

# OpenText Filr 24.2.1 Release Notes

May 2024

The Filr 24.2 release is an update for Filr 23.4. 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 the Filr 24.2 release and its patches.

- ◆ [“What's New in 24.2.1” on page 1](#)
- ◆ [“What's New in 24.2” on page 1](#)

### What's New in 24.2.1

The following defects are fixed in Filr 24.2.1:

- ◆ Filr does not correctly enforce the multi-directory inherited rights when the SMB users or groups have different permission sets between parent and subfolders.
- ◆ Filr cannot send email digest notifications when more than 1000 events are associated with the items that users follow.

### What's New in 24.2

- ◆ [“Password-Protected Share Links” on page 1](#)
- ◆ [“TLS 1.3 Protocol Support” on page 2](#)
- ◆ [“Platform Support” on page 2](#)

#### Password-Protected Share Links

Sharing files through Share Link is made more secure. The users can set the password for the share link. This feature is available only for users with an Advanced or Trial license.

This feature is supported on the Filr Web Client, Windows Desktop Client, and Filr Mobile Clients (Android and iOS). This feature is not supported on the Mac client.

## Share Link Settings

Filr Administrator can now set the share link settings. In the Administrator console, under **Share and Comment Settings > Share Link Settings**, you can see the following options:

- ◆ **Allow Share Links to be password-protected** - when this option is enabled, a user is presented with an option of password-protecting their Share Links at the time of creation or modification.
- ◆ **Apply Filr's Password Policy when setting passwords for Share Links** - when this option is enabled, users can set passwords for the share links adhering to Filr's Password Policy.

For more information, see [Share Link Settings](#)

Based on the Share Link Settings, the user can see the following options in the **Share Link** dialog.

- ◆ **Secure this link toggle button** - The user can secure the share link by turning on this toggle button.
- ◆ **Password** - The user can set a password for the share link adhering to Filr's Password Policy." Adhering to the password policy is required only if the Administrator has configured it.

The recipients must be provided with the share link and the password for the share link in order to view or download a shared file.

For more information, see [What is a Share Link?](#), [How to generate a Share Link or a Password-Protected Share Link?](#), and [How to modify the password for a password-protected share link?](#) in the [OpenText Filr 23.4 - Frequently Asked Questions](#). Also, see [Distributing a Link to a File](#) in the [OpenText Filr 23.4 Mobile App Quick Start Help](#).

## TLS 1.3 Protocol Support

Filr is updated to support TLSv 1.3 along with TLSv 1.2 network security for all Filr transactions. This improves security hardening.

---

**NOTE:** Filr Web Client by default supports TLSv1.3. The other Filr Clients (Desktop, Mobile, Outlook) continue to use TLSv1.2.

---

## Platform Support

For more information, see [Filr System Requirements](#) in the [OpenText Filr 23.4: Installation, Deployment, and Upgrade Guide](#).

## Resolved Customer Issues

The following are the customer issues fixed in Filr 24.2:

- ◆ When renaming a file in Filr, if the file name has an emoji, an invalid error message is displayed.
- ◆ Appserver logs are flooded with JITS and Full sync net folder messages, using excessive disk space.
- ◆ Filr Desktop Client displays 'Logout' in the system tray menu, even though the user is not logged in.
- ◆ Filr doesn't support Elliptic Curve Certificate (ECC).
- ◆ Filr Web and Desktop clients intermittently logout users with Filr 23.4 and Advanced Authentication.
- ◆ Fix for brute force attacks and CAPTCHA in Filr.

- ♦ jQuery -UI (1.13.1) vulnerability update.
- ♦ The Content Editor user 'cool' change password is not reflected in the appliance dashboard.

## Limitations

The following are the limitations found in Filr 24.2:

- ♦ You do not have the option to display share link passwords as clear text in Windows desktop Client for Filr.
- ♦ When you try downloading a file shared through a password-protected share link using the `wget` command, it fails.

## Known Issues

The following are the known issues in Filr 24.2:

- ♦ The application appears to trust the user-supplied Host header. It was found that the Host header is vulnerable to the user's input due to a lack of server-side input validation.

To avoid "Host Header Injection" the admin has to add `host.header.validate=true` in `/opt/novell/filr/apache-tomcat/webapps/ssf/WEB-INF/classes/config/ssf-ext.properties` and restart `filr.service`

- ♦ If a file shared through a protected share link has '%' in its file name, you will not be able to download the file using the share link.
- ♦ If a file is:
  1. Shared using a non-secured Share Link
  2. Sent as Email Via Filr

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

## Update Filr

This section provides you the prerequisites for updating Filr 24.2.1.

### Prerequisites

**Updating Filr and Search Appliances:** You must update the Filr appliance to version 24.2. Filr 24.2.1 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 24.2. For more information, see [Applying Online Updates](#).

**Updating PostgreSQL Appliance:** You must update the PostgreSQL appliance to 24.2, see [Applying Online Updates](#).

## Documentation

- ♦ [Filr 23.4 Documentation](#)

# 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.