OpenText Filr 24.4 Release Notes

December 2024

This release includes new features, enhancements, and defect fixes.

If you have suggestions for documentation improvements, click **Comment on this topic** at the bottom of the page in the HTML version of the documentation posted on the Filr Documentation page.

What's New

This section summarizes the new features and enhancements in this release.

What's New in 24.4.2

The following defects are fixed in Filr 24.4.2:

- The share operation in Net Folders stops working when a Standard License is applied after updating to Filr 24.4.1. The share dialogue does not open.
- A vulnerability is identified in Apache Tomcat running on the FILR 24.4 appliance. Upgrade Apache Tomcat to version 9.0.96 or higher to address the following two critical security issues:
  - CVE-2024-52317 - Incorrect object recycling leading to potential request/response mix-ups.
  - CVE-2024-52316 - An unchecked error condition vulnerability that could allow users to bypass authentication.
- The session hijack in filr application by manipulating the tokens when MFA is configured.

What's New in 24.4.1

The following defects are fixed in Filr 24.4.1:

- Host Header Validation for HTTP requests is now enabled by default in Filr. It was configurable in the earlier versions of Filr.
- Files are automatically downloaded when browsing Filr Files through Finder in macOS 15 when Application Whitelist/Blacklist mode was set to "No restrictions".
- Editing a text file in macOS 15 creates and syncs a temporary folder.

What's New in 24.4

Enhanced Features in Data Leak Prevention Policies

The Data Leak Prevention (DLP) feature enhances capabilities within the Filr application, focusing on Administrative control and user experience. The feature provides DLP capabilities across various Filr clients.

Ability to Create New DLP Policies

Filr administrators are provided with granular control over Data Leakage Prevention (DLP) within the Filr platform. It introduces a two-step process for creating and modifying DLP policies, allowing administrators to define specific restrictions and then configure the policy's behavior.

Alert the Users on the Data Sensitivity

Administrators can define the policy's behavior by choosing the Enforcement Type:

- **Restrict** (Default): Restricts the user from performing the file operation.
- **Warn**: A warning dialog is displayed when a user tries to perform the restricted file operation. If the user chooses to proceed, they are allowed to perform the operation.

For more information, see Data Leak Prevention in the OpenText Filr : Administrative UI Reference guide.

When a user attempts to share a sensitive file, based on the enforcement type that warns the user about the content sensitivity and then allows or restricts the user from performing the file operation configured in the policy. For more information, see What happens when a DLP policy is applied to a file? in the OpenText Filr 24.4 - Frequently Asked Questions.

Encrypting Communication between Filr Server and Search Appliance

 The communication between Filr Server and Search Appliance is encrypted. It aims to ensure that Filr is more secure, reliable, and resistant to potential threats. For more information, see Encrypting Communication between Filr Server and Search Appliance in the OpenText Filr 24.4: Maintenance Best Practices Guide.

NOTE:

- To establish communication encryption, ensure that both the Filr Server and Search Appliance version is 24.4.
- Ensure that communication encryption is enabled in the Filr Server and Search Appliance. If not, **My Files**, **Netfolders**, **Shared with me,** and **Public** will not be displayed on the **Home** page.

Enhancement to Self-registered External Users Settings

A new option called **Phone Number Provisioning** is introduced in the **External User Settings** tab under **Admin Console** > **System** > **Share and Comment Settings**. Based on the settings made by the administrator here, the **Mobile Number** field in the external self-registered user registration form can be made optional, mandatory, or hidden/disabled. For more information, see Managing Sharing, License Terms, and Comments in the OpenText Filr : Administrative UI Reference.

Move Operation is allowed in Shared With Me

In the Filr Web Client, users can move files and folders within the 'Shared with Me' area, respecting their existing access rights. This provides users with greater control over their shared files and folders, allowing them to organize and manage them more effectively.

Security Improvements

The following are the security improvements implemented in Filr 24.4:

- Filr appliances use strong SSH ciphers and MACs to ensure system security and protection against vulnerabilities.
- The Filr desktop client utilises recommended encryption techniques to enhance security and ensure compliance with security standards.
- The Filr Windows Client improves security by encrypting passwords used for authenticated proxies.

Platform Support and Support Matrix Changes

Version updates:

- iOS version is 18 and 17
- NAM 24.2
- Windows 11 24H2
- MS Office 2024
- MS SQL Server 2022 (Enterprise)
- Mariadb 11.4
- MySQL 8.4
- PostgreSQL 15.7 and 16.3

Tech updates:

- Collabora 24.04
- Angular 18
- Tomcat 11

Resolved Customer Issues

The following issues are fixed:

- When the Filr language is set to UK format, the Netfolders and Files are displayed in the US format.

- Notification is set to "Only newly added recipients" and when a file is shared with a new user, a notification is sent to the users with whom the files are already shared.

- On successful registration of an external user, a login screen is not displayed for the external user to log in.

- Filr application crashes and exceptions are recorded in the logs when generating an Orphaned Share Report.

- In the Windows Desktop client, the 'Make Available Offline' feature fails for 0 KB files.

- Filr Desktop client automatically downloads executable (.exe) files.

- Outdated Python packages are used in Filr Desktop clients.

- When changing the vaadmin password, an option to enter the old password is not provided.

Limitations

The following are the limitations found in Filr 24.4:

- There is no option to display share link passwords as clear text in the Windows desktop client for Filr.

- A file fails to download when shared through a password-protected share link, using the wget command.

Known Issues

The following are the known issues in Filr 24.4:

- In the Filr Windows Desktop client, when you double-click the .exe file which is online, it throws an incorrect function error. Also, it fails to copy and move the file when it is in the online state. To resolve this issue, in the context menu, select **Make Available Offline**.

- If a file shared through a protected share link has '%' in its name, you cannot download it using the share link.

- If a file is:

  1. Shared using a non-secured Share Link

  2. Sent as Email Via Filr

  You have to revoke/delete the existing non-secure share link and generate a new Share Link if you want to secure the resource.

- Using **Edit Online**, when you open a JPG file with a size greater than 20 MB, a blank page is displayed.

- The Spreadsheet Preview option limits the number of rows, columns, and sheets so that browsers cannot render some of the content of large spreadsheets. For more information, see Browsers cannot render some of the content of large spreadsheets. in the OpenText Filr 24.4: Maintenance Best Practices Guide.

- You cannot play the embedded video in a document when editing it online in iOS Client.

- Folders or files containing # or % in their name are not supported in the SharePoint netfolders.

Update Filr

This section provides you with the prerequisites for updating Filr 24.4.

Prerequisites

Updating Filr and Search Appliances: You must update the Filr appliance to version 24.4.2. Filr 24.4.2 is available as an online update to Filr 5.0 appliances or later. For more information, see Updating Filr through Online Update Channel.

Updating Content Editor Appliance: You must update the Content Editor appliance to version 24.4. For more information, see Applying Online Updates.

Updating PostgreSQL Appliance: You must update the PostgreSQL appliance to 24.4, see Applying Online Updates.

NOTE:

- When you update Filr 24.3 to Filr 24.4 in ALL IN ONE deployment, while you update PostgreSQL, ensure that 2x of database space is available for the upgrade to succeed.

Documentation

- Filr 24.4 Documentation (https://www.microfocus.com/documentation/filr/filr-24.4/)

Legal Notice

Copyright 2023-2024 Open Text

The only warranties for products and services of Open Text and its affiliates and licensors ("Open Text") are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.