

OpenText Filr 23.4

Administrative User Interface Reference

July 2024

Legal Notice

Copyright 2023-2024 Open Text

The only warranties for products and services of Open Text and its affiliates and licensors ("Open Text") are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Contents

About This Guide	9
1 Administrative Consoles	11
2 Administrative Access	15
Assigning and Managing Port 8443 Direct Administrators	15
Changing Passwords and SSH Access for vaadmin and root	16
Logging In as an Administrator	16
Administration Console	16
Port 9443 Console	17
3 Access to Filr and Its Services	19
Desktop Access—Default Settings	19
Desktop Access—Individual Users and Groups	22
Mobile Device Access—Default Settings	23
Mobile Device Access—Individual Users and Groups	25
Web Browser Access—Default Settings	28
Web Browser Access—Individual Users and Groups	29
Recent Files List	30
Share NetFolders and Home Folders	31
KeyShield Configuration Settings	31
NetIQ Advanced Authentication Configuration	33
Reverse Proxy Configuration Settings	34
Single Sign-On Access	35
OAuth Integration	35
Applications Supported on Filr	35
Register an Application with Filr	36
Generating Client Secret	37
Data Leak Prevention	37
Policies	38
Managing Workspace	39
4 Access Nodes in the Clustered Deployment	41
Filr Cluster Control	41

5	Filr Clustering Configuration	43
6	LDAP Servers and Synchronization	45
7	Content Editor	57
8	Licensing	61
	Installing/Updating the Filr License	61
	Viewing Filr License Details	61
9	Logging and Monitoring	63
	Accessing Filr System Log Files	63
	Automatically Applying Deferred Search Logs	63
	Generating Filr-Monitoring Reports	64
	Credits Report	65
	Data Quota Exceeded Report	65
	Data Quota Highwater Exceeded Report	65
	Disk Usage Report	66
	Email Report	66
	External User Report	67
	File Block Report	67
	Filr Outlook Report	68
	License Report	68
	Login Report	69
	Orphaned User Share Report	69
	System Error Logs Report	70
	User Access Report	70
	User Activity Report	70
	XSS (Cross-Site Scripting) Report	71
	Logging All HTTPS Traffic	71
	Managing Audit Trail Logs of Database Activity	72
	SIEM Integration	72
	SIEM Configuration Dialog	72
10	Management Zones	75
	Managing Zones	75
	Adding and Modifying Zones	75
	Adding a Zone	75
	Modifying a Zone	76
	Deleting Zones	77
	Viewing Zones Information	77
11	Net Folder Servers	79
	Creating and Managing Net Folder Servers	79
	Manage Net Folder Servers Dialog	79
	Creating a Net Folder Server	79
	Editing an Existing Net Folder Server	83
	Deleting a Net Folder Server	84

Enabling Just-in-Time-Synchronization for Filr and eDirectory Rights Usage for OES	84
Proxy User Identities	85
Managing Proxy Identities	86
Creating Proxy Identities	86
Modifying Proxy Identities	86
12 Net Folders	89
Managing Net Folders	89
Creating and Modifying Net Folders	90
Creating a Net Folder	90
Modifying a Net Folder	94
Deleting a Net Folder	94
13 Net Folder System-Level Synchronization	95
Enabling and Tuning Net Folder Synchronization	95
Just-in-Time Synchronization	96
14 Network Infrastructure	97
Changing Network Settings	97
Network Configuration	98
Port Numbers	100
15 Notifications (Email)	103
Configuring an Email Service for Filr to Use	103
Enabling Notifications	105
16 Performance Tuning	107
Changing Configuration Settings for Requests and Connections	107
Changing JVM Configuration Settings	108
17 Personal Storage and Home Folders	109
Enabling Personal Storage for Users and Groups	109
Managing and Restricting Filr-Based Storage	109
18 Product Improvement	113
19 Sharing	115
Managing Shared Items	115
Managing Sharing, License Terms, and Comments	116
The General Tab Controls All Filr Sharing	120

20 File Versioning	121
21 Managing Uploading of Files	123
22 Search and Lucene Indexing	127
Managing Filrsearch Configuration Settings	127
Managing the Lucene Index	129
Managing Search Nodes	130
Memcached (Search Index Appliance Only)	131
Advantages for Using Memcached	131
Managing Memcached	131
23 Security	133
Certificates	133
Firewall Configuration	134
Password Security (Local and External Users)	134
Securing Memcached	135
User Visibility	135
Viewing, Wiping, and Disconnecting Registered Clients	136
WebDAV Authentication Configuration Settings	136
24 SQL Database Connection	139
25 Storage Management	141
Expanding Storage	141
26 Support Files and Online Updates	143
Managing Field Test Patches	143
Managing Online Updates	143
Upgrading the Services Hosted on Filr Appliance	145
Submitting Configuration Files to OpenText Support	145
27 Changing System Services Configurations	147
Managing System Services	147
Shutting Down and Restarting the Appliance	148
28 Time and Locale	149
Changing the Appliance's NTP Configuration	149
Setting a Default Time and Locale for Non-LDAP and External Users	149
29 UI Controls and Customizations	151
Email Notification Template Customization	151
Branding the Web Client	151
Branding the Desktop Apps (Advanced-Edition License Only)	153

Branding the Mobile Apps (Advanced-Edition License Only)	154
UI Language	155
Name Completion Settings—Managing How Group Names Display in Drop-Down Lists	157
Add Custom Templates to Filr	157
30 Users and Groups	159
Managing Users	159
Viewing and Managing User Properties	162
Managing Groups	163
31 Integrating Microsoft and GroupWise with Filr	169
Managing Office Settings	169
Managing Mail Settings	169

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 11](#)
- ♦ [Chapter 2, “Administrative Access,” on page 15](#)
- ♦ [Chapter 3, “Access to Filr and Its Services,” on page 19](#)
- ♦ [Chapter 4, “Access Nodes in the Clustered Deployment,” on page 41](#)
- ♦ [Chapter 5, “Filr Clustering Configuration,” on page 43](#)
- ♦ [Chapter 6, “LDAP Servers and Synchronization,” on page 45](#)
- ♦ [Chapter 7, “Content Editor,” on page 57](#)
- ♦ [Chapter 8, “Licensing,” on page 61](#)
- ♦ [Chapter 9, “Logging and Monitoring,” on page 63](#)
- ♦ [Chapter 10, “Management Zones,” on page 75](#)
- ♦ [Chapter 11, “Net Folder Servers,” on page 79](#)
- ♦ [Chapter 12, “Net Folders,” on page 89](#)
- ♦ [Chapter 13, “Net Folder System-Level Synchronization,” on page 95](#)
- ♦ [Chapter 14, “Network Infrastructure,” on page 97](#)
- ♦ [Chapter 15, “Notifications \(Email\),” on page 103](#)
- ♦ [Chapter 16, “Performance Tuning,” on page 107](#)
- ♦ [Chapter 17, “Personal Storage and Home Folders,” on page 109](#)
- ♦ [Chapter 18, “Product Improvement,” on page 113](#)
- ♦ [Chapter 19, “Sharing,” on page 115](#)
- ♦ [Chapter 20, “File Versioning,” on page 121](#)
- ♦ [Chapter 21, “Managing Uploading of Files,” on page 123](#)
- ♦ [Chapter 22, “Search and Lucene Indexing,” on page 127](#)
- ♦ [Chapter 23, “Security,” on page 133](#)
- ♦ [Chapter 24, “SQL Database Connection,” on page 139](#)
- ♦ [Chapter 25, “Storage Management,” on page 141](#)
- ♦ [Chapter 26, “Support Files and Online Updates,” on page 143](#)
- ♦ [Chapter 27, “Changing System Services Configurations,” on page 147](#)
- ♦ [Chapter 28, “Time and Locale,” on page 149](#)
- ♦ [Chapter 29, “UI Controls and Customizations,” on page 151](#)
- ♦ [Chapter 30, “Users and Groups,” on page 159](#)
- ♦ [Chapter 31, “Integrating Microsoft and GroupWise with Filr,” on page 169](#)

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 *Filr Administration Guide* and other documentation, visit the [OpenText Filr 23.4 Documentation website](#).

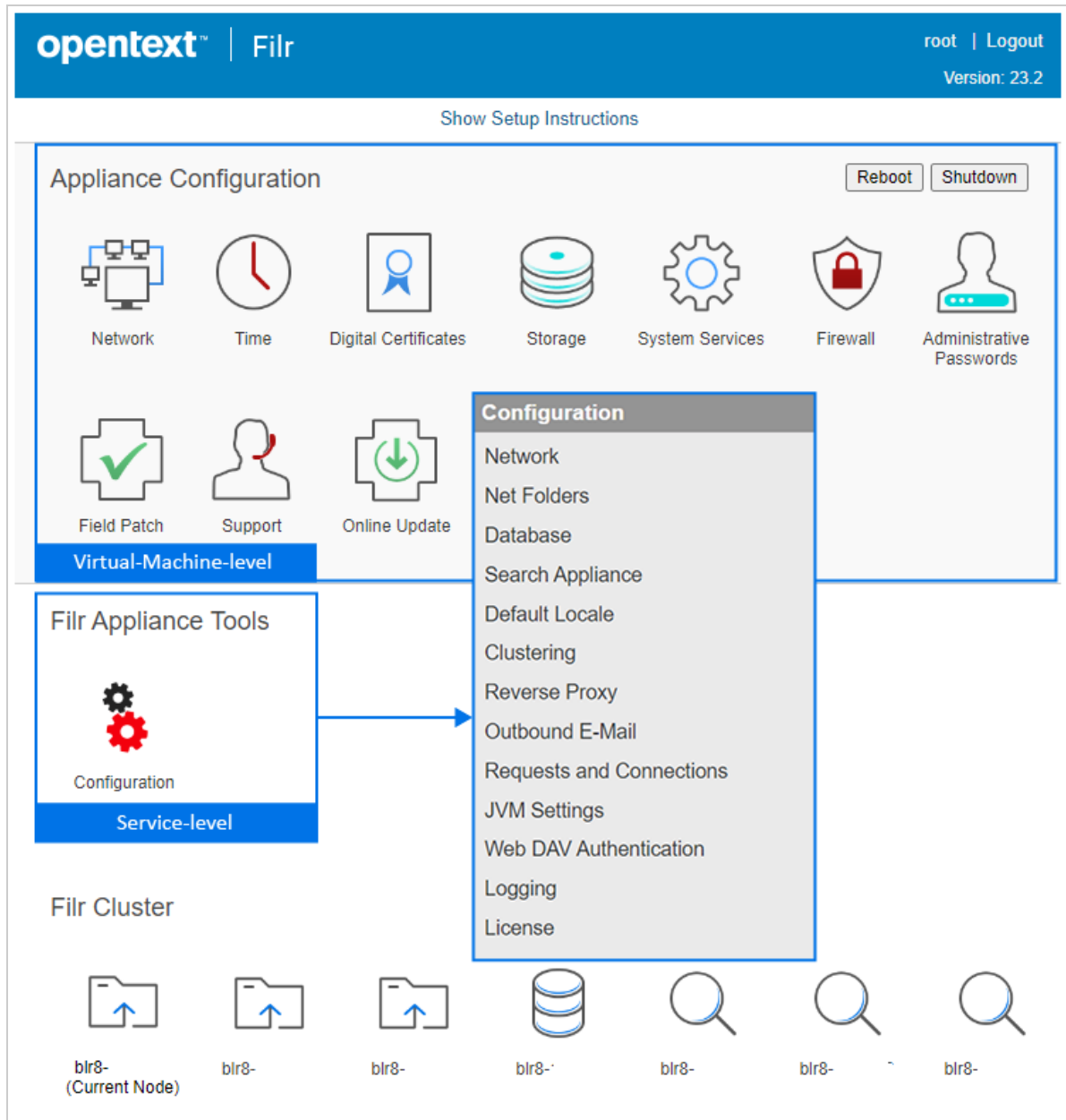
1 Administrative Consoles

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

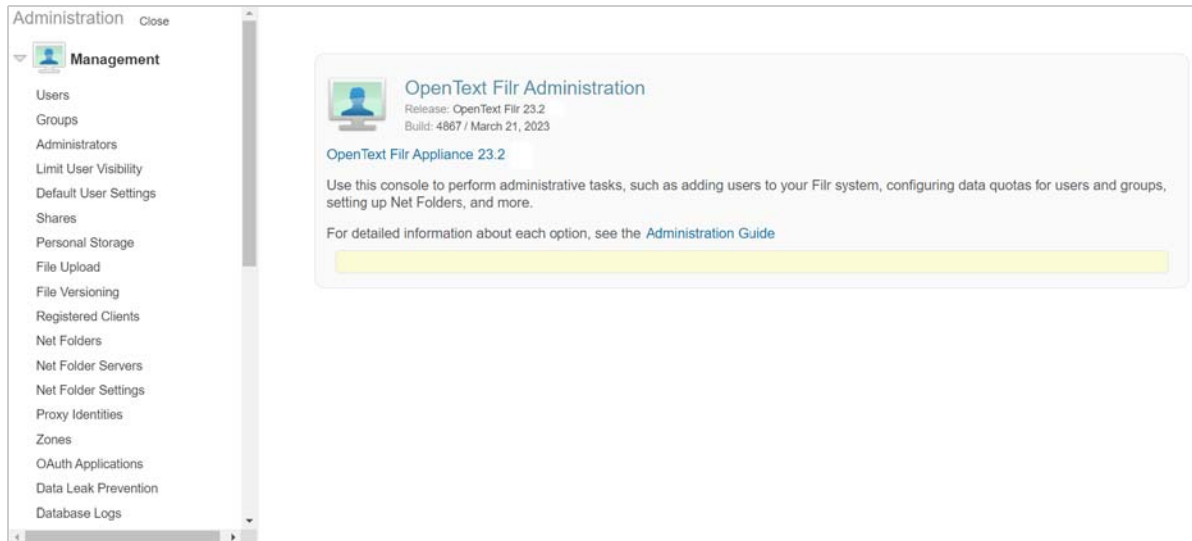
Path: To access the Administration Console, login to the new Filr Web client <https://appliance_ip_or_dns:8443>, then click on **Username** > **Administration Console**.

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 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 97](#).
- ♦ 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 15](#)
- ♦ [“Changing Passwords and SSH Access for vaadmin and root” on page 16](#)
- ♦ [“Logging In as an Administrator” on page 16](#)


For more information about Filr administrator’s tasks, see [“Filr Administrative Users”](#) in the [OpenText Filr 23.4: Understanding How Filr Works](#) guide.

Assigning and Managing Port 8443 Direct Administrators

Path: [“Port 8443 Filr Administration Console” on page 12](#) > **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 147 .

Logging In as an Administrator

Administration Console

Path: [“Port 8443 Filr Administration Console” on page 12](#)

Table 2-3 Using the Sign In dialog

Field, Option, or Button	Information and/or Action
♦ User ID:	♦ First-time login: The username you specified in “ Specify the First Search Appliance, Locale, and Admin user ” in the <i>OpenText Filr 23.4: 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:	♦ 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	♦ 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 19
- ♦ “Desktop Access—Individual Users and Groups” on page 22
- ♦ “Mobile Device Access—Default Settings” on page 23
- ♦ “Mobile Device Access—Individual Users and Groups” on page 25
- ♦ “Web Browser Access—Default Settings” on page 28
- ♦ “Web Browser Access—Individual Users and Groups” on page 29
- ♦ “Recent Files List” on page 30
- ♦ “Share NetFolders and Home Folders” on page 31
- ♦ “KeyShield Configuration Settings” on page 31
- ♦ “NetIQ Advanced Authentication Configuration” on page 33
- ♦ “Reverse Proxy Configuration Settings” on page 34
- ♦ “Single Sign-On Access” on page 35
- ♦ “OAuth Integration” on page 35
- ♦ “Data Leak Prevention” on page 37

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 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 OpenText ZENworks.</p> <p>For more information, see “Client Management Software and the Filr Desktop Applications” in the <i>OpenText Filr 23.4: 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>OpenText Filr 23.4: 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	<p>For more information, see “Controlling File Downloads by the Filr Desktop Applications” in the <i>OpenText Filr 23.4: Maintenance Best Practices Guide</i>.</p>

Field, Option, or Button	Information and/or Action
♦ Restore Defaults...	♦ Click this to restore the defaults for all settings in the Application Whitelist/Blacklist section below.
Mode	♦ Lets you control how antivirus, backup, and other applications download files that are accessible through Filr.
♦ No restrictions - Ignore the lists.	♦ 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.	<p>♦ 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."</p> <p>This option doesn't provide for user control of application-driven downloads.</p> <p>♦ Whitelist can be left empty, however restore defaults will populate the list of default whitelist applications.</p> <p>♦ You can add and remove applications for your organization as needed.</p>
♦ Blacklist - Block the listed applications from downloading files.	<p>♦ 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."</p> <p>This option doesn't provide for user control of application-driven downloads.</p> <p>♦ Filr includes two default blacklists (Windows and Mac) that you can modify as needed.</p> <p>♦ Blacklisted applications are blocked from downloading files through Filr.</p> <p>♦ Unlisted applications are allowed to download files.</p>
♦ Whitelist and Blacklist - Allow and block the listed applications. Prompt users to allow or block unlisted applications.	<p>♦ If you select this option, then</p> <ul style="list-style-type: none"> ♦ Blacklisted applications are always blocked. ♦ Whitelisted applications are always allowed. <p>♦ A download attempt by an unidentified application causes the application to be added to a list of blocked applications.</p> <p>♦ Users can allow downloading by any blocked applications through their desktop Filr console.</p>
Whitelist	<p>♦ Whitelist can be left empty, however restore defaults will populate the list of file types that are default whitelist applications</p> <p>♦ Only the built-in administrator can create a customized list.</p> <p>♦ Applications listed here and in the Blacklist are blocked.</p> <p>In other words, the Blacklist trumps the Whitelist.</p>

Field, Option, or Button	Information and/or Action
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.
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 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 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	<div>♦ Select this to let users download files from Filr to mobile devices.</div> <div>IMPORTANT: If you don't want users downloading files, make sure that you also disable downloading through web browsers.</div> <div>♦ Downloaded files can be viewed in offline mode by accessing the Downloads section in the app.</div> <div>♦ Users are responsible for the security of downloaded files. See "Encrypting Downloaded Files" in the "OpenText Filr 23.4 Mobile App Quick Start Help".</div>
♦ Force PIN Code	<div>♦ Select this to force users running Filr mobile app to have a 4-digit access code set on their devices for accessing Filr</div> <div>See "Configuring a 4-Digit Passcode" in the "OpenText Filr 23.4 Mobile App Quick Start Help."</div>
♦ 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)	<div>♦ Select this to let users take a screen capture while inside the Filr application.</div> <div>IMPORTANT: As noted in the option name, this only applies to Android devices. iOS users can always take screen captures.</div>
♦ 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: ♦ Only Android package names and iOS bundle IDs are valid list entries.</p> <p>♦ To get an Android app package name:</p> <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> <p>♦ To find the bundle ID for an iOS app:</p> <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.
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	<p>♦ Click this to cancel the changes you have made.</p>

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 "OpenText Filr 23.4 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 "OpenText Filr 23.4 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: ♦ Only Android package names and iOS bundle IDs are valid list entries.</p> <p>♦ To get an Android app package name:</p> <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> <p>♦ To find the bundle ID for an iOS app:</p> <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
♦ 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>OpenText Filr 23.4: Understanding How Filr Works</i>.</p> <p>IMPORTANT: ♦Guest access is for web users only.</p> <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.
♦ 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.
♦ 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>
♦ 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 28.</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>

Recent Files List

This is the list of recently accessed files by the logged in user and the files shared (by the logged in user and other users). By default, 10 files accessed by the user, in the past 7 days are listed. The Administrator can configure the number of days. The user can change the number of files to be displayed in the list. By default, the Netfolders flag is enabled. If the Administrator disables Netfolders for the Recent Files, then the files uploaded, renamed, commented, or edited by other users in the Netfolders are not listed under logged in user’s **Recent Files**. All the files that you or other users access recently are listed in this area. There is no need to browse the individual folders to access those files. The list displays:

- ◆ Who has modified the file.
- ◆ What is the operation performed on the file.

Changing the age of the files that appear on the Recent Files

By default, the recent files accessed by the user in the past 7 days are listed in the Recent Files. The Administrator can change the number of days up to 60. To do this, add `recent.activity.for.days=<value>` as a separate line at `/opt/novell/filr/apache-tomcat/webapps/ssf/WEB-INF/classes/config/ssf-ext.properties`.

Figure 3-1 Adding SSH

```
kablink.encryption.key.initial=NDIzNzUxODU4MQ==
recent.activity.for.days=60
recent.activity.netfolders.disable=true
"/opt/novell/filr/apache-tomcat/webapps/ssf/WEB-INF/classes/config/ssf-ext.properties"
```

After adding the line, restart the Filr service.

NOTE: ♦ This setting affects all the users in the Filr including an administrator and the users with equivalent rights as an administrator.

- ♦ The value for `recent.activity.for.days` should be numerical and be less than or equal to 60 (maximum), if value more than 60, then defaulted to the maximum value.
-

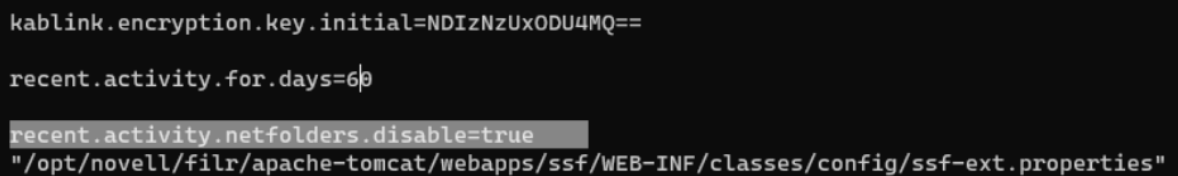
Disabling the Recent Files

The administrator can change the number of days to -1. To do this, add `recent.activity.for.days=<value>` as a separate line at `/opt/novell/filr/apache-tomcat/webapps/ssf/WEB-INF/classes/config/ssf-ext.properties`. Recent files will not be displayed for the users.

Restrict the files in the NetFolders from appearing in the Recent Files list

By default, if any activity like adding comments, move, copy, or share performed by users on the files in My Files, Shared with Me, and Net Folders area are listed in the Recent files. However, the Filr administrator based on the activities can restrict the files from the Netfolder getting displayed in Recent Files. To restrict the files, add `recent.activity.netfolders.disable=true` as a separate line at `/opt/novell/filr/apache-tomcat/webapps/ssf/WEB-INF/classes/config/ssf-ext.properties`, as shown in the figure below and restart the Filr Service.

Figure 3-2 Adding SSH



```
kablink.encrypted.key.initial=NDIzNzUxODU4MQ==
recent.activity.for.days=60
recent.activity.netfolders.disable=true
"/opt/novell/filr/apache-tomcat/webapps/ssf/WEB-INF/classes/config/ssf-ext.properties"
```

NOTE:

- ♦ This setting affects all the users in the Filr including the administrator and users with equivalent rights as an administrator.
 - ♦ This setting does not affect share activities performed on NetFolder files. Share activities continue to show even after setting this flag to true.
-

Share NetFolders and Home Folders

By default, Filr WebClient users are not allowed to share at the root level. An Administrator has an option to turn on/off root level sharing. If the flag `allow.root.level.NF.share` is set to `true` in `ssf-ext.properties` file then share option will be available on root level of Net Folder and user's Home folder.

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 *OpenText Filr 23.4: 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.
♦ KeyShield Server URL (use http or https):	♦ The access URL of the KeyShield server.
♦ API authorization key:	♦ The API Key copied from the KeyShield console.
♦ HTTP connection timeout:	♦ Enter the time in “milliseconds”. This is the time taken by Filr appliance to wait for a response from KeyShield before prompting users for their login credentials. ♦ OpenText does not recommend changing this value unless the network connection does not give quick response. For example, when Filr and KeyShield connect over a WAN.
♦ Connector names:	♦ The names of every KeyShield SSO connector that Filr users will connect through.
♦ Username attribute alias:	♦ The Username attribute entered allows the KeyShield to match username validation requests with the LDAP attribute that requests applications use for usernames. For more detail and a Filr example, see “ KeyShield Attribute Alias Support ” in the <i>OpenText Filr 23.4: Maintenance Best Practices Guide</i> .
Two Factor Authentication	
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.

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.

NetIQ Advanced Authentication Configuration

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

This functionality is only available on Filr Advanced Edition and Power 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 *OpenText Filr 23.4: 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"> Enable multi-factor authentication for internal LDAP users and/or external users to access Filr. Specify the configuration information for the following fields.
<ul style="list-style-type: none"> Internal LDAP users 	<ul style="list-style-type: none"> Select this checkbox to enable multi-factor authentication for internal LDAP users. This checkbox is enabled only for Filr Advanced Edition.
<ul style="list-style-type: none"> External users 	<ul style="list-style-type: none"> Select this checkbox to enable multi-factor authentication for external users. This checkbox is enabled only for Power Advanced Edition.
<ul style="list-style-type: none"> Server URL 	<ul style="list-style-type: none"> The access URL of the Advanced Authentication server that you want to use for multi-factor authentication.
<ul style="list-style-type: none"> Client ID 	<ul style="list-style-type: none"> 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.
<ul style="list-style-type: none"> Client Secret 	<ul style="list-style-type: none"> 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.
<ul style="list-style-type: none"> Tenant Name 	<ul style="list-style-type: none"> Specify the tenant name. The default value is TOP and supports single tenancy.
<ul style="list-style-type: none"> Test connection button 	<ul style="list-style-type: none"> Click this to test the connection between Filr and the Advanced Authentication server.

Field, Option, or Button	Information and/or Action
♦ Redirect URIs	<ul style="list-style-type: none"> ♦ 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. <p>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.</p>
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>
♦ 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.
♦ Reverse Proxy HTTP Port:	♦ If you have enabled Port Redirection and HTTP Port access in the Network dialog, specify port 80.
♦ Reverse Proxy Secure HTTP Port:	♦ If you have enabled Port Redirection and HTTP Port access in the Network dialog, specify port 443.
NetIQ Access Manager Integration	

Field, Option, or Button	Information and/or Action
<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 <code>/AGLogout</code>. <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>filr-nam-auth-class-23.2.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 34 and [Access Manager \(NAM\) and Filr Integration](#) in the *OpenText Filr 23.4: Installation, Deployment, and Upgrade Guide*.

OAuth Integration

OAuth is the industry-standard protocol for authorization and access delegation. Any application that supports the OAuth service, can be integrated with Filr. For this integration, the application has to be registered with Filr. Filr integration with applications enables the application’s users to store their data in Filr, which means the user’s data is maintained within the enterprise firewall.

Applications Supported on Filr

The applications that support OAuth 2.0, can be integrated with Filr.

Table 3-10 List of Applications that support OAuth 2.0

Applications Supported	Version
<ul style="list-style-type: none">♦ Hybrid Workspaces♦ For Filr-Hybrid Workspaces configuration, see Hybrid Workspaces	<ul style="list-style-type: none">♦ 22.7 (and higher)

Register an Application with Filr

Path: [Port 8443 Filr Admin Console](#) > **Management** > **OAuth Applications** > **Register**

Table 3-11 Using the Register New Application dialog

Field, Option, or Button	Information and/or Action
<ul style="list-style-type: none">♦ Enable	<ul style="list-style-type: none">♦ Select the checkbox to enable the application.
<ul style="list-style-type: none">♦ Application Name	<ul style="list-style-type: none">♦ Enter the name of the name of the application you wish to register.
<ul style="list-style-type: none">♦ Application Admin	<ul style="list-style-type: none">♦ Enter the user id of the application's administrator. If the administrator is not a Filr user, create a new user for the application's administrator.
<ul style="list-style-type: none">♦ Redirect URLs (Comma separated values)	<ul style="list-style-type: none">♦ Enter the redirection URLs from the application to be registered for securely exchanging the authentication code and access token.♦ Check with the application's administrator for the redirect URLs.
<ul style="list-style-type: none">♦ OK	<ul style="list-style-type: none">♦ Click OK to save the application details and complete the registration.
<ul style="list-style-type: none">♦ Cancel	<ul style="list-style-type: none">♦ Click this to clear the details entered.

On registration of an application on Filr, a Client ID is generated. This client ID has to be shared with the application administrator. The application administrator has to log in to the Filr web client and provide this client ID to retrieve the client secret.

Modifying an Application Details

Path: [Port 8443 Filr Admin Console](#) > **Management** > **OAuth Applications** > *Select an application > Modify.*

Generally, the information in “[Register an Application with Filr](#)” on page 36 applies to modifying the application. You can modify all the fields, except **Application Name**.

Deleting Applications

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

When you delete an application, all the active user sessions of registered application along with the application details are removed from Filr. The registered applications can no longer access the files and folders in Filr.

Generating Client Secret

When the client ID is shared with the third party application’s administrator, the third party application’s administrator can login to Filr and generate the client secret. For the information on registering an application, see “Register an Application with Filr” on page 36.

The third party application’s administrator has to enter the client secret on the registered application portal. This completes the application registration and it can use Filr as storage repository.

To generate the client secret, perform the following steps:

- 1 Login to the Filr .
- 2 Click on the user name on the top right corner of Filr work area and select **OAuth Applications**.
- 3 Enter the application details in the **OAuth Applications** dialog.

Table 3-12 Generate Client Secret

Field, Option, or Button	Information and/or Action
♦ Password	♦ Enter your Filr password.
♦ Client ID	♦ Enter the client id shared by the Filr administrator.
♦ Get Secret	♦ Click this button to retrieve the client secret for the application.
♦ Cancel	♦ Click this button to close the OAuth Applications dialog.

- 4 Click **Copy** on the **Client Secret** dialog.
- 5 Click **Done**.

Data Leak Prevention

The Data Leak Prevention feature allows you to have control over important organizational documents and helps you adhere to data protection policies while still providing remote access to external partners and users working remotely.

NOTE: This feature is available only under the Advanced Edition license.

Policies

Data leak prevention is managed with a policy-based prevention mechanism. When a policy is applied to a file, the file will adhere to the configuration set in the policy. The policy is assigned with a set of restrictions to be honored.

Path: [Port 8443 Filr Admin Console](#) > **Management** > **Data Leak Prevention** > **Policies**.

A default policy called “Confidential” is available under the **Policies** tab. By default, the policy is in Activated status. The policy will have a color mapped to it.

Modifying a Policy

The **Modify** option allows you to edit the title of the policy and change the color mapped with the policy.

To modify the policy, perform the following:

- 1 Go to
Path: [Port 8443 Filr Admin Console](#) > **Management** > **Data Leak Prevention** > **Policies**.
- 2 Choose **Modify** from the **Options** menu of the policy.
- 3 Perform the following in the **Modify Policy** dialog box.

Table 3-13 *Modify Policy*

Field, Option, or Button	Information and/or Action
♦ Title	♦ Edit the name of the policy.
♦ Color	♦ Click this drop-down menu to choose a color.
♦ Modify	♦ Click this to save the changes.
♦ Cancel	♦ Click this to discard any changes made and close the Modify Policy dialog box.

Managing Policy

A policy will have a set of file operation restrictions. These file operations are restricted on the files to which the policy is applied.

A system-generated policy called ‘Confidential’ is available and the ‘Share Externally’ file operation restriction is mapped to this policy. When this policy is applied to a file, sharing the file with any external user is restricted (Share with external users, Share public, and Share with file links).

Path: [Port 8443 Filr Admin Console](#) > **Management** > **Data Leak Prevention** > **Policies**.

Currently you are not allowed to edit the policy configuration. You can view the file operation restriction configured to a policy.

Managing Workspace

Manage Workspace tab lists all the net folders of your organization. You can enable DLP for any netfolders listed here.

You are allowed to select a DLP policy and apply it to a workspace for which DLP is enabled.

All the built-in administrators are the default moderators. The **Moderators** section allows you to select users who have access to the workspace and make them moderators. If the DLP is enabled for a workspace and the policy is not applied at the netfolder level, then a moderator will have the policy management privileges and can apply policy to the required files in the workspace. The moderators can apply policy to files and manage them in the workspace.

To enable DLP for a workspace, perform the following:

- 1 Go to
Path: [Port 8443 Filr Admin Console](#) > **Management** > **Data Leak Prevention** > **Manage Workspace**
- 2 Perform the following steps to enable DLP for the workspace:

Table 3-14 *Managing workspace*

Field, Option, or Button	Information and/or Action
Workspace	
♦ Workspace	♦ Search and select the workspace (netfolder) from this drop-down menu. You can click the close button to clear the selection made.
♦ Enable DLP for this workspace	♦ Turn on this toggle to enable the DLP feature for the workspace.
♦ Policy	♦ Select the policy from this drop-down menu. You can click the close button to clear the selection made.
Moderators	
♦ Enable workspace Moderators	♦ Turn on this toggle to enable the Add or Remove Moderators button.
♦ Add or Remove Moderators	♦ Click this button to add users as moderators. The Add or Remove Moderators dialog box is displayed. ♦ Enter the usernames to be added as moderators for the workspace. Type the first three alphabets of a username based on the data entered, the system will search and lists the users having access to the workspace. ♦ A workspace can have only ten moderators.
♦ Save	♦ Click this to add the selected users as moderators. You can click the close button to remove the user from this section.
Existing Moderators	
	♦ The names added will appear under the Existing Moderators section. ♦ You can click the close button to remove the user and groups from this section.

Field, Option, or Button	Information and/or Action
♦ Save	♦ Click this to save the changes made under the Manage Workspace tab.
♦ Discard	♦ Click this to discard the changes made.

NOTE: ♦When the DLP is enabled and the policy is applied to a workspace, the policy is applied to all the files in the workspace. An administrator or a moderator is not allowed to remove the policy for a file.

- ♦ When the DLP is enabled and a policy is not applied to a workspace, then an administrator or a moderator can apply policy to files in the workspace.
-

For more information, see [OpenText Filr 23.4 - Frequently Asked Questions](#).

4 Access Nodes in the Clustered Deployment

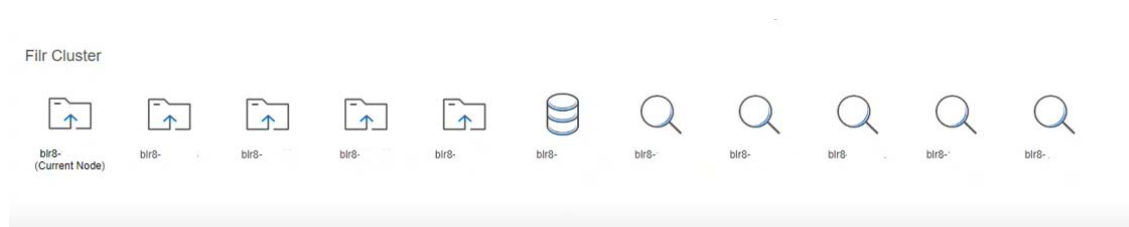
Filr clustering involves two or more Filr VAs sharing the same NFS or CIFS data storage location (/vashare). You can only create a cluster if your Filr appliances were deployed pointing to the same /vashare disk.

Filr Cluster Control

Filr now provides an option to view and access the other nodes configured in the Filr cluster. This feature lets you know the details of how many Filr nodes, Lucene nodes, and the Database appliance node are deployed in the Filr cluster. A new section called Filr Cluster on the 9443-Administrator console page provides you with a set of icons representing the different nodes configured in the Filr cluster deployment. Hence, Filr provides a single point of access to all nodes in the clustered deployment.

Path: [Port 9443 Appliance Console Filr Cluster](#)

Figure 4-1 9443 -Administrator Console- Filr Cluster



The **Filr Cluster** section displays all the nodes configured in the cluster and the database connected to the cluster. The node to which you are logged in is the current node. Click on any of the node to navigate to that node and that node becomes your currently logged in node.

NOTE: If the Postgres appliance is deployed, the database icon is displayed.

5 Filr Clustering Configuration

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

Table 5-1 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 135.
<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.

6 LDAP Servers and Synchronization

- ♦ “LDAP Configuration Dialog” on page 45
- ♦ “LDAP Server Configuration Dialog” on page 48
- ♦ “LDAP Search Dialog (User Version)” on page 52
- ♦ “LDAP Search Dialog (Group Version)” on page 55
- ♦ “Configuring LDAP ID” on page 56

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:

NOTE: It is highly recommended that internal and external users are not imported from the same LDAP server. This ensures clear isolation between external and internal LDAP sources while Filr administrators assign different Access Control Lists for Filr users.

Table 6-1 *Using the LDAP Configuration dialog*

Field, Option, or Button		Information and/or Action
LDAP Configuration dialog		
LDAP Servers tab		
♦ Add button	♦	Click this to begin the process of adding an LDAP server. The LDAP Server Configuration dialog opens.
♦ Delete button	♦	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 .

Field, Option, or Button	Information and/or Action
<ul style="list-style-type: none"> ♦ 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. <p>Or</p> <ul style="list-style-type: none"> ♦ 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> <ul style="list-style-type: none"> ♦ Users and groups that have been modified by running the LDAP sync are reported, along with information about how they have been modified.
<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. <p>Or</p> <ul style="list-style-type: none"> ♦ 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> <ul style="list-style-type: none"> ♦ 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 Creation Type 	<ul style="list-style-type: none"> ♦ This specifies the type of users imported from the LDAP server.
<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.

Field, Option, or Button	Information and/or Action
♦ 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.
<i>For user accounts provisioned from LDAP that are no longer in LDAP sub-section</i>	
♦ 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 OpenText Filr 23.4: Maintenance Best Practices Guide.</p>
♦ 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. ♦ Delete associated user workspaces: This option removes all information, Personal Storage, etc. associated with the user accounts.
<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. <p>If this is not selected, then LDAP group changes are not reflected in Filr.</p> <ul style="list-style-type: none"> ♦ This option also ensures that Filr recognizes group-based file system rights assignment updates. <p>If this is not selected, users with group-based access rights might not qualify for the roles they need to use Filr.</p>
♦ 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	


Field, Option, or Button	Information and/or Action
♦ 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 OpenText support to resolve a service request.
♦ Every day	♦ Select this to run an LDAP synchronization every day at the time or interval specified below.
♦ On selected days	♦ 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.
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	
♦ Allow log in for local user accounts (i.e user accounts not in LDAP)	♦ 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 6-2 *Using the LDAP Server Configuration dialog*

Field, Option, or Button	Information and/or Action
LDAP Server Configuration dialog	
 Server Information tab	

Field, Option, or Button	Information and/or Action
<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 <i>OpenText Filr 23.4: Maintenance Best Practices Guide</i>.</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> <code>ldaps://hostname:port_number</code></p>
<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>OpenText Filr 23.4: 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)

Field, Option, or Button	Information and/or Action
<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.
<ul style="list-style-type: none"> ◆ Create users as: 	<ul style="list-style-type: none"> ◆ Internal users is selected by default. ◆ Select the type of users you want to create: <ul style="list-style-type: none"> ◆ Internal Users: The users from the LDAP server are imported as internal users in Filr. ◆ External Users: The users from the LDAP server are imported as external users in Filr. ◆ You cannot edit this field once the server information is saved. ◆ If you select external users, the Groups tab is not displayed in the LDAP Server Configuration dialog.



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. Consult with your directory administrator to determine which attribute or attributes are used in your directory service. <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. 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. ♦ 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. For example, the mail LDAP attribute could be used so that Filr users can log in by using their email addresses. ♦ External users can only log in to Filr using their email addresses. The default value is mail. Therefore, this option is disabled when creating an external user.
<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. It is populated automatically. ♦ 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 52 wherein you can specify a context where Filr searches for LDAP users.

Field, Option, or Button	Information and/or Action
♦ Delete button	♦ 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.
OK button	♦ 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	♦ Click this to discard your changes and exit.
Groups tab	
♦ Add button	♦ Click this to open the LDAP Search Dialog (Group Version) wherein you can specify a context where Filr searches for LDAP groups.
♦ Delete button	♦ 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	♦ Click OK to save the LDAP server configuration.
Cancel button	♦ 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 6-3 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).

Home-Directory Net Folder Configuration sub-section

NOTE: This configuration is not applicable for external users.



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 79 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 81.
<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 81.

Field, Option, or Button	Information and/or Action
<ul style="list-style-type: none"> ♦ 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 81.
<ul style="list-style-type: none"> ♦ 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 6-4 Using the LDAP Search dialog (Group Version)

Field, Option, or Button	Information and/or Action
 LDAP Search dialog (Group Version)	
<ul style="list-style-type: none"> ♦ 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>
<ul style="list-style-type: none"> ♦ 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).

Configuring LDAP ID

Hide the user IDs of the LDAP users

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`.

User IDs are no longer displayed in the Web client Address Book Search, Show People tab, and so on.

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

Disable Address Book Search for external LDAP users

This setting can prevent external LDAP users from appearing in the Share dialog Address book search.

A new parameter `external.ldap.user.disable.search` in `ssf-ext.properties` is added to control the behavior of share dialog address book search suggestions for external LDAP users.

- 1 In the `/opt/novell/filr/apache-tomcat/webapps/ssf/WEB-INF/classes/config/ssf-ext.properties` file, set the `external.ldap.user.disable.search` parameter to `true`.

Search suggestions will only be displayed for internal users. When you search for external LDAP users in the Share dialog, you have to enter the complete email address to find the desired recipient.

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

7 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 100 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 7-1 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.

While installing CE, ensure that it is installed in the same domain where Filr is installed. For both Filr and CE, at each level, domain names should be the same. For example, top-level domains (such as “.com”), second-level domains (such as “abc.com”), and lower-level domains, also called sub-domains (such as “support.a.com”).

For more information, see [Content Editor](#) .

Table 7-2 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>
NOTE: This option is available with CE 1.0.1 and later versions.	

Self Signed Certificate

If the user is using a self signed certificate, then the self signed certificate needs to be downloaded from the Filr Appliance and exported to the Content Editor Appliance.

To export the self signed certificate from Filr, perform the following steps:

- 1 **Path:** [Port 9443 Appliance Console](#) > **Digital Certificates**
- 2 Select **Web Application** certificate.
- 3 Select certificate which is listed as self-signed_cert and Export as Public certificate.

To import the self signed certificate to Content Editor, perform the following steps:

- 1 **Path:** [Port 9443 Appliance Console](#) > **Digital Certificates.**
- 2 Select **JVM** Certificates.
- 3 Click file options and select Import and Trusted certificate.
- 4 Browse the certificate downloaded from Filr and import it to Content Editor

Adding Fonts

Path: [Port 9443 Appliance Console](#) > **Configuration** > **Custom Fonts**

You can upload new fonts and use them in the Content Editor. You can either upload a font file (.tff or .otf) or upload a .zip file having multiple font files. If the user is already editing a file, then reload the Content Editor page for the newly added fonts to appear in the **Fonts** drop-down menu.

Figure 7-1 Upload Custom Fonts



Table 7-3 Uploading Custom Fonts

Field, Option, or Button	Information and/or Action
◆ Path to font file	◆ Enter the path of the font file or click Browse or select the font file file that you want to add to the Content Editor. Click this to choose the font file (.tff or .otf .zip) file that you want to add to the Content Editor.
◆ Install	◆ Install button. Click this to install the font file that you have selected.

Dashboard

The Dashboard is used for monitoring system utilization and performance of Content Editor. You can do live monitoring of all the user sessions running on Content Editor.

Perform the following steps, to view the dashboard:

- 1 **Path:** [Port 9443 Appliance Console](#) > **Dashboard**
- 2 Specify the credentials. The username is 'cool' and the password is the the vaadmin password.

You can view the list of live documents opened, total users, memory consumption, document URLs with the number of users viewing that document. You can also end the sessions directly from the panel which results in closing the socket connection to the respective document.

Figure 7-2 Dashboard Monitor



8 Licensing

- ♦ “Installing/Updating the Filr License” on page 61
- ♦ “Viewing Filr License Details” on page 61

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 8-1 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 SLD) to your management workstation. NOTE: If the license is not available, contact OpenText 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 8-2 *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. Your contract contains details. Internal users might or might not be restricted; external (Filtr administrator-created) users are not restricted.♦ 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 61.

9 Logging and Monitoring

- ♦ “Accessing Filr System Log Files” on page 63
- ♦ “Automatically Applying Deferred Search Logs” on page 63
- ♦ “Generating Filr-Monitoring Reports” on page 64
- ♦ “Logging All HTTPS Traffic” on page 71
- ♦ “Managing Audit Trail Logs of Database Activity” on page 72
- ♦ “SIEM Integration” on page 72

Accessing Filr System Log Files

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

Table 9-1 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 9-2 The Configure Update Logs dialog

Field, Option, or Button	Information and/or Action
♦ Automatically Apply Deferred Update Logs in Background	IMPORTANT: ♦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.

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 9-3 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. A few reports are displayed in the Reports window.♦ The default file name for CSV-format reports is <code>report.csv</code>. If you create multiple reports without manually renaming them, the default file name is incremented—<code>report (n).csv</code>.♦ CSV-format reports are saved in the default download directory for the browser being used.
♦ 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 65](#)
- ♦ [“Data Quota Exceeded Report” on page 65](#)
- ♦ [“Data Quota Highwater Exceeded Report” on page 65](#)
- ♦ [“Disk Usage Report” on page 66](#)
- ♦ [“Email Report” on page 66](#)
- ♦ [“External User Report” on page 67](#)
- ♦ [“File Block Report” on page 67](#)
- ♦ [“Filr Outlook Report” on page 68](#)

- ♦ “License Report” on page 68
- ♦ “Login Report” on page 69
- ♦ “Orphaned User Share Report” on page 69
- ♦ “System Error Logs Report” on page 70
- ♦ “User Access Report” on page 70
- ♦ “User Activity Report” on page 70
- ♦ “XSS (Cross-Site Scripting) Report” on page 71

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 not effect.
To set a quota for individual users, see [Table 17-2, “Using the Personal Storage \(data quota\) dialog,” on page 110.](#)
 - ♦ **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 17-2, “Using the Personal Storage \(data quota\) dialog,” on page 110.](#)
 - ♦ **Default Data Quota (MB):** Displays the site-wide default quota.
For information on how to set a default data quota, see [Table 17-2, “Using the Personal Storage \(data quota\) dialog,” on page 110.](#)

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 17-2, "Using the Personal Storage \(data quota\) dialog," on page 110.](#)
 - ♦ **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 17-2, "Using the Personal Storage \(data quota\) dialog," on page 110.](#)
 - ♦ **Default Data Quota (MB):** Displays the site-wide default quota.
For information on how to set a default data quota, see [Table 17-2, "Using the Personal Storage \(data quota\) dialog," on page 110.](#)

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, 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 *OpenText Filr 23.4: 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 Filr” in the [Novell Support Knowledgebase](#).

Logging All HTTPS Traffic

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

Table 9-4 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 70.)</p>

Managing Audit Trail Logs of Database Activity

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

Table 9-5 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 and SIEM event logs 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 64.)◆ The Filr desktop application relies on audit trail data when doing full synchronizations.

SIEM Integration

SIEM integration with Filr has made Filr more secure and robust. Filr Administrator can enable or disable the SIEM services on Filr. For more information on SIEM integration, see [SIEM Integration with Filr](#).

SIEM Configuration Dialog

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

Table 9-6 SIEM Configuration Dialog

Field, Option, or Button	Information and/or Action
♦ Enable SIEM	<ul style="list-style-type: none">♦ By default, this checkbox is disabled.♦ Selecting this, CEF events are generated for login and user activities.
♦ Server URL where Zookeeper and Kafka services are running	<ul style="list-style-type: none">♦ 127.0.0.1:9092 is autopopulated. The IP address of the server where Zookeeper and Kafka services are running.
♦ Check Services	<ul style="list-style-type: none">♦ Click this to check if the Zookeeper and Kafka services are running.

10 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 75](#)
- ♦ [“Adding and Modifying Zones” on page 75](#)
- ♦ [“Viewing Zones Information” on page 77](#)

Managing Zones

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

Table 10-1 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 75](#)
- ♦ [“Modifying a Zone” on page 76](#)
- ♦ [“Deleting Zones” on page 77](#)

Adding a Zone

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

Table 10-2 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 10-3 *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 10-4 *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.

11 Net Folder Servers

- ♦ “Creating and Managing Net Folder Servers” on page 79
- ♦ “Enabling Just-in-Time-Synchronization for Filr and eDirectory Rights Usage for OES” on page 84
- ♦ “Proxy User Identities” on page 85

Creating and Managing Net Folder Servers

- ♦ “Manage Net Folder Servers Dialog” on page 79
- ♦ “Creating a Net Folder Server” on page 79
- ♦ “Editing an Existing Net Folder Server” on page 83
- ♦ “Deleting a Net Folder Server” on page 84

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 11-1 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 11-2 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), 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 (With CIFS) 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), 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 86.

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, 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, 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, OpenText 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” on page 84.</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 95).</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 81](#).

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 79](#) applies to the Edit Net Folder Server dialog, with the following exceptions:

- ◆ The **Name** cannot be modified
- ◆ Do not change the **Server Type**.

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

If you have migrated data to a new back-end file server, you must create a new Net Folder Server.

- ◆ Consult with OpenText Support before changing the **Server Path**.

Deleting a Net Folder Server

Refer to the information for the **Delete** button in [Table 11-1 on page 79](#).


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

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



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

Table 11-3 *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. <p>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.</p>

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"> ◆ 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 86](#)
- ◆ [“Creating Proxy Identities” on page 86](#)
- ◆ [“Modifying Proxy Identities” on page 86](#)

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 11-4 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 11-5 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 11-6 *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.

12 Net Folders

- ♦ “Managing Net Folders” on page 89
- ♦ “Creating and Modifying Net Folders” on page 90

Net Folders are connections to specific directories within your Net Folder Servers. You can synchronise Net Folders on a schedule that is independent of the Net Folder Server schedule.

Managing Net Folders

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

Table 12-1 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 90](#)
- ♦ [“Modifying a Net Folder” on page 94](#)
- ♦ [“Deleting a Net Folder” on page 94](#)

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 12-2 *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 79 .
♦ 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 79, 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, OpenText recommends “Dedicating a Filr Appliance to Indexing and Net Folder Synchronization” as explained in the <i>OpenText Filr 23.4: 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” on page 84.</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. You can specify the following types of users, groups, and Organization Units (OUs) for granting rights: <ul style="list-style-type: none"> ♦ Individual users (imported from the LDAP directory) ♦ Groups (either imported from the LDAP directory or that have been created in Filr) <p>NOTE: Users (in the group) created in Filr will not have access to files and folders on the Net Folder.</p> ♦ 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. 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. If you select have selected users or groups that don't currently have access rights on the file system, they see only folder names.
<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>OpenText Filr 23.4: 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>OpenText Filr 23.4: 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 79), 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 90](#) 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 12-1, “Using the Manage Net Folders dialog,” on page 89](#).

13 Net Folder System-Level Synchronization

- ♦ “Enabling and Tuning Net Folder Synchronization” on page 95
- ♦ “Just-in-Time Synchronization” on page 96

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 13-1 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 13-2 *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” on page 84
♦ Enable/Disable JITS for a Net Folder Server	♦ “Enable Just-in-Time synchronization” on page 83
♦ Enable/Disable JITS on a Net Folder	♦ “Enable Just-in-Time synchronization” on page 91
♦ Enable/Disable JITS on a user’s Home folder	♦ “Home Folder button” on page 163

14 Network Infrastructure

- ♦ “Changing Network Settings” on page 97
- ♦ “Network Configuration” on page 98
- ♦ “Port Numbers” on page 100

Changing Network Settings

The settings in this dialog are set during initial deployment.

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

Table 14-1 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.
Proxy Settings	

Field, Option, or Button	Information and/or Action
Use a Proxy ...	<ul style="list-style-type: none"> Select this checkbox if you want to configure a forward proxy server for the appliance.
Proxy URL:	<ul style="list-style-type: none"> The URL address of the proxy server to be used, including the port.
Username:	<ul style="list-style-type: none"> If required, the username for accessing the proxy server
Password:	<ul style="list-style-type: none"> The password for the username.
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 14-2 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 34.</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 100 for more information about port numbers in Filr.</p>

Field, Option, or Button	Information and/or Action
♦ HTTPS Port:	<p>♦ HTTPS Port: The default secure HTTP port for Filr is 8443. As a best practice, do not change this from the default.</p> <p>See “Port Numbers” on page 100 for more information about port numbers in Filr.</p>
♦ AJP Port:	<p>♦ If the AJP connector is listening on port 0.0.0.0, then to avoid the ghostcat vulnerability, a new attribute is added to the AJP Connector in the <code>/opt/novell/filr/apache-tomcat/conf/server.xml</code> file:</p> <ul style="list-style-type: none"> ♦ <code>address="0.0.0.0"</code> ♦ <code>secretRequired="true"</code> ♦ <code>secret="changeit"</code> <p>The secret value should be changed to a complicated value and shared with reverse proxy.</p> <p>♦ For an explanation of the Apache JServ Protocol port, see The AJP Connector (https://tomcat.apache.org/tomcat-9.0-doc/config/ajp.html).</p>
♦ Session Timeout	<p>♦ 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).</p> <p>♦ 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:</p> <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	No longer used. By default, Force Secure Connection is enabled.
OK button	<p>♦ Click this to save your changes, then click Reconfigure Filr Server.</p> <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>

Field, Option, or Button	Information and/or Action
Cancel button	♦ Click this to cancel the changes you have made.

Port Numbers

Table 14-3 lists the ports that you need to take into consideration when setting up Filr. Figure 14-1 is a graphical representation of how some of the ports are used in a Filr deployment.

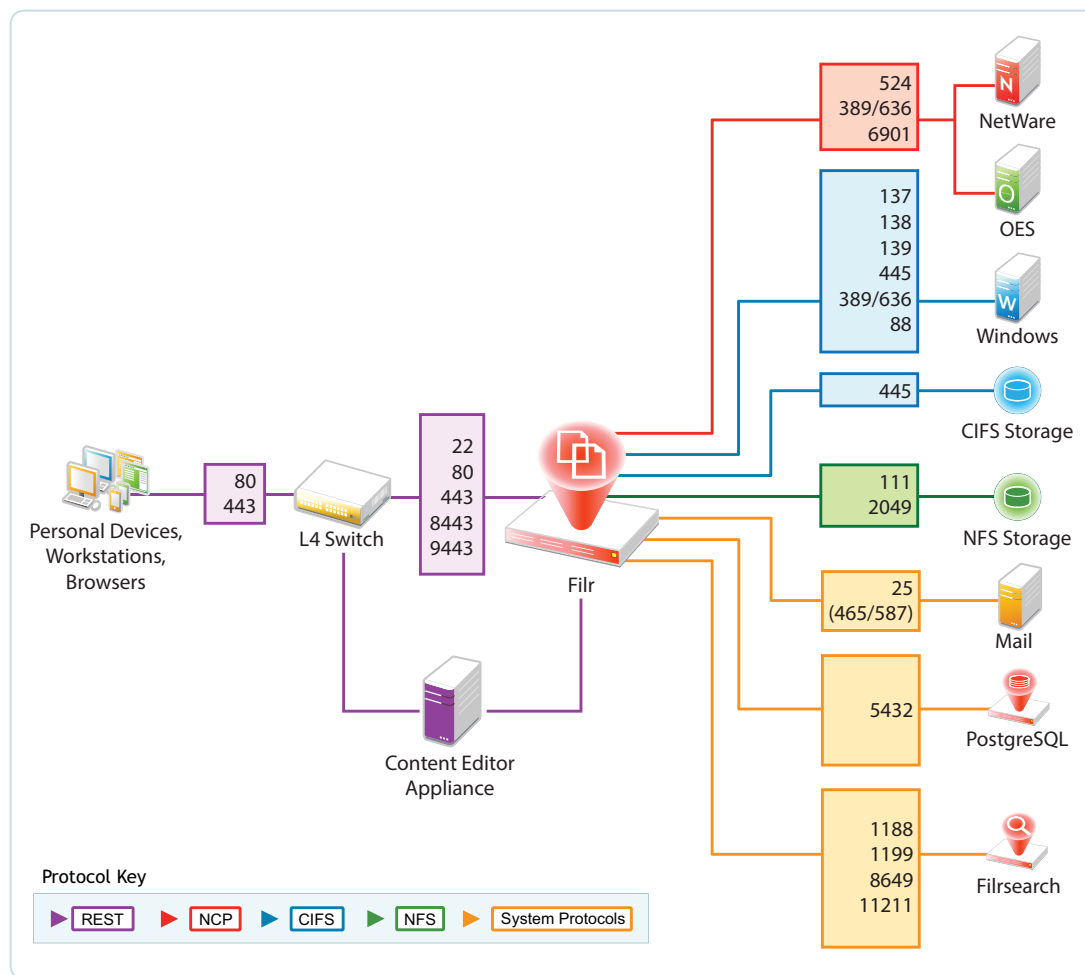
As a best practice, do not change any port numbers from the default ports.

Table 14-3 *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
8380, 8381	Default Jetty ports
1199	Lucene RMI registry port
1188	Lucene server port
5432	PostgreSQL outbound port

Port Numbers	Description
3306	MySQL outbound port
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 14-1 Filr Port Usage



15 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 *OpenText Filr 23.4: Understanding How Filr Works*

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

- ♦ [“Configuring an Email Service for Filr to Use”](#) on page 103
- ♦ [“Enabling Notifications”](#) on page 105

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 15-1 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>OpenText Filr 23.4: 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 105). 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 15-2 *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.

16 Performance Tuning

- ♦ [“Changing Configuration Settings for Requests and Connections” on page 107](#)
- ♦ [“Changing JVM Configuration Settings” on page 108](#)

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 16-1 *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 16-2 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 OpenText Filr 23.4: 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: 12g♦ JVM Max Heap Size: Increase or decrease as needed. Default: 12g♦ 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.

17 Personal Storage and Home Folders

- ♦ “Enabling Personal Storage for Users and Groups” on page 109
- ♦ “Managing and Restricting Filr-Based Storage” on page 109

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 17-1 *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 OpenText Filr 23.4: 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 30-1, “Using the Users dialog,” on page 159.♦ Groups of Users: To enable or disable personal storage for groups of users, see Table 30-3, “Using the Groups dialog,” on page 163.

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.

Irrespective of who has uploaded a file, any file uploaded to a shared folder, the size of the file is attributed to the data quota of the user who has shared the folder.

Table 17-2 *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 And ◆ Enforcement of the data quotas shown for the listed users and groups ◆ 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), an information message is displayed informing the user that the data quota is nearing to exceed. <p>NOTE: This is applicable only to Web Client.</p>
<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.

18 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 OpenText Improve Filr](#)” in the *OpenText Filr 23.4: Maintenance Best Practices Guide*.

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

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

Table 18-1 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 OpenText 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 OpenText via FTP.

19 Sharing

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

- ♦ “Managing Shared Items” on page 115
- ♦ “Managing Sharing, License Terms, and Comments” on page 116

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 19-1 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 5.0 and later 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 19-2 Using the Share and Comment Settings dialog

Field, Option, or Button	Information and/or Action
Share and Comment Settings dialog	
General tab	<p>For a graphical explanation of the settings in this tab, see “The General Tab Controls All Filr Sharing” on page 120.</p> <p>NOTE: Beginning with 24.2, the Rights tab is called as General tab.</p>
<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. <p>All users in the LDAP group then have access to the item that was shared.</p>
<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. <p>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.</p>
<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. <p>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 28</p>

Field, Option, or Button	Information and/or Action
<ul style="list-style-type: none"> ◆ 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>
Share Expiry Settings	
<ul style="list-style-type: none"> ◆ Allow shares to Never expire 	<ul style="list-style-type: none"> ◆ By default, Allow shares to Never expire check box is enabled. ◆ When this option is disabled, the Never option is not displayed for a user. ◆ Share expiry is a zone-specific setting. ◆ Already shared files with Never Expire will continue to be the same even after it is disabled. When a user edits, modifies such shares or sends out a notification on that shared file/folder, expiry for those shares is defaulted to 30 days. ◆ To remove the never expire for the already shared files, the administrator can choose to run the database script to mark all shares with never expire to a predetermined expiry date. For scripts, see Setting Expiry for Shares with Never in OpenText Filr 23.4: Maintenance Best Practices Guide
Comment Settings	
<ul style="list-style-type: none"> ◆ 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 29.
File Request Settings	
<ul style="list-style-type: none"> ◆ Allow users to request files 	<ul style="list-style-type: none"> ◆ 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.
Share Link Settings	
<ul style="list-style-type: none"> ◆ Allow Share Links to be password-protected 	<p>Beginning with Filr 24.2, an Administrator can set up the Share Link Settings.</p> <ul style="list-style-type: none"> ◆ By default, Allow Share Links to be password-protected checkbox is disabled. ◆ This feature is available only for users with an Advanced, Power External License, and Trial License. ◆ When this option is enabled, a user is presented with an option of password-protecting their Share Links at the time of creation or modification. ◆ When this option is disabled, the user is not allowed to generate any new password-protected share links. However, users can still manage existing password-protected share links.

Field, Option, or Button	Information and/or Action
♦ Apply Filr's Password Policy when setting passwords for Share Links	<ul style="list-style-type: none"> ♦ Enable the Apply Filr's Password Policy when setting passwords for Share Links checkbox to allow users to set passwords adhering to Filr's Password Policy. ♦ However, if Allow Share Links to be password-protected is disabled and Apply Filr's Password Policy when setting passwords for Share Links is enabled, you can still modify an existing secured share link, and a new password adhering to Filr's Password Policy can always be provided. For information on Filr's password policy, see "Password Security (Local and External Users)" on page 134 ♦ When both the checkboxes are disabled, the user can modify the password but will not be mandated to follow Filr's password policy while setting the password.
OK button	♦ Click this to save your changes.
Cancel button	♦ Click this to cancel the changes you have made.
Whitelist / Blacklist tab	
Mode	
♦ No restrictions	♦ Lists are ignored and users can share with any email address.
♦ Whitelist	♦ 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	♦ Use the Add and Delete buttons to add and remove email addresses from the list.
♦ Domains list	♦ 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>
OK button	♦ Click this to save your changes.
Cancel button	♦ Click this to cancel the changes you have made.
External Users Licensing Terms tab	

Field, Option, or Button Information and/or Action

♦ **Display Terms and Conditions**

- ♦ 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.

The text entered here must be HTML formatted in order to display correctly.

IMPORTANT: This does not apply to Guest (Public) access.

OK button

- ♦ Click this to save your changes.

Cancel button

- ♦ Click this to cancel the changes you have made.
-

The General 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.

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

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.

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

20 File Versioning

The File Versioning feature allows you to create, store, and maintain multiple versions of a file in the Filr. This feature is applicable only for Personal Storage Files present in My Files, Shared With Me and Shared By Me areas of any user.

User can keep track of file versions when the file versioning feature is enabled. This feature is disabled by default and applicable at a zone level. You can also configure any version of a file to be deleted automatically when it reaches the specified file age limit. This is done using File Version Aging.

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

Table 20-1 Configuration

Field, Option, or Button	Information and/or Action
Configuration	This section allows you to set the configuration for using the versioning feature.
♦ Enable File Versioning	♦ To enable file versioning, turn on this toggle. This allows the users to create and maintain multiple versions of a file.
♦ Discard	♦ Click this button to discard the changes.
Version Cleanup	This section allows you to set up the version aging for the file versions maintained in Filr.
♦ Enable File Version Aging	♦ To enable file version aging, turn on this toggle.
	♦ File versions older than the specified age in the Maximum age of a File Version will be deleted automatically and cannot be recovered. The latest version of the file is exempted from version aging and will not be deleted.
♦ Maximum age of a File Version	♦ Click the dropdown menu and select the age of a file in days.
	♦ This is the maximum age of the file version in days. The file version is deleted when it exceeds the specified age.
♦ Save	♦ Click this button to save the changes.
	♦ After the Versioning is enabled, if an already existing file in Filr is uploaded again, the system will prompt you to create a new version instead of overwriting the file.
♦ Discard	♦ Click this button to discard the changes.

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

- ♦ Enabling versioning would increase disk space usage. it is recommended to expand the vstorage/vashare size at least twice the amount of the current disk space used (a maximum of 10 times). For more information, see [Managing and Restricting File Based Storage](#). Manage the usage of disk space, by making use of data quota. For more information, see [Expanding Storage](#).
-

21 Managing Uploading of Files

The file upload size limit conserves disk space on your 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 21-1 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.

22 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 *OpenText Filr 23.4: Understanding How Filr Works*

This section covers the following:

- ♦ “[Managing Filrsearch Configuration Settings](#)” on page 127
- ♦ “[Managing the Lucene Index](#)” on page 129
- ♦ “[Managing Search Nodes](#)” on page 130
- ♦ “[Memcached \(Search Index Appliance Only\)](#)” on page 131

Managing Filrsearch Configuration Settings

For more information, see “[Filr Search Appliance—Accessibility, and Searchability](#)” in *OpenText Filr 23.4: Understanding How Filr Works*

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

Table 22-1 *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 OpenText 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 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 *OpenText Filr 23.4: Understanding How Filr Works*

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

Table 22-2 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>OpenText Filr 23.4: 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. ♦ Filr recommends setting one of the nodes to write-only and reindexing only the other node. (See “ Managing Search Nodes ” on page 130.)

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 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 *OpenText Filr 23.4: Maintenance Best Practices Guide*

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

Table 22-3 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 135](#).

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 22-4 *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.

23 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 133](#)
- ♦ [“Firewall Configuration” on page 134](#)
- ♦ [“Password Security \(Local and External Users\)” on page 134](#)
- ♦ [“Securing Memcached” on page 135](#)
- ♦ [“User Visibility” on page 135](#)
- ♦ [“Viewing, Wiping, and Disconnecting Registered Clients” on page 136](#)
- ♦ [“WebDAV Authentication Configuration Settings” on page 136](#)

Certificates

For certificate-maintenance procedures associated with this dialog, see [Certificate Maintenance](#) in the [OpenText Filr 23.4: Maintenance Best Practices Guide](#)

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

Table 23-1 *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 23-2 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 23-3 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 [OpenText Filr 23.4: 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 [OpenText Filr 23.4: Understanding How Filr Works](#).

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

Table 23-4 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 23-5](#).

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

Table 23-5 *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 23-6 The WebDAV Authentication dialog

Field, Option, or Button	Information and/or Action
<ul style="list-style-type: none">WebDAV authentication method:	<ul style="list-style-type: none">You should only change this if there is a specific reason for doing so. <p>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.</p> <p>Do not select Basic authentication unless there is a specific reason for doing so.</p> <p>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.</p> <p>Always select this type of authentication when client users are using Windows 7 as their operating system and Microsoft Office as their text editor.</p> <ul style="list-style-type: none">If you change the method, click OK, then click Reconfigure Filr Server.
<p>Filr uses the WebDAV protocol for “Edit with Application” interaction with tools such as OpenOffice and Microsoft Office.</p>	
<p>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 <i>OpenText Filr 23.4: Maintenance Best Practices Guide</i>.</p>	

24 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 24-1 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 Maria DB: Select MySQL♦ 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.

25 Storage Management

- ♦ [“Expanding Storage” on page 141](#)

Expanding Storage

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

Table 25-1 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.

26 Support Files and Online Updates

- “Managing Field Test Patches” on page 143
- “Managing Online Updates” on page 143
- “Upgrading the Services Hosted on Filr Appliance” on page 145
- “Submitting Configuration Files to OpenText Support” on page 145

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 26-1 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 26-2 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 OpenText 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 OpenText 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.

Upgrading the Services Hosted on Filr Appliance

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

NOTE: This option only appears when the service hosted on your appliance is upgraded.

Upgrading appliance-based services requires service-specific instructions

For more information about the upgrade process for your product, see the instructions in your product's online documentation.

Submitting Configuration Files to OpenText Support

Sometimes OpenText 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 26-3 *Using the Support dialog*

Field, Option, or Button	Information and/or Action
Support	
Automatically send the configuration to OpenText using FTP.	<ul style="list-style-type: none"> ♦ With this option selected, you can FTP your configuration to OpenText 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 OpenText 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 OpenText 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.

27 Changing System Services Configurations

- ♦ [“Managing System Services” on page 147](#)
- ♦ [“Shutting Down and Restarting the Appliance” on page 148](#)

Managing System Services

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

Table 27-1 *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 105](#). Click **Download** to access the `mail` file.
- ♦ **Novell FAMT:** This is the OpenText FAMT service that allows communication between Filr and the external OES or Windows 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 Appliance

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

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

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

28 Time and Locale

- ♦ [“Changing the Appliance’s NTP Configuration” on page 149](#)
- ♦ [“Setting a Default Time and Locale for Non-LDAP and External Users” on page 149](#)

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 28-1 *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 28-2 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.

29 UI Controls and Customizations

- ♦ “Email Notification Template Customization” on page 151
- ♦ “Branding the Web Client” on page 151
- ♦ “Branding the Desktop Apps (Advanced-Edition License Only)” on page 153
- ♦ “Branding the Mobile Apps (Advanced-Edition License Only)” on page 154
- ♦ “UI Language” on page 155
- ♦ “Name Completion Settings—Managing How Group Names Display in Drop-Down Lists” on page 157
- ♦ “Add Custom Templates to Filr” on page 157

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 *OpenText Filr 23.4: Maintenance Best Practices Guide* and “[Email Template Customization—A Video Walkthrough](#)” in *OpenText Filr 23.4: Maintenance Best Practices Guide*.

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

Table 29-1 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. Removing a customized template causes Filr to revert to using the default template that ships with Filr.
♦ 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 and later, ensure to reapply the Custom branding changes else the branding changes are lost and it defaults to OpenText branding.

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

Table 29-2 *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: OpenText 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, Reset 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 29-3 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 OpenText Filr 23.4: Maintenance Best Practices Guide.</p> <ul style="list-style-type: none"> ♦ Choose File button Click this to choose the .zip file that you created for your Mac workstations 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 Mac desktop application, 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 desktops as outlined in “Desktop Branding Files” in the OpenText Filr 23.4: Maintenance Best Practices Guide.</p> <ul style="list-style-type: none"> ♦ Choose File button Click this to choose the .zip file that you created for your Windows workstations 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 desktop application, click the Remove Current Branding option.

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 29-4 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 OpenText Filr 23.4: Maintenance Best Practices Guide.</p> <ul style="list-style-type: none"> ♦ Browse button <p>Click this to choose the .zip file that you created for your Android mobile devices 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 Android mobile devices, click the Remove Current Branding option.</p>
<ul style="list-style-type: none"> ♦ 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 OpenText Filr 23.4: Maintenance Best Practices Guide.</p> <ul style="list-style-type: none"> ♦ Browse button <p>Click this to choose the .zip file that you created for your iOS mobile devices 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 iOS mobile devices, click the Remove Current Branding option.</p>

UI Language

For more information about UI language settings in Filr, see “[Language Settings](#)” in the [OpenText Filr 23.4: Maintenance Best Practices Guide](#).

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

Table 29-5 Using the Default Locale dialog

Field, Option, or Button	Information and/or Action
◆ Default Locale:	<div>◆ Use this option to reset the language that you selected during the Filr configuration process.</div> <div>The following points explain more about the Default Locale setting.</div> <div>◆ Filr appliance installations run in English only.</div> <div>◆ 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.</div> <div>Your choices are:</div> <div>◆ Chinese-Simplified</div> <div>◆ Chinese Traditional</div> <div>◆ Czech</div> <div>◆ Danish</div> <div>◆ Dutch</div> <div>◆ English</div> <div>◆ French</div> <div>◆ German</div> <div>◆ Hungarian</div> <div>◆ Italian</div> <div>◆ Japanese</div> <div>◆ Polish</div> <div>◆ Portuguese</div> <div>◆ Russian</div> <div>◆ Spanish</div> <div>◆ Swedish</div> <div>◆ 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.</div> <div>The default language for non-LDAP and self-provisioned users is set in the Default User Settings dialog.</div>

Add Languages to Languages list

You can add the languages to the list of languages by performing the following steps:

- 1 Add the language and the country code to `ssf-ext.properties` file at `/opt/novell/filr/apache-tomcat/webapps/ssf/WEB-INF/classes/config/ssf-ext.properties` `i18n.locale.customized.support=<language code>`
- For example, `i18n.locale.customized.support= cy_GB` here, `cy` is the language code for Welsh language and `GB` is country code for United Kingdom.

- 2 Create and add a .json file to the following locations. The file name convention for the .json file is <language code>-<country code> .
 - ♦ (optional) `opt/novell/filr/apache-tomcat/webapps/filr/assets/i18n`
 - ♦ (mandatory) `/vastorage/filr/customLocales/` or `vashare/filr/customLocales/`
- 3 Restart the Filr server.

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 29-6 Using the Name Completion Settings dialog

Field, Option, or Button	Information and/or Action
♦ Primary display text: drop-down list	♦ 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.
♦ Secondary display text: drop-down list	♦ 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.

Add Custom Templates to Filr

By default Filr advanced edition is shipped with 7 file templates. These file templates are the combination of Microsoft Word and Libre Office extensions (.xlsx, .docx, .pptx, .odt, .ods, .odp, and .txt). You can add only one file template for each file type. An Administrator can add a new file template or replace the existing default file templates with the customized template at the location

where the default file templates are saved. A maximum of 15 templates can be added and the template name length can be up to 10 characters. The location is given below. Perform the following steps to add a customized file template.

- 1 If vashare is available on the Filr server, then add the customized template or a new file template at `vashare/filr/fileTemplates`. Else, you can add the template to `vastorage/filr/fileTemplates`.
- 2 Copy the property `create.file.extensions` from `/opt/novell/filr/apache-tomcat/webapps/ssf/WEB-INF/classes/config/ssf.properties` file to `/opt/novell/filr/apache-tomcat/webapps/ssf/WEB-INF/classes/config/ssf-ext.properties` file along with existing extensions and add the new file template extension in `create.file.extensions` property of `ssf-ext.properties` file
- 3 Restart the Filr server for the custom templates to appear in the **Create New File** template list.

NOTE: The naming convention of a file template must be `filetype.filetype` for example, `docx.docx`.

You can add any type of file template, However users can edit the template in the Filr Web Client only if the file type is supported by CE.

30 Users and Groups

- “Managing Users” on page 159
- “Managing Groups” on page 163

Managing Users

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

Table 30-1 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	<div>♦ 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.</div> <div>♦ Click Choose File, then navigate to and select the file that contains user or group profile information in XML format.</div> <div>♦ 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.</div>
♦ 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 OpenText Filr 23.4: 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 OpenText Filr 23.4: Maintenance Best Practices Guide ◆ Enable User Account: This restores access through a user account that was previously disabled. ◆ Disable/Enable Personal Storage: Chapter 17, “Personal Storage and Home Folders,” on page 109 ◆ Use Default Personal Storage Setting: Chapter 17, “Personal Storage and Home Folders,” on page 109 ◆ Disable File Downloads: “Web Browser Access—Individual Users and Groups” on page 29 ◆ Enable File Downloads: “Web Browser Access—Individual Users and Groups” on page 29 ◆ Use Default File Download Setting: “Web Browser Access—Individual Users and Groups” on page 29 ◆ Disable Web Access: “Web Browser Access—Individual Users and Groups” on page 29 ◆ Enable Web Access: “Web Browser Access—Individual Users and Groups” on page 29 ◆ Use Default Web Access Setting: “Web Browser Access—Individual Users and Groups” on page 29 ◆ 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 22 ◆ Mobile Application Settings...: “Mobile Device Access—Individual Users and Groups” on page 25 ◆ 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 136.
♦ 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 30-2 *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 30-3 *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 17, “Personal Storage and Home Folders,” on page 109 ◆ Use Default Personal Storage Setting: Chapter 17, “Personal Storage and Home Folders,” on page 109 ◆ Disable File Downloads: “Web Browser Access—Individual Users and Groups” on page 29 ◆ Enable File Downloads: “Web Browser Access—Individual Users and Groups” on page 29 ◆ Use Default File Download Setting: “Web Browser Access—Individual Users and Groups” on page 29 ◆ Disable Web Access: “Web Browser Access—Individual Users and Groups” on page 29 ◆ Enable Web Access: “Web Browser Access—Individual Users and Groups” on page 29 ◆ Use Default Web Access Setting: “Web Browser Access—Individual Users and Groups” on page 29 ◆ Desktop Application Settings...: “Desktop Access—Individual Users and Groups” on page 22 ◆ Mobile Application Settings...: “Mobile Device Access—Individual Users and Groups” on page 25 ◆ 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 157.
<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 157.
<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	♦ 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	♦ 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 50 . ♦ 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 45 . ♦ 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 53 .
♦ 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.

31 Integrating Microsoft and GroupWise with Filr

Filr now provides a plugin for integrating Filr with Microsoft Office, and Outlook. The 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.

Beginning with Filr 24.1, Filr allows you to send file attachments as Filr links. Filr lets you protect, expire, and clean up mail attachment links. In addition, you can also send links to Filr files from My Files, Shared With Me, and Net Folders in a GroupWise mail. The GroupWise plugin is provided by GroupWise. For more information, see [GroupWise Documentation](#).

After installing this plugin, Filr users can use the 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 or GroupWise 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 169](#)
- ♦ [“Managing Mail Settings” on page 169](#)

Managing Office Settings

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

For downloading the Filr Plugin for Microsoft Office and Outlook, see [OpenText Filr 23.4: Using Filr with Microsoft Office and Outlook Applications](#) guide.

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

Managing Mail Settings

Path: [Port 8443 Filr Administration Console](#) > **Management** > **Office and Mail 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 31-1 on page 170](#).

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](#).

GroupWise 23.4 extends Filr integration with email plugin APIs for enhanced collaboration. Filr allows you send file attachments as Filr links. Filr lets you protect, expire, and clean up mail attachment links. In addition, you can also send links to Filr files from My Files, Shared With Me, and Net Folders in a GroupWise mail. For more information, see [GroupWise Documentation](#).

Table 31-1 *Using the Mail Settings dialog*

Field, Option, or Button	Information and/or Action
Outlook and GroupWise Settings	
♦ Enable Filr for Outlook and GroupWise	♦ Select this to enable the plugin in Microsoft Outlook. and Groupwise. By default, this option is disabled.
Policy and Permissions	
♦ 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 and Groupwise 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.
Attachment management	
♦ Allow user to modify the policy limits	♦ Select this to enable Filr users to override the policy terms set here. By default, this option is disable.
♦ 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. ♦ File size exceeds X MB: 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.

Field, Option, or Button	Information and/or Action
<ul style="list-style-type: none"> ◆ Attachment link expires after 	<ul style="list-style-type: none"> ◆ 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.
Delete Mail attachments from Filr	<ul style="list-style-type: none"> ◆ 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.
<ul style="list-style-type: none"> ◆ Expired attachments 	<ul style="list-style-type: none"> ◆ This enables all the expired attachments for deletion when Delete Attachments is clicked. This is selected by default and cannot be deselected.
<ul style="list-style-type: none"> ◆ Attachments older than X days 	<ul style="list-style-type: none"> ◆ 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 Attachments to immediately delete attachments older than the specified days.
<ul style="list-style-type: none"> ◆ Delete Attachments 	<ul style="list-style-type: none"> ◆ Click this to immediately delete expired attachments and the attachments older than the specified days from the Filr Appliance storage.
<ul style="list-style-type: none"> ◆ Apply 	<ul style="list-style-type: none"> ◆ Click this to save your changes.
<ul style="list-style-type: none"> ◆ Close 	<ul style="list-style-type: none"> ◆ Click this to return to the previous window.

