

Filr 4.2

Administrative User Interface Reference

July 2020

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 © 2020 Micro Focus. All Rights Reserved.

Contents

About This Guide	7
1 Administrative Consoles	9
2 Administrative Access	11
Assigning and Managing Port 8443 Direct Administrators	11
Changing Passwords and SSH Access for vaadmin and root	12
Logging In as an Administrator	12
Administration Console	12
Port 9443 Console	13
3 Access to Filr and Its Services	15
Desktop Access—Default Settings	15
Desktop Access—Individual Users and Groups	18
Mobile Device Access—Default Settings	18
Mobile Device Access—Individual Users and Groups	21
Web Browser Access—Default Settings	24
Web Browser Access—Individual Users and Groups	25
KeyShield Configuration Settings	26
NetIQ Advanced Authentication Configuration	27
Reverse Proxy Configuration Settings	28
Single Sign-On Access	30
4 Filr Clustering Configuration	31
5 LDAP Servers and Synchronization	33
6 Content Editor	45
7 Licensing	47
Installing/Updating the Filr License	47
Viewing Filr License Details	47
8 Logging and Monitoring	49
Accessing Filr System Log Files	49
Automatically Applying Deferred Search Logs	49
Changing the Ganglia Monitoring Configuration	50
Generating Filr-Monitoring Reports	51
Credits Report	52
Data Quota Exceeded Report	52

Data Quota Highwater Exceeded Report	52
Disk Usage Report	53
Email Report.	53
External User Report	54
File Block Report	54
Filr Outlook Report	55
License Report	55
Login Report.	56
Orphaned User Share Report	56
System Error Logs Report	57
User Access Report	57
User Activity Report.	57
XSS (Cross-Site Scripting) Report	58
Logging All HTTPS Traffic	58
Managing Audit Trail Logs of Database Activity	59

9 Management Zones 61

Managing Zones	61
Adding and Modifying Zones	61
Adding a Zone	61
Modifying a Zone.	62
Deleting Zones	63
Viewing Zones Information	63

10 Net Folder Servers 65

Creating and Managing Net Folder Servers	65
Manage Net Folder Servers Dialog.	65
Creating a Net Folder Server.	65
Editing an Existing Net Folder Server	70
Deleting a Net Folder Server.	70
Enabling Just-in-Time-Synchronization for Filr and eDirectory Rights Usage for OES and NetWare	70
Proxy User Identities.	71
Managing Proxy Identities	72
Creating Proxy Identities.	72
Modifying Proxy Identities	72

11 Net Folders 75

Managing Net Folders.	75
Creating and Modifying Net Folders	76
Creating a Net Folder.	76
Modifying a Net Folder	80
Deleting a Net Folder.	80

12 Net Folder System-Level Synchronization 81

Enabling and Tuning Net Folder Synchronization.	81
Just-in-Time Synchronization	82

13 Network Infrastructure	83
Changing Network Settings	83
Network Configuration	84
Port Numbers	86
14 Notifications (Email)	89
Configuring an Email Service for Filr to Use	89
Enabling Notifications	91
15 Performance Tuning	93
Changing Configuration Settings for Requests and Connections	93
Changing JVM Configuration Settings	94
16 Personal Storage and Home Folders	95
Enabling Personal Storage for Users and Groups	95
Managing and Restricting Filr-Based Storage	95
17 Product Improvement	99
18 Managing Uploading of Files	101
19 Search and Lucene Indexing	105
Managing Filrsearch Configuration Settings	105
Managing the Lucene Index	107
Managing Search Nodes	108
Memcached (Search Index Appliance Only)	109
Advantages for Using Memcached	109
Managing Memcached	109
20 Security	111
Certificates	111
Firewall Configuration	112
Password Security (Local and External Users)	112
Securing Memcached	113
User Visibility	113
Viewing, Wiping, and Disconnecting Registered Clients	114
WebDAV Authentication Configuration Settings	114
21 Sharing	117
Managing Shared Items	117
Managing Sharing, License Terms, and Comments	118
The Rights Tab Controls All Filr Sharing	121

22 SQL Database Connection	123
23 Storage Management	125
Expanding Storage	125
24 Support Files and Online Updates	127
Managing Field Test Patches	127
Managing Online Updates	127
Submitting Configuration Files to Micro Focus Support	129
25 Changing System Services Configurations	131
Managing System Services	131
Shutting Down and Restarting the Micro Focus Appliance	132
26 Time and Locale	133
Changing the Appliance's NTP Configuration	133
Setting a Default Time and Locale for Non-LDAP and External Users	133
27 UI Controls and Customizations	135
Email Notification Template Customization	135
Branding the Web Client	135
Branding the Desktop Apps (Advanced-Edition License Only)	137
Branding the Mobile Apps (Advanced-Edition License Only)	138
UI Language	140
Name Completion Settings—Managing How Group Names Display in Drop-Down Lists	141
28 Users and Groups	143
Managing Users	143
Viewing and Managing User Properties	146
Managing Groups	147
29 Integrating Microsoft Office and Outlook with Filr	153
Managing Office Settings	153
Managing Outlook Settings	153

About This Guide

This guide is for Filr administrators and covers the administrative dialogs and screens for the following services and features:

- ♦ [Chapter 1, “Administrative Consoles,” on page 9](#)
- ♦ [Chapter 2, “Administrative Access,” on page 11](#)
- ♦ [Chapter 3, “Access to Filr and Its Services,” on page 15](#)
- ♦ [Chapter 4, “Filr Clustering Configuration,” on page 31](#)
- ♦ [Chapter 5, “LDAP Servers and Synchronization,” on page 33](#)
- ♦ [Chapter 6, “Content Editor,” on page 45](#)
- ♦ [Chapter 7, “Licensing,” on page 47](#)
- ♦ [Chapter 8, “Logging and Monitoring,” on page 49](#)
- ♦ [Chapter 9, “Management Zones,” on page 61](#)
- ♦ [Chapter 10, “Net Folder Servers,” on page 65](#)
- ♦ [Chapter 11, “Net Folders,” on page 75](#)
- ♦ [Chapter 12, “Net Folder System-Level Synchronization,” on page 81](#)
- ♦ [Chapter 13, “Network Infrastructure,” on page 83](#)
- ♦ [Chapter 14, “Notifications \(Email\),” on page 89](#)
- ♦ [Chapter 15, “Performance Tuning,” on page 93](#)
- ♦ [Chapter 16, “Personal Storage and Home Folders,” on page 95](#)
- ♦ [Chapter 17, “Product Improvement,” on page 99](#)
- ♦ [Chapter 18, “Managing Uploading of Files,” on page 101](#)
- ♦ [Chapter 19, “Search and Lucene Indexing,” on page 105](#)
- ♦ [Chapter 20, “Security,” on page 111](#)
- ♦ [Chapter 21, “Sharing,” on page 117](#)
- ♦ [Chapter 22, “SQL Database Connection,” on page 123](#)
- ♦ [Chapter 23, “Storage Management,” on page 125](#)
- ♦ [Chapter 24, “Support Files and Online Updates,” on page 127](#)
- ♦ [Chapter 25, “Changing System Services Configurations,” on page 131](#)
- ♦ [Chapter 26, “Time and Locale,” on page 133](#)
- ♦ [Chapter 27, “UI Controls and Customizations,” on page 135](#)
- ♦ [Chapter 28, “Users and Groups,” on page 143](#)
- ♦ [Chapter 29, “Integrating Microsoft Office and Outlook with Filr,” on page 153](#)

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 the *Micro Focus Filr Administration Guide* and other documentation, visit the [Micro Focus Filr Documentation website \(http://www.microfocus.com/documentation/filr/filr-4\)](http://www.microfocus.com/documentation/filr/filr-4).

Additional Documentation

You can find more information in the Micro Focus Filr documentation, which is accessible from the [Micro Focus Filr Documentation website \(http://www.microfocus.com/documentation/filr/filr-4\)](http://www.microfocus.com/documentation/filr/filr-4).

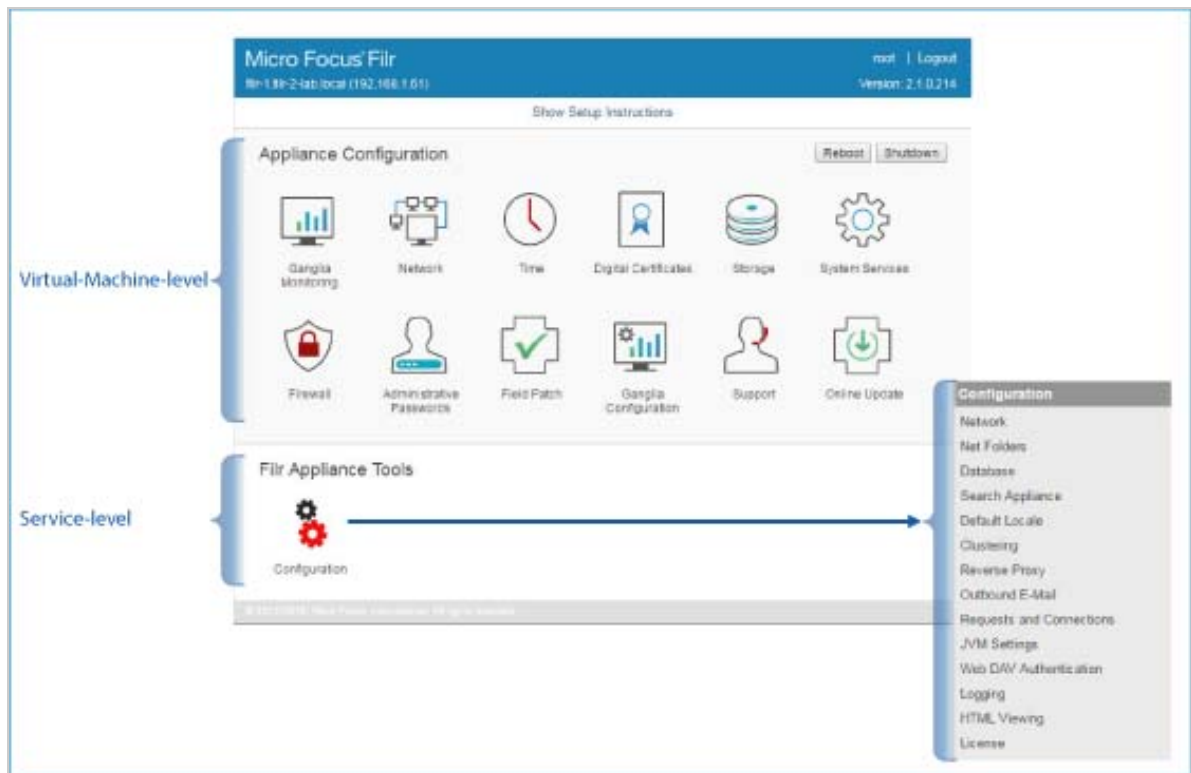
1 Administrative Consoles

Port 9443 Appliance Console

Path: https://appliance_ip_or_dns:9443

- ♦ You and those with the `vaadmin` or `root` user password use this to manage virtual-machine-level settings and Filr service configurations that affect an entire service and its interactions with other services.

Figure 1-1 The Port 9443 Filr Console



Port 8443 Filr Administration Console

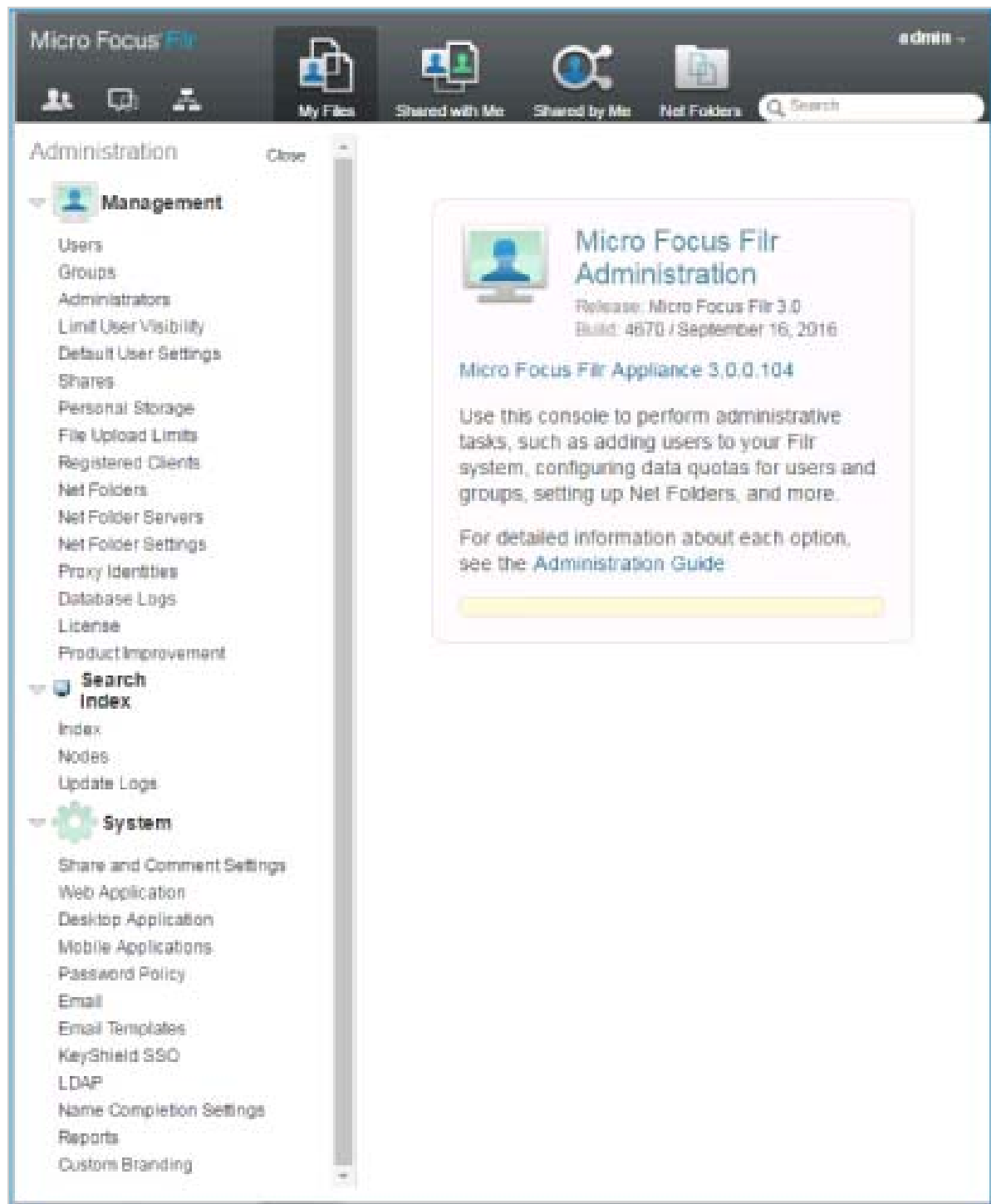
Path: To access the Administration Console, login to the new Filr Web client [<https://appliance_ip_or_dns:8443>](https://appliance_ip_or_dns:8443), then click on **Username** > **Administration Console**.

NOTE: The Administration Console can only be accessed through the New Filr Web client by the Administrators and admin equivalent users.

- ♦ You and other designated Filr administrators use this console to manage all aspects of Filr services.
- ♦ If the Filr appliance is configured for port redirection, Filr users, including administrators, might not need to include the port number.

- ♦ If Filr is configured to use NetIQ Access Manager, the Filr login screen is not used. For more information about Filr configurations that affect login, see [“Changing Network Settings” on page 83](#).
- ♦ Ensure that the hostname does not include the special character “_”. This fails to launch the console and results in “Error 400”.

Figure 1-2 The Port 8443 Filr Console



2 Administrative Access

This section covers the following Filr administrator-related tasks:

- ♦ [“Assigning and Managing Port 8443 Direct Administrators” on page 11](#)
- ♦ [“Changing Passwords and SSH Access for vaadmin and root” on page 12](#)
- ♦ [“Logging In as an Administrator” on page 12](#)


For more information about Filr administrators, see [“Filr Administrative Users”](#) in the [Filr: Understanding How Filr Works](#) guide.

Assigning and Managing Port 8443 Direct Administrators

Path: [“Port 8443 Filr Administration Console” on page 9](#) > Management > Administrators

Best Practice: You can plan your Direct administrators in advance or create them as needs develop. In either case, you should keep a record of those with administrative access.

Table 2-1 Using the Manage Administrators dialog

Field, Option, or Button	Information and/or Action
About Port 8443 Direct Administrators	Port 8443 Direct Administrators can only administer the following: <ul style="list-style-type: none">♦ Users♦ Groups♦ Mobile Devices♦ Net Folders♦ Net Folder Servers
 Administrators	
♦ Add	<ol style="list-style-type: none">1. Click Add to add a new Direct administrator.2. Begin typing the user or group name you want to assign.3. Click a user or group to add it to the list.
♦ Remove	<ol style="list-style-type: none">1. Select one or more users or groups in the Administrators list.2. Click Remove. <p>The selected items are removed.</p>
♦ Filter list	<ol style="list-style-type: none">1. Type an alphanumeric string contained in the user or group names you want to display.2. Press Enter. <p>The list displays only the names that contain the string you entered.</p>

Field, Option, or Button	Information and/or Action
♦ Gear icon	<ol style="list-style-type: none"> 1. Click the icon 2. Select Edit Column Sizes. 3. Follow the instructions in the Edit Column Sizes dialog to adjust column widths. <p>Changes persist from session to session.</p>

Changing Passwords and SSH Access for vaadmin and root

NOTE: Changing both passwords requires logging in as `root`. If you log in as `vaadmin`, you can only change the `vaadmin` password.

Path: [Port 9443 Appliance Console](#) > **Administrative Passwords**

Table 2-2 *The Administrative Passwords dialog*

Field, Option, or Button	Information and/or Action
vaadmin	♦ Acting as either <code>vaadmin</code> or <code>root</code> , type the current password, type and confirm the new password, and click OK .
root	♦ Acting as <code>root</code> , type the current password, type and confirm the new password, and click OK .
root SSH Access	♦ Acting as <code>root</code> , select or deselect Allow root access to SSH and click OK . SSH is disabled by default. For information about how to start SSH on the appliance, see Chapter , “Managing System Services,” on page 131 .

Logging In as an Administrator

Administration Console

Path: [“Port 8443 Filr Administration Console” on page 9](#)

Table 2-3 Using the Sign In dialog

Field, Option, or Button	Information and/or Action
♦ User ID:	<ul style="list-style-type: none"> ♦ First-time login: The username you specified in “Specify the First Search Appliance, Locale, and Admin user” in the <i>Filr: Installation, Deployment, and Upgrade Guide</i>. The default is admin. ♦ Subsequent login: The name of the built-in Filr administrator (default is admin), or a directly assigned administrator.
♦ Password:	<ul style="list-style-type: none"> ♦ First-time login: Enter the username. You are then prompted to change the password. ♦ Subsequent login: Administrative user password set above or changed in the Profile.
♦ Change Password	<ul style="list-style-type: none"> ♦ First-time login only <ol style="list-style-type: none"> 1. Type the current password, which is the username. 2. Type and confirm a new, more secure password.

Port 9443 Console

Path: [Port 9443 Appliance Console](#)

Table 2-4 Port 9443 Sign In dialog

Field, Option, or Button	Information and/or Action
♦ Username	♦ Enter either vaadmin or root.
♦ Password	♦ Type the password for vaadmin or root

3 Access to Filr and Its Services

Users can access Filr through web browsers, desktops, and mobile devices.

- ♦ “Desktop Access—Default Settings” on page 15
- ♦ “Desktop Access—Individual Users and Groups” on page 18
- ♦ “Mobile Device Access—Default Settings” on page 18
- ♦ “Mobile Device Access—Individual Users and Groups” on page 21
- ♦ “Web Browser Access—Default Settings” on page 24
- ♦ “Web Browser Access—Individual Users and Groups” on page 25
- ♦ “KeyShield Configuration Settings” on page 26
- ♦ “NetIQ Advanced Authentication Configuration” on page 27
- ♦ “Reverse Proxy Configuration Settings” on page 28
- ♦ “Single Sign-On Access” on page 30

Desktop Access—Default Settings

Settings made here apply to all Filr users unless Filr access and password caching are overridden by settings made through the [Users](#) or the [Groups](#) management dialogs.

Path: [Port 8443 Appliance Console](#) > **System** > **Desktop Application**

Table 3-1 Using the Configure Desktop Application dialog

Field, Option, or Button	Information and/or Action
Allow Desktop Applications to:	
♦ Access Filr	<ul style="list-style-type: none">♦ Select this to allow all users to access Filr through the Filr desktop application.♦ Deselect this if you want only designated users and groups to have desktop access as controlled through user and group settings
♦ Cache the user’s password	<ul style="list-style-type: none">♦ Select this to allow users to enable the Remember password option on the Account Information page in the Micro Focus Filr Console. <p>Remember password option availability is also configurable for individual users and groups through the Users and the Groups management dialogs (More > Desktop Application Settings).</p>

Field, Option, or Button	Information and/or Action
<ul style="list-style-type: none"> ♦ Be deployed 	<ul style="list-style-type: none"> ♦ Select this to expose the Download Filr Desktop App option in the web client > user drop-down menu. <p>Alternatively, you can download the desktop apps from download.novell.com and distribute them using client management software such as Micro Focus ZENworks.</p> <p>For more information, see “Client Management Software and the Filr Desktop Applications” in the <i>Filr 4.2: Maintenance Best Practices Guide</i>.</p>
<ul style="list-style-type: none"> ♦ Deploy files contained locally 	<ul style="list-style-type: none"> ♦ Select this to allow users to download the Desktop App contained in Filr.
<ul style="list-style-type: none"> ♦ Deploy files accessed via URL to another location 	<ul style="list-style-type: none"> ♦ Select this and specify the URL of the server that is hosting the Desktop App downloads. <p>To set up web server distribution of the desktop app, see “Hosting Desktop Application Installation Files on a Separate Server” in the <i>Filr 4.2: Maintenance Best Practices Guide</i>.</p> <ul style="list-style-type: none"> ♦ This is required if your Filr system is fronted by an L4 or L10 switch. ♦ This is a best practice because it minimizes the load on Filr.
Desktop Synchronization	
<ul style="list-style-type: none"> ♦ Synchronize every ___ Minutes 	<ul style="list-style-type: none"> ♦ Specify how many minutes you want the desktop app to wait after a desktop synchronization ends before it checks again for changes to Available Offline files. <p>Default=15 minutes.</p> <ul style="list-style-type: none"> ♦ You can use this to control the synchronization load that the Filr desktop application puts on Filr. ♦ Changes on the desktop are automatically synchronized to Filr regardless of this setting.
<ul style="list-style-type: none"> ♦ Maximum file size that can be synchronized: 	<ul style="list-style-type: none"> ♦ Specify the maximum file size (in MB) that can be synchronized between the Filr desktop application and Filr.
<ul style="list-style-type: none"> ♦ Remove cached files after X days 	<ul style="list-style-type: none"> ♦ Specify the number of days that locally cached files remain on users’ desktops after they are no longer being accessed or modified.
<ul style="list-style-type: none"> ♦ Allow user to modify cached files lifetime 	<ul style="list-style-type: none"> ♦ Select this to allow users to specify how long they want locally cached files remain on their desktops after the files are no longer being accessed or modified.
Desktop Notifications	
<ul style="list-style-type: none"> ♦ Allow balloon notifications for desktop client users 	<ul style="list-style-type: none"> ♦ Deselect this to disallow balloon notifications from being displayed on the users’ desktops. This option is selected by default.
Application Whitelist/Blacklist	For more information, see “ Controlling File Downloads by the Filr Desktop Applications ” in the <i>Filr 4.2: Maintenance Best Practices Guide</i> .
<ul style="list-style-type: none"> ♦ Restore Defaults... 	<ul style="list-style-type: none"> ♦ Click this to restore the defaults for all settings in the Application Whitelist/Blacklist section below.

Field, Option, or Button	Information and/or Action
Mode	<ul style="list-style-type: none"> ♦ Lets you control how antivirus, backup, and other applications download files that are accessible through Filr.
♦ No restrictions - Ignore the lists.	<ul style="list-style-type: none"> ♦ Select this if you want all applications, including antivirus scanners and backup software, to download files to the workstation's local disk.
♦ Whitelist - Allow only the listed applications to download files.	<ul style="list-style-type: none"> ♦ If you select this, then download attempts by unlisted applications trigger system alerts to users that a download has been "blocked by an administrative setting." This option doesn't provide for user control of application-driven downloads. ♦ Whitelists are empty by default. ♦ You can add and remove applications for your organization as needed.
♦ Blacklist - Block the listed applications from downloading files.	<ul style="list-style-type: none"> ♦ If you select this, then download attempts by blacklisted applications trigger system alerts to users that a download has been "blocked by an administrative setting." This option doesn't provide for user control of application-driven downloads. ♦ Filr includes two default blacklists (Windows and Mac) that you can modify as needed. ♦ Blacklisted applications are blocked from downloading files through Filr. ♦ Unlisted applications are allowed to download files.
♦ Whitelist and Blacklist - Allow and block the listed applications. Prompt users to allow or block unlisted applications.	<ul style="list-style-type: none"> ♦ If you select this option, then <ul style="list-style-type: none"> ♦ Blacklisted applications are always blocked. ♦ Whitelisted applications are always allowed. ♦ A download attempt by an unidentified application causes the application to be added to a list of blocked applications. ♦ Users can allow downloading by any blocked applications through their desktop Filr console.
Whitelist	<ul style="list-style-type: none"> ♦ This is empty by default. ♦ Only the built-in administrator can create a customized list. ♦ Applications listed here and in the Blacklist are blocked. In other words, the Blacklist trumps the Whitelist.
Blacklist	<ul style="list-style-type: none"> ♦ Filr includes a fairly extensive list of common antivirus and backup applications to offer a level of protection against unwanted file downloading. ♦ Only the built-in administrator can customize this list.

Field, Option, or Button	Information and/or Action
OK button	<ul style="list-style-type: none"> Click this to save your changes. <p>Current user sessions are not affected. To see changes, users must log in to a new session.</p>
Cancel button	<ul style="list-style-type: none"> Click this to cancel the changes you have made.

Desktop Access—Individual Users and Groups

Path: [Port 8443 Appliance Console](#) > **Management** > **Users/Groups** > *select one or more users or groups* > **More** > **Desktop Application Settings...**

Table 3-2 Using the Configure Desktop Application dialog (applies in both user and group contexts)

Field, Option, or Button	Information and/or Action
Configure Desktop Application (X users)	
Use default settings option	<ul style="list-style-type: none"> Select this to apply all of the settings in the Configure Desktop Application dialog to the selected users or groups.
Use user settings to allow the desktop application to: option	<ul style="list-style-type: none"> Select this to apply the access and password caching settings below to the selected users or groups. <p>The following two settings override their counterparts in the Configure Desktop Application dialog and all other settings there apply here.</p>
<ul style="list-style-type: none"> Access Filr 	<ul style="list-style-type: none"> Selecting this allows the previously selected users or groups to access Filr through the Filr desktop application. Deselecting this option blocks the previously selected users or groups from accessing Filr through the Filr desktop application.
<ul style="list-style-type: none"> Cache the user's password 	<ul style="list-style-type: none"> Selecting this allows the previously selected users or groups to enable the Remember password option on the Account Information page in the Micro Focus Filr Desktop Console. Deselecting this blocks the previously selected users or groups from enabling the Remember password option on the Account Information page in the Micro Focus Filr Desktop Console.
OK button	<ul style="list-style-type: none"> Click this to save your changes. <p>Current user sessions are not affected. To see changes, users must log in to a new session.</p>
Cancel button	<ul style="list-style-type: none"> Click this to cancel the changes you have made.

Mobile Device Access—Default Settings

Path: [Port 8443 Filr Admin Console](#) > **System** > **Mobile Applications**

Table 3-3 Using the Configure Mobile Applications dialog

Field, Option, or Button	Information and/or Action
Allow mobile applications to:	
♦ Access Filr	♦ Select this to allow access to Filr through Filr mobile apps.
♦ Cache the user's password	♦ Select this to let users enable the Save Password option when logging in to the Filr site through a Filr mobile app.
♦ Allow files to be added to the Downloads area for offline access	<p>♦ Select this to let users download files from Filr to mobile devices.</p> <p>IMPORTANT: If you don't want users downloading files, make sure that you also disable downloading through web browsers.</p> <p>♦ Downloaded files can be viewed in offline mode by accessing the Downloads section in the app.</p> <p>♦ Users are responsible for the security of downloaded files. See "Encrypting Downloaded Files" in the "Micro Focus Filr Mobile App Quick Start Help".</p>
♦ Force PIN Code	<p>♦ Select this to force users running Filr mobile app to have a 4-digit access code set on their devices for accessing Filr</p> <p>See "Configuring a 4-Digit Passcode" in the "Micro Focus Filr Mobile App Quick Start Help".</p>
♦ Cut/Copy	♦ Select this to let users cut or copy data from the Filr mobile app so that the data can be pasted into third-party applications.
♦ Screen capture (affects Android only)	<p>♦ Select this to let users take a screen capture while inside the Filr application.</p> <p>IMPORTANT: As noted in the option name, this only applies to Android devices. iOS users can always take screen captures.</p>
♦ Disable applications on rooted or jail-broken devices	♦ Select this to prevent users from running the Filr mobile app on devices that have been rooted or jail-broken.

Field, Option, or Button	Information and/or Action
Open in: drop-down list	<ul style="list-style-type: none"> Click the drop-down list and select the option that is best for your organization as described in the rows below. This controls whether users can open files in third-party apps through Filr. For example, a user views a file in Filr, opens and modifies the file in a document editing app, then saves the file back to the Filr app. iOS calls this “Open In” functionality; Android devices refer to it as “Share” or “Send To.” <p>IMPORTANT: For MobileIron device management, the following points apply:</p> <ul style="list-style-type: none"> In almost all cases the Filr and MobileIron settings must be consistent with each other. The exception is if you want only the MobileIron-managed devices to have Open In capabilities. To cause this behavior, <ol style="list-style-type: none"> Enable Open In in MobileIron. Disable Open In in Filr.
♦ Disabled option	♦ This prevents users from opening files in Filr using third-party applications.
♦ All applications option	♦ This lets users open files in Filr using any third-party application.

Field, Option, or Button	Information and/or Action
♦ Whitelist option	<p>♦ This opens two Whitelists (Android and iOS) of third-party apps that users are allowed to open files into.</p> <p>IMPORTANT</p> <ul style="list-style-type: none"> ♦ Only Android package names and iOS bundle IDs are valid list entries. ♦ To get an Android app package name: <ol style="list-style-type: none"> 1. Install the Package Name Viewer app from the Google Play store. <p>This app displays the package name for each app that is currently installed on the device.</p> ♦ To find the bundle ID for an iOS app: <ol style="list-style-type: none"> 1. Synchronize the app to iTunes from your device. 2. In the iTunes library, open the Mobile Applications folder. <p>For iTunes on Mac, the default location is your Home directory at: ~ / Music / iTunes / Mobile Applications /</p> <p>For iTunes On Windows, the default location is C : \ Users \ username \ My Music \ iTunes \ Mobile Applications /</p> <ol style="list-style-type: none"> 3. Create a copy of the app's file, and re-save the copy as a .zip file. 4. Unzip the newly created .zip file. <p>You now see a folder by the name of the application name.</p> <ol style="list-style-type: none"> 5. Locate the <code>iTunesMetadata.plist</code> file within the folder and open it in a text editor. 6. The bundle ID is the string displayed below the <code>softwareVersionBundleid</code> key within the file.
Mobile synchronization	
♦ Synchronize every X Minutes	<p>♦ Specify how many minutes the mobile apps wait after a desktop synchronization ends before they start another synchronization with Filr.</p> <p>Default=15 minutes.</p> <p>♦ You can use this to control the synchronization load that the Filr mobile app puts on Filr.</p>
OK button	<p>♦ Click this to save your changes.</p> <p>Current user sessions are not affected. To see changes, users must log in to a new session.</p>
Cancel button	♦ Click this to cancel the changes you have made.

Mobile Device Access—Individual Users and Groups

Path: [Port 8443 Filr Admin Console](#) > [Management](#) > [Users/Groups](#) > *select one or more users or groups* > [More](#) > [Mobile Application Settings...](#)

Table 3-4 Using the Configure User Mobile Application Settings dialog

Field, Option, or Button	Information and/or Action
Configure User Mobile Application Settings (X users)	
Use default settings	<ul style="list-style-type: none"> Select this to apply all of the settings in the Configure Mobile Applications dialog to the selected users or groups.
Use user settings to allow mobile applications to:	<ul style="list-style-type: none"> Select this to apply the settings below to the selected users or groups.
<ul style="list-style-type: none"> Access Filr 	<ul style="list-style-type: none"> Lets selected users/groups access Filr through a Filr mobile app.
<ul style="list-style-type: none"> Cache the user's password 	<ul style="list-style-type: none"> Lets selected user/goups enable the Save Password option when logging in to the Filr site through a Filr mobile app.
<ul style="list-style-type: none"> Allow files to be added to the Downloads area for offline access 	<ul style="list-style-type: none"> Lets selected user/groups download files from Filr to mobile devices. Downloaded files can be viewed in offline mode by accessing the Downloads section in the app. If you don't want users downloading files, make sure that you also disable downloading through web browsers. Users are responsible for the security of downloaded files. See "Encrypting Downloaded Files" in the "Micro Focus Filr Mobile App Quick Start Help".
<ul style="list-style-type: none"> Force PIN Code 	<ul style="list-style-type: none"> Forces selected user/groups running version 2.0 and later apps to have a 4-digit access code set on their devices for accessing Filr, as described in "Configuring a 4-Digit Passcode" in the "Micro Focus Filr Mobile App Quick Start Help."
<ul style="list-style-type: none"> Cut/Copy 	<ul style="list-style-type: none"> Lets selected user/groups cut or copy data from the Filr mobile app so that the data can be pasted into third-party applications.
<ul style="list-style-type: none"> Screen capture (affects Android only) 	<ul style="list-style-type: none"> Lets selected users/groups take a screen capture while inside the Filr application. <p>IMPORTANT: As noted in the option name, this only applies to Android devices. iOS users can always take screen captures.</p>
<ul style="list-style-type: none"> Disable applications on rooted or jail-broken devices 	<ul style="list-style-type: none"> Prevents selected users/groups from running the Filr mobile app on devices that have been rooted or jail-broken.

Field, Option, or Button	Information and/or Action
Open in:	<ul style="list-style-type: none"> Click the drop-down list and select the option that is best for the selected users or groups as described in the rows below. Controls whether selected user/groups can open files in third-party apps through Filr. <p>For example, a user views a file in Filr, opens and modifies the file in a document editing app, then saves the file back to the Filr app.</p> iOS calls this “Open In” functionality; Android devices refer to it as “Share” or “Send To.” <p>IMPORTANT: For MobileIron device management, the following points apply:</p> <ul style="list-style-type: none"> In almost all cases the Filr and MobileIron settings must be consistent with each other. The exception is if you want only the MobileIron-managed devices to have Open In capabilities. <p>To cause this behavior,</p> <ol style="list-style-type: none"> Enable Open In in MobileIron. Disable Open In in Filr.
♦ Disabled	<ul style="list-style-type: none"> Prevents selected users/groups from opening files in Filr using third-party applications.
♦ All applications	<ul style="list-style-type: none"> Lets selected users/groups open files in Filr using any third-party application.

Field, Option, or Button	Information and/or Action
♦ Whitelist	<p>♦ This opens two Whitelists (Android and iOS) of third-party apps that selected users or groups are allowed to open files into.</p> <p>IMPORTANT</p> <ul style="list-style-type: none"> ♦ Only Android package names and iOS bundle IDs are valid list entries. ♦ To get an Android app package name: <ol style="list-style-type: none"> 1. Install the <code>Package Name Viewer</code> app from the Google Play store. <p>This app displays the package name for each app that is currently installed on the device.</p> ♦ To find the bundle ID for an iOS app: <ol style="list-style-type: none"> 1. Synchronize the app to iTunes from your device. 2. In the iTunes library, open the <code>Mobile Applications</code> folder. <p>For iTunes on Mac, the default location is your Home directory at: <code>~/Music/iTunes/Mobile Applications/</code></p> <p>For iTunes On Windows, the default location is <code>C:\Users\username\My Music\iTunes\Mobile Applications/</code></p> <ol style="list-style-type: none"> 3. Create a copy of the app's file, and re-save the copy as a <code>.zip</code> file. 4. Unzip the newly created <code>.zip</code> file. <p>You now see a folder by the name of the application name.</p> <ol style="list-style-type: none"> 5. Locate the <code>iTunesMetadata.plist</code> file within the folder and open it in a text editor. 6. The bundle ID is the string displayed below the <code>softwareVersionBundleid</code> key within the file.
OK button	<p>♦ Click this to save your changes.</p> <p>Current user sessions are not affected. To see changes, users must log in to a new session.</p>
Cancel button	♦ Click this to cancel the changes you have made.

Web Browser Access—Default Settings

Path: [Port 8443 Filr Admin Console](#) > [System](#) > [Web Application](#)

Table 3-5 Using the Configure Web Application dialog

Field, Option, or Button	Information and/or Action
<ul style="list-style-type: none"> ♦ Allow Guest access 	<ul style="list-style-type: none"> ♦ By default, Guest (anonymous) access to Filr is not enabled. ♦ Selecting this enables anonymous access to Filr through the built-in Guest user account. <p>For more information about the Guest and other users, see “Types of Filr Users” in <i>Filr: Understanding How Filr Works</i>.</p> <p>IMPORTANT</p> <ul style="list-style-type: none"> ♦ Guest access is for web users only. <p>Mobile app and desktop users cannot log in as Guest.</p> <ul style="list-style-type: none"> ♦ Using NetIQ Access Manager to provide single sign-on access as described in the installation guide, prevents Guest user access.
<ul style="list-style-type: none"> ♦ Guest access is read only 	<ul style="list-style-type: none"> ♦ By default, this option is not enabled. ♦ Enabling this option prevents Guests from commenting on files or adding files to publicly available folders.
<ul style="list-style-type: none"> ♦ Disable file downloads 	<ul style="list-style-type: none"> ♦ By default, this option is not enabled. ♦ Enabling this option prevents all file downloads through web browsers. <p>Individual user or group settings to allow downloads have no effect unless this is deselected.</p>
<ul style="list-style-type: none"> ♦ Disable web access 	<ul style="list-style-type: none"> ♦ By default, this option is not enabled. ♦ Enabling this option prevents all users from accessing Filr through a Web browser, unless access is allowed on an individual user or group basis.
OK button	<ul style="list-style-type: none"> ♦ Click this to save your changes. <p>Current user sessions are not affected. To see changes, users must log in to a new session.</p>
Cancel button	<ul style="list-style-type: none"> ♦ Click this to cancel the changes you have made.

Web Browser Access—Individual Users and Groups

Path: [Port 8443 Filr Admin Console](#) > **Management** > **Users/Groups** > *select one or more users or groups* > **More** > > *select a file download or web access option from the list below*

Table 3-6 Using the More Options to Control Web Access for Individual Users and Groups

Field, Option, or Button	Information and/or Action
<ul style="list-style-type: none">◆ Disable File Downloads◆ Enable File Downloads◆ Use Default File Download Setting◆ Disable Web Access◆ Enable Web Access◆ Use Default Web Access Setting	<ul style="list-style-type: none">◆ These options do not all appear at the same time. <p>They change, dynamically, to reflect alternate choices to the options configured in “Web Browser Access—Default Settings” on page 24.</p> <ul style="list-style-type: none">◆ Select an available option in the More drop-down list for the selected users or groups. <p>The action is immediately applied to the selected user or group accounts and the drop-down list changes dynamically to reflect the new settings.</p>

KeyShield Configuration Settings

Path: [Port 8443 Filr Admin Console](#) > **System** > **KeyShield SSO**

For dialog usage instructions and other KeyShield integration information, see “[KeyShield Integration with Filr](#)” in the *Filr 4.2: Maintenance Best Practices Guide*.

Table 3-7 Using the KeyShield SSO Configuration dialog

Field, Option, or Button	Information and/or Action
Enable KeyShield SSO	<ol style="list-style-type: none">1. Select this to enable KeyShield SSO and Filr integration.2. Specify the configuration information for the following fields.
<ul style="list-style-type: none">◆ KeyShield Server URL (use http or https):	<ul style="list-style-type: none">◆ The access URL of the KeyShield server
<ul style="list-style-type: none">◆ API authorization key:	<ul style="list-style-type: none">◆ The API Key copied from the KeyShield console.
<ul style="list-style-type: none">◆ HTTP connection timeout:	<ul style="list-style-type: none">◆ How long the Filr appliance will wait for a response from KeyShield before prompting users for their login credentials.◆ Micro Focus doesn’t recommend changing this value unless the network connection might not allow a quick response. For example, when Filr and KeyShield connect over a WAN.
<ul style="list-style-type: none">◆ Connector names:	<ul style="list-style-type: none">◆ The names of every KeyShield SSO connector that Filr users will connect through.
<ul style="list-style-type: none">◆ Username attribute alias:	<ul style="list-style-type: none">◆ These let KeyShield match username validation requests with the LDAP attribute that requesting applications use for usernames. For more detail and a Filr example, see “KeyShield Attribute Alias Support” in the <i>Filr 4.2: Maintenance Best Practices Guide</i>.
Two Factor Authentication	

Field, Option, or Button	Information and/or Action
Require hardware token	<ol style="list-style-type: none"> 1. Select this to require a physical token, such as an access card, for access to Filr through KeyShield. 2. Specify the options for missing tokens below.
♦ Missing token error message for Web interface:	♦ The error message to display when web access is requested and the token is not presented or not recognized.
♦ Missing token error message for WebDAV interface:	♦ The error message to display when WebDAV access is requested and the token is not presented or not recognized.
Allow username/password-based fallback authentication (non-SSO) for LDAP users	♦ Select this to let users enter a username and password as an alternative to the hardware token.
♦ Test connection button	♦ Click this to test the connection between Filr and the KeyShield server.
OK button	♦ Click this to save your changes. Current user sessions are not affected. To see changes, users must log in to a new session.
Cancel button	♦ Click this to cancel the changes you have made.

NetIQ Advanced Authentication Configuration

Path: [Port 8443 Filr Admin Console](#) > **System** > **NetIQ Advanced Authentication**

This functionality is only available on Filr Advanced Edition. Before you configure the advanced authentication options, you must do the following:

- ♦ Ensure that all the Filr clients are updated with the latest patch installed.
- ♦ Configure an OAuth2 Event in the Advanced Authentication server using the Advanced Authentication Administrative Portal to automatically generate the client ID and the client secret. See “[Using Multi-Factor Advanced Authentication with Filr](#)” in the *Filr 4.2: Maintenance Best Practices Guide*.

You must specify these client ID and client secret values in the NetIQ Advanced Authentication Configuration dialog. See [Table 3-8](#).

Table 3-8 *Using the NetIQ Advanced Authentication Configuration dialog*

Field, Option, or Button	Information and/or Action
Enable Multi-factor Authentication	<ol style="list-style-type: none"> 1. Select this to enable multi-factor authentication for Filr. 2. Specify the configuration information for the following fields.

Field, Option, or Button	Information and/or Action
♦ Server URL:	♦ The access URL of the Advanced Authentication server that you want to use for multi-factor authentication.
♦ Client ID:	♦ The client ID that is automatically generated when you use the Advanced Authentication Administrative Portal to create an OAuth2 event. You can copy the ID from the portal and paste it here.
♦ Client Secret:	♦ The client secret key that is automatically generated when you use the Advanced Authentication Administrative Portal to create an OAuth2 event. You can copy the secret key from the portal and paste it here.
♦ Tenant Name:	♦ Specify the tenant name. The default value is TOP and supports single tenancy.
♦ Test connection button	♦ Click this to test the connection between Filr and the Advanced Authentication server.
♦ Redirect URIs	♦ Copy the Filr URIs, that are displayed in this field. This is appended with an additional URI for AAF to work with the New Filr Web Client. When you create an OAuth2 event in the Advanced Authentication Administration Portal, you must paste the copied URIs in the Redirect URIs option to enable users to be redirected to the Filr URI after successful authentication. NOTE: On upgrading to Filr 4.2, ensure to copy the updated URI to the AAF server.
OK button	♦ Click this to save your changes.
Cancel button	♦ Click this to cancel the changes you have made.

Reverse Proxy Configuration Settings

Use this when Filr is fronted by a reverse proxy server or L4 switch that provides a single access point for Filr users.

IMPORTANT: Do not configure Filr appliances that are [dedicated to Net Folder Synchronization and indexing](#).

Path: [Port 9443 Appliance Console](#) > [Configuration icon](#) > [Reverse Proxy](#)

Table 3-9 Using the Reverse Proxy dialog

Field, Option, or Button	Information and/or Action
Host Information	<ul style="list-style-type: none"> Specify the information for the server or switch through which internal and external users access Filr. <p>IMPORTANT: Configure each Filr appliance that is servicing user requests in a Filr-based cluster with the same information.</p> <p>However, do not configure synchronization- and indexing-dedicated Filr appliances with Reverse Proxy Configuration Settings.</p>
<ul style="list-style-type: none"> Host: 	<ul style="list-style-type: none"> For a reverse proxy server or a load balancer/L4 switch, specify the DNS hostname. For NetIQ Access Manager, enter the published DNS name.
<ul style="list-style-type: none"> Reverse Proxy HTTP Port: 	<ul style="list-style-type: none"> If you have enabled Port Redirection and HTTP Port access in the Network dialog, specify port 80.
<ul style="list-style-type: none"> Reverse Proxy Secure HTTP Port: 	<ul style="list-style-type: none"> If you have enabled Port Redirection and HTTP Port access in the Network dialog, specify port 443.
NetIQ Access Manager Integration	
<ul style="list-style-type: none"> Logout URL: 	<ul style="list-style-type: none"> The URL of the published DNS name of the reverse proxy that you have specified for the ESP, plus /AGLogout . <p>You can find the domain used for the ESP by editing the LAG/MAG cluster configuration and then clicking Reverse Proxy / Authentication.</p> <p>For example, if the published DNS name of the proxy service that you have specified for the ESP is <code>esp.yoursite.com</code>, specify the following URL:</p> <pre>https://esp.yoursite.com/AGLogout</pre> <ul style="list-style-type: none"> After clicking OK, you must click Reconfigure Filr Server for your changes to take effect. <p>This stops and restarts your Filr server. Because this results in server downtime, you should restart the server during off-peak hours.</p>
<ul style="list-style-type: none"> Filr plugin for NAM: 	<p>Click Filr Plugin for NAM to download the <code>FilrAuthClass.jar</code> file. This jar file is required to enable Filr users to access the Filr services through NetIQ Access Manager (NAM). For more information about configuring NAM to act as Proxy service for a Filr site, see “Integrating Filr and NetIQ Access Manager” in the Access Manager (NAM) and Filr Integration.</p>
OK button	<ul style="list-style-type: none"> Click this to save your changes, then click Reconfigure Filr Server. <p>This stops and restarts your Filr server. Because this results in server downtime, you should restart the server during off-peak hours.</p> <p>Current user sessions are not affected. To see changes, users must log in to a new session.</p>
Cancel button	<ul style="list-style-type: none"> Click this to cancel the changes you have made.

Single Sign-On Access

NetIQ Access Manager: For information about how to configure NetIQ Access Manager to provide single sign-on functionality in Filr, see [“Reverse Proxy Configuration Settings” on page 28](#) and [Access Manager \(NAM\) and Filr Integration](#) in the *Filr: Installation, Deployment, and Upgrade Guide*.

4 Filr Clustering Configuration

Path: [Port 9443 Appliance Console](#) > [Configuration icon](#) > [Clustering](#)

Table 4-1 *Using the Clustering dialog*

Field, Option, or Button	Information and/or Action
Enable Clustered Environment	<ul style="list-style-type: none">Click this to enable Filr clustering on this appliance and on all appliances using the same /vashare NFS or CIFS mount point.
<ul style="list-style-type: none">JVM Route	<ul style="list-style-type: none">You can leave this field blank unless you plan to use Apache as the reverse proxy.If you plan to use Apache as the reverse proxy, add a JVM route for each Filr Appliance in the Cluster. The purpose of this field is to uniquely identify each Filr Appliance to Apache. In the JVM Route field, specify <code>worker1</code>. On the second Filr node, in the JVM Route field, specify <code>worker2</code>, and so forth for each Filr node, incrementing the JVM Route setting. Each Tomcat instance should have a unique JVM Route setting. <code>worker1</code>, <code>worker2</code>, and so forth are the default names for the matching values used for the reverse proxy configuration. For example, if you have set up Apache or IIS as a reverse proxy, these are the default values. The JVM Route setting in the Filr installer must match these values.
<ul style="list-style-type: none">Hibernate Caching Provider:	<ul style="list-style-type: none">memcached is the only option available when configuring Filr in a clustered environment. The Search appliance runs the Memcached service to enable clustering. Port 11211 is used by the Memcached service. IMPORTANT: To secure Memcached, it is strongly recommended to deploy the Search appliance behind the firewall. For more information on securing Memcached, see “Securing Memcached” on page 113.
<ul style="list-style-type: none">Server Address:	<ul style="list-style-type: none">The hostnames or IP addresses of both Filrsearch servers, separated by a space.After clicking OK, you must 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 during off-peak hours.

5 LDAP Servers and Synchronization

- ♦ “LDAP Configuration Dialog” on page 33
- ♦ “LDAP Server Configuration Dialog” on page 36
- ♦ “LDAP Search Dialog (User Version)” on page 39
- ♦ “LDAP Search Dialog (Group Version)” on page 42
- ♦ “Conceal LDAP ID” on page 43

LDAP Configuration Dialog


Path: [Port 8443 Filr Admin Console](#) > **System** > **LDAP**

Best Practice: Plan your LDAP Servers and use the following table when working in this dialog:

Table 5-1 Using the LDAP Configuration dialog

Field, Option, or Button	Information and/or Action
LDAP Configuration dialog	
LDAP Servers tab	
♦ Add button	<ul style="list-style-type: none">♦ Click this to begin the process of adding an LDAP server. The LDAP Server Configuration dialog opens.
♦ Delete button	<ul style="list-style-type: none">♦ Click this to remove the selected LDAP server from the list. IMPORTANT: Before you remove an LDAP server, make sure you consider the options you have set for users and groups that are no longer in LDAP in the User Settings tab and the Group Settings tab.
♦ Sync All button	<p>TIP: If you have just added or modified the LDAP Servers configuration, you must save it by clicking OK before running an LDAP synchronization.</p> <ul style="list-style-type: none">♦ After your users and groups are synchronized, you can click this to refresh the LDAP information in Filr.♦ To synchronize only certain users or groups, filter the list by entering a string in the Filter List. Or♦ Click the drop-down arrow next to the Filter List and select the type of users or groups to synchronize. For example, Added users, Modified users, Modified groups, and so forth.♦ Users and groups that have been modified by running the LDAP sync are reported, along with information about how they have been modified.

Field, Option, or Button	Information and/or Action
<ul style="list-style-type: none"> ◆ Preview Sync button 	<p>TIP: If you have just added or modified the LDAP Servers configuration, you must save it by clicking OK before previewing an LDAP synchronization.</p> <ul style="list-style-type: none"> ◆ Use this to preview the synchronization results—users and groups that will be added or deleted, users that will be disabled, and so on—before you run the actual synchronization. <ul style="list-style-type: none"> ◆ To preview only certain users or groups, filter the list by entering a string in the Filter List. Or ◆ Click the drop-down arrow next to the Filter List and select the type of users or groups to synchronize. <p>For example, Added users, Modified users, Modified groups, and so forth.</p> ◆ After you are satisfied with the results, use the Sync All option with the same filters to perform the actual synchronization.
<ul style="list-style-type: none"> ◆ Show Sync Results button 	<ul style="list-style-type: none"> ◆ Use this to display the most recent synchronization results <i>for the current browser session</i>. ◆ If you run a synchronization, log out of Filr, and then log in again, no results are available to view.
LDAP servers list	
<ul style="list-style-type: none"> ◆ Server URL 	<ul style="list-style-type: none"> ◆ The URL you specified when creating the LDAP server. ◆ You can click this to access the LDAP Server Configuration dialog.
<ul style="list-style-type: none"> ◆ User DN 	<ul style="list-style-type: none"> ◆ This is the LDAP proxy user information for the LDAP server
User Settings tab	
<ul style="list-style-type: none"> ◆ Register User Profiles Automatically 	<ul style="list-style-type: none"> ◆ Select this option to automatically add LDAP users to the Filr site. ◆ Workspaces are not created until users log in for the first time.
<ul style="list-style-type: none"> ◆ Synchronize User Profiles 	<ul style="list-style-type: none"> ◆ Select this option to automatically update Filr with user information changes following the initial LDAP synchronization. ◆ The attributes that are synchronized are the attributes listed in the “mappings” box in the Server Information tab.
For user accounts provisioned from LDAP that are no longer in LDAP sub-section	
<ul style="list-style-type: none"> ◆ Disable Account 	<ul style="list-style-type: none"> ◆ This is the default because deleting user accounts cannot be undone. <p>For more information about disabled users in Filr, see Disabling Filr User Accounts in the Filr 4.2: Maintenance Best Practices Guide.</p>
<ul style="list-style-type: none"> ◆ Delete Account 	<p>IMPORTANT: A deleted user cannot be undeleted; this action is not reversible.</p> <ul style="list-style-type: none"> ◆ Select this only if you have deleted users from your LDAP directory and you want the LDAP synchronization process to also remove them from Filr. ◆ Also delete associated user workspaces and content: This option removes all information, Personal Storage, etc. associated with the user accounts.

Field, Option, or Button Information and/or Action	
<i>Use the following when creating new users sub-section</i>	
♦ Time zone:	<ul style="list-style-type: none"> ♦ Use this drop-down list to set the time zone for user accounts that are synchronized from the LDAP directory into your Filr site. ♦ The time zone list is grouped first by continent or region, optionally by country or state, and lastly by city.
♦ Locale:	<ul style="list-style-type: none"> ♦ Use this drop-down list to set the locale for user accounts that are synchronized from the LDAP directory into your Filr site. ♦ The locale list is sorted alphabetically by language.
Group Settings tab	
♦ Register LDAP group profiles automatically	<ul style="list-style-type: none"> ♦ Select this to automatically add new LDAP groups to the Filr site.
♦ Synchronize group profiles	<ul style="list-style-type: none"> ♦ Select this to synchronize group information, such as the group description, to the Filr site whenever this information changes in LDAP.
♦ Synchronize group membership	<ul style="list-style-type: none"> ♦ This option ensures that the Filr group includes the same users (and possibly groups) as the corresponding LDAP group. If this is not selected, then LDAP group changes are not reflected in Filr. ♦ This option also ensures that Filr recognizes group-based file system rights assignment updates. If this is not selected, users with group-based access rights might not qualify for the roles they need to use Filr.
♦ Delete groups that were provisioned from LDAP but are no longer in LDAP	<p>IMPORTANT: A deleted group cannot be undeleted; this action is not reversible.</p> <ul style="list-style-type: none"> ♦ Select this only if you have deleted groups from your LDAP directory and you want the LDAP synchronization process to also remove the groups from Filr.
 Synchronization Schedule tab	
♦ Enable schedule	<ul style="list-style-type: none"> ♦ This is selected by default so that LDAP synchronizations occur at regular intervals. ♦ You should not normally de-select this unless you are troubleshooting a problem or working with Micro Focus support to resolve a service request.
♦ Every day	<ul style="list-style-type: none"> ♦ Select this to run an LDAP synchronization every day at the time or interval specified below.
♦ On selected days	<ul style="list-style-type: none"> ♦ Select this if you want the LDAP synchronization to run only on specific days.
At HH:MM	<ul style="list-style-type: none"> ♦ Using the drop-down lists, you can specify synchronizations to occur at a specific time. ♦ Hours start at midnight (0) and continue through 11 p.m. (23). ♦ Minutes can be specified using 5-minute increments.


Field, Option, or Button	Information and/or Action
Repeat every X hours	<ul style="list-style-type: none"> As an alternative to synchronizing at a specific time, you can set a time interval and synchronize multiple times each day (for example, every four hours). The smallest time interval you can set is .25 hours (every 15 minutes).
Local User Accounts tab	
<ul style="list-style-type: none"> Allow log in for local user accounts (i.e user accounts not in LDAP) 	<ul style="list-style-type: none"> Use this to enable or disable logging in by locally created and self-provisioned user accounts.

LDAP Server Configuration Dialog

Path: [Port 8443 Filr Admin Console](#) > **System** > **LDAP** > **Add button**

Best Practice: Plan your LDAP Servers and use the following table when working in this dialog:

Table 5-2 Using the LDAP Server Configuration dialog

Field, Option, or Button	Information and/or Action
LDAP Server Configuration dialog	
 Server Information tab	
<ul style="list-style-type: none"> LDAP Server URL 	<p>WARNING: If you modify an existing LDAP connection, do not modify this LDAP server URL field. Doing so can cause synchronized users to be disabled or deleted.</p> <ul style="list-style-type: none"> This is the host name of the LDAP server where your directory service is running. <p>Specify a URL with the format your server requires, as follows:</p> <ul style="list-style-type: none"> Non-SSL: <code>ldap://hostname</code> Assumes Port 389 is used SSL: <code>ldaps://hostname</code> Assumes Port 636 is used <p>This requires that you import the LDAP server's root certificate into the Java keystore before attempting an LDAP synchronization. See "LDAP Synchronization Security" in the Filr 4.2: Maintenance Best Practices Guide.</p> <ul style="list-style-type: none"> If the LDAP server uses a different port number from those above, you must include the port as follows: <p><code>ldap://hostname:port_number</code></p> <p><code>ldaps://hostname:port_number</code></p>

Field, Option, or Button	Information and/or Action
<ul style="list-style-type: none"> ♦ User DN: (LDAP proxy user) 	<ul style="list-style-type: none"> ♦ This is the LDAP proxy user and it must have sufficient rights to access the user information stored there. See “LDAP Proxy User Role and Rights” in <i>Filr: Understanding How Filr Works</i>. ♦ You must specify a fully qualified, comma-delimited user name, along with its context in your LDAP directory tree, in the format expected by your directory service. <ul style="list-style-type: none"> ♦ eDirectory: <code>cn=username,ou=organizational_unit,o=organization</code> ♦ Active Directory: <code>cn=username,ou=organizational_unit,dc=domain_component</code>
<ul style="list-style-type: none"> ♦ Password: (LDAP proxy user password) 	<ul style="list-style-type: none"> ♦ You must type the password for the User DN.
<ul style="list-style-type: none"> ♦ Directory Type: 	<ul style="list-style-type: none"> ♦ Select the directory type for the LDAP server that you are configuring (eDirectory or Active Directory)
<ul style="list-style-type: none"> ♦ Guid attribute: 	<ul style="list-style-type: none"> ♦ Based on the directory type you have selected, Filr selects the standard LDAP attribute used to identify a user. ♦ GUID and objectGUID: These are the default, binary attributes for eDirectory and Active Directory, respectively They have unique values that do not change if you rename or move a user in the LDAP directory, thus ensuring that Filr modifies the existing user rather than creating a new one. ♦ Other: Selecting this option in the Guid attribute drop-down prompts you to map users to a different LDAP attribute by specifying the attribute name and then clicking OK. <ul style="list-style-type: none"> ♦ You must ensure that the attribute you specify is a binary attribute. For example, the cn attribute cannot be used because it is not a binary attribute. ♦ If you cancel the prompt to specify an attribute or specify an attribute that is not binary, Filr create new Filr users when names or locations change. For example, if you have a Filr user and LDAP user named William Jones, and if William requests that you change his name to Bill in the LDAP directory, then the next time an LDAP synchronization occurs, Filr creates a new user named Bill Jones.



Field, Option, or Button	Information and/or Action
<ul style="list-style-type: none"> ♦ Filr account name attribute: 	<ul style="list-style-type: none"> ♦ Filr uses this attribute <ul style="list-style-type: none"> ♦ To create Filr account names ♦ To locate users in the LDAP directory. ♦ As the User ID for authentication purposes. ♦ The value of this attribute must be unique in LDAP. ♦ Attribute options depend on the directory type selected in the Directory type drop-down list. <p>Consult with your directory administrator to determine which attribute or attributes are used in your directory service.</p> <ul style="list-style-type: none"> ♦ For eDirectory, the default available options are cn and Other. ♦ For Active Directory, the default available options are sAMAccountName, cn, and Other. ♦ If you select Other as the value for this attribute, you are prompted to enter the name of an LDAP attribute to use instead of the default choices. ♦ Based on your findings, you might need to set up two or more LDAP sources that point to the same LDAP server but use different values for the LDAP Attribute Used for Filr Name. <p>For example, if you use Active Directory, you might need to set up one LDAP source and use cn and another to sAMAccountName as the Filr account name attribute.</p> <ul style="list-style-type: none"> ♦ In addition to the attributes already mentioned in this section, other LDAP attributes can be used for the Filr account name attribute, as long as the attribute is unique for each User object. <p>For example, the mail LDAP attribute could be used so that Filr users can log in by using their email addresses.</p>
<ul style="list-style-type: none"> ♦ LDAP Attribute “Mappings” box 	<ul style="list-style-type: none"> ♦ This lists the mappings between Filr user information and the LDAP attributes that correspond to them. <p>It is populated automatically.</p> <ul style="list-style-type: none"> ♦ If Synchronize User Profiles is enabled in the User Settings tab, the information associated with the mappings that are configured here, is updated each time the user account is synchronized.
OK button	<ul style="list-style-type: none"> ♦ If you are modifying previously configured LDAP server information, you can click OK. Otherwise, you must click the Users tab
Cancel button	<ul style="list-style-type: none"> ♦ Click this to discard the LDAP server configuration changes you have made and exit the tab.
Users tab	
<ul style="list-style-type: none"> ♦ Add button 	<ul style="list-style-type: none"> ♦ Click this to open the “LDAP Search Dialog (User Version)” on page 39 wherein you can specify a context where Filr searches for LDAP users.
<ul style="list-style-type: none"> ♦ Delete button 	<ul style="list-style-type: none"> ♦ Click this after selecting one or more list entries. For example, when the context no longer exists or when it is covered by another entry.

Field, Option, or Button	Information and/or Action
OK button	<ul style="list-style-type: none"> ♦ If you are modifying previously configured User information, you can click OK. ♦ If this is a new configuration, you should click the Groups tab and add an LDAP search context. Otherwise, your Filr users might not be recognized as having the roles needed for Filr access (see the information for the “Synchronize group membership” option).
Cancel button	<ul style="list-style-type: none"> ♦ Click this to discard your changes and exit.
Groups tab	
♦ Add button	<ul style="list-style-type: none"> ♦ Click this to open the LDAP Search Dialog (Group Version) wherein you can specify a context where Filr searches for LDAP groups.
♦ Delete button	<ul style="list-style-type: none"> ♦ Click this after selecting one or more group Base DN entries. For example, when the context no longer exists or when it is covered by another entry.
OK button	<ul style="list-style-type: none"> ♦ Click OK to save the LDAP server configuration.
Cancel button	<ul style="list-style-type: none"> ♦ Click this to discard your changes and exit.

LDAP Search Dialog (User Version)

Path: [Port 8443 Filr Admin Console](#) > [System](#) > [LDAP](#) > [Add button](#) > [Users tab](#) > [Add button](#)

Table 5-3 Using the LDAP Search dialog (User Version)

Field, Option, or Button	Information and/or Action
 LDAP Search dialog (User Version)	
♦ Base DN:	<p>Best Practice: Use the Browse icon  next to the Base DN field to browse the LDAP directory for the base DN that you want to use. This eliminates the risk of typing the context incorrectly. Also, if browsing fails, that means the LDAP server configuration is not correct and must be changed.</p> <ul style="list-style-type: none"> ♦ This is the directory context or container under which LDAP User objects are located. ♦ When specifying this you must use the syntax required by your directory service type. <ul style="list-style-type: none"> ♦ eDirectory: <code>ou=organizational_unit,o=organization</code> ♦ Active Directory: <pre>ou=organizational_unit,dc=domain_component</pre> <p>IMPORTANT: Container names cannot exceed 128 characters. If they do, users are not provisioned.</p>

Field, Option, or Button	Information and/or Action
♦ Filter:	<p>Filr sets up a standard User filter for the LDAP server type.</p> <p>IMPORTANT: In most of the cases, you need to modify this to ensure that only the licensed users are added to the Filr server.</p> <p>Use the User filter to provision only the licensed users to the Filr server.</p> <p>♦ About User Filters:</p> <ul style="list-style-type: none"> ♦ By default, Filr identifies potential users by filtering on the following LDAP directory object attributes: <ul style="list-style-type: none"> ♦ Person ♦ orgPerson ♦ inetOrgPerson <p>If needed, you can modify the filter by inserting the following operators:</p> <ul style="list-style-type: none"> ♦ OR (the default) ♦ & AND ♦ ! NOT <p>♦ A Group for Filr Users:</p> <ul style="list-style-type: none"> ♦ You might want to create a group for only Filr users, regardless of where they are located in your LDAP directory. ♦ After creating the group, use the following filters to search for User objects that have the group membership attribute shown below. <p>Make sure you include the parentheses in your filter.</p> <p>♦ eDirectory:</p> <pre>(groupMembership=cn=group_name,ou=organizational_unit,o=organization)</pre> <p>♦ Active Directory:</p> <pre>(memberOf=cn=group_name,ou=organizational_unit,dc=domain_component)</pre> <p>IMPORTANT: Users in eDirectory sub-groups are not synchronized.</p> <p>However, for Active Directory you can create a filter that synchronizes users in sub-groups by using the following rule object identifier (OID):</p> <pre><attribute name>:<matching rule OID>:=<value></pre>
♦ Search subtree	<ul style="list-style-type: none"> ♦ Select this if you want Filr to search for users in containers underneath the base DN (that is, in subtrees).
<i>Home-Directory Net Folder Configuration</i> sub-section	



Field, Option, or Button	Information and/or Action
<ul style="list-style-type: none"> ♦ Use the following custom criteria 	<ul style="list-style-type: none"> ♦ Select this to specify the Net Folder Server and path where user Home directories are located. ♦ Net Folder Server: Click the drop-down list and select the Net Folder Server where Filr should create home folders when the users in this context (Base DN) log in. If the server isn't created yet, click New Net Folder Server and refer to "Creating a Net Folder Server" on page 65 if you need help. ♦ Relative Path: Using UNC syntax, specify the path to where the corresponding Home directories are located. For example, if user Home directories are included in a directory named <code>Home</code> which is located at the root of the specified Net Folder Server, the path would be <code>Home\</code>. In place of the actual directory names, include a replaceable parameter using the syntax: <code>%LDAPAttributeName%</code>. Continuing the example, if the Home directory is associated with the LDAP attribute <code>cn</code>, the complete path with the replaceable parameter included would be <code>Home\%cn%</code>. Filr evaluates replaceable parameters each time a user logs in and replaces the parameter with the value of the LDAP attribute specified in the path. ♦ After the Home Net Folder Server is created, when you log in to the Port 8443 Administration Console, you are prompted to complete the server's configuration by specifying a Net Folder proxy user. See the information starting with "Specify proxy using a Proxy Identity" on page 67.
<ul style="list-style-type: none"> ♦ Use the LDAP home directory attribute 	<ul style="list-style-type: none"> ♦ Select this option to use the LDAP Home directory attribute. ♦ Filr detects the attribute during the LDAP synchronization process. ♦ If the search context of the LDAP synchronization contains an OES or Windows server that has a Home folder attribute associated with at least one user, Filr creates a Home Net Folder Server immediately after running the LDAP synchronization process. ♦ After the Home Net Folder Server is created, when you log in to the Port 8443 Administration Console, you are prompted to complete the server's configuration by specifying a Net Folder proxy user. See the information starting with "Specify proxy using a Proxy Identity" on page 67.

Field, Option, or Button	Information and/or Action
♦ Use the specified LDAP attribute	<ul style="list-style-type: none"> Select this option to specify the name of the LDAP attribute that contains the required home directory information. <p>Attribute Name: This must be of type String and must contain a UNC path, with one of the following forms:</p> <pre>\\server\volume\path</pre> <pre>\\server\share\path</pre> <pre>\\server\share</pre> <ul style="list-style-type: none"> After the Home Net Folder Server is created, when you log in to the Port 8443 Administration Console, you are prompted to complete the server's configuration by specifying a Net Folder proxy user. See the information starting with “Specify proxy using a Proxy Identity” on page 67.
♦ Don't create a home directory Net Folder	<ul style="list-style-type: none"> Select this option if you do not want user Home directories to be created at the time that users are imported into the Filr system.

LDAP Search Dialog (Group Version)

Path: [Port 8443 Filr Admin Console](#) > [System](#) > [LDAP](#) > [Add button](#) > [Groups](#) > [Add button](#)

Table 5-4 Using the LDAP Search dialog (Group Version)

Field, Option, or Button	Information and/or Action
 LDAP Search dialog (Group Version)	
♦ Base DN:	<p>Best Practice: Use the Browse icon  next to the Base DN field to browse the LDAP directory for the base DN that you want to use. This eliminates the risk of typing the context incorrectly. Also, if browsing fails, that means the LDAP server configuration is not correct and must be changed.</p> <ul style="list-style-type: none"> This is the directory context or container under which LDAP Group objects are located. When specifying this you must use the syntax required by your directory service type. <ul style="list-style-type: none"> eDirectory: <code>ou=organizational_unit,o=organization</code> Active Directory: <pre>ou=organizational_unit,dc=domain_component</pre> <p>IMPORTANT: Container names cannot exceed 128 characters. If they do, groups are not provisioned.</p>
♦ Filter:	<p>Filr sets up a standard Group filter for the LDAP server type.</p> <p>IMPORTANT: In most of the cases, you need to modify this to ensure that only the licensed users are added to the Filr server.</p> <p>Use the Group filter to provision only the licensed users to the Filr server.</p>

Field, Option, or Button	Information and/or Action
♦ Search subtree	♦ Select this if you want Filr to search for groups in containers underneath the base DN (that is, in subtrees).

Conceal LDAP ID

Displaying the LDAP ID can cause security threats to the directory service such as unauthorized access to data and modification of configuration. A configurable option is available in the `ssf-ext.properties` file to hide the LDAP IDs.

- 1 In the `/opt/novell/filr/apache-tomcat/webapps/ssf/WEB-INF/classes/config/ssf-ext.properties` file, set the `hide.LDAPId` parameter to `true`.

```
hide.LDAPId=true
```

User IDs are no longer displayed in the Web Client - Address book search, Show People tabs and so on.

- 2 Restart the Filr service after making modifications to the `ssf-ext.properties` file.

6 Content Editor

The Content Editor (CE) appliance enables collaborative editing feature for Filr users. The functionalities are:

- ♦ Secure edits of the documents
- ♦ Multiple files that can be concurrently edited by multiple users
- ♦ Supports collaborative edits for all major file types like documents, spreadsheet, and so on
- ♦ Edits are done by using the Browser, no Native application is required
- ♦ Policies to block copy, print, and download of the content
- ♦ By default, this functionality is available for all files under My Files, Shared With Me, Shared By Me and Net Folder areas.

A separate appliance is required as the collaborative editing is a resource intensive task. Around 40 files can be concurrently edited by using this functionality.

Content Editor Dialog

Path: [Port 8443 Filr Administration Console](#) > [System](#) > [Content Editor](#)

NOTE: This functionality is only available on Filr Advanced Edition. This feature is available with Filr Web UI, desktop clients and mobile apps.

IMPORTANT: CE ships with a self-signed certificate. Ensure to change the self-signed certificate to a valid trusted certificate, so all the clients can use this functionality.

Table 6-1 Edit Online Feature Availability

Apps / Clients	Edit Online Feature Availability	Require Valid Trusted Certificate
iOS Filr Mobile App	Yes	Yes
Android Filr Mobile App	Yes	No
Windows Filr Mobile App	No	Not Applicable
Mac Desktop Client	Yes	Yes
Windows Desktop Client	Yes	No
Linux Desktop Client	No	Not Applicable

Before you configure the Content Editor options, you must do the following:

- ♦ Deploy a Content Editor appliance.

- ◆ Configure the Content Editor appliance with the DNS hostnames of each Filr appliance that you want to be able to connect to it.
- For more information, see [Content Editor](#) .

Table 6-2 Using the Content Editor Configuration dialog

Field, Option, or Button	Information and/or Action
Enable Content Editor	<ol style="list-style-type: none"> 1. Select this to enable collaborative editing for Filr users. 2. Specify the configuration information for the following fields.
◆ Server URL	◆ The server address (IP address or DNS hostname) of the Content Editor appliance.
◆ Test connection button	◆ Click this to test the connection between Filr and the Content Editor appliance.
Content Editor Policies:	<p>Set the policies that will be applicable to the user when performing collaborative edit.</p> <p>When a user is editing the file and if changes are made to the policy, then the file has to be reloaded for the changes to take effect.</p>
◆ Disable copy	◆ Content from the document cannot be copied to any other document.
◆ Disable print and download	◆ The file you are editing cannot be printed or downloaded to your local workstation.
◆ Disable Watermark	<p>◆ By default, this option is enabled.</p> <p>When this option is enabled, watermark is displayed across the document. Email id or name of the user is displayed as watermark. The watermark is also displayed on printing the document.</p> <p>NOTE: This option is available with CE 1.0.1 version.</p>

7 Licensing

- ♦ “Installing/Updating the Filr License” on page 47
- ♦ “Viewing Filr License Details” on page 47

Installing/Updating the Filr License

IMPORTANT: If you have an expandable deployment, you must update the license on each Filr appliance in the cluster.

PostgreSQL and Filrsearch appliances do not require licenses.

Path: [Port 9443 Appliance Console Configuration icon](#) > [License](#)

Table 7-1 Using the License (port 9443) dialog

Field, Option, or Button	Information and/or Action
♦ Choose File button	<ol style="list-style-type: none">1. Download your <code>license-key.xml</code> file (from the Novell Customer Center (NCC)) to your management workstation. NOTE: If the license is not available, contact Micro Focus Support.2. Click Choose File.3. Browse to and select the downloaded license file.4. Click Open.5. Click Reconfigure Filr Server in the Configuration column.

Viewing Filr License Details

Path: [Port 8443 Filr Admin Console](#) > [Management](#) > [License](#)

Table 7-2 *Using the License (port 8443) dialog*

Field, Option, or Button	Information and/or Action
♦ Current License	<p>This section displays information about the installed license, including:</p> <ul style="list-style-type: none">♦ Information about the license key, when it was issued, and who issued it.♦ Product and version information.♦ The effective date range.♦ Information about user allowances. <p>Your contract contains details. Internal users might or might not be restricted; external (Filtr administrator-created) users are not restricted.</p> <ul style="list-style-type: none">♦ The options or features that the license enables for use.
♦ Reload License File	<ul style="list-style-type: none">♦ If the license information displayed doesn't seem correct, click this to reload the file and refresh the display.♦ If you need to install a new license file, see "Installing/Updating the Filr License" on page 47.

8 Logging and Monitoring

- ♦ “Accessing Filr System Log Files” on page 49
- ♦ “Automatically Applying Deferred Search Logs” on page 49
- ♦ “Changing the Ganglia Monitoring Configuration” on page 50
- ♦ “Generating Filr-Monitoring Reports” on page 51
- ♦ “Logging All HTTPS Traffic” on page 58
- ♦ “Managing Audit Trail Logs of Database Activity” on page 59

Accessing Filr System Log Files

Path: [Port 9443 Appliance Console](#) > **System Services icon**

Table 8-1 List of System Log Files

Field, Option, or Button	Information and/or Action
♦ Log Files column	<ul style="list-style-type: none">♦ Click one of the Download links to download the log files for the following services.<ul style="list-style-type: none">♦ Novell Filr: catalina.out, appserver.log The catalina.out file reports all timestamps in UTC/GMT. (Filr appliance)♦ Jetty: jetty.stderrout.log (Filr, Filrsearch, and PostgreSQL database appliances)♦ Postfix: mail (Filr appliance)♦ Novell FAMT: famtd.log (Filr appliance)♦ Search: indexserver.log (Filrsearch appliance)♦ PostgreSQL: postgresql.log (PostgreSQL appliance)♦ Memcached: jetty.stderrout.out (Filrsearch appliance)

Automatically Applying Deferred Search Logs

Path: [Port 8443 Appliance Console](#) > **Search Index** > **Update Logs**

Table 8-2 The Configure Update Logs dialog

Field, Option, or Button	Information and/or Action
<ul style="list-style-type: none"> ♦ Automatically Apply Deferred Update Logs in Background 	<p>IMPORTANT</p> <ul style="list-style-type: none"> ♦ The application of update logs is integral to Filr system design and data integrity. ♦ You should never disable this option unless instructed to do so by a support technician as part of resolving an incident report.

Changing the Ganglia Monitoring Configuration

Ganglia is a scalable, distributed monitoring system that lets you gather important information about your Filr system.

Path: [Port 9443 Appliance Console](#) > **Ganglia Configuration icon**

Table 8-3 Using the Ganglia Monitoring Configuration dialog

Field, Option, or Button	Information and/or Action
Monitoring Services	
Enable Full Monitoring Services	<ul style="list-style-type: none"> ♦ Deselect this if: <ul style="list-style-type: none"> ♦ You already have a monitoring system that you plan to use for Filr. ♦ You plan to configure a dedicated appliance for viewing monitoring information. <p>You do this by selecting Unicast below and then specifying the DNS name or IP address of the appliance where monitoring information will be collected.</p> ♦ (Default) Select this to have this appliance receive and store metrics from other appliances, and to allow the Ganglia Web Interface to run on the same machine as the Filr appliance.
Monitoring Options	
Enable Monitoring on this appliance	<ul style="list-style-type: none"> ♦ (Default) Select this option to enable Ganglia monitoring on this appliance.
<ul style="list-style-type: none"> ♦ Multicast 	<ul style="list-style-type: none"> ♦ (Default) Send performance data to the other appliances on the network (default setting).
<ul style="list-style-type: none"> ♦ Unicast 	<ul style="list-style-type: none"> ♦ Send monitoring information to a single destination. <p>This is a best practice recommendation for performance.</p>
<ul style="list-style-type: none"> ♦ Publish to: 	<ul style="list-style-type: none"> ♦ The URL where you want Ganglia to send monitoring information when it is running in Unicast mode.
Monitoring Tool Options	
<ul style="list-style-type: none"> ♦ Enable direct http port 9080 access 	<ul style="list-style-type: none"> ♦ Select this to allow Ganglia to communicate using HTTP port 9080.

Field, Option, or Button	Information and/or Action
<ul style="list-style-type: none"> ♦ Reset Database button 	<ul style="list-style-type: none"> ♦ Click this to remove all existing Ganglia metrics from this appliance. <p>This option is not related to the Filr database.</p>

See Also

- ♦ “Monitoring” in the *Filr 4.2: Maintenance Best Practices Guide*.
- ♦ The [Ganglia Monitoring System web site \(http://ganglia.info/\)](http://ganglia.info/).

Generating Filr-Monitoring Reports

The report information displays on the same page or gets downloaded to your computer in CSV format. The CSV file downloads in a new tab that automatically opens in the same browser. So, you must ensure that your browser allows pop-ups. Downloading large reports might take considerable time.

IMPORTANT: The Filr server captures logs based on the user's local time zone. Hence, when you generate a report, it is recommended to consider + or - one day depending on the time zone difference between you and the user.

Path: [Port 8443 Filr Admin Console > System > Reports](#)

Table 8-4 Using the Reports dialog

Field, Option, or Button	Information and/or Action
About the Reports	<ul style="list-style-type: none"> ♦ Most reports are created in CSV format for importing into a spreadsheet and manipulating the data to suit your needs. <p>A few reports are displayed in the Reports window.</p> <ul style="list-style-type: none"> ♦ The default file name for CSV-format reports is <code>report.csv</code>. <p>If you create multiple reports without manually renaming them, the default file name is incremented—<code>report (n).csv</code>.</p> <ul style="list-style-type: none"> ♦ CSV-format reports are saved in the default download directory for the browser being used.
<ul style="list-style-type: none"> ♦ Run a Report: 	<ul style="list-style-type: none"> ♦ Click the drop-down list and select a report to run. <p>The following sections describe the contents of each report.</p>

- ♦ “Credits Report” on page 52
- ♦ “Data Quota Exceeded Report” on page 52
- ♦ “Data Quota Highwater Exceeded Report” on page 52
- ♦ “Disk Usage Report” on page 53
- ♦ “Email Report” on page 53
- ♦ “External User Report” on page 54

- ♦ “File Block Report” on page 54
- ♦ “Filtr Outlook Report” on page 55
- ♦ “License Report” on page 55
- ♦ “Login Report” on page 56
- ♦ “Orphaned User Share Report” on page 56
- ♦ “System Error Logs Report” on page 57
- ♦ “User Access Report” on page 57
- ♦ “User Activity Report” on page 57
- ♦ “XSS (Cross-Site Scripting) Report” on page 58

Credits Report

Path: [Port 8443 Filr Admin Console](#) > **System** > **Reports** > **Run a Report:** > **Credits**

This report displays the portions of Filr that are subject to third-party copyrights and licenses.

Data Quota Exceeded Report

Path: [Port 8443 Filr Admin Console](#) > **System** > **Reports** > **Run a Report:** > **Data Quota Exceeded Report**

- ♦ This report is only available when Data Quotas are enabled.
- ♦ It lists users who have exceeded their data quota.
- ♦ The CSV-formatted report contains the following:
 - ♦ **Data Quota Used (MB):** The amount of disk space the user is currently using.
 - ♦ **Data Quota:** If set, this is the user’s individual quota. If not set, the quota displays as zero (0) and has no effect.
To set a quota for individual users, see [Table 16-2, “Using the Personal Storage \(data quota\) dialog,” on page 96](#).
 - ♦ **Max Group Quota (MB):** If group quotas are set for one or more groups that this user belongs to, this is the largest data quota set for any of those groups. If no groups have a quota set, the quota displays as zero (0) and has no effect.
To set group quotas, see [Table 16-2, “Using the Personal Storage \(data quota\) dialog,” on page 96](#).
 - ♦ **Default Data Quota (MB):** Displays the site-wide default quota.
For information on how to set a default data quota, see [Table 16-2, “Using the Personal Storage \(data quota\) dialog,” on page 96](#).

Data Quota Highwater Exceeded Report

Path: [Port 8443 Filr Admin Console](#) > **System** > **Reports** > **Run a Report:** > **Data Quota Highwater Exceeded Report**

- ♦ This report is only available when Data Quotas are enabled and one or more high-water marks are exceeded.

- ♦ It lists users who have exceeded their data high-water mark.
- ♦ The CSV-formatted report contains the following:
 - ♦ **Data Quota Used (MB):** The amount of disk space the user is currently using.
 - ♦ **Data Quota:** If set, this is the user's individual quota. If not set, the quota displays as zero (0) and has no effect.
To set a quota for individual users, see [Table 16-2, "Using the Personal Storage \(data quota\) dialog," on page 96](#).
 - ♦ **Max Group Quota (MB):** If group quotas are set for one or more groups that this user belongs to, this is the largest data quota set for any of those groups. If no groups have a quota set, the quota displays as zero (0) and has no effect.
To set group quotas, see [Table 16-2, "Using the Personal Storage \(data quota\) dialog," on page 96](#).
 - ♦ **Default Data Quota (MB):** Displays the site-wide default quota.
For information on how to set a default data quota, see [Table 16-2, "Using the Personal Storage \(data quota\) dialog," on page 96](#).

Disk Usage Report

Path: [Port 8443 Filr Admin Console](#) > **System** > **Reports** > **Run a Report:** > **Disk Usage Report**

- ♦ This report is only available when Personal Storage is enabled.
- ♦ You specify which of the following information to include in the CSV-formatted report:
 - ♦ **Total Usage by User:** Lists all Filr users whose disk space usage is above the amount specified in the **Include only users or workspaces with usage greater than** field.
 - ♦ **Total Usage by Workspace:** Lists all workspaces where disk space usage is above the amount specified in the **Include only users or workspaces with usage greater than** field. Disk space usage for each folder in each workspace is listed separately. The data is organized by workspace and folder ID.
 - ♦ **Total Usage by User and Workspace:** Combines the user and workspace data into a single report.
 - ♦ **Usage Greater Than:** The number of megabytes above which you want to list disk space usage. Use this to eliminate smaller disk space usages from being reported.

Email Report

Path: [Port 8443 Filr Admin Console](#) > **System** > **Reports** > **Run a Report:** > **Email Report**

- ♦ **Date Range:** The date range defaults to the past month, but dates can be set by clicking in the date fields and using drop-down widgets to change the range.
- ♦ **Sent emails:** Information about sent emails displays in the **Reports** window.
- ♦ **Error emails:** Information about email-associated errors displays in the **Reports** window.
- ♦ **Received emails:** Not operational because Filr cannot receive emails.
- ♦ Displayed reports include the following information:
 - ♦ **Send Date:** When the email was sent.

- ♦ **From Address:** Address that the email was sent from.
This is the email address defined in the user profile.
- ♦ **To Address:** Address that the email was sent to.
- ♦ **Type:** Action that caused the message to be sent.
For example, `sendMail` indicates that an item was shared.
- ♦ **Status:** Status of the message.
- ♦ **Subject Line:** Subject line of the message.
- ♦ **Attached Files:** File name of any attachments that were included in the email message.
- ♦ **Errors:** Any errors associated with the email message.

External User Report

Path: [Port 8443 Filr Admin Console](#) > **System** > **Reports** > **Run a Report:** > **External User Report**

- ♦ Lists the following information about the external users you include in the **People** field. If the **People** field is left blank, all external users are included.
 - ♦ User ID
 - ♦ First Name
 - ♦ Last Name
 - ♦ Email Address
 - ♦ Creation Date
 - ♦ Terms Acceptance Date

File Block Report

Path: [Port 8443 Filr Admin Console](#) > **System** > **Reports** > **Run a Report:** > **File Block Report**

This report lists information about all the files blocked from uploading during a specified period of time.

- ♦ **Date Range:** The date range defaults to the past month, but dates can be set by clicking in the date fields and using drop-down widgets to change the range.
- ♦ **People:** All users are covered by default, but you can begin typing names and use the name-completion widget to select specific users for the report.
- ♦ This report lists the following information about the files that were blocked from uploading.
 - ♦ User
 - ♦ File Name
 - ♦ File Operation
 - ♦ File Operation Time
 - ♦ Reason
 - ♦ IP Address

NOTE: For files that are being uploaded through the web browser, Filr does a minimal check on the files at the browser level itself and does not upload or save files that must be blocked. This report does not include any entry for files that Filr blocks at the browser level.

Filr Outlook Report

Path: [Port 8443 Filr Admin Console](#) > [System](#) > [Reports](#) > [Run a Report:](#) > [Filr Outlook Report](#)

- ♦ **Date Range:** The date range defaults to the past month, but dates can be set by clicking in the date fields and using drop-down widgets to change the range.
- ♦ This report lists the following information about the email sent through Outlook and the details of the file uploaded on the Filr server and shared in the email:
 - ♦ **Sender:** The account from which the Outlook email is sent.
 - ♦ **File Name:** The name of the file on the Filr server that is shared in the email.
 - ♦ **File Size:** The size of the file on the Filr server whose link is shared in the email.
 - ♦ **Sent Date:** The date on which the email is sent.
 - ♦ **Subject:** The subject of the email.
 - ♦ **Recipients:** The email addresses to which the email was sent.
 - ♦ **Accessed on:** The date and time when the Filr file shared in the email was last accessed.
 - ♦ **Expiration Date:** The date and time when the Filr file link sent in the email expires.
 - ♦ **Downloads Allowed:** The total number of times that the Filr file whose link is shared in the email can be accessed.
 - ♦ **Downloads Remaining:** The number of times that the Filr file whose link is shared in the email can still be accessed.

License Report

Path: [Port 8443 Filr Admin Console](#) > [System](#) > [Reports](#) > [Run a Report:](#) > [License Report](#)

The License report lists the following information in the Reports window:

- ♦ Filr version (**ProductTitle**)
- ♦ License key type (**Key uid**)
- ♦ Date the license key was issued (**Key issued**)
- ♦ Date range when the license key is valid (**Effective**)
- ♦ Information regarding registered and external user allowances.
- ♦ The **Date Range** covered by the report (as set before **Create Report** is clicked)
- ♦ **Current Active User Count**—user accounts that are not disabled.
- ♦ List of dates in the date range with the following user license information:
 - ♦ **Date:** The date for which the data in the row applies.
 - ♦ **Local Users:** User accounts created within Filr and not being synchronized from an LDAP directory.

- ♦ **Users Synchronized from LDAP:** User accounts created from an LDAP source. (Only synchronized accounts that are not marked as Deleted or Disabled are counted.)
- ♦ **Users with OpenID Accounts:** OpenID is no longer supported. Users that self-provisioned using an OpenID account.
- ♦ **Self Registered Users:** User accounts created when users self-provisioned.
- ♦ **Guest Access Enabled:** Whether Guest access was enabled on the listed date.
- ♦ **Users in the Past 365 Days:** Users who have logged in at least once in the past year.
- ♦ **Checksum:** <waiting for information from Sanjeev.>

Login Report

Path: [Port 8443 Filr Admin Console](#) > [System](#) > [Reports](#) > [Run a Report:](#) > [Login Report](#)

NOTE: This report only covers web client users. Mobile and Desktop users are not currently tracked.

- ♦ **Date Range:** The date range defaults to the past month, but dates can be set by clicking in the date fields and using drop-down widgets to change the range.
- ♦ **People:** All users are covered by default, but you can begin typing names and use the name-completion widget to select specific users for the report.
- ♦ **Summarize Login Entries:** Summarizes how many times the selected users have logged in using a web browser.

The **Sort Report By** drop-down list, lets you presort the data alphanumerically by **User**, **Last Login**, or **Number of Logins**.

- ♦ **List All Login Entries:** Lists each successful log in to the web client and includes the following data about the action:
 - ♦ User (first name, last name, and user ID)
 - ♦ Account type
 - ♦ Login date and time
 - ♦ IP address

The **Sort report by** drop-down list lets you presort the data alphanumerically by either **Login Date** or **User**.

Orphaned User Share Report

Path: [Port 8443 Filr Admin Console](#) > [System](#) > [Reports](#) > [Run a Report:](#) > [Orphaned User Share Report](#)

The Orphaned User Share report lists the following information in the Reports window:

- ♦ **User:** The name of the user who shared files or folders with other users and whose account is now either disabled or deleted. No information is displayed if the user object is deleted.
- ♦ **User State:** The state of the account of the user who shared the files: disabled or deleted.
- ♦ **Entity Type:** The type of entity (file or folder) that the user shared with other users.
- ♦ **Entity Name:** The name of the file or the folder that the user shared with other users.
- ♦ **Path:** The path of the shared entity.

- ♦ **Revoke:** Displays **Yes** or **No** depending on whether the orphaned user shares are already revoked.

System Error Logs Report

Path: [Port 8443 Filr Admin Console](#) > **System** > **Reports** > **Run a Report:** > **System Error Logs**

Use this to download a `logfiles.zip` file of the error logs currently on the system.

- ♦ **Download Log:** Generates a `logfiles.zip` file that contains the error logs currently on the system.
 - ♦ The zip file is downloaded to the browser's download directory.
 - ♦ If you download multiple zip files without manually renaming them, the file name is incremented—`logfiles (n).zip`

User Access Report

Path: [Port 8443 Filr Admin Console](#) > **System** > **Reports** > **Run a Report:** > **User Access Report**

This report shows each Filr location that the specified user has access to.

- ♦ **User:** Use the name-completion widget (type then select a name) to select a user you want to check.

A report for the user is automatically displayed in the Reports window, showing each location that the user has access to.

User Activity Report

Path: [Port 8443 Filr Admin Console](#) > **System** > **Reports** > **Run a Report:** > **User Activity Report**

This report summarizes the significant actions that specified users have taken on the Filr site during a specified period of time.

- ♦ **Date Range:** The date range defaults to the past month, but dates can be set by clicking in the date fields and using drop-down widgets to change the range.
- ♦ **People:** All users are covered by default, but you can begin typing names and use the name-completion widget to select specific users for the report.
- ♦ **Activity Summary:** This report lists how many times the selected users have performed the following actions in the Filr site:
 - ♦ User reported on
 - ♦ Views
 - ♦ Adds
 - ♦ Edits
 - ♦ Renames
 - ♦ Deletes (purge)
 - ♦ Pre-Delete (delete but not purge)
 - ♦ Restores (restore a deleted item that has not been purged)

- ♦ ACL changes
- ♦ Add shares
- ♦ Modify shares
- ♦ Delete shares
- ♦ **Workspace or Folder Activity:** This report lists each individual user action and includes the following data about the action:
 - ♦ User performing the action
 - ♦ Activity type
 - ♦ Count
 - ♦ Activity date and time
 - ♦ Folder
 - ♦ Entry title
 - ♦ Entity type
 - ♦ Share Recipient
 - ♦ Recipient Type
 - ♦ Share Role

XSS (Cross-Site Scripting) Report

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. For more general information about XSS, see “[XSS—Filr Is Secure](#)” in the *Filr 4.2: Maintenance Best Practices Guide*.

Path: [Port 8443 Filr Admin Console](#) > [System](#) > [Reports](#) > [Run a Report:](#) > [User Activity Report](#)

- ♦ **Select the binders to be checked:** Navigate the directory structure and select the directories you want to scan, then click **Create Report**.

The generated lets you to remove potentially harmful XSS threats from your Filr site.

IMPORTANT: Because XSS attacks often are designed to wait for users with extra privileges (such as the administrator) to view the page where the attack was set, it is important that you don’t navigate to the page after you run the report.

For information about how to run the XSS report and safely remove XSS threats, see “TID 7007381: Running the XSS Report in Micro Focus Filr” in the [Novell Support Knowledgebase](http://www.novell.com/support) (<http://www.novell.com/support>).

Logging All HTTPS Traffic

Path: [Port 9443 Appliance Console](#) > [Configuration icon](#) > [Logging](#)

Table 8-5 Using the Logging dialog

Field, Option, or Button	Information and/or Action
♦ Enable host access logging	<ul style="list-style-type: none">♦ Selecting this generates a single file that contains log information for all HTTPS traffic and can become large very quickly.♦ If the file grows too large, you must disable this option. <p>NOTE: By default, non-https logging is always enabled on the appliance. (For information about how to access the Filr log file, see “System Error Logs Report” on page 57.)</p>

Managing Audit Trail Logs of Database Activity

Path: [Port 8443 Filr Admin Console](#) > **Management** > **Database Logs**

Table 8-6 Using the Manage Database Logs dialog

Field, Option, or Button	Information and/or Action
Automatically Delete Audit Trail Entries Older Than X Days	<ul style="list-style-type: none">♦ This defines the maximum number of days to keep audit trail log entries before they are deleted. <p>The default is 183 days (6 months).</p> <p>The allowed minimum is 30 days, which would prune logs after 30 days.</p> <p>Specifying a value 0 means that the audit logs are never pruned.</p> <p>IMPORTANT: Before changing this, consider the following:</p> <ul style="list-style-type: none">♦ Audit trail entries are used to build the Activity and Login reports. Removing older entries limits the time span that these reports can cover. (For more information about these reports, see “Generating Filr-Monitoring Reports” on page 51.)♦ The Filr desktop application relies on audit trail data when doing full synchronizations.

9 Management Zones

Filr supports multi-tenancy by using Filr zones. Filr Administrators can now set Filr zones to create multiple virtual Filr sites within a single physical Filr site. Each Filr zone is completely independent and can be accessed using its own unique URL. Zone assets such as users, groups, shares, comments, and data cannot be accessed across zones. A maximum of 12 zones per Filr server is supported. This functionality is only available on Filr Advanced Edition.

Access to the Filr zones through NetIQ Access Manager is not supported.

- ♦ [“Managing Zones” on page 61](#)
- ♦ [“Adding and Modifying Zones” on page 61](#)
- ♦ [“Viewing Zones Information” on page 63](#)

Managing Zones

Path: [Port 8443 Filr Admin Console](#) > **Management** > **Zones**

Table 9-1 Using the Manage Zones dialog

Field, Option, or Button	Information and/or Action
♦ Add button	♦ Click this to launch the Add Zone dialog.
♦ Delete button	♦ Use this to remove the selected zones.
♦ Modify button	♦ Use this to modify the information for the selected zone.

Adding and Modifying Zones

- ♦ [“Adding a Zone” on page 61](#)
- ♦ [“Modifying a Zone” on page 62](#)
- ♦ [“Deleting Zones” on page 63](#)

Adding a Zone

Path: [Port 8443 Filr Admin Console](#) > **Management** > **Zones** > **Add**

Table 9-2 Using the Add Zone dialog

Field, Option, or Button	Information and/or Action
♦ Zone Name	♦ Specify a unique name to describe the zone. The name can include alphanumeric characters and should use less than or equal to 128 characters.
♦ Virtual Host	♦ Specify the hostname or fully qualified domain name of the zone that you have set up in DNS. The name should include less than or equal to 255 characters. ♦ Ensure that the hostname does not include the special character “_”.
♦ Description	♦ Specify a short description for the zone. This is an optional field and is limited to 128 characters.
♦ Unrestricted Storage	♦ Specifies the total amount of storage space that all the users in the zone can use in the Filr site. By default, the Unrestricted Storage option is selected, which means that the storage space in the Filr site is not restricted for the zone. ♦ To restrict the storage space for the zone: <ol style="list-style-type: none"> 1. Deselect the Unrestricted Storage option. 2. Specify values for the following: <ul style="list-style-type: none"> ♦ Storage Quota: Specify the total amount of disk space (in GB or TB) that all the users in the zone can use in the Filr site. IMPORTANT: Do not specify a zero value (0) for the Storage Quota. ♦ Default High-Water Mark: Specify the percentage of the zone storage quota utilization, when the zone administrator has to be notified that the zone users are approaching the storage quota. The default high-water mark is 90% of the total storage quota for the zone. IMPORTANT: Do not specify a zero value (0) for the Default High-Water Mark.

Modifying a Zone

Path: [Port 8443 Filr Admin Console](#) > [Management](#) > [Zone](#) > *Select a zone* > *Modify*.

Generally, the information in [Adding a Zone](#) applies to modifying a zone. You can modify the value of the **Virtual Host** and **Unrestricted Storage**. On modifying the new value for the virtual host, ensure the following:

- ♦ You must remove the DNS record for the previous virtual host value specified for the zone.
- ♦ The new value does not include the special character “_”. This fails to launch the console and results in “Error 400”.

Deleting Zones

Path: [Port 8443 Filr Admin Console](#) > **Management** > **Zone** > *Select one or more zones* > **Delete**.

When you delete a zone, you must remove the DNS record for the virtual host specified for the zone.

WARNING: Deleting the zone permanently deletes all zone-related entities and data from Filr and it cannot be undone.

Viewing Zones Information

Path: [Port 8443 Filr Admin Console](#) > **Management** > **Zones**

The Manage Zones page lists the following information about all the existing zones in the Filr site:

Table 9-3 Using the Manage Zone page

Field, Option, or Button	Information and/or Action
♦ Zone Name:	♦ Name of the zone.
♦ Virtual Host:	♦ The hostname or fully qualified domain name of the zone that you have set up in DNS.
♦ Description	♦ Description of the zone.
♦ Storage Space Used:	♦ The amount of the storage space, in percentage, used by all users in the zone. Depending on the space used, the storage space indicator displays one of the following colors: <ul style="list-style-type: none">♦ Green: The storage space used is within the high-water mark limit set for the zone.♦ Yellow: The storage space used is beyond the high-water mark limit set for the zone.

By default, the first zone in the list is highlighted. The Zone Information pane on the right hand side of the Manage Zones page displays the following additional information about the highlighted zone. To view the additional information for a zone, click the zone name to highlight that zone

Table 9-4 Using the Zone Information panel

Field, Option, or Button	Information and/or Action
♦ Internal Users Count:	♦ Number of internal users logged in to this zone.
♦ External Users Count:	♦ Number of external users logged in to this zone.
♦ Users Logged in Since 30 Days:	♦ Number of users logged in to this zone since 30 days.
♦ Storage Quota:	♦ The total storage space allocated for the zone

Field, Option, or Button	Information and/or Action
♦ Storage Space Used:	♦ The amount of the zone storage space already consumed by the zone users.
♦ Default High-Water Mark:	♦ The high-water mark set for the zone, which is the percentage of the zone storage quota utilization when the zone administrator has to be notified that the zone users are approaching the storage quota.

10 Net Folder Servers

- ♦ “Creating and Managing Net Folder Servers” on page 65
- ♦ “Enabling Just-in-Time-Synchronization for Filr and eDirectory Rights Usage for OES and NetWare” on page 70
- ♦ “Proxy User Identities” on page 71

Creating and Managing Net Folder Servers

- ♦ “Manage Net Folder Servers Dialog” on page 65
- ♦ “Creating a Net Folder Server” on page 65
- ♦ “Editing an Existing Net Folder Server” on page 70
- ♦ “Deleting a Net Folder Server” on page 70

Manage Net Folder Servers Dialog

Net Folder Servers are “connections” to physical file servers and their associated NSS volumes, CIFS shares, or SharePoint sites. You can set up as many Net Folder Servers as needed.

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

Table 10-1 Using the Manage Net Folder Servers dialog


Field, Option, or Button	Information and/or Action
♦ Add button	♦ Click this to create a new Net Folder Server .
♦ Delete button	♦ Before you can delete a Net Folder Server, you must first delete all Net Folders associated with it. ♦ After completing the first step and selecting a listed Net Folder Server, click this button to remove the connection to this Net Folder Server from Filr. Data on the back-end server is unaffected.
♦ Sync button	♦ After selecting a Net Folder Server, click this to immediately synchronize Net Folder meta data with Filr according to the Synchronization Options you have set.
♦ Name	♦ Click a Net Folder Server name to begin editing its configuration settings .
♦ Path	♦ This shows the connection path to the Net Folder Server.


Creating a Net Folder Server



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


Best Practice: Plan your Net Folder Servers in advance and use the following table when working in this dialog:

Table 10-2 Using the New Net Folder Server dialog

Field, Option, or Button	Information and/or Action
 Configuration tab	
<ul style="list-style-type: none">♦ Name:	<ul style="list-style-type: none">♦ Specify a name for this Net Folder Server.♦ In most cases this should be a name that clearly indicates the file server and volume.♦ If the server and volume are defined in your LDAP directory services as a Home Directory location, a Home Net Folder Server is created automatically and the name is assigned using the information in LDAP, as follows: <i>defined_dns_or_ip_path_to_server-volume_or_share_name</i> For example,<ul style="list-style-type: none">♦ <code>\\oes-fs-1.my-company.local\HOME_NSS</code> Is automatically named: <code>oes-fs-1.my-company.local-HOME_NSS</code>♦ <code>\\Win2012.my-company.local\Home_Folders\$</code> Is automatically named: <code>Win2012.my-company.local-Home_Folders\$</code>

Field, Option, or Button	Information and/or Action
<ul style="list-style-type: none"> ♦ Server Type: 	<ul style="list-style-type: none"> ♦ Server types include OES, OES 2015 or later (NSS for AD), NetWare, Windows or SharePoint 2013. ♦ For OES 2015 or later NSS AD servers, you must consider whether the Volume is enabled for NSS AD and the protocol that the volume uses: <ul style="list-style-type: none"> ♦ Volume enabled for NSS AD Uses the CIFS or NCP protocol Select Micro Focus Open Enterprise Server (NSS for AD) as the server type ♦ Volume not enabled for NSS AD Uses CIFS protocol Select Micro Focus Open Enterprise Server (NSS for AD) as the server type For more information on NSS AD, see the NSS AD Administration Guide. ♦ Volume not enabled for NSS AD Uses NCP protocol Select Micro Focus Open Enterprise Server as the server type ♦ For NSS volumes on OES 2015 or later servers that have DFS junction targets that point to an older OES server, you must select Micro Focus Open Enterprise Server as the server type. Otherwise, the trustee assignments on the target will not be reflected in Filr. If an NSS volume on an OES 2015 or later server has DFS junctions and you are planning to select the OES 2015 NSS for AD server type, you must scan the volume from iManager as instructed in “Managing Junctions” in the <i>OES 2018 SP2: Domain Services for Windows Administration Guide</i>. ♦ For Home Net Folder Servers, this is set automatically
<ul style="list-style-type: none"> ♦ Server Path: 	<ul style="list-style-type: none"> ♦ The path to the NSS volume (OES or NetWare), NSS volume on OES 2015, Windows share, or SharePoint 2013 site on the file server. ♦ For Home Net Folder Servers, this is set automatically
 Authentication tab	
<ul style="list-style-type: none"> ♦ Specify proxy using a Proxy Identity <ul style="list-style-type: none"> ♦ Proxy identity: 	<ul style="list-style-type: none"> ♦ Best Practice: Select this option to specify a Proxy Identity. ♦ Click the Proxy Identity field and begin typing to expose the list of Proxy Identities. Select a previously defined Proxy Identity created in “Creating Proxy Identities” on page 72.

Field, Option, or Button	Information and/or Action
<ul style="list-style-type: none"> Specify proxy using a name and password <ul style="list-style-type: none"> Proxy name: Proxy password: 	<ul style="list-style-type: none"> Alternate Practice: Select this option to specify a Proxy User and Password. Click the LDAP browse icon to find and select the Proxy Name. Type the Proxy Password. <p>Proxy name and password: Specify the fully qualified, comma-delimited name and password for the proxy user used to access the OES, NetWare, Windows, or SharePoint 2013 server. (You can use the Browse icon  next to the Proxy field to browse the LDAP directory for the proxy user that you want to use.)</p>
<ul style="list-style-type: none"> Test Connection button 	<ul style="list-style-type: none"> Always click this button to ensure that the path is accurate and that the credentials are valid. <p>Sometimes proxy users with the incorrect context pass this test. Ensure that the context for your proxy user is correct.</p>
<ul style="list-style-type: none"> Authentication Type: 	<ul style="list-style-type: none"> Select the authentication service for the file server that you are connecting to. <p>Option availability reflects the Server type setting that you selected in the Configuration tab.</p> <ul style="list-style-type: none"> For OES or NetWare, only Micro Focus NMAS is available. For OES (NSS for AD), only Auto Detect (Kerberos then NTLM) is available. For Windows, you can select Kerberos, NTLM, or Auto detect (meaning that Kerberos is attempted first, and if it fails, NTLM is used.) <p>Kerberos requires</p> <ul style="list-style-type: none"> That the DNS name server can resolve DNS queries for the Active Directory domains. <p>And</p> <ul style="list-style-type: none"> Kerberos port 88 communication is available. <p>If either requirement is not met, you must select NTLM as the authentication type.</p>
 Synchronization Schedule tab	
<ul style="list-style-type: none"> Enable Scheduled Synchronization 	<ul style="list-style-type: none"> Select this option to enable full metadata synchronization between the back-end file server and Filr according to the schedule you specify below this option.
<ul style="list-style-type: none"> Every Day On Selected Days At <p>Repeat every XX hours</p>	<ul style="list-style-type: none"> The options you select and configure in this section set a default schedule for each Net Folder associated with this Net Folder Server. The synchronization options you specify can greatly affect system performance. <p>As a best practice, Micro Focus recommends that you set the options here only after completing the planning.</p>

Field, Option, or Button	Information and/or Action
 Synchronization Options tab	
<ul style="list-style-type: none"> ♦ Index the Content of files in the Net Folders 	<ul style="list-style-type: none"> ♦ Select this to have Filr index the files in all associated Net Folders for searchability. <p>IMPORTANT: Enabling indexing at the Net Folder Server level is not usually a best practice. Rather, indexing should be confined to Net Folders. This is why disk space planning should be done at the Net Folder level.</p> <p>A possible exception to this rule is enabling content indexing of Home Net Folder Servers.</p>
<ul style="list-style-type: none"> ♦ Enable Just-in-Time synchronization 	<p>IMPORTANT: This is always available as a selectable option, but it has no effect unless JITS is enabled for the Filr system. See “Enabling Just-in-Time-Synchronization for Filr and eDirectory Rights Usage for OES and NetWare” on page 70.</p> <ul style="list-style-type: none"> ♦ Click this to enable JITS on this Net Folder Server with the following options enforced. ♦ For Home Net Folder Servers, JITS is automatically enabled.
<ul style="list-style-type: none"> ♦ Maximum age for Just-in-Time results 	<ul style="list-style-type: none"> ♦ How long Filr waits from the last JITS synchronization before re-syncing. <p>Default is 60 seconds.</p>
<ul style="list-style-type: none"> ♦ Maximum age for ACL Just-in-Time results 	<ul style="list-style-type: none"> ♦ How long Filr waits from the last ACL retrieval before retrieving the information again. <p>The default is 3600 seconds (60 minutes).</p>
<ul style="list-style-type: none"> ♦ Allow the desktop app to trigger initial home folder sync 	<ul style="list-style-type: none"> ♦ Select this option to ensure that user Home folders are synchronized with users’ desktops. <p>If this option is not selected, user Home folders are synchronized to the Filr desktop application only after the user has logged in to Filr on the web, or after the Filr administrator triggers a full initial synchronization from the administration console (as described in “Enabling and Tuning Net Folder Synchronization” on page 81).</p> <ul style="list-style-type: none"> ♦ For Home Net Folder Servers, this is automatically selected.
OK button	<ul style="list-style-type: none"> ♦ Click this to save your changes. <p>Current user sessions are not affected. To see changes, users must log in to a new session.</p>
Cancel button	<ul style="list-style-type: none"> ♦ Click this to cancel the changes you have made.

Editing an Existing Net Folder Server

NOTE: To fix a Home Net Folder Server configuration that was created automatically, you need only provide a Proxy Identity or proxy user. See [“Specify proxy using a Proxy Identity” on page 67](#).

Path: [Port 8443 Filr Admin Console](#) > [Management](#) > [Net Folder Servers](#) > *Click a listed Net Folder Server*

Generally, the information in [“Creating a Net Folder Server” on page 65](#) applies to the Edit Net Folder Server dialog, with the following exceptions:

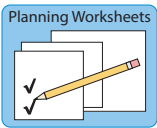
- ♦ The **Name** cannot be modified
- ♦ Do not change the **Server Type**.
If you have migrated data to a new back-end file server, you must create a new Net Folder Server.
- ♦ Consult with Micro Focus Support before changing the **Server Path**.

Deleting a Net Folder Server

Refer to the information for the **Delete** button in [Table 10-1 on page 65](#).


Enabling Just-in-Time-Synchronization for Filr and eDirectory Rights Usage for OES and NetWare

Path: [Port 8443 Filr Admin Console](#) > [Management](#) > [Net Folder Settings](#)



Best Practice: Plan for Just-in-Time Synchronization (JITS) in advance.

Table 10-3 *Using the Net Folder Settings dialog*

Field, Option, or Button	Information and/or Action
 Net Folder Global Settings	
♦ Enable Just-in-Time synchronization of Net Folders	<ul style="list-style-type: none">♦ This controls general availability of Just-in-Time Synchronization.♦ Selecting this allows the JITS settings on Net Folders and Net Folder Servers to function.♦ De-selecting this disables JITS system-wide. In other words, if you disable JITS here, then even though it can still be selected or deselected on individual Net Folder Servers and Net Folders, it won't actually work.

Field, Option, or Button	Information and/or Action
<ul style="list-style-type: none"> ◆ Maximum wait time for results X Seconds 	<ul style="list-style-type: none"> ◆ This sets the default value for how long the JITS process retrieves file and folder metadata within a folder before returning the results to the user. If all Metadata for the folder was not retrieved, retrieval continues in the background. <p>The default is 5 seconds.</p>
<ul style="list-style-type: none"> ◆ Use directory rights in addition to file system rights 	<ul style="list-style-type: none"> ◆ This is enabled by default and causes Filr to check eDirectory for user and group trustee information when accessing Net Folders. <p>For example, users and groups who have Supervisor rights on the NCP server object have implicit rights on the volume in eDirectory and are therefore trustees from an NCP perspective.</p> <ul style="list-style-type: none"> ◆ If you are certain that no users inherit needed rights from eDirectory, you can consider disabling this. However, if you miss something, disabling this option might affect users' ability to access certain files and folders. ◆ Checking eDirectory rights is a resource intensive task, hence Filr only checks for these rights in the below scenarios: <ul style="list-style-type: none"> ◆ When a Filr server is restarted., or ◆ They take effect on a Net Folder Server, the next time the Net Folder Server is reconfigured.
Refresh cached rights information every X Minutes	<ul style="list-style-type: none"> ◆ This is the frequency that the Filr server checks the rights information from the OES file system. ◆ The default is every 5 minutes. ◆ Rights information is available in Filr only after one of the following occurs since the last successful cache refresh: <ul style="list-style-type: none"> ◆ Just-in-Time synchronization on the folder. ◆ A scheduled or manual Full synchronization happens on the Net Folder or Net Folder Server. ◆ This option applies only to OES back-end servers. <ul style="list-style-type: none"> ◆ NetWare servers refresh every 60 minutes. ◆ Windows and SharePoint servers refresh only when Net Folder and Net Folder Server synchronizations occur.

Proxy User Identities

Proxy User Identities simplify the selection and password maintenance processes associated with Net Folder Proxy Users. After [defining a Proxy Identity](#), you can select it in a list rather than browsing the LDAP tree, and when the user's password changes on the backend, you only change it in the Proxy User Identity dialog rather than in each Net Folder Server.

- ◆ [“Managing Proxy Identities” on page 72](#)
- ◆ [“Creating Proxy Identities” on page 72](#)
- ◆ [“Modifying Proxy Identities” on page 72](#)

Managing Proxy Identities

Path: [Port 8443 Filr Admin Console](#) > **Management** > **Proxy Identities**

Best Practice: Plan your Proxy Identities in advance and use the following table when working in this dialog:


Table 10-4 Using the Manage Proxy Identities dialog

Field, Option, or Button	Information and/or Action
Proxy Identities	
♦ New Proxy Identity... button	♦ Click this to launch the Creating Proxy Identities .
♦ Delete button	♦ Use this to remove the selected Proxy Identity. The LDAP proxy user associated with the Proxy Identity is unaffected.
♦ Filter List field	♦ Begin typing a string to limit the displayed list of Proxy Identities.
♦ Gear icon	♦ Click this and select Edit Column Sizes to open the Edit Column Sizes dialog. You can then modify the column widths to fit your requirements.

Creating Proxy Identities

Path: [Port 8443 Filr Admin Console](#) > **Management** > **Proxy Identities** > **New Proxy Identity...**

Table 10-5 Using the New Proxy Identity dialog

Field, Option, or Button	Information and/or Action
 New Proxy Identity	
♦ Title:	♦ Type the name you want displayed in the Proxy Identities list. Specify a name that is easily associated with the Net Folder servers to which the associated LDAP Proxy user has rights.
♦ Proxy name:	♦ Use the LDAP browser icon to browse to and select the target proxy user.
♦ Proxy password:	♦ Type the current password of the target proxy user.
♦ Verify password:	♦ Retype the password.

Modifying Proxy Identities

Path: [Port 8443 Filr Admin Console](#) > **Management** > **Proxy Identities** > **New Proxy Identity...**

Table 10-6 *Using the New Proxy Identity dialog*

Field, Option, or Button	Information and/or Action
Modify Proxy Identity	
◆ Title:	◆ You can change the name you want displayed in the Proxy Identities list. The changed name then replaces the previous name in all lists and dialogs.
◆ Proxy name:	◆ You can associate a different LDAP proxy user with the Proxy Identity by using the LDAP browser.
◆ Proxy password:	◆ When the password changes in LDAP, you can change it here rather than needing to change each Net Folder Server’s proxy information.
◆ Verify password:	◆ All changes require that you type and verify the password.

11 Net Folders

- ♦ [“Managing Net Folders” on page 75](#)
- ♦ [“Creating and Modifying Net Folders” on page 76](#)

Net Folders are connections to specific directories within the Net Folder Servers you have created. You can synchronize Net Folders on a schedule independent of the schedule set for the Net Folder Server.

Managing Net Folders

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

Table 11-1 *Using the Manage Net Folders dialog*

Field, Option, or Button	Information and/or Action
♦ Add button	♦ Click this to create a new Net Folder .
♦ Delete button	♦ Select a Net Folder in the list, then click this and confirm that you want to remove the Net Folder from Filr. Filr users no longer have access to the Net Folder. No data is affected on the back-end file server.
♦ Sync button	♦ Click this to start a manual synchronization of the Net Folder.
♦ Stop sync button	♦ Click this to stop a synchronization operation that is in progress.
♦ Filter List field	♦ To filter the list of Net Folders, specify the name of a Net Folder in this field.
♦ Arrow drop-down	♦ To display User Home Directories in the list, click this and select Show Home Directories .
♦ Name	♦ This column lists all of the standard Net Folders associated with the Filr appliance.
♦ Sync status icon	♦ The icon indicates the current synchronization status. ♦ Click the icon to view more information about the current synchronization status.
♦ Server Name	♦ The name of the Net Folder Server to which this Net Folder belongs.
♦ Relative Path	♦ The directory path to this Net Folder from its parent Net Folder Server.

Creating and Modifying Net Folders

- ♦ [“Creating a Net Folder” on page 76](#)
- ♦ [“Modifying a Net Folder” on page 80](#)
- ♦ [“Deleting a Net Folder” on page 80](#)

Creating a Net Folder

Path: [Port 8443 Filr Admin Console](#) > **Management** > **Net Folders** > **Add**

Best Practice: Plan your Net Folders in advance and use the following table when working in this dialog:

Table 11-2 *Using the New Net Folder dialog*

Field, Option, or Button	Information and/or Action
Configuration tab	
♦ Name:	♦ Specify a name that you want users to see when accessing the Net Folder.
♦ Net Folder Server:	♦ Using the drop-down list, select the Net Folder Server that the new Net Folder is associated with.
♦ New Net Folder Server: button	♦ If you have not already established a Net Folder Server for this Net Folder, you can create it by clicking this and following the instructions in “Creating and Managing Net Folder Servers” on page 65 .
♦ Relative path:	<div>♦ Specify the relative path to the folder on the Net Folder Server. If this field is left blank, it uses the Net Folder Server path.</div> <div>When connecting to a SharePoint site, if you leave the Relative Path field blank, all document libraries shown in Site Contents are synchronized to Filr. These libraries include the following: Documents, Form Templates, Site Assets, Site Pages, Style Library, and any user-created document libraries.</div>
♦ Test Connection button	♦ Click this to verify that the path that you have typed is valid.
♦ Use the index content setting defined on the Net Folder Server	<div>♦ This is selected by default and causes this Net Folder to use the content indexing setting defined for the Net Folder Server, which is that content-indexing is not enabled.</div> <div>As noted in “Creating a Net Folder Server” on page 65, enabling indexing at the Net Folder Server level is not a best practice and there is no disk space planning support in the planning worksheets for this.</div>

Field, Option, or Button	Information and/or Action
<ul style="list-style-type: none"> ♦ Use the index content setting defined below 	<ul style="list-style-type: none"> ♦ If the Content Searchable? value is set to Yes, select this option to configure this Net Folder for content indexing. <p>Because indexing happens in the background and can take several hours or even days to complete for large datasets, Micro Focus recommends “Dedicating a Filr Appliance to Indexing and Net Folder Synchronization” as explained in the <i>Filr: Installation, Deployment, and Upgrade Guide</i>.</p>
<ul style="list-style-type: none"> ♦ Index the content of files within this Net Folder 	<ul style="list-style-type: none"> ♦ If you selected the option to Use the index content setting defined below, you must select this if you want to enable content indexing for the Net Folder. <p>This is presented as a separate option from its parent option to allow for those cases where content indexing is enabled at the Net Folder Server level (not a best practice) but this Net Folder should not be indexed.</p>
<ul style="list-style-type: none"> ♦ Use the Just-in-Time settings defined on the Net Folder Server 	<ul style="list-style-type: none"> ♦ This is selected by default and causes this Net Folder to use the JITS settings defined for the associated Net Folder Server.
<ul style="list-style-type: none"> ♦ Use the Just-in-Time settings defined below 	<ul style="list-style-type: none"> ♦ Select this if you want to use different JITS settings than are defined on the associated Net Folder Server.
<ul style="list-style-type: none"> ♦ Enable Just-in-Time synchronization 	<p>IMPORTANT: This is always available as a selectable option, but it has no effect unless JITS is enabled for the Filr system. See “Enabling Just-in-Time-Synchronization for Filr and eDirectory Rights Usage for OES and NetWare” on page 70.</p> <ul style="list-style-type: none"> ♦ If you selected the option to Use the Just-in-Time settings defined below, you must select this if you want to enable JITS synchronization for the Net Folder. <p>This is presented as a separate option from its parent option to allow for those cases where JITS is enabled at the Net Folder Server level but JITS should not apply to this Net Folder.</p>
<ul style="list-style-type: none"> ♦ Maximum age for Just-in-Time results 	<ul style="list-style-type: none"> ♦ How long Filr waits from the last JITS synchronization before re-syncing. <p>Default is 60 seconds.</p>
<ul style="list-style-type: none"> ♦ Maximum age for ACL Just-in-Time results 	<ul style="list-style-type: none"> ♦ How long Filr waits from the last ACL retrieval before retrieving the information again. <p>The default is 3600 seconds (60 minutes).</p>
Rights tab	Net Folder Sharing Settings

Field, Option, or Button	Information and/or Action
<ul style="list-style-type: none"> ♦ User or Group: 	<ul style="list-style-type: none"> ♦ After clicking the Rights tab, begin typing the name of a User or Group that you want to have access to the files and folders on the Net Folder. ♦ Click the name when it appears in the drop-down list. <p>You can specify the following types of users, groups, and Organization Units (OUs) for granting rights:</p> <ul style="list-style-type: none"> ♦ Individual users (either imported from the LDAP directory or that have been created in Filr) ♦ Groups (either imported from the LDAP directory or that have been created in Filr) ♦ Organization Units (when using eDirectory as the LDAP directory) <p>After you specify the user, group, or Organization Unit and select it, the Grant Rights dialog box displays.</p>
Grant Rights dialog	
<ul style="list-style-type: none"> ♦ Allow access to the Net Folder 	<ul style="list-style-type: none"> ♦ You must select this for the associated user or group to access the Net Folder. <p>Users are granted a Filr role that roughly corresponds to the same level of access rights that they currently have on the back-end server's file system.</p> <p>If you select have selected users or groups that don't currently have access rights on the file system, they see only folder names.</p>
<ul style="list-style-type: none"> ♦ Recipient can share files in this Net Folder with: 	<ul style="list-style-type: none"> ♦ If you want the associated user or group to be able to share the files within this Net Folder, select from the following options. <ul style="list-style-type: none"> ♦ Internal users ♦ External users ♦ Public ♦ Share using File Link ♦ Allow the recipient to grant files re-share privilege <p>For more information about sharing in Filr, see "Understanding Sharing" in <i>Filr: Understanding How Filr Works</i>.</p> <p>IMPORTANT: Users and groups must first be included in the Managing Sharing, License Terms, and Comments > Rights tab, and their maximum sharing privileges defined there before they can be granted rights to share files here.</p> <p>Furthermore, the rights available here are restricted to only those granted in the Managing Sharing, License Terms, and Comments.</p>

Field, Option, or Button	Information and/or Action
<ul style="list-style-type: none"> ◆ Recipient can share folders in this Net Folder with: 	<p>IMPORTANT: This functionality is only available when an Advanced-Edition license is installed on the Filr appliances.</p> <ul style="list-style-type: none"> ◆ If you want the associated user or group to be able to share folders within this Net Folder, select from the following options. <ul style="list-style-type: none"> ◆ Internal users ◆ External users ◆ Public ◆ Allow the recipient to grant folders re-share privilege <p>For more information about folder sharing in Filr, see “Folder Sharing (Advanced-Edition License Only)” in <i>Filr: Understanding How Filr Works</i>.</p> <p>IMPORTANT: Users and groups must first be included in the Managing Sharing, License Terms, and Comments > Rights tab, and their maximum sharing privileges defined there before they can be granted rights to share folders here.</p> <p>Furthermore, the rights available here are restricted to only those granted in the Managing Sharing, License Terms, and Comments.</p>
Synchronization Schedule tab	Net Folder Synchronization
<ul style="list-style-type: none"> ◆ Use the synchronization schedule defined on the Net Folder Server 	<ul style="list-style-type: none"> ◆ If you already set a synchronization schedule for the Net Folder Server (as described in “Creating and Managing Net Folder Servers” on page 65), and if you want the Net Folder to use that same schedule, select this option.
<ul style="list-style-type: none"> ◆ Use the synchronization schedule defined below 	<ul style="list-style-type: none"> ◆ Select this option to create an independent synchronization schedule for the Net Folder.
<ul style="list-style-type: none"> ◆ Enable scheduled synchronization: 	<ul style="list-style-type: none"> ◆ Select this option to enable synchronization, then select from the following synchronization options: <ul style="list-style-type: none"> ◆ Every day: Synchronize files every day. ◆ On selected days: Synchronize files only on designated days of the week. ◆ At: Select the time of day to synchronize files. ◆ Repeat every xx hours: Select how frequently the synchronization occurs. ◆ This is presented separately from the parent option to allow for those cases where full synchronization is enabled at the Net Folder Server level but should not apply to this Net Folder.
Data Synchronization tab	
<ul style="list-style-type: none"> ◆ This folder can be accessed from the user's desktop 	<ul style="list-style-type: none"> ◆ This option is enabled by default on upgrading to Filr 3.4 or later. If selected, Filr desktop users can view this Net folder using the desktop application. <p>If deselected, this Net folder is hidden from the desktop users.</p>

Field, Option, or Button	Information and/or Action
♦ Users can access this folder only in an online mode	♦ If this option is selected, the Make available offline option is not available for the users. However, a user can double-click a file to cache it locally.
♦ Users can access this folder both in an online and offline mode	♦ If this option is selected, users can perform all operations on the files and folders.

Modifying a Net Folder

Path: [Port 8443 Filr Admin Console](#) > **Management** > **Net Folders** > *Click a Net Folder in the list*

Generally, the information in “[Creating a Net Folder](#)” on [page 76](#) applies to the Edit Net Folder Server dialog, with the following exception:

- ♦ Do not change the associated **Net Folder Server** or attempt to create a different Net Folder Server for this Net Folder.

Deleting a Net Folder

Path: [Port 8443 Filr Admin Console](#) > **Management** > **Net Folders** > *Select a listed Net Folder* > **Delete**

See the information for the **Delete** button in [Table 11-1, “Using the Manage Net Folders dialog,”](#) on [page 75](#).

12 Net Folder System-Level Synchronization

- ♦ “Enabling and Tuning Net Folder Synchronization” on page 81
- ♦ “Just-in-Time Synchronization” on page 82

Enabling and Tuning Net Folder Synchronization

Use the following dialog to allow the full synchronization of Net Folders to happen.

Path: [Port 9443 Appliance Console](#) > [Filtr Appliance Tools](#) > [Configuration icon](#) > [Net Folders](#)

Table 12-1 Using the Net Folders (synchronization) dialog

Field, Option, or Button	Information and/or Action
Net Folders dialog	
♦ Allow Synchronization	<ul style="list-style-type: none">♦ Select this option to allow manual and scheduled full synchronizations of Net Folders on the appliance. <p>IMPORTANT: This setting must be selected for at least one Filr appliance in a Filr cluster. If it is not, no manual or scheduled full synchronizations can happen.</p>
♦ Max Simultaneous Syncs:	<ul style="list-style-type: none">♦ The number of Net Folders that can be synchronized simultaneously during a manual or scheduled full synchronization. <p>The default is 5.</p>
♦ Threads Per Sync:	<ul style="list-style-type: none">♦ The number of threads that each synchronization can use. <p>The default is 4.</p> <ul style="list-style-type: none">♦ For optimal performance, modify this value to be equal to the number of CPUs on the appliance, multiplied by 1.5. <p>For example, if your appliance has 2 CPUs, change this value to 3.</p> <ul style="list-style-type: none">♦ The max value that you can set is the number of CPUs on the appliance multiplied by 3. <p>For example, if your appliance has 2 CPUs, the max value is 6.</p>
OK button	<ul style="list-style-type: none">♦ Click this to save your changes. Then click Reconfigure Filr Server so that the changes are used by Filr.
Cancel button	<ul style="list-style-type: none">♦ Click this to cancel the changes you have made.

Just-in-Time Synchronization

Just-in-time synchronization is a process whereby the metadata for files and folders is immediately downloaded from the file server to Filr when users browse to a folder.

It affects many different parts of Filr services as reflected in the following table.

Table 12-2 *JITS Task Summary*

To do this	See this
♦ Enable/Disable JITS for the Filr system	♦ “Enabling Just-in-Time-Synchronization for Filr and eDirectory Rights Usage for OES and NetWare” on page 70
♦ Enable/Disable JITS for a Net Folder Server	♦ “Enable Just-in-Time synchronization” on page 69
♦ Enable/Disable JITS on a Net Folder	♦ “Enable Just-in-Time synchronization” on page 77
♦ Enable/Disable JITS on a user’s Home folder	♦ ““Home Folder button” on page 147”

13 Network Infrastructure

- ♦ [“Changing Network Settings” on page 83](#)
- ♦ [“Network Configuration” on page 84](#)
- ♦ [“Port Numbers” on page 86](#)

Changing Network Settings

The settings in this dialog are set during initial deployment.

Path: [Port 9443 Appliance Console](#) > **Network icon**

Table 13-1 Using the Network (DNS, IP, Access restrictions) dialog

Field, Option, or Button	Information and/or Action
Network (IP Infrastructure) dialog	Network Support (IP Address Infrastructure Information and Appliance-Specific IP Configuration Settings)
DNS Configuration section	
♦ Name Servers:	♦ You can modify the name servers.
♦ Search Domains:	♦ If this field is left blank, it is auto-populated with the domain of the appliance hostname. For example, if the hostname of the appliance is <code>filr.mycompany.com</code> , the domain is auto-populated with <code>mycompany.com</code> .
♦ Gateway:	♦ Make sure that this matches any of the other changes you have made in this dialog.
NIC Configuration section	<ul style="list-style-type: none">♦ In this section, you can modify the IP address, hostname, and network mask of any Network Interface Controller (NIC) associated with the appliance. (If you configured multiple NICs for the Filr appliance, you can configure the additional NICs.)<ul style="list-style-type: none">♦ In the NIC Configuration section, click the ID of the NIC.♦ Edit the IP address, hostname, or network mask. If you change the IP address, you must restart the appliance in order for the change to be reflected.♦ Click OK.
Appliance Administration UI (Port 9443) Access Restrictions section	<ul style="list-style-type: none">♦ In this section, specify the IP address of any networks for which you want to allow access to the Filr site.♦ Leave this section blank to allow administrative access from any network.

Field, Option, or Button	Information and/or Action
OK button	<ul style="list-style-type: none"> Click this to save your changes, then click Reconfigure Filr Server. <p>This stops and restarts your Filr server. Because this results in server downtime, you should restart the server during off-peak hours.</p> <p>User sessions can be affected by the above changes.</p>
Cancel button	<ul style="list-style-type: none"> Click this to cancel the changes you have made.

Network Configuration

Path: [Port 9443 Appliance Console](#) > **Configuration icon** > **Network**

Table 13-2 Using the Network (Port Redirection) dialog

Field, Option, or Button	Information and/or Action
Network (Communication Configuration) dialog	Network Support (Network Communication Configuration)
<ul style="list-style-type: none"> Port Redirection 	<ul style="list-style-type: none"> Select this option to have Filr automatically redirect from ports 80 or 443 (which are the standard ports for Web browsers) to ports 8080 and 8443 (which are the default ports that Filr listens on). Enabling port redirection in this way allows users to specify the Filr site URL without including the port number. If port redirection is not enabled, users must include the port number in the site URL when accessing the Filr site. <p>IMPORTANT: When port redirection is enabled, ensure that the reverse proxy ports are set to 80 for the HTTP port and to 443 for the secure HTTP port. If they are not, URLs that are sent with Filr email notifications will continue to have the default port (8443) in them.</p> <p>For information about how to change the reverse proxy ports, see “Reverse Proxy Configuration Settings” on page 28.</p>
<ul style="list-style-type: none"> HTTP Port: 	<ul style="list-style-type: none"> The default HTTP port is 8080. As a best practice, do not change this from the default port. <ul style="list-style-type: none"> Select Enabled if you want to enable the HTTP port. By default, only the Secure HTTP port is enabled. Select Force Secure Connection to force users to connect to Filr over a secure connection (HTTPS). <p>See “Port Numbers” on page 86 for more information about port numbers in Filr.</p>
<ul style="list-style-type: none"> HTTPS Port: 	<ul style="list-style-type: none"> HTTPS Port: The default secure HTTP port for Filr is 8443. As a best practice, do not change this from the default. <p>See “Port Numbers” on page 86 for more information about port numbers in Filr.</p>

Field, Option, or Button	Information and/or Action
♦ AJP Port:	♦ For an explanation of the Apache JServ Protocol port, see The AJP Connector (http://tomcat.apache.org/tomcat-6.0-doc/config/ajp.html) .
♦ Session Timeout	♦ By default, if the Admin Console session is idle for four hours (240 minutes), Filr logs the idle user out. For increased convenience to Filr users, you can make the session timeout interval longer. For increased security for your Filr site, you can make the session timeout shorter. The minimum value for this field is 20 (minutes). ♦ This setting is not valid for the Web UI that is available in Filr 4.2 and later. The default session timeout for Web UI is 15 minutes and the token gets refreshed every 5 minutes. If you want to change these values, add the following parameters to the <code>ssf-ext.properties</code> file: <ul style="list-style-type: none"> ♦ <code>filr.token.expiration.interval=900</code> ♦ <code>filr.token.refresh.window=300</code> <p>The <code>filr.token.expiration.interval</code> is the session expiry timeout and value is given in seconds. The value recommended is 900 (15 minutes - (15 X 60)).</p> <p>The <code>filr.token.refresh.window</code> is for token Refresh and value is specified in seconds. After this period of time, a new token is issued and it extends the session. The refresh timeout recommended is 300 (5 minutes - (5 X 60)).</p>
♦ Forward Proxy Host Name	No longer used.
♦ Forward Proxy Port	No longer used.
♦ Enable TLS v1.2 Protocol ONLY	♦ Restricts the Filr clients (Desktop, Mobile, Web) to use only TLS 1.2 protocol for communicating with the Filr server. This option is disabled by default. WARNING: To allow Filr desktop clients to continue working seamlessly, you MUST ensure that the desktop clients are updated to the latest version before you enable this option.
OK button	♦ Click this to save your changes, then click Reconfigure Filr Server . This stops and restarts your Filr server. Because this results in server downtime, you should restart the server during off-peak hours. Current user sessions are not affected. To see changes, users must log in to a new session.
Cancel button	♦ Click this to cancel the changes you have made.

Port Numbers

Table 13-3 lists the ports that you need to take into consideration when setting up Filr. Figure 13-1 is a graphical representation of how some of the ports are used in a Filr deployment.

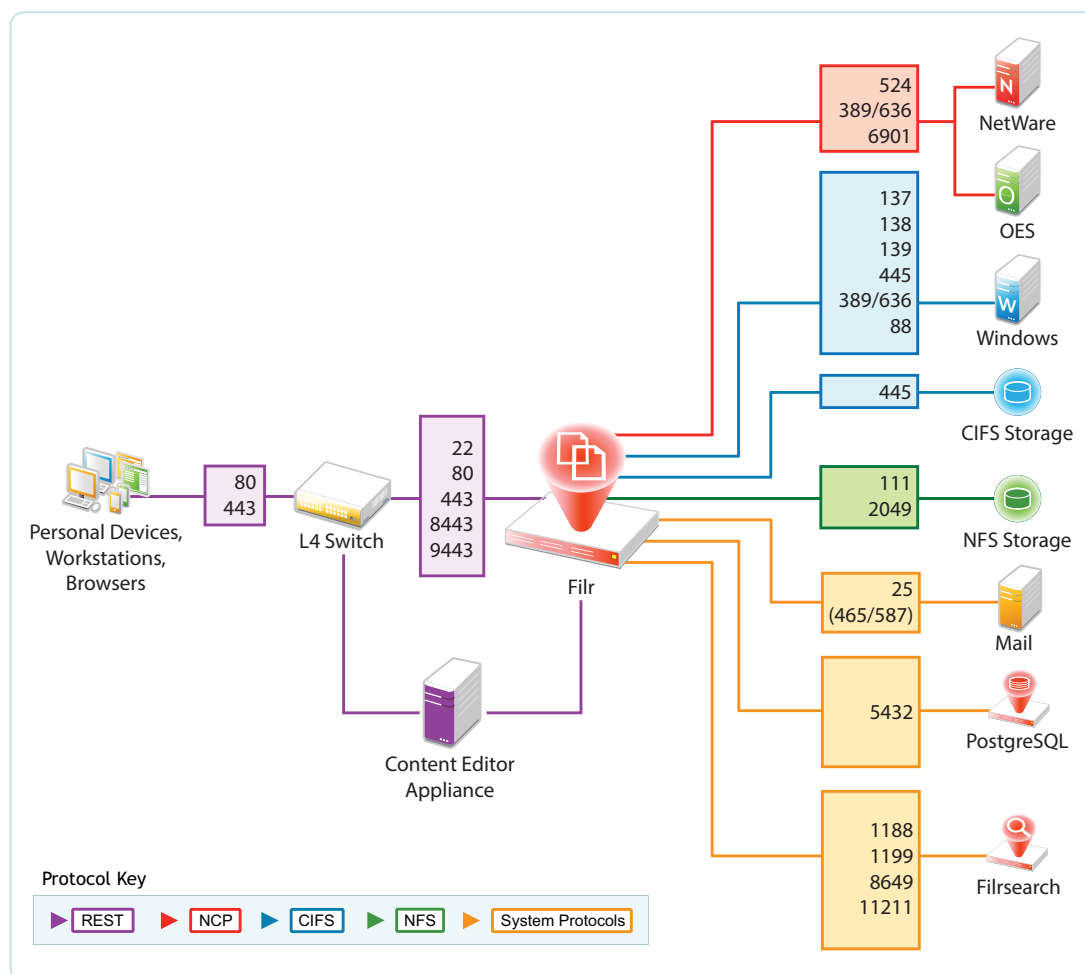
As a best practice, do not change any port numbers from the default ports.

Table 13-3 *Filr Port Numbers*

Port Numbers	Description
80, 443	Standard Web server ports
8080, 8443	Default Tomcat ports for the Filr appliance When you install Filr, Tomcat is installed along with the Filr software. Filr uses Tomcat as a stand-alone web server for delivering data to Filr users in their web browsers. For more information about Tomcat, see the Apache Tomcat Web site (http://tomcat.apache.org) .
9090, 9443	Jetty port for the appliance (Administrator Interface)
9080	Apache/HTTPD port
8005	Default shutdown port For an explanation of the shutdown port, see Tomcat - Shutdown Port (http://www.wellho.net/mouth/837_Tomcat-Shutdown-port.html) .
8009	Default AJP port For an explanation of the Apache JServ Protocol port, see The AJP Connector (http://tomcat.apache.org/tomcat-6.0-doc/config/ajp.html) .
22	SSH port for the appliance
111	rpcbind utility
1099	Java RMI port
4330	FAMT port
7380, 7443	Ganglia RRD-REST ports
8380, 8381	Default Jetty ports
8642, 8649, 8650, 8651, 8652	Ganglia web interface port
1199	Lucene RMI registry port
1188	Lucene server port
5432	PostgreSQL outbound port
3306	MySQL outbound port

Port Numbers	Description
1433	Microsoft SQL server port
25, 465	SMTP and SMTPS outbound ports
6901	OES DFS JetStream port
524/tcp	Access OES server over NCP
137/tcp, 137/udp, 138/udp, 139/tcp, 445/tcp	Access servers over CIFS
88	Kerberos port
11211	Used for memcached caching in an appliance cluster
636	Secure LDAP port
389	Non-secure LDAP port

Figure 13-1 Filr Port Usage



14 Notifications (Email)

Filr can send notifications through email about what is happening on the system. For an overview of Filr's notification services, see [“Filr Email Notifications”](#) in *Filr: Understanding How Filr Works*

To configure Filr's notification services, see the following sections:

- ♦ [“Configuring an Email Service for Filr to Use”](#) on page 89
- ♦ [“Enabling Notifications”](#) on page 91

Configuring an Email Service for Filr to Use

Path: [Port 9443 Appliance Console Configuration icon](#) > **Outbound E-Mail**

TIP

- ♦ If you make changes in this dialog, you must select **Reconfigure Filr Server** for them to take effect.

Because reconfiguring Filr restarts the Filr service, you should only change these settings during off-peak hours.

Table 14-1 *Outbound Email dialog*

Field, Option, or Button	Notes
Outbound Email dialog	
♦ Use Local Postfix Mail Server	By default, Filr is configured with an active Postfix mail server system. <ul style="list-style-type: none">♦ To use another mail system (such as GroupWise), deselect this option, then specify the appropriate information for the system that Filr will use instead.
♦ Protocol:	<ul style="list-style-type: none">♦ Specify whether the email system that Filr will leverage uses SMTP or SMTPS (secure SMTP). <p>For GroupWise, check how the Internet Agent is configured.</p> <ul style="list-style-type: none">♦ If the email system requires SMTPS, see “Email Transfer Security” in the <i>Filr 4.2: Maintenance Best Practices Guide</i>.
♦ Host:	<ul style="list-style-type: none">♦ Specify the host name of the mail server that Filr will leverage. <p>If you are using GroupWise, this is the host name of a server where the Internet Agent is running.</p>

Field, Option, or Button	Notes
♦ Port:	<p>♦ Specify the port through which Filr can connect to the SMTP mail server.</p> <p>GroupWise always uses port 25, even when SSL is enabled.</p> <p>Some mail servers require port 465 or 587 for SMTPS connections.</p>
♦ Time zone:	<p>♦ You can change the time zone if you want Filr to use an email time stamp that is different from the time zone where the server is located.</p> <p>The time zone list is grouped first by continent or region, optionally by country or state, and lastly by city.</p>
♦ User Name:	<p>♦ Specify the email address that Filr will use when sending emails.</p> <p>If the email server requires authentication, Filr sends this username.</p> <p>Many SMTP mail hosts require a valid email address before they establish the SMTP connection.</p> <p>Although some email systems can construct a valid email address if you specify only a valid user name, you should provide a valid email address to ensure a successful connection.</p> <p>Email notifications from Filr will show this email address in the From field.</p>
♦ Password:	<p>♦ If the email server requires passwords, specify the password for the user name.</p>
♦ Authentication Required	<p>♦ If the email server Filr is leveraging requires authentication, select this option.</p> <p>GroupWise The GroupWise Internet Agent does not require authentication for inbound messages. However, the /forceinboundauth startup switch in <code>gwia.cfg</code> will cause the Internet Agent to refuse SMTP connections unless a valid email user name and password are provided.</p> <p>The Internet Agent can accept just the user name or the full email address.</p> <p>Exchange If you set up the outbound email server to require authentication (by selecting the option Authentication Required), Exchange must be configured to allow the From address to be different from the user who is configured for Exchange authentication. The Exchange permission that you need to add is <code>ms-Exch-SMTP-Accept-Any-Sender</code>.</p> <p>This is needed because Exchange, by default, requires that the From address of outbound emails match the exchange user who is configured for authentication, and many Filr emails place the email address of the user performing an action in the From field.</p>
♦ Allow sending e-mail to all users	<p>♦ If you select this option, users can send email to the All Users group.</p> <p>This is disabled by default because of the potential for users to send large numbers of emails.</p>
♦ Force HTTPS links	<p>♦ Select this if all links in Filr-generated email messages should be HTTPS instead of HTTP.</p> <p>Otherwise, Filr uses its connection (HTTP or HTTPS) with the emailing user as the link protocol.</p>

Field, Option, or Button	Notes
♦ Enable STARTTLS	♦ Select this option if the email service that Filr is leveraging requires TLS over SMTP for secure email.
♦ From e-mail address override:	♦ If you don't want the User Name email address used in the From field in Filr messages, specify a different address here.
♦ Use from e-mail address override for all outbound e-mail	♦ Select this option to have Filr always use the From email address override email address in system-generated emails (summarized in “Enabling Notifications” on page 91). If this option is not selected, the From email address override field is used only in digest subscription emails.
♦ Connection Timeout:	♦ Specify the amount of time for Filr to wait before timing out on a connection request to the email host.
♦ Test Connection	♦ Click this to test your Outbound E-Mail configuration.

Enabling Notifications

Path: [Port 8443 Filr Admin Console](#) > **System** > **Email**

By default, Filr users can have the Filr system send email notifications when they create folders, add files, share files and folders, and so on.

Table 14-2 *Using the Email dialog*

Field, Option, or Button	Notes
Email dialog	
♦ Enable Outgoing Email	♦ Use this option to control whether the Filr system generates email notifications. If you de-select this option, no notifications are sent. This option has no effect on the ability for Filr users to email each other.
♦ Default Digest Schedule	♦ Use this section to schedule how often Filr sends activity digests to subscribers.

Field, Option, or Button	Notes
<ul style="list-style-type: none"> ♦ Outgoing Email Quotas 	<ul style="list-style-type: none"> ♦ When users subscribe themselves or others to receive email notifications, there is an option to have the email include changed or new files as attachments. <p>Use the options in this section to control the size of email attachments, as follows:</p> <ul style="list-style-type: none"> ♦ To preserve the default of no size restrictions, leave the fields blank. ♦ To limit attachment sizes, specify the maximum amounts for either or both fields. ♦ To prevent any attachments from being sent, specify 0 (zero) in each field.

15 Performance Tuning

- ♦ [“Changing Configuration Settings for Requests and Connections” on page 93](#)
- ♦ [“Changing JVM Configuration Settings” on page 94](#)

See also [Tuning Filr 3 for Performance](#).

Changing Configuration Settings for Requests and Connections

Configure the number of client requests and database connections that Filr supports.

Path: [Port 9443 Appliance Console](#) > **Configuration** > **Requests and Connections**

Table 15-1 *Using the Requests and Connections dialog*

Field, Option, or Button	Information and/or Action
Requests and Connections	<ul style="list-style-type: none">♦ Max Threads: The maximum number of simultaneous client request threads that Filr will support. Default: 250♦ Max Active: The maximum number of database connections that can be allocated simultaneously from this pool. Default: 300♦ Max Idle: The maximum number of database connections that can be simultaneously idle in this pool. Default: 300♦ Scheduler Threads: The size of the thread pool used for background execution of scheduled tasks. Default: 20♦ Max REST Requests (upload/download): The maximum number of concurrent desktop and mobile, upload and download requests that Filr will handle simultaneously. Default: 150 Ensures that Filr does not exceed capacity. Excess requests are cached so that Filr can respond when it has bandwidth.
OK button	<ul style="list-style-type: none">♦ After clicking this, you must click Reconfigure Filr Server for the changes to take effect.

TIP: Extremely large Filr sites requesting numerous client requests and database connections might see improved performance by increasing these settings.

Changing JVM Configuration Settings

Path: [Port 9443 Appliance Console](#)[Configuration icon](#) > [JVM Settings](#)

Table 15-2 Using the JVM Settings dialog

Field, Option, or Button	Information and/or Action
JVM Settings	<p>Best practice recommendation: Set both sizes to 66% of total RAM (see “Appliance Memory and CPU” in the Filr: Installation, Deployment, and Upgrade Guide).</p> <p>Although Filr can begin with the minimum and adjust up to the maximum as needed, the adjustment process is resource intensive and degrades system performance.</p> <p>IMPORTANT: Values must end with <code>g</code> or <code>m</code> and cannot contain fractional values. For example, to set the JVM min heap size to 1.5 GB, specify <code>1536m</code>.</p> <ul style="list-style-type: none">♦ JVM Min Heap Size: Increase or decrease as needed. Default: 9g♦ JVM Max Heap Size: Increase or decrease as needed. Default: 9g♦ Java Home: Informational only; cannot be changed.♦ Allow generation of a system dump on a user signal: Causes generation of a system dump in addition to a heap dump and java core dump at the time a dump is triggered on a user signal. This can be useful when troubleshooting issues with your Filr system. However, a system dump takes more time and the files consume more disk space than a heap dump or java core dump.
OK button	<ul style="list-style-type: none">♦ After clicking this, you must click Reconfigure Filr Server for the changes to take effect.

16 Personal Storage and Home Folders

- ♦ “Enabling Personal Storage for Users and Groups” on page 95
- ♦ “Managing and Restricting Filr-Based Storage” on page 95

Enabling Personal Storage for Users and Groups

Path: Port 8443 Filr Admin Console Management > Personal Storage > Allow LDAP Users to Have Personal Storage Area

Table 16-1 Using the Personal Storage (enable) dialog

Field, Option, or Button	Information and/or Action
Personal Storage dialog	Personal Storage (Enabling Personal Storage)
♦ Allow LDAP users to have personal storage area	<ul style="list-style-type: none">♦ Select or deselect this, depending on whether you want all users whose accounts are synchronized via LDAP to have access to personal storage in the My Files area. <p>To learn more about personal storage, see My Files (Personal Storage) in the Filr: Understanding How Filr Works.</p> <p>IMPORTANT: This lets you enable personal storage for all users. Unlike some other configuration options, it is not required for personal storage to be available. Personal storage can also be enabled or disabled on a user or group basis irrespective of this setting.</p> <ul style="list-style-type: none">♦ Individual Users: To enable or disable personal storage for individual users, see Table 28-1, “Using the Users dialog,” on page 143.♦ Groups of Users: To enable or disable personal storage for groups of users, see Table 28-3, “Using the Groups dialog,” on page 147.

Managing and Restricting Filr-Based Storage

Disk space usage almost always increases over time. You can limit on the amount of data that can be uploaded to Filr’s shared storage disk at the system level or for individual users and groups.

Only files count toward the data quota. Empty folders don’t count. Files in Net Folders don’t count.

You can limit the amount of disk space for individual users and groups as well as for individual folders.

Path: Port 8443 Filr Admin Console > Management > Personal Storage

IMPORTANT: Data quotas at all levels are strictly enforced. If uploading a file would cause a user to exceed the assigned quota, Filr rejects the upload attempt and the attempt is aborted. This is also true with data quotas that are set on folders.

When a file is added to a shared folder, the size of the file is attributed to the quota of the user who uploaded the file.

Table 16-2 *Using the Personal Storage (data quota) dialog*

Field, Option, or Button	Information and/or Action
Enable User Data Quotas section	Personal Storage (Enable User Data Quotas section)
<ul style="list-style-type: none"> ◆ Enable User Data Quotas 	<p>NOTE: Data quotas only apply to personal storage.</p> <p>Enabling Data Quota Enforcement</p> <ul style="list-style-type: none"> ◆ Select this to enable <ul style="list-style-type: none"> ◆ Enforcement of the default data quota for all unlisted users and groups <p>And</p> ◆ Enforcement of the data quotas shown for the listed users and groups <ul style="list-style-type: none"> ◆ Specify a high-water mark for both the default data quota and the quotas set for users and groups. <p>Disabling Data Quota Enforcement</p> <ul style="list-style-type: none"> ◆ Deselect this to disable all data quota enforcement.
<ul style="list-style-type: none"> ◆ Default User Data Quota Size 	<ul style="list-style-type: none"> ◆ This applies to users who do not have another data quota (user or group) that applies to them. <p>Default is 100 MB.</p>
<ul style="list-style-type: none"> ◆ Default High-Water Mark 	<ul style="list-style-type: none"> ◆ When a user exceeds the data quota high-water mark (the default is 90% of the applicable data quota), a warning message displays on the user's profile page informing the user that he or she is approaching the data quota. Filr displays how many kilobytes of disk space are still available.
<ul style="list-style-type: none"> ◆ Add a Group button 	<p>IMPORTANT: Group quotas override default quota settings. If users belong to more than one group, they are assigned the highest quota to which they are entitled through group membership.</p> <ol style="list-style-type: none"> 1. Click this to add a group of users. 2. 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. 3. In the Quota field, specify the disk space limit for the group. 4. Click OK, then click Apply > Close to save the group data quota settings.

Field, Option, or Button	Information and/or Action
♦ Add a User button	<p>IMPORTANT: User quotas override default quota settings and the settings on any groups to which users belong.</p> <ol style="list-style-type: none"> 1. Click this to add an individual user quota. 2. 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. 3. In the Quota field, specify the disk space limit for the user. 4. Click OK, then click Apply > Close to save the user data quota settings.

17 Product Improvement

The first time you log in to Filr, after changing the admin user's password, a dialog displays that explains that the purpose of the Filr data collection system is to help improve the Filr product.

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

For additional information, see “[Helping Micro Focus Improve Filr](#)” in the *Filr 4.2: Maintenance Best Practices Guide*.

IMPORTANT: Micro Focus collects nothing that identifies your organization, your data, or your users.

Path: [Port 8443 Filr Admin Console](#) > [Management](#) > [Product Improvement](#)

Table 17-1 Using the Product Improvement dialog

Field, Option, or Button	Information and/or Action
<ul style="list-style-type: none">♦ Collect and send the product name and version, and the number of LDAP users.	<ul style="list-style-type: none">♦ This option causes the Filr system to send Micro Focus information about the product version and build, license type, and number of users.
<ul style="list-style-type: none">♦ Also collect and send information about the deployment size and configuration, the number of files and folders, and so on.	<ul style="list-style-type: none">♦ This option causes the Filr system to send additional information about the installation, most of which is self-explanatory.<ul style="list-style-type: none">♦ The user information doesn't include the LDAP user count because that is already available under the Tier1.♦ The user count numbers do not include system user accounts, such as <code>admin</code>, <code>_filesyncagent</code>, and so on.♦ The group count numbers do not include system groups, such as <code>allusers</code>, <code>allexusers</code>, and so on.♦ <code>workspaceCount</code> does not include system workspaces, such as the <code>/Home</code> workspace and so on.♦ The numbers in <code>fileCounts</code> and <code>folderCounts</code> in the <code>netFolder</code> section correspond to each other by position.♦ The mobile device type is derived from the value of the description field associated with the device information captured in the system. Any descriptions that don't match one of the pre-defined keywords are included as <code>other</code>.
<ul style="list-style-type: none">♦ View the information collected.	<ul style="list-style-type: none">♦ After the system has been running 24 hours, this link displays so that you can download and review the <code>.json</code> file created by the collection process. This is the file that is sent to Micro Focus via FTP.

18 Managing Uploading of Files

The file upload size limit conserves disk space on your Micro Focus Filr site because it prevents users from uploading large files to the Filr site. The default size limit for uploading files into your Filr site is 2 GB. You can also allow or block the types of files that users can upload.

Path: [Port 8443 Filr Admin Console Management > File Upload](#)

Table 18-1 Using the Filr Upload dialog

Field, Option, or Button	Information and/or Action
File Upload Limits tab	Use the options under this tab to limit the size of the file that users can upload.
Default File Upload Size Limit	<ul style="list-style-type: none">◆ Unlike data quotas, there is no option to enable or disable file upload size checks.◆ The default file upload size limit is 2 GB, but you can modify this if needed.◆ You can also add different upload limits for individual users and groups as explained below.
◆ Add a Group button	<p>IMPORTANT: Group upload limits override the default limit. If users belong to more than one group, they are assigned the highest upload limit to which they are entitled through group membership.</p> <ol style="list-style-type: none">1. Click this to add a group of users.2. In the Group field, start typing the name of the group for which you want to set an upload limit, 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 upload limit.3. In the File Size Limit field, specify the size limit for the group.4. Click OK, then click Apply > Close to save the group file size limit.
◆ Add a User button	<p>IMPORTANT: User upload limits override default upload limits and the limits set for any groups to which users belong.</p> <ol style="list-style-type: none">1. Click this to add an individual user upload limit.2. In the User field, start typing the name of the user for which you want to set an upload limit, 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 upload limit.3. In the File Size Limit field, specify the file size limit for the user.4. Click OK, then click Apply > Close to save the user file size limit.

Field, Option, or Button	Information and/or Action
File Type Blocking tab	<p>IMPORTANT: This functionality is only available when an Advanced-Edition license is installed on the Filr appliances.</p> <p>Use the options under this tab to allow or block the types of files that users can upload.</p>
<ul style="list-style-type: none"> ◆ No restrictions 	<ul style="list-style-type: none"> ◆ Select this to allow users to upload files of all types. This is selected by default.
<ul style="list-style-type: none"> ◆ Whitelist - Allow uploading of only the listed file types 	<ul style="list-style-type: none"> ◆ If you select this: <ul style="list-style-type: none"> ◆ Users can only upload files of the type listed in the Whitelist. ◆ Users cannot upload a file for which Filr cannot detect the file type. ◆ Users can upload archive and compressed files of the type listed in the Whitelist irrespective of whether the type of the files contained within the archive and compressed file is listed in Whitelist or not. The supported archive and compressed files include 7z, ar, arj, cpio, dump, tar and zip. <p>For example: Users can upload a ZIP file containing an RTF file, even if the Whitelist includes ZIP but not RTF.</p> ◆ Whitelists are empty by default. ◆ You can add file types as needed: <ul style="list-style-type: none"> ◆ The Add dialog provides some examples of the supported file types based on the category of files such as Document and Media. You can choose to add other file types. ◆ You can also specify file types and add them to the list. ◆ You can remove file types as needed.
<ul style="list-style-type: none"> ◆ Blacklist - Block uploading of the listed file types 	<ul style="list-style-type: none"> ◆ If you select this <ul style="list-style-type: none"> ◆ Users can upload files of the type that is not listed in the Blacklist. ◆ Users can upload files of any type for which Filr cannot detect the file type. ◆ Users cannot upload archive and compressed files that are not blacklisted if the first-level folder within the archive and compressed file contains at least one blacklisted file. The supported archive and compressed files include 7z, ar, arj, cpio, dump, tar and zip. <p>For example: If the Black list includes PDF but not ZIP, users cannot upload a ZIP file that contains a PDF file in the first-level folder.</p> ◆ Blacklists are empty by default. ◆ You can add file types as needed. <ul style="list-style-type: none"> ◆ The Add dialog provides some examples of the supported file types based on the category of files such as Document and Media. You can choose to add other file types. ◆ You can also specify file types and add them to the list. ◆ To remove file types, select the file types you want to remove and click Delete.
Apply button	<ul style="list-style-type: none"> ◆ Click this to save your changes.

Field, Option, or Button	Information and/or Action
Close button	♦ Click this to return to the previous window.

19 Search and Lucene Indexing

Indexing is key to all access within Filr, including files and folders, searching on content, and even users and groups.

For more information, see “[Filr Search Appliance—Accessibility, and Searchability](#)” in *Filr: Understanding How Filr Works*

This section covers the following:

- ♦ “[Managing Filrsearch Configuration Settings](#)” on page 105
- ♦ “[Managing the Lucene Index](#)” on page 107
- ♦ “[Managing Search Nodes](#)” on page 108
- ♦ “[Memcached \(Search Index Appliance Only\)](#)” on page 109

Managing Filrsearch Configuration Settings

For more information, see “[Filr Search Appliance—Accessibility, and Searchability](#)” in *Filr: Understanding How Filr Works*

Path: [Port 9443 Filr Appliance Console](#) > [Configuration Icon](#) > [Search Appliance](#)

Table 19-1 *Using the Search Appliance dialog*

Field, Option, or Button	Information and/or Action
Configuration Type:	The options that follow depend on the configuration type selected, as shown below.
♦ Local	<ul style="list-style-type: none">♦ This is the default configuration type for a small Filr deployment, wherein the Lucene search index, the PostgreSQL database, and the Filr software are running on the same virtual machine.<ul style="list-style-type: none">♦ Host Name: local host indicates that the indexing process is running on the same appliance and the Filr process.♦ RMI Port: 1199 is the port used and cannot be changed.

Field, Option, or Button	Information and/or Action
♦ Server	<p>♦ This option is for when only one Lucene search index is running as a stand-alone appliance.</p> <p>This is not a best practice configuration.</p> <ul style="list-style-type: none"> ♦ Host Name: The DNS host name of the stand-alone search appliance. This is set at install time. ♦ RMI Port: 1199 is the default and Micro Focus does not recommend changing this. ♦ Lucene User Name: The default name is <code>lucene_service</code> but you can type a different name as long as you use the same name throughout your deployment. ♦ Lucene User Password: The password for the Lucene user.
♦ High Availability	<p>♦ Select this when two Lucene search indexes are running as stand-alone appliances.</p> <p>This is the best practice configuration.</p> <ul style="list-style-type: none"> ♦ Lucene User Name: The default name is <code>lucene_service</code> but you can type a different name in the User Name field as long as you use the same name throughout your deployment. ♦ Lucene User Password: The password for the Lucene user. <p>NOTE: The following options apply to only High Availability configurations.</p>
♦ Add button	♦ Click this to open the New Search Node dialog.
♦ Remove button	<p>♦ Select a listed Filrsearch appliance by clicking in the white space of its row.</p> <p>Then click Remove to remove the appliance.</p>
New Search Node	
♦ Name	<p>♦ Specify a name for the Lucene search index appliance you are adding.</p> <p>You must specify the same name on each Filr appliance in the cluster. For example, if from one Filr appliance you specify <code>filrsearch_index1</code> for this appliance, then you must specify <code>filrsearch1_index1</code> on each of the Filr appliances in the cluster.</p>
♦ Description	♦ Specify a short description for the Lucene appliance.
♦ Host Name	♦ Specify the DNS host name or IP address of the Filrsearch appliance you are adding.
♦ RMI Port	<p>♦ 1199 (informational only).</p> <p>(See Remote Method Invocation (http://java.sun.com/javase/technologies/core/basic/rmi/index.jsp).)</p>
Filrsearch List	
♦ Name	♦ You can click this to open the New Search Node dialog.
♦ Host Name	♦ 1199 (informational only).

Field, Option, or Button	Information and/or Action
♦ RMI Port	♦ 1199 (informational only).
OK button	♦ To save your changes, click this, then click Reconfigure Filr Server . This stops and restarts your Filr server. Because this results in server downtime, you should restart the server at off-peak hours.
Cancel button	♦ Click this to cancel the changes you have made.

Managing 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.

For more information, see “[Filr Search Appliance—Accessibility, and Searchability](#)” in *Filr: Understanding How Filr Works*

Path: [Port 8443 Filr Admin Console](#) > [Search Index](#) > [Index](#)

Table 19-2 Using the Search Index page

Field, Option, or Button	Information and/or Action
Manage Search Index tab	Use the options under this tab if users report that they can’t find information or people that they know should be available in Filr. Chances are good that the index has become damaged or out-of-date for some reason. This is not a good option to correct slow performance. Re-indexing takes much longer and requires more resources than optimization (available in the Optimize Search Index tab). For more information, see “ Rebuilding the Lucene Index ” in the <i>Filr 4.2: Maintenance Best Practices Guide</i> .
♦ Re-Index Everything	♦ Use this option to rebuild all of the indexes for your entire site. ♦ Keep in mind that no one will be able to access any of the files, folders, users, groups, etc. until a corresponding synchronization process has taken place and the metadata index for the items is re-created. ♦ Depending on the size of your Filr site, this can be a very time-consuming process.
♦ Select the Places to Be Re-Indexed:	♦ If you know that there are problems with specific portion of the site, you can choose to reindex only those portions.
♦ Select the Nodes to Apply Re-Indexing to:	♦ You can choose which of the appliances to apply the reindexing to. ♦ Micro Focus recommends setting one of the nodes to write-only and reindexing only the other node. (See “ Managing Search Nodes ” on page 108 .)

Field, Option, or Button	Information and/or Action
Optimize Search Index tab	<p>Use the options under this tab if you notice that search performance in Micro Focus Filr is becoming slower over time.</p> <p>As a rule of thumb, you should run the optimization once a week during off hours or on weekends when the Filr system is not being heavily used.</p> <p>IMPORTANT: For optimization to run, there must be at least 51% free disk space on the Lucene search index appliance.</p> <p>Optimizing the Lucene index does not repair a damaged or out-of-date index. You must use the Manage Search Index tab in those cases.</p>
<ul style="list-style-type: none"> ♦ Optimizing the Search Index <ul style="list-style-type: none"> ♦ Run Immediately ♦ Run at Scheduled Time 	<ul style="list-style-type: none"> ♦ You can either choose to run the optimization immediately, or schedule it during off hours or on weekends as the options indicate.
<ul style="list-style-type: none"> ♦ Exclude File Types 	<p>Use the options under this tab to specify the type (extension) of files that should not be indexed.</p>

Managing Search Nodes

This dialog lets you control access to the Filrsearch appliances (search nodes) and is integral to certain index maintenance operations.

For example, 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.

For more information, see “[Search Index Maintenance](#)” in *Filr 4.2: Maintenance Best Practices Guide*

Path: [Port 8443 Filr Admin Console](#) > [Search Index](#) > [Nodes](#)

Table 19-3 Using the Search Nodes dialog

Field, Option, or Button	Information and/or Action
<ul style="list-style-type: none"> ♦ Node information <ul style="list-style-type: none"> ♦ <i>IP_address</i> ♦ Host: ♦ RMI Port: 	<ul style="list-style-type: none"> ♦ This is informational only.

Field, Option, or Button	Information and/or Action
<ul style="list-style-type: none"> ♦ User Mode Access: 	<ul style="list-style-type: none"> ♦ Read and Write: This is the normal operating mode and allows the Filr system to both retrieve information from the index and modify the index. ♦ Write Only: Select this if you are performing a re-index on the search index node. ♦ No Access: Selecting this option ensures that no data is written to the index while maintenance is being performed, such as upgrading the appliances or adding more disk space or memory
<ul style="list-style-type: none"> ♦ Enable Deferred Update Log 	<ul style="list-style-type: none"> ♦ Do not deselect this unless instructed to do so by a support technician as part of resolving an incident report.

Memcached (Search Index Appliance Only)

Memcached is a high-performance, distributed memory object caching system used by a number of large Internet sites such as Wikipedia, Flickr, Twitter, and Youtube, as well as enterprise systems. Memcached is not designed for authentication and is protected only by firewalls and similar mechanisms.

IMPORTANT: To secure Memcached, it is strongly recommended to deploy the Search appliance behind the firewall.

For more information, see [“Securing Memcached” on page 113](#).

Advantages for Using Memcached

Memcached offers the following advantages over other caching systems:

- ♦ Better utilization of memory resources from the server farm.

No replication (and therefore no overhead involved in replication). This results in a reduction of 60 or more threads per node in a two-node cluster.

The number of servers and the size of data scale together.

- ♦ Scales out much better than replication-based cluster cache.

Managing Memcached

Path: [Port 9443 Appliance Console](#) > [Memcached icon](#)

Table 19-4 *Managing Memcached*

Field, Option, or Button	Information and/or Action
♦ Listen Interface:	♦ The URL that Memcached listens on.
♦ Number of Threads:	♦ The number of threads to use when processing incoming requests.
♦ Max Memory:	♦ Max memory that can be used by Memcached.
♦ Max Simultaneous Connections:	♦ Specify the number of network connections that can be handled by memcached simultaneously.

20 Security

Enterprise data is a critical resource that must be protected from unauthorized access, eavesdropping, corruption, unintended modification, or Trojan horses.

Generating, storing, and protecting enterprise data requires significant investments in time, money, and other resources.

Filr is designed to enhance an organization's ability to use and leverage its data. It has been carefully engineered to guard against exposing data to additional vulnerabilities.

- ♦ [“Certificates” on page 111](#)
- ♦ [“Firewall Configuration” on page 112](#)
- ♦ [“Password Security \(Local and External Users\)” on page 112](#)
- ♦ [“Securing Memcached” on page 113](#)
- ♦ [“User Visibility” on page 113](#)
- ♦ [“Viewing, Wiping, and Disconnecting Registered Clients” on page 114](#)
- ♦ [“WebDAV Authentication Configuration Settings” on page 114](#)

Certificates

For certificate-maintenance procedures associated with this dialog, see [Certificate Maintenance](#) in the [Filr 4.2: Maintenance Best Practices Guide](#)

Path: [Port 9443 Appliance Console](#) > **Digital Certificates icon**

Table 20-1 *Using the Digital Certificates Page*

Field, Option, or Button		Information and/or Action
Certificates in the Selected Key Store		
♦ Key Store drop-down	♦	Use this drop-down list to filter whether JVM or Web Application Certificates are listed.
♦ File drop-down	♦	This drop-down list lets you create a new key pair, import a trusted certificate or key pair, export a certificate you have selected in the list, or generate a CSR for a web application you have selected.
♦ Edit drop-down	♦	This exposes the option to delete a certificate you have selected.
♦ View Info	♦	This lets you view the information for a selected certificate
♦ Reload	♦	This lets you reload a selected certificate.

Firewall Configuration

Path: [Port 9443 Appliance Console](#) > Firewall icon

Table 20-2 Using the Firewall Details page

Field, Option, or Button	Information and/or Action
Firewall Details	<p>This page is only informational, not editable.</p> <p>It lists the port numbers that Filr expects to use on your network and the current status of each port.</p>

Password Security (Local and External Users)

You can require that user passwords to the Filr site meet certain criteria by enabling password complexity checking. Only locally created users and external users are affected by this setting; users whose accounts are synchronized to Filr via LDAP are not affected.

Users' existing passwords are not forced to comply with the password policy; only when a user changes his or her password is the password policy put into effect.

Path [Port 8443 Filr Admin Console](#) > System > Password Policy

Table 20-3 Using the Configure Password Policy dialog

Field, Option, or Button	Information and/or Action
Password complexity changing requires that passwords:	
<ul style="list-style-type: none">◆ Enable Password Complexity Checking for Local and External Users	<ul style="list-style-type: none">◆ When this is enabled, Filr requires that passwords:<ul style="list-style-type: none">◆ Are at least 8 characters in length◆ Do not contain the user's first name, last name, or user ID (these restrictions are not case-sensitive)◆ Contain at least 3 of the following:<ul style="list-style-type: none">◆ A lower-case character◆ An upper-case character◆ A number◆ One of the following symbols: ~ @ # \$ % ^ & * () - + { } [] \ ? / , . < >

Securing Memcached

Memcached is a high-performance, distributed memory object caching system used by a number of large Internet sites such as Wikipedia, Flickr, Twitter, and Youtube, as well as enterprise systems. Memcached is not designed for authentication and is protected only by firewalls and similar mechanisms.

The Search appliance runs the Memcached service to enable clustering. To secure Memcached, it is strongly recommended to deploy the Search appliance behind the firewall. Memcached service uses port 11211 and the firewall must allow this port for communication. For more information, see [Ports Used in Filr Deployments](#) in the [Filr: Understanding How Filr Works](#).

For more information about Memcached, see [Memcached \(http://memcached.org/\)](http://memcached.org/).

User Visibility

By default, each Filr user can see all other Filr users on the Filr site.

In a large organization it can be daunting for users to sort through a long list of people they don't work with to find those in their groups or on their teams.

Filr lets you restrict the users that appear in sharing dialogs and so on, to only those within groups to which a user belongs.

For a detailed explanation of Filr's User Visibility feature, see "[Key Points About User Visibility in Filr](#)" in [Filr: Understanding How Filr Works](#).

Path: [Port 8443 Filr Admin Console: Management](#) > [Limit User Visibility](#)

Table 20-4 Using the Limit User Visibility dialog

Field, Option, or Button	Information and/or Action
♦ Add Limitation	♦ Click this, begin typing, select a listed user or group to limit them to seeing only other members of the groups they belong to.
♦ Add Override	♦ Click this, begin typing, select a listed user or group to enable them to see everyone.
♦ Remove Visibility Settings	♦ Select a user or group and click this to remove them from the list.
♦ Filter List	♦ Type a string within the user or group names to filter the displayed list to only those containing the string.
♦ Gear icon	♦ Select this to change the column sizes.
♦ Limited Visibility On	♦ Select the box next to the option to activate the visibility limitations for all listed users and groups. Or ♦ Select the users and groups you want to be affected by their limitations.

Viewing, Wiping, and Disconnecting Registered Clients

Filr lets you manage registered client devices from the Filr Administration Console.

You can remove devices from the registration list and schedule the removal (wiping) of all Filr data from the device the next time the user logs in.

For more detail, refer to the descriptions of dialog buttons, fields, and so on in [Table 20-5](#).

Path: [Port 8443 Filr Admin Console](#) > **Management** > **Registered Clients**

Table 20-5 *Using the Registered Clients dialog*

Field, Option, or Button	Information and/or Action
Registered Clients - System Wide	
♦ Delete button	♦ Click this to remove a device from the list. This doesn't affect the device, only its registration status with Filr. The device is re-registered if the user logs in again.
♦ Wipe drop-down	♦ Schedule Devices to be Wiped: If you select this, then the next time the user logs in to the device, the user password and all online and available-offline files are removed from the device, although the folder structure remains the same. The Filr application then exits, but it is not uninstalled or removed from the device. ♦ Clear Scheduled Wipe from Devices: This removes the scheduled wipe and no information is removed the next time the user logs in to the device.
♦ Device Name	♦ The name given to the device by the device owner.
♦ OS Version	♦ The operating system on the device.
♦ Client	♦ The version of the Filr application that is installed on the registered device.
♦ User	♦ The name of the Filr user who logged in from the listed device.
♦ Last Login	♦ The date and time when the device was last used to log in to the Filr system.
♦ Wipe Scheduled	♦ This indicates whether a wipe has been scheduled to occur so that all Filr data is removed from the device the next time the user logs in from it.
♦ Last Wipe	♦ The last time Filr data was wiped from the device.
♦ Filter List	♦ Filter the displayed list by typing a string found in any of the rows. For example, you could type "7" to see a list of Windows 7 registered clients.
♦ Gear icon	♦ Click this to access the Edit Column Sizes dialog.

WebDAV Authentication Configuration Settings

Path: [Port 9443 Appliance Console](#) > **Configuration icon** > **WebDAV Authentication**

Table 20-6 The WebDAV Authentication dialog

Field, Option, or Button	Information and/or Action
◆ WebDAV authentication method:	<div>◆ You should only change this if there is a specific reason for doing so.</div> <div>Basic Authentication: Encodes the user name and password with the Base64 algorithm and if used, should be combined with SSL/TLS (HTTPS). It is unsafe if transmitted over HTTP.</div> <div>Do not select Basic authentication unless there is a specific reason for doing so.</div> <div>Digest Authentication (Default): Applies MD5 cryptographic, one-way hashing with nonce values to a password before sending it over the network. This option is safer than Basic authentication when used over HTTP.</div> <div>Always select this type of authentication when client users are using Windows 7 as their operating system and Microsoft Office as their text editor.</div> <div>◆ If you change the method, click OK, then click Reconfigure Filr Server.</div>
Micro Focus Filr uses the WebDAV protocol for “Edit with Application” interaction with tools such as OpenOffice and Microsoft Office.	
IMPORTANT: Windows 7 users as the client operating system, various issues can be introduced because of WebDAV limitations in Windows 7. If your Filr users are using the Windows 7 operating system, see “ WebDAV Support ” in the Filr 4.2: Maintenance Best Practices Guide .	

21 Sharing

The following sections cover the main administrative controls for sharing in Filr.

- ♦ [“Managing Shared Items” on page 117](#)
- ♦ [“Managing Sharing, License Terms, and Comments” on page 118](#)

Managing Shared Items

Use this dialog to manage the share settings for all shared files and folders.

Path: [Port 8443 Filr Admin Console](#) > **Management** > **Shares**

Table 21-1 *Using the Shares dialog*

Field, Option, or Button	Information and/or Action
Manage Shares	
Find share items by: drop-down list	<ul style="list-style-type: none">♦ Use this to filter the list of shares by one of the options below.
♦ User	<ul style="list-style-type: none">♦ Begin typing the name of a user in the User field, then select the user name when it appears in the drop-down list. All active shares from that user are displayed in the table.
♦ File	<ul style="list-style-type: none">♦ Begin typing the name of a file in the File field, then select the file name when it appears in the drop-down list. All active shares associated with that file are displayed in the table.
♦ Folder	<ul style="list-style-type: none">♦ Begin typing the name of a folder in the Folder field, then select the folder name when it appears in the drop-down list.♦ Or click the Browse icon next to the Folder field and browse to the folder. All active shares associated with that folder are displayed in the table.
♦ Find all shares	<ul style="list-style-type: none">♦ Select this to display all active shares in the Filr system.
Shared With sub-section	<ul style="list-style-type: none">♦ This section lists all of the shared items and who has access to them.♦ You can also use the checkbox next to this label to select all of the listed shares. <p>After the shares are selected, you can modify the shared-access rights.</p>
♦ Delete button	<ul style="list-style-type: none">♦ Use this to remove any of the listed shares from the list. Only the share is removed, shared items themselves are not affected.
♦ Access Rights	<ul style="list-style-type: none">♦ After selecting a shared item, you can decrease the granted access rights or increase them within the limits available to the user who shared the item.
♦ Allow re-share with	<ul style="list-style-type: none">♦ You can adjust the re-share privileges within the limits available to the user who shared the item.

Field, Option, or Button	Information and/or Action
♦ Expires	<ul style="list-style-type: none"> ♦ The default share expiry is set to 30 days. The maximum value you can set is 9999 days. <p>You can adjust the expiration so that the share never expires, expires on a certain date, or expires after a specified number of days.</p>
♦ Note:	<ul style="list-style-type: none"> ♦ You can include a note about the changes you have made. This will then be distributed according to the option that you select for the Notify option.
♦ Notify:	<ul style="list-style-type: none"> ♦ You can choose among four notification options: <ul style="list-style-type: none"> ♦ All recipients: An email that includes your note is sent to all of those with the share. ♦ Only newly added recipients: An email that includes your note is sent to newly added recipients. ♦ New and modified recipients: An email that includes your note is sent to all newly added recipients and those whose privileges have changed. ♦ None: No email is sent.
♦ Share Access Report	<ul style="list-style-type: none"> ♦ Click Share Access Report to view the share access details of the sharee. <p>The Access report displays the following information:</p> <ul style="list-style-type: none"> ♦ User: Name of the user who has accessed the share ♦ IP Address: The IP address of the device that was used to access the share ♦ First Access Time: The date and time when the share was first accessed. No information is received when the share is accessed again. ♦ Group: If the user has shared to a group, then the name of the group is displayed that the user is part of. <p>The sharer receives an email notification with access details when the share is accessed by the sharee. A report is generated per share when the following conditions are satisfied:</p> <ul style="list-style-type: none"> ♦ Users having Filr 4.0 Advanced Edition license ♦ File or folder shared with Filr 3.4 or later
OK button	<ul style="list-style-type: none"> ♦ Click this to save your changes and send notifications as specified.
Cancel button	<ul style="list-style-type: none"> ♦ Click this to cancel the changes you have made.

Managing Sharing, License Terms, and Comments

For users to be able to share files and folders in Filr, they must be enabled directly or as a group member through this dialog.

- ♦ My Files sharing is then automatic for those listed, unless [explicitly restricted](#).
- ♦ Net Folder sharing requires [further configuration](#).

Path: [Port 8443 Filr Admin Console](#) > **System** > **Share and Comment Settings**

Table 21-2 Using the Share and Comment Settings dialog

Field, Option, or Button	Information and/or Action
Share and Comment Settings dialog	
Rights tab	For a graphical explanation of the settings in this tab, see “The Rights Tab Controls All Filr Sharing” on page 121.
<ul style="list-style-type: none"> ♦ Allow all users to share with groups that have been imported from LDAP 	<ul style="list-style-type: none"> ♦ If you select this option, groups that were imported from the LDAP directory are displayed in the Share with field when users are sharing an item. All users in the LDAP group then have access to the item that was shared.
<ul style="list-style-type: none"> ♦ User or Group: 	<p>IMPORTANT: For users or groups to share items in Filr, they must be listed here.</p> <ul style="list-style-type: none"> ♦ Begin typing a user or group name and then select it in the list. The Grant Share Rights dialog displays.
<ul style="list-style-type: none"> ♦ User/Group List <ul style="list-style-type: none"> ♦ Name ♦ Rights ♦ Type 	<ul style="list-style-type: none"> ♦ This lists the users and groups that are granted rights to share files and folders in Filr. ♦ Users that are listed individually and also as members of groups have all of the rights that are granted in their applicable listings.
Grant Share Rights dialog	
<ul style="list-style-type: none"> ♦ Re-share items 	<ul style="list-style-type: none"> ♦ When users share a file or folder, they can give the users they are sharing with the ability to re-share the file or folder. IMPORTANT: Exercise caution here because even a user's access rights to an item are removed, that does not remove the access rights of the user with whom the item was re-shared.
<ul style="list-style-type: none"> ♦ Share with internal users 	<ul style="list-style-type: none"> ♦ Lets users share items with internal users.
<ul style="list-style-type: none"> ♦ Share with “All Internal Users” group 	<ul style="list-style-type: none"> ♦ Lets users perform a mass share to all internal users by sharing with the All Internal Users group.
<ul style="list-style-type: none"> ♦ Share with External Users 	<ul style="list-style-type: none"> ♦ Lets users share items with users external to the organization through the external users’ email addresses. ♦ Email notifications include a link to the shared item. Users can then log in to the Filr site and self provision.
<ul style="list-style-type: none"> ♦ Share with the Public 	<ul style="list-style-type: none"> ♦ Lets users make items publicly available. Anyone with the URL to the Filr site can access the Public folder and see the item along with everything else in the folder. Public access requires that you enable Guest access to the Filr site. For information about how to enable Guest access to the Filr site, see “Web Browser Access—Default Settings” on page 24

Field, Option, or Button	Information and/or Action
♦ Share using File Link	<ul style="list-style-type: none"> ♦ Lets users share a link to a file in Filr. <p>Any user with the link can then access the file.</p> <p>The file is not displayed in the Public area, so users must have direct access to the link in order to access the file.</p> <p>Users can share a link of the Filr file even with email addresses that are listed in the Blacklist field.</p>
Whitelist / Blacklist tab	
Mode	
♦ No restrictions	<ul style="list-style-type: none"> ♦ Lists are ignored and users can share with any email address.
♦ Whitelist	<ul style="list-style-type: none"> ♦ Allows sharing only with email addresses and domains that have been specified in the Email addresses and Domains fields.
♦ Blacklist	<ul style="list-style-type: none"> ♦ Disallows sharing with any email addresses and domains that have been specified in the Email addresses and Domains fields. ♦ Users with Share using File Link rights can share links of Filr files even with email addresses listed in the Blacklist field.
♦ Email addresses list	<ul style="list-style-type: none"> ♦ Use the Add and Delete buttons to add and remove email addresses from the list.
♦ Domains list	<ul style="list-style-type: none"> ♦ Use the Add and Delete buttons to add and remove domains (such as yahoo.com) from the list.
♦ Delete shares that don't meet the criteria	<ul style="list-style-type: none"> ♦ Select this option to delete all existing shares in the Filr system that do not match the criteria you set. <p>For example, if you selected Blacklist and then specified yahoo.com in the Domains field, selecting this option would delete all Filr shares made to Yahoo email addresses.</p>
External Users Licensing Terms tab	
♦ Display Terms and Conditions	<ul style="list-style-type: none"> ♦ Enable this tab so that the external users who access the Filr site after receiving an email invitation accept the terms and conditions that you specify in the field provided before being granted access. <p>The text entered here must be HTML formatted in order to display correctly.</p> <p>IMPORTANT: This does not apply to Guest (Public) access.</p>
Comment Settings tab	
♦ Allow Commenting on Files	<ul style="list-style-type: none"> ♦ Disabling this option prevents all users from logging comments in Filr. ♦ You can also disable commenting for only Guest (Public) users. See “Guest access is read only” on page 25.
OK button	<ul style="list-style-type: none"> ♦ Click this to save your changes.
Cancel button	<ul style="list-style-type: none"> ♦ Click this to cancel the changes you have made.

File Request Settings
tab

◆ Allow users to request for files	◆ Allows you to request files from other users. The user to whom you send the file request receives an email with an upload request link pointing to the location where you want the file to be uploaded.
OK button	◆ Click this to save your changes.
Cancel button	◆ Click this to cancel the changes you have made.

The Rights Tab Controls All Filr Sharing

To use Filr sharing, users must listed here, either individually or as a member of a group.

1. Select this option to let Filr users share with all LDAP-imported groups.

2. Begin typing a user or group name.

3. Select a name to add it to the list.

4. Specify the maximum Filr sharing rights for the user or group.
You cannot grant rights elsewhere that aren't granted here.
For example, Black Knight will not be allowed to reshare items that have been shared with him unless that right is added here.

5. Repeat from Step 2 until all users who need to share have been granted sharing rights.

Share Settings

Rights | Whitelist / Blacklist | External Users Licensing Terms

☐ Allow all users to share with groups that have been imported from LDAP

Select a user or group to add to the list and then grant share rights.

User or Group: bl

Name	Rights	Type
blackknight	Internal / External / Share File Link	User

Grant Share Rights

Recipients will be granted share rights to:

- ☐ Re-share items
- ☒ Share with Internal users
 - ☐ Share with "All Internal Users" group
- ☒ Share with External users
- ☐ Share with the Public
- ☒ Share using File Link

22 SQL Database Connection

Filr uses the SQL database for storing file and folder, and user and group metadata. You can change any of the fields in this dialog to match corresponding changes to the database server.

Path: [Port 9443 Appliance Console](#) > [Configuration icon](#) > [Database](#)

Table 22-1 Using the Database Connection dialog

Field, Option, or Button	Information and/or Action
Database Connection dialog	
♦ Database Type:	♦ Select the appropriate option for the database server. <ul style="list-style-type: none">♦ MySQL or PostgreSQL: Select PostgreSQL♦ Microsoft SQL Server: Select MS SQL Server
♦ Host Name or IP Address:	♦ The DNS host name or IP address of your SQL server.
♦ Port:	♦ The port used for communications with Filr. The standard port for the database type is automatically selected.
♦ User Name:	♦ The user id that Filr uses to log in to the database server.
♦ User Password:	♦ The password for the User Name.
♦ Encrypt Database Communication:	♦ Select this option to encrypt data communication from the Filr server to the database server.
OK button	♦ Click this to save your changes. Then click Reconfigure Filr Server so that the changes are used by Filr.
Cancel button	♦ Click this to cancel the changes you have made.

23 Storage Management

- ♦ [“Expanding Storage” on page 125](#)

Expanding Storage

Path: [Port 9443 Appliance Console](#) > **Storage icon**

Table 23-1 *Using the Storage Expansion dialog*

Field, Option, or Button	Information and/or Action
Prerequisite	<ul style="list-style-type: none">♦ Storage expansion requires unallocated free disk space associated with the <code>/vastorage</code> and/or <code>/var</code> partitions.♦ Use the tools and processes provided by your hypervisor vendor to expand the virtual disks that contain the partitions you want to expand.♦ Restart the appliance so that the operating system can detect the disks that have been expanded.
Appliance Disks Containing Unallocated Free Space: If no disks are listed, nothing is available to be expanded.	
Expand partitions	<ul style="list-style-type: none">♦ After selecting the devices you want to expand, click this option. Appliance services are stopped, the selected partitions are expanded to the size of their respective disks, and appliance services are restarted.♦ Restart the appliance again so that the management software detects that the unallocated disk space has been used.

24 Support Files and Online Updates

- ♦ [“Managing Field Test Patches” on page 127](#)
- ♦ [“Managing Online Updates” on page 127](#)
- ♦ [“Submitting Configuration Files to Micro Focus Support” on page 129](#)

Managing Field Test Patches

You can manage field test patches for the Filr appliance directly from the appliance. You can install new patches, view currently installed patches, and uninstall patches.

Path: [Port 9443 Appliance Console](#) **Field Patch icon**

Table 24-1 *Using the Field Patch dialog*

Field, Option, or Button	Information and/or Action
Field Test Patch	
<i>Install a Downloaded Patch</i> sub-section	
♦ Path to Field Patch:	♦ Use the Browse button to navigate to a downloaded patch, then click Install to apply the patch.
<i>Manage Installed Patches</i> sub-section	
♦ Uninstall Latest Patch button	♦ Patches must be uninstalled in reverse order and only the latest patch can be uninstalled. ♦ Select the latest installed patch, then click this button and confirm that you want the patch uninstalled.
♦ Download Log File button	♦ Click this to download the log file that tracks patch installations.

Managing Online Updates

Path: [Port 9443 Appliance Console](#) > **Online Update icon**

Table 24-2 Using the Online Update dialog

Field, Option, or Button	Information and/or Action
Online Update (Automatic Update Schedule: X)	<ul style="list-style-type: none"> ◆ This is the dialog title and it also shows which Schedule option is selected (represented by X).
Register Online Update Service dialog	<ul style="list-style-type: none"> ◆ This dialog appears whenever the appliance is not registered with an update service. For example, the first time Online Update icon is clicked or when a service has been de-registered. ◆ You must register the appliance for it to receive online updates.
◆ Service Type:	<ul style="list-style-type: none"> ◆ Select the service type that the appliance will use to obtain online updates: a local Subscription Management Tool (SMT) or the Micro Focus Customer Center
◆ Local SMT	<p>This is a server from where you can download the software updates and automatically install them to update the product.</p> <ul style="list-style-type: none"> ◆ Hostname: The hostname of the server from where you want the appliance to download software updates. ◆ SSL cert URL (optional): The path to the SSL certificate for encrypting communications with the server. ◆ Namespace path (optional): To enable the client to use the staging group, specify a value. Do not specify any value if you want to use the default production repositories.
◆ Micro Focus Customer Center	<ul style="list-style-type: none"> ◆ Email: Your email address for registering the appliance to receive updates. ◆ Activation Key: This displays in your NCC Portal in the same dialog as your product license. ◆ Allow Data send: Select from the following options if you want to share information with the Micro Focus Customer Center: <ul style="list-style-type: none"> ◆ Hardware Profile: Shares the hardware information. ◆ Optional Information: Shares information such as host type, product version, release, architecture, timezone, and processor.
Update service: X	<ul style="list-style-type: none"> ◆ After you register the appliance for an update service, the service name appears in this field (represented by X).
◆ Patches drop-down	<ul style="list-style-type: none"> ◆ Needed Patches: Selecting this option lists that patches that will be installed during the next manual or automatic update. ◆ Installed Patches: Selecting this option lists all patches that have been previously installed.

Field, Option, or Button	Information and/or Action
♦ Schedule drop-down	<ul style="list-style-type: none"> ♦ Click this to set a schedule for when the appliance will download updates. ♦ If you select Manual, the appliance immediately downloads all available patches. ♦ If you select Daily, Weekly, or Monthly, you must then choose to apply either All Needed Patches or Security Patches Only. ♦ For interactive patches, you must select the Automatically agree with all license agreements and Automatically install all interactive patches options.
Update Now tab	<ul style="list-style-type: none"> ♦ This is selectable only when the Patches drop-down is set to Needed Patches. ♦ After clicking the option, you must choose to apply either All Needed Patches or Security Patches Only. ♦ For interactive patches, you must select the Automatically agree with all license agreements and Automatically install all interactive patches options.
View Info tab	<ul style="list-style-type: none"> ♦ Clicking this displays information such as a brief summary of the patch and the bug fixes in the patch.
Register tab	<ul style="list-style-type: none"> ♦ Clicking this displays the appliance's registration status, and an option to Deregister the appliance. ♦ If you deregister the appliance, the Register Online Update Service dialog reappears.
Refresh tab	<ul style="list-style-type: none"> ♦ Clicking this refreshes the status of updates on the Appliance.

Submitting Configuration Files to Micro Focus Support

Sometimes Micro Focus Support needs to review your appliance's system configuration when processing a service request. This dialog facilitates the process and saves you time.

Path: [Port 9443 Appliance Console](#) > **Support icon**

Table 24-3 Using the Support dialog

Field, Option, or Button	Information and/or Action
Support	
Automatically send the configuration to Micro Focus using FTP.	<ul style="list-style-type: none"> ♦ With this option selected, you can FTP your configuration to Micro Focus Support and include the Service Request Number if desired. ♦ The configuration is sent when you click OK and confirm your selection.
Download and save the configuration file locally, then sent it to Micro Focus manually.	<ul style="list-style-type: none"> ♦ With this option selected, the configuration is downloaded when you click OK and confirm your selection. ♦ You must then send the file to Micro Focus through email or some other arrangement.
OK or Cancel	<ul style="list-style-type: none"> ♦ Click OK to send or download the file, or click Cancel to exit.

25 Changing System Services Configurations

- ♦ “Managing System Services” on page 131
- ♦ “Shutting Down and Restarting the Micro Focus Appliance” on page 132

Managing System Services

Path: [Port 9443 Appliance Console](#) > [System Services icon](#)

Table 25-1 Using the System Services dialog

Field, Option, or Button	Information and/or Action
Available System Services: This varies by appliance type as listed below this table.	
♦ Action drop-down	♦ Use this to start , stop , or restart the selected service. Before doing any of these, make sure you understand how your action will affect the appliance.
♦ Options drop-down	♦ Use this to set the selected service to start automatically or require a manual start.
♦ Refresh List	♦ Click this if the information displayed is outdated.

Filr Appliance

- ♦ **SSH:** This is the SSH service that is running on the appliance.
- ♦ **Novell Filr:** This is the Filr service that is running on the appliance. Click **Download** to access the `appserver.log` and `catalina.out` files.
- ♦ **Jetty:** This is the Jetty service that is running on the appliance. Click **Download** to access the `jetty.stderrout.out` file.
- ♦ **Postfix:** This is the Postfix SMTP outbound mail server. This allows email to be sent from the Filr site, as described in “[Enabling Notifications](#)” on page 91. Click **Download** to access the `mail` file.
- ♦ **Novell FAMT:** This is the Micro Focus FAMT service that allows communication between Filr and the external OES, Windows, or NetWare file system. Click **Download** to access the `famtd.log` file.
- ♦ **PostgreSQL:** This is the PostgreSQL service that is running on the appliance. Click **Download** to access the `postgresql.log` file.

The PostgreSQL service runs on the Filr appliance in a small deployment, and on the PostgreSQL appliance in a large deployment.

Lucene Search Index Appliance

- ♦ **SSH:** This is the SSH service that is running on the appliance.

- ♦ **Jetty:** This is the Jetty service that is running on the appliance. Click **Download** to access the `jetty.stderrout.out` file.
- ♦ **Search:** Click **Download** to access the `indexserver.log` file
- ♦ **Memcached:** Click **Download** to access the `jetty.stderrout.out` file.

PostgreSQL Database Appliance

- ♦ **SSH:** This is the SSH service that is running on the appliance.
- ♦ **PostgreSQL:** This is the PostgreSQL service that is running on the appliance. Click **Download** to access the `postgresql.log` file.

Shutting Down and Restarting the Micro Focus Appliance

Path: [Port 9443 Appliance Console](#) > **Reboot** or > **Shutdown**

- ♦ **Reboot:** Use this if you need to restart the Micro Focus appliance after performing maintenance.
- ♦ **Shutdown:** To ensure that appliance processes are properly terminated, you should always use this when you need to shutdown a Micro Focus appliance.

Using the hypervisor's management features to power down or restart an appliance can result in system corruption.

26 Time and Locale

- ♦ [“Changing the Appliance’s NTP Configuration” on page 133](#)
- ♦ [“Setting a Default Time and Locale for Non-LDAP and External Users” on page 133](#)

Changing the Appliance’s NTP Configuration

This dialog lets you adjust the NTP configuration settings that were established when the appliance was deployed.

Path: [Port 9443 Appliance Console](#) > [Time icon](#)

Table 26-1 *Using the Time dialog*

Field, Option, or Button	Information and/or Action
♦ NTP Servers:	♦ Type a new default NTP server.
♦ Region:	♦ Click the drop-down list and select a region for the appliance.
♦ Time Zone:	♦ Click the drop-down list and select a time zone for the appliance.
♦ Hardware clock set to UTC	♦ Use this option to change the hardware clock setting.

Setting a Default Time and Locale for Non-LDAP and External Users

NOTE: You specify the default locale and time zone for LDAP users when you [configure LDAP synchronization](#).

On the other hand, when you create non-LDAP internal users and when external users self-provision, Filr assigns `English (US)` as the default locale and `Greenwich Mean Time (GMT)` as the default time zone.

This dialog lets you change the non-LDAP internal user and external user defaults.

Path: [Port 8443 Filr Admin Console](#) > [Management](#) > [Default User Settings](#)

Table 26-2 Using the Default User Settings dialog

Field, Option, or Button	Information and/or Action
<i>Section: Settings for new internal (non-LDAP) users:</i>	
♦ Time Zone:	♦ Use the drop-down list to select a default time zone for Filr to assign when you create Internal, non-LDAP users.
♦ Locale:	♦ Use the drop-down list to select a default locale for Filr to assign when you create Internal, non-LDAP users.
<i>Section: Settings for new external users:</i>	
♦ Time Zone:	♦ Use the drop-down list to select a default time zone for Filr to assign when external users self-provision to Filr.
♦ Locale:	♦ Use the drop-down list to select a default locale for Filr to assign when external users self-provision to Filr.
OK or Cancel	♦ Click OK to apply the settings you have specified and exit this dialog, or Cancel to discard your changes and exit.

27 UI Controls and Customizations

- ♦ “Email Notification Template Customization” on page 135
- ♦ “Branding the Web Client” on page 135
- ♦ “Branding the Desktop Apps (Advanced-Edition License Only)” on page 137
- ♦ “Branding the Mobile Apps (Advanced-Edition License Only)” on page 138
- ♦ “UI Language” on page 140
- ♦ “Name Completion Settings—Managing How Group Names Display in Drop-Down Lists” on page 141

Email Notification Template Customization

You can customize the email notifications that Filr generates as part of your branding efforts, to provide localized messages, to comply with organizational policies, and so on.

For more information about the templates, see “[Notification \(Email\) Customization](#)” in the *Filr 4.2: Maintenance Best Practices Guide* and “[Email Template Customization—A Video Walkthrough](#)” in *Filr 4.2: Maintenance Best Practices Guide*.

Path: [Port 8443 Filr Admin Console](#) > **System** > **Email Templates**

Table 27-1 Using the Manage Email Templates dialog

Field, Option, or Button	Information and/or Action
♦ Delete button	<ul style="list-style-type: none">♦ This button is activated when you select a template in the list that has been customized.♦ Use it to delete a customized template that you have uploaded to Filr by using the Add Files button. <p>Removing a customized template causes Filr to revert to using the default template that ships with Filr.</p>
♦ Add Files button	<ul style="list-style-type: none">♦ Use this to upload a customized template file to the Filr system.
♦ Name	<ul style="list-style-type: none">♦ The names of the email templates that Filr uses.
♦ Type	<ul style="list-style-type: none">♦ This indicates whether Filr is using a customized or default template.
♦ Gear icon	<ul style="list-style-type: none">♦ This lets you adjust column sizes on this page.

Branding the Web Client

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

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

You can brand the Filr web client to match your organization's brand. You can brand the Filr page with company-specific name, logo, and background image.

Images must be uploaded to Filr before they can be used for branding. You can upload them using **Company Name**, **Company Logo** and **Background Image** option.

NOTE: On upgrading to Filr 4.2, ensure to reapply the Custom branding changes else the branding changes are lost and it defaults to Micro Focus branding.

Path: [Port 8443 Filr Admin Console](#) > **System** > **Custom Branding** > **Web Client Branding**

Table 27-2 Using the Web Client Branding

Field, Option, or Button	Information and/or Action
♦ Enable Web Client Branding	Select to enable company-specific branding.
♦ Company Name	The name can include maximum 60 characters. It is displayed on the Filr Login page. To specify title in multiple lines, use tag. For example: Micro Focus Filr.
♦ Company Logo	<p>The logo appears on all the web interfaces except the Content Editor. The logo and the title will appear on the Follow Notification emails.</p> <p>Supported formats: jpeg, jpg, gif, png, apng, svg, bmp, and ico.</p> <p>Recommended resolution: 164px X 164px (square shaped image).</p> <ul style="list-style-type: none">♦ Browse button Click this to choose the logo file.♦ Apply button Click this to apply the logo. If you choose to apply a different branding file without remove the existing branding, then a dialog prompts you that the existing branding file will be overwritten. Click Yes to overwrite the branding file or click No to retain the existing branding.♦ Remove Current Branding button To remove an existing branding for the web client, click the Remove Current Branding option.

Field, Option, or Button	Information and/or Action
<ul style="list-style-type: none"> ♦ Background Image 	<p>The background image appears on the Login page, External User Self Registration page, Rest Password page, and File Request page.</p> <p>Supported Formats: jpeg, jpg, gif, png, apng, svg, bmp, and ico.</p> <p>Recommended Resolution:</p> <p>Length: From 1000px to 1920px</p> <p>Height: 1080px</p> <ul style="list-style-type: none"> ♦ Browse button <ul style="list-style-type: none"> Click this to choose the image file. ♦ Apply button <ul style="list-style-type: none"> Click this to apply the image. If you choose to apply a different branding file without remove the existing branding, then a dialog prompts you that the existing branding file will be overwritten. Click Yes to overwrite the branding file or click No to retain the existing branding. ♦ Remove Current Branding button <ul style="list-style-type: none"> To remove an existing branding for the web client, click the Remove Current Branding option.
OK or Cancel	<ul style="list-style-type: none"> ♦ Click OK to apply your changes, or Cancel to discard them. Canceling doesn't remove uploaded image files.

Branding the Desktop Apps (Advanced-Edition License Only)

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

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

To customize desktop application branding, you must first create a branding file and then upload the file to the Filr server.

Path: [Port 8443 Filr Admin Console](#) > **System** > **Custom Branding** > **Desktop Site Branding**

Table 27-3 Using the Desktop App Branding dialog

Field, Option, or Button	Information and/or Action
<ul style="list-style-type: none">♦ Mac Branding File	<p>IMPORTANT: You must first create a .zip branding file for your Mac desktops as outlined in “Desktop Branding Files” in the Filtr 4.2: Maintenance Best Practices Guide.</p> <ul style="list-style-type: none">♦ Choose File button <p>Click this to choose the .zip file that you created for your Mac workstations as mentioned above.</p> <ul style="list-style-type: none">♦ Apply button <p>Click this to apply the branding .zip file you have created.</p> <p>If you choose to apply a different branding file without remove the existing branding, then a dialog prompts you that the existing branding file will be overwritten. Click Yes to overwrite the branding file or click No to retain the existing branding.</p> <ul style="list-style-type: none">♦ Remove Current Branding button <p>To remove an existing branding for the Mac desktop application, click the Remove Current Branding option.</p>
<ul style="list-style-type: none">♦ Windows Branding File	<p>IMPORTANT: You must first create a .zip branding file for your Windows desktops as outlined in “Desktop Branding Files” in the Filtr 4.2: Maintenance Best Practices Guide.</p> <ul style="list-style-type: none">♦ Choose File button <p>Click this to choose the .zip file that you created for your Windows workstations as mentioned above.</p> <ul style="list-style-type: none">♦ Apply button <p>Click this to apply the branding .zip file you have created.</p> <p>If you choose to apply a different branding file without remove the existing branding, then a dialog prompts you that the existing branding file will be overwritten. Click Yes to overwrite the branding file or click No to retain the existing branding.</p> <ul style="list-style-type: none">♦ Remove Current Branding button <p>To remove an existing branding for the Windows desktop application, click the Remove Current Branding option.</p>

Branding the 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](#).

Path: [Port 8443 Filr Admin Console](#) > **System** > **Custom Branding** > **Mobile Site Branding**

Table 27-4 Using the Mobile App Branding dialog

Field, Option, or Button	Information and/or Action
<ul style="list-style-type: none"> ♦ Android Branding File 	<p>IMPORTANT: You must first create a .zip branding file for your Android mobile devices desktops as outlined in “Android UI Branding” in the <i>Filr 4.2: Maintenance Best Practices Guide</i>.</p> <ul style="list-style-type: none"> ♦ Browse button Click this to choose the .zip file that you created for your Android mobile devices as mentioned above. ♦ Apply button Click this to apply the branding .zip file you have created. If you choose to apply a different branding file without remove the existing branding, then a dialog prompts you that the existing branding file will be overwritten. Click Yes to overwrite the branding file or click No to retain the existing branding. ♦ Remove Current Branding button To remove an existing branding for the Android mobile devices, click the Remove Current Branding option.
<ul style="list-style-type: none"> ♦ Windows Branding File 	<p>IMPORTANT: You must first create a .zip branding file for your Windows mobile devices as outlined in “iOS UI Branding” in the <i>Filr 4.2: Maintenance Best Practices Guide</i>.</p> <ul style="list-style-type: none"> ♦ Browse button Click this to choose the .zip file that you created for your Windows mobile devices as mentioned above. ♦ Apply button Click this to apply the branding .zip file you have created. If you choose to apply a different branding file without remove the existing branding, then a dialog prompts you that the existing branding file will be overwritten. Click Yes to overwrite the branding file or click No to retain the existing branding. ♦ Remove Current Branding button To remove an existing branding for the Windows mobile devices, click the Remove Current Branding option.

Field, Option, or Button	Information and/or Action
♦ iOS Branding File	<p>IMPORTANT: You must first create a .zip branding file for your iOS mobile devices as outlined in “iOS UI Branding” in the Filtr 4.2: Maintenance Best Practices Guide.</p> <ul style="list-style-type: none"> ♦ Browse button Click this to choose the .zip file that you created for your iOS mobile devices as mentioned above. ♦ Apply button Click this to apply the branding .zip file you have created. If you choose to apply a different branding file without remove the existing branding, then a dialog prompts you that the existing branding file will be overwritten. Click Yes to overwrite the branding file or click No to retain the existing branding. ♦ Remove Current Branding button To remove an existing branding for the iOS mobile devices, click the Remove Current Branding option.

UI Language

For more information about UI language settings in Filr, see “[Language Settings](#)” in the [Filtr 4.2: Maintenance Best Practices Guide](#).

Path: [Port 9443 Appliance Console](#) > [Configuration icon](#) > [Default Locale](#)

Table 27-5 Using the Default Locale dialog

Field, Option, or Button	Information and/or Action
<ul style="list-style-type: none">◆ Default Locale:	<ul style="list-style-type: none">◆ Use this option to reset the language that you selected during the Filr configuration process. <p>The following points explain more about the Default Locale setting.</p> <ul style="list-style-type: none">◆ Micro Focus appliance installations run in English only.◆ When you install the Filr software, you can set the primary language, thereby establishing the UI language for text in locations where all Filr users see it, such as in the Workspace tree. <p>Your choices are:</p> <ul style="list-style-type: none">◆ Chinese-Simplified◆ Chinese Traditional◆ Czech◆ Danish◆ Dutch◆ English◆ French◆ German◆ Hungarian◆ Italian◆ Japanese◆ Polish◆ Portuguese◆ Russian◆ Spanish◆ Swedish <ul style="list-style-type: none">◆ The language that you select or change here also establishes the default interface language and locale for new user profiles that are imported through LDAP. <p>The default language for non-LDAP and self-provisioned users is set in the Default User Settings dialog.</p>

Name Completion Settings—Managing How Group Names Display in Drop-Down Lists

Filr includes a name completion (or Type-to-Find) feature that displays the names of users or groups as you begin typing a name or string.

For example, as you share an item and begin typing in the **Share with field**, names of users or groups that match what you have typed so far display so that you can select a listed item.

To help you distinguish between multiple groups with the same name, Filr includes secondary information.

This dialog lets you specify how group names are displayed in the drop-down list.

Path: [Port 8443 Filr Admin Console](#) > **System** > **Name Completion Settings**

Table 27-6 *Using the Name Completion Settings dialog*

Field, Option, or Button	Information and/or Action
<ul style="list-style-type: none">◆ Primary display text: drop-down list	<ul style="list-style-type: none">◆ Click the drop-down list and select either<ul style="list-style-type: none">◆ Name: The name of the group as it appears in Filr.Or◆ Title: The title as it appears in the LDAP directory.
<ul style="list-style-type: none">◆ Secondary display text: drop-down list	<ul style="list-style-type: none">◆ Click the drop-down list and select either<ul style="list-style-type: none">◆ Description: The description of the group as it appears in Filr.Or◆ Fully Qualified DN. The Fully Qualified Domain Name as it appears in the LDAP directory.

28 Users and Groups

- ♦ [“Managing Users” on page 143](#)
- ♦ [“Managing Groups” on page 147](#)

Managing Users

Path: [Port 8443 Filr Admin Console](#) > [Users](#)

Table 28-1 *Using the Users dialog*

Field, Option, or Button	Information and/or Action
Users dialog (header row)	
♦ New button	♦ Click this to begin creating a new non-LDAP internal user .
♦ Import Profiles... button	<ul style="list-style-type: none">♦ You can manage local users and groups by importing profile files that contain user or group information in XML format. This is a good way to simultaneously perform multiple actions on non-LDAP users and group, such as creating, modifying, or deleting users, and creating or modifying groups.♦ Click Choose File, then navigate to and select the file that contains user or group profile information in XML format.♦ Click View a Sample File and make sure that the format of your file matches the format that is shown in the provided sample file.
♦ Delete button	♦ The effects of this button on user accounts depends on whether the user is an LDAP, non-LDAP Internal, or External user. For more detail, see Deleting Filr Users in the Filr 4.2: Maintenance Best Practices Guide .

Field, Option, or Button	Information and/or Action
<ul style="list-style-type: none"> ◆ More drop-down 	<p>With one or more users selected, you can choose from the following options.</p> <ul style="list-style-type: none"> ◆ Disable User Account: Disabling Filr User Accounts in the Filr 4.2: Maintenance Best Practices Guide ◆ Enable User Account: This restores access through a user account that was previously disabled. ◆ Disable/Enable Personal Storage: Chapter 16, “Personal Storage and Home Folders,” on page 95 ◆ Use Default Personal Storage Setting: Chapter 16, “Personal Storage and Home Folders,” on page 95 ◆ Disable File Downloads: “Web Browser Access—Individual Users and Groups” on page 25 ◆ Enable File Downloads: “Web Browser Access—Individual Users and Groups” on page 25 ◆ Use Default File Download Setting: “Web Browser Access—Individual Users and Groups” on page 25 ◆ Disable Web Access: “Web Browser Access—Individual Users and Groups” on page 25 ◆ Enable Web Access: “Web Browser Access—Individual Users and Groups” on page 25 ◆ Use Default Web Access Setting: “Web Browser Access—Individual Users and Groups” on page 25 ◆ Workspace Share Rights...: Opens the Set User Workspace Sharing Rights dialog, wherein you can restrict Personal Storage sharing privileges. ◆ Desktop Application Settings...: “Desktop Access—Individual Users and Groups” on page 18 ◆ Mobile Application Settings...: “Mobile Device Access—Individual Users and Groups” on page 21 ◆ Add Administrator Rights: Lets you assign selected users as Direct administrators. ◆ Remove Administrator Rights: Lets you remove Direct-administration rights from selected users.
<ul style="list-style-type: none"> ◆ Filter List field 	<ul style="list-style-type: none"> ◆ Begin typing a name and press enter to filter the list to only those users who match what you have entered.
<ul style="list-style-type: none"> ◆ Filter Arrow drop-down 	<ul style="list-style-type: none"> ◆ This lets you filter the displayed list of users using the following criteria: <ul style="list-style-type: none"> ◆ Internal Users ◆ External Users ◆ Disabled Users ◆ Enabled Users ◆ Administrators ◆ Non-administrators <p>By default, all of the above are selected for display.</p>

Field, Option, or Button	Information and/or Action
♦ Gear icon	♦ Click this to adjust column sizes.
♦ Trash Can icon	♦ This displays a list of Personal Workspace trash items that can be recovered. <ul style="list-style-type: none"> ♦ Restore button: This lets you undelete selected items. ♦ Delete button: This lets you permanently erase the selected items. ♦ Restore All button: This restores everything in Personal Workspace trash. ♦ Delete All button: This permanently erases everything in Personal Workspace trash.
Users List (below header row)	
♦ Full Name column	♦ Displays the user's first and last names combined
♦ Arrow drop-down column	♦ Provides access to the following settings for the user: <ul style="list-style-type: none"> ♦ User Properties dialog: Opens the User Properties dialog. ♦ Personal Storage settings: Depending on what has already been configured for the user, you can enable the user's personal storage, disable the user's personal storage, or specify that the default personal storage settings be used for the user. ♦ File Downloads settings: Depending on what has already been configured, you can enable file downloading for the user, disable file downloading for the user, or specify that the default file downloading settings be used for the user. ♦ Web Access settings: Depending on what has already been configured, you can enable web access for the user, disable web access for the user, or specify that the default web access settings be used for the user.
♦ Type column	♦ Icons indicate whether users are LDAP, non-LDAP internal, External self-provisioned, System-created, and so on.
♦ Admin column	♦ This indicates whether users are assigned administrative responsibilities.
♦ Email column	♦ This displays the email address to which Filr sends notifications
♦ Device Icon column	♦ Click this to view the Registered Clients list filtered to include only this user. This lets you manage all the user's devices from one place. For more detail, see "Viewing, Wiping, and Disconnecting Registered Clients" on page 114.
♦ User Id column	♦ The login name of each user
Set User Workspace Sharing Rights dialog	Use this to restrict Personal Storage sharing privileges.
♦ Internal Users ♦ External Users ♦ Public ♦ File Link ♦ Allow Re-Sharing of granted rights	♦ After you have enabled sharing of files for the entire Filr system , you can restrict Personal Storage shared-access-rights-granting by clearing any of the settings shown in this dialog (listed in the left column). ♦ Asterisks (*) indicate rights that are not enabled site-wide. You cannot grant individual users more rights than are currently defined for the site-wide setting.

Field, Option, or Button	Information and/or Action
New User dialog	
♦ User ID	♦ You must assign a unique user ID for each non-LDAP internal user.
♦ Password	♦ You must assign (type and confirm) a password for the user to log in with.
♦ First Name	♦ You can include the user's first name
♦ Last Name	♦ You can also include the user's last name.
♦ Picture	♦ You can include a picture of the user, or the user can add it later.
♦ Time Zone	♦ Make sure the time zone setting is accurate.
♦ Locale	♦ Make sure the locale setting matches the user's language preference.
<i>Personal Information</i>	Users normally provide the following information for themselves.
♦ Job Title	
♦ About Me	
♦ Email	
♦ Phone	
♦ Text Messaging Email	
OK or Cancel	♦ Click OK to save the user information you have entered, or click Cancel to discard your entries.

Viewing and Managing User Properties

Path: [Port 8443 Filr Administration Console Management](#) > [Users](#) > drop-down arrow next to the user > [User Properties](#)

Table 28-2 *Using the User Properties dialog*

Field, Option, or Button	Information and/or Action
♦ Profile button	♦ You can change any of the following that is not synchronized from an LDAP source: <ul style="list-style-type: none"> ♦ User ID ♦ Picture ♦ Time Zone ♦ Locale ♦ Job Title ♦ About Me ♦ Email ♦ Phone ♦ Text Messaging Email

Field, Option, or Button	Information and/or Action
♦ Home Folder button	♦ Lets you change some configuration for the User's Home folder including: <ul style="list-style-type: none"> ♦ The name that displays under My Files ♦ The content indexing settings ♦ The Just-in-Time Synchronization settings ♦ The synchronization schedule
♦ Personal Storage button	♦ Lets you enable or disable Personal Storage
♦ Quotas button	♦ Lets you adjust the data quota
♦ Sharing... button	♦ Lets you change the Personal Storage Sharing options
♦ Net Folders... button	♦ Lets you manage the assigned Net Folder settings

Managing Groups

Path: [Port 8443 Filr Admin Console](#) > **Groups**

Table 28-3 *Using the Groups dialog*

Field, Option, or Button	Information and/or Action
Manage Groups dialog (header row)	
♦ New button	♦ Click this to begin adding a new non-LDAP internal group .
♦ Delete button	♦ Click this to remove the selected groups from the list.

Field, Option, or Button	Information and/or Action
<ul style="list-style-type: none"> ◆ More drop-down 	<p>With one or more groups selected, you can choose from the following options:</p> <ul style="list-style-type: none"> ◆ Disable/Enable Personal Storage: Chapter 16, “Personal Storage and Home Folders,” on page 95 ◆ Use Default Personal Storage Setting: Chapter 16, “Personal Storage and Home Folders,” on page 95 ◆ Disable File Downloads: “Web Browser Access—Individual Users and Groups” on page 25 ◆ Enable File Downloads: “Web Browser Access—Individual Users and Groups” on page 25 ◆ Use Default File Download Setting: “Web Browser Access—Individual Users and Groups” on page 25 ◆ Disable Web Access: “Web Browser Access—Individual Users and Groups” on page 25 ◆ Enable Web Access: “Web Browser Access—Individual Users and Groups” on page 25 ◆ Use Default Web Access Setting: “Web Browser Access—Individual Users and Groups” on page 25 ◆ Desktop Application Settings...: “Desktop Access—Individual Users and Groups” on page 18 ◆ Mobile Application Settings...: “Mobile Device Access—Individual Users and Groups” on page 21 ◆ Add Administrator Rights: Lets you assign selected group members as Direct administrators. ◆ Remove Administrator Rights: Lets you remove Direct-administration rights from selected groups.
<ul style="list-style-type: none"> ◆ Filter List field 	<ul style="list-style-type: none"> ◆ Begin typing a name and press enter to filter the list to only those users who match what you have entered.
Manage Groups (below header row)	
<ul style="list-style-type: none"> ◆ Type column 	<ul style="list-style-type: none"> ◆ Icons indicate whether the groups are LDAP, non_LDAP internal, LDAP with Direct Admin rights, non-LDAP with Direct Admin rights.
<ul style="list-style-type: none"> ◆ Title column 	<ul style="list-style-type: none"> ◆ Displays group titles as defined in LDAP or specified when the group was created. LDAP titles cannot be changed in Filr, non-LDAP titles can be changed. ◆ Click this to edit the group, including changing the group title and the membership configuration.

Field, Option, or Button	Information and/or Action
<ul style="list-style-type: none"> ♦ Arrow drop-down column 	<ul style="list-style-type: none"> ♦ Provides access to the following settings for the group: <ul style="list-style-type: none"> ♦ Personal Storage settings: Depending on what has already been configured for the group, you can enable personal storage for all group members, disable personal storage for all group members, or specify that the default personal storage settings be used for all group members. ♦ File Downloads settings: Depending on what has already been configured, you can enable file downloading for all group members, disable file downloading for all group members, or specify that the default file downloading settings be used for all group members. ♦ Web Access settings: Depending on what has already been configured, you can enable web access for all group members, disable web access for all group members, or specify that the default file downloading settings be used for all group members.
<ul style="list-style-type: none"> ♦ Name column 	<ul style="list-style-type: none"> ♦ Displays group names as defined in LDAP or specified when the group was created. Group names cannot be changed.
<ul style="list-style-type: none"> ♦ Admin column 	<ul style="list-style-type: none"> ♦ This indicates whether the group members are allowed Direct administrative responsibilities because of membership in the group.
Add Group dialog	
<ul style="list-style-type: none"> ♦ Name: field 	<ul style="list-style-type: none"> ♦ Specify a unique name under which the group is to be stored in the Filr database. You can use only alphanumeric characters (a-z, A-Z, 0-9), hyphens (-), and underscores (_). ♦ Once the group is created, the name cannot be modified. ♦ By default, after the group is added, this is what appears in lists of Filr groups. However, you can specify whether the group Name or Title is displayed when users are selecting groups, for example in the Share dialog, by modifying the name completion settings, see “Name Completion Settings—Managing How Group Names Display in Drop-Down Lists” on page 141.
<ul style="list-style-type: none"> ♦ Title: field 	<ul style="list-style-type: none"> ♦ Enter a descriptive group title. This string can include any characters that you can type. ♦ The title can be modified ♦ You can specify whether the group Name or Title is displayed when users are selecting groups, for example in the Share dialog, by modifying the name completion settings, see “Name Completion Settings—Managing How Group Names Display in Drop-Down Lists” on page 141.
<ul style="list-style-type: none"> ♦ Description: box 	<ul style="list-style-type: none"> ♦ If desired, include some text that describes the group, such as what the members of this group have in common.
<ul style="list-style-type: none"> ♦ Group membership is static option 	<ul style="list-style-type: none"> ♦ Static groups are groups whose membership is directly specified and does not change based on LDAP queries.
<ul style="list-style-type: none"> ♦ Group membership is dynamic option 	<ul style="list-style-type: none"> ♦ Dynamic groups are populated based on LDAP queries made by Filr. Their membership changes as the meta data returned from Filr’s LDAP queries changes.

Field, Option, or Button	Information and/or Action
♦ Edit group membership button	♦ Click this to configure the type of group you have selected:
OK or Cancel	<ul style="list-style-type: none"> ♦ Click OK to save the changes you've made in this dialog or Cancel to discard your changes. ♦ Make sure you have edited the group membership. Otherwise your group will have no members.
Static Membership for Group dialog	
Allow external users and groups option	♦ Select this to allow external users and groups to be added to the list.
Users tab	♦ User field: Begin typing a user name, then select a listed user to add it to the Membership list.
Groups tab	♦ Group field: Begin typing a group name, then select a listed group to add it to the Membership list.
♦ Remove button	♦ Click this to remove a selected user or group (depending on which dialog you are in).
<i>Membership list</i>	♦ A list of the users/groups in the static group.
OK or Cancel	♦ Click OK to save the changes you've made in this dialog or Cancel to discard your changes.
Edit Dynamic Membership dialog	
Tips and Caveats	<ul style="list-style-type: none"> ♦ Users must already have existing Filr user accounts in order for them to be added to a Filr group as described in this section. If your LDAP query includes users who are not already Filr users, the users are not added to the Filr group ♦ When you configure your LDAP connection, you must specify the name of the LDAP attribute that uniquely identifies the user (the value of this attribute never changes). For eDirectory, this value is GUID. For Active Directory, this value is objectGUID. For more information about this attribute, see "Guid attribute:" on page 37. ♦ The Filr process that creates a dynamic group uses the LDAP configuration settings in Filr to authenticate to the LDAP directory server used to specify the Base DN (below). The credentials that are used are the LDAP server URL, user DN, and password. For more information on how to configure these and other LDAP configuration settings in Filr, see "LDAP Servers and Synchronization" on page 33. ♦ The Base DN set below must exist in each LDAP source. Otherwise, the membership of the dynamic group might not be updated correctly. ♦ If your Filr site is configured with multiple LDAP sources and the base DN that you define for the dynamic group exists in each LDAP source, the membership of the dynamic group contains users from each LDAP source that match the dynamic group's filter.
♦ Current Membership: button	♦ Click this to open the Dynamic Group Membership windows and view the users that are included in the group based on the current configuration.

Field, Option, or Button	Information and/or Action
♦ Base DN:	♦ Use the LDAP browse button to locate the context where you want the search for users to begin.
♦ LDAP Filter:	♦ Specify the LDAP filter you want to use for the query. This is required for the search to return any results. ♦ For an example and more information, see “Filter:” on page 40 .
♦ Search subtree option	♦ Select this to have the search extended into sub-containers.
♦ Update group membership during scheduled ldap synchronization option	♦ You must either select this or perform a manual ldap synchronization before any users are added to the group you are defining. ♦ If you do not select this option, the group will not be automatically updated when changes occur in your LDAP directory.
♦ Test ldap query button	♦ Use this to see whether the configuration you have specified is working.
OK or Cancel	♦ Click OK to save the changes you’ve made in this dialog or Cancel to discard your changes.
Dynamic Group Membership window	
Users tab	♦ This displays a list of the users and groups that are members of the dynamic group.
♦ Close button	♦ Use this to return to the previous window.

29 Integrating Microsoft Office and Outlook with Filr

Filr now provides a plugin for integrating Filr with Microsoft Office and Outlook. The Micro Focus Filr Plugin for Microsoft Office and Outlook enables Filr users to work with files in their **My Files** and **Netfolders** area of the Filr server directly from a Microsoft Office 2013, 2016, and Office 365 application such as Excel, Word, Outlook, or PowerPoint.

After installing this plugin, Filr users can use the Microsoft applications as follows:

- ♦ **Microsoft Outlook:** Browse local or Filr-based files and attach the files in an email. Depending on the policy settings, the files are either directly attached to the email or the files are first uploaded to the Filr server and the link of the uploaded files is then shared in the email.

NOTE: Users can use the Outlook feature only if an Advanced-Edition license is installed on the Filr appliance.

- ♦ **Microsoft Excel, Word, PowerPoint:** Users can do the following:
 - ♦ Browse to a file that is located on a Filr server, open the file, edit it, and then save it back to the Filr server.
 - ♦ Create a new file and upload it to the Filr server.
 - ♦ Share a file with Filr users.
- ♦ [“Managing Office Settings” on page 153](#)
- ♦ [“Managing Outlook Settings” on page 153](#)

Managing Office Settings

Path: [Port 8443 Filr Admin Console](#) > **Management** > **Office and Outlook Settings**

For downloading the Micro Focus Filr Plugin for Microsoft Office and Outlook, see [Filr 4: Using Micro Focus Filr with Microsoft Office and Outlook Applications](#) guide.

To enable the plugin in Microsoft Office, select the **Enable Filr Office Plugin** option. By default, this option is disabled.

Managing Outlook Settings

Path: [Port 8443 Filr Administration Console](#) > **Management** > **Office and Outlook Settings**

For downloading the Filr Outlook Plugin, configuring Filr settings in Microsoft Outlook, and using Microsoft Outlook for sending email attachments through Filr, see [Downloading and Installing the Filr Outlook Plugin](#) in the [Using Micro Focus Filr with Microsoft Outlook Quick Start](#).

To configure the Outlook settings, see [Table 29-1 on page 154](#).

To view information about the email sent through Outlook and the details of the file uploaded on the Filr server and shared in the email, see the [Filr Outlook Report](#).

Table 29-1 *Using the Outlook Settings dialog*

Field, Option, or Button	Information and/or Action
♦ Enable Filr Outlook Plugin	♦ Select this to enable the plugin in Microsoft Outlook. By default, this option is disabled.
Filr Outlook Policy	
♦ Allow download of email attachments without authentication	♦ Select this to enable the external users to access email attachments without authenticating to Filr. By default, this option is disabled and the Filr Administrator defines the policy.
♦ Allow user to define the policy	♦ Select this to enable Filr users to define the Filr Outlook policy terms, such as when to send attachments using Filr and when attachment links sent in the email expires. By default, this option is disabled and the Filr Administrator defines the policy.
♦ Send attachments using Filr	♦ Select one of the following: <ul style="list-style-type: none"> ♦ Always: Select this to ensure that all of the files that Microsoft Outlook users attach to emails through the Filr Plug-in are not directly sent as email attachments. All the files are first uploaded to the Filr server irrespective of the file size and then the link of the uploaded files is shared in the email. <p>File size exceeds X MB:</p> <p>Select this to specify the maximum file size beyond which a file attached to the email through the Filr Plug-in is first uploaded to the Filr server and then the link of the uploaded file is shared in the email sent to the recipient.</p>
♦ Attachment link expires after	♦ Click one of the following to specify when an attachment link sent through email should expire: <ul style="list-style-type: none"> ♦ X days: Select this to specify the number of days after which the attachment link sent in the email should expire. ♦ X downloads: Select this to specify the maximum number of times the attachment can be downloaded, after which the attachment link sent in the email should expire.
♦ Allow user to modify the policy limits	♦ Select this to enable Filr users to override the values and specify a value less than what the Filr Administrator has set for the Send attachments using Filr and Attachment link expires after .
Delete attachments stored in the Filr Outlook storage	♦ If the Filr Appliance storage is 90% utilized, the Filr system sends email notifications to the Filr administrator provided that the administrator's profile has an email address configured. ♦ To automatically delete all the expired attachments, Filr initiates a clean up process everyday at 1 a.m. GMT.

Field, Option, or Button	Information and/or Action
♦ Expired attachments	♦ This enables all the expired attachments for deletion when Delete is clicked. This is selected by default and cannot be deselected.
Attachments older than X days	♦ Select this to specify the age (in days) of the attachments that you want to delete from the Filr Appliance storage. You can click Delete to immediately delete attachments older than the specified days.
♦ Delete	♦ Click this to immediately delete expired attachments and the attachments older than the specified days from the Filr Appliance storage.
♦ Apply	♦ Click this to save your changes.
♦ Close	♦ Click this to return to the previous window.

