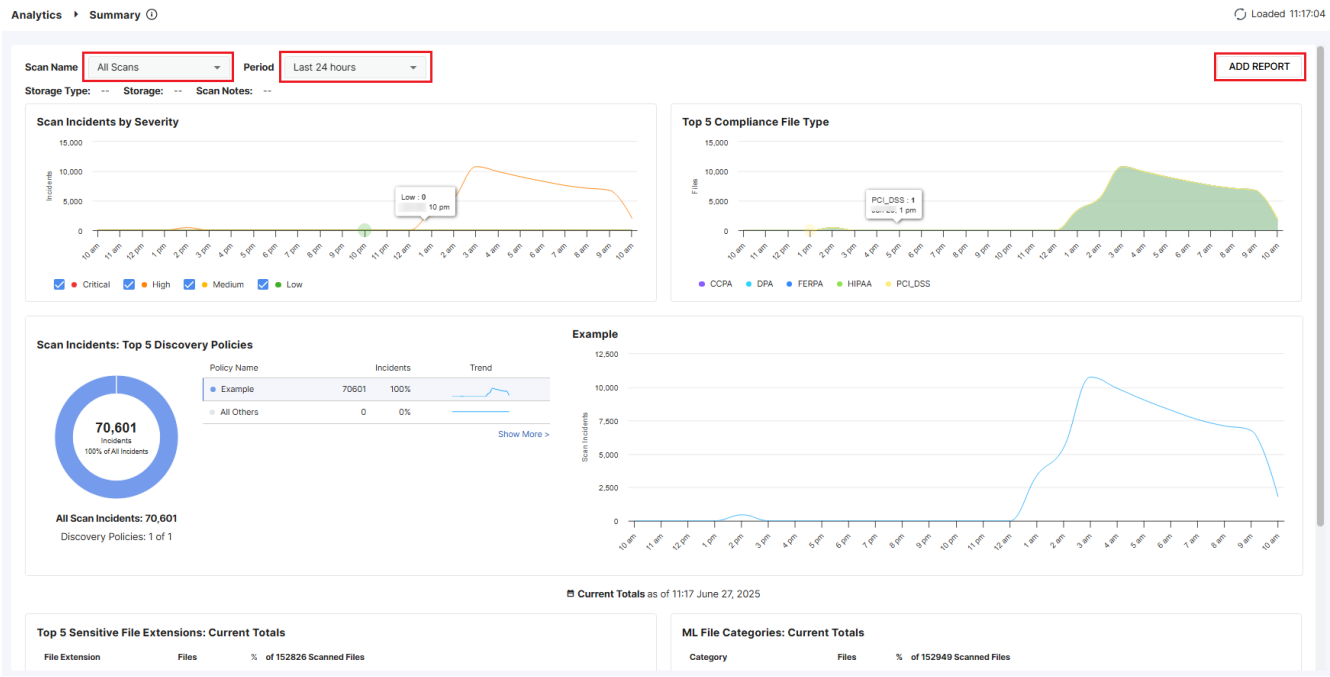
Alternatively, run the `execute shutdown` command via the CLI.

Analytics

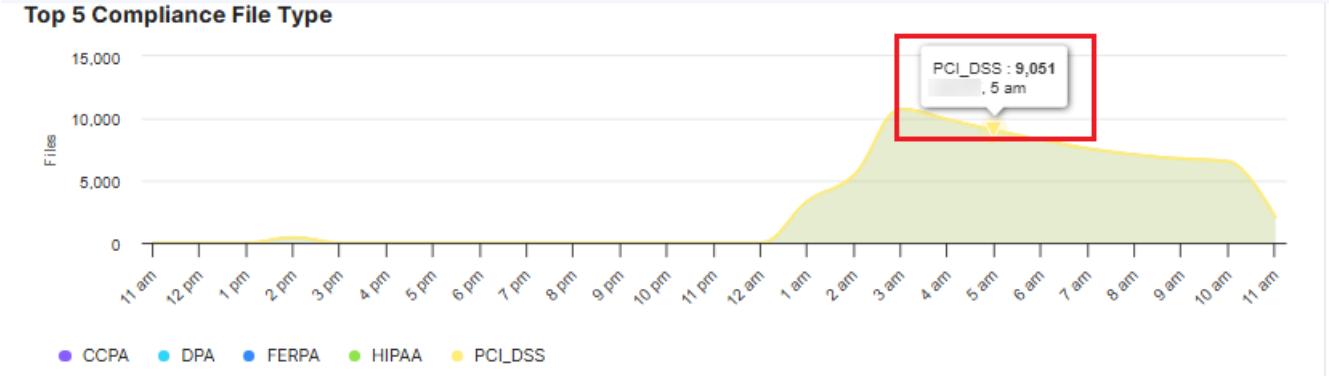
Go to the *Analytics* page to view a summary of the scan results, a list of scanned files, and scan incidents.

Summary

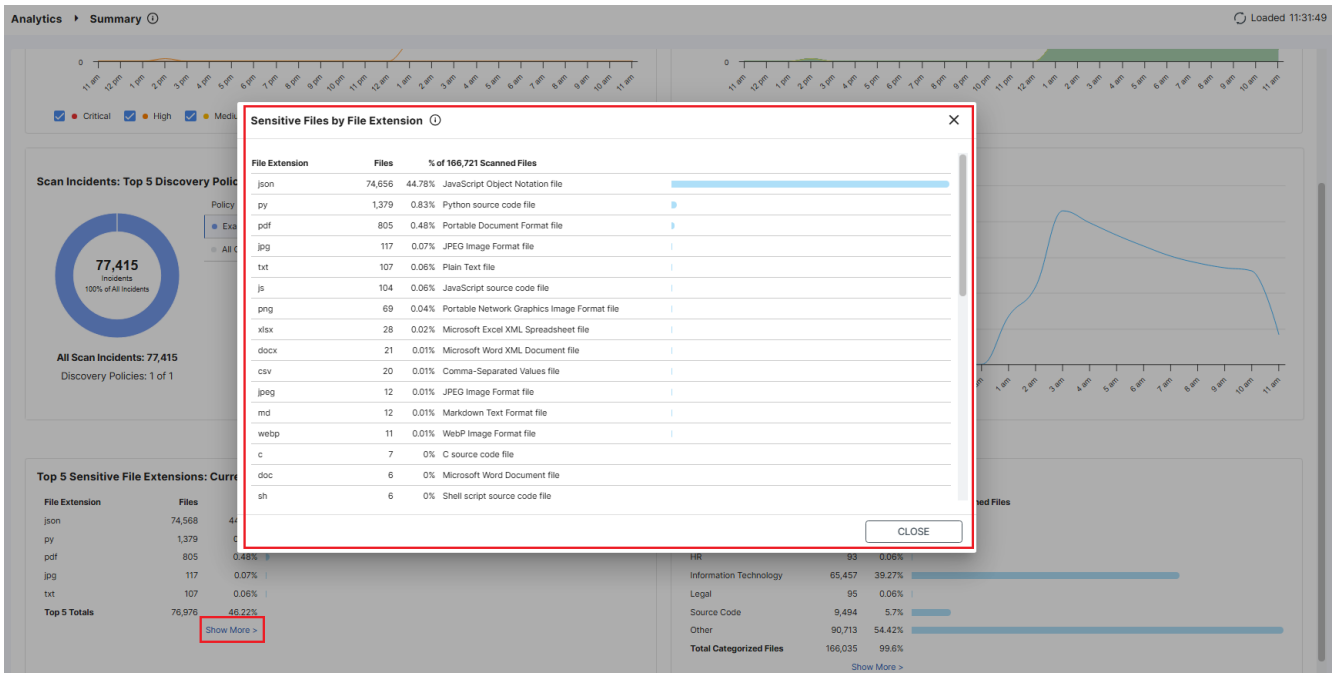
A summary of scan result is available in the *Analytics* > *Summary* page with interactive graphs and charts. You can filter the result by scan name and time period. You can also add an analytics summary report using the *ADD REPORT* button on the top-right corner. The report will then be available in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



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



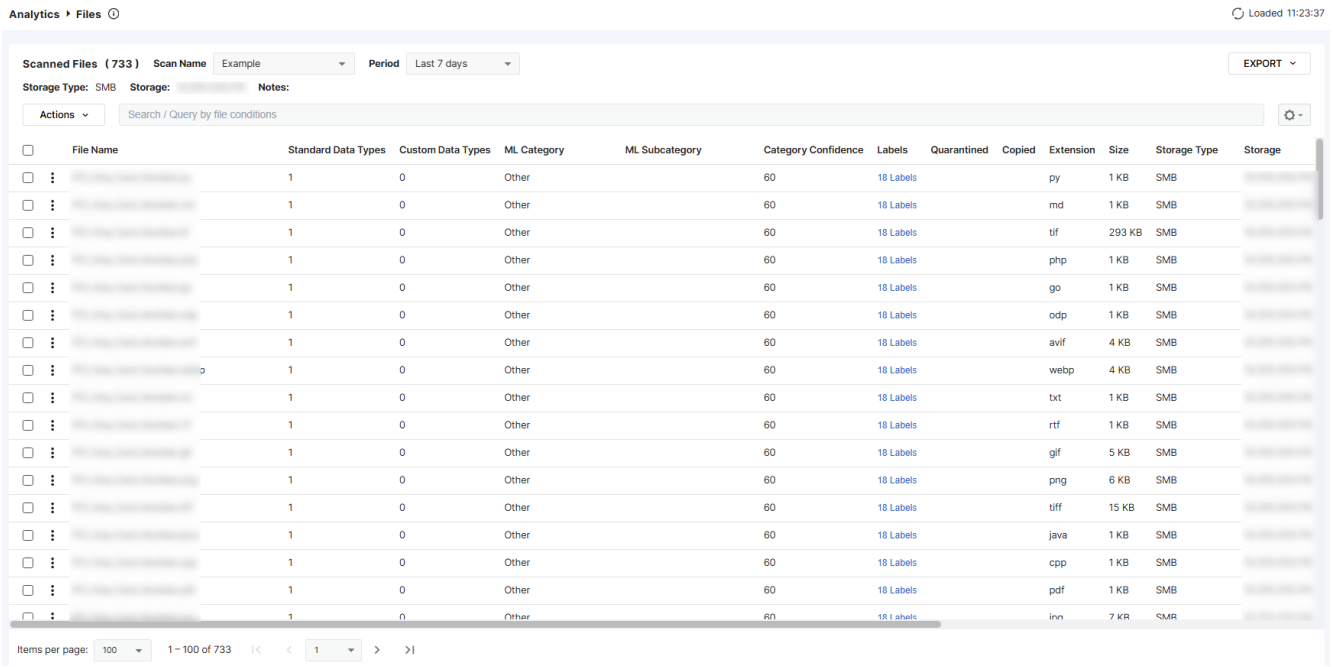
Click *Show More* to view more details about the data points.



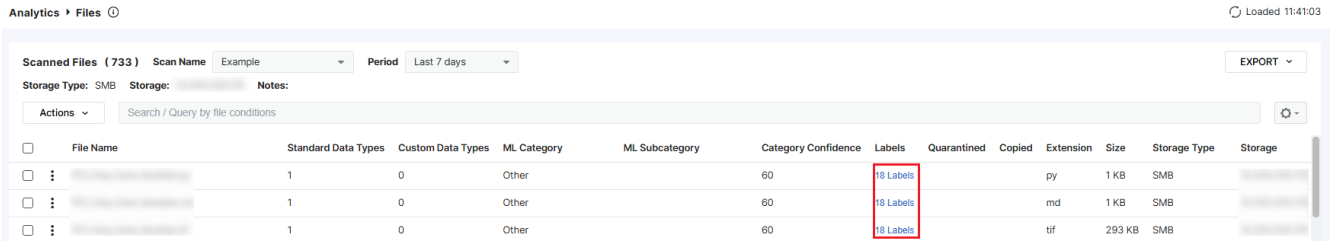
Files

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

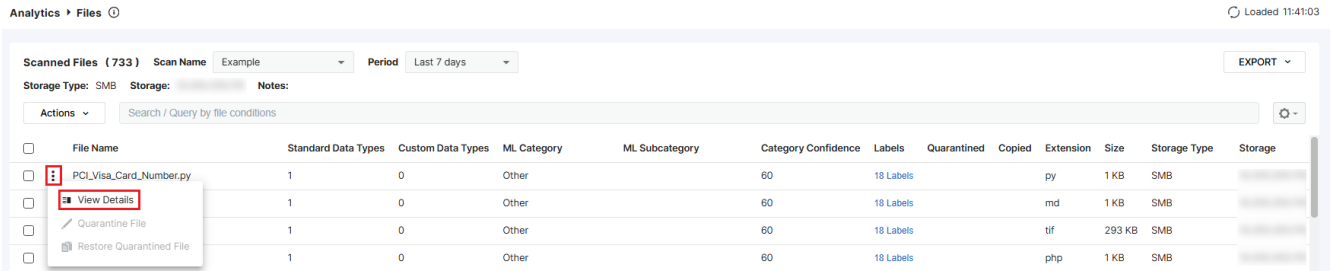
- To customize the columns to display in the table, use the *Configure* button on the top-right.
- To export the scanned file list, click *EXPORT* > *Export JSON/CSV*.

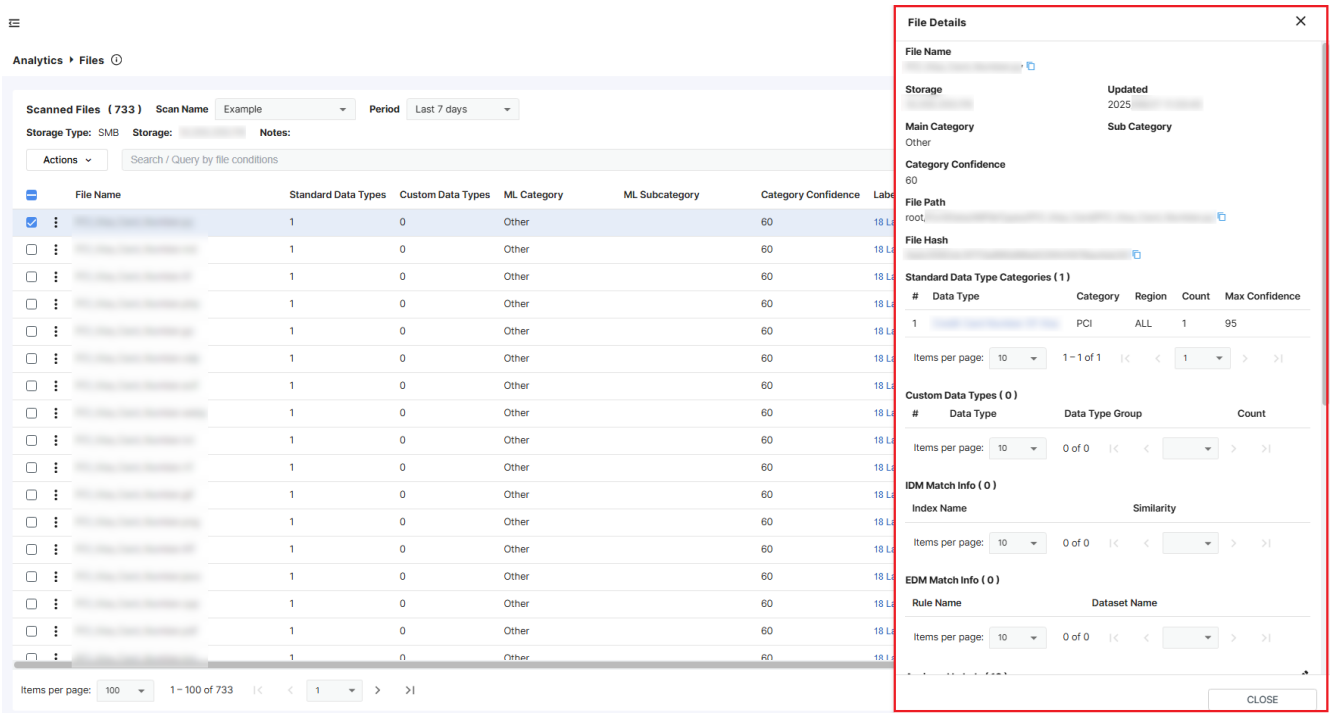


To see the assigned labels for a sensitive file, click the link in the *Labels* column.

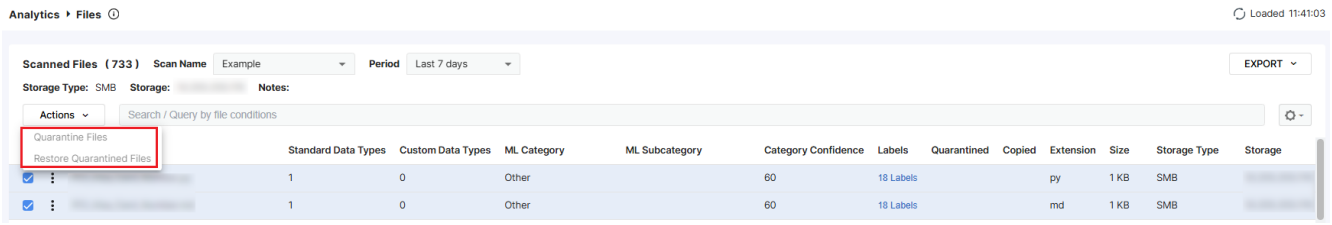


To view more details of a scanned file, click the three dots at the front of the row and select *View Details*. The *File Details* pane appears on the right.





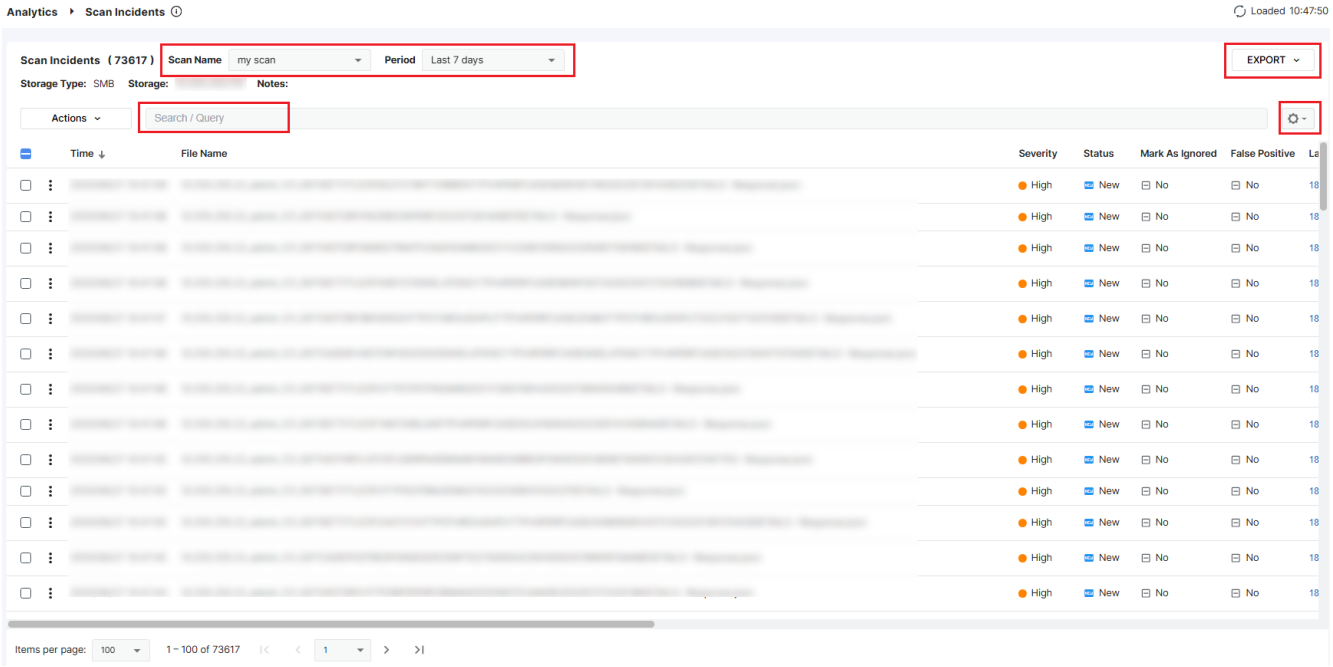
Select one or more scanned files and click the *Actions* button to perform the following operations:



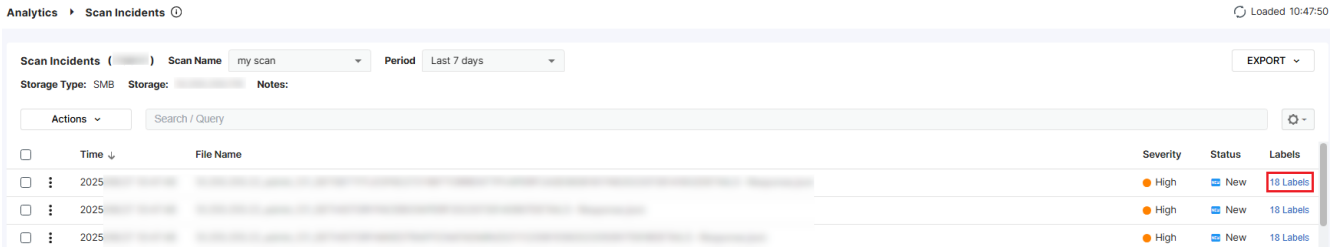
Scan Incidents NEW

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

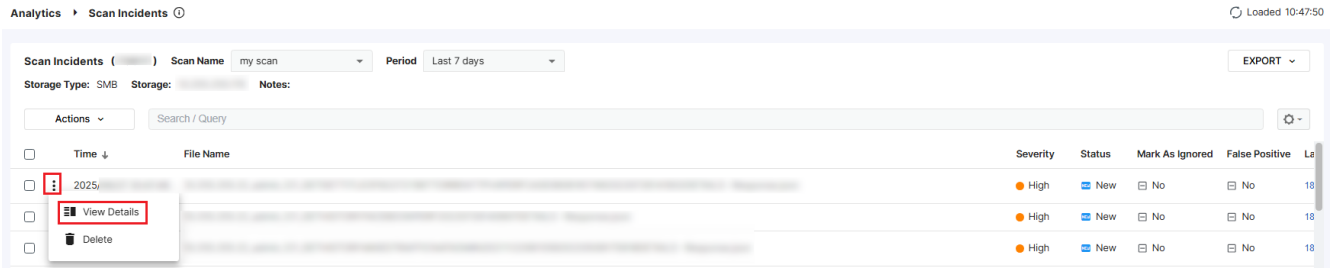
- To customize the columns to display in the table, use the *Configure* button on the top-right.
- To export the logs, click *EXPORT > Export JSON/CSV*.

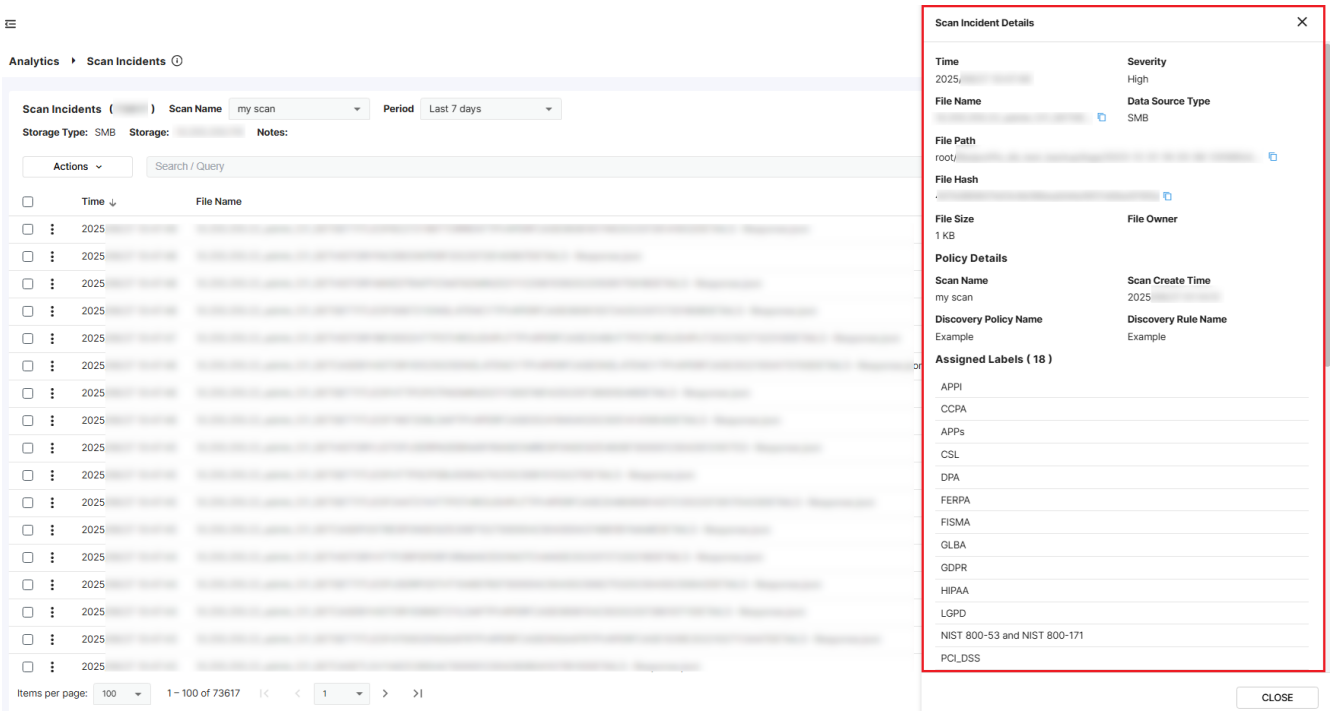


To see the assigned labels for an incident, click the link in the *Labels* column.

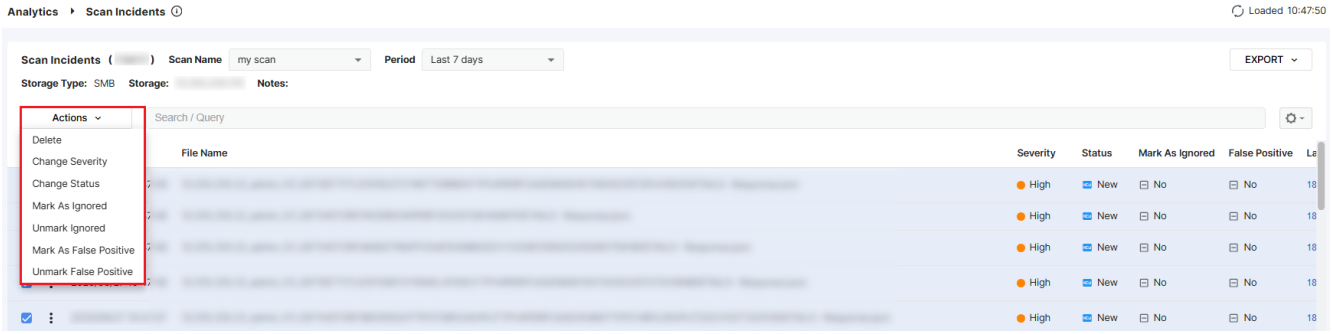


To view more details of an incident, click the three dots at the front of the row and select *View Details*. The *Scan Incident Details* pane appears on the right.





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



Discovery

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

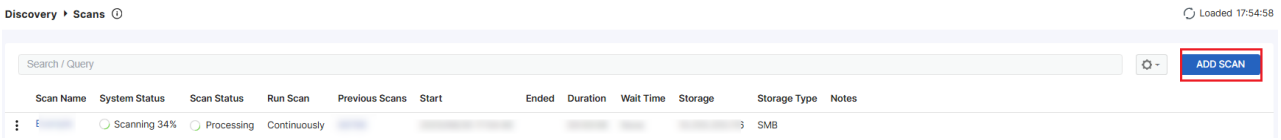
1. Create data discovery policies to look for specific types of data (using data types) in files and assign specific tags (using data labels) to files that meet the specified conditions. See Policies on page 23.
2. Create data discovery profiles to copy or quarantine sensitive files to a specific local or remote folder. See Profiles NEW on page 29.
3. Define a scan to access and analyze files in a target location (for a storage type) using the conditions and actions defined in the discovery policy with a proper schedule and apply a profile as needed. See Scans on page 16.
4. View scan and classification results in the *Analytics on page 10* pages.

Scans

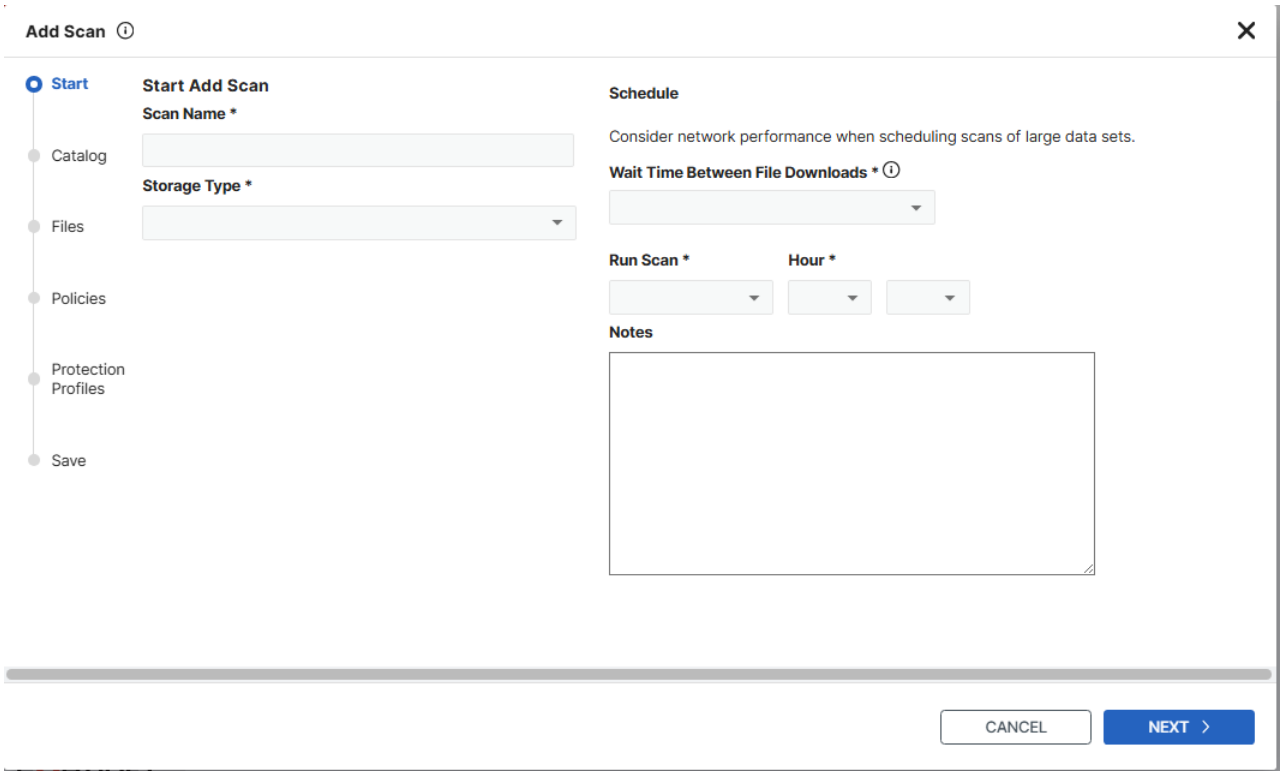
On the *Discovery* > *Scans* page, you can define a scan to access and analyze files in a target location (for a storage type) using the conditions and actions defined in the discovery policy with a proper schedule and apply a profile as needed. Scan and classification results can then be viewed in the *Analytics on page 10* pages. You can create up to 16 scans.

To create a scan:

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



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



a. Specify the scan name.

b. Select the storage type from one of the following:

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

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

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

Permission	Type	Description
Microsoft Graph		
Application.Read.All	Application	Read all applications.
AuditLog.Read.All	Application	Read all audit log data.
Directory.Read.All	Application	Read directory data.
Files.ReadWrite.All	Application	Read and write files in all site

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

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

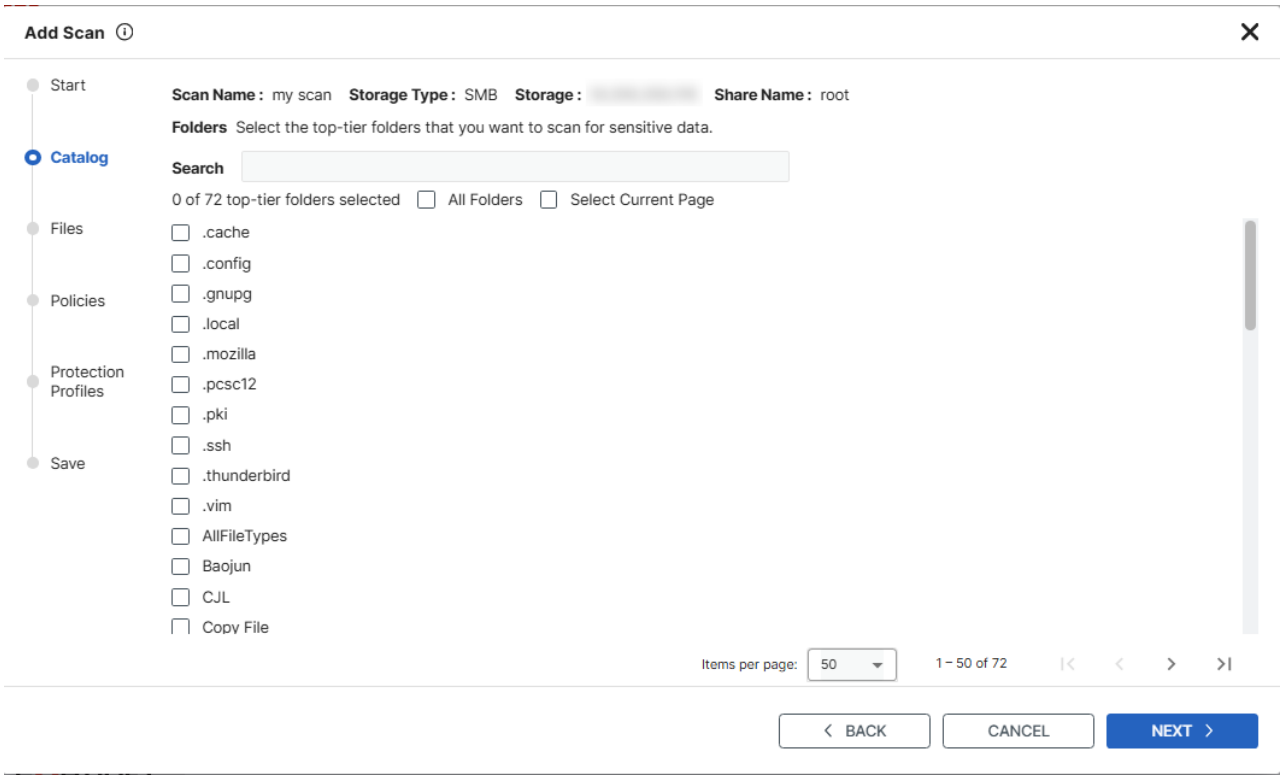
The wait time will affect the speed of the scan and the traffic load on your network. A shorter wait time will result in faster scans but may increase network traffic load. The first run of a scan will be relatively slow as every file is downloaded for processing. Subsequent runs of that scan will likely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

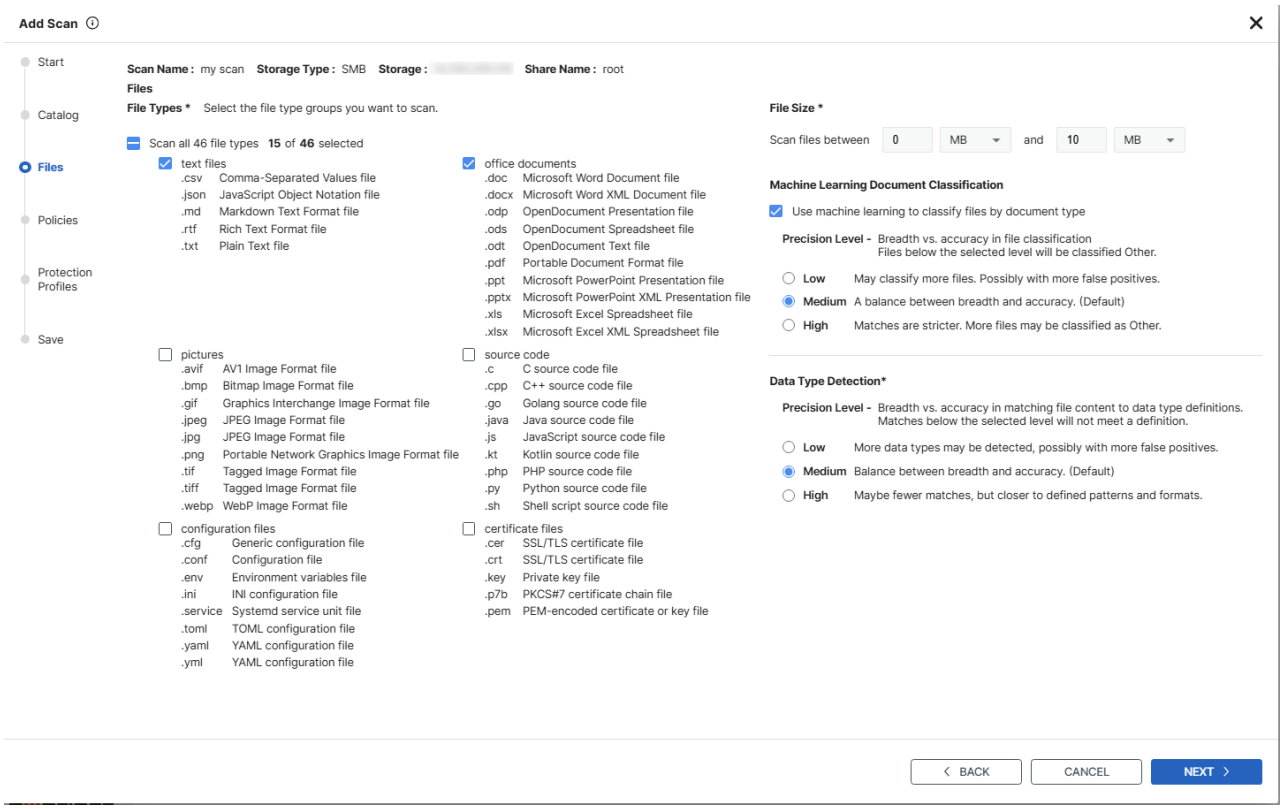
h. Click *NEXT*.

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

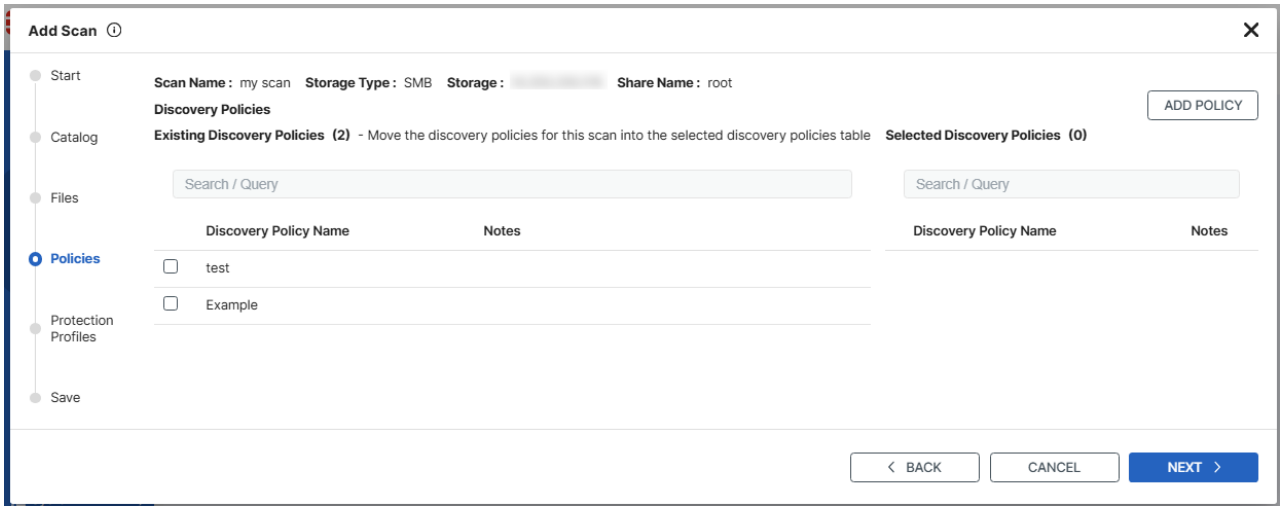


4. Configure the file types to scan, including file extensions, file size, machine learning document classification, and precision level.

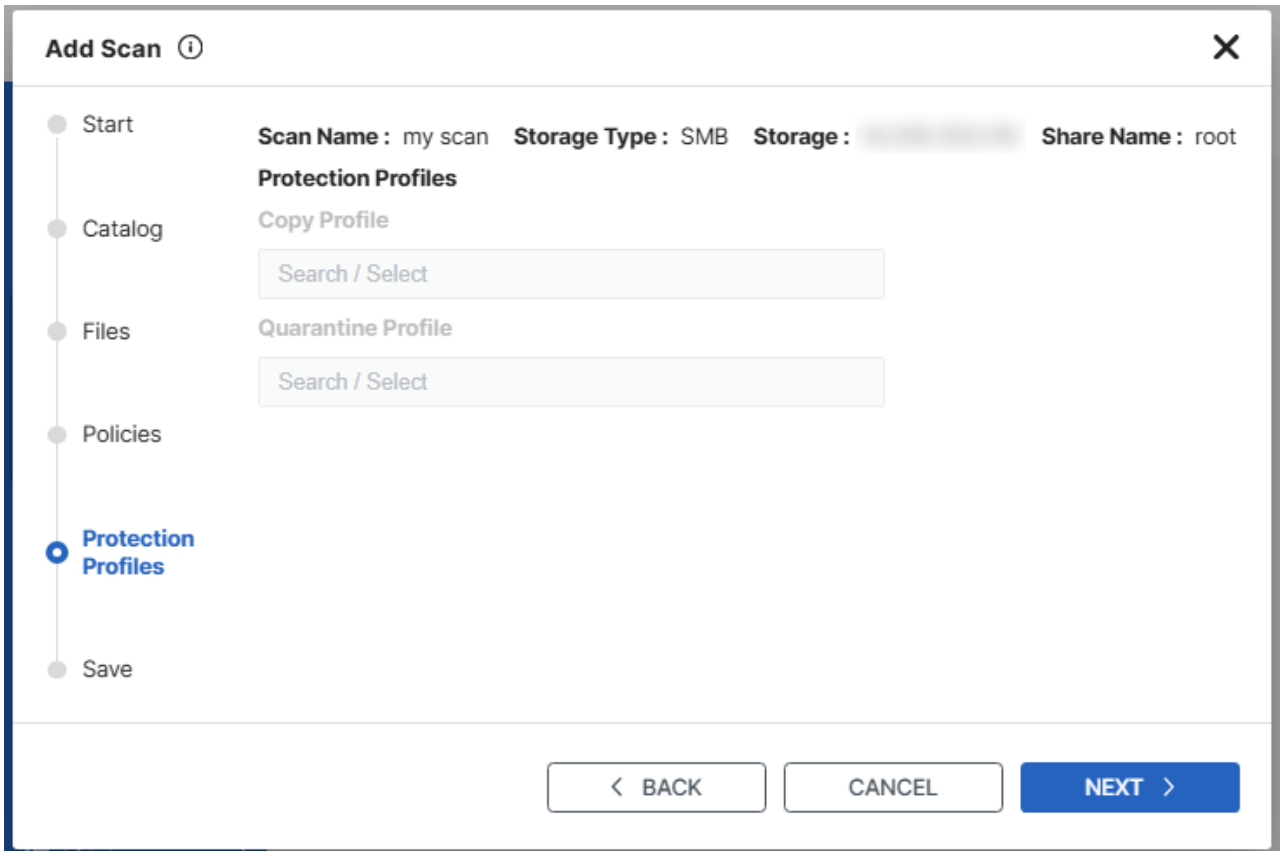
   The precision level determines the threshold confidence level for ML file classification and data type detection. For example, if you select *High* in *Precision Level* under *Data Type Detection*, only data types with a confidence level of high (as predefined in FortiData) will be detected and displayed.



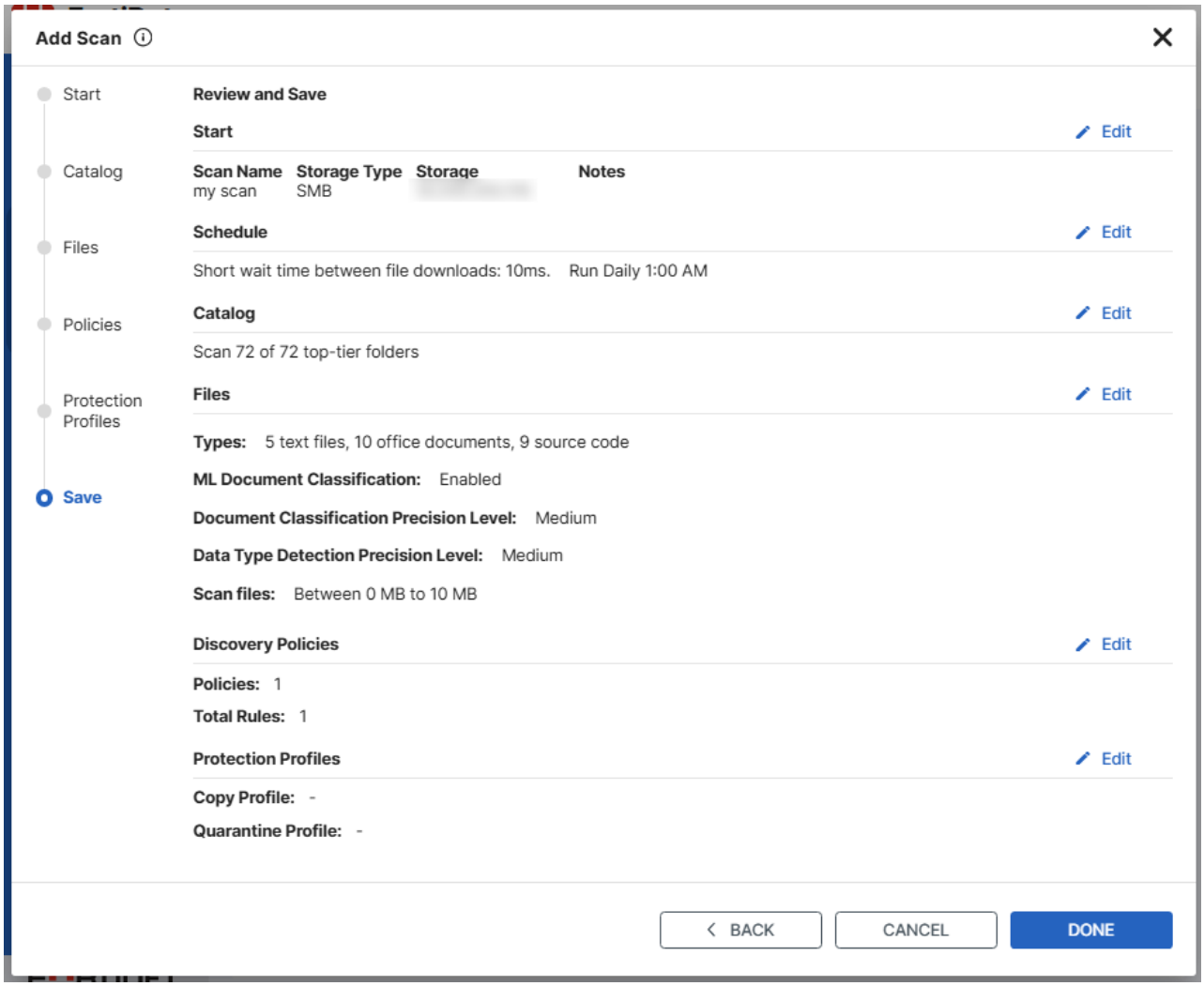
5. Click *NEXT*.
6. Select the discovery policies to apply to the scan and click *NEXT*.



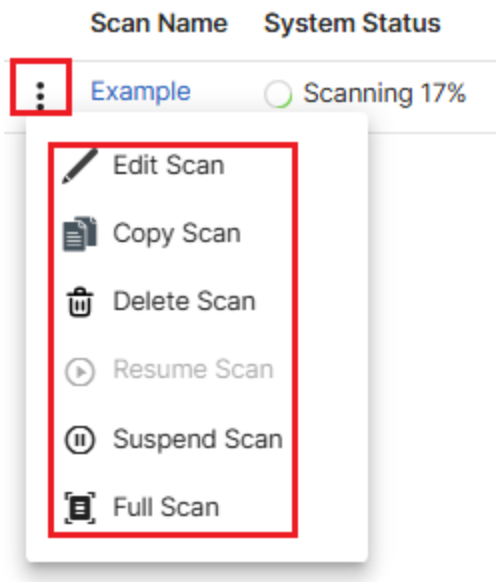
7. Select the copy and quarantine profile (see Profiles NEW on page 29) to handle sensitive files as needed and click *NEXT*.



8. 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, assign labels to files matching the conditions, and copy or quarantine sensitive files as needed. You can perform the following operations on the scan by clicking the three dots at the beginning of the scan row and selecting an option from the list. To view scan results, go to *Analytics on page 10*.



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

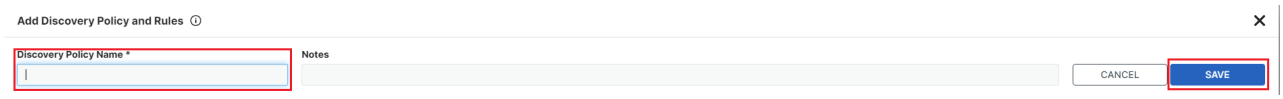
Policies

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

To create a discovery policy:

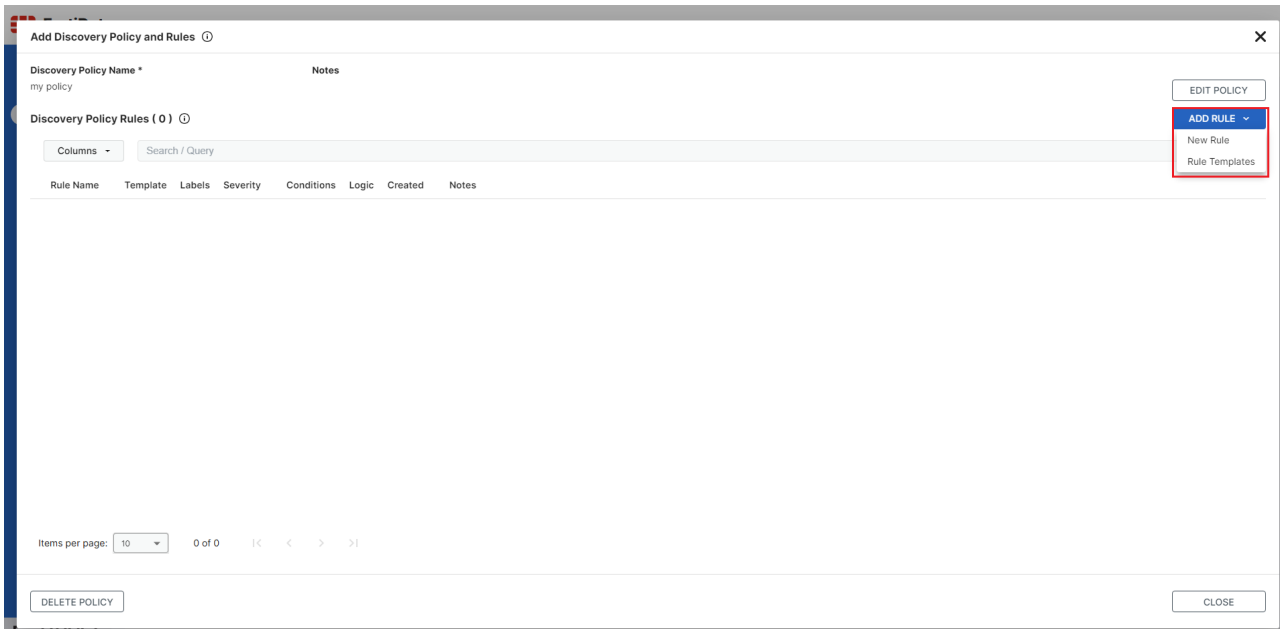
1. Go to *Discovery* > *Policies*.
2. Click *ADD DISCOVERY POLICY*.

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



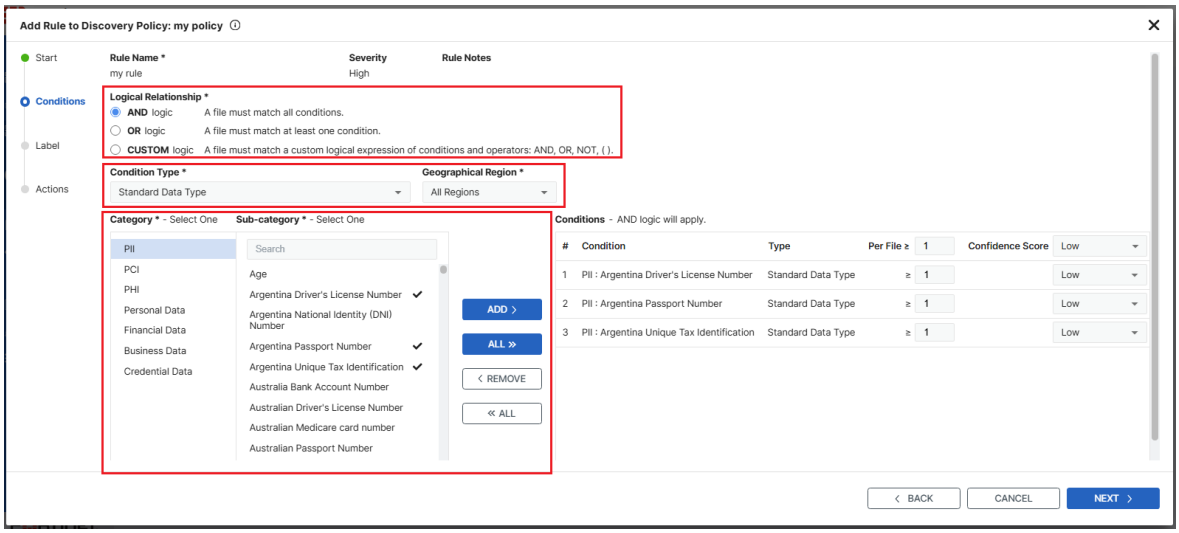
4. Click *ADD RULE* and select *New Rule* or *Rule Templates*, depending on whether you want to create your own data discovery rule or use a rule template predefined in FortiData.

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



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

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



Option	Description
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 31 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. • *ML Classified Document Type*—List of data types that are created and dynamically updated by FortiData based on machine learning algorithms. • NEW *Exact Data Match*—EDM data types that you created. • NEW *Indexed Document Match*—IDM data types that you created. • NEW *File Extension*—Choose from the following file extensions:

Option	Description
	• **Text Files**—Select from the following file extensions: `.csv`, `.json`, `.rtf`, `.txt`. • **Office Documents**—Select from the following file extensions: `.doc/.docx`, `.odp/ods/odt`, `.pdf`, `.ppt/pptx`, `.xls/xlsx`. • **Pictures**—Select from the following file extensions: `.avif`,`.bmp`, `.gif`, `.jpeg/jpg`, `.png`, `.tif/.tiff`, `.webp`. • **Source Code**—Select from the following file extensions: `.c/.cpp`,`.go`, `.java`, `.js`, `.kt`, `.php`, `.py`, `.sh`. • **Configuration files**—Select from the following file extensions: `.cfg`,`.conf`, `.env`, `.ini`, `.service`, `.toml`, `.yaml/.yml`. • **Certificate files**—Select from the following file extensions: `.cer`,`.crt`, `.key`, `.p7b`, `.pem`. • *File Type*—Choose from the following file types: • **Office Documents**—Select from the following file types: `.doc/.docx`, `.odp/ods/odt`, `.pdf`, `.ppt/pptx`, `.xls/xlsx`. • **Pictures**—Select from the following file types: `.avif`,`.bmp`, `.gif`, `.jpeg/jpg`, `.png`, `.tif/.tiff`, `.webp`. • **Text Files**—Select from the following file types: `.csv`, `.json`, `.md`, `.rtf`, `.txt`. • **Other**—Select from the following file types: • Generic binary file with unknown or arbitrary content type • Plain text file with an ambiguous or unrecognized file extension
• *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*.
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.

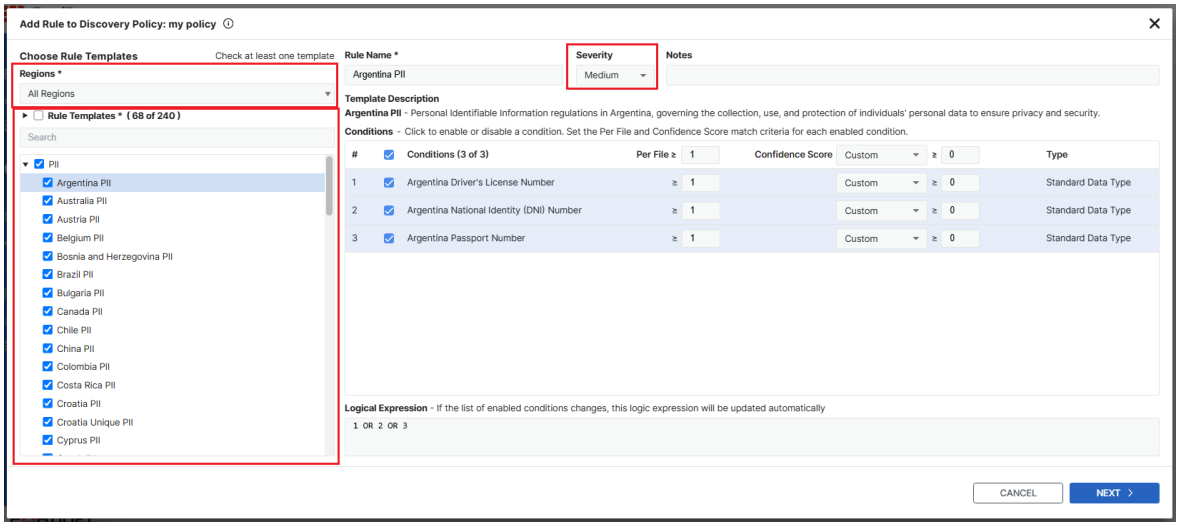
Option	Description
	For *File Type* and *Machine Learning Document Classification Type* condition types, the match criteria is always exact match.

iii. Add or remove conditions as needed.

iv. Click *NEXT*.

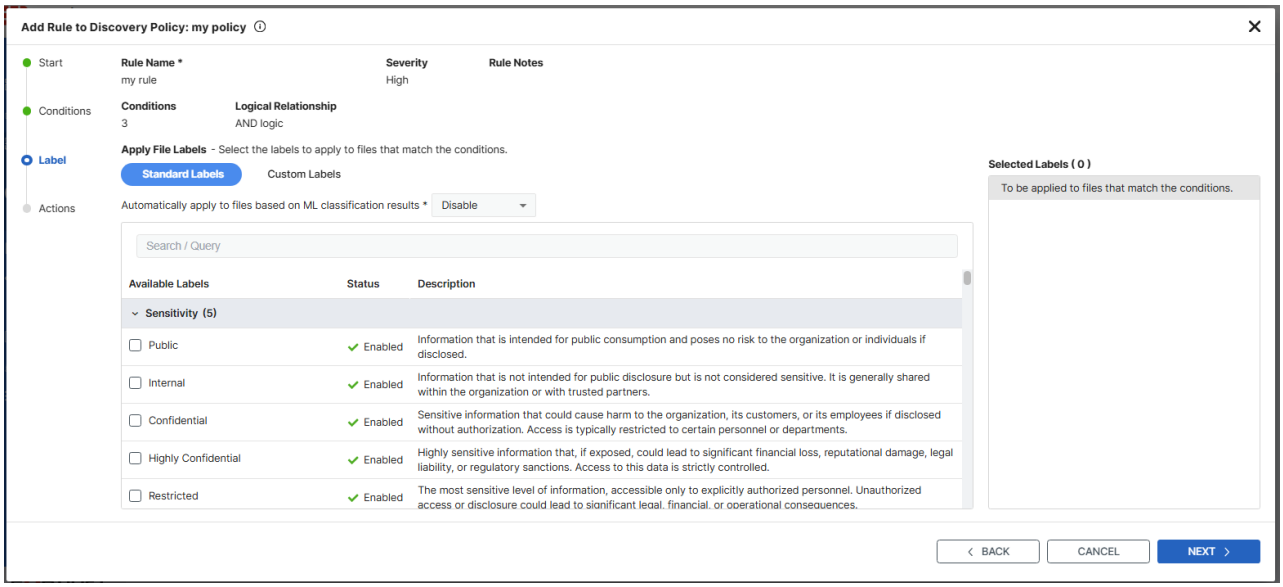
- To add a rule based on the FortiData templates:

i. Specify the region and severity for the rule template and select the categories and sub-categories from the rule template list, as needed.



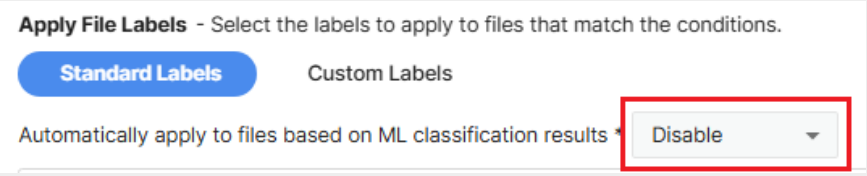
ii. Click *NEXT*.

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

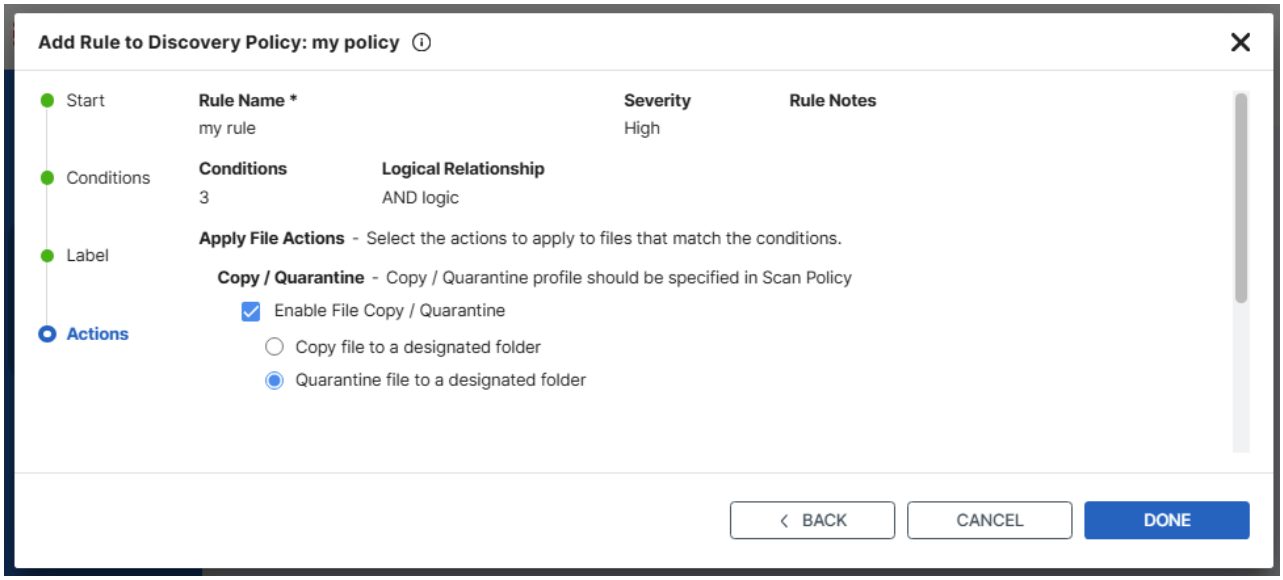


Choose from the following types and select labels under each type:

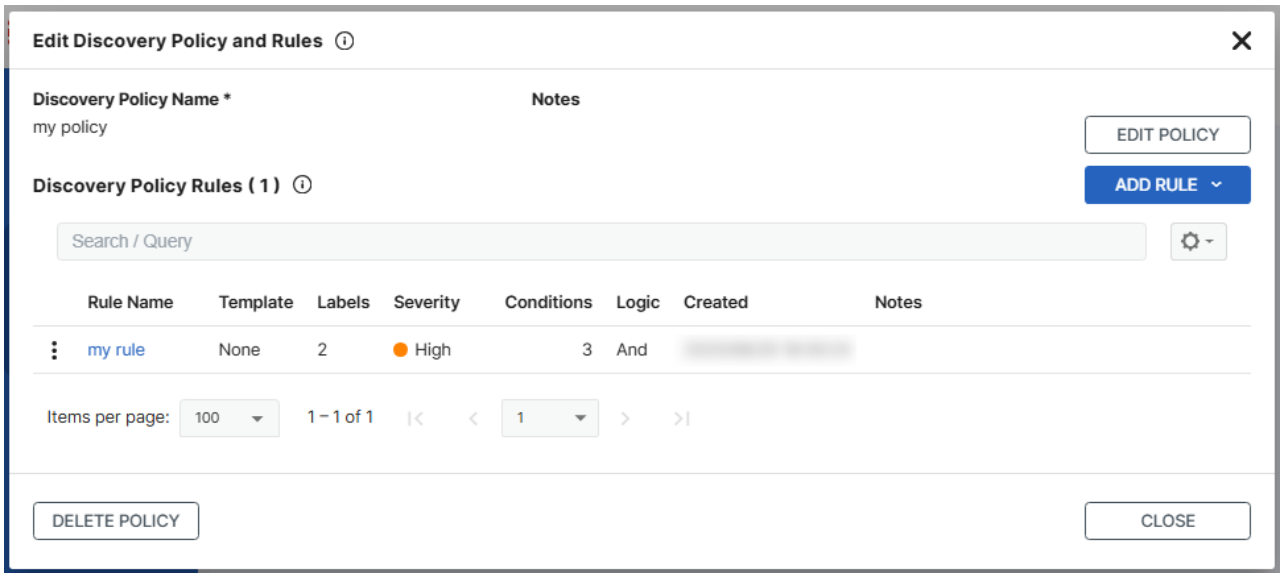
- Use the *Search/Query* box to filter the results. A complete list of each label type is available in the Data Labels on page 45 page.
- Before selecting any labels, make sure the label status is enabled. Otherwise, the label will not be applied to any files even if they match the selected conditions.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

Label Type	Description
Standard Labels	Predefined labels by FortiData, including machine learning labels. You can choose whether to apply machine learning labels to matching files using the following option.  When enabled, ML labels are applied to files based on the FortiData machine learning model. The application of machine learning labels depends on the condition matching of this discovery policy. If there is condition match for a file, FortiData applies machine learning labels in addition to the standard and custom labels as selected by the administrator.
Custom Labels	Custom labels that you created.

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



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



Profiles NEW

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

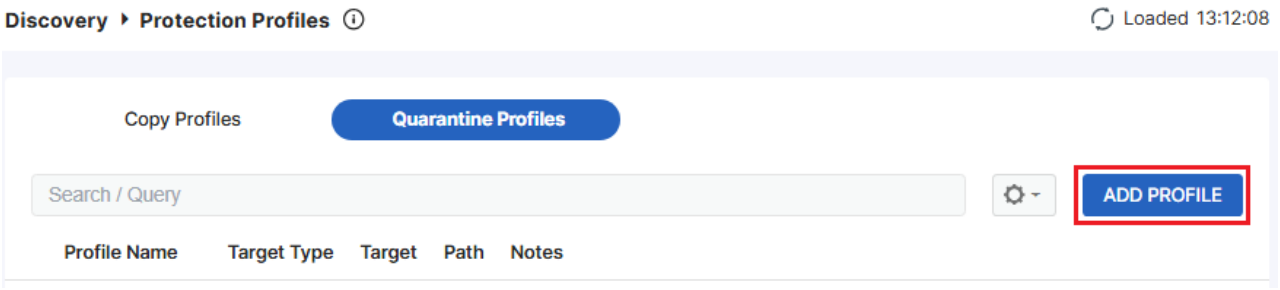
Before quarantining a sensitive file for further investigation, FortiData creates a placeholder TXT file notifying you that the original file violated compliance policies and has been quarantined. A CSV metadata file is also generated to record information about the original file before it is quarantined.

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

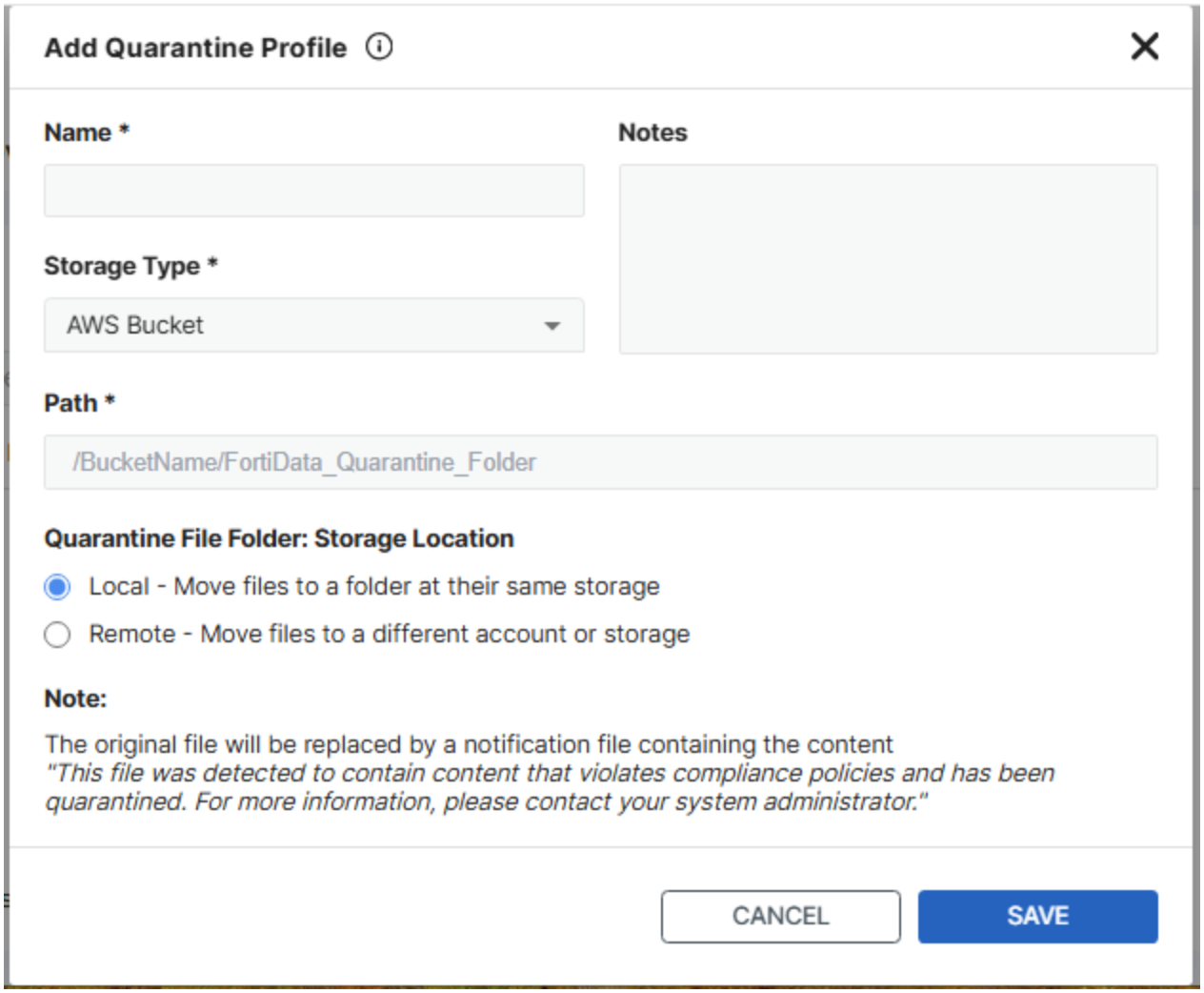
- **Copy**—Read/write permission of the destination folder
- **Quarantine**—Read/write permission of both the original files and destination folder

To create a copy or quarantine profile:

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



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



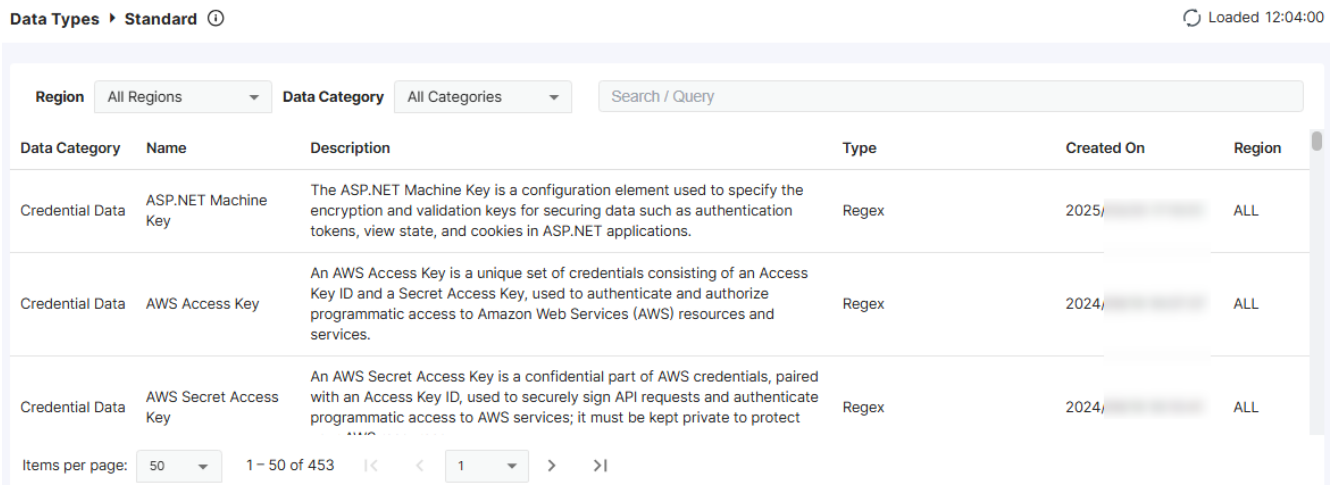
Data Types

In a DLP system, data types are categories of sensitive information that the system can detect and protect. Common data types include PII (Personally Identifiable Information), PHI (Protected Health Information), and PCI (Payment Card Information). Use the *Data Types* page to view different categories of data types in FortiData. You can also see a list of predefined rule templates defined for specific data types and regions that meet specific industry needs.

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

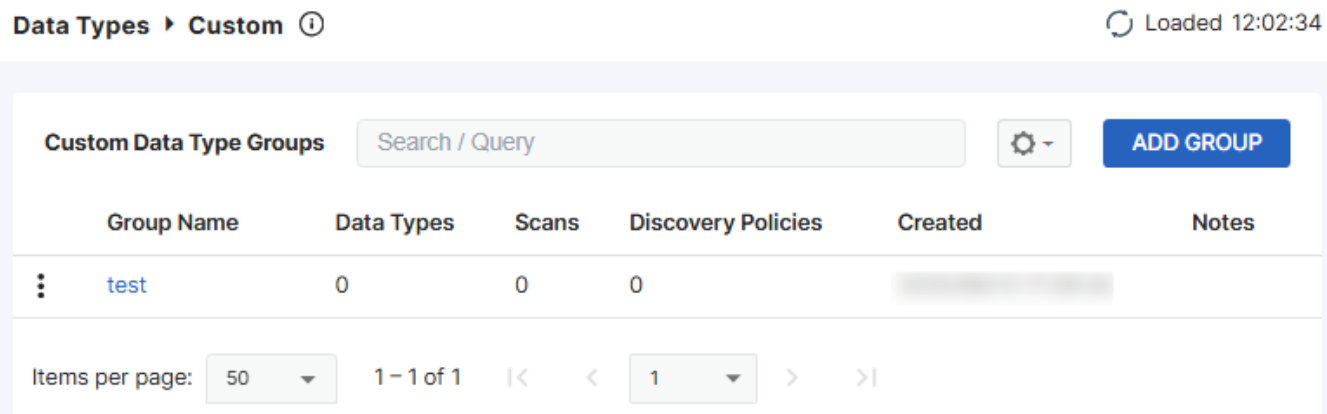
Standard

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



Custom

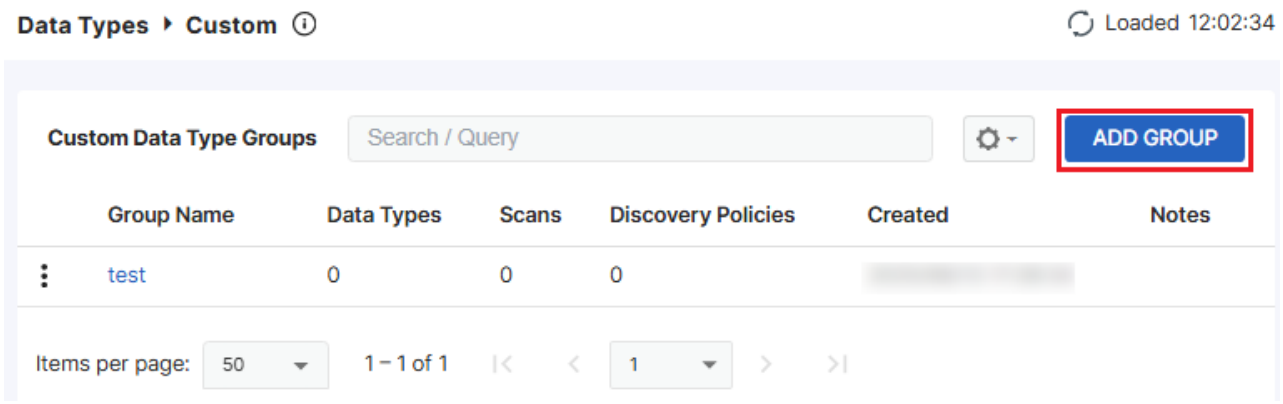
The *Custom* page displays a list of custom data type groups that you defined in FortiData. You can search the custom data type groups by group name and/or notes.



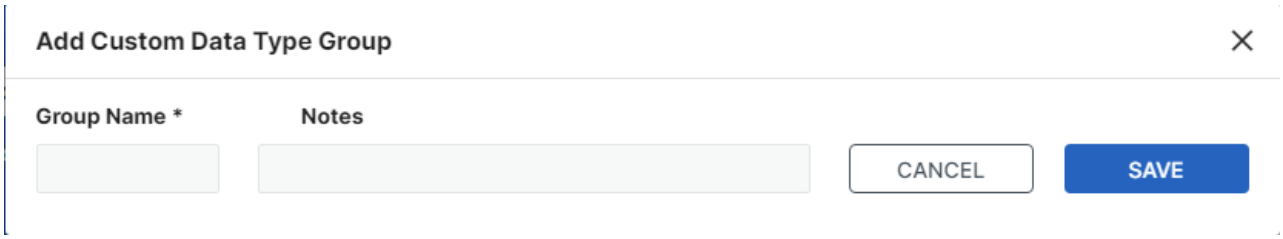
Custom data type groups are useful if the system's predefined data type do not meet your needs.

To create a custom data type group:

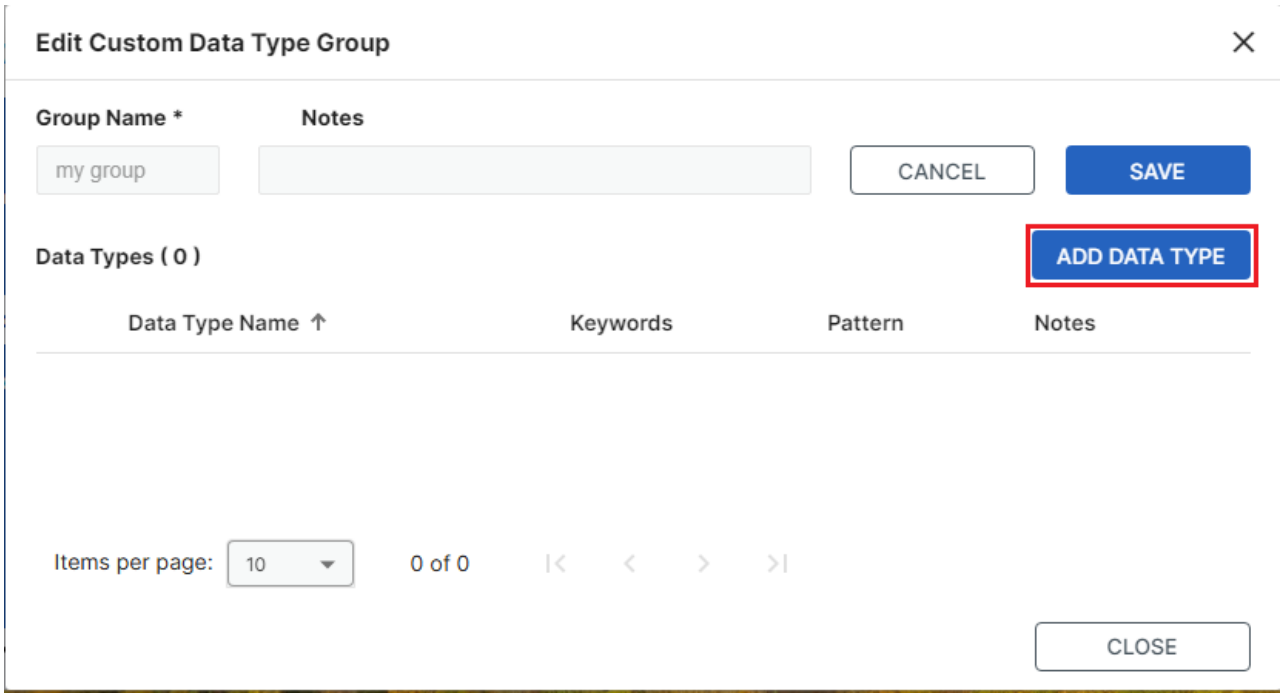
1. Go to *Data Types* > *Custom*.
2. Click *ADD GROUP*.



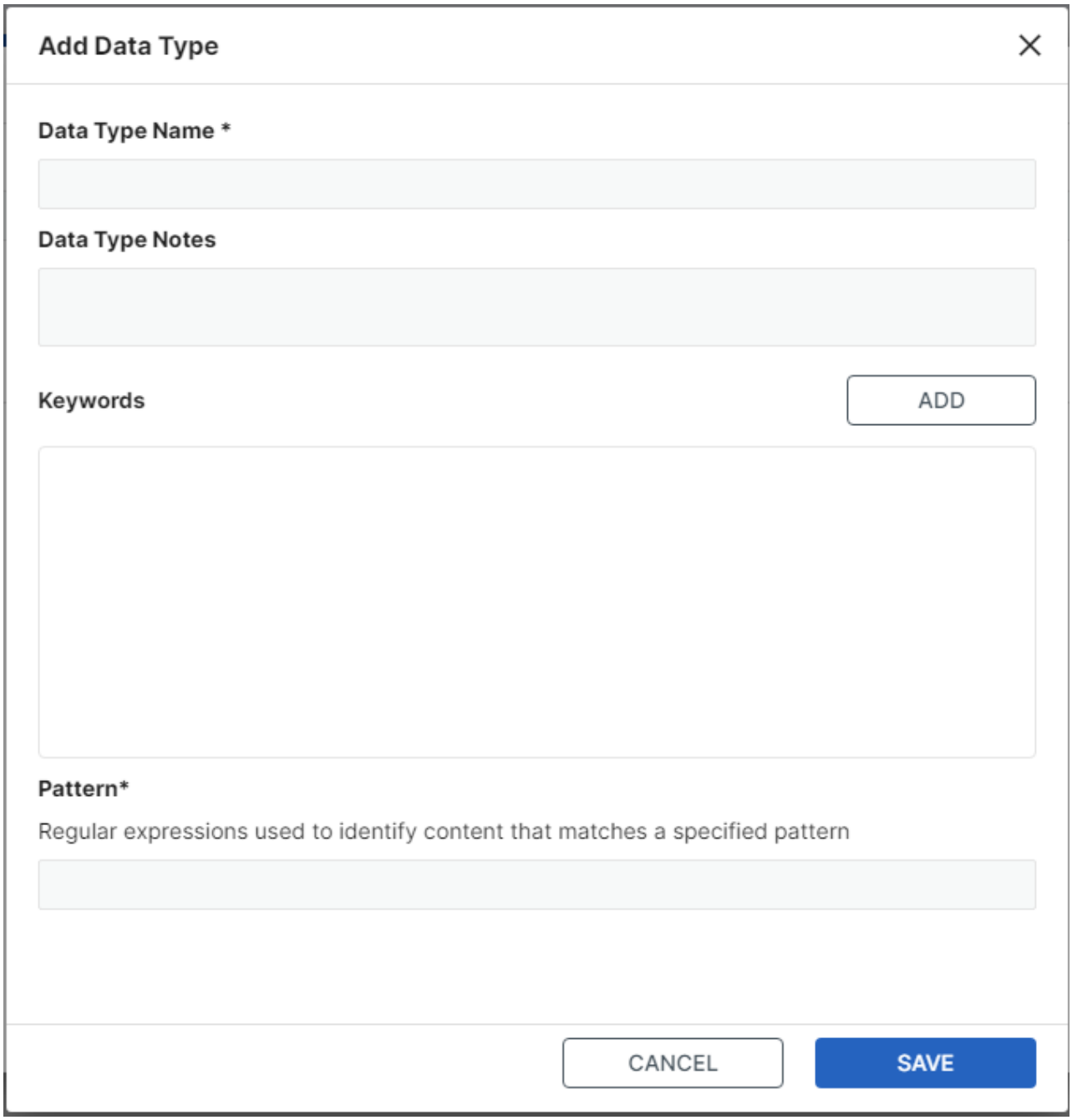
3. Specify the group name and notes, if needed.



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.

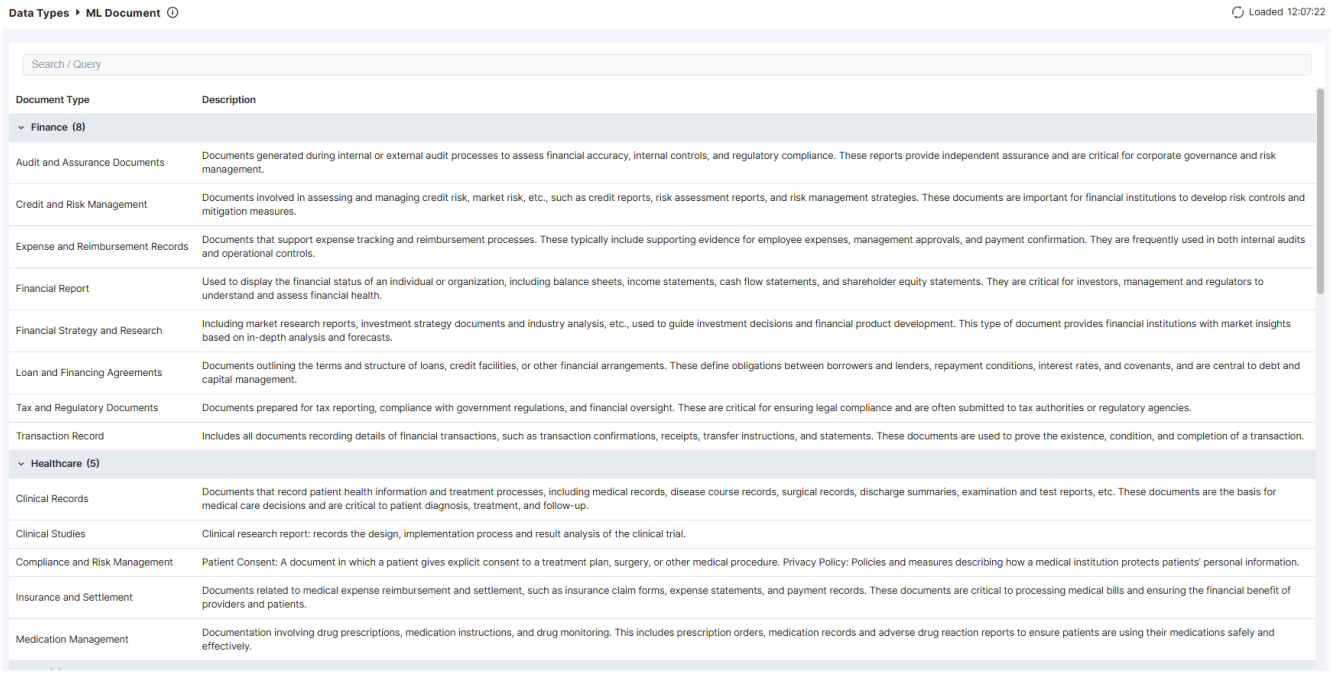
d. Click *SAVE*.

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

8. Click *CLOSE*.

Documents

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



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

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

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

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

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

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

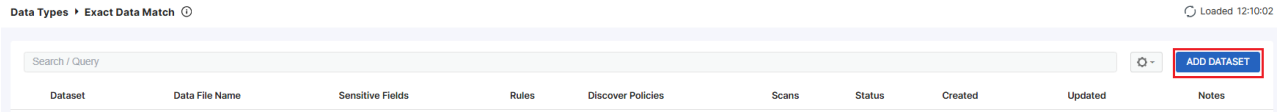
EDM NEW

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

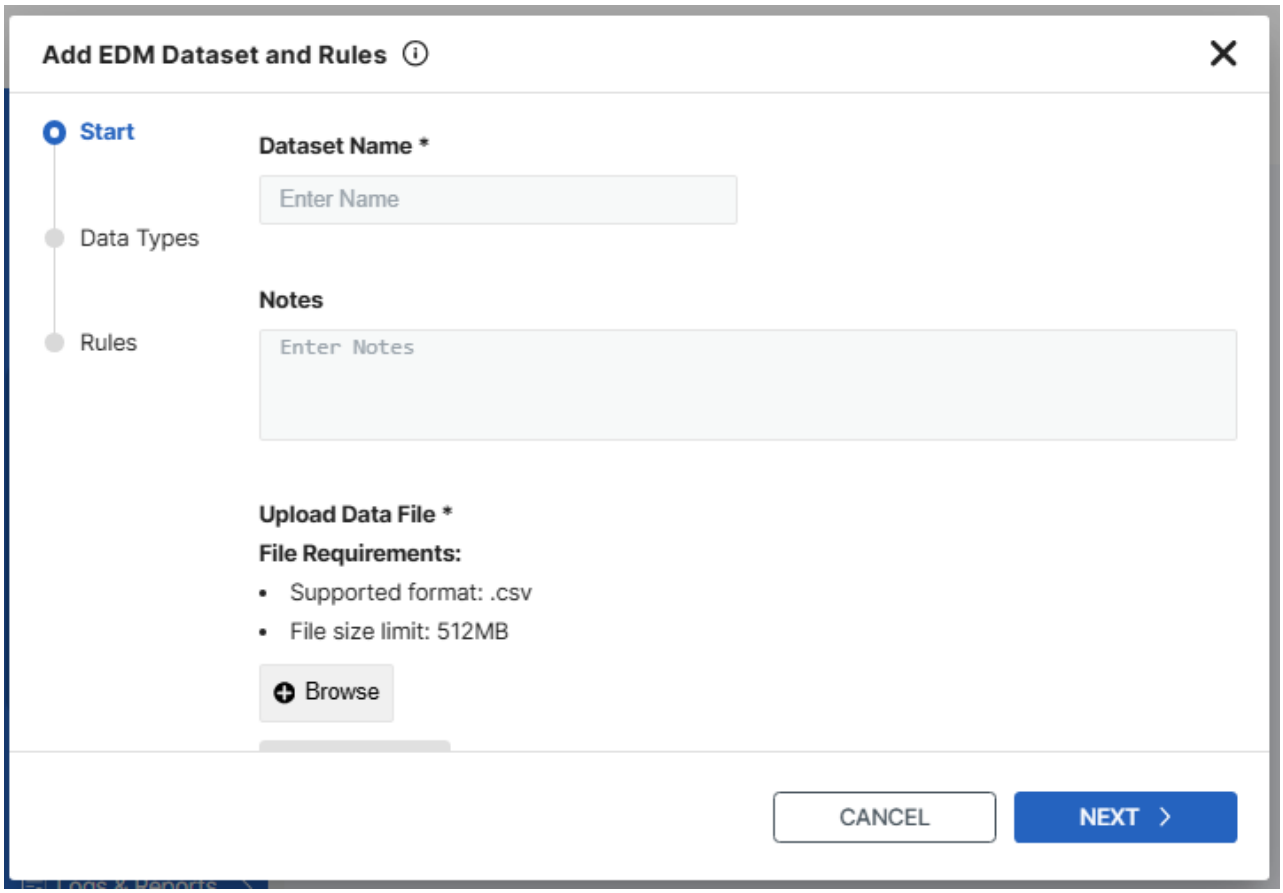
The *EDM* page displays a list of EDM data types that you defined in FortiData. You can search the EDM data type by dataset value, creation or update time, and notes.

To create an EDM data type:

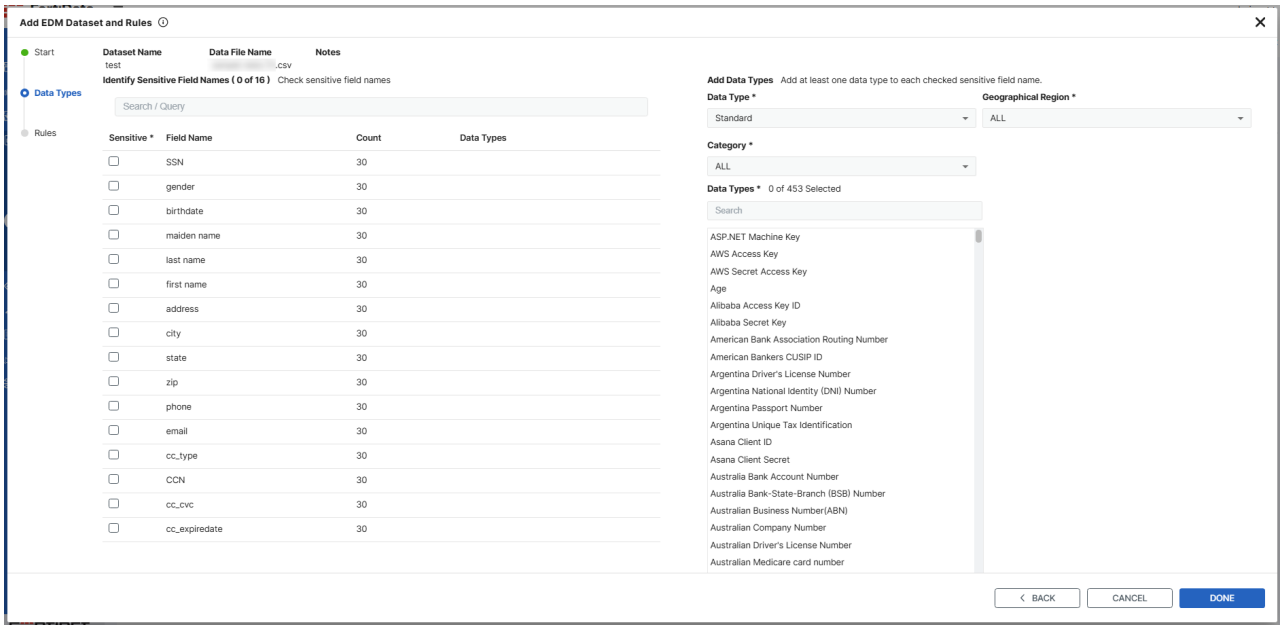
1. Go to *Data Types* > *EDM*.
2. Click *ADD DATASET*.



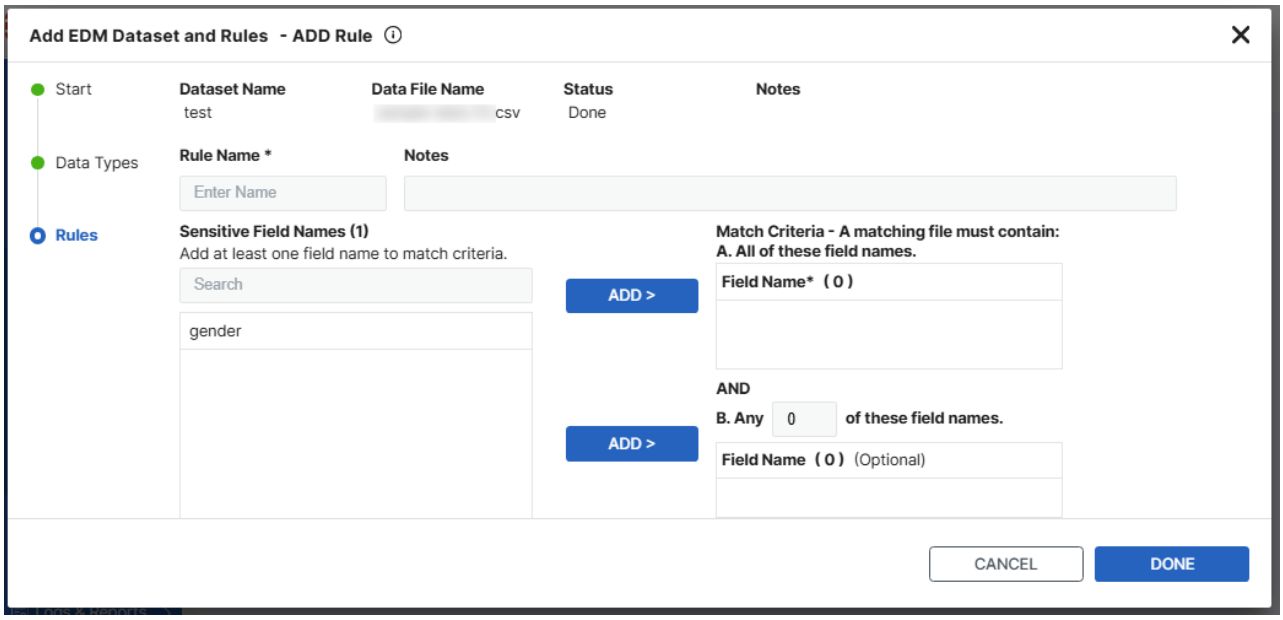
3. Specify the dataset name and notes (as needed), upload the data file (`.csv`), and click *NEXT*.



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



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



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

IDM NEW

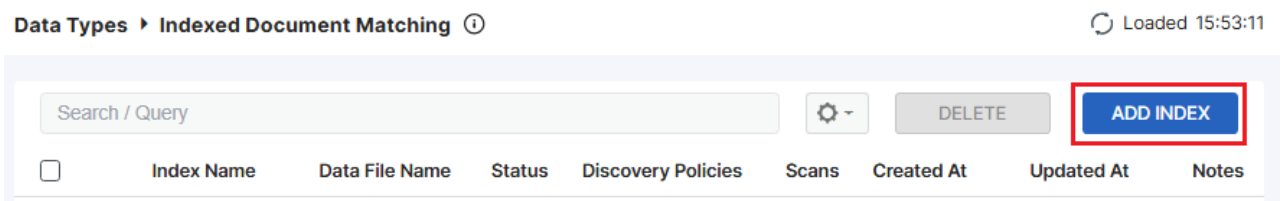
IDM (Indexed Document Matching) is a fast, interpretable, and accurate document matching approach, ideal for recognizing structured documents based on predefined formats or templates. It is especially effective in high-security, compliance-driven environments such as finance, government, and enterprise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

FortiData builds the index by processing uploaded documents, extracting key features such as text content, and storing them as searchable templates for future matching. FortiData then parses the scanned files to extract key structural features, compares them against the indexed of templates using similarity, and determines a match if the similarity exceeds a predefined threshold.

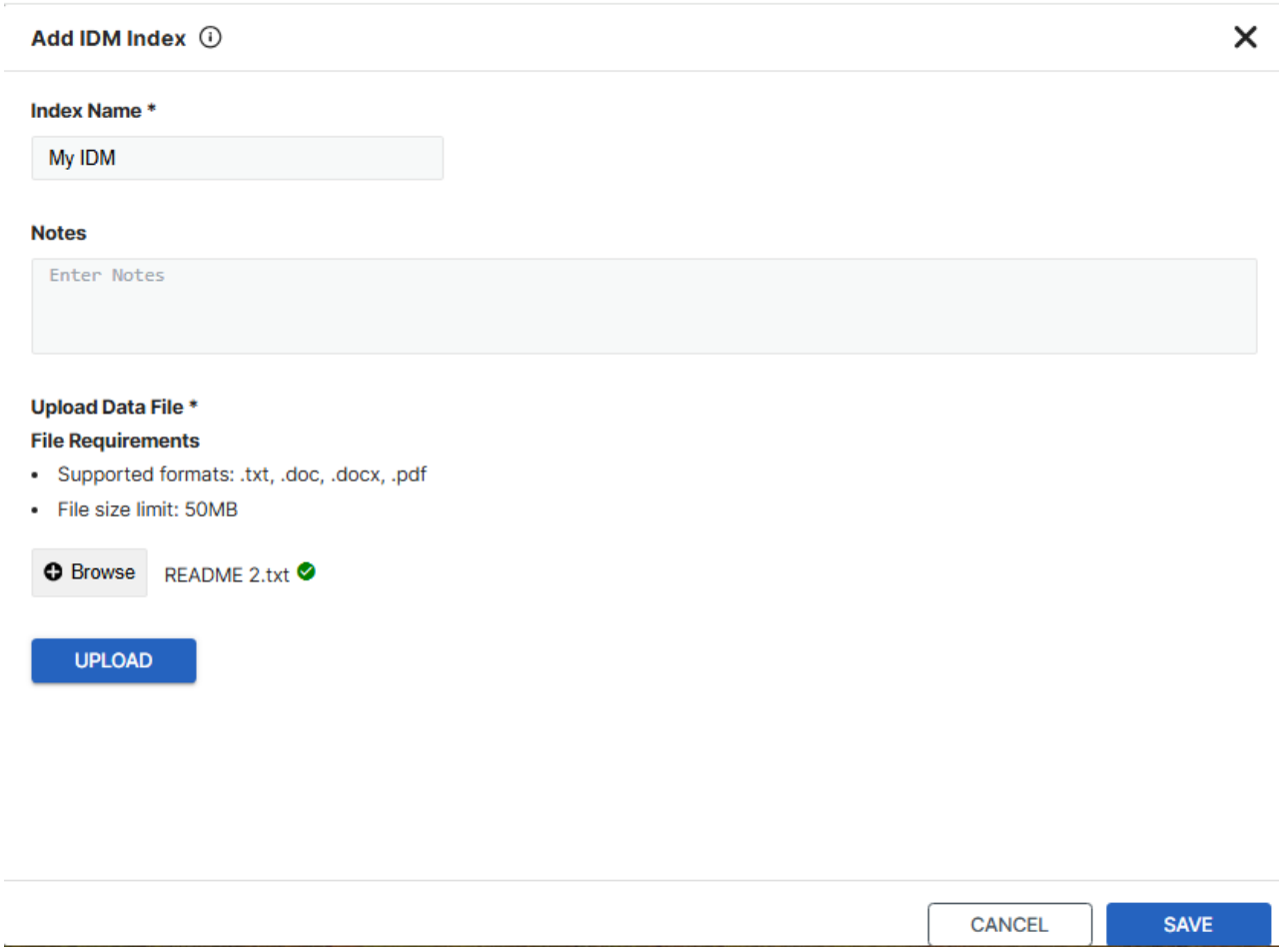
The *IDM* page displays a list of IDM data types that you defined in FortiData. You can search the IDM data type by index name, data file name, and notes.

To create an IDM data type:

1. Go to *Data Types* > *IDM*.
2. Click *ADD INDEX*.

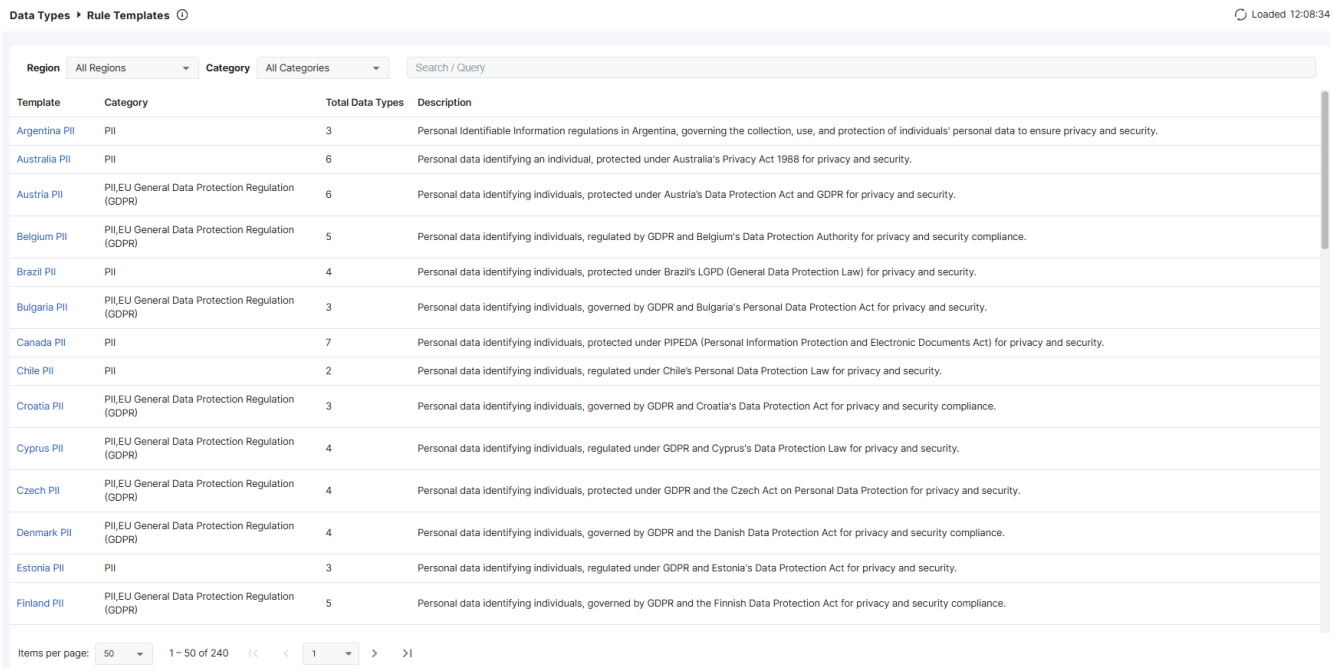


3. Specify the index name and notes (as needed), upload the data file (`.txt`, `.doc`, `.docx`, `.pdf`), and click *SAVE*.



Templates

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



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

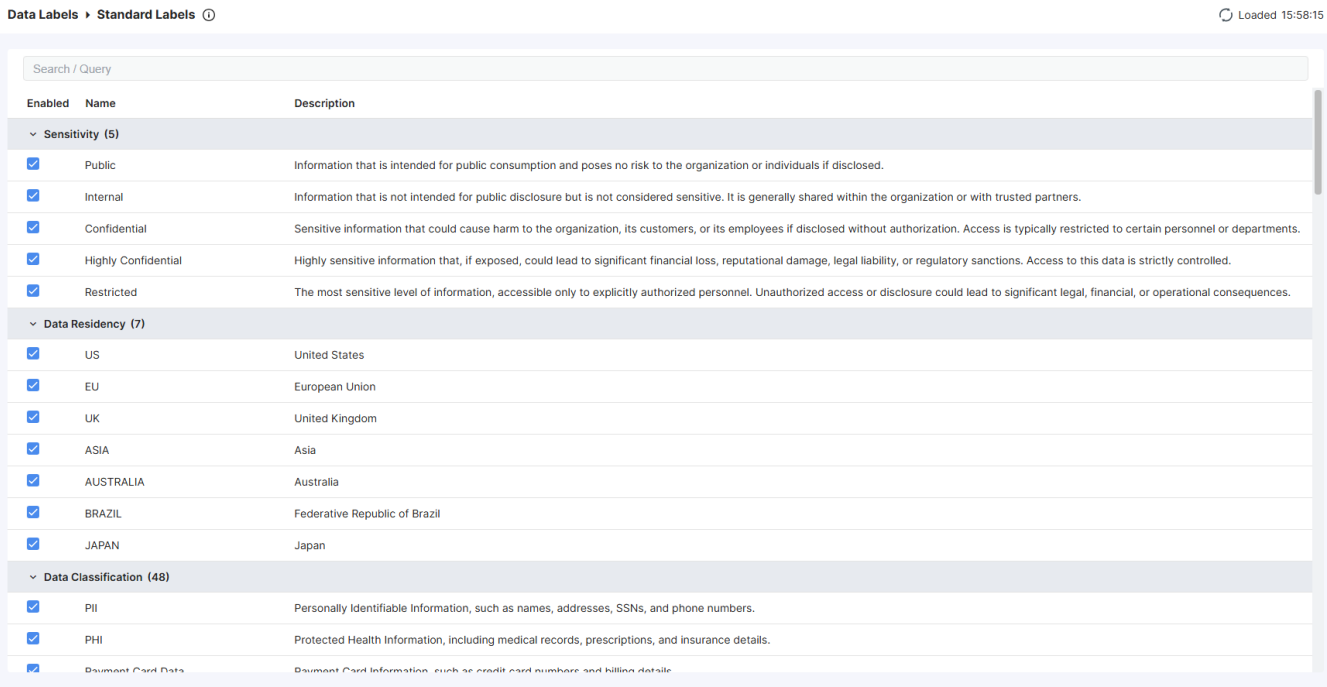
Data Labels

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

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

Standard Labels

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



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

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

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

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

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

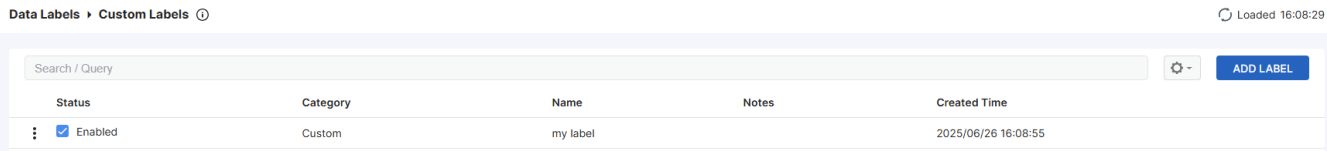
ML label	Description
NDA Form	Legal document in which one or more parties agree to maintain the confidentiality of proprietary or sensitive information disclosed during a business or professional relationship. NDAs are designed to protect trade secrets, business plans, technical data, or personal information,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

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

Custom Labels

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

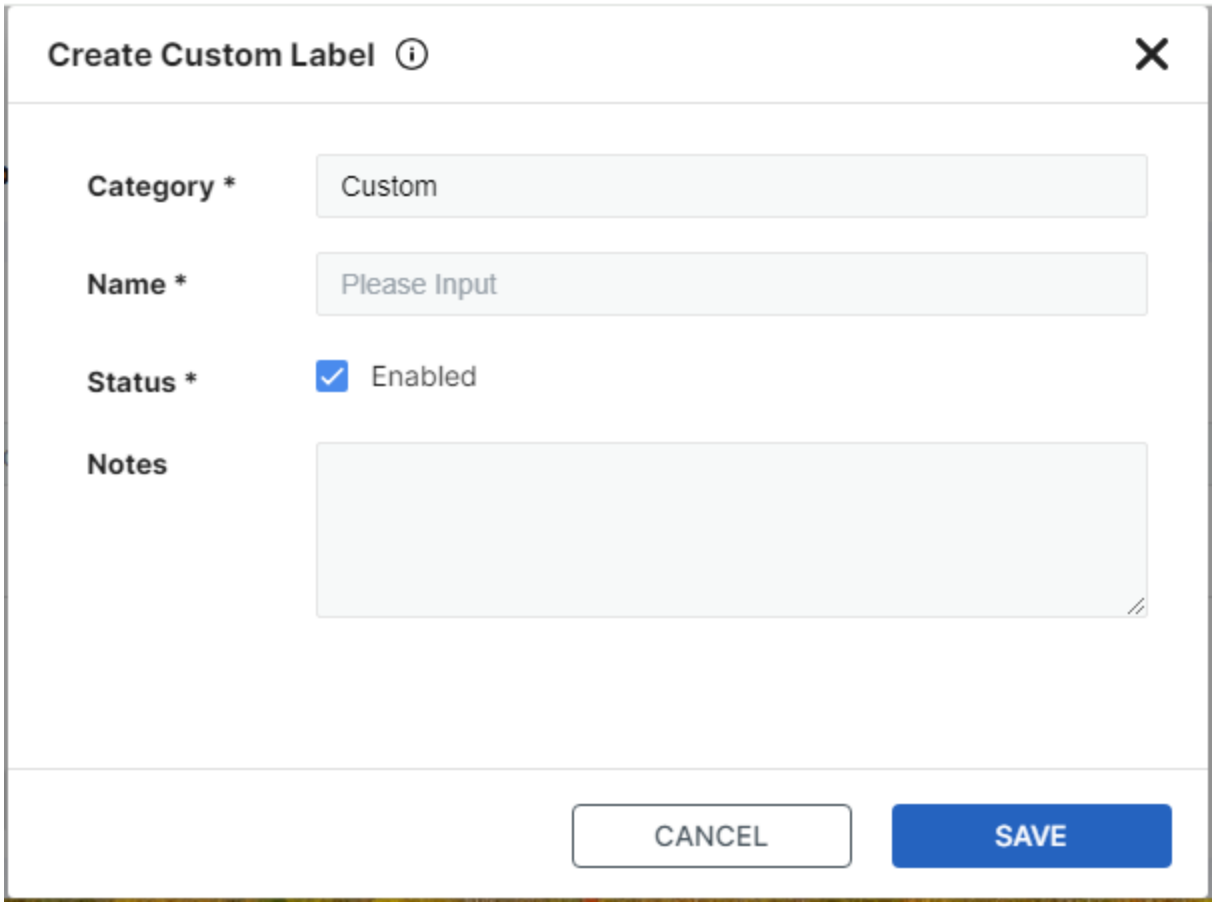
- ID
- Status
- Category
- Name
- Notes



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.



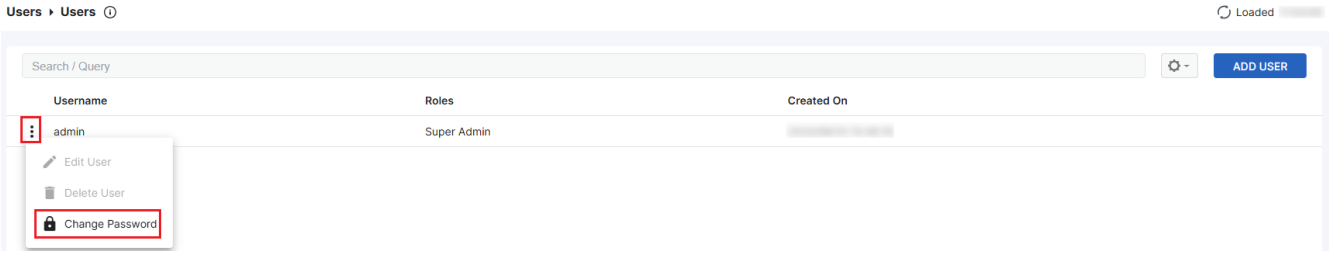
4. Click *SAVE*.
5. Click *CREATE* to confirm.

Users

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

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

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



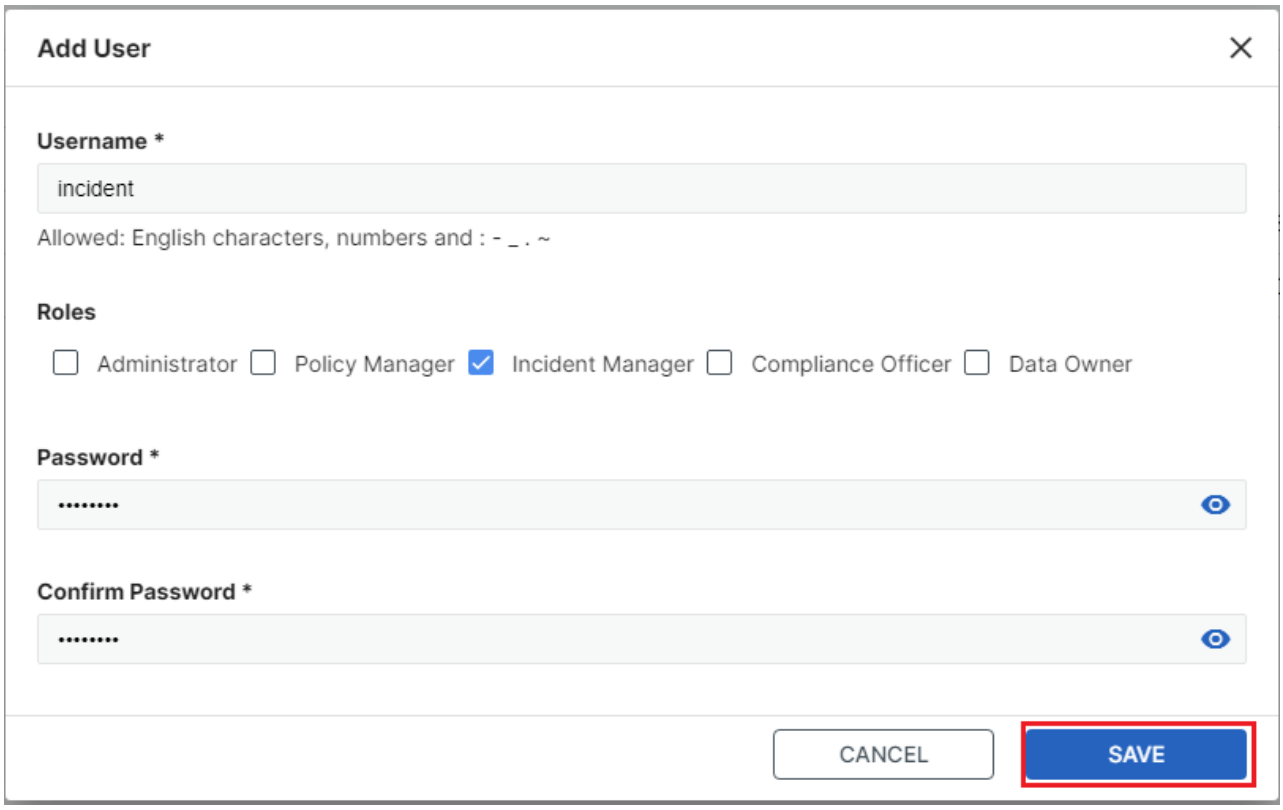
To create a user:

1. On the *Users* > *Users* page, click *ADD USER*.
2. Specify the username. Only alphabetical letters, numbers, and the following special characters are allowed in a username: : - _ . ~
3. Select a role. See role definitions below or in the *Users* > *Role Permissions* page.

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

4. Specify the password and confirm it.

5. Click *SAVE*.



6. Click *YES* to confirm.

To change the role of a user:

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

To delete a user:

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

To change the password of a user:

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

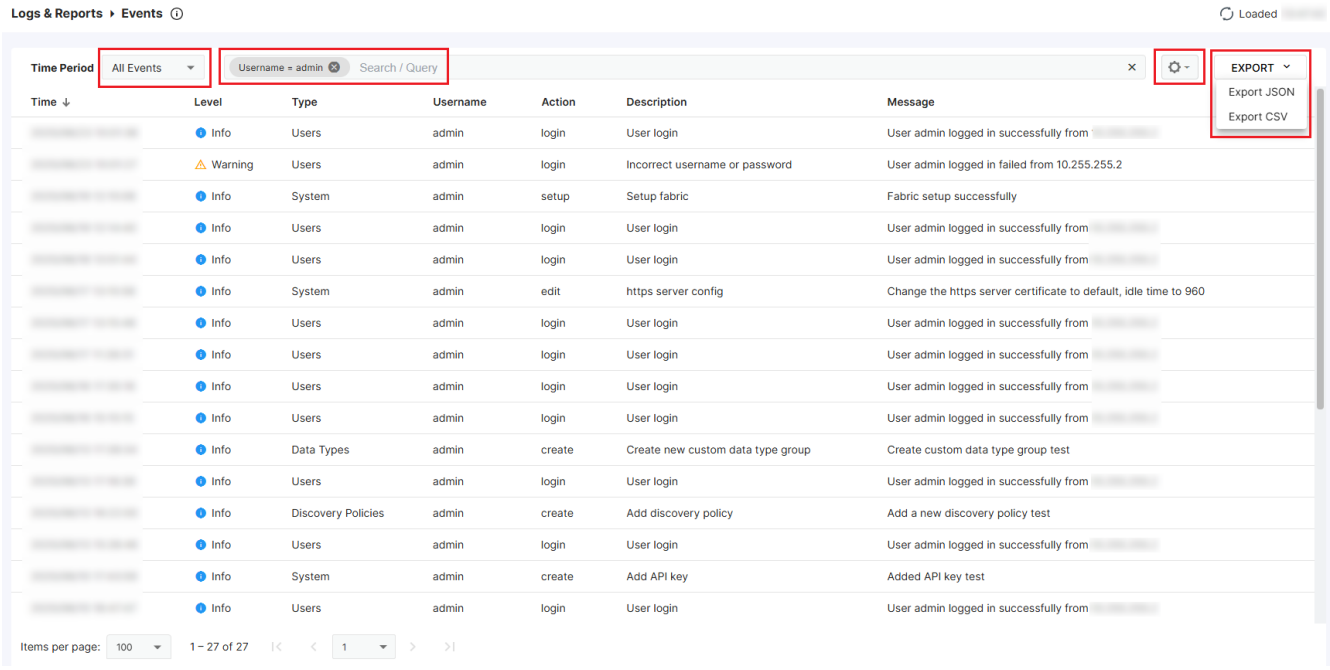
Logs & Reports

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

Events

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

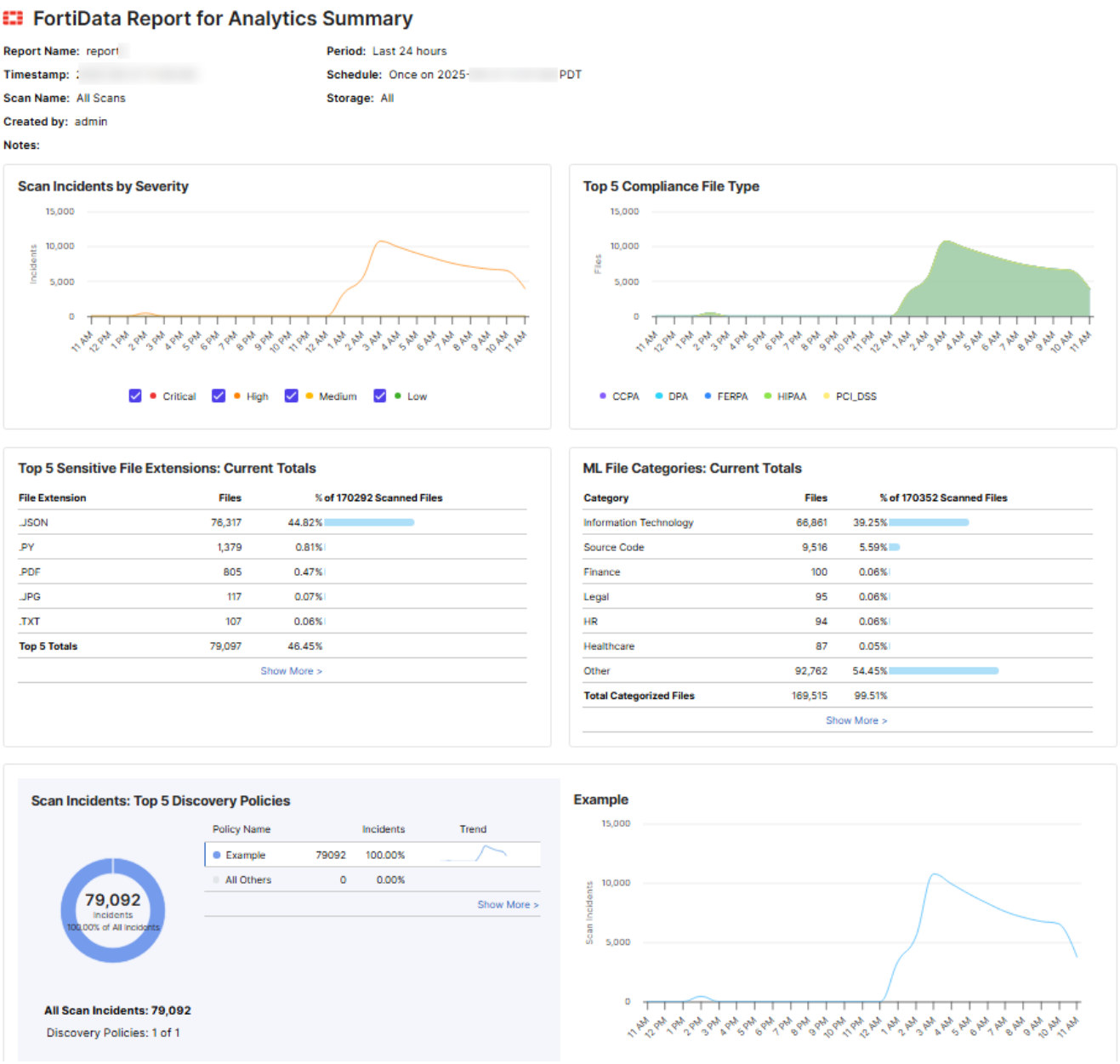
- To customize the columns to display in the table, use the *Configure* button on the top-right.
- To export the logs, click *EXPORT > Export JSON/CSV*.



Reports NEW

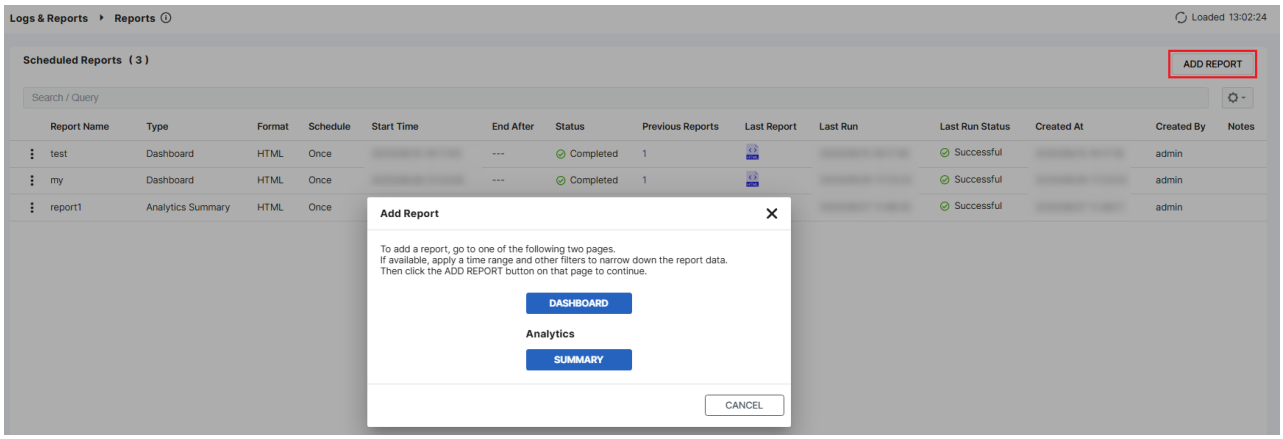
The *Logs & Reports* > *Reports* page displays a list of configured reports and the running history and status. You can create one-time or recurring Dashboard on page 7 and analytics Summary on page 10 reports (in HTML or PDF format) for a specific time period. The last report can be downloaded by clicking the file icon in the *Last Report* column.

Sample report:



To create a report:

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

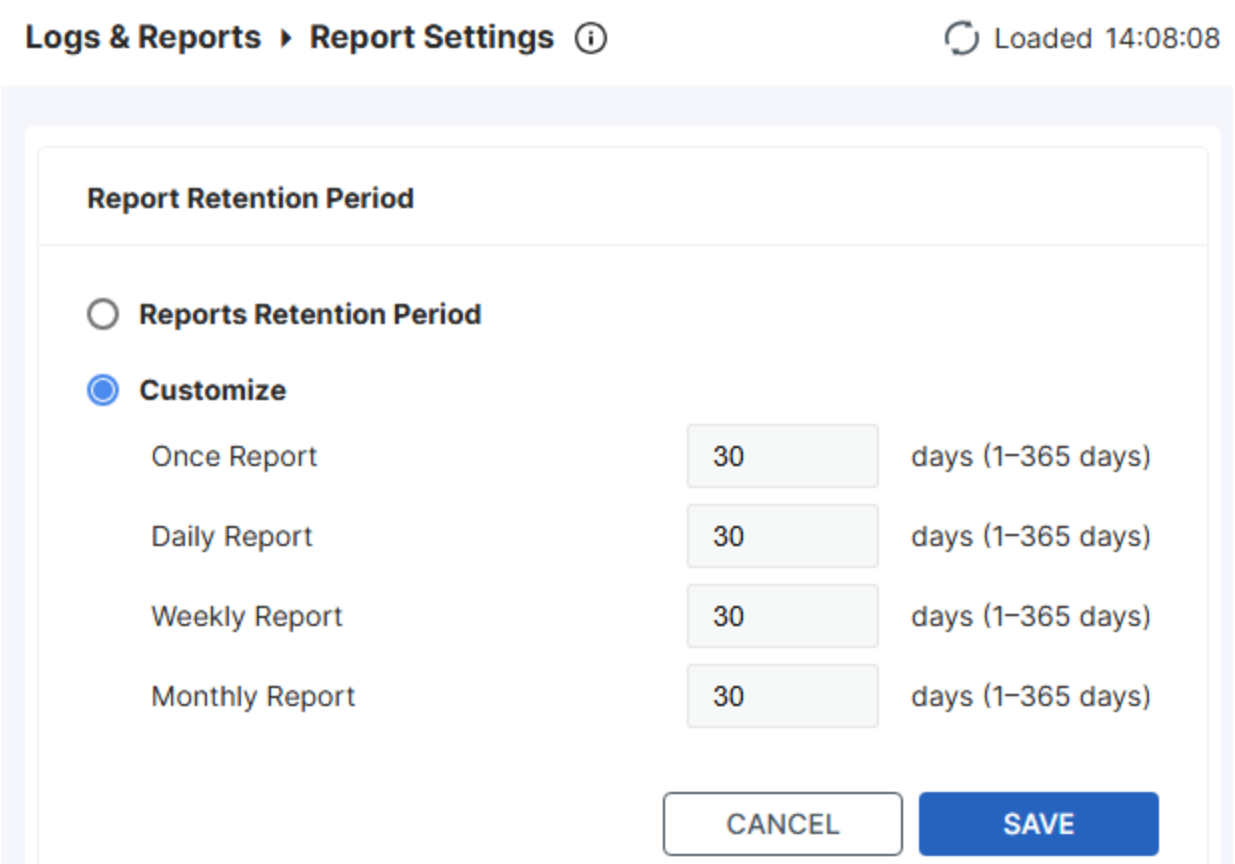


2. Click *Dashboard* or *Summary*, depending on the type of report you are creating.
3. Specify the report name, running frequency, start time, format (HTML or PDF), scan period, and notes (if needed).
4. For analytics summary reports, select the scan from the list as well.
5. Click *SAVE*.

   The report appears in the list.
6. **(Optional)** Configure the retention period for the reports in the Report Settings NEW on page 56 page as needed. The default is 30 days for all report types.

Report Settings NEW

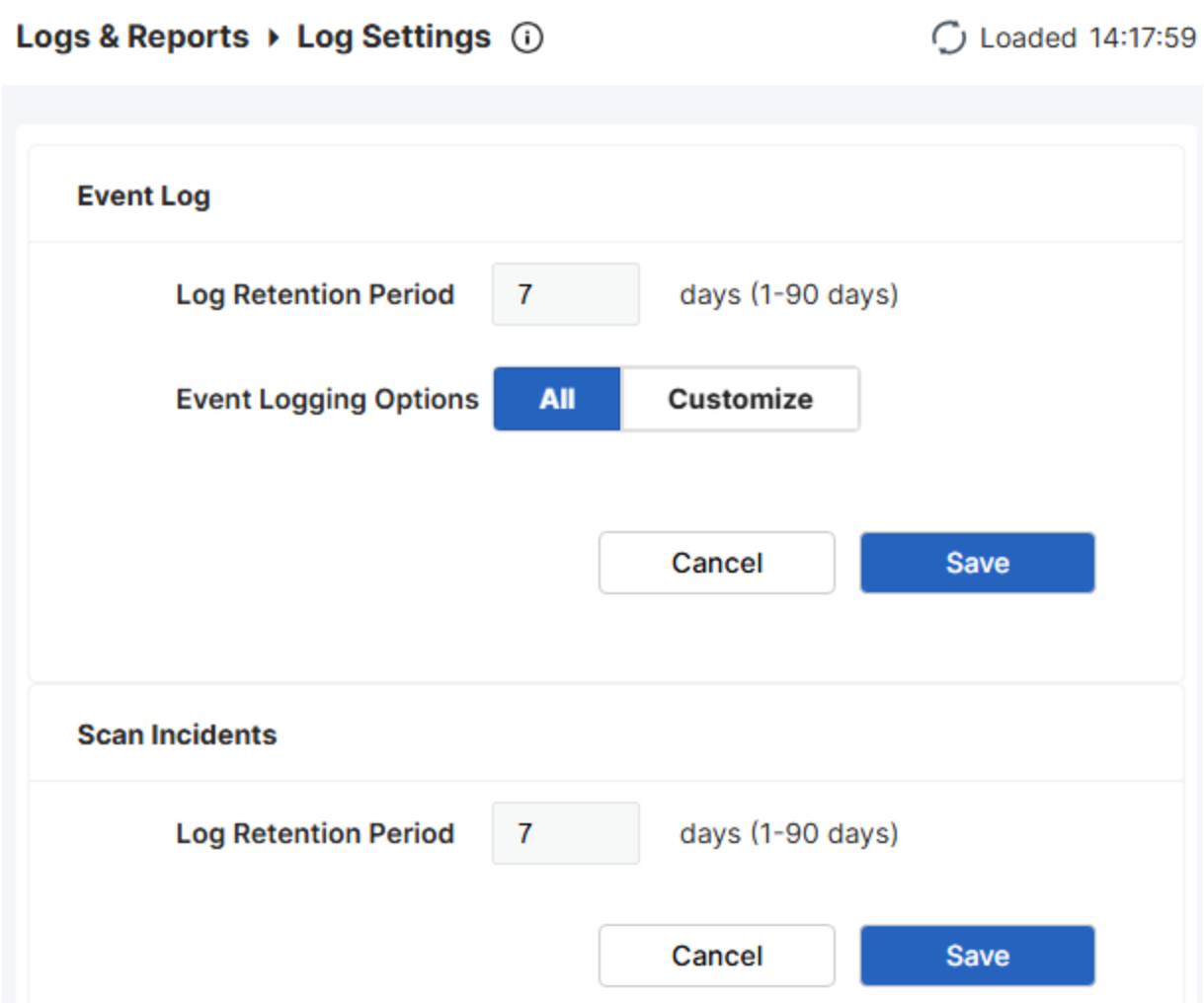
In the *Logs & Reports* > *Report Settings* page, you can configure the retention period for dashboard and analytics summary reports. See Reports NEW on page 55.



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

Log Settings

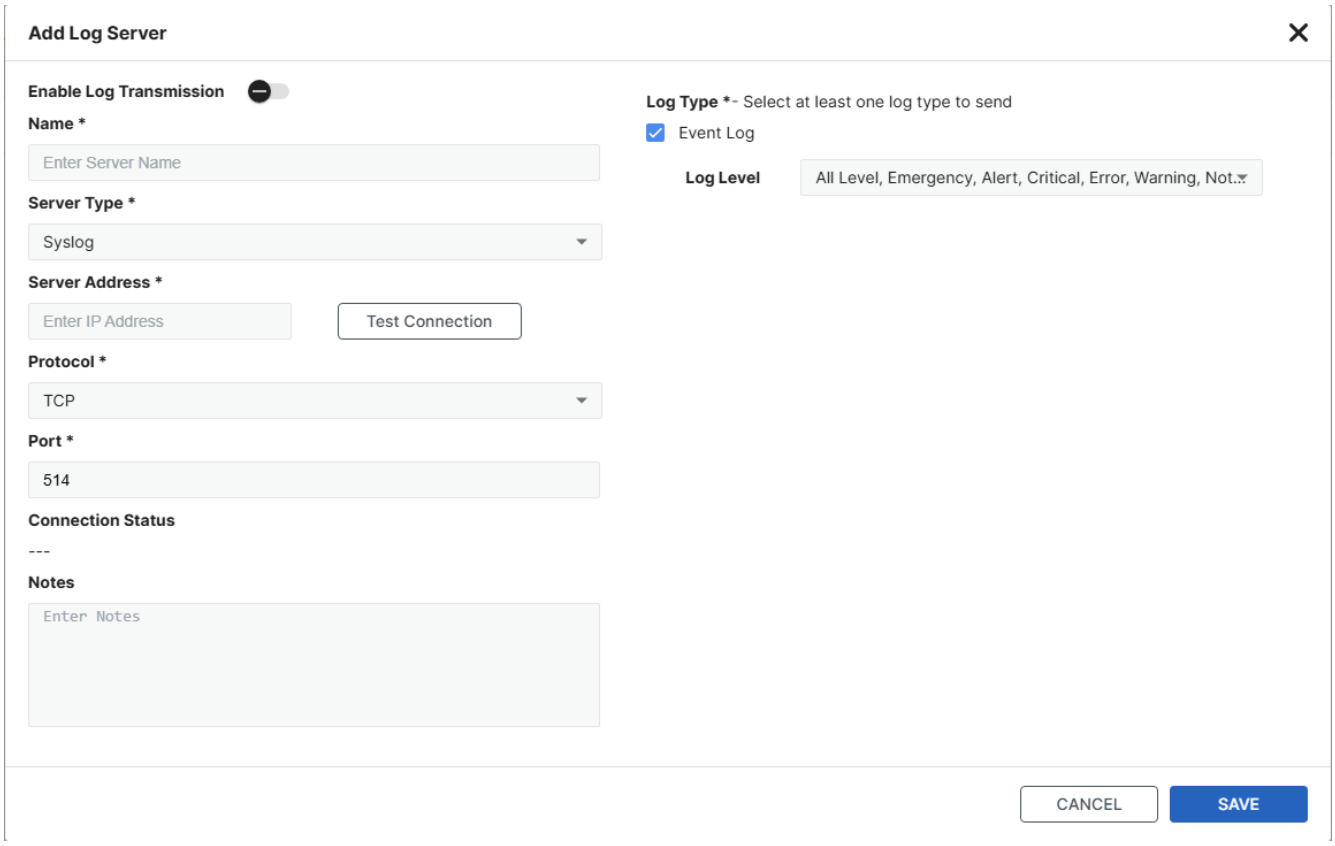
In the *Logs & Reports* > *Log Settings* page, you can configure the following options:



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

Log Servers

Configure log servers to send the logs. Click *ADD LOG SERVER* and configure the following options.



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

System

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

Network

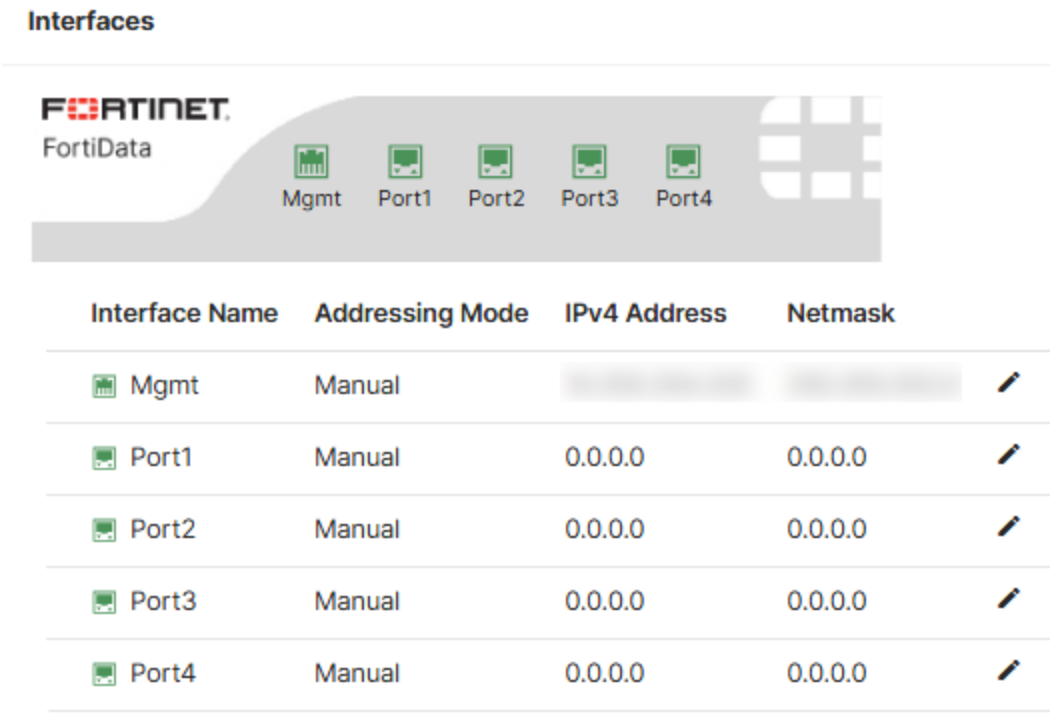
Configure the interfaces and DNS settings for FortiData in the *System* > *Network* tab.

Interfaces

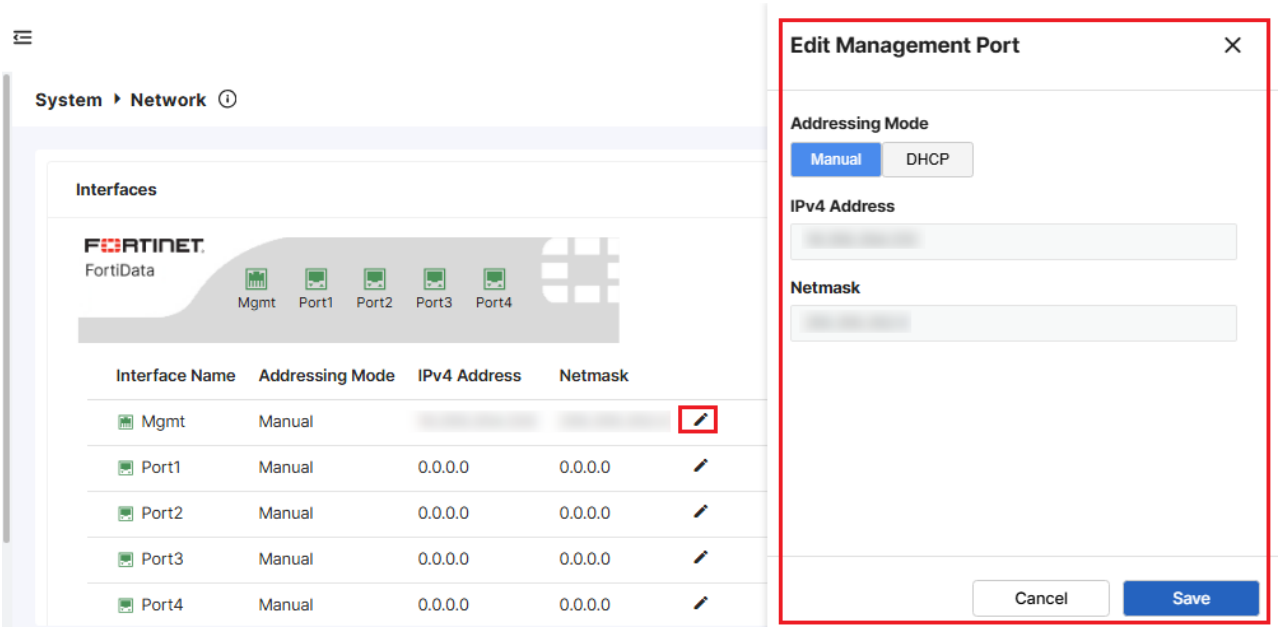
FortiData includes five interfaces: management and port 1 to 4.

To configure the interfaces:

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



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



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

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

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

DNS

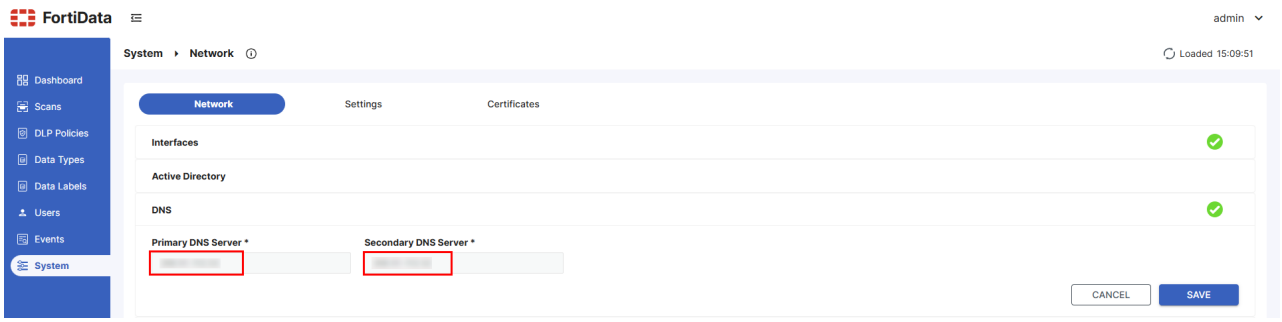
Like many other types of network devices, FortiData appliances require connectivity to DNS servers for DNS lookups.

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*.

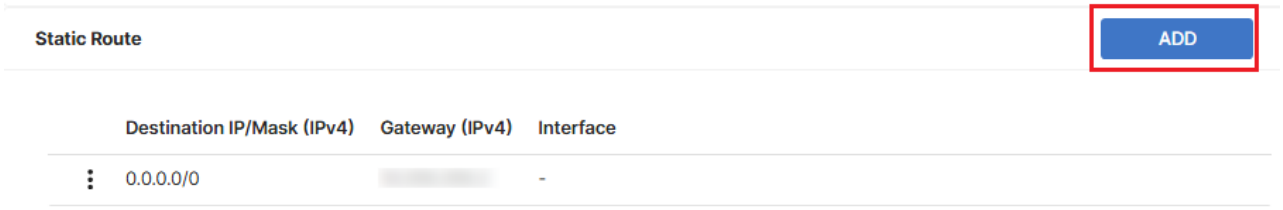
   FortiData queries the DNS servers whenever it needs to resolve a domain name into an IP address, such as for NTP system time.

Static Route NEW

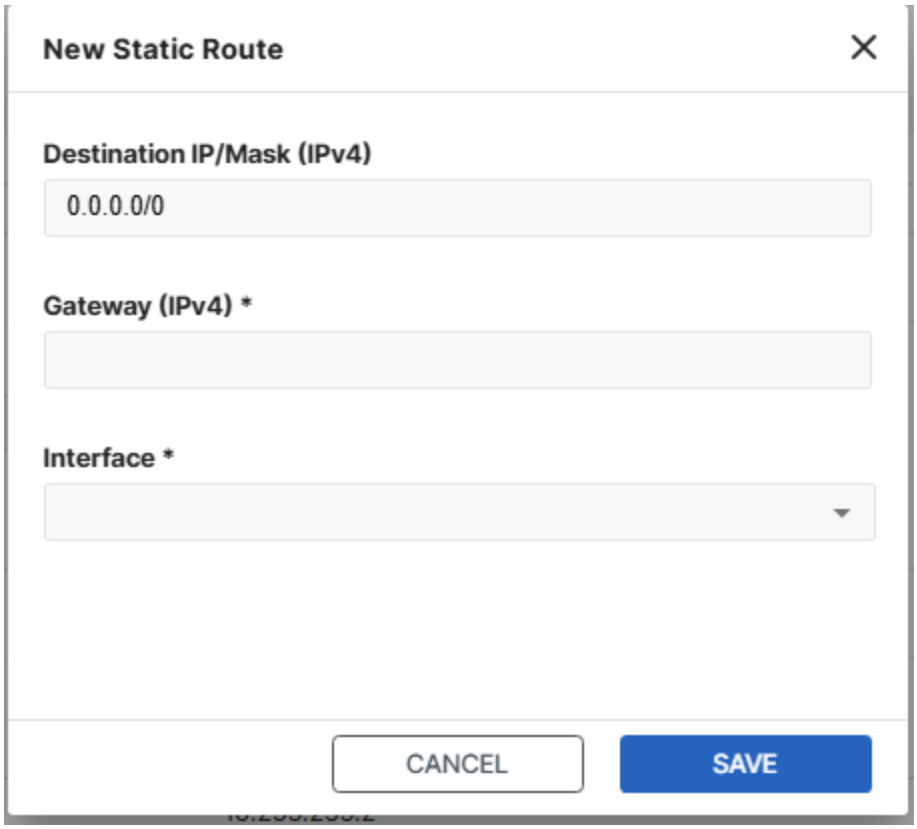
The default route has a destination of 0.0.0.0/0.0.0.0, representing the least specific route in the routing table.

To add a static route in the GUI:

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



2. Enter the following information:



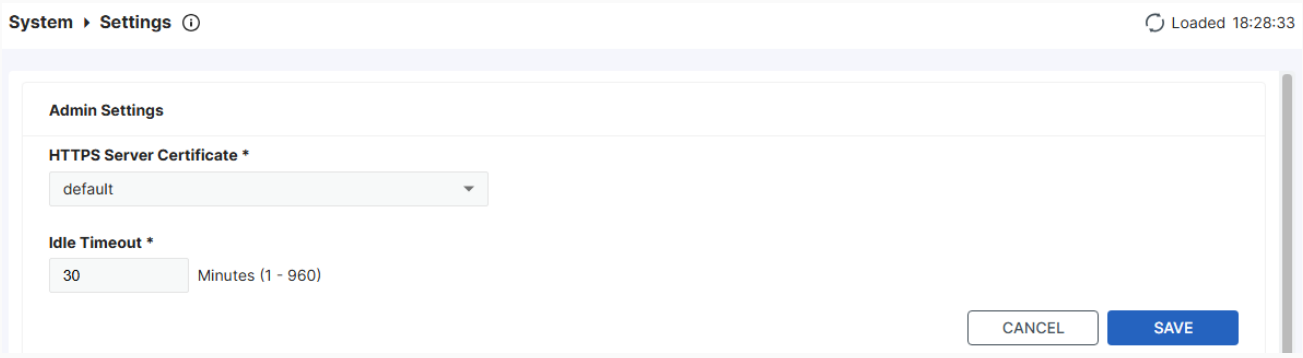
Destination IP/Mask (IPv4)	Enter the destination IP address and netmask. A value of `0.0.0.0/0.0.0.0` creates a default route.
Gateway (IPv4)	Enter the gateway IP address.
Interface	Select the name of the interface that the static route will connect through.

3. Click *SAVE*.

Settings

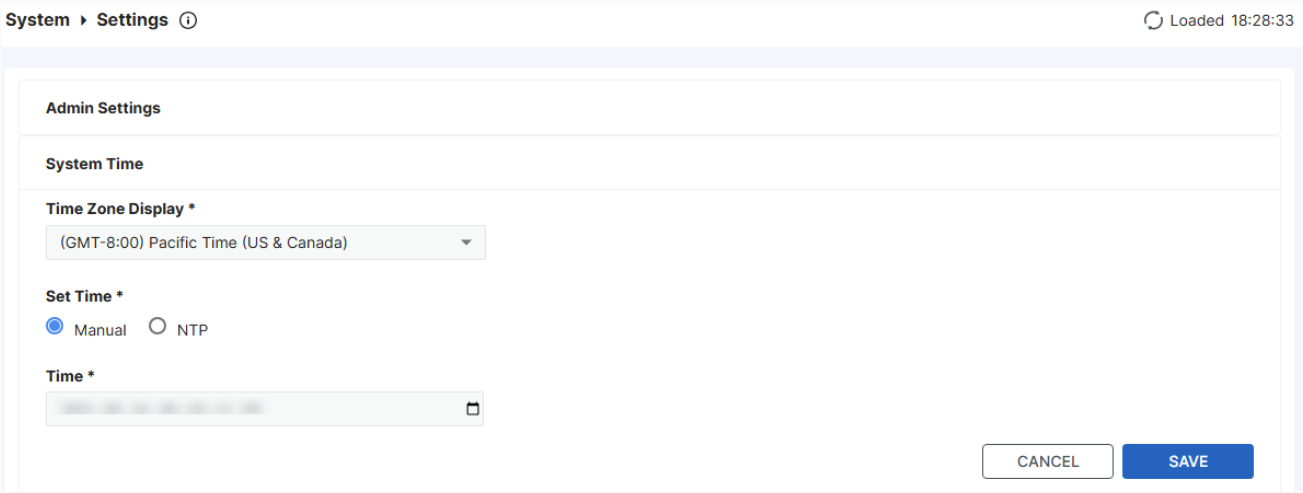
In this section, you can configure the following:

Admin Settings



HTTPS Server Certificate	Select the TLS certificates uploaded in *System* > *Certificates on page 66*.
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.

FortiGuard NEW

FortiData uses the following FortiGuard packages:

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

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

Services could be renewed via Fortinet authorised partners and distributors.

Registering or renewing the service

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

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

Upgrading the package

Follow steps below to upgrade the package:

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

Configuring FortiGuard server

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

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

To use explicit proxy for FortiGuard server:

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

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

d. Click *Apply*.

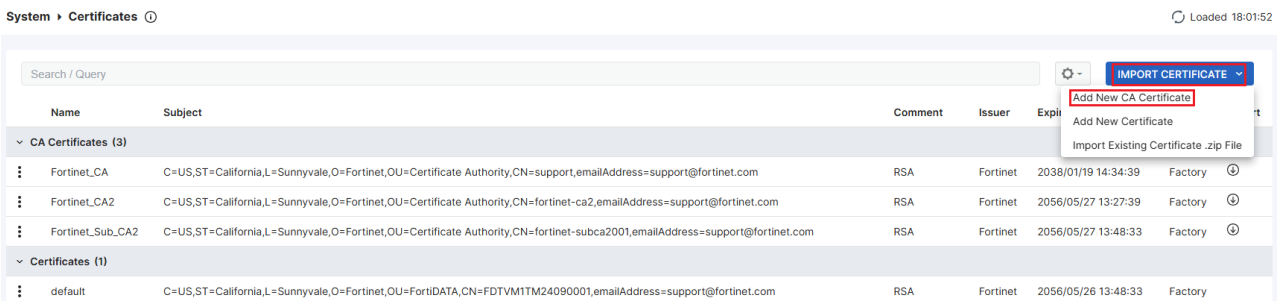
Certificates

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

- **CA certificates**—Use this option to import private or well-known CA certificates to the FortiData so that certificates signed by this CA are trusted by the FortiData.
- **Customized TLS certificates**—Use this option to import customized TLS certificates for HTTPS access to FortiData's GUI.

To import a new CA certificate:

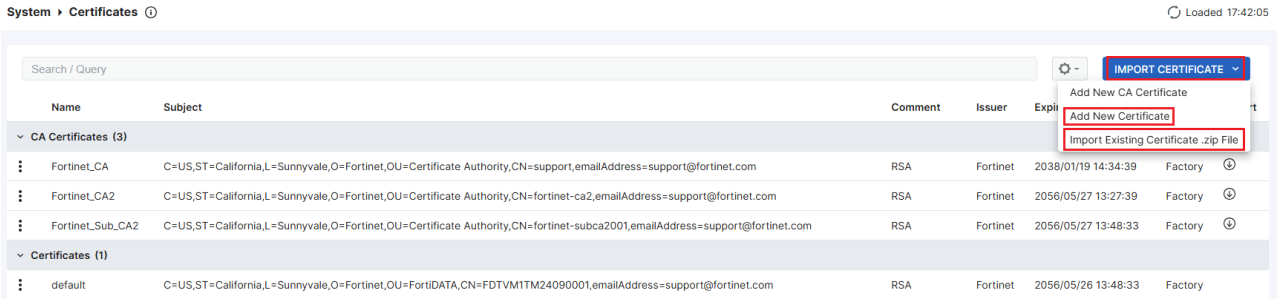
1. Go to *System > Certificates*.
2. Click *IMPORT CERTIFICATE > Add New CA Certificate*.



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

To import a customized TLS certificate:

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

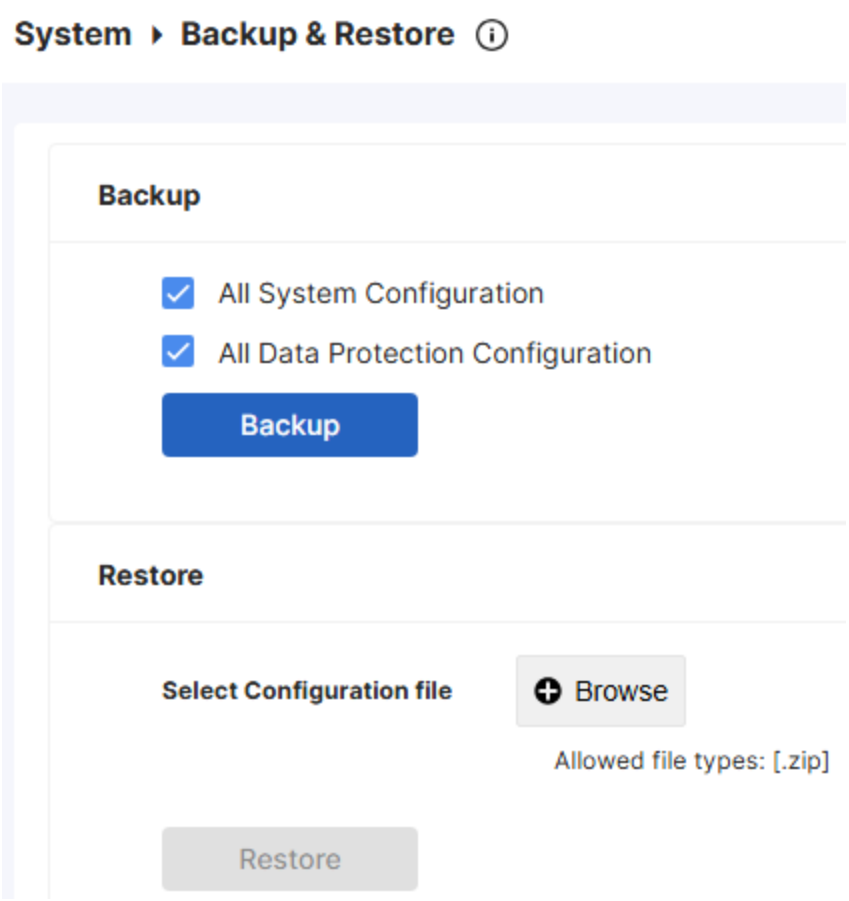


   - *Add New Certificate*—Import a certificate using certificate file and key file
   - *Import Existing Certificate .zip File*—Import an existing certificate .zip file
3. Click *BROWSE* to select the certificate file and key file or the certificate `.zip` file from your local directory.
4. **(Optional)**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

To apply the customized TLS certificate, go to the *System* > *Settings on page 64* tab.

Backup/Restore

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



To back up the FortiData configurations:

1. In the *Backup* section, select *All System Configuration* and/or *All Data Protection Configuration* (including scans and schedules, policies, data types, and data labels, which are related to data protection).
2. Click *Backup*.

To restore a saved FortiData configuration:

1. In the *Restore* section, click *Browse* to locate and select the saved configuration file (`.zip`).
2. Click *Restore*.

www.fortinet.com