Release Notes

FortiData 7.6.2

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

December 24, 2025
FortiData 7.6.2 Release Notes
96-762-1228591-20251224

TABLE OF CONTENTS

Change log

Date	Change Description
2025-12-24	Initial release.

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 7.6.2, build 0133.

What's new

The following sections describe new features, enhancements, and changes in FortiData7.6.2:

Dashboard

- Support for Google Drive—You can now view data about Google Drive files in the dashboard if you have configured *Google Drive* storage in a scan.
- Support file metadata visualization and report for SharePoint and Google Drive files (such as Internal User, External User, Collaborator, and Share Link) for a unified file metadata structure.

Storages

The new *Storages* menu lists all storage locations you have configured in FortiData.

Incident Center

The new *Incident Center* menu replaces the *Analytics > Scan Incidents* tab in 7.6.1:

- The *Incident Center > Issues* tab lists scan-based incidents in an aggregated dynamic view (with a shorter list of events displayed).
- The *Incident Center > Integration Events* tab lists integration-based incidents, including scan incident for files uploaded by FortiClient.

Analytics

- The *Summary* tab has been renamed *Visualization*.
- The *Files* tab has been renamed *Data*.
- The *Analytics > Scan Incidents* tab has been integrated into the new *Incident Center* menu, with scan-based incidents now listed under *Incident Center > Issues* and integration-based incidents now listed under *Incident Center > Integration Events*.
- The new page *Analytics > Identities* tab lists the users and groups fetched from cloud storage systems.

Discovery

- **Support for Google Drive**—You can now select *Google Drive* as the storage type when configuring a scan.
- **Predefined discovery policies**—You can now select from or build your own policy from a list of predefined discovery policies without the need to create one from scratch.
- Support for applying file tags to remote cloud storage systems when labeling is enabled.
- Scanning all files (by selecting *ANY*) without the need to select specific file extensions when configuring a scan.
- Copying a policy without the need to start from scratch, which improves the policy creation efficiency. To do so, click the eclipsis in front of the policy name and select *Derive/Copy Policy*, depending on whether you are copying a built-in or personal policy. You will be then prompted to review the policy details, apply any changes, and save the new policy.
- A storage can be referenced by only one scan policy in 7.6.2.

Content Insight

- The *Data Types* and *Data Labels* menus have been consolidated into the new *Content Insight* menu with a new *Data Fingerprinting* sub-menu for IDM and EDM.
- New Data Classifiers tab which allows you to create or use predefined data classifiers based on mix of data identifiers.
- New machine learning ML document categories have been added.

Logs & Reports

- **Support for generating data inventory report in HTML and CSV format**—To add a data inventory report, go to *Logs & Reports* > *Reports* and click *Add Report* > *DATA INVENTORY REPORT*.
- Support file metadata report for SharePoint and Google Drive files (such as Internal User, External User, Collaborator, and Share Link) for a unified file metadata structure.

Integration

- Support for generating scan incident for files uploaded by FortiClient, which will be listed in the *Incident Center* > *Integration Events* tab.
- GUI support for label query logs (*Integration* > *Label Query* > *Label Query Logs*)

System

- Support for integration with external IdPs using the following protocols for user management (see *System > User Management > External IdPs*):
  - LDAP
  - Kerberos
  - SAML 2.0
- **Upgrading FortiData models and data type DB automatically or manually**—Go to the *System > FortiGuard* page and enable *Scheduled Updates* under *FortiData Model & Data Type Database Updates* to automatically update FortiData models and data type DB on a schedule. You can also manually do it using the *Update AI Classification, NLP and Data Type Definitions* button.
- **Encrypting backup files with a password in the *System > Backup & Restore > Backup* section**—The password is required to restore the system.
- **Exporting debug log file from GUI**—Enable the feature using the `diagnose gui upload enable` command and you will see the relevant options in the *System > Backup & Restore > Diagnose File Upload & Download* section.

Notifications

Use the new *Notifications* menu to configure email notifications, such as setting up SMTP servers and enabling email notification for data issues using built-in email templates.

Others

The data disk is encrypted using Linux Unified Key Setup (LUKS) in 7.6.2 for better security.

For systems upgraded from 7.6.0 or 7.6.1 to 7.6.2 to benefit from this feature, you must back up all configuration in the *System > Backup & Restore > Backup* section, manually enable disk encryption by running `execute force-format-logdisk`, and then restore the configuration in the *System > Backup & Restore > Restore* section.

Product integration and support

The following table lists product integration and support information for FortiData 7.6.2 build 0133:

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)

Upgrade information

You can also upgrade an existing FortiData deployment to 7.6.2. Refer to Product integration and support on page 9 for a list of supported platforms.

All scan data, including scan configuration and results, will be cleared after upgrade to 7.6.2 due to data compatibility issues.

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 7.6.2:

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.
5. Back up all configuration in the *System > Backup & Restore > Backup* section.
6. Manually enable disk encryption by running the following command: `execute force-format-logdisk`.
7. Restore the configuration that you backed up earlier in the *System > Backup & Restore > Restore* section.

Resolved issues

The following issues have been fixed in FortiData 7.6.2. For inquiries about a particular bug, please contact Customer Service & Support.

Description	Bug ID
1122965	Enhancement to show single view of files categorized in multiple locations.
1167461	No support for configuring multiple AWS cloud trails.
1174560	Certificates inherited from 7.6.0 no longer have source value after the upgrade to 7.6.1.
1169031	No firmware version information in the report file.
1213397	SMB file share scans fail intermittently.

Known issues

FortiData 7.6.2 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.
1167084	Cannot scan files in buckets of the directory type on AWS.
1234199	New classifiers created from the *Add Policy* dialog are not automatically selected.
1234702	Relevant dashboard and visualization report files are not included in notification emails.

www.fortinet.com

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.