

Filr 5.0 Release Notes

March 2023

Micro Focus Filr allows you to easily access all your files and folders from your desktop, browser, or a 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 the [Filr: Understanding How Filr Works](#).

From your desktop, as described in the following guides:

- ♦ **Linux:** *Filr Desktop Application for Linux Guide* (<https://www.microfocus.com/documentation/filr/filr-5/filr-desktop-linux/bookinfo.html>)
- ♦ **Mac:** *Filr Desktop Application for Mac Guide* (<https://www.microfocus.com/documentation/filr/filr-5/filr-desktop-mac/bookinfo.html>)
- ♦ **Windows:** *Filr Desktop Application for Windows Guide* (<https://www.microfocus.com/documentation/filr/filr-5/filr-desktop/bookinfo.html>)

Filr 5.0 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 multitenancy, 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 [Micro Focus Filr Product Page](#).

What's New in Filr

This section summarizes the new features and enhancements in Micro Focus Filr 5.0 release and its patches

- ♦ ["What's New in Filr 5.0.0.2" on page 2](#)
- ♦ ["What's New in Filr 5.0.0.1" on page 2](#)
- ♦ ["What's New in Filr 5.0" on page 3](#)

What's New in Filr 5.0.0.2

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

- ♦ ["Changes from Filr 4.x to Filr 5.0" on page 4](#)
- ♦ ["Data Leak Prevention" on page 4](#)
- ♦ ["File Versioning" on page 5](#)
- ♦ ["Multifactor Authentication for External Users" on page 6](#)

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 [Filr 5.0: 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 [Filtr 5.0: Administrative UI Reference](#) and [Micro Focus Filr - Frequently Asked Questions \(FAQ\)](#).

File Versioning

Filtr 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 [Filtr 5.0: Administrative UI Reference](#) and [Micro Focus Filr - 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 [Micro Focus Filr - 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".
◆ User's name column	◆ For PostgreSQL, enter "emailaddress" ◆ For MySQL and MSSQL enter "emailAddress".

Field, Option, or Button	Information and/or Action
♦ 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 [Filr 5.0: Maintenance Best Practices Guide](#).

Upgrade Filr

The supported path for upgrade is Filr 4.3.1.2 to Filr 5.0. For more information, refer to the [Upgrading from Filr 4.3.1.2 to Filr 5.0](#) and [Upgrade Issues](#) in the *Filr 5.0: Installation, Deployment, and Upgrade Guide*.

Installation Notes

To enable the Filr 5.0 server to communicate with OES 2018 SP3 and OES 2015 SP1 servers, you must ensure that the OES servers are updated with the latest patches.

For information about the system requirements to install Filr, see “[Filr System Requirements](#)” in the *Filr 5.0: Installation, Deployment, and Upgrade Guide*.

For information about installing Filr, see the *Filr 5.0: Installation, Deployment, and Upgrade Guide*.

Known Issues

- ♦ Expanding /var partition or clubbing expansion of /vastorage along with /var fails. Hence, ensure only /vastorage partition is expanded when needed.
- ♦ When a file with versions is moved across the folders, for example, from MyFiles to Net Folders or Local File System (in the case of desktop users), the versions are not retained. This is expected behavior. This does not happen when a file is moved to a file system that does not support versioning.
- ♦ The Filr Host entries are not removed or cleared from the loolwsd.xml in Content Editor 2.0.
- ♦ WebDAV access to Filr from Mac is read only.

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, is not KeyShield is not supported.

Mobile Devices

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

Documentation

- ♦ [Filr 5.0 Documentation \(https://www.microfocus.com/documentation/filr/filr-5/\)](https://www.microfocus.com/documentation/filr/filr-5/)

Legal Notice

Copyright © 2023 Micro Focus or one of its affiliates.

The only warranties for products and services of Micro Focus and its affiliates and licensors (“Micro Focus”) 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. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

