OpenText Filr 23.3.1 Release Notes

October 2023

OpenText Filr allows you to easily access all your files and folders from your desktop, browser, or mobile device. In addition, you can promote collaboration around your files by sharing files and folders with others. For a detailed overview of Filr, see *OpenText Filr 23.3: Understanding How Filr Works*.

From your desktop, as described in the following guides:

- **Windows:** *Filr Desktop Application for Windows Guide*
- **Mac:** *Filr Desktop Application for Mac Guide*

Filr 23.3 accommodates three types of licenses:

- **Standard-Edition License:** Focused on modernizing the way users access their data with lightweight collaboration and protection capabilities.
- **Advanced-Edition License:** Provides advanced collaboration and protection capabilities, including multi-tenancy, custom branding, secure online content editor capabilities, and much more.
- **Power External User License:** Provides advanced collaboration and protection capabilities, including multitenancy, custom branding, secure online content editor capabilities, enables Multifactor Authentication (MFA) for external users, and much more.

For more comparison between the standard and advanced editions of Filr, see the OpenText Filr Product Page.

What's New in Filr

This section summarizes the new features and enhancements in Filr 23.3 release and its patches

What's New in Filr 23.3.1

macOS 14 Support

Filr Desktop Client for Mac now supports macOS 14.0 Sonoma.

What's New in Filr 23.3

This section summarizes the new features and enhancements in Filr 23.3 release.

Extended Collaboration

- Support for Active Directory multi-forest
- Support password-protected document online editing.

Advanced Security

- Node-based selective multi-factor authentication.
- Quality Improvements

Bug Fix List

The following is the list of bugs that are fixed in the Filr 23.3 release:

- When AAF is enabled, a user is unable to login into Filr Web Client.
- Sporadically the Desktop client logs the user out and after the logout, the login prompt appears. The user fails to log in and the User has to restart the Filr Web Client to log in again.
- Within the Filr Administration Console -> Desktop Application, when the Windows Filr client is deployed from another location, the “The auto-update URL is not valid" error is displayed.
- When AAF is enabled, an LDAP User is prompted to enter the password after the user is logged out of the Filr application.
- Provide configuration to suppress advanced authentication chain at Filr user login on a per Filr node basis.
- In Filr 5.0.0.2 Web Client, viewing a folder with a file and attempting to drag and drop it into a subfolder, initiates the upload which you cannot be canceled without clicking back to the root of my files or Netfolders.
- Filr is not disabling the accounts, even though “Disable account” is checked.

Update Filr

Pre-requisites

Updating Filr and Search Appliances: Filr 23.3.1 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 the version 23.3. For more information, see Applying Online Updates.

Updating PostgreSQL Appliance: You must update the PostgreSQL appliance to 23.3, see Applying Online Updates.

Upgrade Filr

The supported upgrade path is from Filr version 4.3.1.2 to Filr version 5.0. For more information, refer to the *Upgrading from Filr 4.3.1.2 to Filr 5.0* and Upgrade Issues in *OpenText Filr 23.3: Installation, Deployment, and Upgrade Guide*.

Installation Notes

Ensure that the OES servers are updated with the latest patches so that the Filr 5.0 server communicates with OES 2018 SP3 and OES 2023 servers.

For information about the system requirements to install Filr, see "Filr System Requirements" in the *OpenText Filr 23.3: Installation, Deployment, and Upgrade Guide*.

For information about installing Filr, see *OpenText Filr 23.3: Installation, Deployment, and Upgrade Guide*.

Documentation

- Filr 23.3 Documentation

What's New in Previous Releases

- "What's New in Filr 23.3" on page 1
- "What's New in Filr 23.2.1" on page 3
- "What's New in Filr 23.2" on page 3
- "What's New in Filr 5.0.0.2" on page 5
- "What's New in Filr 5.0.0.1" on page 6
- "What's New in Filr 5.0" on page 6

What's New in Filr 23.2.1

This section summarizes the new features and enhancements in Filr 23.2.1 patch release.

Security Updates

Bug fixes are provided to resolve the security vulnerabilities.

What's New in Filr 23.2

- "Filr Cluster Control" on page 3
- "HTML Rendering Improvements" on page 4
- "Upgrades to Content Editor" on page 4
- "Filr Web Client" on page 5

Filr Cluster Control

This feature lets you know the details of how many Filr nodes, Lucene nodes, and the Database appliance node are deployed in the Filr cluster. A new section called Filr Cluster on the 9443-Administrator Console page provides you with a set of icons representing the different nodes configured in the Filr cluster deployment. For more information, see Access Nodes in the Clustered Deployment in OpenText Filr 23.3: Administrative UI Reference.

HTML Rendering Improvements

In Filr 23.2 we have improved HTML rendering capabilities by updating IDOL KeyView Engine to 12.13

The following are some of the new HTML rendering capabilities which are now supported.

- Supports new file types for HTML rendering: ONE, MDB, TIFF, HEIC, HEIF, and EPUB.
- Renders a wide range of SmartArt diagrams in Microsoft Word (.docx) documents.
- Upgraded security updates for third-party packages.
- Provides better performance and latency for previewing files with the updated KeyView version.

Upgrades to Content Editor

In Content Editor appliance 23.2, Filr provides you with many new capabilities as the Collabora Online packages are updated to the latest.

- **Content Editor Cluster Deployment:** Enhancements are made to Content Editor Appliance configuration using HAProxy for load balancing to support the Content Editor version 23.2 and later. For more information, see the Load Balancing for CE 23.2 and above versions section in the OpenText Filr 23.3: Installation, Deployment, and Upgrade Guide.
- **Configuration of NetIQ Access Manager With Content Editor:** For the Content Editor version 23.2 and later, new options are added to the **HTML Rewriter Profile List** and the **URL Path List.** For more information, see Content Editor With NetIQ Access Manager For Online Edit Feature section in OpenText Filr 23.3: Installation, Deployment, and Upgrade Guide.
- **Features and Enhancements:**
  - For opening a document through Content Editor for an online update, you can set, change or delete a password. The feature is accessible through the document's Properties dialog.
  - Jumbo Spreadsheets with 16k Columns in Calc
  - Webapp support available for all types of documents
  - Faster Rotation of Bitmap Graphics
  - Export forms built with content controls to functional PDF forms: Users can create fillable forms using content controls, and export them to PDF. During export content controls are mapped to PDF form widgets, therefore the resulting PDF form will be fillable, too.
  - IP Address support for Online Edit - Now Content Editor appliance can be configured with IP addresses or Hostnames with different domains.
  - Playback of embedded video: With new support for embedded media files, it is now possible to click on an embedded video, in edit mode, and have the video played back in the browser. Standard video controls, including the ability to pause, seek, control the volume, and maximize the video to full screen. In addition, the user can move the placement of the video by using drag-and-drop interactions and resizing it.
  - Content Editor Cluster Deployment - We have not made any enhancements to Content Editor Appliance configuration using HAProxy.

NOTE: After upgrading to CE 23.2 to access Content Editor in cluster deployment we need to do configuration changes. For more information see, Load Balancing for CE 23.2 and above versions section in the OpenText Filr 23.3: Installation, Deployment, and Upgrade Guide

---

Filr Web Client

Filr Web Client now uses Angular 14 and ngRx 7, which provide improved performance, stability, and security. Filr Web Client also adopts UX Aspect 7.2, which enhances the user interface and user experience with new components. These updates will help you access and manage your files more efficiently and effectively with Filr Web Client.

What's New in Filr 5.0.0.2

This section summarizes the new features and enhancements in OpenText Filr 5.0.0.2 release.

Filr 5.0.0.2 has been modified for bug fixes. There are no new features or enhancements in this release.

Bug Fixes

- Unable to apply the maintenance patches to the Content Editor 2.0.0.1 appliance and Postgres 2.0.0.2 appliance, due to the vendor change issue. This issue is now resolved.
- The external Filr users were unable to change their password when using the Forgotten Password feature. This issue is now resolved.
- Filr 5.0.0.1 "Modified" Field reports Sync Timestamp and not original file timestamp in NetFolders.
- Installed patches were not listed post to the SLES update in the online update portal. This issue is now resolved.
- On editing and saving a PDF document using the Adobe Acrobat Reader DC in Filr, the file gets corrupted. This issue is now resolved.
- Filr appliance crashes due to file version cleanup. This issue is now resolved.
- PostgreSQL and Content Editor appliance Interactive SLES patches are skipped on automatic update.

Update Content Editor and PostgreSQL

PostgreSQL and Content Editor appliance Interactive patches are not installed on automatic update. You need to perform the online update procedure two times to update to the latest build.

To update CE 2.0 to CE 2.0.0.1 and PostgreSQL 2.0 /2.0.0.1 to PostgreSQL 2.0.0.2 through the Online Update channel, perform the following:

1. Ensure that the version of the Filr appliance is 5.0 or later.
2. Log in to the Filr Appliance Configuration Console (`https://appliance_ip_or_dns:9443`) as vaadmin.
3. Click **Online Update**.
4. In the **Patches** drop-down option, select **Needed Patches.**
5. Click **Update Now**.
6. Click **OK**.

All the Software Management Stack updates will be installed.

To install all the interactive patches, perform Step 3 through Step 6.

NOTE: Once the CE appliance is updated to 2.0.0.1 and the PostgreSQL appliance is updated to 2.0.0.2, for any further patches, performing the update procedure twice is not required.

What's New in Filr 5.0.0.1

This section summarizes the new features and enhancements in Filr 5.0.0.1 release.

Enhancements

WebDAV Support: WebDAV Support with updated Milton jars.

Desktop Platforms (for the Desktop Application):

Table 1 *Desktop Platforms (Desktop Application)*

Platform	Versions
◆ Mac	◆ macOS 13

PostgreSQL DB Migration

Filr 5.0 Postgres appliance migration from 10.x to 14.x fails. This issue is resolved.

Before applying the PostgreSQL 2.0.0.1 patch,

- Stop all services accessing the database and back up your disk
- Ensure that the vastorage has more than 50% free space. For more information, see (https://www.microfocus.com/documentation/postgresql/postgresql-2.0/postgresql-admin/productupgrade.html)

The PostgresSQL upgrade process might take some time to complete. The duration of the upgrade varies based on the size of the database. When the upgrade is in progress, The `pg_upgrade` logs are recorded. To view the logs, perform the following steps:

1. Login to **Port 9443 Appliance > System Services** and enable SSH.
2. In the SSH terminal of the Postgres server, navigate to `/vastorage/postgres/upgrade/pg_upgrade_internal.log.` to view the `pg_upgrade` logs.

On completion of the upgrade, the logs are automatically deleted.

Fixes for customer-reported bugs

- When a file is dragged and dropped into the "My Files" folder of Filr Web Console, the file list does not get refreshed.

What's New in Filr 5.0

This section summarizes the new features and enhancements in Filr 5.0 release.

- "Changes from Filr 4.x to Filr 5.0" on page 7
- "Data Leak Prevention" on page 7
- "File Versioning" on page 8

- “Multifactor Authentication for External Users” on page 9
- “Deprecations” on page 11

Changes from Filr 4.x to Filr 5.0

Table 2 *Version Changes*

Components	Filr Appliance 4.0	Filr Appliance 5.0
Base Appliance	SLES 12 SP3	SLES 15 SP4
	OpenJDK 1.8	OpenJDK 11
	PostgreSQL	PostgreSQL version 14.3

For more information, see Filr System Requirements in the OpenText Filr 23.3: Installation, Deployment, and Upgrade Guide.

Data Leak Prevention

Filr 5.0 provides the Data Leak Prevention feature that helps to have fine-grained control over important organizational documents and helps you adhere to various global data protection policies while still providing remote access to external partners and users working remotely.

- An option called **Data Leak Prevention** is available on the Administrator Console. An administrator is allowed to enable DLP and assign a DLP policy to the netfolders of an organization and manage them.
- The **Workspace Moderators** option in DLP, allows the Filr administrator to delegate the file sensitivity management privileges to users who have access to a workspace. These users are called moderators. The moderators and an administrator can apply policy to files and manage them in the workspace.
- A system-generated policy called “Confidential” is available and the “Share Externally” file operation is mapped to this policy. When this policy is applied to a file, sharing a file with any external user will be restricted (Share with external users, Share public, and Share with file links).

NOTE: This feature is available for the Advanced Edition license.

DLP Workflow

On the Administrator Console, perform the following steps to Enable DLP for Netfolders:

1. Go to the **Manage Workspace** tab.
2. Select the netfolder from the list of **Workspace** dropdown list.
3. Turn on the **Enable DLP for this workspace** toggle.

   An administrator can apply a DLP policy to the netfolder. This is optional.
4. Select the DLP policy from the **Policy** dropdown list.

NOTE:

- When the DLP is enabled and the policy is applied to a workspace, the policy is applied to all the files in the workspace. A moderator is not allowed to remove the policy applied to a file.
- When the DLP is enabled and the policy is not applied to a workspace, A moderator is allowed to apply or remove the policy to files.

An administrator can delegate users with the net folder DLP moderation rights. This allows these users to classify the individual files based on the content sensitivity as required. This is optional.

5 Turn on the **Enable Workspace Moderators** toggle.

6 Click **Add OR Remove Moderators**. The **Add or Remove Moderators** dialog box is displayed.

7 Enter the usernames to be added as moderators for the workspace. Type the first three characters of a username, based on the data entered, the system will search and lists the users having access to the workspace. A netfolder can have only ten moderators.

8 Click **Save**.

For more details see Data Leak Prevention in the OpenText Filr 23.3: Administrative UI Reference and OpenText Filr 23.3 - Frequently Asked Questions (FAQ).

File Versioning

Filr 5.0 provides the File Versioning feature that allows users to manage multiple versions of files. This feature is supported for Personal Storage (My Files).

An administrator can configure File Versioning from the administrator console:

- Enable or disable file versioning.
- Enable or disable file version aging.
- Set the number of days (default 90 days) for file aging. Any files that exceed the set days, except for the current version of the file, will be deleted automatically, and the deleted versions cannot be retrieved.
- Max 10 versions per file can be maintained in personal storage.

When the file versioning is enabled, users can do the following from the Web Client:

- List and maintain multiple versions of a file, up to 10 versions per file.
- When a file with the same name is uploaded to Filr, the user will be prompted to "Create a new version", instead of "Overwriting" the existing file.
- Using the Filr Web Client users can delete, download and promote an existing version of a file.
- In Share With Me area:
  - Users with the 'VIEWER' rights can only download file versions.
  - Users with the 'EDITOR' rights can download and promote file versions.
  - Users with the 'CONTRIBUTOR' rights can download, promote, and delete file versions.

NOTE: •This feature is available for the Advanced Edition license.

- When this feature is enabled, it is recommended to expand the vastorage/vashare size at least twice the amount of the current disk space used (a maximum of 10 times). For more information, see Expanding Storage. Manage the usage of disk space, by making use of data quota. For more information, see Managing and Restricting Filr Based Storage.

For more information, see File Versioning in the OpenText Filr 23.3: Administrative UI Reference and OpenText Filr 23.3 - Frequently Asked Questions (FAQ).

Multifactor Authentication for External Users

Filr 5.0 provides you with the ability to enable Multifactor Authentication (MFA) for external users. The self-registration page for external users now contains a Mobile Number field. Users can provide their mobile number, if they wish to enable SMS OTP for 2FA. For more information see What is a Self Registration page? in the OpenText Filr 23.3 - Frequently Asked Questions (FAQ).

Power External User License: Provides advanced collaboration and protection capabilities, including multi-tenancy, custom branding, secure online content editor capabilities, enables MFA for external users, and much more.

The **External user** checkbox is available at **Administrator Console > System > NetIQ Advanced Authentication** for the Power External User license.

Configuring OAuth2 Event in Advanced Authentication Server Appliance for Power External Users

External users are allowed to connect to Filr through the Multi Factor Authentication. A new SQL repository is configured with the table that provides a power external user's details like email address and phone number.

To create SQL repository,

1. Log into the Advanced Authentication Administrative Portal as follows:

   `https://advanced_authentication_dns_name_or_IP_Address/admin/repositories`

2. Enter the following details to add a new SQL repository:

Table 3 *AAF Repository page*

Field, Option, or Button	Information and/or Action
◆ **Name**	◆ Enter the name of the repository. For example, "External DB"
◆ **Database Type**	◆ For small deployment, select Postgresql. For large deployment, select the configured database type.
◆ **DB host**	◆ Enter the IP address of the database. For small deployment, enter the IP address of the Filr appliance.
◆ **DB name**	◆ Enter the name of the database.
◆ **DB user**	◆ Enter the name of the database user.
◆ **Password**	◆ Enter the database password.
◆ **Table or view name**	◆ For PostgreSQL, enter the table name as ss_principals. ◆ For MySQL and MSSQL enter the table name as SS_Principals.
◆ **User's id column**	◆ Enter "id".
◆ **User's id type**	◆ Select "Integer".

Field, Option, or Button	Information and/or Action
◆ **User's name column**	◆ For PostgreSQL, enter "emailaddress" ◆ For MySQL and MSSQL enter "emailAddress".
◆ **User's name type column**	◆ Select "String".
◆ **User's phone column**	◆ Enter "phone".
◆ **User's email column**	◆ For PostgreSQL, enter "emailaddress" ◆ For MySQL and MSSQL enter "emailAddress".

3 In the Advanced Authentication Administrative Portal, go to:

`https://advanced_authentication_dns_name_or_IP_Address/admin/chains`

4 Configure an authentication method for Advanced Authentication.

NOTE: The following methods have been tested with Filr:

- SMS OTP

  The administrator must choose another authentication method along with SMS OTP. Since the Mobile Number field is optional in the Self-registration form, the external users who have not entered the mobile number or have entered an incorrect mobile number will not be able to receive the SMS OTP and may not be able to log in to Filr.

- Email OTP

  Other authentication methods that NetIQ Advanced Authentication with OAuth2 event supports would also work, but they have not been explicitly tested. All the users must be registered at Advanced Authentication Self-Service Portal with the specific method else the user is not allowed to log in to the Filr application.

5 Create an authentication chain that is a combination of all the authentication methods that users must pass for successful authentication.

6 Configure OAuth2 type event.

6a Specify a name for the event.

6b Enable the event by changing **Is enabled** to **ON**.

6c Select the **OAuth2** event type. The client ID and client secret are generated automatically.

6d Note down the client ID and client secret values. You must specify these values in the **NetIQ Advanced Authentication** page of the Filr Administration Console (**Port 8443 Filr Admin Console > System > NetIQ Advanced Authentication**). You can copy the values and paste them in the Filr admin Console.

6e Select the chains that you want to assign to the event.

6f In the **Redirect URIs** option, specify the following redirect URIs for redirection to the Filr page after successful authentication:

- The URI of the Filr web page
- The URI of the Filr client application

You can copy the URIs from the **Redirection URIs** option on the **NetIQ Advanced Authentication** page of the Filr Administration Console (**Port 8443 Filr Admin Console > System > NetIQ Advanced Authentication**) and paste them here.

6g Click **Save**.

For more information, see Using Multi-Factor Advanced Authentication with Filr in the OpenText Filr 23.3: Maintenance Best Practices Guide.

Deprecations

The following are the deprecations in Filr 5.0.

NetWare is not supported as a server type for Net Folder Servers

Beginning with Filr 5.0, NetWare is not supported as a server type for Net Folder Servers. However, it is supported on the existing Net Folder Servers, and you are allowed to change the server type of such servers to other supported server types if required.

Ganglia is not supported

Beginning with Filr 5.0, Ganglia is not supported.

KeyShield

Beginning with Filr 5.0, KeyShield is not supported.

Mobile Devices

The Filr app is not supported on the Windows (version 8.0 and 8.1) mobile devices.

Legal Notice