

Filr 3.4

Maintenance Best Practice Guide

September 2018

Legal Notice

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see <https://www.microfocus.com/about/legal/>.

Copyright © 2018 Micro Focus company. All Rights Reserved.

Contents

About This Guide	9
1 Access to Filr—Maintenance Tasks	11
Desktop Application Access	11
Guest User (Public) Access	11
Local User (non-LDAP) Access	11
Making Public URLs Searchable	11
Mobile Device App Access	11
Web Browser Access	11
2 Adding a Filr Appliance to an Existing Deployment	13
Prerequisites	13
Adding Filr Appliances to an Existing Deployment	13
3 Administrative Access Maintenance	15
Adding or Removing Administrative Rights for Users and Groups	15
Administrative Maintenance—Port 8443 Admins	15
About Port 8443 Administrators	15
Modifying Port 8443 Administrators	15
Simplifying Management through Administrative Groups	16
4 Branding and Changing the User Interface	17
Branding Desktop Apps (Advanced-Edition License Only)	17
Branding Mobile Apps (Advanced-Edition License Only)	19
Android UI Branding	19
iOS UI Branding	25
Windows Phone Branding	33
Branding the Web User Interface	34
Changing the Title of the People Page	35
5 Desktop Application Maintenance	37
Client Management Software and the Filr Desktop Applications	37
Customizing the Installation for the Filr Desktop Application	37
Controlling Windows Explorer Restart	40
Controlling File Downloads by the Filr Desktop Applications	40
Why File-Download Control Is Important	41
How File-Download Control Works	41
Always Blacklist Macintosh Antivirus Applications	41
Managing File Downloading	41
Desktop Application Installation Files—Location	42
Desktop Application Software Management	42
Understanding Missing Dependencies Related to Updating the Filr Desktop Application by Using the MSI File	43
Updating the Filr Desktop Application on the Filr Appliance	43
Enabling Desktop Access for Users	44

Synchronization-Traffic Management	44
Distributing Filr Desktop Application Traffic Separately from Other Applications	44
Distributing Filr Desktop Traffic in Conjunction with Other Applications	45
Load Balancer and Reverse Proxy Server Configuration	45
6 Helping Micro Focus Improve Filr	47
Organizational Privacy Is Protected	47
How Micro Focus Collects Product Improvement Data	47
How Micro Focus Receives Product Improvement Data	48
Submitting Your Product Improvement Ideas	48
7 Hosting Desktop Application Installation Files on a Separate Server	49
8 KeyShield Integration with Filr	51
Prerequisites	51
(Conditional) Allowing the Authorization Connectors to Access the API Key	51
Configuring Filr for KeyShield SSO Support	51
KeyShield Attribute Alias Support	52
A Filr Example	52
Configuring Attribute Alias Support	53
Configuring Two-Factor Authentication	53
Downloading and Installing the KeyShield SSO SSL Certificate	54
Testing the KeyShield SSO Configuration	54
9 Using Multi-Factor Advanced Authentication with Filr	55
Prerequisites for Using Advanced Authentication with Filr	55
Configuring OAuth2 Event in Advanced Authentication Server Appliance	56
10 Language Settings	59
About the Filr Site Default Language	59
Changing the Language on the Login Page	59
11 Migrating the Filr's MySQL Database to Microsoft SQL	61
Prerequisites	61
Configuring the Existing Microsoft SQL Database Server	62
Connecting to the MySQL Database Server	62
Connecting to the Microsoft SQL Server	63
Customizing Data Types	63
Migrating the Database Schema	64
Migrating Data	65
Running Post-Migration Scripts	65
Post-Migration Steps	66
Modifying Liquibase Tables	67
12 Mobile Device Management	69
Key-Value Pairs	69
Configuring ZMM to Manage the Filr App	71
Configuring MobileIron to Manage the Filr App	71

MobileIron Environment Support	71
Device-Specific Support Information	71
Adding the Filr App to MobileIron	72
Pre-Populating Fields for Filr Login	73
Configuring Data Loss Prevention Policies	75
Distributing the Filr App to Devices	76
Preventing Frequent Prompts for a Passcode	76
Managing Mobile Devices with Filr	76
13 Monitoring	77
Enabling Debug Logging	77
Enabling Debug Logging for Filr	77
Enabling Debug Logging for FAMT	78
Configuring Debug Logging for SMB Communications	78
Monitoring with Ganglia	79
Ganglia Monitoring Tips	80
Viewing Metrics for an Individual Node	80
Viewing Metrics for Multiple (Clustered) Filr Nodes	80
Filr Monitoring Metrics	81
Configuring Ganglia to Monitor MySQL or MariaDB Database	83
Monitoring File Meta-Data Synchronization in a Filr Cluster	84
Monitoring the Indexing Process	85
Monitoring User Access, including the Guest User	86
14 MySQL—Backup and Restore from the Command Prompt	87
Backing Up MySQL from the Command Line	87
Restoring MySQL from a Backup File	87
15 Net Folder Maintenance	89
Manually Synchronizing a Net Folder Server	89
Manually Synchronizing a Net Folder	89
Viewing the Synchronization Status of a Net Folder	89
16 Notification (Email) Customization	91
About Filr's Email Templates	91
Template Tips and Documentation	92
Modifying the Email Template Files	92
Email Template Customization—A Video Walkthrough	92
17 Search Index Maintenance	93
Optimizing the Lucene Index to Improve Search Performance	93
Optimizing a Single Search Index	93
Optimizing the Search Index with Multiple Index Servers	94
Maintaining Your High Availability Lucene Index	95
Rebuilding the Lucene Index	98
Rebuilding a Single Search Index	98
Rebuilding the Search Index with Multiple Index Servers	99
18 Security	101
Antivirus	101

Audit Trail	102
Backup and Restore	102
Brute-Force Attacks and CAPTCHA	102
Certificate Maintenance	102
Using the Digital Certificate Tool	103
Using an Existing Certificate and Key Pair	104
Activating the Certificate	104
Managing Certificates	105
Comments and Security	105
Database Communication Encryption	105
Configuring the Database Settings	106
Configuring the Filr Server Settings	107
Desktop Application Security	107
DMZ Setup for Filr	107
Downloads through Filr—Disabling	109
Disabling Downloads for All Users	109
Disabling or Enabling Downloads for Individual Users	110
Disabling or Enabling Downloads for Individual Groups	111
Email Transfer Security	112
Encryption	112
File Server Security	112
Filr Component Security	112
Filr Data Security	113
Understanding Administrator Access to Filr Data	113
Limiting Physical Access to Filr Servers	113
Protecting the Filr Database	113
Filr's Rights Model	113
Filr Security Defaults	114
Filr Site Security	114
Configuring a Proxy Server	114
Setting the Filr Administrator Password	114
XSS—Filr Is Secure	115
LDAP Synchronization Security	115
Exporting a Root Certificate	116
Importing the Root Certificate into the Java Keystore	117
Mobile Device Data Security	117
App Security	117
File Security	118
NESSUS Scans	118
Proxy User Security	118
Security Scan Risk Reports	118
Sharing and Security	119
SSH Access for the Root User	119
Universal Passwords (eDirectory) Security	120
Users and Security	120
WebDAV Support	120
Planning Your WebDAV Implementation	120
Disabling WebDAV for Filr Site	122
Editing Files with Edit-in-Place Functionality	122
Mapping a Filr Folder as a WebDAV Folder	123
Configuring Windows to Use a Self-Signed Certificate with Filr	123
Allowing Basic Authentication over an HTTP Connection on Windows 7	125
XSS Security Filter	125

19 Storage Management	127
Backing Up Filr Data	127
Locating Filr Data to Back Up	127
Scheduling and Performing Backups	128
Restoring Filr Data from Backup	128
Manually Restoring Individual Files and Folders	128
Changing the CIFS /vashare Mount Point Login Credentials	129
Configuring Home Folders for Display in the My Files Area	129
Configuring Home Folders	129
Editing Home Folders for Individual Users	130
Understanding How Home Folders Relates to Personal Storage	131
Disk Usage Checks	131
Personal Storage (My Files) Management	131
Navigating the Workspace Tree	132
Managing Workspace Disk Space Usage	132
Restoring Files and Folders from the Trash	132
Managing User Data Quotas	133
Permanently Deleting Files from the Trash	140
20 Troubleshooting	141
Migration Fails to Modify the Owner Details and ACLs	141
Configuring Filr Server Fails When Using NetApp ONTAP version 8.3.2 As a CIFS Vashare	141
eDirectory Users Can Log In But Cannot Upload Files	141
Email Notification URLs Are Not Working	142
NetApp Net Folder Server Test Connection Fails	142
Online Update Service Registration Fails With an Error Message	142
Previously Available Files and Folders Disappear	142
Unable to Connect to the Filr Site (HTTP 500 Error)	143
Using VACONFIG to Modify Network Information	143
Unable to Access Data on a DFS Junction In an OES Server Cluster Environment	143
21 User and Group Maintenance	145
Adding and Creating Filr Users and Groups	145
Creating Groups of Users	145
Creating Static Groups	145
Creating Dynamic Groups	146
Deleting Filr Users	146
Consider Disabling User Accounts Instead	146
Deleting User Objects and Workspaces	147
Deleting an LDAP User	149
Recovering User Workspaces from the Trash	149
Disabling Filr User Accounts	149
Disabling or Re-enabling a Local User Account	150
Disabling an LDAP User Account	150
Renaming a Filr User	150
Renaming a Filr User from LDAP	150
Renaming a Local Filr User	150
User Maintenance Task Links	150
With Multiple Users Selected	151
With a Single User Selected	151
Group Maintenance Task Links	151
With Multiple Groups Selected	151
With a Single Group Selected	152

A A Simulation and Some Best Practice Sizing Recommendations	153
Sample Filr Deployment Description	153
Filr Appliances	154
Number of Filr Appliances	154
Configuring the Dedicated Filr Appliance	154
Use the Dedicated Filr Appliance for Upgrade Testing	154
Separate Filr REST and Web Requests at L4 Switch	154
Filr CPUs	154
Index Maintenance—Just Let It Run	154
Synchronization Best Practices	155
Synchronization Priorities	155
Never Overlap Synchronizations	155
Limit Synchronization Size	155
Utilize Just-in-Time Synchronization Rather than Scheduled Synchronizations	155
JITS Settings	155
If a Manual Net Folder Synchronization Is Required	156
Anticipating Disk-Space Growth	156
The /var Mount Point	157
Monitoring Commands and Tips	157
SQL Database Monitoring Commands	157
Monitoring Net Folder Synchronization	157
Monitoring the Impact of Your Tuning Changes to the Overall System	158
Ganglia Graphs	159

About This Guide

- ◆ Chapter 1, “Access to Filr—Maintenance Tasks,” on page 11
- ◆ Chapter 2, “Adding a Filr Appliance to an Existing Deployment,” on page 13
- ◆ Chapter 3, “Administrative Access Maintenance,” on page 15
- ◆ Chapter 4, “Branding and Changing the User Interface,” on page 17
- ◆ Chapter 5, “Desktop Application Maintenance,” on page 37
- ◆ Chapter 6, “Helping Micro Focus Improve Filr,” on page 47
- ◆ Chapter 7, “Hosting Desktop Application Installation Files on a Separate Server,” on page 49
- ◆ Chapter 8, “KeyShield Integration with Filr,” on page 51
- ◆ Chapter 9, “Using Multi-Factor Advanced Authentication with Filr,” on page 55
- ◆ Chapter 10, “Language Settings,” on page 59
- ◆ Chapter 11, “Migrating the Filr’s MySQL Database to Microsoft SQL,” on page 61
- ◆ Chapter 12, “Mobile Device Management,” on page 69
- ◆ Chapter 13, “Monitoring,” on page 77
- ◆ Chapter 14, “MySQL—Backup and Restore from the Command Prompt,” on page 87
- ◆ Chapter 15, “Net Folder Maintenance,” on page 89
- ◆ Chapter 16, “Notification (Email) Customization,” on page 91
- ◆ Chapter 17, “Search Index Maintenance,” on page 93
- ◆ Chapter 18, “Security,” on page 101
- ◆ Chapter 19, “Storage Management,” on page 127
- ◆ Chapter 20, “Troubleshooting,” on page 141
- ◆ Chapter 21, “User and Group Maintenance,” on page 145
- ◆ Appendix A, “A Simulation and Some Best Practice Sizing Recommendations,” on page 153

This guide is for Filr 3.0 administrators and covers various Filr administrative tasks that come into play after your Filr system is deployed and providing services to end users.

Audience

This guide is intended for Filr administrators.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the **comment on this topic** link at the bottom of each page of the online documentation.

Documentation Updates

For the most recent version of this guide and other documentation, visit the [Micro Focus Filr 3.0 Documentation website \(http://www.novell.com/documentation/filr-3\)](http://www.novell.com/documentation/filr-3).

Additional Documentation

You can find more information in the Micro Focus Filr documentation, which is accessible from the [Micro Focus Filr 3.0 Documentation website \(http://www.novell.com/documentation/filr-3\)](http://www.novell.com/documentation/filr-3).

1 Access to Filr—Maintenance Tasks

All of the links below point to rows within UI help tables in the [Filr 3.4.1: Administrative UI Reference](#). See the Path statements before each table for UI navigation help.

Desktop Application Access

- ♦ [Desktop Default—Enable/Disable](#)
- ♦ [Desktop Selected Users—Enable/Disable](#)

Guest User (Public) Access

- ♦ [Guest \(Public\)—Enable/Disable](#)

Local User (non-LDAP) Access

- ♦ [Local \(non-LDAP\) Users—Enable/Disable](#)

Making Public URLs Searchable

You can provide Internet search engines (such as Google) with the Filr permalinks for folders that you want to make publicly available on the Internet.

- 1 Access the folder in Filr.
- 2 Click **Permalinks** at the bottom of the folder page.

Mobile Device App Access

- ♦ [Mobile Default—Enable/Disable](#)
- ♦ [Mobile Selected Users—Enable/Disable](#)

Web Browser Access

- ♦ [Web Default—Enable/Disable](#)
- ♦ [Web Selected Users—Enable/Disable](#)

2 Adding a Filr Appliance to an Existing Deployment

To accommodate additional load, you can add Filr appliances to the Filr system only if your original Filr system was configured with shared storage (`/vashare`).

- ♦ [“Prerequisites” on page 13](#)
- ♦ [“Adding Filr Appliances to an Existing Deployment” on page 13](#)

Prerequisites

You can add a Filr appliance to an existing Filr deployment only if your Filr deployment meets the following prerequisites:

- ♦ **It is an expandable deployment:** Small (all-in-one) and non-expandable Filr deployments cannot be expanded.
- ♦ **Shared storage is enabled:** Ensure that a shared storage CIFS or NFS mount (`/vashare`) exists for the Filr deployment. You configure shared storage during the Filr appliance installation, as described in [“Setting Up Shared Storage”](#) in the *Filr 3.4: Installation, Deployment, and Upgrade Guide*.

IMPORTANT: If shared storage (`/vashare`) was not configured at the time you installed your original Filr system, you cannot add Filr appliances to the system.

- ♦ **The CIFS or NFS mount is accessible to all Filr appliances:** All Filr appliances in the cluster need to have access to the CIFS or NFS mount.
- ♦ **(Recommended) A load balancing solution is in place:** If you want to provide a common access URL for all your Filr users, you must provide a solution for load balancing between the Filr appliances.

Micro Focus does not provide a load balancing appliance; however, there are many software solutions available, such as Apache, HAProxy, and NGINX.

There are also hardware solutions available, such as F5 Networks, Juniper, Riverbend, and A10 Networks.

Searching the web for Layer 4-7 switches or Application Delivery Controller is a good place to start finding a solution that meets your requirements.

Adding Filr Appliances to an Existing Deployment

To add Filr appliances to an exiting large Filr deployment:

- 1 Ensure that your system meets the necessary [prerequisites](#).
- 2 Assuming that you have planned the installation, downloaded the software, and so on, install the additional Filr appliance, beginning with [“Deploying the Virtual Machines”](#) in the *Filr 3.4: Installation, Deployment, and Upgrade Guide*.

The process is the same as when you installed the original Filr appliance.

IMPORTANT: Choose the same configuration options (including the same CIFS and NFS mount) that you chose when you installed the original Filr appliance.

- 3 Run the installation wizard for a large deployment (at port 9443), as described in “[Setting Up the Filr Appliances](#)” in the *Filr 3.4: Installation, Deployment, and Upgrade Guide*.
- 4 After the configuration is complete, complete the steps in “[Completing the Expandable Filr Deployment](#)” in the *Filr 3.4: Installation, Deployment, and Upgrade Guide*. Then verify that clustering is enabled and that the Memcached configuration matches the configuration of the original Filr appliance.

3 Administrative Access Maintenance

- ♦ “Adding or Removing Administrative Rights for Users and Groups” on page 15
- ♦ “Administrative Maintenance—Port 8443 Admins” on page 15
- ♦ “Simplifying Management through Administrative Groups” on page 16

Adding or Removing Administrative Rights for Users and Groups

See “Assigning and Managing Port 8443 Direct Administrators” in the *Filr 3.4.1: Administrative UI Reference*.

Administrative Maintenance—Port 8443 Admins

About Port 8443 Administrators

There are two types of Port 8443 Administrators

- ♦ **Built in:** Have full rights to the Port 8443 console, including the right to add or remove Direct administrators.
- ♦ **Direct:** Have rights to administer only
 - ♦ Users
 - ♦ Groups
 - ♦ Mobile Devices
 - ♦ Net Folders
 - ♦ Net Folder Servers

Modifying Port 8443 Administrators

The modifications you can make depend on the type of user, as follows:

- ♦ **Built in admin:** You can change this username and password by logging in as the user, clicking the **Username** (upper right), selecting **View Profile**, clicking **Edit**, and making the changes.

Changing this affects

- ♦ The name you enter to log in as the built-in administrator
- ♦ The name that appears in the upper-right corner of the Port 8443 console
- ♦ The name that appears in the administration console under **Administrators**
- ♦ **LDAP users (Direct administrators):** User names and passwords are controlled in the LDAP source.
- ♦ **Internal Filr users:** User names cannot be changed; passwords can.

Administrators click the user in the Users list, click the Profile button, and enter a new password.
Internal users edit their profile to change their passwords.

Simplifying Management through Administrative Groups

You can simplify your management tasks by creating administrative groups and assigning group members with specific administrative tasks.

For example, Net Folder setup and indexing, etc. is time-intensive.

1. Create a group.
2. Add it to the **Administrators** list.

See “[Assigning and Managing Port 8443 Direct Administrators](#)” in the *Filr 3.4.1: Administrative UI Reference*

3. Assign users to the group.
4. Task group members with setting up Net Folders.

4 Branding and Changing the User Interface

- ♦ “Branding Desktop Apps (Advanced-Edition License Only)” on page 17
- ♦ “Branding Mobile Apps (Advanced-Edition License Only)” on page 19
- ♦ “Branding the Web User Interface” on page 34
- ♦ “Changing the Title of the People Page” on page 35

Branding Desktop Apps (Advanced-Edition License Only)




As the built-in Port 8443 administrator, you can brand your Filr desktop apps to match your organization’s brand.









IMPORTANT: Direct Port 8443 administrators [do not have rights to administer branding](#).

To customize the branding of the desktop application, you must first create a ZIP file containing the files outlined in [Table 4-1 on page 17](#).

IMPORTANT: The following files must be directly zipped and should not be contained within a folder.

Table 4-1 Desktop Branding Files

File Name and format	File Size	Sample File Format	Description
about.png	418 x 200 Pixels		<p>To view the about image:</p> <ul style="list-style-type: none">♦ On Windows: Right-click  and then click About Company Name - Filr.♦ On Mac: Click  and then click About Company Name - Filr. <p>NOTE: Ensure that your custom branded image is of the same size as the sample file. Otherwise, the text information such as version number and the copyright information that Filr adds might overlap your custom branded image.</p>

File Name and format	File Size	Sample File Format	Description
console_header.png	205 x 48 Pixels		<p>To view the console header image:</p> <ul style="list-style-type: none"> ♦ On Windows: Right-click  and then click Open Filr console. ♦ On Mac: Click  and then click Open Filr Console. <p>NOTE: Ensure that your custom branded image is of the same size as the sample file. Otherwise, the Desktop Console text that Filr adds might overlap your custom branded image.</p>
login_header.png	400 x 56 Pixels		<p>To view the login header image:</p> <ul style="list-style-type: none"> ♦ On Windows: Right-click  and then click Login. ♦ On Mac: Click  and then click Login.
FilrBranding.xml	NA	<pre><?xml version="1.0" ?> <FilrBranding> <CompanyName>Company Name</CompanyName> <AboutFilrColor>Font_Color_in_hexadecimal_format</AboutFilrColor> <AboutFilrBgColor>background_Color_in_hexadecimal_format</AboutFilrBgColor> </FilrBranding></pre>	<p>Create an XML file using the sample file format.</p> <p>The company name that you specify in this file replaces all the instances where company name is displayed in the desktop application. For example, in the About <i>Company Name</i> - Filr option that appears when you right-click  on Windows or click  on Mac.</p> <p>The font color and the background color that you specify is applied on all the text information such as Filr version and copyright information. You must specify the color only in hexadecimal format. For example: #17202A.</p>

Branding Mobile Apps (Advanced-Edition License Only)

As the built-in Port 8443 administrator, you can brand your Filr mobile apps to match your organization's brand.

IMPORTANT: Direct Port 8443 administrators [do not have rights to administer branding](#).

- ♦ [“Android UI Branding” on page 19](#)
- ♦ [“iOS UI Branding” on page 25](#)
- ♦ [“Windows Phone Branding” on page 33](#)

Android UI Branding

To custom brand the Android Filr app, you must first create a folder on your system that will be used to hold the resources used for custom branding. We will refer to this as the *android-branding* folder in the rest of this document.

You can customize the colors and the images that Android uses to customize the filr app. Let's deal with the images first and then the colors.

- ♦ [“Customizing Images for Android Branding” on page 19](#)
- ♦ [“Customizing Colors for Android Branding” on page 21](#)
- ♦ [“Android Image Examples” on page 22](#)
- ♦ [“Android Color Examples” on page 23](#)
- ♦ [“Downloading Example Files” on page 25](#)

Customizing Images for Android Branding

- ♦ [“About Image Density” on page 19](#)
- ♦ [“Creating and Naming the Images” on page 20](#)

About Image Density

Because Android runs on devices with a wide variety of screen densities, you should always provide bitmap resources tailored to each of the generalized density buckets: low, medium, high and extra-high density. This will help in achieving good graphical quality and performance on all screen densities. If for some reason, you can't provide images for all of the density buckets, then you must provide at least one image matching the XXXHDPI/XXHDPI/XHDPI scale factor. The higher resolution image, the better the display quality.

First start with a base image and then generate the images for each density using the following scale table. Remember in Android, 1dp (device independent) is equal to 160 pixels.

Density Bucket Name	Scale Factor	Pixels
LDPI	0.75	160 x 0.75 = 120 pixels
MDPI	1.0	160 x 1 = 160 pixels
HDPI	1.5	160 x 1.5 = 240 pixels
XHDPI	2.0	160 x 2 = 320 pixels
XXHDPI	3.0	160 x 3 = 480 pixels
XXXHDPI	4.0	160 x 4 = 640 pixels

For example, if you create a 75x75 image for LDPI then you need to create the following images to match other densities.

Density Bucket Name	Density Scale	Create Image
LDPI	0.75 – Base Image	0.75 x 0.75
MDPI	1.0 - 100	100 x 100
HDPI	1.5 – (100 x 1.5) - 150	150 x 150
XHDPI	2.0 – (150 x 2) - 200	200 x 200
XXHDPI	4.0 – (200 x 3) - 600	600 x 600
XXXHDPI	HDPI6.0 – (600 x 4) - 2400	2400 x 2400

Creating and Naming the Images

Filr Android-app customizing involves the following branding images.

Table 4-2 *Android Image Names and Default Sizes*

Image Name	Location Where Displayed	Recommended Dimension Ratio*
<code>ic_launcher.png</code>	This image is shown on the passcode lock screen.	144 x 144 pixels
<code>login_header.png</code>	This image is shown on the login screen.	775 x 144 pixels
<code>main_page_logo.png</code>	This image is shown next to the up button.	475 x 96 pixels

* Images that conform with the ratios shown will render without distortion in the locations indicated. For example, an `ic_launcher.png` image that is 288 X 288 pixels will render without distortion.

Create the following folder/folders in the *android-branding* folder that you created on your system. You don't have to create all folders matching different scaling factors. You can create one generic folder called "drawable" and place higher resolution images in this folder. This higher resolution image will be scaled dynamically by Android to make it look good on different Android devices. Providing a lower resolution image will not yield satisfactory results.

Table 4-3

Folder Name	Description
drawable-ldpi	Place all lower resolution images here
drawable-mdpi	Place all base resolution images here
drawable-hdpi	Place all high resolution images here
drawable-xhdpi	Place all extra high resolution images here
drawable-xxhdpi	Place all extra extra high resolution images here
drawable-xxxhdpi	Place all extra extra extra high resolution images here
drawable	Place the highest possible resolution images here. Images placed here may not be required to be placed in other folders. Images placed in this folder are dynamically scaled by Android to make them look good on various devices.

Customizing Colors for Android Branding

To customize the colors in Filr's Android mobile app, create a file called `colors.xml` in the `android-branding` folder and add the colors with your chosen values. Filr's Android app supports customizing the following colors.

Table 4-4 Android Color Tags

Color Name	Where it is shown
main_header_start	These two colors are used for creating a gradient shade that is applied to the header bar. This change is visible only in the What's New section.
main_header_end	
view_header_start	These two colors are used for creating a gradient shade that is applied to the header bar. This change is visible throughout the UI, except in the What's New section and on the main page where the tabs are shown.
view_header_end	
list_header_text	This color is used for list-header text. It is visible in the Share-action dialogs.
form_background	This color is used in the Add Comments dialog.
property_value_text	This color is used to display links and text.

Example content of the `colors.xml` file:

```
<branding>
  <main_header_start>#75717c</main_header_start>
  <main_header_end>#4D2525</main_header_end>
  <view_header_start>#9CCDC</view_header_start>
  <view_header_end>#519217</view_header_end>
  <list_header_text>#7EB5C1</list_header_text>
  <form_background>#F7G2G4</form_background>
  <property_value_text>#246d9g</property_value_text>
</branding>
```

NOTE: The custom-branding-resource subsystem is very stringent in interpreting hex codes. You must specify the fully valid color hex code including the pound sign (#). If you miss specifying this sign, then the color value is ignored and default color hex code is used. The supported formats are #FFFFFF and #FFFFFFF

Select the `colors.xml` file and the `drawable...` folders in your `android-branding` equivalent folder and create a zip archive. Store the zip archive somewhere on your system for use when configuring the branding on the Android client.

To apply the branding you have created, see “Using the Mobile App Branding dialog” in the [Filtr 3.4.1: Administrative UI Reference](#).

Android Image Examples



Powered by Digital Airlines

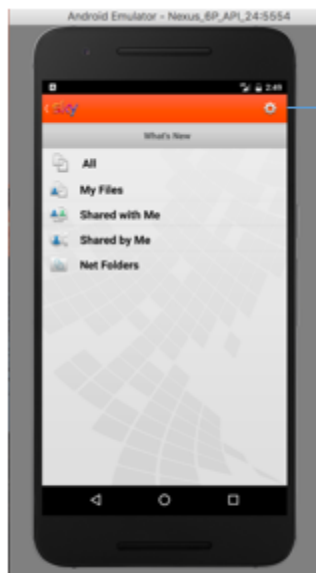


main_page_logo.png



ic_launcher.png

Android Color Examples



main_header_start

main_header_end



`view_header_start`

`view_header_end`

`list_header_text`



`form_background`



Downloading Example Files

You can download an example set of Android Branding Files [here](#).

iOS UI Branding

To brand your iOS mobile devices, you create a .zip file that includes branding images and color specifications, as described in the following sections.

- ◆ “Tips and Caveats” on page 25
- ◆ “Downloading iOS Example Files” on page 26
- ◆ “iOS Branding File Details” on page 26
- ◆ “iOS Color Customization Details” on page 30
- ◆ “Creating an iOS Branding .zip File” on page 33

Tips and Caveats

The following points apply to iOS branding files:

- ◆ Inclusion of any of the customized branding files is optional.
The iOS app will work fine whether or not they are found in the .zip file.
- ◆ If a file is in the zip file it will be used.
Otherwise, the default Micro Focus branding displays.
- ◆ Files must be named exactly as specified or iOS applications will not find them.
- ◆ All image files should be set to 72 PPI (pixels per inch). Increasing the resolution beyond this can negatively affect app performance.

Downloading iOS Example Files

You can download an example set of iOS Branding Files [here](#).

iOS Branding File Details

- ◆ “Overview of iOS Branding Files” on page 26
- ◆ “Example: PIN Code and Document Picker Extension” on page 26
- ◆ “Example: Account Settings Dialogs and the Login Dialog for iPhone” on page 27
- ◆ “Example: iPad Login Dialog” on page 28
- ◆ “Example: Home Selection View” on page 29

Overview of iOS Branding Files

Table 4-5 iOS Branding File Summary

Image Names	Where Used	Dimensions in Pixels
◆ Filr_40_ios.png	PIN/Passcode and Document Picker dialogs	◆ 40 X 40
◆ Filr_40_ios@2x.png *		◆ 80 X 80
◆ Filr_40_ios@3x.png *		◆ 120 X 120
◆ Filr_header.png	Account Settings dialogs and Login dialog for iPhone	◆ 300 X 72
◆ Filr_header@2x.png *		◆ 600 X 144
◆ Filr_header@3x.png *		◆ 900 X 216
◆ Filr_icon_login.png	iPad Login dialog	◆ 600 X 233
◆ Filr_icon_login@2x.png *		◆ 1200 X 466
◆ Filr_icon_login@3x.png *		◆ 1800 X 699
◆ Filr_signature.png	Home Selection View	◆ 248 X 60
◆ Filr_signature@2x.png *		◆ 496 X 120
◆ Filr_signature@3x.png *		◆ 640 X 155

* The files named ...@2x and ...@3x support optimal image scaling on multiple devices.

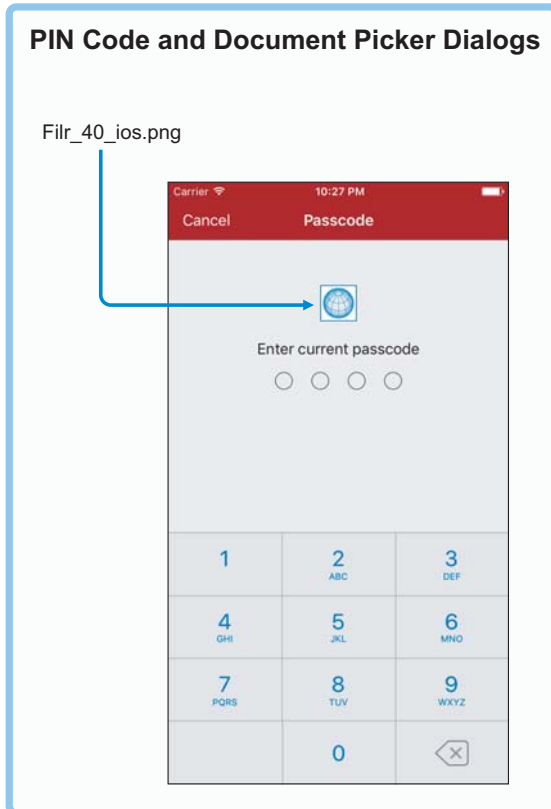
Although it is not required that you create scaled images, Micro Focus recommends that you follow the image guidelines in the [iOS Human Interface Guidelines published by Apple](https://developer.apple.com/ios/human-interface-guidelines/graphics/image-size-and-resolution/) (<https://developer.apple.com/ios/human-interface-guidelines/graphics/image-size-and-resolution/>).

The [iOS sample files](#) include examples of each file in the sizes indicated.

Example: PIN Code and Document Picker Extension

To brand the PIN Code and Document Picker Extension dialogs, create a `Filr_40_ios.png` file and include it in the `.zip` file.

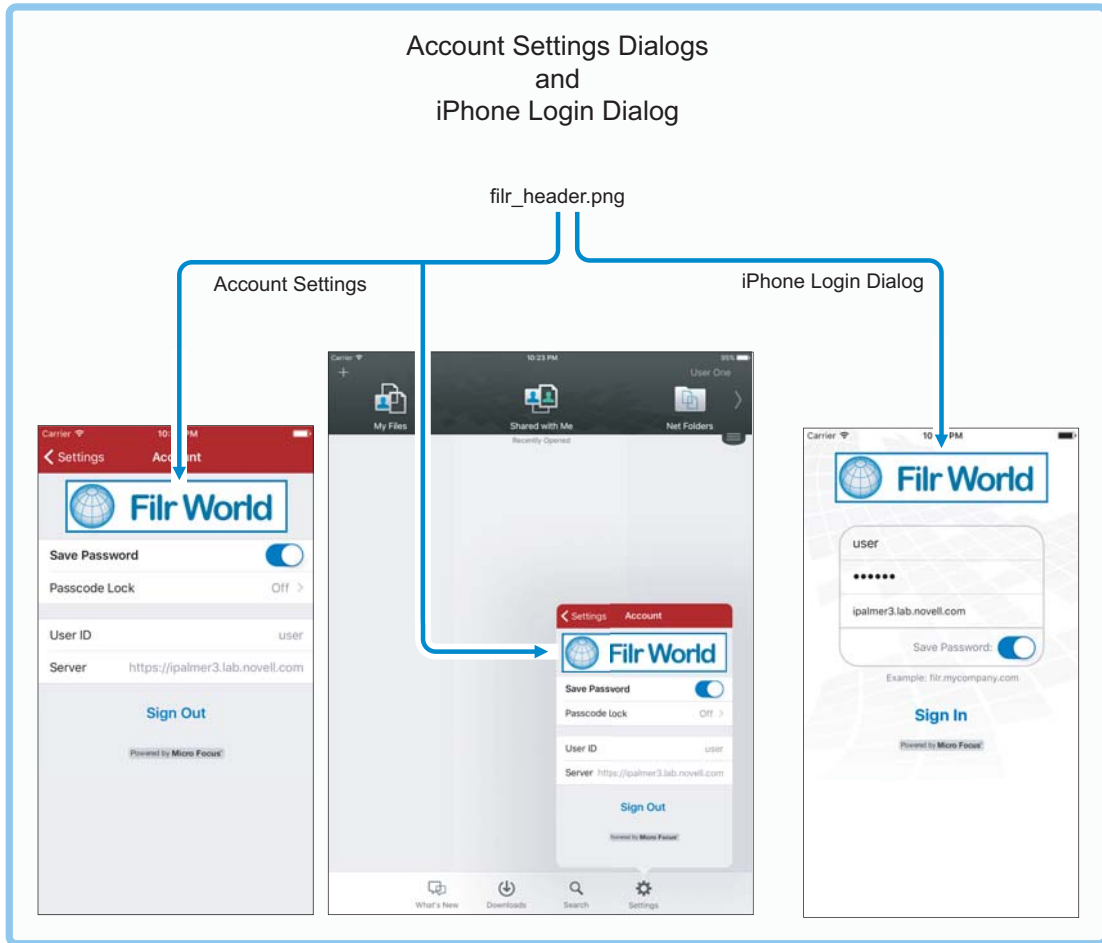
Figure 4-1 Filr_40_ios.png Example



Example: Account Settings Dialogs and the Login Dialog for iPhone

To brand the account settings dialog and the login dialog for iPhone devices, create a `filr_header.png` and include it in the zip file.

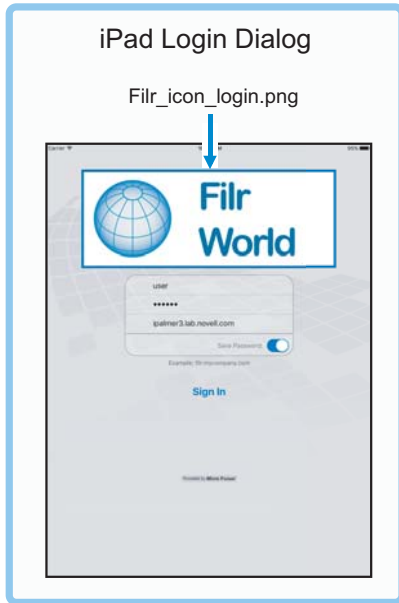
Figure 4-2 filr_header.png Example



Example: iPad Login Dialog

To brand the login dialog on iPad devices, create a `Filr_icon_login.png` file and include it in the .zip file.

Figure 4-3 *Filr_icon_login.png Example*



Example: Home Selection View

For branding the Home Selection View, create a `Filr_signature.png` file and include it in the `.zip` file.

Figure 4-4 Filr_signature.png Example



iOS Color Customization Details

The FilrBranding.xml file defines the colors displayed. Examples are included after the XML sample below.

```
<?xml version="1.0"?>
<FilrBranding>
  <ViewHeaderColor>#0d467f</ViewHeaderColor>
  <SubheadColor>#c1d7ec</SubheadColor>
  <ListHeadTextColor>#0d467f</ListHeadTextColor>
  <FormHeadTextColor>#0d467f</FormHeadTextColor>
  <FormBackgroundColor>#d7e6f5</FormBackgroundColor>
  <HighlightBlendStartColor>#afd4fa</HighlightBlendStartColor>
  <HighlightBlendEndColor>#3d86ce</HighlightBlendEndColor>
  <StatusBarTextColor>light</StatusBarTextColor>
</FilrBranding>
```

Hex values are valid as well as the colors defined in the iOS UIColor class such as red, blue, yellow, etc. They can be defined in upper, lower or mixed case.

An example would be <ViewHeaderColor>green</ViewHeaderColor>.

There are two valid values for StatusBarTextColor: “dark” and “light”.

The following are examples.

Figure 4-5 Example 1

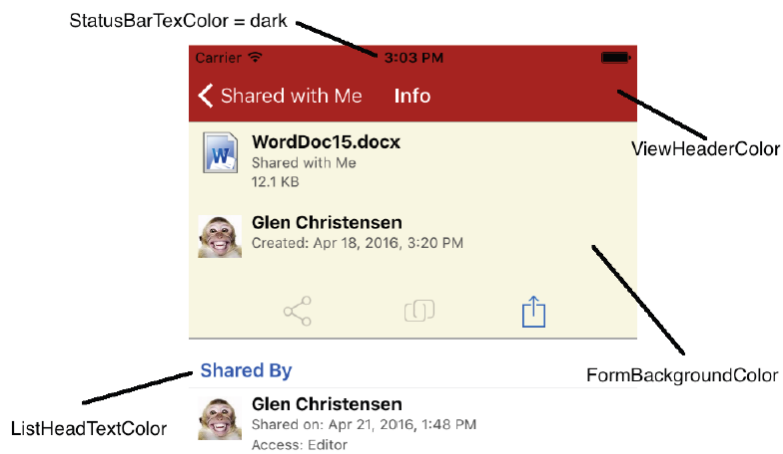


Figure 4-6 Example 2

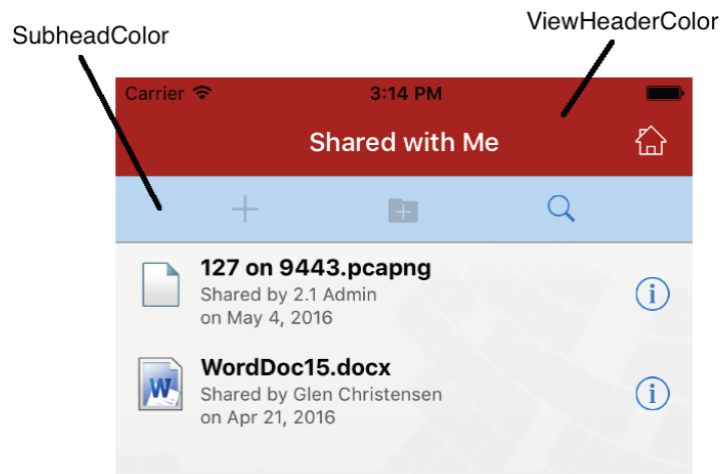


Figure 4-7 Example 3

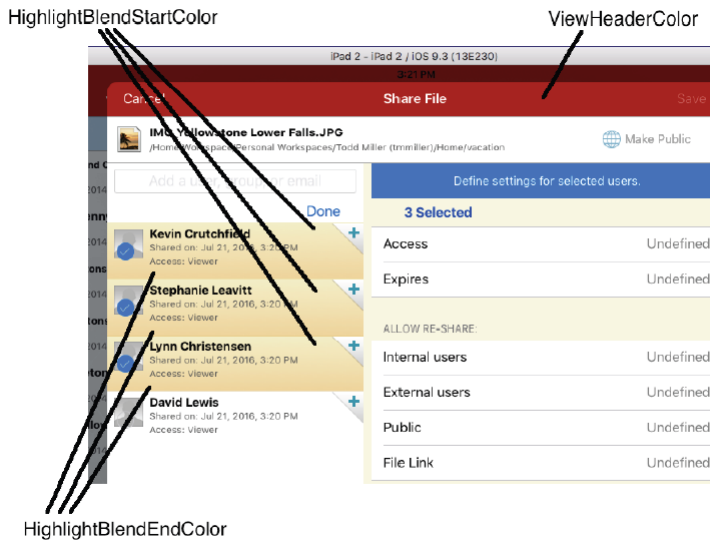
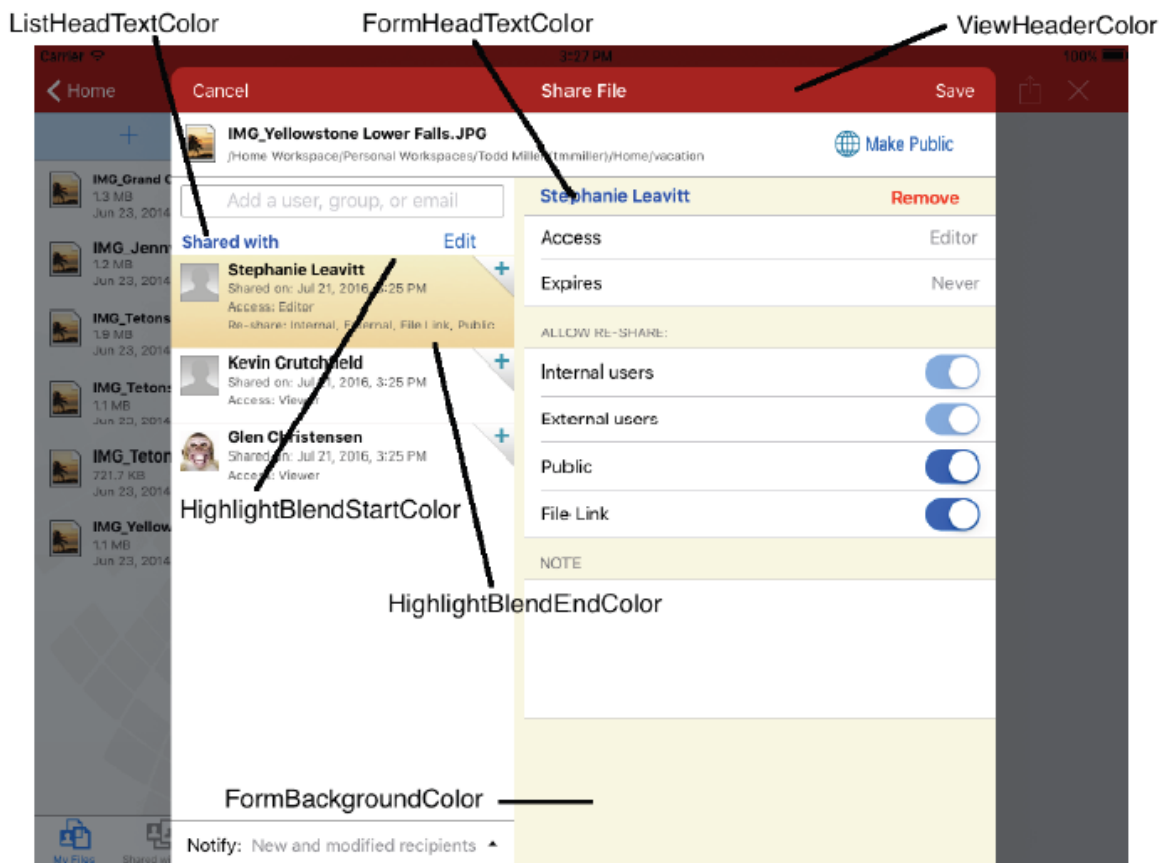


Figure 4-8 Example 4



Creating an iOS Branding .zip File

To apply custom branding to the iOS client, you create the image files for the dialogs you want to brand and define banner and other colors, as follows:

- 1 Create .png files for the dialogs that you want to brand.

Example files are contained in the downloadable `ios-branding-sample.zip` ([../resources/ios-branding-sample.zip](#)) file.

To support optimal image scaling on multiple devices, Micro Focus recommends that you follow the imaging naming conventions outlined in the [iOS Human Interface Guidelines published by Apple \(https://developer.apple.com/ios/human-interface-guidelines/graphics/image-size-and-resolution/\)](#).

- 2 Define the colors you want to use in banners and so on, by creating a `FilrBranding.xml` file.
- 3 Compress the files that you have created into an arbitrarily named .zip file.
- 4 Upload the .zip file using the instructions in “[Branding the Mobile Apps \(Advanced-Edition License Only\)](#)” in the *Filr 3.4.1: Administrative UI Reference*.

Windows Phone Branding

You can download a sample Windows app branding .zip file [here](#).

- ♦ “[Settable Colors](#)” on page 33
- ♦ “[A Sample FilrBranding.xml File](#)” on page 34
- ♦ “[Customizable Images](#)” on page 34
- ♦ “[Assembling and Uploading the Zip File](#)” on page 34

Settable Colors

The colors displayed in the Filr Windows Mobile Client can be customized using the following properties defined in the `FilrBranding.xml` file.

- ♦ `LoginFontColor`
- ♦ `ApplicationBackgroundColor`
- ♦ `ApplicationFontColor`
- ♦ `AppBarBackgroundColor`
- ♦ `AppBarForegroundColor`
- ♦ `StatusBarBackgroundColor`
- ♦ `StatusBarForegroundColor`
- ♦ `DetailsPageBackgroundColor`
- ♦ `SearchIconColor`
- ♦ `HamburgerMenuColor`
- ♦ `ApplicationTitle`

A Sample FilrBranding.xml File

```
<branding>
  <LoginFontColor>#000000</LoginFontColor>
  <ApplicationBackgroundColor>#FFD700</ApplicationBackgroundColor>
  <ApplicationFontColor>#FFFFFF</ApplicationFontColor>
  <AppBarBackgroundColor>#FF6347</AppBarBackgroundColor>
  <AppBarForegroundColor>#FFFFFF</AppBarForegroundColor>
  <StatusBarBackgroundColor>#FF7F50</StatusBarBackgroundColor>
  <StatusBarForegroundColor>#FFFFFF</StatusBarForegroundColor>
  <DetailsPageBackgroundColor>#FF4500</DetailsPageBackgroundColor>
  <SearchIconColor>#FF4500</SearchIconColor>
  <HamburgerMenuColor>#FF4500</HamburgerMenuColor>
  <ApplicationTitle>My Filr</ApplicationTitle>
</branding>
```

Customizable Images

You can customize two images that are located on the login page.

The two image must be named as follows:

- ◆ `Loginbackground.png` (for login page background)
- ◆ `Loginheader.png` (for login page header)

Assembling and Uploading the Zip File

You can download a sample Windows app branding .zip file [here](#).

After creating your own Windows branding components, do the following:



1. Zip these three files together and then upload to the server.
The branding changes are applied on the background thread.
2. In some cases the branding is not applied properly due to a resource contention.
Stopping and restarting the app should resolve the issues.
3. After creating your .zip file, see “[Using the Mobile App Branding dialog](#)” in the *Filr 3.4.1: Administrative UI Reference*.

Branding the Web User Interface

See “[Branding the Web Client](#)” in the *Filr 3.4.1: Administrative UI Reference*.

Changing the Title of the People Page

Filr enables you to modify the name of the People page. (This is an alternate way of viewing users in your Filr system.) This name is displayed when navigating the Workspace tree (as described in [“Navigating the Workspace Tree”](#) in the *Filr 3.4: Maintenance Best Practices Guide*) and when performing a search.

- 1 Click the People icon  in the masthead.
- 2 Click the Configure icon  next to the folder name, then click **Rename Workspace**.
- 3 In the **New Name** field, specify a new name for the workspace, then click **OK**.

5 Desktop Application Maintenance

- ◆ “Client Management Software and the Filr Desktop Applications” on page 37
- ◆ “Controlling File Downloads by the Filr Desktop Applications” on page 40
- ◆ “Desktop Application Installation Files—Location” on page 42
- ◆ “Desktop Application Software Management” on page 42
- ◆ “Enabling Desktop Access for Users” on page 44
- ◆ “Synchronization-Traffic Management” on page 44

Client Management Software and the Filr Desktop Applications

You can manage the Filr desktop application on users’ workstations with client management software such as Micro Focus ZENworks.

When following the instructions in this section, you must use the `.msi` file, which is bundled in the `MicroFocusFilrAutoUpdate.tgz` file, and is available on the [Filr software download site](#).

If you use the `.msi` file to distribute the Filr desktop application to user workstations, you need to install the following items to each user workstation, independent of the Filr software:

- ◆ Microsoft .NET Framework 4.6.2 or later
You can download Microsoft .NET Framework from the [Microsoft .NET Downloads page](#).
- ◆ Microsoft Visual C++ 2013 Redistributable Package (Applies to all workstations)
You can download the redistributable package from the [Microsoft Download Center](#).

NOTE: The ability to manage the Filr desktop application is available only with Filr desktop 1.0.2 and later.

You can customize the installation and control whether Windows Explorer is restarted.

Customizing the Installation for the Filr Desktop Application

You can customize the installation process of the Filr desktop application for your organization in the following ways:

- ◆ Configure default values for each installation option of the Filr desktop application. (Users can change these default values when configuring the Filr desktop application.)
- ◆ Auto-configure all values for each installation option of the Filr desktop application. (Users specify only their user name and password when configuring the Filr desktop application; users cannot change the default values during initial configuration.)
- ◆ Disallow users from modifying configuration options in the Filr desktop application. (Users cannot change the default values during initial configuration, and cannot modify the values via the Filr console after initial configuration.)

NOTE: This does not prevent users from manually modifying configuration settings in the registry or file system.

The following sections describe how to make these customizations.

Configuring Default Values

You can configure the default values for each installation option of the Filr desktop application. Users can change these default values when configuring the Filr desktop application.

You accomplish this on Windows by creating registry values, and on Mac by adding properties to the application's `Info.plist` file.

- 1 Windows:** Access the following location where you will create registry values:

```
\\HKLM\Software\Novell\Filr
```

Mac: Access the `Info.plist` file where you will add properties. This file is usually in the following location:

```
/Applications/Micro Focus Filr/Contents/Info.plist
```

- 2** Create Windows registry values and add properties to the `Info.plist` file for the values for which you want to configure defaults.

The following table displays the available options for configuring default values.

Table 5-1 Default Value Configuration Options

Windows Registry Value Name	Value Type	Mac Property Name	Value Type	Supports Env Variables	Default Value
Default Server URL	REG_SZ	FilrDefaultServerURL	string	No	https://
Default Username	REG_SZ	FilrDefaultUsername	string	Yes	%USERNAME% or \$USER
Default Account Name	REG_SZ	FilrDefaultAccountName	string	No	Hostname in server URL
Default Remember Password	REG_SZ ("true" or "false")	FilrDefaultRememberPassword	<true/> or <false/>	No	false
Default Sync Dir	REG_SZ	FilrDefaultSyncDir	string	Yes	%USERNAME%\Filr or \$USER\Filr
Default Start On Login	REG_SZ ("true" or "false")	FilrDefaultStartOnLogin	<true/> or <false/>	No	true

Enabling Auto-Configuration

After you have configured default values for the Filr desktop application installation, you can enable auto-configuration. When auto-configuration is enabled, users cannot change the default values during initial configuration. (Users specify only their user name and password when configuring the Filr desktop application.)

You accomplish this on Windows by creating registry values, and on Mac by adding properties to the application's `Info.plist` file.

- 1 **Windows:** Access the following location where you will create registry values:

```
\\HKLM\Software\Novell\Filr
```

Mac: Access the `Info.plist` file where you will add properties. This file is usually in the following location:

```
/Applications/Micro Focus Filr/Contents/Info.plist
```

- 2 Create Windows registry values and add properties to the `Info.plist` file for the values for which you want to configure defaults.

The following table displays the available options for auto-configuration.

Table 5-2 Auto-Configuration Options

Windows Registry Value Name	Value Type	Mac Property Name	Value Type	Supports Env Variables	Default Value
Auto Configure	REG_SZ ("true" or "false")	FilrAutoConfigure	<true/> or <false/>	No	false

Disallowing User Configuration

You can disallow users from modifying configuration options in the Filr desktop application. This means that users cannot change the default values during initial configuration, and they cannot modify the values via the Filr console after initial configuration.

NOTE: This does not prevent users from manually modifying configuration settings in the registry or file system.

You accomplish this on Windows by creating registry values, and on Mac by adding properties to the application's `Info.plist` file.

- 1 **Windows:** Access the following location where you will create registry values:

```
\\HKLM\Software\Novell\Filr
```

Mac: Access the `Info.plist` file where you will add properties. This file is usually in the following location:

```
/Applications/Micro Focus Filr/Contents/Info.plist
```

- 2 Create Windows registry values and add properties to the `Info.plist` file for the values for which you want to configure defaults.

The following table displays the available options for disallowing user configuration.

Table 5-3 Disallow User Configuration Options

Windows Registry Value Name	Value Type	Mac Property Name	Value Type	Supports Env Variables	Default Value
Allow User Configuration	REG_SZ (“true” or “false”)	FilrAllowUserCo nfiguration	<true/> or <false/ >	No	true

Modifying the Filr Desktop Configuration

If you have configured the Filr desktop application with auto-configuration (as described in [“Enabling Auto-Configuration” on page 39](#)), you can modify the configuration settings:

- 1 Change the options in the registry or `.plist` file, then restart the Filr desktop application. When the Filr desktop application starts, it detects that the default settings have changed and applies the new settings.

NOTE: The one exception is that the synchronization directory cannot be changed after the Filr desktop application has been configured.

Controlling Windows Explorer Restart

The Filr desktop application for Windows includes overlay icons that do not appear until Windows Explorer is restarted. Prior to the Filr 1.0.2 desktop application, the Windows `.msi` always restarted Windows Explorer during the installation (except when using the `No UI` option). Because restarting Explorer might not always be desirable, the Filr 1.0.2 desktop application allows you to override the default.

The Windows installer supports four basic user interface levels for installing `MSI` files:

- ◆ No UI (“`msiexec /qn`”)
 - Windows Explorer is never restarted when using this option.
- ◆ Basic UI (“`msiexec /qb`”)
- ◆ Reduced UI (“`msiexec /qr`”)
- ◆ Full UI (“`msiexec /qf`” or simply “`msiexec`”, since this is the default)

For example, use the following command to install the `MSI` with basic UI and without restarting Windows Explorer:

```
msiexec /qb /i MicroFocusFilr-version.msi RESTARTEXPLORER=no
```

Controlling File Downloads by the Filr Desktop Applications

Path to Configuration Page: Filr Administration Console > **System** > **Desktop Application** > **Application Whitelist/Blacklist**

Why File-Download Control Is Important

Filr can download large numbers of online files when workstation-based applications, such as antivirus scanners and backup software, request access to them. Downloading the files stored in Net Folders can quickly fill up a local disk.

How File-Download Control Works

To let you control application-driven downloads and prevent Filr from filling up local disks, Filr provides the **Application Whitelist/Blacklist** dialog and the following options:

NOTE: for more information regarding the user experience, see “Preventing Application-Driven Downloads From Filling Up the Local Disk” in the [Desktop Guide for Windows](#) and the [Desktop Guide for Mac](#).

Always Blacklist Macintosh Antivirus Applications

Antivirus software running on Mac workstations downloads files automatically. Therefore, you should always include Mac antivirus applications in the Blacklist.

Managing File Downloading

If your organization deploys the Filr desktop application, we recommend that you identify a file-download control strategy by doing the following:

- 1 Log in to the Filr administration console and navigate to **System > Desktop Application > Application Whitelist/Blacklist**.
- 2 Review the list of applications that are blocked by default for the desktop platforms (Windows and Mac) that your organization uses.
- 3 If you want to only block certain applications from downloading files through Filr, ensure that the applications are listed in the appropriate Windows and Mac blacklists.

For example, if you know that a specific set of company-approved virus scanners are the only applications that could trigger mass downloads, then simply ensure that those scanners are in your blacklists.

Download requests from applications that are listed, such as virus scanners, will trigger a system alert to users.

If you add entries to the blacklists, use the existing entries as a pattern. Windows and Mac have unique requirements for identifying the applications to be blocked.

- 4 If you want to control exactly which applications can download files through Filr, you should create a whitelist.

For example, if your users are only authorized to work with the applications in an office suite, then you should create a whitelist with only those applications listed.

Applications that are not listed, such as virus scanners, will trigger a system alert to users. Attempts to open any online-only files by unauthorized applications will fail.

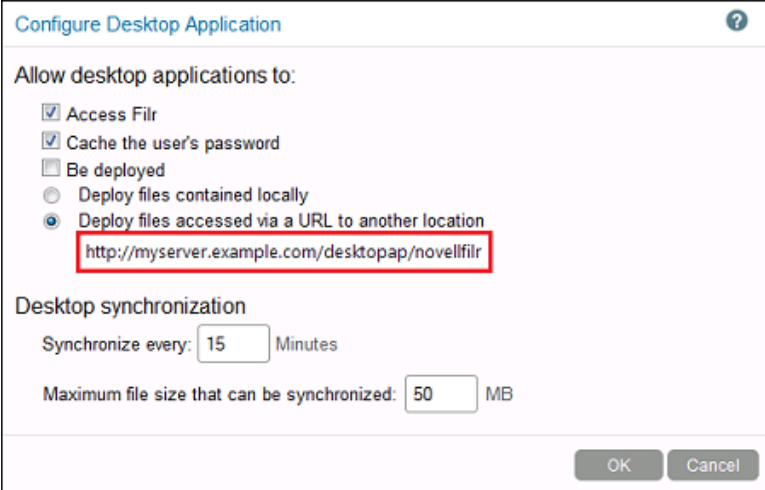
As you create a whitelist, use the existing blacklist entries as a pattern. Windows and Mac have unique requirements for identifying the applications to be allowed.

- 5 If you want a flexible approach that allows downloading by specified applications, blocks downloading by other applications, and lets users deny or approve download requests by unlisted applications, then deploy both a whitelist and a blacklist.
- 6 Periodically review and update your file-download strategy. Make sure that new antivirus and backup software is included. Consult with users about applications that they have allowed or blocked, and consider adding these to your lists as applicable.

Desktop Application Installation Files—Location

Although you can specify that the clients be downloaded from the local appliance, Micro Focus recommends hosting the Filr desktop applications on a separate web server, as documented in [Chapter 7, “Hosting Desktop Application Installation Files on a Separate Server,”](#) on page 49.

For example, if the server host name is `myserver.example.com`, then a URL similar to the following would need to be set in the Web Administration Console (port 8443). Click **Desktop Application** in the left frame.



The screenshot shows a dialog box titled "Configure Desktop Application". It has a question mark icon in the top right corner. The main section is "Allow desktop applications to:" and contains several options: "Access Filr" (checked), "Cache the user's password" (checked), "Be deployed" (unchecked), "Deploy files contained locally" (radio button), and "Deploy files accessed via a URL to another location" (radio button, selected). Below the selected option, a text field contains the URL "http://myserver.example.com/desktopap/novellfilr", which is highlighted with a red rectangular box. Below this is the "Desktop synchronization" section, which includes "Synchronize every: 15 Minutes" and "Maximum file size that can be synchronized: 50 MB". At the bottom right, there are "OK" and "Cancel" buttons.

The Filr desktop applications can also be hosted on Filr appliances, as documented in [Chapter 7, “Hosting Desktop Application Installation Files on a Separate Server,”](#) on page 49, provided that the appliances are not fronted by an L4 or L10 switch.

For more information on configuring the desktop applications, see “[Desktop Access—Default Settings](#)” in the *Filr 3.4.1: Administrative UI Reference*.

Desktop Application Software Management

You can update the Filr desktop application on users’ workstations by updating the application on the Filr server or on a separate web server. You can also distribute the application using the `.msi` file in conjunction with client management software such as Micro Focus ZENworks. However, there are certain dependencies that are not installed by default when using the `.msi` file. These are described in the following sections:

Understanding Missing Dependencies Related to Updating the Filr Desktop Application by Using the MSI File

If you use the .msi file to distribute the Filr desktop application to user workstations (by using client management software such as Micro Focus ZENworks), you need to install the following items to each user workstation, independent of the Filr software:

- ◆ Microsoft .NET Framework 4.6.2 or later
You can download Microsoft .NET Framework from the [Microsoft .NET Downloads page \(http://www.microsoft.com/net/downloads\)](http://www.microsoft.com/net/downloads).
- ◆ Microsoft Visual C++ 2013 Redistributable Package (Applies to all workstations)
You can download the redistributable package from the [Microsoft Download Center \(https://www.microsoft.com/en-us/download/details.aspx?id=40784\)](https://www.microsoft.com/en-us/download/details.aspx?id=40784).

Updating the Filr Desktop Application on the Filr Appliance

If you have configured your Filr system to deploy the Filr desktop application (as described in “[Enabling Desktop Access for Users](#)” on page 44), or if you have configured a separate web server to deploy the Filr desktop application (as described in [Chapter 7, “Hosting Desktop Application Installation Files on a Separate Server,”](#) on page 49), you can replace the Filr desktop application download files on the Filr back end so that users are prompted to update the Filr desktop application on their individual workstations.

The files to use for updating the Filr desktop application are the same for all versions of Windows.

To download the Filr desktop application:

- 1 Before downloading the new version of the Filr desktop application, you need to preserve your existing Filr desktop installation. This will allow you to roll back to the older version if the need arises.

To preserve your existing installation of the Filr desktop application, rename the existing directory on the server so that the old files are not overwritten when the new version is downloaded:

- 1a Change to the directory where the files are being stored. For example:

```
cd /opt/novell/filr/apache-tomcat/webapps/desktopapp/
```

This is the default location if the Filr desktop application is installed on the Filr server.

- 1b Rename the `novellfilr` directory to `novellfilr.bak`. For example:

```
mv novellfilr novellfilr.bak
```

- 1c (Optional) If you need to roll back to the older version of the Filr desktop application, you can do so by deleting the new `novellfilr` directory and renaming the `novellfilr.bak` directory to `novellfilr`.

- 2 Download and extract the `MicroFocusFilrAutoUpdate.tgz` file onto your Filr server or separate web server.

```
tar xvzf MicroFocusFilrAutoUpdate.tgz
```

You can download the `MicroFocusFilrAutoUpdate.tgz` file from the [Filr software download site](#).

If you are installing onto the Filr server, download and extract this file to the `opt/novell/filr/apache-tomcat/webapps/desktopapp/` directory.

```
cd /opt/novell/filr/apache-tomcat/webapps/desktopapp
```

This compressed file contains all of the files required for updating the Filr desktop application.

- 3 Run the following commands on the extracted directory to appropriately modify the file permissions:

```
chown -R wwwrun:www novellfilr/  
chmod -R g-w novellfilr/  
chmod -R o-rwx novellfilr/
```

Enabling Desktop Access for Users

Desktop access is not enabled by default.

The Filr desktop application lets users synchronize their Micro Focus Filr files with their personal computers. You can enable this functionality for all users in the Filr system, or for individual users and groups.

In addition to enabling or disabling this functionality for users, you can also make configuration changes that affect the load that the Filr desktop application puts on your Filr system, as well as make changes that ensure tighter security.

Users need to download, install, and configure the Filr desktop application on their personal computers. For more information, see the *Micro Focus Filr Desktop Application Guide for Windows* (<http://www.novell.com/documentation/filr-3/filr-desktop/data/bookinfo.html>) and the *Micro Focus Filr Desktop Application Guide for Mac* (<https://www.novell.com/documentation/filr-3/filr-desktop-mac/data/bookinfo.html>).

Synchronization-Traffic Management

The Filr desktop application can cause a large amount of traffic on the Filr servers. To prevent the Filr desktop application synchronization process or the Filr site from becoming slow, you can distribute the Filr desktop application traffic among dedicated Filr servers with your load balancer or reverse proxy server.

For example, if you have a Filr installation with four servers, you could dedicate one server to handle the Filr desktop application traffic and use the remaining three servers to serve the main Filr Web application. This configuration prevents an unusual spike in the Filr desktop application traffic from impacting the Filr site.

You can distribute the Filr desktop application traffic differently, depending on whether you want traffic from all applications (not just the Filr desktop application) that are accessing Filr to be handled in the same way, or whether you want the Filr desktop application traffic to be handled independently from each other and from other applications that are accessing Filr.

Distributing Filr Desktop Application Traffic Separately from Other Applications

You can configure your load balancer or reverse proxy server to distribute Filr desktop application synchronization traffic among multiple Filr servers. Filr desktop application traffic is independent of traffic from other applications that are accessing Filr.

NOTE: Your load balancer or reverse proxy server must be able to make routing decisions based on the request headers.

- 1 Configure your load balancer or reverse proxy server to use the user agent request header. For the Filr desktop application, the request header begins with `NovellFilrDesktop`. For example:
`User-Agent: NovellFilrDesktop/1.0 (Windows NT 6.1; Python/2.7.0; en_US) suds/0.4.`

For specific information on how to configure the load balancer or reverse proxy server, see [“Load Balancer and Reverse Proxy Server Configuration”](#) on page 45.

Distributing Filr Desktop Traffic in Conjunction with Other Applications

You can configure your load balancer or reverse proxy server to distribute Filr desktop application synchronization traffic (along with traffic coming from all other applications that use the Filr Web service interface) among multiple Filr servers.

Examples of other applications that use the Filr Web service interface:

- ◆ GroupWise client SOAP requests
- ◆ All other SOAP requests from third-party applications

NOTE: Your load balancer or reverse proxy server must be able to make routing decisions based on the HTTP URL path.

- 1 Configure your load balancer or reverse proxy server to send all HTTP requests for the Filr desktop application (designated by the following paths `/ssf/ws/TeamingServiceV1` and `/rest/*`) to one pool of Filr servers.

All other requests are sent to another pool of Filr servers.

For specific information on how to configure the load balancer or reverse proxy server, see [“Load Balancer and Reverse Proxy Server Configuration”](#) on page 45.

Load Balancer and Reverse Proxy Server Configuration

To configure a reverse-proxy server for your Filr site, see [“Reverse Proxy Configuration Settings”](#) in the *Filr 3.4.1: Administrative UI Reference*.

6 Helping Micro Focus Improve Filr

In order to improve the Filr product, it is critical that the Filr development team understands how organizations are deploying Filr.

- ◆ [“Organizational Privacy Is Protected” on page 47](#)
- ◆ [“How Micro Focus Collects Product Improvement Data” on page 47](#)
- ◆ [“How Micro Focus Receives Product Improvement Data” on page 48](#)
- ◆ [“Submitting Your Product Improvement Ideas” on page 48](#)

Organizational Privacy Is Protected

We do not collect information that can be used to identify specific organizations. Rather we collect the following, depending on how you [configure your system](#).

At a basic level (Tier 1), Filr collects the following information:

- ◆ Product version
- ◆ License type
- ◆ Number of users

If you allow us to, we also collect basic information about the deployment size and configuration:

- ◆ Number of files
- ◆ Number of folders
- ◆ And so on

You can view the information collected after the system has been running for 24 hours, by using the [View the information collected link](#) in the Product Improvement dialog.

How Micro Focus Collects Product Improvement Data

The first time you log in to Filr, after changing the admin user’s password, a dialog displays that explains the purpose of the Filr data collection system and lets you change the configuration.

The data collection process runs for the first time when a Filr appliance has been running for 24 hours. Thereafter, it runs weekly.

See [“Product Improvement”](#) in the *Filr 3.4.1: Administrative UI Reference*.

How Micro Focus Receives Product Improvement Data

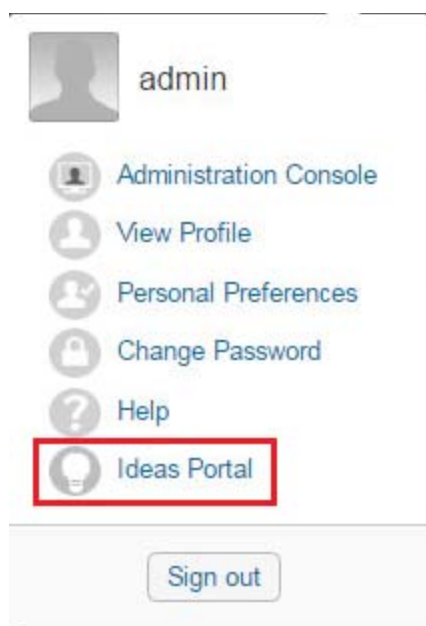
After the weekly data collection process concludes, the system creates a .json data file and sends it to `ftp://productfeedback.novell.com/stats/filr`.

If the FTP transfer is unsuccessful, the system attempts to send it again during the next weekly cycle. No send attempts are made outside of the weekly cycles.

Data files are sent through a regular non-secure FTP connection. File contents are not encrypted because no sensitive or identifying information is included.

Submitting Your Product Improvement Ideas

When you are logged in as an administrative user, you can access the Micro Focus Filr Ideas Portal page from the [Port 8443 Filr Administration Console](#) by clicking your user name and selecting the [Ideas Portal](#) link.



You can also view the ideas that others have submitted, add comments, and vote for your favorite product-improvement ideas.

7 Hosting Desktop Application Installation Files on a Separate Server

By default, the Filr server is configured to deploy the Filr desktop application and to provide the auto-update information. As a best practice to minimize load on the Filr server, we recommend that you set up a separate web server and configure it to deploy the desktop application and provide the auto-update information.

- 1 Set up a web server as a host for the Filr desktop application auto-update information.

This web server must be set up so that it does not require authentication.

- 2 Download and extract the `MicroFocusFilrAutoUpdate.tgz` file onto the web server. (You can download the `MicroFocusFilrAutoUpdate.tgz` file from the Filr downloads page on the [Micro Focus Downloads site \(https://download.novell.com\)](https://download.novell.com).)

This compressed file contains all of the files required for installing the Filr desktop application.

For example, if you download this file to the Desktop, extracting the file results in the following directories:

```
https://web_server_DNS_or_IP/filr/desktop/novellfilr/osx
```

```
https://web_server_DNS_or_IP/filr/desktop/novellfilr/windows
```

- 3 (Optional) Ensure that you can access the files on your web server through one of the following methods:

- ◆ From a browser

For example:

```
http://web_server_address/desktopapp/novellfilr/windows/x64/version.json
```

- ◆ From a command line

For example, from the Web server, SSH to the Filr appliance and run the following command:

```
#wget http://web_server_address/desktopapp/novellfilr/windows/x64/  
version.json
```

- 4 Configure the Filr desktop application using the [Port 8443 Administrative Console > System > Desktop Application](#) dialog.

In the **Deploy files accessed via a URL to another location** field, specify one of the following URLs, depending on whether your web server is configured with secure HTTP:

```
https://web_server_DNS_or_IP:8443/file_path/desktopapp/
```

```
http://web_server_DNS_or_IP:8080/file_path/desktopapp/
```

- 5 Click **OK**.

8

KeyShield Integration with Filr

Use the information and instructions in the following sections to configure Filr to work with an existing KeyShield installation.

- ♦ “Prerequisites” on page 51
- ♦ “(Conditional) Allowing the Authorization Connectors to Access the API Key” on page 51
- ♦ “Configuring Filr for KeyShield SSO Support” on page 51
- ♦ “KeyShield Attribute Alias Support” on page 52
- ♦ “Configuring Two-Factor Authentication” on page 53
- ♦ “Downloading and Installing the KeyShield SSO SSL Certificate” on page 54
- ♦ “Testing the KeyShield SSO Configuration” on page 54

Prerequisites

For Filr to work with an existing KeyShield installation, you must have the following already in place.

- ♦ A KeyShield SSO server that is registered with DNS and provides single sign-on services to your network users.
- ♦ An API Key that is displayed in a defined API Authorization configuration.
- ♦ One or more Authentication Connectors (defined on the KeyShield server) that are allowed to be used with the API Key.
- ♦ Administrative Access to the KeyShield server for obtaining the following:
 - ♦ The API Authorization Key associated with the KeyShield Connectors you are leveraging for Filr
 - ♦ The SSL certificate, downloadable as a .CER file for importing into the Filr keystore.

(Conditional) Allowing the Authorization Connectors to Access the API Key

Continuing in the **General** tab (accessed in the previous section), if access to the KeyShield SSO APIs is restricted to users on specific connectors, ensure that the connectors that your Filr users will be connecting through are listed by doing the following:

- 1 If the connectors your users will use are not listed, click the bar below the already-allowed connectors.
- 2 Select the connectors for your users, then click **OK**.


Configuring Filr for KeyShield SSO Support

- 1 Open a new tab or a new browser session to access Filr on port 8443:

`https://filr-ip-address-or-dns-name:8443`

For example `https:192.168.30.150:8443`

Having a new session will let you easily switch between the KeyShield administration console and the Filr Administration console.

- 2 In the new browser session, log in to Filr as an administrator.
- 3 Click the admin link in the upper-right corner of the page, then click the Administration Console icon  .
- 4 In the left frame, click **KeyShield SSO**.
- 5 In the KeyShield SSO Configuration dialog, click **Enable KeyShield SSO**.
- 6 In the **KeyShield Server URL** field, type the access URL for the KeyShield server:
`https://ks-server-dns-name_or_ip-address:ks-server-https-port/`
- 7 Switch to the KeyShield browser-based console, toggle open the API Key, then select and copy the key to your clipboard.
- 8 Switch to the Filr Administration panel and paste the API Key into the **API Authorization** field.
- 9 The **HTTP Connection Timeout** controls how long the Filr Appliance will wait for a response from the KeyShield server before prompting users for their login credentials.
Micro Focus doesn't recommend changing this value unless the connection between the Filr Appliance and the KeyShield SSO server doesn't facilitate a quick response. For example the appliance and server are connected over a WAN.
- 10 In the Connector Names field, type the names of each KeyShield SSO connector that Filr users will connect through.
- 11 Continue with the next section, "[KeyShield Attribute Alias Support](#)."

KeyShield Attribute Alias Support

Filr lets administrators provision users from different LDAP sources, such as eDirectory and Active Directory. It also allows for flexibility in specifying which LDAP attribute will be imported as the Filr username.

In addition to Filr, organizations have email applications, RADIUS clients, and so on, that use different LDAP attributes for their usernames.

KeyShield 6 includes support for **Attribute Aliases**. These let KeyShield match username validation requests from each application with the LDAP attribute that the application uses for its usernames.

A Filr Example

1. Jane Smith logs in through KeyShield's SSO service using `jsmith` (her UID in LDAP) as her Username.
2. Jane then launches Filr.
Unfortunately, the Filr administrator who configured the LDAP import, specified CN as the LDAP username attribute and `JaneSmith` was imported as Jane's Filr username.
3. When Filr tries to authenticate Jane Smith, KeyShield doesn't find her as an authenticated user and the attempt fails.
Jane is then prompted to log in to Filr.
4. To fix the mismatch of LDAP attributes, Jane's KeyShield administrator adds `x-filr = cn` as an **Attribute Alias** in Keyshield.

5. Jane's Filr administrator adds `x-filr` as the **Username Attribute Alias** in Filr.
6. The next time Jane launches Filr after signing in through KeyShield' SSO service, KeyShield verifies to Filr that JaneSmith is authenticated and no additional login is required.

Configuring Attribute Alias Support

- 1 In Keyshield, specify the appropriate **Attribute Alias** for each Authentication Connector.

For example, if your Filr deployment uses the CN attribute as the username for an eDirectory server that is defined as an Authentication Connector in KeyShield, then in the Attribute Alias field in the connector configuration, you would specify

```
x-filr = cn
```

This means that for this Authentication Connector, when authentication verification requests arrive with the Attribute Alias `x-filr`, KeyShield needs to request a match in the CN attributes in the targeted eDirectory Authentication Connector.

- 2 By default, the Filr 2.0 KeyShield SSO Configuration dialog, the Username Attribute Alias is set to `x-filr`.

We strongly recommend that you not change this value. However, if you do, be sure that the name is changed in each KeyShield Authentication Connector configuration as well.

- 3 Continue with "[Configuring Two-Factor Authentication.](#)"

Configuring Two-Factor Authentication

KeyShield 6.1 adds the ability to require a hardware token in addition to usernames and passwords for LDAP users seeking access through a web browser or WebDAV.

NOTE: Two-factor authentication doesn't apply to desktop or mobile device applications.

Filr 2.0 supports KeyShield's two-factor authentication capability through two new options in the KeyShield SSO Configuration dialog:

- ♦ **Require Hardware Token:** Requires a physical token, such as an access card, for access to Filr.

You can also specify the error messages that you want displayed when the required token is either not presented or not recognized by KeyShield for web browser or WebDAV access.

- ♦ **Allow Username/Password based Fallback Authentication (non-SSO) for LDAP Users:**

Allows authentication by entering a username and password as an alternative to the hardware token.

Use this option if you want users to be able to effectively bypass the hardware token requirement by typing in their username and password.

- 1 If you want to configure two-factor authentication for your KeyShield 6.1 SSO service, select the options and specify the text accordingly.
- 2 Click **Test Connection**.
Because the Filr appliance doesn't yet have the KeyShield SSO SSL certificate in its keystore, the test fails.
- 3 Continue with "[Downloading and Installing the KeyShield SSO SSL Certificate](#)" on page 54

Downloading and Installing the KeyShield SSO SSL Certificate

- 1 Open a third browser session and access the Filr appliance on port 9443:
`https://filr-ip-address-or-dns-name:9443`
For example `https:192.168.30.150:9443`
- 2 Log in as `vaadmin`.
- 3 Switch to the KeyShield browser-based console and under General/Web Interface, click Edit.
- 4 Click the **Download** button for the **HTTPS Keystore**.
- 5 Save the `keyshield.cer` file on the workstation running the browser.
- 6 Switch to the browser session opened in [Step 1 on page 54](#) and click the **Appliance Configuration** icon.
- 7 Click the **Digital Certificates** icon.
- 8 Click **File > Import > Trusted Certificate**.
- 9 Click **Browse**, then browse to the location where you saved the `keyshield.cer` file and click **Open**.
- 10 Click **OK** to import the certificate file.
- 11 Acknowledge the message about restarting the appliance by clicking **OK**.
- 12 Click the back arrow in the browser, then select **Reboot**.
- 13 After the system restarts, continue with the next section, [Testing the KeyShield SSO Configuration](#).

Testing the KeyShield SSO Configuration

- 1 Switch back to the Filr administration console (port 8443).
- 2 Click **Test Connection**.
The test should succeed.
- 3 Click **OK** to finalize the configuration and complete the Keyshield SSO integration.

9 Using Multi-Factor Advanced Authentication with Filr

Filr 3.2 introduces Advanced Authentication support for LDAP users. An LDAP user is prompted for additional authentication steps in addition to the typical username and password authentication to log in to Filr provided the Filr administrator has enabled multi-factor authentication on the Filr server.

Non-LDAP users are prompted only for the username and password to log into Filr.

Advanced Authentication is a multi-factor authentication solution that enables you to protect your sensitive data by using a more advanced way of authentication, in addition to the typical username and password authentication. This additional layer of security helps to ensure the identity of a user and reduce the risk of unauthorized access to Filr.

Advanced Authentication provides a single authentication framework that ensures secure access to all your devices with minimal administration. With Advanced Authentication, you can use different types of authenticators such as a Security Question, a PIN, and an OTP to authenticate on diverse platforms.

Authentication comprises the following three factors:

- ◆ Something that you know such as password, PIN, and security questions.
- ◆ Something that you have such as smartcard, token, and mobile phone.
- ◆ Something that you are such as biometrics (fingerprint or iris).

You can achieve multi-factor or strong authentication by using any two factors out of this list. For example, multi-factor authentication can include the combination of a password and a token or a smartcard and a fingerprint.

For more information about using the NetIQ Advanced Authentication Framework and the supported authentication providers, see the [NetIQ Advanced Authentication Framework \(https://www.netiq.com/documentation/advanced-authentication-framework/\)](https://www.netiq.com/documentation/advanced-authentication-framework/) documentation website.

Prerequisites for Using Advanced Authentication with Filr

- A Filr appliance is installed and configured with an advanced-edition license.
- Latest versions of NetIQ Advanced Authentication Framework 5.x or 6.x appliance is installed and configured. For more information, see [Advanced Authentication 5.x](#) or [Advanced Authentication 6.x](#).
- All the Filr clients must be up-to-date with the latest patch installed before enabling multi-factor authentication.

When multi-factor authentication is enabled on a Filr server, users with older versions of the Filr client cannot log into the server and therefore will not receive any system alerts to update the client.

- A valid SSL certificate that is signed by a well-known certificate authority (CA). Self-signed certificates are not supported.

Configuring OAuth2 Event in Advanced Authentication Server Appliance

In the Advanced Authentication Administration Portal, you can configure and manage various authentication settings such as methods, events, and so on. You can also configure various policies that are required for authentication. For more information about configuring Advanced Authentication Server Appliance, see [Advanced Authentication Administration Guide](#) on the [documentation website](#).

To configure:

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

```
https://advanced_authentication_dns_name_or_IP_Address/admin
```

- 2 Add an Active Directory or eDirectory repository where your Filr users are stored.
- 3 Configure an authentication method for Advanced Authentication.

NOTE: The following methods have been tested with Filr.

- ◆ LDAP Password
- ◆ Password
- ◆ SMS OTP
- ◆ Email OTP
- ◆ Security Questions
- ◆ Smartphone
- ◆ TOTP

Other authentication methods that NetIQ Advanced Authentication with OAuth2 event supports would also work, but they have not been explicitly tested.

- 4 Create an authentication chain that is a combination of all the authentication methods that users must pass for successful authentication.
- 5 Configure OAuth2 type event.
 - 5a Specify a name for the event.
 - 5b Enable the event by changing **Is enabled** to **ON**.
 - 5c Select the **OAuth2** event type. The client ID and client secret are generated automatically.
 - 5d 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. See [NetIQ Advanced Authentication Configuration](#) in the [Filr 3.4.1: Administrative UI Reference](#).
 - 5e Select the chains that you want to assign to the event.
 - 5f In the **Redirect URIs** option, specify the following redirect URIs for redirection to 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. See [NetIQ Advanced Authentication Configuration](#) in the [Filr 3.4.1: Administrative UI Reference](#).

5g Click **Save**.

10 Language Settings

- ◆ [“About the Filr Site Default Language” on page 59](#)
- ◆ [“Changing the Language on the Login Page” on page 59](#)

About the Filr Site Default Language

There can be only one default language for the entire Micro Focus Filr site.

When you create Filr users, you can select a locale for each user, which determines the language of each personal profile. However, when users who speak various languages work together on a Filr site, they can often see interface text that is not in their preferred language. For example:

- ◆ Standardized text such as **Home Workspace**, **Global Workspaces**, **Personal Workspaces**, and **Team Workspaces** in the Workspace tree
- ◆ Standardized group names, such as All Users
- ◆ Login page

You cannot change standardized group names, such as All Users. Although the Filr login page can be displayed in only one language, you can change the page’s default language. You must be logged in as the Filr administrator.

Changing the Language on the Login Page

The language of the Filr login page is decided by the Guest user account. Because of this, you can display only one language for your entire Filr site in the login page.

To change the language of the Guest user account and change the language that is displayed on the Filr login page:

- 1 Navigate to the Guest profile.
- 2 On the Profile page, click **Edit**.
The User page is launched.
- 3 In the **Locale** drop-down list, select the language that you want to be displayed on your login page.
Users who log in as Guest view the Filr site in the language that you select.
- 4 Click **OK**.

Each Filr user can change the language on a per-user basis by changing the **Locale** setting in the user profile, as described in [“Modifying Your Profile”](#) in the *Filr 3.4: User Access Guide*.

11 Migrating the Filr's MySQL Database to Microsoft SQL

You can migrate the Filr database from the MySQL database appliance that ships with Filr to an enterprise database.

This section describes how to migrate from the MySQL database appliance to Microsoft SQL.

IMPORTANT: When migrating from the MySQL database appliance to Microsoft SQL, you must first migrate the database schema and then the data as described in this section.

- ♦ “Prerequisites” on page 61
- ♦ “Configuring the Existing Microsoft SQL Database Server” on page 62
- ♦ “Connecting to the MySQL Database Server” on page 62
- ♦ “Connecting to the Microsoft SQL Server” on page 63
- ♦ “Customizing Data Types” on page 63
- ♦ “Migrating the Database Schema” on page 64
- ♦ “Migrating Data” on page 65
- ♦ “Running Post-Migration Scripts” on page 65
- ♦ “Post-Migration Steps” on page 66
- ♦ “Modifying Liquibase Tables” on page 67

Prerequisites

- ♦ Download the latest MySQL Connector/ODBC driver to the Microsoft SQL server. You can get this driver from the [MySQL development website \(http://dev.mysql.com/downloads/connector/odbc/\)](http://dev.mysql.com/downloads/connector/odbc/).

This driver enables you to establish a connection between the MySQL server and the Microsoft SQL server.

- ♦ Download and install the Microsoft SQL Server Migration Assistant for MySQL onto the Microsoft SQL server, as described in the [Microsoft Developer Network \(http://msdn.microsoft.com/en-us/library/hh313147\(v=sql.110\).aspx\)](http://msdn.microsoft.com/en-us/library/hh313147(v=sql.110).aspx).
- ♦ Modify an existing user on the MySQL Appliance so that the user is associated with the IP address or DNS name of the Microsoft SQL server where the Microsoft SQL Server Migration Assistant for MySQL is installed. This can be accomplished via phpMyAdmin or the MySQL appliance.
- ♦ Stop the Filr service on any Filr appliances in the Filr system, as described in “[Managing System Services](#)” in the *Filr 3.4.1: Administrative UI Reference*.

Configuring the Existing Microsoft SQL Database Server

For information regarding which versions of the Microsoft SQL database Filr supports, see “[SQL Database Server](#)” in the *Filr 3.4: Installation, Deployment, and Upgrade Guide*.

To configure an existing Microsoft SQL database to be used with your Filr system:

- 1 Enable remote access to the Microsoft SQL database server.
- 2 Open port 1433 on the Windows firewall where the database is running.
- 3 Identify a user account configured with SQL Server Authentication and that this user has sufficient rights to manage the Filr database.
Filr supports only SQL Server Authentication. Filr does not support Windows Authentication or Windows Domain User Authentication to Microsoft SQL.
- 4 Using Microsoft SQL Server Management Studio, create a new database to use as the Filr database.

Select the Master database in the list of databases, then paste the following script into the **New Query** window and execute it to create the new Filr database:

```
USE master;
GO
IF DB_ID (N'filr') IS NOT NULL
DROP DATABASE filr;
GO
CREATE DATABASE filr
COLLATE Latin1_General_100_BIN;
GO

--Verify the collation setting.
SELECT name, collation_name FROM sys.databases WHERE name = N'filr';
GO
```

If your database name is something other than `filr`, replace `filr` with the name of your database in the script.

- 5 Continue with “[Connecting to the MySQL Database Server](#)” on page 62.

Connecting to the MySQL Database Server

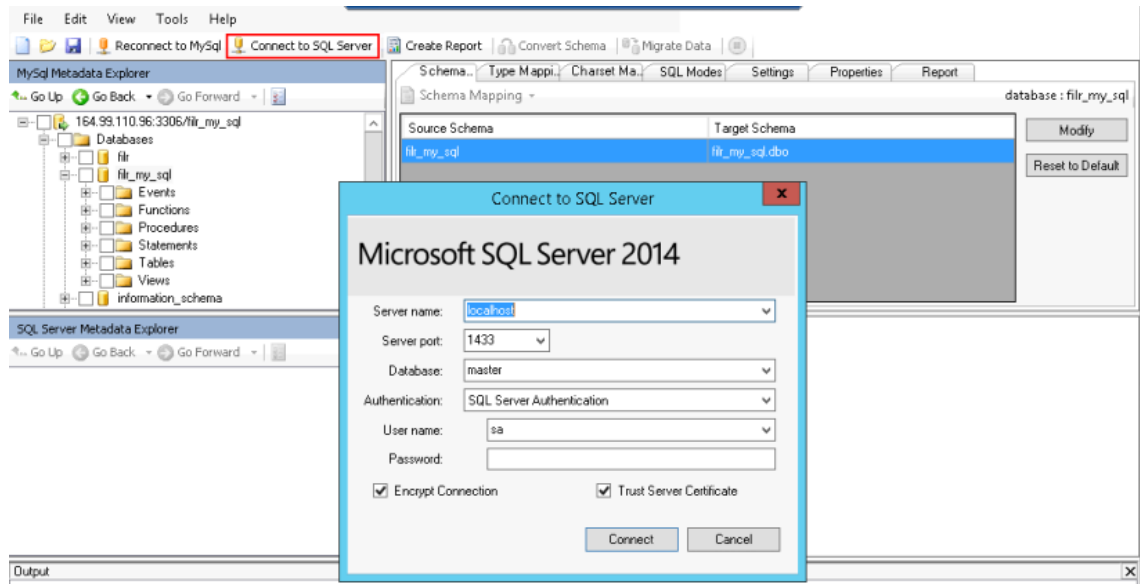
- 1 On the Microsoft SQL server, launch the Microsoft SQL Server Migration Assistant for MySQL.
- 2 Create a new project by clicking **File > New Project**.
The New Project dialog box is displayed.
- 3 Accept the defaults for the project by clicking **OK**.
- 4 Click **Connect to MySql**.
The Connect to MySql dialog box is displayed.
- 5 In the **Provider** drop-down list, select the **MySQL ODBC 5.3 Unicode Driver (v5.3.x)**.
This option must be selected because the Filr database uses a Unicode character set.
- 6 In the **Server name** field, specify the IP address of the MySQL database appliance that you are migrating from.
- 7 Specify the user name and password for the MySQL database, then click **Connect**.

A connection to the MySQL server is established.

- Continue with [“Connecting to the Microsoft SQL Server”](#) on page 63.

Connecting to the Microsoft SQL Server

- In the **MySQL Metadata Explorer** window, browse to and select your MySQL database.
- Click **Connect to SQL Server**.



- Accept the defaults for connecting to the Microsoft SQL server, then specify the user name and password for a user with sufficient rights on the database.
- Click **Connect**.
A connection to the Microsoft SQL server has been established.
- Continue with [“Customizing Data Types”](#) on page 63.

Customizing Data Types

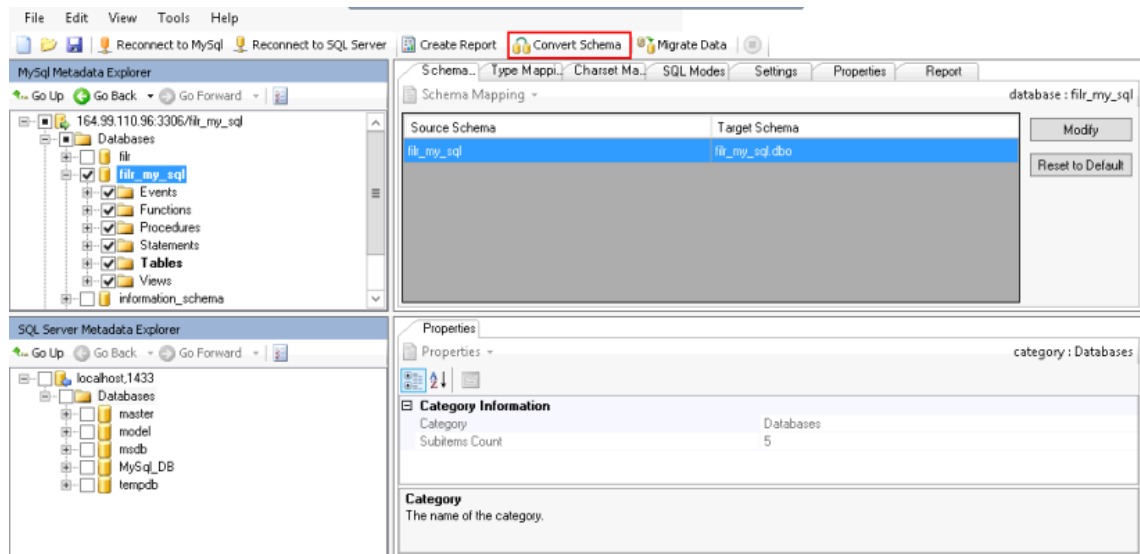
- On the Microsoft SQL server, launch the Microsoft SQL Server Migration Assistant for MySQL.
- Click **Tools > Project Settings**.
The Project Settings dialog box is displayed.
- Click **Type Mapping**, select **bigint(*..255)** in the **Source Type** column, then click **Edit**.
The Edit Type Mapping dialog box is displayed.
- In the **Target Type** drop-down list, select **Numeric (Precision, Scale)**.
- In the **Precision** section, specify 19.
- In the **Scale** section, specify 0, then click **OK**.
- Select **datetime** in the **Source Type** column, then click **Edit**.
The Edit Type Mapping dialog box is displayed.
- In the **Target Type** drop-down list, select **datetime**, then click **OK**.

- 9 Click **Apply** > **OK**.
- 10 Continue with “[Migrating the Database Schema](#)” on page 64.

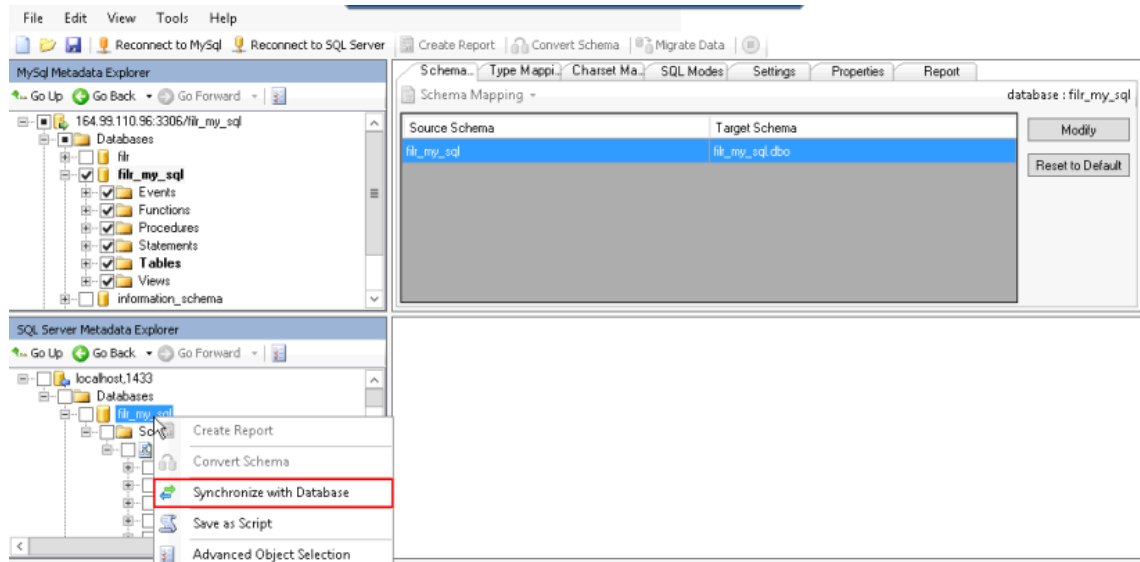
Migrating the Database Schema

- 1 In the MySQL Metadata Explorer window, select the Firl MySQL database and tables that you want to migrate, then click **Convert Schema**.

This creates the database schema on the target Microsoft SQL server. Ensure that the target schema has the *database_name* with a .dbo extension. If the target schema does not have the *database_name* or has an extension other than .dbo, then click **Modify** and select the correct schema.



- 2 In the SQL Server Metadata Explorer section, right-click the MySQL database that you are migrating, then click **Synchronize with Database**.



- 3 In the Synchronize with the Database dialog box, verify that the tables will be created, then click **OK**.
- 4 Continue with [“Migrating Data” on page 65](#).

Migrating Data

- 1 In the MySQL Metadata Explorer window, select the Filr MySQL database and tables that contain the data that you want to migrate. Right-click and select **Migrate Data**.
To avoid timeout errors, migrate large tables individually, as described in [Step 6](#).
The Connect to MySQL dialog box is displayed.
- 2 Accept the defaults for connecting to the Microsoft SQL server, then specify the user name and password for a user with sufficient rights on the database.
- 3 Click **Connect**.
The Connect to SQL Server dialog box is displayed.
- 4 Accept the defaults for connecting to the Microsoft SQL Server, then specify the user name and password for a user with sufficient rights on the database.
- 5 Click **Connect**.
The data is migrated. Depending on the amount of data and number of tables in your database, this process can take a few minutes.
After the migration finishes, the Data Migration Report is displayed. You can save the report for your records, or close it without saving.
- 6 (Optional) To migrate individual tables, repeat [Step 1](#) through [Step 5](#) and select the table that you want to migrate in the MySQL Metadata Explorer window.
- 7 Run the following queries in sequence against the migrated database using the SQL Query Editor of the Microsoft SQL Server:

```
ALTER DATABASE filr SET SINGLE_USER WITH ROLLBACK IMMEDIATE;  
ALTER DATABASE filr COLLATE Latin1_General_CI_AS_KS_WS;  
ALTER DATABASE filr SET MULTI_USER;  
SELECT name, collation_name FROM sys.databases WHERE name = N'filr';
```


If your database name is something other than `filr`, replace `filr` with the name of your database.
These queries must be successfully executed in the correct order before continuing.
- 8 Continue with [“Running Post-Migration Scripts” on page 65](#).

Running Post-Migration Scripts

- 1 After the database schema and data is successfully migrated, run the post-migration script (`MySQL_MSSQL_Post_Migration.sql`) on the migrated database by using the SQL Query Editor of the Microsoft SQL Server. You can download the script [here](#) or from the Micro Focus Customer Center.

IMPORTANT: Use this script on a Filr site that is currently on Filr 3.4 or later. If you are running a different version / patch-level of Filr, do not use this script and consult the Micro Focus Customer Care team.

After running the script, you should see the following message in the SQL Query Editor for both the Parse and Execute actions:

```
Command(s) completed successfully.
```

- 2 Continue with [“Post-Migration Steps” on page 66](#).

Post-Migration Steps

IMPORTANT: In a large Filr deployment with multiple Filr appliances, this procedure must be done for each Filr appliance in the Filr system.

- 1 Access the Micro Focus Filr appliance at port 9443.

For example, `https://ip_address_or_DNS:9443`

Use the IP address or DNS name of the server that you specified during the appliance installation.

- 2 Log in to the appliance using the `vaadmin` user and the password that you set.



- 3 Click the **Filr Server Configuration** icon.

The Filr Server Configuration page is displayed.

- 4 Click **Database**.

- 5 In the **Database Type** drop-down, select **SQLServer**.

- 6 Change the **Host Name or IP Address** and **Port** fields to match the new host name or IP address and port number for the Microsoft SQL server.

- 7 Change the **User Name** and **User Password** fields to match that of a user on with sufficient rights on the Microsoft SQL server.

- 8 Click **OK** to save the new database configuration settings.

In the Configuration Summary, verify that the database information has changed.

- 9 Click **Reconfigure Filr Server**.

- 10 Repeat this process for each Filr appliance in the Filr system.

- 11 Continue with [“Modifying Liquibase Tables” on page 67](#).

Modifying Liquibase Tables

Filr ships with Liquibase scripts that validate database schema, keep track of schema changes, compare changes with the reference database, and so forth. In order to use these scripts, the Liquibase tables need to be deleted and re-created. (This is because the Liquibase tables contain metadata specific for the MySQL database that you are migrating from.)

You need to remove the MySQL tables and create new tables that are compatible with the Microsoft SQL database.

- 1 Delete the Liquibase tables (`databasechangelog` and `databasechangeloglock`) from the migrated MSSQL database.
- 2 Modify the `sqlserver-liquibase.properties` file and set the database password to be clear text so that it can be read by the Liquibase scripts:

2a SSH to the Filr appliance and log in to the appliance as the root user.

2b In the console of the Filr appliance, change to the `/filrinstall/db` directory.

2c Make a copy of the `sqlserver-liquibase.properties` file.

For example, to copy the file to the root partition:

```
cp sqlserver-liquibase.properties /
```

2d Open the `sqlserver-liquibase.properties` file in a text editor.

For example, you can use the vi Editor to edit the file:

```
vi sqlserver-liquibase.properties
```

2e Change the password value to the password of the Microsoft SQL database.

2f Save and close the `sqlserver-liquibase.properties` file.

In the vi Editor, you can type the following command when in command mode:

```
:wq
```

- 3 Run the `manage-database.sh` script with the `markDatabaseAsUpdated` switch.

This creates the Liquibase tables and populates them with the definitions read from the Microsoft SQL version of the changelog files that are available in the Filr installation directory.

To run the `manage-database.sh` script with the `markDatabaseAsUpdated` switch:

3a SSH to the Filr appliance and log in to the appliance as the root user.

3b Run following commands:

```
cd /filrinstall/db
```

```
sh /filrinstall/db/manage-database.sh sqlserver markDatabaseAsUpdated
```

- 4 Perform the final validation by running `manage-database.sh` with the `updateDatabase` switch.

To run the `manage-database.sh` script with the `updateDatabase` switch:

4a SSH to the Filr appliance and log in to the appliance as the root user.

4b Get Executable permission to the `manage-database.sh` script by running the following commands:

```
cd /filrinstall/db/
```

```
chmod x+ manage-database.sh
```

4c Run following commands:

```
sh /filrinstall/db/manage-database.sh sqlserver updateDatabase
```

```
sh /filrinstall/db/manage-database.sh sqlserver validate
```

The Liquibase script should find no need to perform any further schema changes, and this run should complete without making any changes and without any errors.

- 5 Replace the `sqlserver-liquibase.properties` file that you edited in [Step 2d](#) with the one that you copied in [Step 2c](#).
- 6 Start the Filr service on any Filr appliances in the Filr system, as described in “[Managing System Services](#)” in the *Filr 3.4.1: Administrative UI Reference*.
- 7 Users can now access the Filr site at port 8443.

For example, `https://ip_address_or_DNS:8443`

12 Mobile Device Management

- ◆ “Key-Value Pairs” on page 69
- ◆ “Configuring ZMM to Manage the Filr App” on page 71
- ◆ “Configuring MobileIron to Manage the Filr App” on page 71
- ◆ “Managing Mobile Devices with Filr” on page 76

NOTE: If the Filr server uses a self-signed certificate, then you cannot preview some applications such as .pdf, .odt, .odp, .dwg on an iOS device. To preview these applications on an iOS device, you must ensure that the Filr server uses a valid SSL certificate that is signed by a well-known certificate authority (CA).

Key-Value Pairs

Key-value pairs allow you to populate user login information and set configuration options, such as whether the Filr app allows for opening into other apps or copying information to other apps.

Select the key-value pairs depending on your MDM solution for setting the configuration options. For example, if you are using MobileIron as your MDM solution, you can set configuration options for opening into third-party apps by using the MobileIron interface.

Table 12-1 Filr Key-Value Pairs

Key	Value
server	Specify the URL of your Filr site. For example, <code>filr.acme.com</code> .
username	Specify <code>\$(USERNAME)</code> to cause MDM to automatically populate the app with the user’s MDM user ID. Alternatively, you can specify an individual user’s user ID.
password	(optional) Specify <code>\$(PASSWORD)</code> to cause MDM to automatically populate the app with the user’s MDM password. Alternatively, you can specify an individual user’s password.
configLocked	The value is true or false. If the value is true, the app users cannot modify the settings of the Filr app on their devices.
allowOpenIn	Specify 1 as the value if you have disabled Open In or Send To support for the mobile apps in the Filr administration console, but you want to allow the Filr secure app to integrate with other secure apps. A value of 1 indicates that users can open Filr files into any secure app. A value of 2 allows you to designate specific apps that users can open Filr files into. You do this by creating a whitelist of apps using the <code>openInWhitelist</code> key.

Key	Value
openInWhitelist	<p>Specify 1 as the value if you want to allow the Filr secure app to integrate with only the specific secure apps that you designate. To designate apps for the whitelist, specify the applications' bundle ID (for iOS apps) and package name (for Android apps) in a comma-delimited list.</p> <p>In order for the <code>openInWhitelist</code> values to be recognized, the value for the <code>allowOpenIn</code> key must be set to 2.</p> <p>An easy way to find the package name for an Android app is to install the <code>Package Name Viewer</code> app from the Google Play store. This app displays the package name for each app that is currently installed on the device.</p> <p>To find the bundle ID for an iOS app:</p> <ol style="list-style-type: none"> (Conditional) If the app for which you want to location the bundle ID has not yet been synchronized to iTunes from your device, you must sync the device with iTunes. In your iTunes library on your Mac or PC, open the <code>Mobile Applications</code> folder. <p>On a Mac, this is usually in your Home directory, at the following location: <code>~/Music/iTunes/Mobile Applications/</code></p> <p>On Windows 7, this is usually at the following location: <code>C:\Users\username\My Music\iTunes\Mobile Applications/</code></p> In the <code>Mobile Applications</code> folder, locate the app for which you want the bundle ID. Create a copy of the file, and re-save the copy as a <code>.zip</code> file. Unzip the newly created <code>.zip</code> file. <p>You now see a folder by the name of the application name.</p> Locate the <code>iTunesMetadata.plist</code> file within the folder and open it in a text editor. Locate the <code>softwareVersionBundleid</code> key within the file. <p>The string value below this key is the bundle ID.</p>
allowCutCopy	Specify 1 as the value if you want users to be able to copy information from the Filr app and paste it into other apps.

Sample Format of the Configuration File

```
<dict>
  <key>server</key>
  <string>filr.acme.com</string>
  <key>username</key>
  <string>admin</string>
  <key>password</key>
  <string></string>
  <key>configLocked</key>
  <string>>true</string>
</dict>
```

Configuring ZMM to Manage the Filr App

IMPORTANT: ZENworks Mobile Management (ZMM) can be used with the iOS and Android Filr mobile apps with the following version requirements:

- ◆ **Android requirements:** Filr mobile app 1.0.3 or later with Android 4.1 or later.
- ◆ **iOS requirements:** Filr mobile app 1.0.4 or later with iOS 8.0 or later.

For information about how to configure ZMM to manage the Filr app, see “[Micro Focus Filr \(http://www.novell.com/documentation/zenworksmobile29/pdfdoc/zen_mobile_organization_admin.pdf#page=41\)](http://www.novell.com/documentation/zenworksmobile29/pdfdoc/zen_mobile_organization_admin.pdf#page=41)” in the *ZENworks Mobile Management 2.9.x Organization Administration Guide* (http://www.novell.com/documentation/zenworksmobile29/pdfdoc/zen_mobile_organization_admin.pdf).

Configuring MobileIron to Manage the Filr App

- ◆ “[MobileIron Environment Support](#)” on page 71
- ◆ “[Device-Specific Support Information](#)” on page 71
- ◆ “[Adding the Filr App to MobileIron](#)” on page 72
- ◆ “[Pre-Populating Fields for Filr Login](#)” on page 73
- ◆ “[Configuring Data Loss Prevention Policies](#)” on page 75
- ◆ “[Distributing the Filr App to Devices](#)” on page 76
- ◆ “[Preventing Frequent Prompts for a Passcode](#)” on page 76

MobileIron Environment Support

The Filr 3 mobile apps have been validated in the following MobileIron environments:

- ◆ Sentry-AppTunneling
- ◆ MobileIron 8.4 AppConnect

Device-Specific Support Information

When using MobileIron to manage the Filr app, the following features are supported:

iOS Supported Features

- ◆ Populate the **Server IP Address** field for login
- ◆ Populate the **User ID** field for login
- ◆ Open In support to allow or disallow users to open files in other applications

If you are using MobileIron to manage devices in your organization, the Open In setting exists both in the Filr administration console and in the MobileIron administration console. This setting should be consistent in both locations (if it is enabled in Filr, it should also be enabled in MobileIron). The one exception to this rule is if you want Open In functionality to be enabled for devices that are being managed by MobileIron and disabled for devices that are not being managed by MobileIron. To achieve this, you can enable this setting in MobileIron and disable it

in Filr. In this case, only devices that are being managed by MobileIron are able to use Open In functionality; devices that are not being managed by MobileIron are not able to use Open In functionality.

To configure Open In functionality for all users, see “[Mobile Device Access—Default Settings](#)” in the [Filr 3.4.1: Administrative UI Reference](#). To configure Open In functionality for individual users and groups, see

Android Supported Features

- ◆ Populate the **Server URL** field for login
- ◆ Populate the **User ID** field for login
- ◆ Populate the **User Password** field for login

Adding the Filr App to MobileIron

- ◆ “[Adding the Android Filr App](#)” on page 72
- ◆ “[Adding the iOS Filr App](#)” on page 73

Adding the Android Filr App

To add the Android Filr app to MobileIron, you need to upload the `.apk` file and then apply the Android label to the application:

- 1 Download the `.apk` file for the Filr mobile app from the Micro Focus downloads site.
- 2 Upload the file to MobileIron.
 - 2a In the MobileIron Admin Portal, click the **Apps** tab.
 - 2b On the **App Distribution Library** tab, in the **Select Platform** drop-down list, select the platform for the app that you want to add. For example, if you are uploading the Filr mobile app for Android, select **Android**.
 - 2c Click **Add App**.

The Add App Wizard is displayed.
 - 2d Click **Next**, then specify the following information:
 - Distribution Type:** Select **In-house App**.
 - Silently Install:** If your device supports a silent install, you can select **Yes**. If the device does not support a silent install or you are unsure, select **No**.
 - App Upload:** Browse to and select the `.apk` file that you downloaded in [Step 1](#).
 - 2e Click **Next**, then specify the following information:
 - App Name:** `Micro Focus Filr` is already specified for you. This cannot be changed.
 - Display Version:** The version is already specified for you. This cannot be changed.
 - Code Version:** The version is already specified for you. This cannot be changed.
 - Description:** Specify a short description for the app.
 - Override URL:** For information about this feature, see the blue information icon next to this field.
 - Featured:** Select whether you want to feature this app.
 - Category:** Select the category that most closely matches the app. You can add a new category as described in the dialog box.

- 2f Click **Next**, then click **Browse** to upload any screen shots that you have for the app.
The mandatory image size is displayed in the dialog box.
 - 2g Click **Finish** to close the Add App Wizard.
 - 3 Apply the Android label to your application:
 - 3a From the **App Distribution Library** tab on the **Apps** tab, select the Micro Focus Filr app that you just created, then click **Actions** > **Apply To Label**.
The Apply To Label dialog box is displayed.
 - 3b Select the **Android** label, then click **Apply** > **OK**.

Adding the iOS Filr App

To add the iOS Filr app to MobileIron, you need to import it from the Apple Appstore and then apply the iOS label to the application:

- 1 Import the app from the Apple Appstore.
 - 1a In the MobileIron Admin Portal, click the **Apps** tab.
 - 1b On the **App Distribution Library** tab, in the **Select Platform** drop-down list, select **iOS**.
 - 1c Click **App Store Import**.
The App Store Search dialog box is displayed.
 - 1d In the **App Name** field, type `Micro Focus Filr`.
 - 1e In the **App Store** field, select the country appropriate to your location.
 - 1f Click **Search**.
 - 1g Click **Import** next to the Micro Focus Filr app, then click **OK** after it is imported.
 - 1h Close the App Store Search dialog box.
 - 1i From the **App Distribution Library** tab on the **Apps** tab, click the **Edit** icon next to the Micro Focus Filr app that you just imported.
The Edit App for iOS dialog box is displayed.
 - 1j Make any desired changes to the app details and icon, then click **Save**.
- 2 Apply the iOS label to your application:
 - 2a From the **App Distribution Library** tab on the **Apps** tab, select the Micro Focus Filr app that you just created, then click **Actions** > **Apply To Label**.
The Apply To Label dialog box is displayed.
 - 2b Select the **iOS** label, then click **Apply** > **OK**.

Pre-Populating Fields for Filr Login

You can pre-populate the fields on the Filr login screen for users in your system by configuring the Filr key-value pairs in MobileIron. You can pre-populate the server URL and user ID fields for both the iOS and Android apps. For the Android app, you can also pre-populate the user password field.

You accomplish this within MobileIron by modifying the app configuration for Android, and by creating a new app configuration for iOS.

- ◆ [“Modifying the Android Filr App Configuration for MobileIron” on page 74](#)
- ◆ [“Creating the iOS Filr App Configuration for MobileIron” on page 74](#)
- ◆ [“Key-Value Pairs” on page 74](#)

Modifying the Android Filr App Configuration for MobileIron

- 1 In the MobileIron Admin Portal, click the **Policies & Configs** tab.
- 2 On the **Configuration** tab, in the **Name** column, click the name of the Filr configuration for the Filr app that you uploaded, as described in [“Adding the Android Filr App” on page 72](#).
- 3 Click **Edit**.
The Modify AppConnect App Configuration dialog is displayed.
- 4 Specify the following information:
 - Name:** Provide a name for the configuration, or keep the default.
 - Description:** (Optional) Provide a description for the configuration, or keep the default.
 - Application:** Select `Micro Focus Filr` from the drop-down list.
- 5 In the **App-specific Configurations** section, keep or remove the key-value pairs that are shown in [“Key-Value Pairs” on page 69](#). Key-value pairs that remain in the table represent the information that will be pre-populated for Filr login.
- 6 Click **Save**.

Creating the iOS Filr App Configuration for MobileIron

- 1 In the MobileIron Admin Portal, click the **Policies & Configs** tab.
- 2 On the Configuration tab, click **Add New > AppConnect > Configuration**.
The New AppConnect App Configuration dialog box is displayed.
- 3 Specify the following information:
 - Name:** Provide a name for the configuration, such as `Filr iOS Configuration`.
 - Description:** (Optional) Provide a description for the configuration.
 - Application:** Specify the Filr iOS bundle ID, which is `com.novell.vibefilr`.
- 4 In the **App-specific Configurations** section, click the **Plus** icon to add a new field to the key-value pair table; you can then specify the key-value pair to be included in the configuration. The key-value pairs that you can add are shown in [“Key-Value Pairs” on page 69](#). Key-value pairs that you add to the table represent the information that will be pre-populated for Filr login.
- 5 Click **Save**.

Key-Value Pairs

If you modify key-value information after the Filr app has already been pushed to user devices, devices where the app is already installed are not refreshed with the updated information.

The key-value pairs are server, username, and password. For more details, see [“Key-Value Pairs” on page 69](#).

Configuring Data Loss Prevention Policies

You can configure policies to restrict users from performing actions that could lead to data loss. For iOS devices, you can restrict users' ability to print, copy or paste, and open in other apps. For Android, you can restrict users' ability to take a screen capture.

You accomplish this within MobileIron by modifying the app policy for Android, and by creating a new app policy for iOS.

- ♦ [“Modifying the Android Filr App Policy for MobileIron” on page 75](#)
- ♦ [“Creating the iOS Filr App Policy for MobileIron” on page 75](#)

Modifying the Android Filr App Policy for MobileIron

- 1 In the MobileIron Admin Portal, click the **Policies & Configs** tab.
- 2 In the **Name** column, click the name of the Filr policy for the Filr app that you uploaded, as described in [“Adding the Android Filr App” on page 72](#).
- 3 Click **Edit**.
The Modify AppConnect App Container Policy dialog is displayed.
- 4 Specify the following information:
Name: Provide a name for the policy, or keep the default.
Description: (Optional) Provide a description for the policy, or keep the default.
Application: Select `Micro Focus Filr` from the drop-down list.
- 5 In the **Data Loss Prevention Policies** section, you can change the following configuration option for Android devices:
Screen Capture: Allow users to take a screen capture from within any AppConnect app (including Filr).
- 6 Click **Save**.

Creating the iOS Filr App Policy for MobileIron

- 1 In the MobileIron Admin Portal, click the **Policies & Configs** tab.
- 2 On the Configuration tab, click **Add New > AppConnect > Container Policy**.
The New AppConnect App Configuration dialog box is displayed.
- 3 Specify the following information:
Name: Provide a name for the policy, such as `Filr iOS Policy`.
Description: (Optional) Provide a description for the policy.
Application: Specify the Filr iOS bundle ID, which is `com.novell.vibefilr`.
- 4 In the **Data Loss Prevention Policies** section, you can change the following configuration options for iOS devices:
Print: This setting is not honored in the Filr app. There is no printing ability from within the Filr app.
Copy/Paste To: This setting is ignored in this release of the Filr mobile app. Copy/Paste functionality is included in the Open In setting. In other words, you must disable Open In in order to disable Copy/Paste.

Open In: Allow users to use the Open In functionality. If allowed, specify whether users can open into all apps on the device, only into AppConnect apps, or only into a list of apps that you specify.

To specify individual apps via the whitelist option, specify the apps bundle ID. For example, the bundle ID for the Pages app is `com.apple.iwork.pages`.

5 Click **Save**.

Distributing the Filr App to Devices

You need to distribute the Filr app to devices in your organization via MobileIron if this is the first time your organization is using MobileIron with Filr, or any time a new device enters the organization.

It is possible that some users independently download the Filr app from the app store before their device is managed by MobileIron. In this case, you still need to push the app to their device via MobileIron. (These devices will lose any cached or downloaded files within the Filr app after their device becomes managed and the Filr app is pushed to their device.)

Preventing Frequent Prompts for a Passcode

Each time the Filr app checks in with MobileIron, it is briefly forced into the background by the MobileIron app. This happens so quickly, that users might not notice unless they are looking directly at the screen.

When the Filr app returns to the foreground, if it is set to require an Access Passcode/PIN, the user is prompted for the code.

To control how often app users are interrupted, access the MobileIron administrative console and adjust the [Global Policy > App Check-in Interval](#).

Managing Mobile Devices with Filr

You can view users who have accessed your Filr system from a mobile device, and if necessary, wipe all Filr data from the user's device.

For more information, see [Viewing, Wiping, and Disconnecting Registered Clients](#).

13 Monitoring

For information on all Filr monitoring capabilities, see “Logging and Monitoring” in the *Filr 3.4.1: Administrative UI Reference*.

- ♦ “Enabling Debug Logging” on page 77
- ♦ “Monitoring with Ganglia” on page 79
- ♦ “Monitoring File Meta-Data Synchronization in a Filr Cluster” on page 84
- ♦ “Monitoring the Indexing Process” on page 85
- ♦ “Monitoring User Access, including the Guest User” on page 86

Enabling Debug Logging

IMPORTANT: Do not adjust the settings described in this section unless you are instructed to do so by a Filr support engineer.

Adjusting the settings without guidance from Filr support can negatively impact the performance of your Filr deployment.

- ♦ “Enabling Debug Logging for Filr” on page 77
- ♦ “Enabling Debug Logging for FAMT” on page 78
- ♦ “Configuring Debug Logging for SMB Communications” on page 78

Enabling Debug Logging for Filr

IMPORTANT: These steps should only be followed in consultation with a Filr support engineer.

- 1 In a text editor, open the `log4j.properties` file from the following directory:

```
/opt/novell/filr/apache-tomcat/conf
```

- 2 Uncomment each line for which you want to enable debug logging in the `log4j.properties` file.

For example, to trace file synchronization and accesses through mirrored folders, uncomment the following lines in the `log4j.properties` file:

```
log4j.category.com.novell.teaming.module.folder.impl.PlusFolderModule=DEBUG
log4j.category.org.kablink.teaming.module.file.impl.FileModuleImpl=DEBUG
log4j.category.org.kablink.teaming.fi=DEBUG
log4j.category.com.novell.teaming.fi=DEBUG
log4j.category.com.novell.teaming.repository.fi=DEBUG
```

To trace interactions with resource drivers, uncomment the following lines in the `log4j.properties` file:

```
log4j.category.org.kablink.teaming.util.TraceableInputStreamWrapper=DEBUG
log4j.category.com.novell.teaming.fi.TraceableAclResourceDriverWrapper=DEBUG
log4j.category.com.novell.teaming.fi.TraceableAclResourceSessionWrapper=DEBUG
```

- 3 Monitor the `/var/opt/novell/tomcat-filr/logs/appserver.log` file.
- 4 Restart the Filr service.

Enabling Debug Logging for FAMT

IMPORTANT: The instructions in this section should only be followed in consultation with a Filr support engineer.

- ◆ [“Setting Debug Logging for FAMT” on page 78](#)
- ◆ [“Viewing FAMT Log Files” on page 78](#)
- ◆ [“Clearing FAMT Log Files” on page 78](#)

Setting Debug Logging for FAMT

- 1 From the command line of the Filr appliance, change to the following directory:

```
/opt/novell/filr/bin
```

- 2 Set the FAMT log level as follows:

```
./famtconfig -s loglevel 4
```

or

To view the current log level:

```
./famtconfig -g loglevel
```

Viewing FAMT Log Files

- 1 Change to the following location on the Filr server:

```
/var/opt/novell/filr/log
```

The `famtd.log`, `debug`, and `core` files are available for debugging functionality issues related to FAMT.

Clearing FAMT Log Files

- 1 Run the following command to clear the log files:

```
/etc/logrotate.d/novell-famt-logs
```

FAMT logs are rotated after the log size exceeds 5MB.

Configuring Debug Logging for SMB Communications

IMPORTANT: These steps should only be followed in consultation with a Filr support engineer.

The `/var/opt/novell/filr/log/smbclient.log` log file captures SMB/CIFS communications with Net Folders on Windows and Micro Focus OES servers (including OES for NSS AD).

About the smbclient.log File

Filr support engineers use the information captured in the `smbclient.log` file to troubleshoot SMB communication issues.

Log levels can range from 1 (the default) to 10. Each increase in level causes the system to log additional information.

The `smbclient.log` file gets rotated to `smbclient.log.old` when it reaches approximately 5 MB in size. Depending on the scope of the issue being addressed, your Filr support engineer might instruct you to increase the log-file size setting by modifying the `max log size` parameter under the `[global]` section of the `smb.conf` file.

Your Filr support engineer might also ask you to redirect log output to another file by using the following command at the terminal prompt: `# tail -F /var/opt/novell/filr/log/smbclient.log >> file-name-with-path`

Changing the Debug Level

As directed by a Filr support engineer, do the following:

- 1 At the appliance terminal prompt, launch a text editor such as VI and open the `smb.conf` file located here:

```
/etc/opt/novell/filr/.smb/smb.conf
```

- 2 Add a parameter to control the SMB log level by inserting the following line under the `[global]` section in `smb.conf`:

```
log level = number-specified-by-Filr-support-engineer
```

- 3 Save the `smb.conf` file.

- 4 Restart `famtd` by entering the following command:

```
# rcnovell-famtd restart
```

- 5 After your support issue is resolved, ensure that you reset the log level to 1 and restart `famtd` by using the instructions above.

Monitoring with Ganglia

Ganglia is a scalable, distributed monitoring system that lets you gather important metric data about your Filr system's performance. The default metrics that you can monitor are CPU, disk, load, memory, network, and process.

You can view metrics for individual nodes or for multiple Filr nodes that are running in a clustered environment:

For information about how to configure Ganglia for your environment, including changing from multicast mode to unicast mode, see [“Changing the Ganglia Monitoring Configuration”](#) in the *Filr 3.4.1: Administrative UI Reference*. [Accessing Filr System Log Files](#)

- ◆ [“Ganglia Monitoring Tips”](#) on page 80
- ◆ [“Viewing Metrics for an Individual Node”](#) on page 80
- ◆ [“Viewing Metrics for Multiple \(Clustered\) Filr Nodes”](#) on page 80
- ◆ [“Filr Monitoring Metrics”](#) on page 81
- ◆ [“Configuring Ganglia to Monitor MySQL or MariaDB Database”](#) on page 83

Ganglia Monitoring Tips

- ◆ When reading the Ganglia chart, make sure to factor in the units as well.
For example, 15 M x kb is not 15 MB. Rather, it is 15,000,000 kb or 15 GB. Units are shown to the left of the Y-axis.
- ◆ When viewing a Ganglia graph, take into consideration the actual sequence of system events that occurred on the appliance. This provides insight into the events that are reflected in the graph.
- ◆ Make sure that you have a good understanding of the timeline of events reflected in a graph by first studying the applicable logs and then interpreting the graph.

Viewing Metrics for an Individual Node

You can view metrics for individual nodes in your Filr system, including the Filr appliance, search index appliance or database appliance.

Path: [Port 9443 Appliance Console](#) > [Ganglia Monitoring icon](#) > [Grid-Node drop-down list](#) > *select an appliance*

Table 13-1 Individual Node Ganglia Monitoring

Field, Option, or Button	Information and/or Action
Host Overview section	◆ Displays graphs of appliance load, memory usage, CPU percentage, and network traffic.
Gray bar	◆ You can set how the detailed graphs that follow are displayed: the number of columns and the graph size. The larger the graphs, the more detail is available.
Detailed Graphs	◆ The metrics available depend on the appliance type. ◆ For definitions of the available metrics, see " Filr Monitoring Metrics " on page 81 .

Viewing Metrics for Multiple (Clustered) Filr Nodes

If your Filr site is running in a clustered environment, use this to see information about a particular metric for all Filr nodes in a combined view:

Path: [Port 9443 Appliance Console](#) > [Ganglia Monitoring icon](#) > [Aggregate Graphs](#)

Table 13-2 Using the Aggregate Graphs Tab

Field, Option, or Button	Information and/or Action
Create aggregate graphs	<ol style="list-style-type: none">1. Specify the appropriate information for the following fields to create the aggregate graph.2. Graph Type: Select whether you want a line or stacked graph to be created. Legend options: Select whether to show or hide the legend.3. Click Create Graph.

Field, Option, or Button	Information and/or Action
◆ Title:	◆ The title that you want on the generated aggregate graph.
◆ Vertical (Y-Axis) label:	◆ The label you want on the Y-axis of the graph.
◆ Limits	◆ The lower and upper limits of the Y-axis (the scale of the graph).
◆ Host Regular expression:	◆ The nodes you want to compare, separated by a vertical bar (). Use the node names as shown in Ganglia.
◆ Metric Regular expression:	◆ The name of the metric defined in Ganglia that you want to view. ◆ Type any lower-case letter in the field and select the metric you want. “ Filtr Monitoring Metrics ” on page 81 provides definitions for many of the metrics listed.
◆ Graph Type:	◆ Specify Line or Stacked .
◆ Legend Options:	◆ Specify whether to show or hide the legend
◆ Create Graph button	1. When you have everything set the way you want it, click this. 2. To save the graph for future use, click Direct Link to this aggregate graph , then save the resulting URL.

Filtr Monitoring Metrics

- ◆ “[Filtr Appliance Metrics](#)” on [page 81](#)
- ◆ “[Filtrsearch Appliance Metrics](#)” on [page 82](#)

Filtr Appliance Metrics

Total Failed Logins: Number of failed logins from the web client since the server started.

This does not include failed logins from the Filr desktop or mobile clients.

Failed Logins: Number of failed logins from the web client since the last metric interval.

This does not include failed logins from the Filr desktop or mobile clients.

Sessions: Number of valid sessions in memory.

Peak Sessions: Peak number of valid sessions in memory.

Unique Logged in Users: Number of unique users who have logged in to Filr by using the web client since the server started.

These users might not be currently logged in.

Unique Logged in Users Since: Number of unique users since the last time the information was dumped (dumps occur at a 60-minute interval).

File Writes: Number of file writes to the file repositories, including the remote file systems that are exposed through Net Folders and Home directories, as well as the local file repository that is exposed through file folders in personal storage.

File Writes Since: Number of file writes since the last time the information was dumped (dumps occur at a 60-minute interval).

File Reads: Number of file reads from the file repositories, including the remote file systems that are exposed through Net Folders and Home directories, as well as the local file repositories that are exposed through file folders in personal storage.

File Reads Since: Number of file reads since the last time the information was dumped (dumps occur at a 60-minute interval).

Files Shared: Number of files shared since the server started.

This number indicates the number of shares made through the Filr interface. This does not include shares made via the file system.

Files Shared Since: Number of files shared since the last time the information was dumped (dumps occur at a 60-minute interval).

This number indicates the number of shares made through the Filr interface. This does not include shares made via the file system.

Folders Shared: Number of folders shared since the server started.

This number indicates the number of shares made through the Filr interface. This does not include shares made via the file system.

Folders Shared Since: Number of folders shared since the last time the information was dumped (dumps occur at a 60-minute interval).

This number indicates the number of shares made through the Filr interface. This does not include shares made via the file system.

Total Filr Preview Conversions: Number of actual file preview requests since the last metric interval.

Represents only those requests that resulted in a conversion.

Filr Preview Conversions: Number of actual file preview requests since the server started.

Represents only those requests that resulted in a conversion.

Total Filr Preview Requests: Number of file preview requests since the last metric interval.

Represents any request for a file preview whether a conversion is required or cache is used.

Filr Preview Requests: Number of file preview requests since the server started.

Represents any request for a file preview whether a conversion is required or cache is used.

REST Requests: Number of REST calls made to this server.

REST Requests Since: Number of REST calls since the last time the information was dumped (dumps occur at a 60-minute interval).

Filrsearch Appliance Metrics

Adds: Number of adds to the index since the server started. This indicates the number of Lucene documents added to the index.

This number is not necessarily the same as the number of Filr entities that are indexed. For example, indexing a file entry results in two Lucene documents being created. Also, this number is not necessarily the same as the number of remote invocations that the Filr server makes to the index server, because in many cases, the Filr server combines multiple Lucene documents to add in a single remote invocation.

Add Since: Number of adds to the index since the last time the information was dumped (dumps occur at a 60-minute interval).

Deletes: Number of deletes from the index since the server started. This indicates the number of delete operations made on the index.

This number is not necessarily the same as the number of Lucene documents deleted from the index as the result of the request. In some cases, a single such request can result in a large number of Lucene documents being deleted from the index (for example, during system re-indexing). Also, this number is not necessarily the same as the number of remote invocations that the Filr application server makes to the index server, because of request batches from the application server.

Deletes Since: Number of deletes from the index since the last time the information was dumped (dumps occur at a 60-minute interval).

File Searches: Number of searches on the index since the server started. This includes all search operations, including user-directed searches, system-directed searches (such as folder listing), tag searches, and searches used by type-to-find functionality (name completion).

Searches Since: Number of searches on the index since the last time the information was dumped (dumps occur at a 60-minute interval).

Configuring Ganglia to Monitor MySQL or MariaDB Database

If you want to use Ganglia to monitor the existing database, you need to change the database name on the Filr appliance that Ganglia is configured to monitor to match the name of your database:

- 1 Edit the following file:

```
/opt/novell/ganglia/monitor/lib64/ganglia/python_modules/mysql.py
```

- 2 Modify the value of the following parameter (`filr`) to match the name of your database:

```
param dbname {
    value = "filr"
}
```

- 3 Save and close the file.
- 4 Restart the Ganglia service by using the following command:

```
rcnovell-gmond restart
rcnovell-gmetad restart
```

Monitoring File Meta-Data Synchronization in a Filr Cluster

Synchronization requests can go to any of the Filr appliances in a Filr cluster, regardless of which appliance a user logs in to. This makes monitoring the status of outstanding synchronization requests a little more involved.

All synchronization status is logged to `/var/opt/novell/tomcat-filr/logs/ssf.log`. However, this is a per-server log. In a Filr clustered implementation, all of the Filr appliances' `ssf.log`s need to be examined.

- 1 On each server, run the following command:

```
grep -i "(full) Starting" /var/opt/novell/tomcat-filr/logs/ssf.log
```

This lists all of the sync processes that have been started and have been recorded in the log file.

If the command finds any log entries, it returns something similar to:

```
2013-07-08 14:27:54,418 INFO [Sitescape_Worker-1]
[com.novell.teaming.module.folder.impl.PlusFolderModule] - (full) Starting
synchronization on folder [/Home Workspace/Net Folders/shared] (id=41)

2013-07-08 09:05:25,969 INFO [http-apr-8443-exec-1]
[com.novell.teaming.module.folder.impl.PlusFolderModule] - (full) Starting
synchronization on folder [/Home Workspace/Net Folders/support] (id=305)

2013-07-08 09:29:36,566 INFO [http-apr-8443-exec-3]
[com.novell.teaming.module.folder.impl.PlusFolderModule] - (full) Starting
synchronization on folder [/Home Workspace/Net Folders/shared] (id=41)

2013-07-08 09:32:27,887 INFO [http-apr-8443-exec-6]
[com.novell.teaming.module.folder.impl.PlusFolderModule] - (full) Starting
synchronization on folder [/Home Workspace/Net Folders/shared] (id=41)
```

This shows that on this particular server, four full synchronization tasks were started in the last 24 hours. Prior to this time, the `ssf.log` would have already been rolled over to a different file name. The lines extracted from the log show the folder name that is being synced.

- 2 After the Filr Appliance that executed the sync has been found, another `grep` can be used:

```
grep -i "(full) Completed synchronization" /var/opt/novell/tomcat-filr/logs/
ssf.log
```

This shows the number of completed synchronization tasks within the scope of the log file.

- 3 Based on the previous output, the following text could be retrieved.

```
grep -i "(full) Completed synchronization" /var/opt/novell/tomcat-filr/logs/
ssf.log

2013-07-08 08:29:39,215 INFO [Sitescape_Worker-1]
[com.novell.teaming.module.folder.impl.PlusFolderModule] - (full) Completed
synchronization on folder [/Home Workspace/Net Folders/shared] (id=41) -

2013-07-08 09:05:26,084 INFO [http-apr-8443-exec-1]
[com.novell.teaming.module.folder.impl.PlusFolderModule] - (full) Completed
synchronization on folder [/Home Workspace/Net Folders/support] (id=305) -

2013-07-08 09:31:03,127 INFO [http-apr-8443-exec-3]
[com.novell.teaming.module.folder.impl.PlusFolderModule] - (full) Completed
synchronization on folder [/Home Workspace/Net Folders/shared] (id=41) -
```

```
2013-07-08 09:33:28,973 INFO [http-apr-8443-exec-6]
[com.novell.teaming.module.folder.impl.PlusFolderModule] - (full) Completed
synchronization on folder [/Home Workspace/Net Folders/shared] (id=41)
```

This shows that each of the tasks that started on the server actually finished.

- 4 Further details of a completed synchronization can be extracted by using the `vi` or `less` commands on the log file in question.

In `vi`, issue the following command to see the first occurrence of the “Completed” string.

```
/Completed
```

This will find the text “Completed” in the log file and will show something similar to the text below:

```
2013-07-08 08:29:39,215 INFO [Sitescape_Worker-1]
[com.novell.teaming.module.folder.impl.PlusFolderModule] - (full) Completed
synchronization on folder [/Home Workspace/Net Folders/shared] (id=41) -

Sync time: 104.010406956 seconds

Files: found=2484 add=0 modify=0 expunge=0 acl=0 ownership=0

Folders: found=260 add=0 expunge=0 acl=0 ownership=0 processed=261 qsize=120

Entries: expunge=0

Failure count=0
```

If this is not the sync in question, then selecting “n” will page through the log file until you find the correct information.

Monitoring the Indexing Process

1. On the Filr appliance (or on any appliance in a Filr cluster), append the following line to the `/opt/novell/filr/apache-tomcat/webapps/ssf/WEB-INF/log4j.properties` file:

```
log4j.category.org.kablink.teaming.module.binder.impl.BinderModuleImpl=INFO
```

2. Restart the filr process with `rcfilr restart`.
3. After re-indexing has started, watch the `ssf.log` file for the following statement:

```
2013-06- INFO [http-bio-8080-exec-1]
[org.kablink.teaming.module.binder.impl.BinderModuleImpl] - indexTree took
1480.470827 ms
```

4. Check the results using `grep indexTree /var/opt/novell/apache-tomcat/logs/ssf.log`. Look for the key words “indexTree took” as shown above.

This shows that the re-indexing previously triggered has now completed.

Please note that the indexing recommendations made elsewhere in this guide still apply, and a pair of Filr Search appliances should be deployed as part of your system. Start both Filr Search appliances as `read/write` and make them available to Filr Clients. Change one of the appliances to be indexed to `write` and use that server for the re-index process.

This forces all the Filr clients to use the other indexing server.

After the re-indexing process is complete, as indicated by the log file discussed earlier, the appliance can be changed back to `Read/Write`. Any deferred updates should be applied, and the second server can then be re-indexed by using the same process.

Monitoring User Access, including the Guest User

1. Create a report for any system user with the [User Access Report](#) functionality.

14 MySQL—Backup and Restore from the Command Prompt

IMPORTANT: If you deploy the Micro Focus MySQL appliance, use the phpMyAdmin web front end to back up the Filr database.

A “Hot Backup” process for MySQL is available from Oracle as part of the paid-for version of MySQL.

- ♦ [“Backing Up MySQL from the Command Line” on page 87](#)
- ♦ [“Restoring MySQL from a Backup File” on page 87](#)

Backing Up MySQL from the Command Line

If you need to back up or restore the Filr database from the command line, do the following:

1. Shut down the MySQL service.
2. Run the following command:

```
mysqldump -u root -p filr >/backupdir/filrback.sql
```

This creates a file named `filrback` that can be used to restore the database.

3. Restart MySQL.

Restoring MySQL from a Backup File

1. (Optional) If a `filr` table does not exist in the location where you want to restore the Filr database, you must create it as follows:

- a. Log in to MySQL using the following command:

```
mysql -p
```

- b. Create the database using the following command:

```
create database filr;
```

2. When a `filr` table exists on the location where you want to restore the database, do the following:

- a. Quit MySQL

- b. Run the following command:

```
mysql -p filr < /backupdir/filr-back.sql
```

This completes the restore of the Filr database and its associated tables.

15 Net Folder Maintenance

- ♦ “Manually Synchronizing a Net Folder Server” on page 89
- ♦ “Manually Synchronizing a Net Folder” on page 89
- ♦ “Viewing the Synchronization Status of a Net Folder” on page 89

Manually Synchronizing a Net Folder Server

Path: [Port 8443 Filr Administration Console Management > Net Folder Servers](#)

Table 15-1 Net Folder Server Manual Synchronization

Field, Option, or Button	Information and/or Action
Manage Net Folder Servers page	<ol style="list-style-type: none">1. Select the Net Folder Server that you want to manually synchronize2. Click Sync.

Manually Synchronizing a Net Folder

Path: [Port 8443 Filr Administration Console Management > Net Folders](#)

Table 15-2 Net Folder Manual Synchronization

Field, Option, or Button	Information and/or Action
Manage Net Folders page	<ol style="list-style-type: none">1. Select the Net Folder that you want to manually synchronize.2. Click Sync.

Viewing the Synchronization Status of a Net Folder

Path: [Port 8443 Filr Administration Console Management > Net Folders](#)

Table 15-3 Net Folder Synchronization Status

Field, Option, or Button	Information and/or Action
Manage Net Folders page	<ol style="list-style-type: none">1. The Sync status column displays the synchronization status of each Net Folder.2. Click the icon for more detailed status information.

16 Notification (Email) Customization

You can customize many of the Filr-generated strings that appear in notifications sent to Filr users.

- ♦ [“About Filr’s Email Templates” on page 91](#)
- ♦ [“Template Tips and Documentation” on page 92](#)
- ♦ [“Modifying the Email Template Files” on page 92](#)
- ♦ [“Email Template Customization—A Video Walkthrough” on page 92](#)

About Filr’s Email Templates

Filr generates email notifications using Apache Velocity version 1.5 templates.

You can customize the following templates:

Template Name	Purpose
externalConfirmation.vm	Confirmation notification sent to an external user after the user is successfully registered with Filr server.
fileRequestNotification.vm	A mail is sent requesting the external user to upload a file to the Filr server.
fileRequestUploadNotification.vm	A confirmation mail is received by the Filr user when the file is uploaded to the Filr server.
footer.vm	Text or images applied at the end of each email
forgottenPasswordNotification.vm	Forgotten password notification sent to a user when the user clicks Can't login link on the login page to request for a new password.
header.vm	Text or images applied at the beginning of each email
passwordChangedNotification.vm	Notification that user's password changed
publicLinkNotification.vm	Notification of a publicly available link to a file
selfRegistrationRequired.vm	Shared item notification to user who must register with Filr in order to view it
shareAccessedNotification.vm	Notification that the file or folder is accessed by the user.
sharedEntryInvite.vm	Shared file invitation to an external user
sharedEntryNotification.vm	Shared file notification of change to existing Filr user
sharedFolderInvite.vm	Shared folder invitation to external user
sharedFolderNotification.vm	Shared folder notification of change to existing Filr user
storageAlertEmail.vm	Storage notification that the Filr server sends to Filr administrators when vashare or vastorage storage is 90% filled.
style.vm	CSS style sheet for email notifications

Template Name	Purpose
teaming.vm	Macros that get applied to all emails
zoneQuotaAlertEmail.vm	An alert mail to the zone administrator and inbuilt (main) administrator when a user has used all the allocated space.

Template Tips and Documentation

IMPORTANT: Micro Focus doesn't attempt to document third-party products, such as Apache Velocity.

For complete information and instructions for the Apache Velocity version 1.5 template language, visit the [Apache Velocity Project website \(https://velocity.apache.org/engine/1.5/\)](https://velocity.apache.org/engine/1.5/).

The following are tips about the template files in Filr.

- ◆ Each template contains a brief explanation about what it affects and what you can customize in it.
- ◆ Filr system-generated emails contain both text and HTML MIME parts.
You can customize these independently.
- ◆ You can customize for specific languages to localize the emails your Filr system generates.
- ◆ You can revert back to the default template by selecting a customized template in the list and then clicking the Delete button.
- ◆ Make sure you use the [Velocity documentation \(https://velocity.apache.org/engine/1.5/user-guide.html\)](https://velocity.apache.org/engine/1.5/user-guide.html).

For example, one user assumed that the hash marks (#) indicated comments, when in fact they are part of the Velocity scripting language.

Modifying the Email Template Files

The default email templates that reside on the Filr system cannot be changed or deleted, but you can create and deploy customized copies of them by doing the following:

- 1 Download a template to your local disk by clicking it in the Email Templates dialog.
- 2 Open the downloaded template in a text editor.
- 3 Customize the file as discussed in the Video Walkthrough below and documented on the [Apache Velocity Project website \(https://velocity.apache.org/engine/1.5/\)](https://velocity.apache.org/engine/1.5/).
- 4 Save the template on your local disk.
- 5 Upload the customized file by dragging and dropping it into the Email Templates dialog.

The **Type** then changes to **Customized**.

Email Template Customization—A Video Walkthrough

To see a demonstration of the email template customization process, view the following video:



<http://www.youtube.com/watch?v=AA4A-nG3dIY>

17 Search Index Maintenance

- ♦ [“Optimizing the Lucene Index to Improve Search Performance” on page 93](#)
- ♦ [“Maintaining Your High Availability Lucene Index” on page 95](#)
- ♦ [“Rebuilding the Lucene Index” on page 98](#)

Optimizing the Lucene Index to Improve Search Performance

IMPORTANT: In order for optimization to run, there must be at least 51% free disk space on the Lucene search index appliance.

For a medium to large Filr system, you should run the optimization once a week during off hours or on weekends when the Filr system is not being heavily used.

Optimizing the Lucene index does not repair a damaged or out-of-date index. To repair a damaged or out-of-date index, you must rebuild the index, as described in [“Rebuilding the Lucene Index” on page 98](#).

- ♦ [“Optimizing a Single Search Index” on page 93](#)
- ♦ [“Optimizing the Search Index with Multiple Index Servers” on page 94](#)

Optimizing a Single Search Index

1 Log in to the Filr site as the Filr administrator.


1a Launch a web browser.

1b Specify one of the following URLs, depending on whether you are using a secure SSL connection:

```
http://Filr_hostname:8080  
https://Filr_hostname:8443
```

Replace *Filr_hostname* with the host name or fully qualified domain name of the Filr server that you have set up in DNS.

Depending on how you have configured your Filr system, you might not be required to enter the port number in the URL. If you are using NetIQ Access Manager, the Filr login screen is not used.

- 2 Click the **admin** link in the upper-right corner of the page, then click the **Administration Console** icon .
- 3 Under **Management**, click **Search Index**.
- 4 Click the **Optimize Search Index** tab.

- 5 Select **Run Immediately** if you want to run the optimization right now.
- 6 Select **Run at Scheduled Time**, then specify the days and times that you want the optimization to occur.
- 7 Click **OK**.


Optimizing the Search Index with Multiple Index Servers

- 1 Log in to the Filr site as the Filr administrator.
 - 1a Launch a web browser.
 - 1b Specify one of the following URLs, depending on whether you are using a secure SSL connection:

```
http://Filr_hostname:8080
https://Filr_hostname:8443
```

Replace *Filr_hostname* with the host name or fully qualified domain name of the Filr server that you have set up in DNS.

Depending on how you have configured your Filr system, you might not be required to enter the port number in the URL. If you are using NetIQ Access Manager, the Filr login screen is not used.

- 2 Click the **admin** link in the upper-right corner of the page, then click the **Administration Console** icon .
- 3 In the **Search Index** section, click **Index**.
- 4 Click the **Optimize Search Index** tab.
- 5 Select **Run Immediately** if you want to run the optimization right now.

- 6 Select **Run at Scheduled Time**, then specify the days and times that you want the optimization to occur.
- 7 Select each node that you want to optimize.
- 8 Click **OK**.

Maintaining Your High Availability Lucene Index


If you have a high availability Lucene configuration, you can take one Lucene node out of service for maintenance while other Lucene nodes continue to operate. Then you can synchronize the out-of-date Lucene node with the current indexing data.

- 1 Log in to the Micro Focus Filr site as the Filr administrator.
 - 1a Launch a web browser.
 - 1b Specify one of the following URLs, depending on whether you are using a secure SSL connection:

```
http://Filr_hostname:8080  
https://Filr_hostname:8443
```

Replace *Filr_hostname* with the host name or fully qualified domain name of the Filr server that you have set up in DNS.

Depending on how you have configured your Filr system, you might not be required to enter the port number in the URL. If you are using NetIQ Access Manager, the Filr login screen is not used.

- 2 Take the Lucene node that needs maintenance out of service:
 - 2a Click the **admin** link in the upper-right corner of the page, then click the **Administration Console** icon .
 - 2b Under **Search Index**, click **Nodes**.

Node A (node a)

Host: 5int252.lab.com
RMI port: 1199

User Mode Access

Read and Write
 Write Only
 No Access

Enable Deferred Update Log

No Deferred Update Log Record Exists

Node B (node b)

Host: 5int252.lab.com
RMI port: 1199

User Mode Access


Read and Write
 Write Only
 No Access

Enable Deferred Update Log

No Deferred Update Log Record Exists

Apply
Close

- 2c** In the list, locate the node that needs maintenance.
- 2d** Ensure that **Enable Deferred Update Log** is selected.
- 2e** In the **User Mode Access** box, change **Read and Write** to one of the following options, depending on the type of maintenance that you want to perform:
- ◆ **Write Only:** Select this option if you are performing a re-index on the search index node.
 - ◆ **No Access:** Select this option if you are performing other types of maintenance on the search index node, such as upgrading it, adding more disk space or memory, and so forth.
- Selecting this option ensures that no data is written to the index while the maintenance is being performed.
- 2f** Click **Apply**, then click **Close**.
- The new setting is put into effect immediately, so that the Lucene node is no longer accessible to Filr users.
- 3** Perform the needed maintenance on the Lucene node. For example, for information about how to perform a re-index on the node, see [“Rebuilding the Lucene Index” on page 98](#).

- 4 Return the out-of-date Lucene node to full service:
 - 4a Click the **admin** link in the upper-right corner of the page, then click the **Administration Console** icon .
 - 4b Under **Search Index**, click **Nodes**.

Node A (node a)

Host: 5int252.lab.com
RMI port: 1199

User Mode Access

Read and Write
 Write Only
 No Access

Enable Deferred Update Log

No Deferred Update Log Record Exists

Node B (node b)

Host: 5int252.lab.com
RMI port: 1199

User Mode Access

Read and Write
 Write Only
 No Access

Enable Deferred Update Log

Deferred Update Log Records Exist

Apply Deferred Update Log Records to the Index
 Discard Deferred Update Log Records
 Do Nothing

Apply
Close

If you moved the Lucene node to **No Access**, the out-of-date Lucene node is flagged with **Deferred Update Log Records Exist**.

The **User Mode Access** option shows **Read and Write** because this is the last selected setting.

- 4c Select **Apply Deferred Update Log Records to the Index**, then click **Apply**.

The Deferred Update Log options disappear if the update is successful.

- 4d Click **Close**.

The Lucene node that was out of service has now been updated with current indexing data.

- 5 (Conditional) If both Lucene nodes require maintenance, repeat [Step 1](#) through [Step 4](#) for the second Lucene node.

Rebuilding the Lucene Index

The Lucene index provides access to all data in your Micro Focus Filr site, including objects, such as users, groups, files and folders, and file contents where content indexing is enabled.

If the index becomes damaged or out-of-date for some reason, you can rebuild it.

Users might first notice a problem with the Lucene index if they cannot find information or people that they know should be available on the Filr site. If you are running multiple Lucene Index Servers, follow the instructions in [“Maintaining Your High Availability Lucene Index” on page 95](#).

Rebuilding the Lucene search index can consume a significant amount of resources on your Filr appliance. In a clustered environment, it is a good idea to set aside a single Filr appliance to handle the load of rebuilding the search index.

For information about how to set aside a Filr appliance, see [“Dedicating a Filr Appliance to Indexing and Net Folder Synchronization” in the *Filr 3.4: Installation, Deployment, and Upgrade Guide*](#).

The steps to reset the search index differ depending on whether you have multiple Lucene Index servers.

- ♦ [“Rebuilding a Single Search Index” on page 98](#)
- ♦ [“Rebuilding the Search Index with Multiple Index Servers” on page 99](#)

Rebuilding a Single Search Index

1 Log in to the Filr site as the Filr administrator.

1a Launch a web browser.

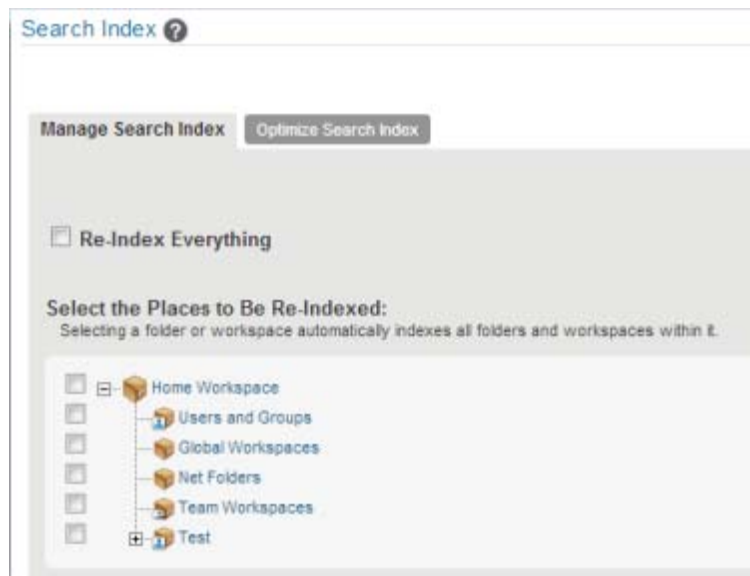
1b Specify one of the following URLs, depending on whether you are using a secure SSL connection:

```
http://Filr_hostname:8080  
https://Filr_hostname:8443
```

Replace *Filr_hostname* with the host name or fully qualified domain name of the Filr server that you have set up in DNS.

Depending on how you have configured your Filr system, you might not be required to enter the port number in the URL. If you are using NetIQ Access Manager, the Filr login screen is not used.

- 2 Click the **admin** link in the upper-right corner of the page, then click the **Administration Console** icon .
- 3 In the **Management** section, click **Search Index**.



- 4 To reindex the entire Filr site, select **Re-Index Everything**.

Depending on the size of your Filr site, this can be a very time-consuming process.

or

Select one or more parts of your Filr site to re-index.

- 5 Click **OK** to start the indexing.

Users can still access the Filr site during the indexing process, but search results might not be accurate until the index has been completely rebuilt.

To view when indexing is complete, keep the Search Index dialog box open to see the status. Alternatively, a message is displayed in either the `appserver.log` files stating that reindexing is complete.

- 6 To ensure that the rebuild was successful, verify that the following messages appear in the `appserver.log` file:

```
Completed indexing of tree with xxx binders. Time taken for indexing is xxx.xxx
msAdministrative reindexing completed on binders [1]
```

For information about how to access the `appserver.log` file, see [“Accessing Filr System Log Files”](#) in the *Filr 3.4.1: Administrative UI Reference*.

Rebuilding the Search Index with Multiple Index Servers

To avoid downtime when rebuilding the search index with multiple search index servers:

- 1 Take the first search index node out of service to rebuild it while the other is still running.

For information about how to take a node out of service, see [“Maintaining Your High Availability Lucene Index” on page 95](#).

- 2 Rebuild the search index node from the **Index** section of the Administration Console.

- 3 After the first search index node is rebuilt, put it back into service.

For information about how to put a node back into service, see [“Maintaining Your High Availability Lucene Index” on page 95](#).

- 4 Repeat this process for the second search index node.

To view when indexing is complete, keep the Search Index dialog box open to see the status. Alternatively, a message is displayed in either the `appserver.log` files stating that reindexing is complete.

- 5 To ensure that the rebuild was successful, verify that the following messages appear in the `appserver.log` file:

```
Completed indexing of tree with xxx binders. Time taken for indexing is xxx.xxx  
msAdministrative reindexing completed on binders [1]
```

For information about how to access the `appserver.log` file, see see [“Accessing Filr System Log Files”](#) in the *Filr 3.4.1: Administrative UI Reference*..

18 Security

- ◆ “Antivirus” on page 101
- ◆ “Audit Trail” on page 102
- ◆ “Backup and Restore” on page 102
- ◆ “Brute-Force Attacks and CAPTCHA” on page 102
- ◆ “Certificate Maintenance” on page 102
- ◆ “Comments and Security” on page 105
- ◆ “Database Communication Encryption” on page 105
- ◆ “Desktop Application Security” on page 107
- ◆ “DMZ Setup for Filr” on page 107
- ◆ “Downloads through Filr—Disabling” on page 109
- ◆ “Email Transfer Security” on page 112
- ◆ “Encryption” on page 112
- ◆ “File Server Security” on page 112
- ◆ “Filr Component Security” on page 112
- ◆ “Filr Data Security” on page 113
- ◆ “Filr’s Rights Model” on page 113
- ◆ “Filr Security Defaults” on page 114
- ◆ “Filr Site Security” on page 114
- ◆ “LDAP Synchronization Security” on page 115
- ◆ “Mobile Device Data Security” on page 117
- ◆ “NESSUS Scans” on page 118
- ◆ “Proxy User Security” on page 118
- ◆ “Security Scan Risk Reports” on page 118
- ◆ “Sharing and Security” on page 119
- ◆ “SSH Access for the Root User” on page 119
- ◆ “Universal Passwords (eDirectory) Security” on page 120
- ◆ “Users and Security” on page 120
- ◆ “WebDAV Support” on page 120
- ◆ “XSS Security Filter” on page 125

Antivirus

- ◆ You can leverage what you are doing on your file servers.

Audit Trail

- ◆ Every authorization change is logged in Filr.
- ◆ Every authentication decision is logged in Filr.
- ◆ Enhanced reporting features are planned in this area in future releases.
- ◆ Enhanced integration with audit trail analysis tools, such as NetIQ Sentinel, are planned in future releases.

Backup and Restore

- ◆ You can leverage what you are doing on your file servers.
- ◆ VMware lets you create virtual disks on remote storage that is able to be backed up and restored independent of Filr.

Brute-Force Attacks and CAPTCHA

CAPTCHA (<http://en.wikipedia.org/wiki/CAPTCHA>) provides additional security against brute-force attacks on the Filr web application.

Brute-force attack monitoring is enabled on the Filr system by default. Filr considers a brute-force attack to be taking place if any user has 5 failed login attempts to the Filr system within a 30-minute timeframe. During the time that Filr believes that a brute-force attack is occurring, Filr requires all users to specify the CAPTCHA response when logging in to the Filr web application. Filr considers the system to be safe from the brute-force attack as soon as there have been fewer than 5 failed login attempts within the past 30 minutes. At that time, specifying a CAPTCHA response is no longer required.

Certificate Maintenance

Micro Focus appliances ship with a self-signed digital certificate. However, you should use a trusted server certificate that is signed by a trusted certificate authority (CA) such as VeriSign or Equifax.

The certificate works for both the Micro Focus Appliance and the Filr software (ports 9443 and 8443). You do not need to update your certificate when you update the Filr software.

Complete the following sections to change the digital certificate for your Micro Focus Appliance. You can use the digital certificate tool to create your own certificate and then have it signed by a CA, or you can use an existing certificate and key pair if you have one that you want to use.

NOTE: If you are using a Godaddy SSL certificate with Filr, follow the steps in “TID 7023569” (<https://support.microfocus.com/kb/doc.php?id=7023569>) at the **Micro Focus Support website** (<https://www.microfocus.com/support-and-services/knowledge-base/>).

- ◆ “Using the Digital Certificate Tool” on page 103
- ◆ “Using an Existing Certificate and Key Pair” on page 104
- ◆ “Activating the Certificate” on page 104
- ◆ “Managing Certificates” on page 105

Using the Digital Certificate Tool

- ♦ [“Creating a New Self-Signed Certificate” on page 103](#)
- ♦ [“Getting Your Certificate Officially Signed” on page 103](#)
- ♦ [“Exporting a Self-Signed Certificate” on page 104](#)

Creating a New Self-Signed Certificate

Path: Port 9443 Appliance Console

- 1 Log in to the Micro Focus appliance at https://server_url:9443.
- 2 Click **Digital Certificates**.
- 3 In the **Key Store** drop-down list, ensure that **Web Application Certificates** is selected.
- 4 Click **File > New Certificate (Key Pair)**, then specify the following information:
 - Alias:** Specify a name that you want to use to identify and manage this certificate.
 - Validity (days):** Specify how long you want the certificate to remain valid.
 - Key Algorithm:** Select either **RSA** or **DSA**.
 - Key Size:** Select the desired key size.
 - Signature Algorithm:** Select the desired signature algorithm.
 - Common Name (CN):** This must match the server name in the URL in order for browsers to accept the certificate for SSL communication.
 - Organizational Unit (OU):** (Optional) Small organization name, such as a department or division. For example, Purchasing.
 - Organization (O):** (Optional) Large organization name. For example, Micro Focus
 - City or Locality (L):** (Optional) City name. For example, Provo.
 - State or Province (ST):** (Optional) State or province name. For example, Utah.
 - Two-letter Country Code (C):** (Optional) Two-letter country code. For example, US.
- 5 Click **OK** to create the certificate.

After the certificate is created, it is self-signed.
- 6 Make the certificate official, as described in [“Getting Your Certificate Officially Signed” on page 103](#).

Getting Your Certificate Officially Signed

- 1 On the Digital Certificates page, select the certificate that you just created, then click **File > Certificate Requests > Generate CSR**.
- 2 Complete the process of emailing your digital certificate to a certificate authority (CA), such as Verisign.

The CA takes your Certificate Signing Request (CSR) and generates an official certificate based on the information in the CSR. The CA then mails the new certificate and certificate chain back to you.

- 3 After you have received the official certificate and certificate chain from the CA:
 - 3a Revisit the Digital Certificates page by clicking **Digital Certificates** from the Micro Focus Appliance.
 - 3b Click **File > Import > Trusted Certificate**. Browse to the trusted certificate chain that you received from the CA, then click **OK**.
 - 3c Select the self-signed certificate, then click **File > Certification Request > Import CA Reply**.
 - 3d Browse to and upload the official certificate to be used to update the certificate information.
On the Digital Certificates page, the name in the **Issuer** column for your certificate changes to the name of the CA that stamped your certificate.
- 4 Activate the certificate, as described in [“Activating the Certificate” on page 104](#).

Exporting a Self-Signed Certificate

Path: Port 9443 Appliance Console

- 1 Log in to the Micro Focus appliance at `https://server_url:9443`.
- 2 Click **Digital Certificates**.
- 3 In the **Key Store** drop-down list, select **Web Application Certificates**.
- 4 Select the `self-signed_cert` file.
- 5 Click **File > Export > Public Certificate**.

This downloads the `self-signed_cert.crt` certificate file.

Using an Existing Certificate and Key Pair

When you use an existing certificate and key pair, use a .P12 key pair format.

- 1 Go to the Digital Certificates page by clicking **Digital Certificates** from the Micro Focus Appliance.
- 2 Click **File > Import > Trusted Certificate**. Browse to and select your existing certificate, then click **OK**.
- 3 Click **File > Import > Trusted Certificate**. Browse to your existing certificate chain for the certificate that you selected in [Step 2](#), then click **OK**.
- 4 Click **File > Import > Key Pair**, then browse to and select your .P12 key pair file, specify your password if needed, then click **OK**.

Because of a browser compatibility issue with HTML 5, the path to the certificate is sometimes shown as `c:\fakepath`. This does not adversely affect the import process.

- 5 Continue with [“Activating the Certificate” on page 104](#).

Activating the Certificate

- 1 On the Digital Certificates page, select the certificate that you want to make active, click **Set as Active**, then click **Yes**.
- 2 Verify that the certificate and the certificate chain were created correctly by selecting the certificate and clicking **View Info**.

Managing Certificates

All certificates that are included with the IBM Java package that is bundled with the version of SLES that Filr ships with are installed when you install Filr.

Filr uses only the certificates that relate to LDAP and SMTP.

You can use the Digital Certificates tool on the Filr appliance to remove certificates that are not used by your organization if you are concerned about keeping them.

Also, you can use the Digital Certificates tool on the Filr appliance to maintain the certificate store by removing certificates that have expired and then installing new certificates as needed, according to your organization's security policies.

To access the Digital Certificates tool:

- 1 Click **Digital Certificates** from the Micro Focus Appliance.

Comments and Security

- ♦ All users that have access to a file or folder (via native rights or shared) can read the comments on that file or folder.
- ♦ All users, except public users, can write comments.

Comment writing for public users is configurable, but it is off by default for two reasons:

- ♦ Because public users are anonymous, there is a risk that they might be abusive, offensive, or meddlesome.
- ♦ Comments cannot be deleted.
- ♦ Micro Focus plans to add more granular control over who can see comments in the future:
 - ♦ Add private comments that are directed at a specific set of users or groups. (In addition to open comments that are visible to all users with access.)
 - ♦ External users cannot write comments; they can only view comments.
 - ♦ Public users cannot read any comments.

Database Communication Encryption

Filr Administrator can now enable or disable data encryption between the Filr server and the database.

The Database Connection page on the Appliance Console now includes a new option **Encrypt Database Communication** that enables you to encrypt the data from the Filr server. This option is disabled by default. Before selecting this option, you must ensure that the settings for your database are enabled to allow encryption of the data from the database server to the Filr server.

- ♦ [“Configuring the Database Settings” on page 106](#)
- ♦ [“Configuring the Filr Server Settings” on page 107](#)

Configuring the Database Settings

To enable the data encryption between the Filr server and the database server, you must first configure your database settings to support data encryption followed by configuring the settings on the Filr server.

- ♦ “For MySQL Appliance” on page 106
- ♦ “For Other Database Servers” on page 106

For MySQL Appliance

If you are using the MySQL appliance, perform the following steps to secure the database communication:

- 1 On the MySQL database server, create a folder named `/vastorage/conf/ssl-certs-dir/`.
- 2 Download the `ssl_mysql.sh` script from the [Filr 3.0 download site \(https://www.microfocus.com/products/filr/trial-download\)](https://www.microfocus.com/products/filr/trial-download) to the folder you created in the previous step.

Registration with Micro Focus is required. If you have already registered and received an email with a download link, the file is on the linked page.

- 3 Run the following command to install the files required for data encryption:

```
# sh ssl_mysql.sh INSTALL
```

- 4 Run the following command to enable the SSL setting:

```
# sh ssl_mysql.sh ENABLE <db-root-password>
```

- 5 Run the following command to check if SSL is enabled in the MySQL database server. The value of `have_ssl` flag should have changed from **DISABLED** to **YES**.

```
# mysql -uroot -p<db-root-password> -e "SHOW GLOBAL VARIABLES LIKE 'have_%ssl';"
```

NOTE: To disable the secure database communication, run the following command:

```
# sh ssl_mysql.sh DISABLE <db-root-password>
```

For Other Database Servers

If you using your existing database server instead of the MySQL appliance, refer to the following database-specific documentation to enable the data encryption from the database server to the Filr server:

- ♦ **MS SQL Server:** See *Enable Encrypted Connections to the Database Engine (SQL Server Configuration Manager)* on the [Microsoft Website \(https://msdn.microsoft.com/en-us/library/ms191192\)](https://msdn.microsoft.com/en-us/library/ms191192).
- ♦ **MySQL Server:** See *Server-Side Configuration for Secure Connections* in the [MySQL Documentation \(https://dev.mysql.com/doc/refman/5.7/en/using-secure-connections.html\)](https://dev.mysql.com/doc/refman/5.7/en/using-secure-connections.html).
- ♦ **MariaDB Server:** See the following MariaDB Documentation pages:
 - ♦ [Configuring MariaDB with my.cnf \(https://mariadb.com/kb/en/mariadb/configuring-mariadb-with-mycnf/\)](https://mariadb.com/kb/en/mariadb/configuring-mariadb-with-mycnf/)
 - ♦ [SSL/TLS System Variables \(https://mariadb.com/kb/en/mariadb/ssltls-system-variables/\)](https://mariadb.com/kb/en/mariadb/ssltls-system-variables/)

Configuring the Filr Server Settings

Before you configure your Filr server to enable data encryption from the Filr server to the database, you must ensure that you have already configured your database to enable data encryption from the database server to the Filr server. See [“Configuring the Database Settings” on page 106](#).

To configure the Filr server to encrypt data:

- 1 Log in to the Filr appliance at `https://server_url:9443`.
- 2 Click **Configuration > Database**.
- 3 Specify the configuration options:
 - ♦ **Existing Options:** For information about the options that existed before this beta release, click the help icon.
 - ♦ **New Option:** This beta release introduces the **Encrypt Database Communication** option. Select this option to encrypt data communication from the Filr server to the database server.
- 4 A message that you must have the encryption from the database server already enabled pops up. Ensure that the encryption from the database server is enabled and then click **OK**.
- 5 Click **OK**, then click **Reconfigure Filr Server** for your changes to take effect.

This stops and restarts your Filr server. Because this results in server downtime, you should restart the server at off-peak hours.

NOTE: To disable the data encryption between the Filr server and the database server, you must first disable the secure database communication and then deselect the **Encrypt Database Communication** option. For information about configuring the database settings, see [“Configuring the Database Settings” on page 106](#).

Desktop Application Security

To review and adjust security-related settings for the Filr desktop application, see [Desktop Access—Default Settings](#) in the [Filr 3.4.1: Administrative UI Reference](#).

DMZ Setup for Filr

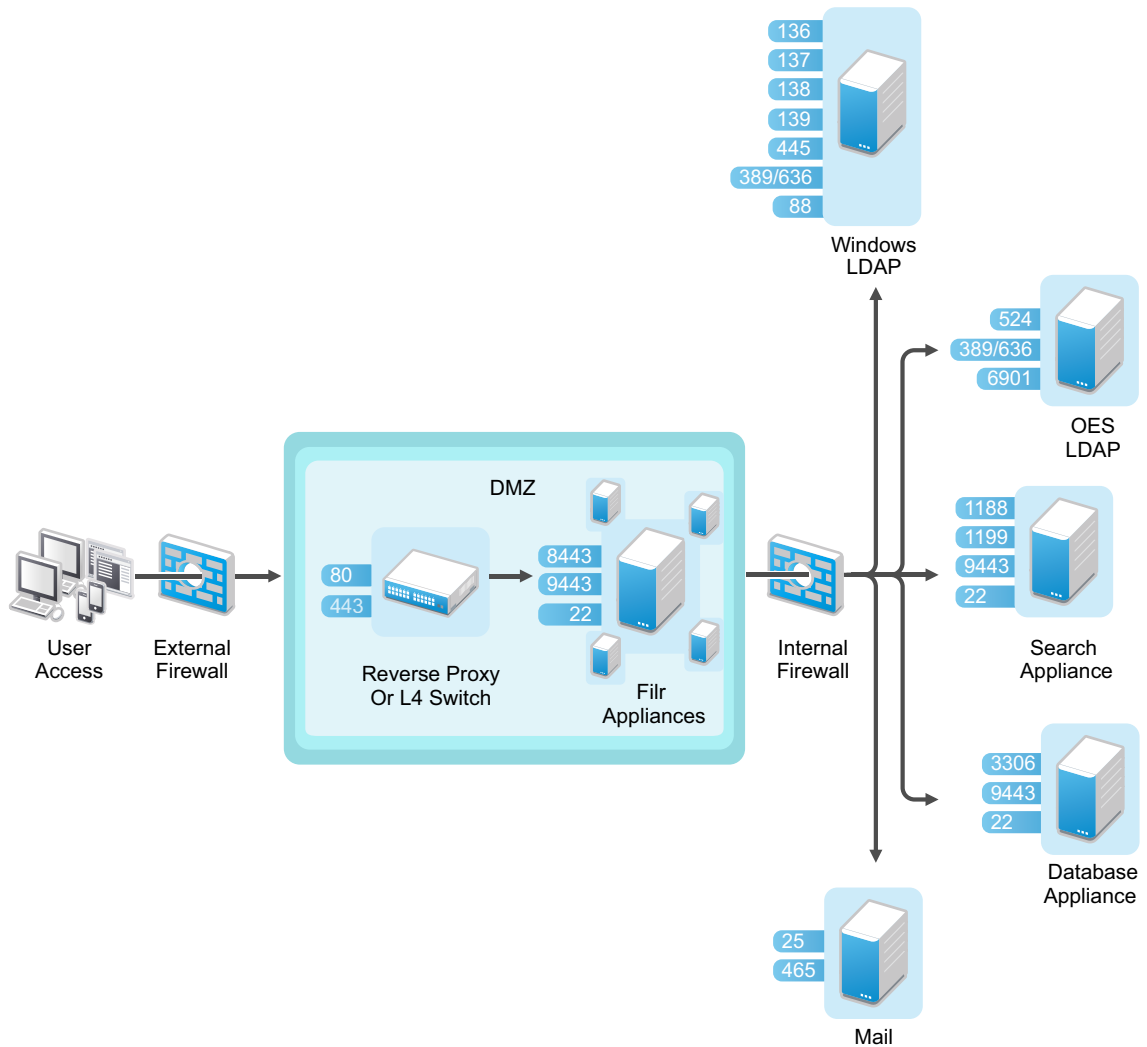
IMPORTANT: Security is a complex subject and Micro Focus does not attempt to suggest a complete defense solution with this example. Micro Focus recommends that you consult with your security professional to implement Filr in a DMZ.

To provide an additional level of security, you can set up Filr in a DMZ. You might want to consider setting up Filr in a DMZ especially if you are planning to [allow external users to access the Filr system](#). It is most secure to restrict external user access to Filr appliances that are located in the DMZ, rather than allowing external users access to a Filr appliance behind the internal firewall.

The actual data is never stored in the DMZ. It is stored behind the internal firewall on the database and search appliances, on the Windows and OES servers (for your Net Folders), and on a SAN for files in personal storage.

[Figure 18-1](#) illustrates a basic setup with Filr running in a DMZ, including information about the ports that you need to open for the firewalls and for communication between the various servers.

Figure 18-1 Filr in a DMZ



Only traffic destined to the DMZ is allowed through the front-end firewall, and only traffic from the DMZ to the internal network is allowed through the back-end firewall.

In a clustered environment, it is also possible for some of the Filr appliances in the cluster to run behind the internal firewall while others run in the DMZ. Doing so can result in performance benefits for internal users. Setting up Filr in this way requires that you use memcached caching. For more information about configuring memcached caching, see [Filr Clustering Configuration](#) in the *Filr 3.4.1: Administrative UI Reference*.

For more information about port configuration in Filr, see “[Port Numbers](#)” in the *Filr 3.4.1: Administrative UI Reference*.

For information about setting up NetIQ Access Manager as a reverse proxy, see “[Access Manager \(NAM\) and Filr Integration](#)” in the *Filr 3.4: Installation, Deployment, and Upgrade Guide*.

Downloads through Filr—Disabling

You can disable the ability for users to download files from the Filr site on the web. If you do not disable downloads as described in this section, users can download files to their personal workstations, as described in “[Downloading Files](#)” in the *Filr 3.4: User Access Guide*.

IMPORTANT: If you do disable file downloads as described in this section, users can view files only as HTML in a web browser. However, some file types (such as PDF files) cannot be viewed as HTML, and therefore cannot be viewed in Filr if the ability to download files is disabled.

You can disable the ability for users to download files from the Filr site on the web for all users, or for specific users and groups. Alternatively, you can disable downloads for all users and then enable downloads for specific users and groups.

- ♦ “[Disabling Downloads for All Users](#)” on page 109
- ♦ “[Disabling or Enabling Downloads for Individual Users](#)” on page 110
- ♦ “[Disabling or Enabling Downloads for Individual Groups](#)” on page 111

Disabling Downloads for All Users

1 Log in to the Filr site as the Filr administrator.


1a Launch a web browser.

1b Specify one of the following URLs, depending on whether you are using a secure SSL connection:

```
http://Filr_hostname:8080  
https://Filr_hostname:8443
```

Replace *Filr_hostname* with the hostname or fully qualified domain name of the Filr server that you have set up in DNS.

Depending on how you have configured your Filr system, you might not be required to enter the port number in the URL. If you are using NetIQ Access Manager, the Filr login screen is not used.

2 Click the **admin** link in the upper-right corner of the page, then click the **Administration Console** icon .

3 Under **System**, click **Web Application**.

Configure Web Application

- Allow Guest access
- Guest access is read only
- Disable file downloads
- Disable web access

- 4 Select **Disable file downloads**.
- 5 Click **OK**.


Disabling or Enabling Downloads for Individual Users

- 1 Log in to the Filr site as the Filr administrator.
 - 1a Launch a web browser.
 - 1b Specify one of the following URLs, depending on whether you are using a secure SSL connection:

```
http://Filr_hostname:8080  
https://Filr_hostname:8443
```

Replace *Filr_hostname* with the hostname or fully qualified domain name of the Filr server that you have set up in DNS.

Depending on how you have configured your Filr system, you might not be required to enter the port number in the URL. If you are using NetIQ Access Manager, the Filr login screen is not used.

- 2 Click the **admin** link in the upper-right corner of the page, then click the **Administration Console** icon .
- 3 Under **Management**, click **Users**.

The Manage Users page is displayed.
- 4 (Conditional) If you have not disabled downloads for all users (as described in “[Disabling Downloads for All Users](#)” on page 109), you can disable downloads for an individual user by clicking the drop-down arrow next to the user’s name and then clicking **Disable File Downloads for this User**.

or

To disable access for multiple users, select the users whose access you want to disable, then click **More > Disable File Downloads**.

- 5 (Conditional) If you have disabled downloads for all users, you can enable downloads for an individual user by clicking the drop-down arrow next to the user's name and then clicking **Enable File Downloads for this User**.

or

To enable downloads for multiple users, select the users who you want to allow to download files, then click **More > Enable File Downloads**.

Disabling or Enabling Downloads for Individual Groups

- 1 Log in to the Filr site as the Filr administrator.


- 1a Launch a web browser.

- 1b Specify one of the following URLs, depending on whether you are using a secure SSL connection:

```
http://Filr_hostname:8080  
https://Filr_hostname:8443
```

Replace *Filr_hostname* with the hostname or fully qualified domain name of the Filr server that you have set up in DNS.

Depending on how you have configured your Filr system, you might not be required to enter the port number in the URL. If you are using NetIQ Access Manager, the Filr login screen is not used.

- 2 Click the **admin** link in the upper-right corner of the page, then click the **Administration Console** icon .

- 3 Under **Management**, click **Groups**.

The Manage Groups page is displayed.

- 4 (Conditional) If you have not disabled access for all users (as described in “[Disabling Downloads for All Users](#)” on page 109), you can disable access for users who belong to an individual group by clicking the drop-down arrow next to the group name and then clicking **Disable Web Access for Users in this Group**.

or

To disable access for multiple users, select the users whose access you want to disable, then click **More > Disable File Downloads**.

- 5 (Conditional) If you have disabled downloads for all users, you can enable downloads for users who belong to an individual group by clicking the drop-down arrow next to the group name and then clicking **Enable File Downloads for Users in this Group**.

or

To enable access for multiple users, select the users whose access you want to enable, then click **More > Enable File Downloads**.

Email Transfer Security

When you install Micro Focus Filr, you can choose whether the Filr internal mail host uses TLS (Transport Layer Security) when it communicates with other SMTP mail hosts.

If your Filr site needs to send email messages to an email system that requires secure SMTP (SMTPS), the Filr site must have the same type of root certificate that is required for secure LDAP (LDAPS). If you have not already set up secure LDAP for your Filr site, follow the instructions in [“LDAP Synchronization Security” on page 115](#) to set up secure SMTP for communications with your email system.

Encryption

- ◆ Filr encrypts all sensitive authentication credentials and all data on the wire between each Filr appliance.
- ◆ Filr does not encrypt any back-end data on local or remote file servers.
- ◆ Filr should work well with compatible back-end servers that support full-disk encryption.
- ◆ Filr clients should work well with any client solutions, either desktop or mobile, including Micro Focus ZENworks Full Disk Encryption.
- ◆ Communication between the Filr desktop application and the Filr server is sent with SSL encryption.
- ◆ Communication between the Filr mobile apps and the Filr server is sent with SSL encryption.
- ◆ Additional encryption features are planned for future releases.

File Server Security

- ◆ Filr honors and respects all trustee rights, file attributes, and folder attributes on all targeted file systems.
- ◆ Filr never changes any rights or attributes on targeted file systems.
- ◆ The only time file system rights are effectively bypassed is when a Filr user shares a file or folder with another user. In this case, the proxy user's rights are used on behalf of the user receiving the share.

For example, if a user with full file system rights to a folder shares Contributor privileges on that folder with another user, the other user has rights to create new files in the folder via the proxy user, as authorized by Filr.

Filr Component Security

- ◆ **Filr Software:** The Filr software is a customized version of Apache Tomcat. The version of Apache used for the Filr software contains all security fixes and patches that were available when Filr was released.
- ◆ **MySQL Database:** The Filr database is a MySQL database built with SuSE Studio, and contains all security fixes and patches that were available when Filr was released.
- ◆ **Filrsearch:** The Filrsearch index is a Lucene search index. It contains all security fixes and patches that were available when Filr was released.

Filr Data Security

- ◆ [“Understanding Administrator Access to Filr Data” on page 113](#)
- ◆ [“Limiting Physical Access to Filr Servers” on page 113](#)
- ◆ [“Protecting the Filr Database” on page 113](#)

Understanding Administrator Access to Filr Data

The Filr administrator can see all files and folders:

- ◆ In each user's My Files area (includes files in personal storage or files in a home directory on a remote file server)
- ◆ In every Net Folder

This includes file content as well as file metadata (comments, creation and modification information, and so forth).

Limiting Physical Access to Filr Servers

Servers where Micro Focus Filr data resides should be kept physically secure so that unauthorized persons cannot gain access to the server consoles.

Protecting the Filr Database

Depending on your local security guidelines, you might want to encrypt the database connections between the Filr software and the Filr database. SSL-encrypted data between the Filr application and the database server imposes a performance penalty because of the increased overhead of encrypting and decrypting the retrieved data.

Support for this is highly dependent on the database client drivers and JDBC connector support, and on how you are configuring your database client and server certificates. You should check with your database vendor on how to set up SSL connections on both the client and server sides of the connection. You might need to modify the JDBC URL on an all-in-one (small) Filr deployment. For example, for MySQL, you might add `useSSL=true&requireSSL=true` to the `options` part of the JDBC URL.

Filr's Rights Model

- ◆ Filr supports the following file systems:
 - ◆ Microsoft NTFS
 - ◆ Micro Focus NSS
- ◆ Filr supports the following native file access protocols:
 - ◆ Microsoft SMB/CIFS
 - ◆ Micro Focus NCP
- ◆ Many more storage subsystems and protocols are planned to be supported in future Filr releases.
- ◆ Instead of mapping the intricate and sophisticated rights models from each of the possibly many storage systems, Filr adopted a simplified rights model that maps to the rights models of many storage systems.

The four roles in Filr:

- ◆ **None:** No rights
- ◆ **Viewer:** READ and VISIBILITY rights
- ◆ **Editor:** READ, WRITE and VISIBILITY rights (WRITE includes modifying the contents of a file)
- ◆ **Contributor:** READ, WRITE, CREATE, DELETE, RENAME, MOVE, COPY

IMPORTANT: Folders only, not Files.

Also, the rights apply only to folder contents, not to the folder itself.

- ◆ Filr attempts to mimic the visibility features of each file system.

For example, if a user Tom has rights to a file in some sub-folders, Filr will ensure that Tom has VISIBILITY rights to all parent folders up to the top level of the Net Folder or My Files container.

Filr Security Defaults

- ◆ Client access is only allowed using REST over SSL (HTTPS), using unique self-signed certificates for each instance.
- ◆ All access through Filr is turned off by default.
- ◆ All Filr sharing is off by default.
- ◆ User provisioning can be done via LDAP over SSL (LDAPS).
- ◆ Filr supports replacing self-signed certificates with certificates that have been signed by a trusted certificate authority (CA).
- ◆ All security-related credentials and passwords are encrypted with unique 2048-bit keys.
- ◆ Communication between virtual machines is authenticated and encrypted.

Filr Site Security

- ◆ [“Configuring a Proxy Server” on page 114](#)
- ◆ [“Setting the Filr Administrator Password” on page 114](#)
- ◆ [“XSS—Filr Is Secure” on page 115](#)

Configuring a Proxy Server

Your Micro Focus Filr system should be located behind your firewall. If Filr users want to access the Filr site from outside your firewall, you should set up a proxy server outside your firewall to provide access. You can use NetIQ Access Manager to protect your Filr site, as described in [Access Manager \(NAM\) and Filr Integration](#) in the [Filr 3.4: Installation, Deployment, and Upgrade Guide](#).

Setting the Filr Administrator Password

The Filr site is initially installed to allow administrator access by using the user name `admin` and the password `admin`. You are prompted to change the Filr administrator password the first time you log in to the [Port 9443 Appliance Console](#). Thereafter, you can change the password as described in [“Modifying Port 8443 Administrators” on page 15](#).

XSS—Filtr Is Secure

Cross-site scripting (XSS) is a client-side computer attack that is aimed at web applications. Because XSS attacks can pose a major security threat, Micro Focus Filr contains a built-in security filter that protects against XSS vulnerabilities. This security filter is enabled by default.

The following sections describe the types of content that the security filter blocks from the Filr site, where exactly it blocks it from entering, and how you can disable the security filter or enable specific users to bypass the security filter.

- ◆ [“Understanding What Content Is Not Permitted” on page 115](#)
- ◆ [“Understanding Where the Content Is Not Permitted” on page 115](#)
- ◆ [“Listing All XSS Threats in Your System” on page 115](#)

Understanding What Content Is Not Permitted

By default, the XSS security filter in Filr is very strict, and does not allow users to add certain types of content. For example, the following content is not permitted:

- ◆ HTML that contains JavaScript
- ◆ Forms
- ◆ Frames
- ◆ Objects
- ◆ Applets

Understanding Where the Content Is Not Permitted

The type of content discussed in [“Understanding What Content Is Not Permitted” on page 115](#) is filtered by Filr in the following areas:

- ◆ Text and HTML fields in entries and folders
- ◆ Uploaded HTML files

Listing All XSS Threats in Your System

Filtr enables you to run an XSS report that lists XSS threats that are contained in your Filr system. For more information, see [“XSS \(Cross-Site Scripting\) Report”](#) in the *Filtr 3.4.1: Administrative UI Reference*.

LDAP Synchronization Security

If your LDAP directory service requires a secure LDAP connection (LDAPS), you must configure Micro Focus Filr with a root certificate. The root certificate identifies the root certificate authority (CA) for your Filr site, which enables you to export a self-signed root certificate based on your eDirectory or Active Directory tree.

- ◆ [“Exporting a Root Certificate” on page 116](#)
- ◆ [“Importing the Root Certificate into the Java Keystore” on page 117](#)

Exporting a Root Certificate

- ♦ [“Exporting a Root Certificate for eDirectory” on page 116](#)
- ♦ [“Exporting the Root Certificate for Active Directory” on page 116](#)

Exporting a Root Certificate for eDirectory

- 1 Launch and log in to iManager for your tree.
- 2 Click **Directory Administration**.
- 3 Click **Modify Object**.
- 4 Click the magnifying glass icon to browse to and select the “*Tree Name CA*” object in the Security container of the eDirectory tree.
- 5 Click **OK**.
- 6 Click the **Certificates** tab.
- 7 Select the check box for the root certificate (this is not the certificate titled **Self Signed Certificate**, but rather the root certificate), then click **Validate**.
- 8 Select the check box for the root certificate, then click **Export**.
- 9 Deselect **Export private key**, then click **Next**.
- 10 Click **Save the exported certificate**, then select **File in binary DER format**.
- 11 Save the file to a location where it can be accessed later and with a file name that you can remember, such as `SelfSignCert.der`.
- 12 Click **Close > OK**.
- 13 Continue with [“Importing the Root Certificate into the Java Keystore” on page 117](#).

Exporting the Root Certificate for Active Directory

- 1 On the Windows server, click **Start > Run**, then enter `mmc`.
- 2 In MMC, type `Ctrl+M`.
- 3 If the **Internet Information Services (IIS) Manager** snap-in is not installed on your Windows server, install it.
- 4 With IIS selected, click **Add**, then click **OK**.
- 5 In the left frame, click **Internet Information Services**, then click a Windows server that Filr can connect to for synchronizing users.
- 6 In the Filter list, scroll down to **Server Certificates** and double-click the icon.
- 7 In the **Actions** list, click **Create Self-Signed Certificate**.
- 8 Name the certificate with a name you can remember, such as the server name, then click **OK**.
- 9 Type `Ctrl+M`, select the **Certificates** plug-in, then click **Add**.
- 10 Select **Computer account**, then click **Next**.
- 11 Click **Finish**.
- 12 In the Snap-ins dialog, click **OK**.
- 13 In MMC, expand the **Certificates** plug-in, expand **Personal**, then click **Certificates**.
- 14 Right-click the certificate you created, select **All Tasks**, then click **Export...**
- 15 In the Certificate Export wizard, click **Next**.

- 16 Ensure that **No, do not export the private key** is selected, then click **Next**.
- 17 Ensure that **DER encoded binary** is selected, then click **Next**.
- 18 Name the certificate, then click **Next**.
- 19 Click **Finish > OK**.
The certificate is saved in `C:\Users\Your-User-Name`.
- 20 Ensure that the certificate is accessible from your management browser.
- 21 Continue with [“Importing the Root Certificate into the Java Keystore”](#) on page 117.

Importing the Root Certificate into the Java Keystore

- 1 Navigate to the management console of your Micro Focus Appliance:

```
https://ip_address:9443
```

- 2 Under Appliance Configuration, click **Digital Certificates**.
- 3 In the **Key Store** drop-down list, select **JVM Certificates**.
- 4 Click **File > Import > Trusted Certificate**.

A `.der` certificate is required for the import to be successful.

- 5 Browse to and select the trusted root certificate that you want to import.

If you want to import multiple certificates, ensure that the certificate names are different for each certificate.

- 6 Do not make any changes to the **Alias** field. It is populated by default.
- 7 Click **OK**.

The certificate should now be displayed in the list of JVM certificates.

- 8 Restart Filr so that Tomcat rereads the updated Java keystore file.

You can restart the Filr service as described in [“Shutting Down and Restarting the Micro Focus Appliance”](#) in the *Filr 3.4.1: Administrative UI Reference*.

You are now ready to configure your Filr site for secure LDAP synchronization, as described in see [“LDAP Servers and Synchronization”](#) in the *Filr 3.4.1: Administrative UI Reference*.

Mobile Device Data Security

- ♦ [“App Security”](#) on page 117
- ♦ [“File Security”](#) on page 118

App Security

On Android devices, the application itself and cached content are stored on internal storage. Internal storage on Android devices is always secure (unless the device has been rooted contrary to manufacturer recommendations). iOS devices do not have a concept of external storage, so data within the application is always secure.

File Security

Files that are downloaded or opened in third-party apps are by nature less secure than files that remain within the app. On Android devices, downloaded files are stored on the device's external storage.

It is up to you as the Filr administrator to decide whether to allow users to download files and open them in third-party applications, as described in “[Mobile Device Access—Default Settings](#)” in the *Filr 3.4.1: Administrative UI Reference*.

In order for downloaded files to remain secure, users should configure their devices to encrypt files. However, not all devices support file encryption. For information about how to enable file encryption on iOS and Android devices, see “[Encrypting Downloaded Files](#)” in the *Micro Focus Filr Mobile App*.

NESSUS Scans

The Filr development team runs NESSUS scans on all Filr code and fixes all reported problems.

This means that no unexpected ports are open and all open ports are protected according to industry standards.

Proxy User Security

- ♦ Filr uses administrator-created proxy users for communicating with LDAP providers and Net Folder servers.
- ♦ LDAP proxy users must have sufficient rights to read user and group objects from the desired contexts within LDAP providers.
- ♦ Net Folder proxy users must have full rights to the file server volumes or shares that contain the Net Folders.
- ♦ Proxy users' identities and credentials are secured, encrypted, and protected in Filr.

Security Scan Risk Reports

Running regular security scans on your network is critical to security administration. Security is a top priority for the Filr development team.

Occasionally, reputable security scanning software reports risks that the Filr team considers to be less significant than reported. The following are specific examples:

- ♦ **PHP as a Security Vulnerability:** Although in many cases the presence of PHP scripts is a legitimate concern, in the case of Filr, there is no PHP access without first authenticating through port 9443. Since access through port 9443 is secure by definition, Filr's PHP implementation is secure.
- ♦ **Diffie-Hellman 1024 Keys:** If you run a Nessus or equivalent security scan, you might receive a report of “Medium Risk” associated with Diffie-Hellman 1024-bit keys.

The Filr team is aware of this and is considering increasing the key size in a future release. At this time, however, the team does not feel that this is a significant threat to Filr installations; breaking 1024-bit keys requires computing resources that only a nation-state would have at its disposal.

If you are concerned or feel that your organization might be vulnerable to nation-state attacks, you can specify a stronger key through the Java security policy.

Sharing and Security

- ◆ Sharing is turned off by default.
- ◆ Sharing controls must be configured for files in the My Files area (includes users' personal storage and Home directories) and for Net Folders.
 - ◆ Sharing for files in the My Files area can be configured on a global level for all users or for individual users or groups.
 - ◆ Even if sharing is turned on for a given user or group, it must also be turned on at every Net Folder and for each user for files in their Home folder.
- ◆ My Files vs. Net Folders
 - ◆ **My Files:** Filr expects that you want users to be able to share their own files and folders. After sharing is enabled at the global level, users can share files and folders in their **My Files** area by default (includes users' personal storage and Home directories).
 - ◆ **Net Folders:** Filr expects that you do not want users sharing files in **Net Folders** unless they are specifically authorized to do so. Sharing is enabled at the global level for **Net Folders**. However, users cannot share the files in any Net Folder until you specifically turn sharing on for them at the Net Folder level (either individually or as part of a group). Folders within Net Folders cannot be shared.
- ◆ Sharing privileges are granular:
 - ◆ **Share Internal:** Users can share only with internal users (provisioned and administrator-created local users).
 - ◆ **Share External:** Users can share with external users. These are users that have been invited via an email notification to provision themselves as users in Filr based on their email address identity.
 - ◆ **Share public:** Users can share with the public. No authentication is required. The URL that is shared in public sharing can be forwarded, posted, emailed, tweeted, blogged, and disseminated in any way. Anyone who has that URL can access the shared information.

SSH Access for the Root User

By default, the root user is able to SSH to each appliance in the Filr system. You can disable this access on each appliance so that only the vaadmin user can SSH to the system.

See "[Changing Passwords and SSH Access for vaadmin and root](#)" in the *Filr 3.4.1: Administrative UI Reference*.

Universal Passwords (eDirectory) Security

If you use Universal Passwords and eDirectory LDAP is not NMAS-aware, users are able to log in to Filr with case-insensitive passwords even though the passwords are actually case sensitive. For example, they can log in with 'p@\$wrD1!' when their password is 'P@\$Wrd1!'

In addition to the security concern, when users log in with the incorrect case, they cannot upload any files.

To prevent users from logging in to Filr with an incorrect password, set eDirectory LDAP to be NMAS-aware by following the instructions in this [TID \(https://www.novell.com/support/kb/doc.php?id=3307424\)](https://www.novell.com/support/kb/doc.php?id=3307424).

Users and Security

- ◆ Filr supports authentication using IDs and credentials that are validated with the LDAP identity source from which they were provisioned. The credentials from these LDAP providers are cached within Filr, but they are never really synchronized from the LDAP provider.
- ◆ Local users that are not provisioned via LDAP have their local credentials stored in Filr. These credentials are secured, encrypted, and protected.

WebDAV Support

WebDAV is a standard collaborative editing and file management protocol. Micro Focus Filr relies on the WebDAV protocol to edit files, as described in “[Working with files](#)” in the *Filr 3.4: User Access Guide*.

If your Filr users are running a supported client operating system other than Windows 7, editing files works without any problems. Windows 7 must be configured to use a self-signed certificate in order to work with WebDAV.

The information in this section assumes that your environment requires the use of Microsoft Office. If your environment does not require the use of Microsoft Office, see “[Using OpenOffice as Your Document Editor for WebDAV](#)” on page 122.

- ◆ “[Planning Your WebDAV Implementation](#)” on page 120
- ◆ “[Disabling WebDAV for Filr Site](#)” on page 122
- ◆ “[Editing Files with Edit-in-Place Functionality](#)” on page 122
- ◆ “[Mapping a Filr Folder as a WebDAV Folder](#)” on page 123
- ◆ “[Configuring Windows to Use a Self-Signed Certificate with Filr](#)” on page 123
- ◆ “[Allowing Basic Authentication over an HTTP Connection on Windows 7](#)” on page 125

Planning Your WebDAV Implementation

- ◆ “[Understanding the Different Types of WebDAV Authentication Methods](#)” on page 121
- ◆ “[Using WebDAV When Filr Is Fronted by NetIQ Access Manager](#)” on page 121
- ◆ “[Meeting Filr Certificate Requirements on Windows 7](#)” on page 121
- ◆ “[Using OpenOffice as Your Document Editor for WebDAV](#)” on page 122

Understanding the Different Types of WebDAV Authentication Methods

Micro Focus Filr supports the following WebDAV authentication methods:

- ♦ **Basic Authentication:** The user name and password are encoded with the Base64 algorithm. The Base64-encoded string is unsafe if transmitted over HTTP, and therefore should be combined with SSL/TLS (HTTPS).

For more information, see “[WebDAV Authentication Configuration Settings](#)” in the *Filr 3.4.1: Administrative UI Reference*.

If you plan to use Basic authentication over a non-secure connection (HTTP), you need to modify the registry on each Windows 7 client workstation, as described in “[Allowing Basic Authentication over an HTTP Connection on Windows 7](#)” on page 125. The registry modification allows users to use WebDAV with Microsoft Office 2007. However, Microsoft Office 2010 is not supported.

- ♦ **Digest Authentication:** Applies MD5 cryptographic, one-way hashing with nonce values to a password before sending it over the network. This option is more safe than Basic Authentication when used over HTTP.

For more information, see “[WebDAV Authentication Configuration Settings](#)” in the *Filr 3.4.1: Administrative UI Reference*.

Using WebDAV When Filr Is Fronted by NetIQ Access Manager

If your Filr system is fronted by NetIQ Access Manager, you must use the designated WebDAV authentication method:

Product Fronting Filr	Designated Authentication Method
NetIQ Access Manager	<p>If your Filr installation is fronted by NetIQ Access Manager, as described in see “Access Manager (NAM) and Filr Integration” in the <i>Filr 3.4: Installation, Deployment, and Upgrade Guide</i>, you must use basic authentication for your WebDAV implementation.</p> <p>During the Filr appliance configuration, select basic when configuring WebDAV, as described in see “WebDAV Authentication Configuration Settings” in the <i>Filr 3.4.1: Administrative UI Reference</i>.</p>

Meeting Filr Certificate Requirements on Windows 7

If you are using WebDAV functionality with Filr on Windows 7 with a secure (HTTPS) connection, ensure that the Filr server certificate requirements are met. If all of the requirements are not met, various Windows 7 services fail.

Filr server certificate requirements:

- ♦ You must use a trusted server certificate that is accepted by Windows 7. This server certificate must be signed by a trusted certificate authority (CA) such as VeriSign or Equifax.

NOTE: You can use a self-signed certificate only if the certificate is imported into the Trusted Root Certification Authorities store on each Windows 7 client computer.

- ♦ The trusted server certificate must be issued to a name that exactly matches the domain name of the URL that you are using it for. This means that it must match the URL of your Filr site.
- ♦ The date range for the trusted server certificate must be valid. You cannot use an expired server certificate.
- ♦ The Windows 7 system must be adjusted to enable FIPS-compliant algorithms for encryption, hashing, and signing, unless you are using Micro Focus Access Manager 4.1.1 or later.
 1. From the Start menu, type **Local Security Policy**, then press Enter.
 2. Expand **Local Policies**, then select **Security Options**.
 3. Enable the following setting:

System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing.

Using OpenOffice as Your Document Editor for WebDAV

If your environment does not require the use of Microsoft Office, you might consider migrating users to OpenOffice 3.1 or later as their document editor. Using OpenOffice 3.1 or later provides seamless integration between the WebDAV server and Filr, regardless of which operating system is being used.

Disabling WebDAV for Filr Site

If you do not want your Filr users to use the edit-in-place functionality, then disable WebDAV for the Filr site.

To disable WebDAV for a Filr site, perform the following steps or review the [KB article \(https://www.netiq.com/support/kb/doc.php?id=7021147\)](https://www.netiq.com/support/kb/doc.php?id=7021147).

- 1 In a text editor, open the `/opt/novell/filr/apache-tomcat/webapps/ssf/WEB-INF/classes/config/ssf-ext.properties` file.
- 2 Add the following setting:


```
access.webdav.enable=false
```

Editing Files with Edit-in-Place Functionality

IMPORTANT

- ♦ Due to security concerns about the NPAPI cross platform plug-in architecture, Google's Chrome browser version 45 and later and Microsoft's Edge browser have discontinued support for the Java browser plug-in. Because Filr's Edit-in-Place functionality relies on the plug-in, Edit-in-Place is no longer supported in these browsers.

Micro Focus anticipates that other browser vendors might also discontinue support for the Java browser plug-in in the near future.

- ♦ Users can use the edit-in-place functionality to edit a file only if WebDAV is enabled on the Filr site. If you do not want your Filr users to use the edit-in-place functionality, then disable WebDAV for the Filr site. See [“Disabling WebDAV for Filr Site” on page 122](#).
-

If you are using a browser that still supports the NPAPI plug-in architecture, you can leverage Edit-in-Place functionality. For information on how to edit files in Filr with Edit-in-Place functionality, see [“Working with files”](#) in the *Filr 3.4: User Access Guide*.

If you are using Edit-in-Place functionality over HTTP, no additional setup is required. However, if you are using Edit-in-Place functionality over HTTPS on Windows 7, ensure that you have met the Filr server certificate requirements, as described in [“Meeting Filr Certificate Requirements on Windows 7” on page 121](#).

For more information about editing Filr documents in Microsoft Office with Windows 7, see “TID 7006717: Document editing failure with Windows 7 and Microsoft Office” in the [Support Knowledgebase \(http://www.novell.com/support/kb/\)](#).

Mapping a Filr Folder as a WebDAV Folder

Mapping a Micro Focus Filr folder as a WebDAV folder on the client computer allows access to Filr files from a WebDAV-compliant file navigation tool such as Windows Explorer or Nautilus. For information on how to map a Filr folder, see [“Adding Files to a Folder through WebDAV”](#) in the *Filr 3.4: User Access Guide*.

When you map a Filr folder as a WebDAV folder on Windows 7, ensure that all Filr server certificate requirements are met, as described in [“Meeting Filr Certificate Requirements on Windows 7” on page 121](#).

Configuring Windows to Use a Self-Signed Certificate with Filr

Configuring Windows to use a self-signed certificate with Micro Focus Filr is a two-step process. The first step is accomplished by the Filr administrator on the Filr server, and the second step is accomplished by each Filr user on his or her Windows workstation.

- ◆ [“Administrator Configuration Responsibilities” on page 123](#)
- ◆ [“User Configuration Responsibilities on Windows 7 Workstation” on page 123](#)
- ◆ [“User Configuration Responsibilities on Windows 10 Workstation” on page 124](#)

Administrator Configuration Responsibilities

- 1 Ensure that the following prerequisites are met in order to configure Windows to use a self-signed certificate with Filr:
 - ◆ The self-signed server certificate must be issued to a name that exactly matches the domain name of the URL that you use it for. This means that it must match the URL of your Filr site.
 - ◆ The date range for the trusted server certificate must be valid. You cannot use an expired server certificate.

User Configuration Responsibilities on Windows 7 Workstation

Each Windows 7 workstation user must import the self-signed certificate of the Filr server into the **Trusted Root Certification** Authorities store.

In a controlled corporate environment where the system administrator sets up each client workstation before use, this certificate can be preinstalled on each Windows 7 workstation. This can minimize end-user error and frustration.

- 1 Launch the Internet Explorer browser.
- 2 Click **Tools > Internet Options** to display the Internet Options dialog box.

- 3 Click the **Security** tab, then select **Trusted sites**.
- 4 Click **Sites**.
- 5 In the **Add this website to the zone** field, specify the URL of the Filr web site, then click **Add > Close**.
- 6 Browse to your Filr site.
- 7 (Conditional) If a prompt displays indicating that there is a problem with this web site's security certificate, complete the following steps:
 - 7a Click **Continue to this website (not recommended)**.
 - 7b Click **Certificate Error** at the right of the address bar, then click **View certificates**.
 - 7c Click **Install Certificate**, then click **Next** in the wizard.
 - 7d Select **Place all certificates in the following store**.
 - 7e Click **Browse**, browse to and select **Trusted Root Certification Authorities**, then click **OK**.
 - 7f In the wizard, click **Next**, then click **Finish**.
 - 7g (Conditional) If a Security Warning dialog box displays, click **Yes**.
 - 7h Click **OK** to close the Certificate Import Wizard.
 - 7i Click **OK** to close the Certificate window.
 - 7j Shut down all instances of the Internet Explorer browser, then restart the browser.
 - 7k Browse to the Filr site. You should no longer see the certificate error message.

If you continue to see the certificate error message, the server's self-signed certificate might not match the site URL, as described in ["Administrator Configuration Responsibilities" on page 123](#).

User Configuration Responsibilities on Windows 10 Workstation

Each Windows 10 workstation user must import the self-signed certificate of the Filr server into the **Trusted Root Certification Authorities** store.

In a controlled corporate environment where the system administrator sets up each client workstation before use, this certificate can be preinstalled on each Windows 10 workstation. This can minimize end-user error and frustration.

- 1 On the workstation, click **Start > Run**, then enter `mmc` and click **OK**.
- 2 In the Console, click **File > Add/Remove Snap-in**
- 3 In the Add or Remove Snap-ins window, select **Certificates** in left panel and click **Add** to move to right panel, then click **OK**.
- 4 Select **Computer account** and click **Next**.
- 5 Select the **Local computer** option, then click **Finish**.
- 6 Click **OK**.
- 7 To import trusted certificate, expand **Certificates**. Right-click **Personal > All tasks > Import**.
- 8 In the Certificate Import Wizard, click **Next**.
- 9 Click **Browse** to select the `self-signed_cert.crt` certificate file and click **Next**.
For more about self-signed certificate, see ["Exporting a Self-Signed Certificate" on page 104](#).
- 10 Select **Place all certificates in the following store** and click **Next**.
- 11 Click **Finish** to import the certificate.
- 12 Click **OK**.

Browse to the Filr site. You should no longer see the certificate error message.

If you continue to see the certificate error message, the server's self-signed certificate might not match the site URL, as described in [“Administrator Configuration Responsibilities” on page 123](#).

Allowing Basic Authentication over an HTTP Connection on Windows 7

You can modify the Windows registry to allow Basic authentication to WebDAV over an HTTP connection. This registry change allows users to use Microsoft Office 2007 on the Windows 7 operating system, but does not allow them to use Microsoft Office 2010. Microsoft Office 2010 is not supported with Basic Authentication over an HTTP connection.

To modify the Windows registry:

- 1 On each Windows 7 workstation, click **Start > Run**, then specify `regedit` in the **Open** field.
- 2 Click **OK**.
- 3 In the Registry Editor window, navigate to the following registry entry:

```
\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlset\services\WebClient\Parameters\BasicAuthLevel
```

- 4 Change the value of this registry entry to 2.
- 5 Navigate to the Services interface, then restart the **WebClient** service.

XSS Security Filter

Cross-site scripting (XSS) is a client-side computer attack that is aimed at Web applications. Because XSS attacks can pose a major security threat, Micro Focus Filr contains a built-in security filter that protects against XSS vulnerabilities.

The XSS security filter protects the Filr site from XSS in two key areas:

- ♦ Text and HTML fields in entries and folders
- ♦ Uploaded HTML files

19 Storage Management

- ◆ [“Backing Up Filr Data” on page 127](#)
- ◆ [“Changing the CIFS /vashare Mount Point Login Credentials” on page 129](#)
- ◆ [“Configuring Home Folders for Display in the My Files Area” on page 129](#)
- ◆ [“Disk Usage Checks” on page 131](#)
- ◆ [“Personal Storage \(My Files\) Management” on page 131](#)

Backing Up Filr Data

Reliable backups are critical to the stability of your Micro Focus Filr site.

IMPORTANT: Do not use VMware snapshots as a backup method for Filr. Doing so creates problems when managing the system disk and inhibits your ability to update Filr in the future.

- ◆ [“Locating Filr Data to Back Up” on page 127](#)
- ◆ [“Scheduling and Performing Backups” on page 128](#)
- ◆ [“Restoring Filr Data from Backup” on page 128](#)
- ◆ [“Manually Restoring Individual Files and Folders” on page 128](#)

Locating Filr Data to Back Up

In order to keep adequate backups of your Micro Focus Filr data, you must back up the following types of data:

- ◆ [“Filr File Repository \(/vastorage\)” on page 127](#)
- ◆ [“Filr Database” on page 127](#)
- ◆ [“Lucene Search Index” on page 128](#)
- ◆ [“Certificates” on page 128](#)

Filr File Repository (/vastorage)

Back up the following location on the Filr appliance. In a large deployment, back up this location on each Filr appliance in the cluster.

```
/vastorage/filr/filerepository
```

Filr Database

Back up the following location on the Filr appliance (in a small deployment) or on the MySQL database appliance (in a large deployment):

```
/vastorage/mysql
```

Specifically, you should back up the following databases: `filr`, `information_schema`, `mysql`

Refer to the [database backup method information \(http://dev.mysql.com/doc/refman/5.0/en/backup-methods.html\)](http://dev.mysql.com/doc/refman/5.0/en/backup-methods.html) in the MySQL documentation.

Lucene Search Index

You can back up the following location on the Filr appliance (in a small deployment) or the Lucene search index appliance (in a large deployment):

```
/vastorage/search
```

The Lucene search index does not need to be backed up because it can be rebuilt at any time. For information about how to rebuild the Lucene search index, see [“Rebuilding the Lucene Index” on page 98](#).

Certificates

Back up the following location on the Filr appliance. In a large deployment, back up this location on each Filr appliance in the cluster.

```
/vastorage/conf
```

Scheduling and Performing Backups

You do not need to bring your Micro Focus Filr site down in order to perform backups. You might want to back up the Filr file repository and the Filr database every night, perhaps doing a full backup once a week and incremental backups on other days. You can back up the Lucene index whenever it is convenient. You can always reindex the Filr site in order to re-create the Lucene index, but being able to restore content from a backup can save time in case of an outage.

Restoring Filr Data from Backup

If you need to restore your Micro Focus Filr site from a backup, restoring the same backup version for both the file repository and the database creates a Filr site that is consistent within itself but might be missing information that was added after the backups were created. If you lose the file repository but not the database, you can restore the backed-up file repository and keep the more current database, but some files are missing from the file repository.

Manually Restoring Individual Files and Folders

Files and folders from users' My Files area (personal storage) that were moved to the trash and were not permanently deleted can be restored from the trash. Unlike files from users' personal storage, files from Net Folders cannot be restored from the Filr trash.

The Filr administrator can view all items that were moved to the trash and restore them to their previous location, as described in [“Restoring Files and Folders from the Trash” on page 132](#).

Individual Filr users can restore items from the trash, as described in [“Restoring Items from the Trash”](#) in the *Filr 3.4: User Access Guide*.

Changing the CIFS /vashare Mount Point Login Credentials

If the user name and/or password changes for the [CIFS share that you created for your Filr appliances](#), you can change credentials by doing the following:

- 1 At the Filr terminal prompt, log in as `root`.
- 2 Type the following command to navigate to the `base` directory:

```
cd /etc/opt/novell/base
```
- 3 Display the first lines of the file:

```
vi .smbcredentials
```
- 4 In the vi editor, modify the credentials as desired.

Configuring Home Folders for Display in the My Files Area

Most organizations using Open Enterprise Server (OES) or Windows will have user Home folders. If your organization has existing Home folders for users, the Net Folder Server will be discovered and created automatically when you provision users during the LDAP synchronization process. (For information about how to synchronize users via LDAP, see [“LDAP Servers and Synchronization”](#) in the *Filr 3.4.1: Administrative UI Reference*.) After the synchronization is complete, you are reminded to complete the Net Folder Server setup (by adding proxy credentials) when logging in to the Filr administration console.

If your organization does not currently leverage user Home folders on OES or Windows, you must first create a connection to your existing file system by creating a Net Folder Server. Then you can create a connection to specific volumes (on OES servers) and shares (on Windows servers) by creating a Net Folder.

- ♦ [“Configuring Home Folders” on page 129](#)
- ♦ [“Editing Home Folders for Individual Users” on page 130](#)
- ♦ [“Understanding How Home Folders Relates to Personal Storage” on page 131](#)

Configuring Home Folders

- ♦ [“Prerequisites” on page 129](#)
- ♦ [“Configuring Home Folders” on page 130](#)

Prerequisites

If you are using Active Directory, the Active Directory Home folder for users must be configured as if it were on a network folder, even if the Home folder is local to the server. It cannot be configured on a local path.

To change a user’s Home folder to be configured as a network folder:

- 1 In the Active Directory Administrative Center, access a user’s profile information.
- 2 In the **Profile** section, in the **Home folder** area, select **Connect**.

- 3 Select a drive in the drop-down list, then use the **To** field to specify the path to the local directory.
For example, \\172.17.2.3\HOME\jchavez

Configuring Home Folders

To configure Home Folders to be displayed in the My Files area:

- 1 Configure synchronization from your LDAP directory, as described in “[LDAP Servers and Synchronization](#)” in the *Filr 3.4.1: Administrative UI Reference*.
- 2 Configure the Net Folder Server, as described in “[Creating and Managing Net Folder Servers](#)” in the *Filr 3.4.1: Administrative UI Reference*

IMPORTANT: The Filr administrator must supply proper proxy account information for Net Folder Servers that contain home directories before any end user logs in to Filr. This is because Filr automatically synchronizes the metadata for each user’s Home folder using the appropriate Net Folder Server with its associated proxy user credentials when the user logs in for the first time. See “[How Filr Makes Files and Folders Visible to Users](#)” in the *Filr 3.4: Understanding How Filr Works*.

If you do not supply the proxy account information before the user logs in, the Home directories’ metadata is not synchronized correctly and the internal log files contain Null Pointer Exceptions.

Similarly, if the user Home folder is moved on the file system to a different volume or share or a different server, a new Net Folder Server is created and its metadata must be synchronized the first time the user logs in to Filr after the move.

-
- 3 (Optional) Allow users to have files and folders in personal storage in the My Files area in addition to the Home folder.

Whether users are allowed to have files in personal storage in the My Files area affects how the Home folder is displayed in the My Files area. For more information, see “[Enabling Personal Storage for Users and Groups](#)” in the *Filr 3.4.1: Administrative UI Reference*.

NOTE: A user’s personal workspace (including the Home folder) is not displayed until the user has logged in to one of the Filr clients (web, mobile, or desktop) at least one time.

Editing Home Folders for Individual Users


After Home folders have been configured as described in “[Configuring Home Folders](#)” on page 129, you can edit the Home folder settings for individual users:

- 1 Log in to the Filr site as the Filr administrator.
 - 1a Launch a web browser.
 - 1b Specify one of the following URLs, depending on whether you are using a secure SSL connection:

```
http://Filr_hostname:8080  
https://Filr_hostname:8443
```

Replace *Filr_hostname* with the hostname or fully qualified domain name of the Filr server that you have set up in DNS.

Depending on how you have configured your Filr system, you might not be required to enter the port number in the URL. If you are using NetIQ Access Manager, the Filr login screen is not used.

- 2 Click the **admin** link in the upper-right corner of the page, then click the **Administration Console** icon .
- 3 Under **Management**, click **User Accounts**.
- 4 Click the drop-down arrow next to the user whose properties you want to view, then click **User Properties**.
The User Properties page is displayed.
- 5 Click **Edit Home Folder**. (This option is displayed only if a Home folder has been configured for the user, as described in [“Configuring Home Folders” on page 129.](#))
- 6 Make any modifications to the configuration, synchronization schedule, and data synchronization settings.
For information about each option that you can modify for Net Folders, see [“Creating and Modifying Net Folders”](#) in the *Filr 3.4.1: Administrative UI Reference*.
- 7 Click **OK** to save your changes.

Understanding How Home Folders Relates to Personal Storage

For information about how Home folders relate to Personal storage in Filr, see [“Understanding My Files”](#) in the *Filr 3.4: Understanding How Filr Works*.

Disk Usage Checks

Each hour, Filr checks the amount of disk space that is being used on the system drive for a given appliance. If disk usage reaches 90% capacity or greater on the system drive for any appliance, the Filr and FAMT services are stopped.

Following are the scripts that are used to monitor disk usage for each type of appliance:

- ♦ **Filr Appliance:** `/etc/cron.hourly/filr-diskcheck.sh`
- ♦ **Search Index Appliance:** `/etc/cron.hourly/lucene-diskcheck.sh`
- ♦ **Database Appliance:** `/etc/cron.hourly/mysql-diskcheck.sh`

When the Filr and FAMT services are stopped because of low disk space, a message is logged to both the `/var/opt/novell/va_status` and `/var/log/messages` files.

After the services are stopped, you must clean up unneeded data or add additional disk space to the appliance before restarting the services.

Personal Storage (My Files) Management

As an administrator for Micro Focus Filr, you can perform management functions on all Filr folders. For information on how to perform general folder management functions, such as creating a folder, deleting a folder, moving a folder, and so forth, see [“Managing and Using Folders”](#) in the *Filr 3.4: User Access Guide*.

You can perform additional folder management tasks as the Filr administrator:

- ♦ [“Navigating the Workspace Tree” on page 132](#)
- ♦ [“Managing Workspace Disk Space Usage” on page 132](#)

- ♦ [“Restoring Files and Folders from the Trash” on page 132](#)
- ♦ [“Managing User Data Quotas” on page 133](#)
- ♦ [“Permanently Deleting Files from the Trash” on page 140](#)

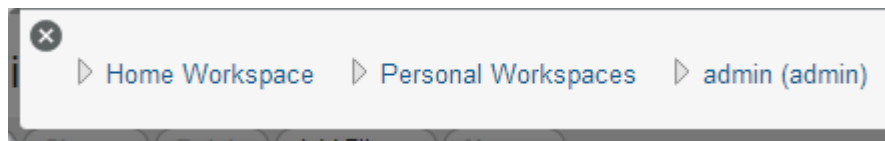
Navigating the Workspace Tree

You can use the Workspace Tree to navigate to any location on the Filr site. The Workspace Tree displays the path of all of the workspaces and folders that contain the place you are currently viewing, without leaving the current page.

This is the only way to navigate to another user’s My Files area.

Only the Filr administrator has access to the Workspace Tree.

- 1 Click the **Workspace Tree** icon  in the upper-left corner of any Filr page.



- 2 Navigate to and click the linked name of the desired location in the Workspace Tree.
- 3 (Optional) To navigate to a user’s My Files area, click a folder within that user’s personal workspace.

Managing Workspace Disk Space Usage

Disk space usage is managed on a folder basis as well as on an individual user or group basis.

For more information, see [“Managing and Restricting Filr-Based Storage”](#) in the *Filr 3.4.1: Administrative UI Reference*.

Restoring Files and Folders from the Trash

You can view all items that have been sent to the trash and restore them to their previous location.



IMPORTANT: Only items from a user’s My Files area (Personal Storage) that were moved to the trash are able to be restored from the trash. Items that were permanently deleted from a user’s My Files area cannot be restored. Items deleted from a Net Folder are never sent to the trash, and cannot be restored.

- 1 Log in to the Filr site as the Filr administrator.
 - 1a Launch a web browser.
 - 1b Specify one of the following URLs, depending on whether you are using a secure SSL connection:

```
http://Filr_hostname:8080
https://Filr_hostname:8443
```

Replace *Filr_hostname* with the host name or fully qualified domain name of the Filr server that you have set up in DNS.

Depending on how you have configured your Filr system, you might not be required to enter the port number in the URL. If you are using NetIQ Access Manager, the Filr login screen is not used.

- 2 Click the **admin** link in the upper-right corner of the page, then click the **Administration Console** icon .
- 3 Under **Management**, click **Users**.
The Manage Users page is displayed.
- 4 Click the **Trash** icon , located in the upper-right corner of the page.
- 5 Select the items that you want to restore, then click **Restore**.

Managing User Data Quotas

Each user's data quota establishes how much disk space the user's files can occupy in the Filr site. Folders that do not contain files do not count toward a user's data quota.

By default, users are not limited in the disk space that their files occupy in the Filr site. As the Filr administrator, you can decide when limiting users' disk space usage becomes appropriate.

- ♦ ["Planning User Data Quotas" on page 133](#)
- ♦ ["Setting User Data Quotas" on page 135](#)
- ♦ ["Modifying User Data Quotas" on page 136](#)
- ♦ ["Removing User Data Quotas" on page 138](#)
- ♦ ["Repairing a User's Data Quota" on page 139](#)
- ♦ ["Managing Your Personal Data Quota" on page 139](#)
- ♦ ["Monitoring User Data Quotas" on page 140](#)

Planning User Data Quotas

- ♦ ["Understanding User Data Quota Priority" on page 133](#)
- ♦ ["Selecting the Default User Data Quota for All Users" on page 134](#)
- ♦ ["Selecting an Appropriate High-Water Mark" on page 134](#)
- ♦ ["Determining Data Quotas for Specific Users" on page 134](#)
- ♦ ["Determining Data Quotas for Specific Groups" on page 134](#)

Understanding User Data Quota Priority

Because users can have multiple data quotas assigned to them (either individually, through group membership, or through the site-wide default), Filr prioritizes the existing data quotas and uses only one for each individual Filr user. If users have multiple data quotas that pertain to them, the priority level is as follows:

1. **User Quota:** A quota that is set for an individual user overrides the site-wide default quota and any other quotas that are associated with any groups where the user is a member.
2. **Group Quota:** A quota that is set for an individual group overrides the site-wide default quota. This pertains to all users who are members of that group.

When a user is a member of multiple groups that have data quotas associated with them, the user is given the highest data quota. For example, if a Filr user is a member of Group A, Group B, and Group C, and the data quotas for each of these groups is 10, 20, and 30, the Filr user's data quota is 30.

- 3. Site-Wide Default:** The site-wide default quota is used for all Filr users who have not been assigned individual quotas, and who are not associated with any groups where a quota has been set.

Selecting the Default User Data Quota for All Users

When you enable the data quota feature, the initial default data quota is 100 MB. This means that each Filr user can upload 100 MB of files and attachments to the Filr site.

When you select the default data quota for your Filr site, consider the size of your Filr site, the number of Filr users, the amount of available disk space, and so on. You can override the default data quota on a per-user and per-group basis, as described in [“Setting User Data Quotas” on page 135](#).

When a user adds enough files and attachments to exceed the data quota, the user can no longer attach files or create versions until existing files have been deleted and purged to free up storage space.

For information about purging deleted files to make storage space available, see [“Permanently Deleting Files from the Trash” on page 140](#).

For information about which data quota is used when users have multiple data quotas that pertain to them, see [“Understanding User Data Quota Priority” on page 133](#).

Selecting an Appropriate High-Water Mark

The high-water mark is the percentage of the data quota that must be reached before the user is made aware that he or she is approaching the data quota (a warning message is displayed on the user's profile page). The default high-water mark is 90% of a user's data quota.

This high-water mark also applies to data quotas that are set on workspaces and folders.

Determining Data Quotas for Specific Users

If there is a user in your Filr site who needs either a higher or lower data quota than the site-wide default, you can assign that user an individual user data quota.

When you set data quotas for specific users, remember that individual user data quotas override the default user data quota, as well as quotas that are assigned to any groups where the user is a member, as described in [“Understanding User Data Quota Priority” on page 133](#).

Determining Data Quotas for Specific Groups

When you set data quotas for specific groups, remember that group data quotas override the default site-wide data quota, but do not override individual user quotas, as described in [“Understanding User Data Quota Priority” on page 133](#).

Setting User Data Quotas

You can set data quotas for the entire Filr site, for individual groups, and for individual users.

- ♦ “Setting a Default Data Quota” on page 135
- ♦ “Setting Data Quotas for Individual Groups” on page 135
- ♦ “Setting Data Quotas for Individual Users” on page 136

Setting a Default Data Quota

Path: [Port 8443 Filr Administration Console](#)


When you set a default data quota, the quota applies to all Filr users who have not been assigned individual quotas, and who are not associated with any groups where a quota has been set.

- 1 Log in to the Filr site as the Filr administrator.
 - 1a Launch a web browser.
 - 1b Specify one of the following URLs, depending on whether you are using a secure SSL connection:

```
http://Filr_hostname:8080  
https://Filr_hostname:8443
```

Replace *Filr_hostname* with the host name or fully qualified domain name of the Filr server that you have set up in DNS.

Depending on how you have configured your Filr system, you might not be required to enter the port number in the URL. If you are using NetIQ Access Manager, the Filr login screen is not used.

- 2 Click the **admin** link in the upper-right corner of the page, then click the **Administration Console** icon .
- 3 Under **Management**, click **Personal Storage**.
- 4 Select **Enable User Data Quotas**.
- 5 Set the **Default User Data Quota Size** and **Default High-Water Mark** options as determined in “Planning User Data Quotas” on page 133.
- 6 Click **Apply** > **Close** to save the user data quota settings.


Setting Data Quotas for Individual Groups

- 1 Log in to the Filr site as the Filr administrator.
 - 1a Launch a web browser.
 - 1b Specify one of the following URLs, depending on whether you are using a secure SSL connection:

```
http://Filr_hostname:8080  
https://Filr_hostname:8443
```

Replace *Filr_hostname* with the host name or fully qualified domain name of the Filr server that you have set up in DNS.

Depending on how you have configured your Filr system, you might not be required to enter the port number in the URL. If you are using NetIQ Access Manager, the Filr login screen is not used.


- 2 Click the **admin** link in the upper-right corner of the page, then click the **Administration Console** icon .
- 3 Under **Management**, click **Personal Storage Quotas**.
- 4 Select **Enable User Data Quotas**.
- 5 Click **Add a Group**.
- 6 In the **Group** field, start typing the name of the group for which you want to set a quota, then click the group name when it appears in the drop-down list.
Repeat this process to add additional groups for which you want to assign the same data quota.
- 7 In the **Quota** field, specify the disk space limit for the group.
- 8 Click **OK**, then click **Apply > Close** to save the user data quota settings.

Setting Data Quotas for Individual Users

- 1 Log in to the Filr site as the Filr administrator.
 - 1a Launch a web browser.
 - 1b Specify one of the following URLs, depending on whether you are using a secure SSL connection:


```
http://Filr_hostname:8080  
https://Filr_hostname:8443
```


Replace *Filr_hostname* with the host name or fully qualified domain name of the Filr server that you have set up in DNS.

Depending on how you have configured your Filr system, you might not be required to enter the port number in the URL. If you are using NetIQ Access Manager, the Filr login screen is not used.
- 2 Click the **admin** link in the upper-right corner of the page, then click the **Administration Console** icon .
- 3 Under **Management**, click **Personal Storage Quotas**.
- 4 Select **Enable User Data Quotas**.
- 5 Click **Add a User**.
- 6 In the **User** field, start typing the name of the user for which you want to set a quota, then click the user's name when it appears in the drop-down list.
Repeat this process to add additional users for which you want to assign the same data quota.
- 7 In the **Quota** field, specify the disk space limit for the user.
- 8 Click **OK**, then click **Apply > Close** to save the user data quota settings.

Modifying User Data Quotas

Filr enables you to modify data quotas that you have previously set. You can modify data quotas for your entire Filr site, or modify data quotas for individual groups and users.

- ♦ [“Modifying User Data Quotas for the Entire Filr Site” on page 137](#)
- ♦ [“Modifying User Data Quotas for Individual Groups and Users” on page 137](#)

Modifying User Data Quotas for the Entire Filr Site


Filr enables you to easily modify the site-wide default user data quota.

- 1 Log in to the Filr site as the Filr administrator.
 - 1a Launch a web browser.
 - 1b Specify one of the following URLs, depending on whether you are using a secure SSL connection:

```
http://Filr_hostname:8080  
https://Filr_hostname:8443
```

Replace *Filr_hostname* with the host name or fully qualified domain name of the Filr server that you have set up in DNS.

Depending on how you have configured your Filr system, you might not be required to enter the port number in the URL. If you are using NetIQ Access Manager, the Filr login screen is not used.

- 2 Click the **admin** link in the upper-right corner of the page, then click the **Administration Console** icon .
- 3 Under **Management**, click **Personal Storage Quotas**.
- 4 In the **Default User Data Quota Size** field, delete the existing quota and specify the new quota. You can also modify the default high-water mark in the **Default High-Water Mark** field. For more information about the high-water mark, see [“Selecting an Appropriate High-Water Mark” on page 134](#).
- 5 Click **Apply > Close** to save the user data quota settings.

Modifying User Data Quotas for Individual Groups and Users


Filr enables you to easily modify individual group and user data quota settings that you have previously set.

- 1 Log in to the Filr site as the Filr administrator.
 - 1a Launch a web browser.
 - 1b Specify one of the following URLs, depending on whether you are using a secure SSL connection:

```
http://Filr_hostname:8080  
https://Filr_hostname:8443
```

Replace *Filr_hostname* with the host name or fully qualified domain name of the Filr server that you have set up in DNS.

Depending on how you have configured your Filr system, you might not be required to enter the port number in the URL. If you are using NetIQ Access Manager, the Filr login screen is not used.

- 2 Click the **admin** link in the upper-right corner of the page, then click the **Administration Console** icon .
- 3 Under **Management**, click **Personal Storage Quotas**.
- 4 In the **Group Quotas** table or **User Quotas** table, click the group name or user name that represents the group or user whose quota you want to modify.

- 5 In the **Quota** field, delete the existing quota and specify a new quota.
- 6 Click **OK**, then click **Apply > Close** to save the user data quota settings.

Removing User Data Quotas

Filr enables you to disable data quotas that you have previously set. You can disable data quotas for your entire Filr site, or remove data quotas from individual groups and users.

- ♦ [“Disabling User Data Quotas for the Entire Filr Site” on page 138](#)
- ♦ [“Removing User Data Quotas from Individual Groups and Users” on page 138](#)

Disabling User Data Quotas for the Entire Filr Site


If you decide that you no longer need to impose limits on the amount of data that users are permitted to upload into the Filr site, you can disable the data quota feature. Disabling the data quota feature enables all Filr users to upload as much data to the Filr site as they want.

- 1 Log in to the Filr site as the Filr administrator.
 - 1a Launch a web browser.
 - 1b Specify one of the following URLs, depending on whether you are using a secure SSL connection:

```
http://Filr_hostname:8080  
https://Filr_hostname:8443
```

Replace *Filr_hostname* with the host name or fully qualified domain name of the Filr server that you have set up in DNS.

Depending on how you have configured your Filr system, you might not be required to enter the port number in the URL. If you are using NetIQ Access Manager, the Filr login screen is not used.

- 2 Click the **admin** link in the upper-right corner of the page, then click the **Administration Console** icon .
- 3 Under **Management**, click **Personal Storage Quotas**.
The Data Quotas and File Upload Limits page is displayed.
- 4 Deselect **Enable User Data Quotas**, then click **Apply**.
Data quotas are no longer enabled for your Filr site.

Removing User Data Quotas from Individual Groups and Users


You can remove data quotas that you have previously set for individual groups and users. Users are held to the site-wide data quota default setting if they do not have an individual quota defined for them and they are not members of any groups where a group quota has been assigned.

- 1 Log in to the Filr site as the Filr administrator.
 - 1a Launch a web browser.
 - 1b Specify one of the following URLs, depending on whether you are using a secure SSL connection:

```
http://Filr_hostname:8080  
https://Filr_hostname:8443
```

Replace *Filr_hostname* with the host name or fully qualified domain name of the Filr server that you have set up in DNS.

Depending on how you have configured your Filr system, you might not be required to enter the port number in the URL. If you are using NetIQ Access Manager, the Filr login screen is not used.

- 2 Click the **admin** link in the upper-right corner of the page, then click the **Administration Console** icon .
- 3 Under **Management**, click **Personal Storage Quotas**.
- 4 In the **Group Quotas** table or **User Quotas** table, select the check box next to the group or user whose quota you want to remove.
- 5 Click **Delete**, then click **Apply > Close** to save the user data quota settings.

Repairing a User's Data Quota

It is possible for a user's data quota calculation to become inaccurate if errors occur during processing that is related to a user's file handling. If this happens and a user's quota calculation is inaccurate, you can repair the data quota:

- ♦ [“Repairing a User's Quota When an Individual Data Quota Is Set” on page 139](#)
- ♦ [“Repairing a User's Quota When a Default or Group Data Quota Is Set” on page 139](#)

Repairing a User's Quota When an Individual Data Quota Is Set

You can repair a user's data quota when an individual data quota is set on the user.

- 1 Remove the data quota that is set on the user, as described in [“Removing User Data Quotas from Individual Groups and Users” on page 138](#).
- 2 Set the data quota for the user again, as described in [“Setting Data Quotas for Individual Users” on page 136](#).

Repairing a User's Quota When a Default or Group Data Quota Is Set

You can repair a user's data quota when a default data quota is set, or when a group data quota is set and the user is a member of the group.

- 1 Set an individual data quota for the affected user, as described in [“Setting Data Quotas for Individual Users” on page 136](#).
- 2 Remove the individual data quota that you just set, as described in [“Removing User Data Quotas from Individual Groups and Users” on page 138](#).

Managing Your Personal Data Quota

NOTE: As a Filr administrator, you are also held to a data quota if quotas are enabled. If you want to assign yourself a larger quota than the site-wide default, you can add an individual quota for yourself, as described in [“Setting Data Quotas for Individual Users” on page 136](#).

All Filr users need to manage their personal data quotas. When you have a limited allocation of disk space, you need to be aware of the amount of disk space that you have available and how to make more disk space available as you approach your quota.

For information on how to accomplish these and other important tasks as you manage your data quota, see [“Managing Your Data Quota”](#) in the *Filr 3.4: User Access Guide*.

Monitoring User Data Quotas

You can monitor which users in the Filr site have exceeded or are close to exceeding their data quotas by generating the following reports, as described in [“Generating Filr-Monitoring Reports”](#) in the *Filr 3.4.1: Administrative UI Reference*:

- ◆ [Data Quota Exceeded Report](#)
- ◆ [Data Quota Highwater Exceeded Report](#)

Permanently Deleting Files from the Trash

You might want to permanently delete files in order to make space available within a data quota or to recover disk space.

- ◆ [“Permanently Deleting Files to Create Data Quota Space”](#) on page 140
- ◆ [“Permanently Deleting Files to Recover Disk Space”](#) on page 140

Permanently Deleting Files to Create Data Quota Space

When users delete files or file versions, the disk space occupied by the deleted files and versions counts against the data quotas until users permanently delete the files and versions, as described in [“Making Disk Space Available by Deleting Trashed Items”](#) in the *Filr 3.4: User Access Guide*.

As a Filr administrator, you can permanently delete files and versions anywhere on the Filr site in order to make space available within a user’s data quota.

Permanently Deleting Files to Recover Disk Space

Whether disk space is recovered after you permanently delete files using the Filr interface differs depending on whether you are deleting files in Net Folders or files from a user’s personal storage in the My Files area:

- ◆ [“Permanently Deleting Files in Net Folders”](#) on page 140
- ◆ [“Permanently Deleting Files in Personal Storage”](#) on page 140

Permanently Deleting Files in Net Folders

If you want to recover disk space on your file system, permanently deleting files in Net Folders using the Filr interface should also delete the files from the underlying file system, depending on the underlying implementation of the storage.

Permanently Deleting Files in Personal Storage

If you want to recover disk space on the Filr system, you must permanently delete the files from Filr

For information about how to purge items, see [“Making Disk Space Available by Deleting Trashed Items”](#) in the *Filr 3.4: User Access Guide*.

20 Troubleshooting

- ◆ [“Migration Fails to Modify the Owner Details and ACLs” on page 141](#)
- ◆ [“Configuring Filr Server Fails When Using NetApp ONTAP version 8.3.2 As a CIFS Vashare” on page 141](#)
- ◆ [“eDirectory Users Can Log In But Cannot Upload Files” on page 141](#)
- ◆ [“Email Notification URLs Are Not Working” on page 142](#)
- ◆ [“NetApp Net Folder Server Test Connection Fails” on page 142](#)
- ◆ [“Online Update Service Registration Fails With an Error Message” on page 142](#)
- ◆ [“Previously Available Files and Folders Disappear” on page 142](#)
- ◆ [“Unable to Connect to the Filr Site \(HTTP 500 Error\)” on page 143](#)
- ◆ [“Using VACONFIG to Modify Network Information” on page 143](#)
- ◆ [“Unable to Access Data on a DFS Junction In an OES Server Cluster Environment” on page 143](#)

Migration Fails to Modify the Owner Details and ACLs

Resolution: Before performing the migration, ensure to stop all Filr related processes to resolve this issue.

Problem: The Filr folder is only a mount point view and if it is in use during migration, then the user details and ACLs for that folder are not updated. Hence, stopping the Filr operations ensures successful migration of the owner details and ACLs.

Configuring Filr Server Fails When Using NetApp ONTAP version 8.3.2 As a CIFS Vashare

Problem: If you use NetApp ONTAP version 8.3.2 as a CIFS vashare, then you might encounter a HTTP 500 error when you configure the Filr server for the first time.

To workaround this issue, enter the MySQL and Lucene IP addresses again to reconfigure the Filr Server.

eDirectory Users Can Log In But Cannot Upload Files

See [““Universal Passwords \(eDirectory\) Security” on page 120.”](#)

Email Notification URLs Are Not Working

The network and reverse proxy settings that you configure after installing Filr affect how email notification URLs are constructed. If you have configured port redirection and have failed to verify the reverse proxy ports, email notifications from Filr can be constructed in such a way that users who click on the email notification URL are not able to access the Filr site.

When port redirection is enabled (as described in “[Using the Network \(Port Redirection\) dialog](#)” in the [Filr 3.4.1: Administrative UI Reference](#).), ensure that the reverse proxy ports are set to 80 for the HTTP port and to 443 for the secure HTTP port. To change the reverse proxy ports, see “[Reverse Proxy Configuration Settings](#)” in the [Filr 3.4.1: Administrative UI Reference](#).

NetApp Net Folder Server Test Connection Fails

Problem: Clicking the **Test Connection** option when creating a Net Folder Server for a NetApp device causes the following error to be logged in `/var/opt/novell/filr/log/smbclient.log`:
Could not retrieve case sensitivity flag: NT_STATUS_REVISION MISMATCH.

NetApp ONTAP versions earlier than 8.3.x have only limited support for the SMB v2 protocol. Nevertheless, NetApp sets the default protocol level to SMB v2.

If your NetApp devices are running an ONTAP version earlier than 8.3.x, you must set the protocol level to SMB v1 on the NetApp devices. Filr will then use SMB v1 for connecting and communicating with the devices.

Online Update Service Registration Fails With an Error Message

Problem: While registering the online update service, if you do not specify a value for the **Namespace** path when staging is enabled on the SMT server, the registration fails with a "An error occurred while communicating with the server" message.

On refreshing the page, the update service registration with the SMT server message is displayed on the page. However, no patches are displayed on the page even if they are available. Clicking the **Deregister** option in the Registration Status dialog fails to deregister the online update service.

To correctly register the online update service, perform the following steps:

- 1 In the SSH terminal, run the following command to deregister the existing incorrect registration:

```
zypper rs SMT-http_<HOSTNAME_OF_SMT_SERVER>
```
- 2 Log in to the Filr Appliance Console and register the online update service again.

Previously Available Files and Folders Disappear

Problem: Filr users (desktop, mobile, and web) are suddenly unable to see files and folders that were previously visible.

This happens when the metadata index no longer contains information for the objects that have disappeared, either because the Search server goes down, or because the index itself changes (for example, during a rebuild).

To understand how the index affects object availability and how to prevent file/folder disappearance, see “[Filtr Search Appliance—Accessibility, and Searchability](#)” in the *Filtr 3.4: Understanding How Filtr Works*.

Unable to Connect to the Filtr Site (HTTP 500 Error)

Problem: Trying to connect to Filtr yields an HTTP 500 error.

To fix this problem, ensure that your DNS server is properly configured and that your Filtr server is directed at the proper DNS server.

For information about how to configure Filtr to point to your DNS server, see “[Changing Network Settings](#)” in the *Filtr 3.4.1: Administrative UI Reference*.

Using VACONFIG to Modify Network Information

The easiest way to update the configuration information for the appliance (such as the IP address, host name, and so forth) after Filtr is already installed is to use the VACONFIG utility from the appliance command prompt:

- 1 In the vSphere client, select the Filtr appliance, then click the **Console** tab.
- 2 From the command prompt, log in to the appliance.
- 3 Type `vaconfig`, then press Enter.
- 4 In the VACONFIG utility, select **Configure**, then press Enter.
- 5 Press the Tab key until the IP address is selected, then modify the IP address as desired.
- 6 Select **Next**, then press Enter.

Unable to Access Data on a DFS Junction In an OES Server Cluster Environment

Problem: When the Filtr server encounters issue accessing data on a DFS junction in an OES cluster environment, the following error displays:

```
ERROR:ConvertXplatErrToFAMTErr xplat status: 0xc7e90503, sending generic error
```

To fix this problem, ensure that the VLDB service is up and running. For more information about the VLDB service, see [OES Documentation](#).

21 User and Group Maintenance

User accounts change over time and need periodic maintenance.

- ♦ “Adding and Creating Filr Users and Groups” on page 145
- ♦ “Creating Groups of Users” on page 145
- ♦ “Deleting Filr Users” on page 146
- ♦ “Disabling Filr User Accounts” on page 149
- ♦ “Renaming a Filr User” on page 150
- ♦ “User Maintenance Task Links” on page 150
- ♦ “Group Maintenance Task Links” on page 151

Adding and Creating Filr Users and Groups

You can add new users to your Filr site in any of the following ways:

- ♦ **LDAP:** Synchronize newly-added users from an LDAP directory, as described in “LDAP Servers and Synchronization” in the *Filr 3.4.1: Administrative UI Reference*.
- ♦ **Local:** Add local users and groups, as described in [Managing Users](#) and [Managing Groups](#) in the *Filr 3.4.1: Administrative UI Reference*.
- ♦ **Profile Files:** Import XML profile files to add and manage local users and groups, as described in “Import Profiles... button” in the *Filr 3.4.1: Administrative UI Reference*.

Creating Groups of Users

This section describes how to create groups within Filr. You can also synchronize groups of users from your LDAP directory to your Micro Focus Filr site, as described in “LDAP Servers and Synchronization” in the *Filr 3.4.1: Administrative UI Reference*.

You can create either static or dynamic groups.

Creating Static Groups

Path: [Port 8443 Filr Administration Console](#) > [Management](#) > [Groups](#) > [Add](#) > [Group Membership Is Stasis](#) > [Edit Group Membership](#)

For help specifying group membership, see “Static Membership for Group dialog” in the *Filr 3.4.1: Administrative UI Reference*.

Static groups contain only the users and groups that you specifically select as group members.

Static groups exist in Filr and can contain any users and groups in Filr, including LDAP-synchronized users and groups.

Creating Dynamic Groups

Groups based on LDAP queries are dynamic because they can be configured to have their membership updated when the information in the LDAP directory changes.

Creating groups based on LDAP queries is a quick way to create Filr groups that consist of users who match specific criteria. You can create dynamic groups as described in the following sections:

Creating Dynamic Groups within LDAP

Depending on the LDAP directory that you are using, you might be able to create dynamic groups within your LDAP directory. For example, you can create dynamic group objects in eDirectory with NetIQ iManager (for more information, see the [iManager Documentation \(https://www.netiq.com/documentation/imanager27/\)](https://www.netiq.com/documentation/imanager27/)).

Dynamic groups created within LDAP are stored in your LDAP directory and can then be synchronized to Filr, as described in “[LDAP Servers and Synchronization](#)” in the *Filr 3.4.1: Administrative UI Reference*.

Creating Dynamic Groups within Filr

Advantages of Filr Dynamic Groups:

- ♦ Allows Port 8443 admins, including Direct administrators, to control group membership without having direct access to the group object in the LDAP user store.
- ♦ Provides dynamic group functionality whether or not your LDAP directory supports dynamic groups.
- ♦ Filr-based dynamic groups don't synchronize to applications other than Filr that are leveraging your LDAP directory.

Path: [Port 8443 Filr Administration Console](#) > [Management](#) > [Groups](#) > [Add](#) > [Group Membership Is Dynamic](#) > [Edit Group Membership](#)

For help specifying group membership, see “[Edit Dynamic Membership dialog](#)” in the *Filr 3.4.1: Administrative UI Reference*.

Deleting Filr Users

When users no longer need access to your Micro Focus Filr site, you have two options to revoke their access to the Filr site: disabling or deleting their Filr user accounts.

Consider Disabling User Accounts Instead

Micro Focus recommends that you disable user accounts rather than deleting them, especially if there is a chance that a users might need Filr access in the future.

When you delete a user account, the deleted account can never be re-activated. Also, all files and folders that the user shared with other users are no longer accessible.

When you disable a user account, all the active shares from that user are still accessible. Also, the Filr administrator can use the Admin Console to edit the Filr share rights set on these shares. For more information about editing the shared settings, see “[Managing Shared Items](#)” in the *Filr 3.4.1: Administrative UI Reference*.

For information on how to disable a user, see [“User and Group Maintenance” on page 145](#).

Deleting User Objects and Workspaces

Path: [Port 8443 Filr Administration Console](#) > [Management](#) > [Users](#) > *select the users to delete* > **Delete**

Important Terminology

- ◆ **User Object:** This represents the user in the Filr system and contains:
 - ◆ The user’s profile information, including the profile picture and other information the user has entered.
 - ◆ Access controls to Personal Storage, individually assigned Quotas, and individually assigned Sharing rights.

If you delete a user object, the above information is permanently deleted from Filr and the user can no longer access Filr.

- ◆ **User Workspace:** This is a physical location in the Filr system where the following is stored:
 - ◆ Personal Storage, including any files and folders that were shared with other users.

If you move the workspace to trash, it can be recovered, as described in [“Recovering User Workspaces from the Trash” on page 149](#).

If you delete a user’s workspace, the Personal Storage associated with the users is permanently deleted and cannot be recovered.

However, the User Object still exists, and the user still has access to Filr, the user’s assigned Net Folders, items shared with the user, comments, and so on.

Options

When you choose to delete users, you can select from the following options before confirming the action.

Table 21-1 Available Options when Deleting Users

Users Have Home Directories	Options Available and Actions Taken
◆ Yes	<ul style="list-style-type: none">◆ Delete all selected user objects:<ol style="list-style-type: none">1. Deletes the User Objects Cannot be restored. However, if the user is an LDAP user, a synchronization will create a new user account.2. Deletes the User Workspaces (Personal Storage). Personal Storage cannot be restored.

Users Have Home Directories	Options Available and Actions Taken
-----------------------------	-------------------------------------

◆ No

◆ **Move User Workspaces to Trash:**

1. Moves User Workspaces (Personal Storage) to the trash.
Personal Storage can be restored.
2. Does not delete the User Objects.
3. You can restore the user workspaces from the trash, as described in ["Recovering User Workspaces from the Trash" on page 149.](#)

◆ **Delete User Workspaces:**

1. Deletes User Workspaces (Personal Storage).
Personal Storage cannot be restored.
2. Does not delete the User objects.
3. If the user logs back in, a New User Workspace is created as if the user is new to the Filr system.

◆ **Delete User Objects:**

1. Also deletes the User Objects.

Users no longer exist on the system.

◆ Mixed (some yes, some no)

◆ **Move local user workspaces with only Personal Storage to the trash and delete others:**

1. Moves User Workspaces that do not reference Home folders to the trash.
You can restore user workspaces that were moved to the trash, as described in ["Recovering User Workspaces from the Trash" on page 149.](#)
2. Deletes user workspaces that reference Home folders.
3. Does not delete the user objects unless sub-option is selected.

◆ **Delete user objects whose workspaces are deleted:**

1. Also deletes the user objects that are associated with the user workspaces that are being deleted.
2. The users no longer exist in the Filr system and cannot log in.
3. Neither the user objects nor the user workspaces can be restored.

◆ **Delete all user workspaces:**

1. Deletes all user workspaces, regardless of whether user workspaces contain a Home folder.
2. Does not delete the user objects.
3. The user workspaces cannot be restored.
4. If the user logs back in, a new workspace is created as if the user is new to the Filr system.

◆ **Delete user objects:**

1. Deletes the user objects and the user workspaces from the Filr system.
 2. The users no longer exist in the Filr system and cannot log in.
 3. Neither the user objects nor the user workspaces can be restored.
-

Deleting an LDAP User

If you delete user accounts that were created by the LDAP synchronization process without following the instructions in this section, new users with the same name are created the next time the users log in or the next time the LDAP synchronization occurs.

User accounts can be synchronized to the Filr site with an LDAP directory. Although you can delete Filr user accounts, Micro Focus recommends that you disable them, as described in [“User and Group Maintenance” on page 145](#).

If you decide to delete Filr user accounts, it is safer to manually delete than to delete them through the LDAP synchronization process. Because user accounts that are deleted cannot be recovered, ensure that you know exactly which users you are deleting; the only way to be sure is to manually delete them.

Manually Deleting User Accounts That Are Being Synchronized through LDAP

The following method is preferred for deleting user accounts from the Filr site if the accounts are being synchronized from an LDAP directory:

- 1 In your LDAP directory, modify the User objects that you want to delete from the Filr site so that the User objects no longer match the LDAP synchronization criteria that you previously set.

For information about setting LDAP synchronization criteria, see [“LDAP Servers and Synchronization”](#) in the *Filr 3.4.1: Administrative UI Reference*.

- 2 In Filr, manually delete the user accounts, as described in [“Deleting User Objects and Workspaces” on page 147](#).

Having LDAP Automatically Delete User Accounts Is Not Recommended

CAUTION: Micro Focus recommends against having the LDAP synchronization process automatically delete Filr users and workspaces because it might result in unwanted deletion of users!

For example, if the LDAP context is entered incorrectly and none of the users match the incorrect LDAP context, all of the users are permanently deleted.

For more information about configuring LDAP synchronization to automatically delete Filr users and workspaces, see [“For user accounts provisioned from LDAP that are no longer in LDAP sub-section”](#) in the *Filr 3.4.1: Administrative UI Reference*.

Recovering User Workspaces from the Trash

Path: [Port 8443 Filr Administration Console](#)Management > Users > Trash Can icon (upper right) > *select a workspace to restore* > select Restore

If you have deleted user workspaces, you can restore the workspaces from the trash.

NOTE: It is not possible to restore user objects that have been deleted.

Disabling Filr User Accounts

Path: [Port 8443 Filr Administration Console](#)

Micro Focus recommends that you disable user accounts instead of deleting them. When you delete a user account, the account can never be re-activated. If there is the slightest possibility that the user might return to your Filr site, disable the user account rather than delete it. Also, all files and folders that the user shared with other users are no longer accessible.

Disabled accounts do not count as licensed users. When you disable a user account, all the active shares from that user are still accessible. Also, the Filr administrator can use the Admin Console to edit the Filr share rights set on these shares. For more information about editing the shared settings, see [Managing Shared Items](#) in the *Filr 3.4.1: Administrative UI Reference*.

The way to disable a user account differs depending on whether the user was created in Filr or in an LDAP directory and then synchronized to Filr.

Disabling or Re-enabling a Local User Account

Path: [Port 8443 Filr Administration Console](#)Management > Users > *select user accounts* > More > Disable or Enable

Disabling an LDAP User Account

If users are being synchronized from an LDAP directory, you must disable the accounts directly from the LDAP directory. User accounts that are disabled in the LDAP directory are disabled in Filr at the next LDAP synchronization.

For more information about LDAP synchronization in Filr, see “[LDAP Servers and Synchronization](#)” in the *Filr 3.4.1: Administrative UI Reference*.

Renaming a Filr User

Micro Focus Filr users are identified by

- ◆ **User Names:** Identify personal profiles—can be changed.
- ◆ **User IDs:** Used for logging in—cannot be changed.

The way you change a user’s name depends on how the user was created.

Renaming a Filr User from LDAP

1. In the LDAP directory, change the user’s first, middle, and/or last name.

The name changes with the next LDAP synchronization.

Renaming a Local Filr User

Path: [Port 8443 Filr Administration Console](#) > Management > Users > *select a user name* > Profile > *Change the First Name and/or Last Name*

User Maintenance Task Links

Path: [Port 8443 Filr Administration Console](#) > Management > Users

The following are links to specific UI fields or dialogs where the tasks indicated are performed. All links point to rows within UI help tables in the *Filr 3.4.1: Administrative UI Reference*. See the Path statements before each table for UI navigation help.

With Multiple Users Selected

- ◆ [Desktop Application Settings...](#)—Set
- ◆ [Direct Admin Rights](#)—Add/Remove
- ◆ [Direct Admin Status](#)—View
- ◆ [Email Addresses](#)—View
- ◆ [File Downloading](#)—Enable/Disable/Use Default Settings
- ◆ [Mobile Application Settings...](#)—Set
- ◆ [Personal Storage](#)—Restore from Trash
- ◆ [Personal Storage Settings](#)—Enable/Disable/Use Default Settings
- ◆ [Personal Storage Sharing Rights](#)—Set
- ◆ [Registered Devices](#)—View
- ◆ [User Accounts](#)—Enable/Disable
- ◆ [User IDs](#)—View
- ◆ [User List](#)—Filter with a text string
- ◆ [User List](#)—Filter by a user type
- ◆ [User Type](#)—View
- ◆ [Web Access](#)—Enable/Disable/Use Default Settings

With a Single User Selected

- ◆ [Home Folder Settings \(Search Indexing, Sync/JITS, Name\)](#)—Set
- ◆ [Personal Storage](#)—Enable/Disable
- ◆ [Net Folders Sharing Settings](#)—Set
- ◆ [Personal Storage Sharing Settings](#)—Set
- ◆ [Profile](#)—View
- ◆ [Quota](#)—Set

Group Maintenance Task Links

Path: [Port 8443 Filr Administration Console](#) > [Management](#) > [Groups](#)

The following are links to specific UI fields or dialogs where the tasks indicated are performed. All links point to rows within UI help tables in the *Filr 3.4.1: Administrative UI Reference*. See the Path statements before each table for UI navigation help.

With Multiple Groups Selected

- ◆ [Desktop Application Settings...](#)—Set
- ◆ [Direct Admin Rights](#)—Add/Remove

- ◆ Direct Admin Status—View
- ◆ File Downloading—Enable/Disable/Use Default Settings
- ◆ Group List—Filter with a text string
- ◆ Group Type—View
- ◆ Mobile Application Settings...—Set
- ◆ Personal Storage Settings—Enable/Disable/Use Default Settings
- ◆ Web Access—Enable/Disable/Use Default Settings

With a Single Group Selected

- ◆ Delete the group
- ◆ File Downloading—Enable/Disable/Use Default Settings
- ◆ Personal Storage—Enable/Disable
- ◆ Web Access—Enable/Disable/Use Default Settings

A A Simulation and Some Best Practice Sizing Recommendations

Based on support experiences with large customers, Micro Focus testers created a Filr deployment in a lab environment as outlined in [“Sample Filr Deployment Description” on page 153](#):

After running simulations and monitoring performance, the test team made some best practice recommendations.

- ◆ [“Sample Filr Deployment Description” on page 153](#)
- ◆ [“Filr Appliances” on page 154](#)
- ◆ [“Index Maintenance—Just Let It Run” on page 154](#)
- ◆ [“Synchronization Best Practices” on page 155](#)
- ◆ [“Anticipating Disk-Space Growth” on page 156](#)
- ◆ [“The /var Mount Point” on page 157](#)
- ◆ [“Monitoring Commands and Tips” on page 157](#)
- ◆ [“Ganglia Graphs” on page 159](#)

Sample Filr Deployment Description

Back-end File Server and LDAP Identity Store Statistics:	
◆ Files:	◆ 39,000,000 (assumed to be mostly static)
◆ Folders:	◆ 3,500,000
◆ Users:	◆ 29,000
◆ Groups:	◆ 15,000
Filr Deployment Statistics:	
◆ Four Filr appliances	◆ Three assigned to servicing user requests ◆ One dedicated to Filr administration, Net Folder synchronization, and content indexing.
◆ Net Folder Servers:	◆ 95
◆ Net Folders (including Home Folders):	◆ 200
◆ Two Filrsearch appliances	◆ /vastorage = 144 GB (size of index after deployment and tests)
◆ One MySQL appliance	◆ /vastorage = 155 GB (size of database after deployment and tests)

Filr Appliances

Number of Filr Appliances

- ◆ Deploy 4 Filr appliances (minimum) in a Filr cluster (farm).
- ◆ Locate 3 behind a load-balancing / round-robin switch.
- ◆ Dedicate 1 to Filr administration and to Net Folder synchronization and indexing.

Configuring the Dedicated Filr Appliance

- ◆ Include the dedicated appliance in the farm, but do not include it in the load balancing/round robin configuration.
- ◆ Disable Net Folder synchronization on the 3 load-balanced Filr appliances so that any scheduled synchronizations are forced to occur on the dedicated appliance.
- ◆ For instructions, see [“Dedicating a Filr Appliance to Indexing and Net Folder Synchronization”](#) in the [Filr 3.4: Installation, Deployment, and Upgrade Guide](#).

Use the Dedicated Filr Appliance for Upgrade Testing

When upgrading, use the dedicated appliance as the “test” appliance as follows:

1. Shut down all other appliances
2. Upgrade the dedicated appliance.
3. Make sure the appliance is performing as expected before upgrading the other three Filr appliances and bringing the Filr system back online.

Separate Filr REST and Web Requests at L4 Switch

- ◆ To help balance the load between REST requests (from the Filr desktop and mobile applications), and web browser requests, configure the L4 switch to direct REST requests to one of the three load-balanced Filr appliances and web requests to another Filr appliance. (The third load-balanced Filr appliance can continue to service both request types.)

Filr CPUs

- ◆ As a best practice, you should always leave the CPU setting on Filr Appliances at 4 CPUs.
- ◆ Do not set the CPUs on the dedicated Filr appliance at less than 4 CPU's.

Index Maintenance—Just Let It Run

- ◆ Do not re-index after Filr is up and running.
- ◆ Net Folder synchronizations will index the file and folder meta-data.

-
- ♦ **IMPORTANT:** Re-Indexing is not necessary to maintain and optimize a Filr environment, only to restore search functionality if issues arise.

If a future upgrade requires re-indexing because of database version or schema changes, this will be clearly called out in the documentation.

Synchronization Best Practices

- ♦ [“Synchronization Priorities” on page 155](#)
- ♦ [“Never Overlap Synchronizations” on page 155](#)
- ♦ [“Limit Synchronization Size” on page 155](#)
- ♦ [“Utilize Just-in-Time Synchronization Rather than Scheduled Synchronizations” on page 155](#)
- ♦ [“JITS Settings” on page 155](#)
- ♦ [“If a Manual Net Folder Synchronization Is Required” on page 156](#)

Synchronization Priorities

- ♦ Synchronize the most frequently accessed files and folders first so that they are accessible and searchable in Filr.

Never Overlap Synchronizations

- ♦ Make sure that Net Folder synchronizations never overlap.

Each synchronization must have time to complete before another starts. Of course, completion time depends on the size and number of Net Folders being synced.

Limit Synchronization Size

- ♦ Do not synchronize more than 10 Million files at a time.

Utilize Just-in-Time Synchronization Rather than Scheduled Synchronizations

- ♦ After the initial synchronization completes, disable scheduled synchronization at the [Filr system level](#), on [Net Folder Servers](#), or on [Net Folders](#).
- ♦ Enable Just-in-Time Synchronization (JITS) for your Net Folders. See [“Just-in-Time Synchronization”](#) in the [Filr 3.4.1: Administrative UI Reference](#).

JITS Settings

In general, JITS settings should be based on the environment.

They can be set in the [Synchronization Options tab](#) for a Net Folder Server or in the [Configuration tab](#) for a Net Folder.

- ♦ **Maximum Age for Just-inTime Results:** This is set to 60 seconds by default.

This means that Filr will not check with the back-end file server for changes to the requested folder if the previous JITS request was less than 1 minute ago.

Considering that the files on back-end file servers are mostly static, set this value to 300 seconds (5 minutes).

- ♦ **Maximum Age for ACL Just-in-Time Results:** This is set for 3600 Seconds by default.

This means that JITS will retrieve ACL changes on your back-end file server when the last JITS request was more than one hour ago (3600 seconds).

Keep this setting at the default.

If a Manual Net Folder Synchronization Is Required

- ♦ If a manual Net Folder synchronization is required for some reason, synchronize only a limited number of Net Folders and never more than 10 million files at a time.

For help, see [“Manually Synchronizing a Net Folder” on page 89](#).

Anticipating Disk-Space Growth

Anticipating Filr Disk Space Growth

- ♦ The `/vashare` disk can grow quickly if Personal Storage is enabled.

To constrain growth, set disk space quotas. See [“Managing and Restricting Filr-Based Storage”](#) in the *Filr 3.4.1: Administrative UI Reference*.

Filrsearch Disk Space Growth

- ♦ The `/vastorage` disk will see the most growth because this is where the indexes reside.

SQL Disk Space Growth

- ♦ SQL disk space growth is confined to the database (`/vastorage` on the MySQL appliance).
- ♦ Depending on the current size of `/vastorage`, you should expand `/vastorage` to allow for growth as follows:

1. After synchronizing the first 20 million files, run the following query on the database.

```
SELECT sum(round(((data_length + index_length) / 1024 / 1024 / 1024), 2))
as "Size in GB" FROM information_schema.TABLES WHERE table_schema =
"<database name>"
```

2. Based on the results, calculate the disk space required for 100 Million files.
3. Include anticipated growth that in the total.

innodb_buffer_pool_size

- ♦ Set the DB `innodb_buffer_pool_size` to 66-75% of the total memory available to the appliance.
- ♦ This parameter is set on initial configuration with new installs, but if the HyperVisor guest OS's memory increases, this parameter needs to be manually set in the `/etc/my.cnf` file.

In `/etc/my.cnf`, the exact setting is

```
innodb_buffer_pool_size = 2048M
```

- ♦ The byte specifier is mandatory.
Setting this to more than the available memory on the system prevents the database from starting.

The /var Mount Point

- ♦ For all appliances, /var must be large enough to host logs files and at least one core, one javacore, and one heapdump file at a minimum.
- ♦ For Filrsearch, /var should be 3 times total RAM.

Monitoring Commands and Tips

- ♦ [“SQL Database Monitoring Commands” on page 157](#)
- ♦ [“Monitoring Net Folder Synchronization” on page 157](#)
- ♦ [“Monitoring the Impact of Your Tuning Changes to the Overall System” on page 158](#)

SQL Database Monitoring Commands

Table A-1 SQL Monitoring Commands

To Find	Use This
MySQL DB size = IMPORTANT: This is an important query for tuning the MySQL appliance. 1. First, make sure that the total RAM is set to about 8% of the database size. 2. Then set the <code>innodb_buffer_pool_size</code> to between 60 and 75% of the total RAM.	<pre>SELECT sum(round(((data_length + index_length) / 1024 / 1024 / 1024), 2)) as "Size in GB" FROM information_schema.TABLES WHERE table_schema = "filr";</pre>
Number of Files =	<pre>select count(*) from SS_Attachments;</pre> <p>NOTE: This query will take some time. Divide the output number by 2.</p>
Number of Folders =	<pre>select count(*) from SS_Forums;</pre>
Number of Net Folders (including Home Folders) =	<pre>select count(*) from SS_NetFolderConfig;</pre>
Number of Net Folder Servers =	<pre>Select count(*) from SS_ResourceDriver;</pre>
Number of users =	<pre>select count(*) from SS_Principals where type='user';</pre>
Number of Groups =	<pre>select count(*) from SS_Principals where type='group';</pre>

Monitoring Net Folder Synchronization

- ♦ If you are running a re-index you can compare the numbers churning in the Administration Console > Search Index > Re-Index UI with the following DB query:

```
select count(*) from SS_Forums;
```

- ♦ During Net Folder synchronization, keep watch on the Search appliance's Ganglia graphs and keep an eye on /vastorage and /var during the sync.
- ♦ If you are running a Net Folder sync you can compare the numbers in the [Port 8443: Administration Console > Net Folders > Sync Status icon](#) (click the churning wheel) with the following DB query:

```
select count(*) from SS_FolderEntries;
```

Monitoring the Impact of Your Tuning Changes to the Overall System

- ♦ Monitor all Filrsearch, MySQL and Filr appliances using `top`, `df -h`, `du -h` (on specific directories), through Ganglia and using the DB queries listed above.
- ♦ There are 3rd party tools that can be used to specifically monitor the JVM, such as `jvmtop`.
- ♦ Watch the `top` and Ganglia metrics.

As you study the Ganglia graphs, consider the sequence of events that have occurred on the system, such as synchronization and indexing processes.

When you read a Ganglia chart, make sure you understand the units represented. For example, look at the memory graphs in [Figure A-1 on page 159](#) that were retrieved from the example system.

The maximum that the chart is showing is not 15 MB but rather 15 M x KIB. In other words, 15,000,000 KB or 15 GB. The units are shown to the left of the Y-axis. The minimum is about 200 MB (not 6 MB).

Ganglia Graphs

Figure A-1 Memory Monitoring



Figure A-2 Disk Metrics Monitoring

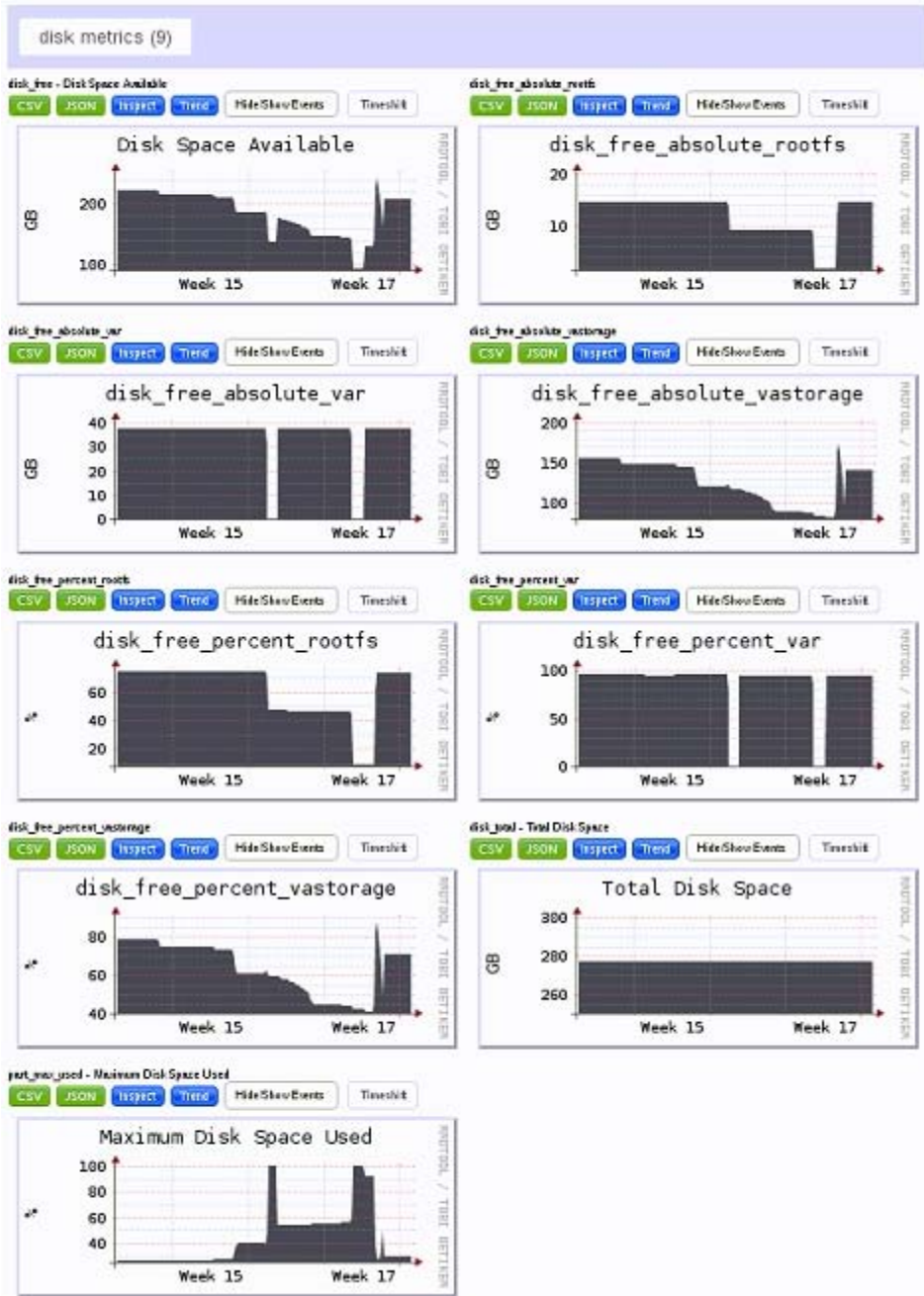


Figure A-3 CPU Metrics Monitoring



Figure A-4 Search Metric Monitoring



Figure A-5 Host Memory History

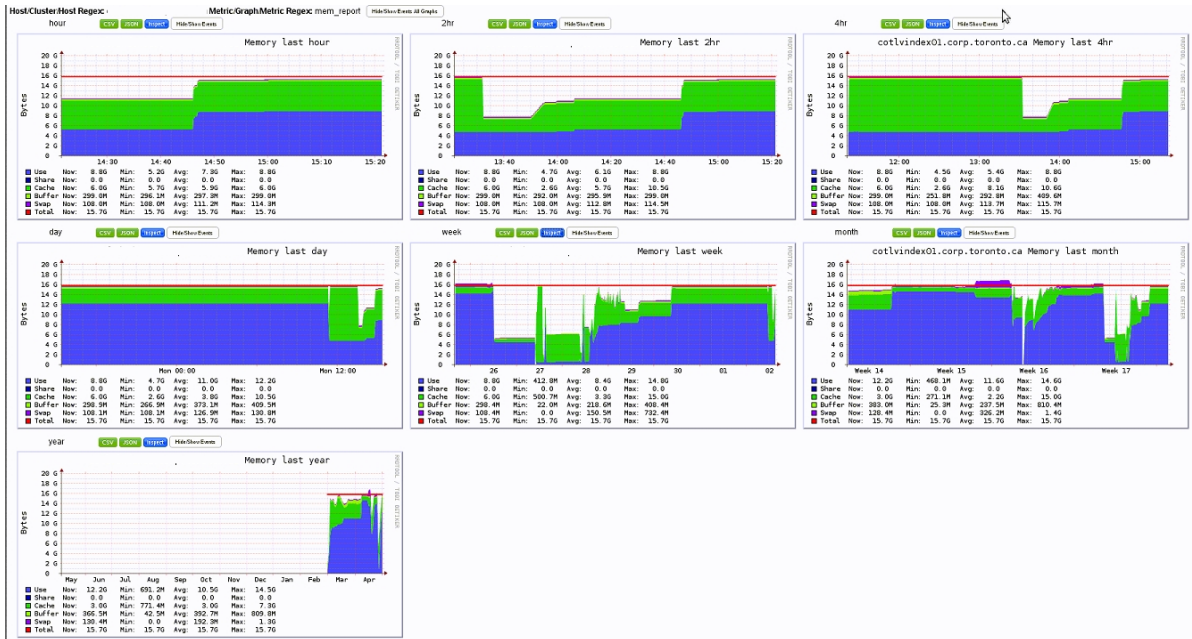


Figure A-6 Host CPU History

