FORTINET

Release Notes

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 19, 2025
FortiData 7.6.1 Release Notes
96-761-1155159-20251119

TABLE OF CONTENTS

Change log **4**
Introduction **5**
What's new **6**
Dashboard 6
Analytics 7
Discovery 8
Copying or quarantining files 8
New scan file type support 8
Configuring ML classification precision level 9
Data Types 10
EDM and IDM support 10
Changes to machine learning (ML) data types 11
Data Labels 12
Logs & Reports 13
System 15
Integration with FortiGuard 16
Adding static routes 16
Certificate enhancements 16
Cloud 16
Product integration and support **17**
Upgrade information **18**
Downloading the firmware file 18
Upgrading the FortiData 18
Resolved issues **19**
Known issues **20**

Change log

Date	Change Description
2025-07-03	Initial release.
2025-11-19	Updated Introduction on page 5 and Product integration and support on page 17.

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.

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.

The Release Notes cover product support and integration and known issues for FortiData 7.6.1, build 0103.

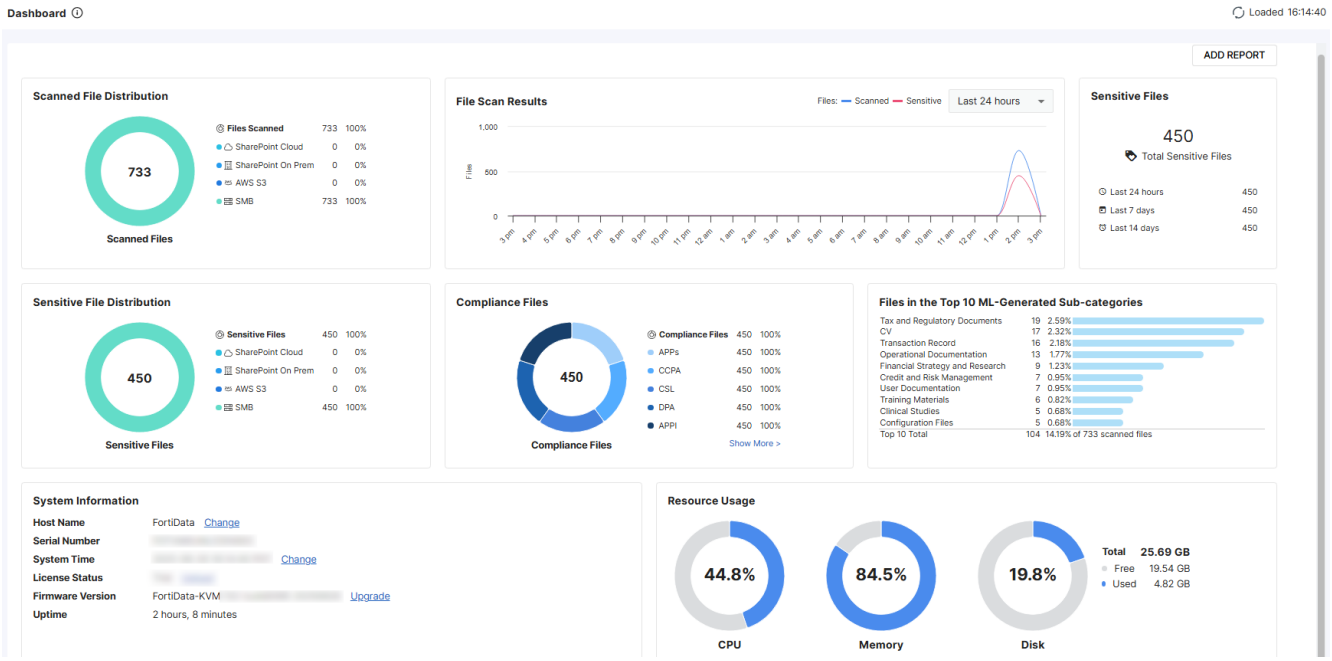
What's new

The following sections describe new features, enhancements, and changes in FortiData7.6.1:

- Dashboard on page 6
- Analytics on page 7
- Discovery on page 8
- Data Types on page 10
- Data Labels on page 12
- Logs & Reports on page 13
- System on page 15
- Cloud on page 16

Dashboard

FortiData 7.6.1 has a brand new dashboard for enhanced usability and experience. New widgets are added for sensitive file distribution, compliance files, and files in the top 10 ML-generated sub-categories.



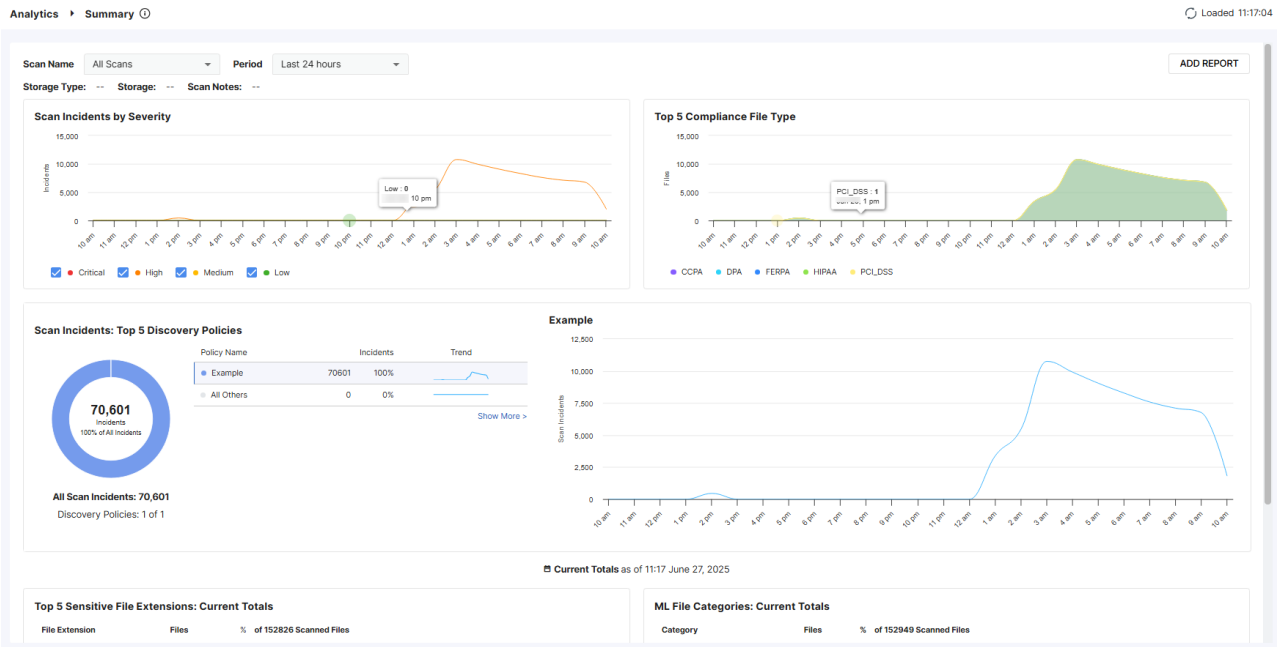
You can also add dashboard reports using the *ADD REPORT* button on the top-right corner. Reports will then be available in the *Logs & Reports* > *Reports* page.

See Dashboard in the Administration Guide for more details.

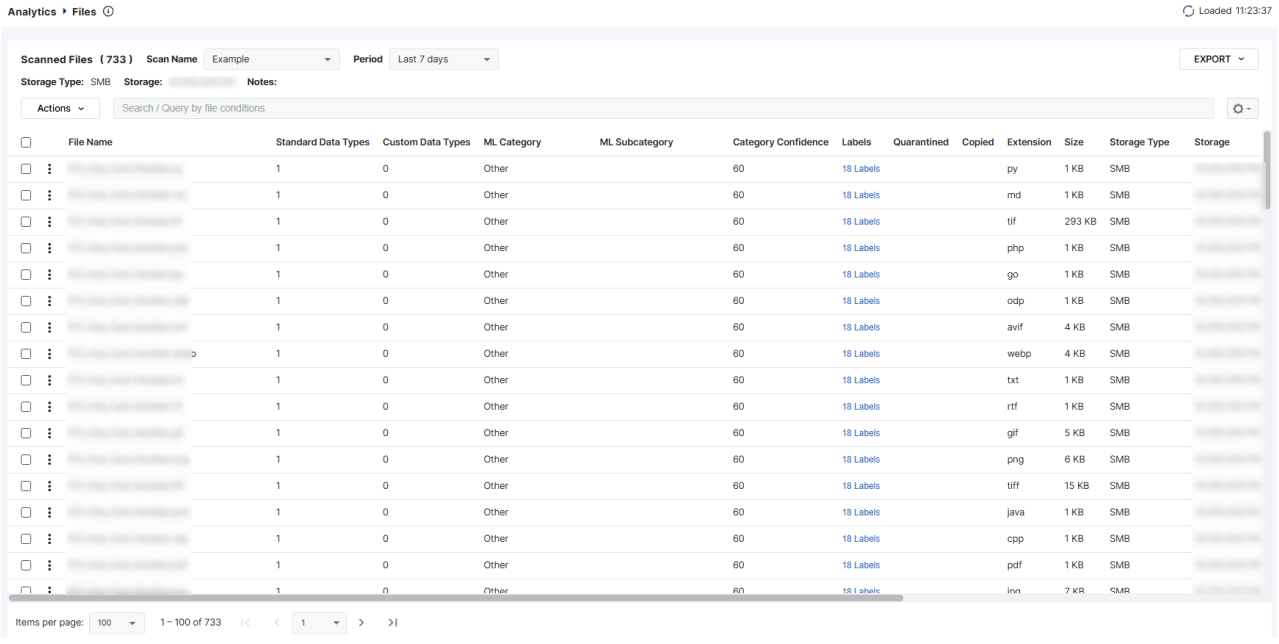
Analytics

FortiData 7.6.1 adds the *Analytics* menu with the following features:

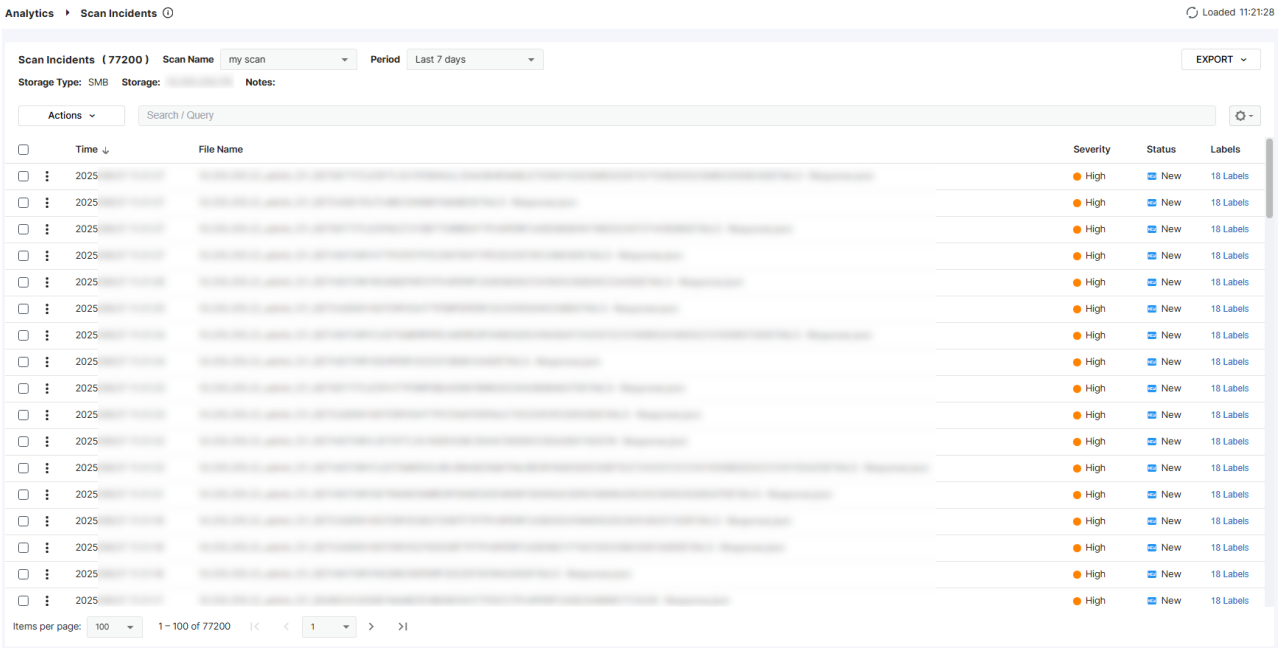
- A summary of scan results with interactive graphs and charts



- A list of scanned files with assigned labels



- Detailed log of each scan incidents



Discovery

The *Scans* and *Policies* pages are moved under the new *Discovery* menu with the following features and enhancements:

- Copying or quarantining files on page 8
- New scan file type support on page 8
- Configuring ML classification precision level on page 9

Copying or quarantining files

You can now configure FortiData to copy or move sensitive files to a specific directory for further investigation by creating a copy or quarantine profile and then applying the profile to your scan and enabling the copy/quarantine action in your policy.

See Profiles in the Administration Guide for more details.

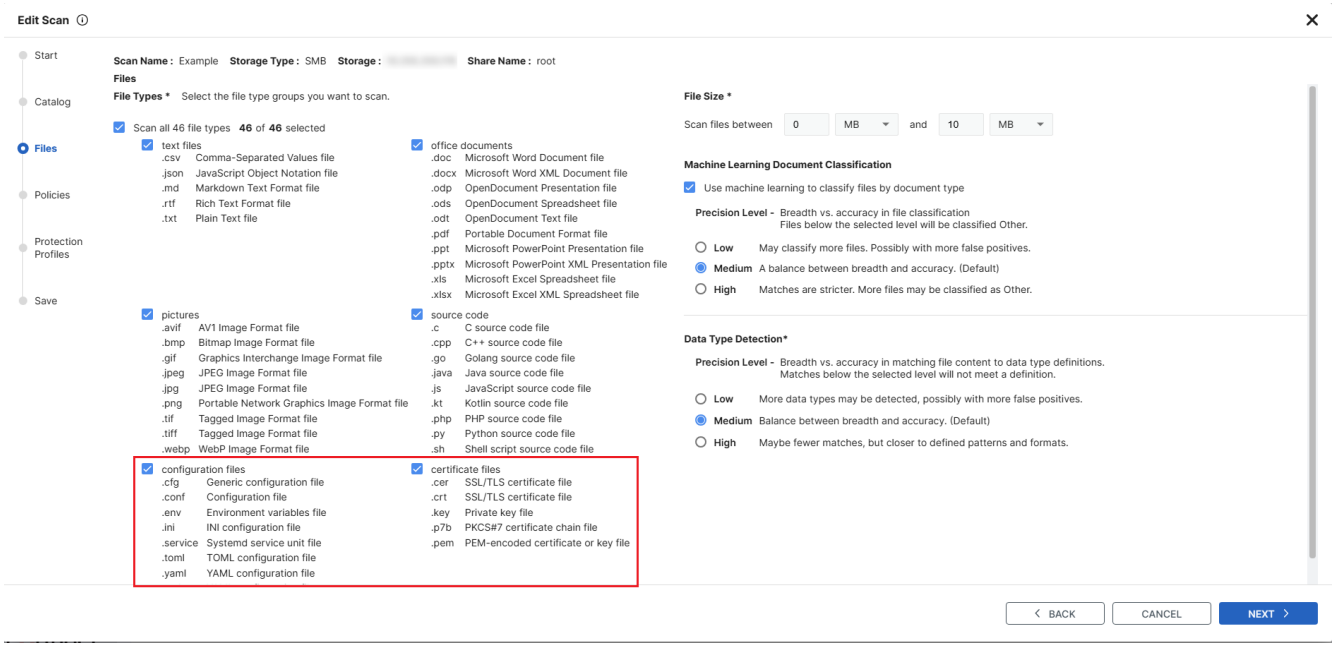
New scan file type support

FortiData 7.6.1 adds support for scanning the following file types:

- **Configuration files**—Includes the following file extensions: `.cfg`,`.conf`, `.env`, `.ini`, `.service`, `.toml`, `.yaml`.

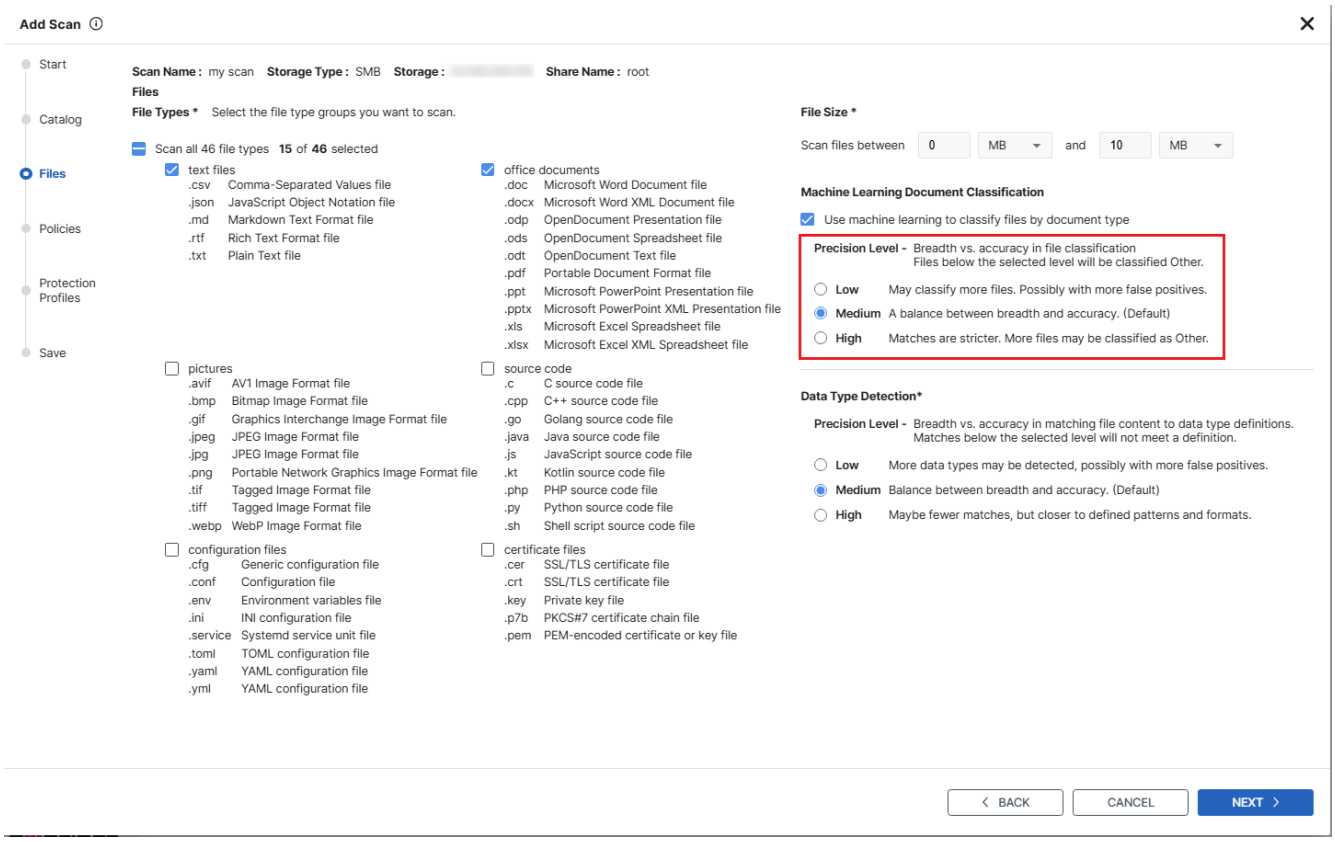
- **Certificate files**—Includes the following file extensions: `.cer`,`.crt`, `.key`, `.p7b`, `.pem`.

You can select the file types to scan when configuring a scan. See Scans in the Administration Guide for more details.



Configuring ML classification precision level

In FortiData 7.6.1, you can configure the precision level for machine learning classification when configuring a scan (see Scans).



Data Types

FortiData 7.6.1 includes the following enhancements to data types:

- EDM and IDM support on page 10
- Changes to machine learning (ML) data types on page 11

EDM and IDM support

FortiData 7.6.1 adds support for the following Data Types:

- **EDM (Exact Data Match)**—Identifies particular data values within an indexed data source that require safeguarding.
- **IDM (Indexed Document Matching)**—Creates unique fingerprints for your organization's crucial documents that hold sensitive information. This process involves analyzing the content of these documents and generating a checksum for each one.

Changes to machine learning (ML) data types

FortiData 7.6.1 includes the following enhancements and changes to ML Data Types:

New ML data types

Main type	Sub- types
Finance	Tax and Regulatory Documents
	Expense and Reimbursement Records
	Loan and Financing Agreements
	Audit and Assurance Documents
HR NEW	CV
	Employee Record
	Performance Review
	Recruitment
	Timesheet
Information Technology	Log
Legal NEW	Contracts and Agreements
	License Agreement
	NDA Form
	Patent
Source Code NEW	C#
	C Language
	Golang
	Java
	JavaScript
	Kotlin
	PHP
	Python
	Shell

Changed ML data types

- *Strategy and Research* is renamed *Financial Strategy and Research*
- *Legal and Compliance* is renamed *Compliance and Risk Management*
- *Research* is renamed *Clinical Studies*

Removed ML data types	Legal and Compliance
	Research
	Education
	Manufacture

Data Labels

FortiData 7.6.1 includes the following enhancements and changes to data labels:

- Machine learning (ML) labels are integrated into the *Data Classification* category under standard labels with the following additions and changes:

New ML labels	Tax and Regulatory Documents
	Expense and Reimbursement Records
	Loan and Financing Agreements
	Audit and Assurance Documents
	HR
	CV
	Employee Record
	Performance Review
	Recruitment
	Timesheet
	Log
	Legal
	Contracts and Agreements
	License Agreement
	NDA Form
	Patent
	Source Code
	C#
	C Language
	Golang

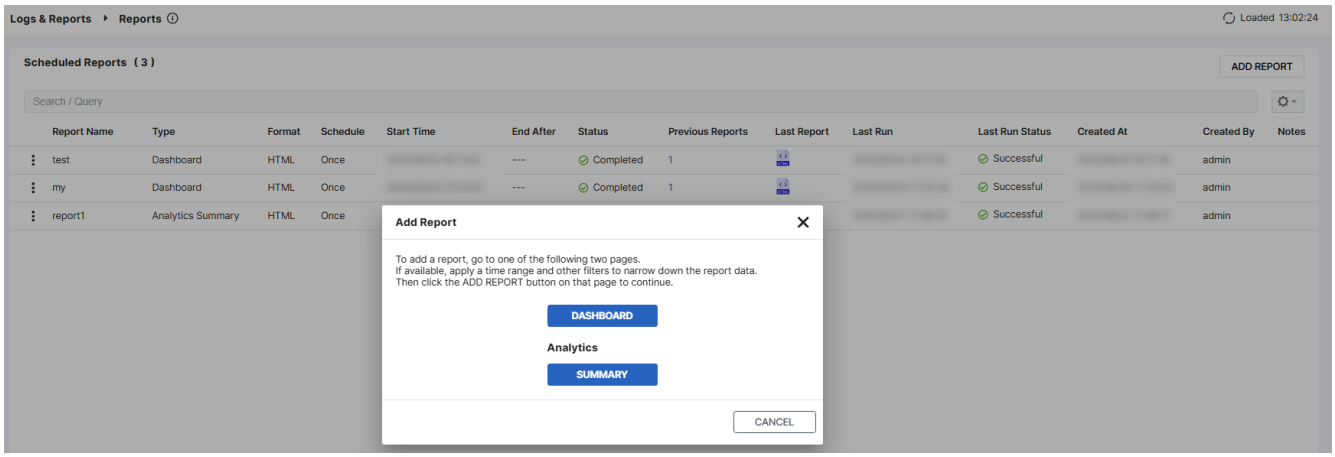
	Java
	JavaScript
	Kotlin
	PHP
	Python
	Shell
Changed ML labels	• *Strategy and Research* is renamed *Financial Strategy and Research* • *Legal and Compliance* is renamed *Compliance and Risk Management* • *Research* is renamed *Clinical Studies*
Removed ML labels	Legal and Compliance
	Research
	Education
	Manufacture

- Standard labels include the following additions and changes:

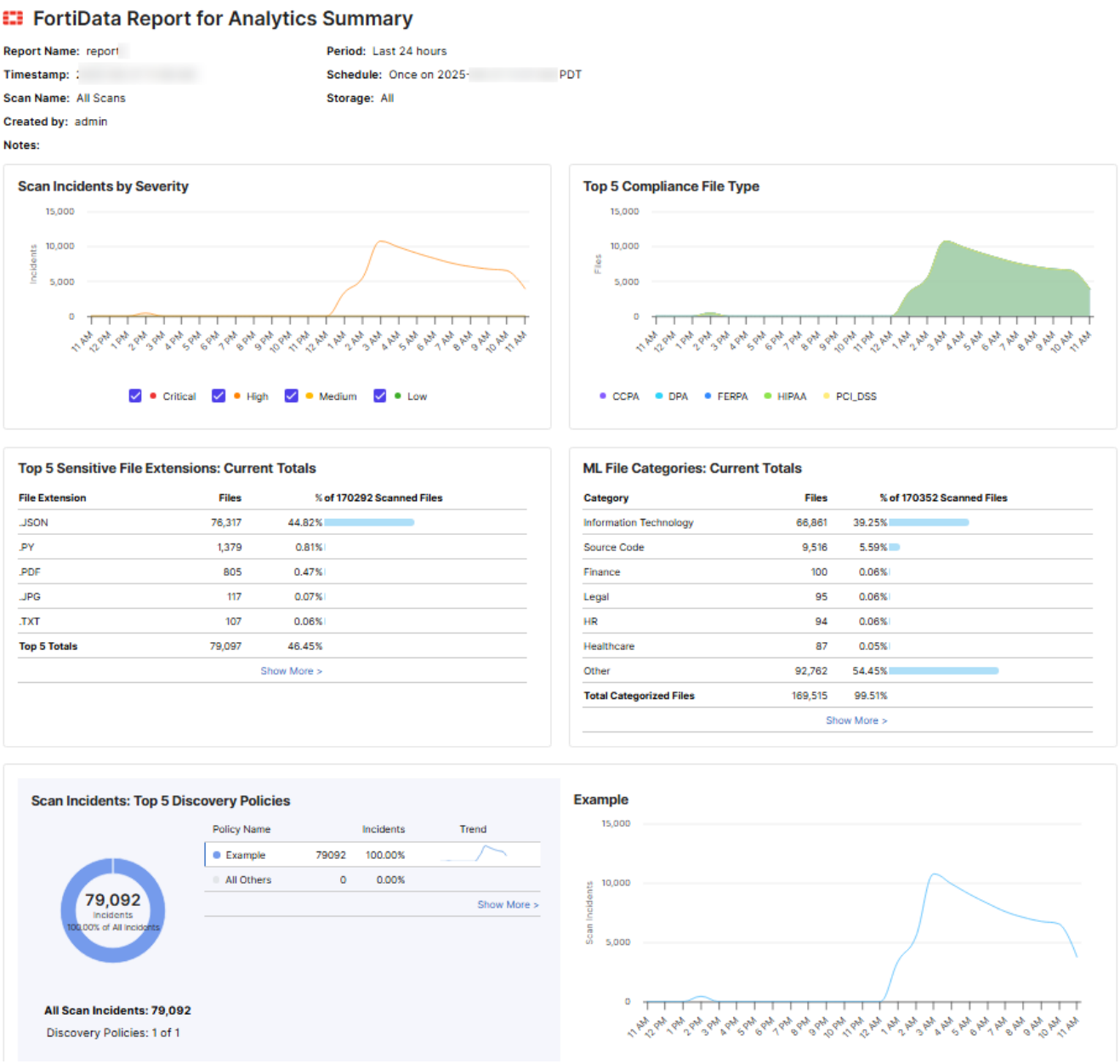
New standard label	HIPAA
Changed standard labels	• *Highly Confidential* is split into two labels: *Highly Confidential* and *Restricted*. • *Certificates and Credential* is integrated into *Credentials and Keys*
Removed standard labels	PHI
	PII

Logs & Reports

On the new *Logs & Reports* > *Reports* page, you can create one-time or recurring dashboard and analytics summary reports (in HTML or PDF format) for a specific time period. You can then download the report by clicking the file icon in the *Last Report* column.



Below is an example report:



System

This section includes information about system related new features:

- Integration with FortiGuard on page 16
- Adding static routes on page 16
- Certificate enhancements on page 16

Integration with FortiGuard

FortiData 7.6.1 uses the following FortiGuard packages which you can upgrade with the corresponding license:

- **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.

See FortiGuard in the Administration Guide for more details.

Adding static routes

FortiData 7.6.1 allows you to configure static routes to the system on the top of the existing default static route.

See Static Route in the Administration Guide for more details.

Certificate enhancements

FortiData 7.6.1 adds the following enhancements to certificates:

- You can now import a customized TLS certificate using an existing certificate .zip file.
- You can now import a custom CA certificate.

See Certificates in the Administration Guide for more details.

Cloud

FortiData 7.6.1 adds support for AWS. For detailed instructions about deploying FortiData on AWS, refer to the FortiData AWS Deployment Guide.

Product integration and support

The following table lists product integration and support information for FortiData 7.6.1 build 0103:

Type	Product and version
Fortinet products	• FortiGate 7.6.4 or later • FortiClient 7.4.4 or later
Web browsers	Google Chrome version 130 or later Other web browsers may work correctly, but Fortinet does not support them.
Virtualization environments	Fortinet recommends running the FortiData VM with at least 16 GB of memory. Refer to the FortiData Private Cloud Deployment Guides for detailed deployment instructions. **KVM** Linux kernel 2.6, 3.0, 3.1 or later **ESXi** 7.0 or later
Cloud platforms	AWS (Amazon Web Services) NEW

Upgrade information

You can also upgrade an existing FortiData deployment to 7.6.1. Refer to Product integration and support on page 17 for a list of supported platforms.

Downloading the firmware file

1. Go to https://support.fortinet.com.
2. Click *Login* and log in to the Fortinet Support website.
3. From the *Support > Downloads* menu, select *Firmware Download*.
4. In the *Select Product* dropdown menu, select *FortiData*.
5. On the *Download* tab, navigate to the FortiData firmware file for your FortiData VM platform in the *Image Folders/Files* section. `.out` files are for upgrade or downgrade. `.zip` and `.gz` files are for new deployments.
6. Click *HTTPS* to download the firmware that meets your needs.

Upgrading the FortiData

To upgrade your FortiData to 7.6.1:

1. In the Dashboard, click *Upgrade* in the *System Information* widget.
2. Click *Browse*.
3. Select the firmware file you just downloaded and click *Open*.
4. Click *Upgrade*.
   The system will reboot automatically after the upgrade is complete.

Resolved issues

The following issues have been fixed in FortiData 7.6.1. For inquiries about a particular bug, please contact Customer Service & Support.

Description	Bug ID
1106229	Drive License file is categorized as Manufacture.
1107597	Passports are incorrectly classified as Finance.
1117166	No log records for editing the users.
1118562	Import cert failed with error: A duplicate file name already exists.
1120944	The upgrade will fail if the disk space is less than 10 GB.
1122965	The firmware upgrade will proceed even if the file download fails.

Known issues

FortiData 7.6.1 includes the known issues listed in this section. For inquiries about a particular bug, please contact Customer Service & Support.

Bug ID	Description
1113782	Health problem can be recognized in CSV but not in Excel.
1121871	The power off signal is not effective for the KVM instance.
1122965	Enhancement to show single view of files categorized in multiple locations.
1167084	Cannot scan files in buckets of the directory type on AWS.
1167461	No support for configuring multiple AWS cloud trails.
1169031	No firmware version information in the report file.
1174560	Certificates inherited from 7.6.0 no longer have source value after the upgrade to 7.6.1.

www.fortinet.com

Copyright© 2025 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.