Filr 2.0
Administration Guide

September 2016

Novell.

Contents

7 Setting Up Personal Storage   73

8 Setting Up Net Folders   77

9 Creating Groups of Users   115

About This Guide

The *Novell Filr 2.0 Administration Guide* provides the following administration information for Filr 2.0.

- Part I, "Changing Appliance Configuration Options," on page 15
- Part II, "Setting Up the Filr Site before Users Log In," on page 49
- Part III, "Maintaining the Filr Site," on page 191
- Part IV, "Interoperability," on page 285
- Part V, "Site Security," on page 291
- Part VI, "Appendixes," on page 315

Audience

This guide is intended for NovellFilr 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 *Novell Filr 2.0 Administration Guide* and other documentation, visit the Novell Filr 2.0 Documentation website (http://www.novell.com/documentation/novell-filr-2/).

Additional Documentation

You can find more information in the Novell Filr documentation, which is accessible from the Novell Filr 2.0 Documentation website (http://www.novell.com/documentation/novell-filr-2/).

Changing Appliance Configuration Options

1 Configuring and Maintaining the Filr Appliance

Before you perform any of the procedures in this section, you must do the initial configuration of the Filr appliance, as described in "Configuring a Small Deployment for the First Time" or "Configuring a Large Deployment for the First Time," in the *Filr 2.0: Installation and Configuration Guide*.

If you chose a small deployment, all vital configuration options to get the Filr system up and running were chosen for you during the initial configuration. You can change those options as discussed in this section.

If you chose a large deployment, most configuration options were chosen for you. You chose other configuration options during the initial configuration. You can change those options as discussed in this section. However, configuration options that are specific to the MySQL database appliance and the search index appliance must be reconfigured as described in "Configuring and Maintaining the Search Index Appliance" and "Configuring and Maintaining the MySQL Database Appliance," in the *Filr 2.0: Installation and Configuration Guide*.

Section 1.1, "Changing Configuration Options for the Filr Appliance," on page 18 describes how to modify configuration options for the Filr appliance. Other sections in this chapter provide additional information for each configuration option.

1.1   Changing Configuration Options for the Filr Appliance

1 Ensure that you have deployed the Novell Filr Appliance, as described in "Configuring a Small Deployment for the First Time" or "Configuring a Large Deployment for the First Time," in the *Filr 2.0: Installation and Configuration Guide*.

2 Navigate to the following URL:

`https://ip_address:9443`

Replace **ip_address** with the IP address of your Filr appliance.

3 Sign in to the Filr appliance using the `root` user and the default password that you specified during the appliance installation.

The Novell Filr Appliance landing page is displayed.
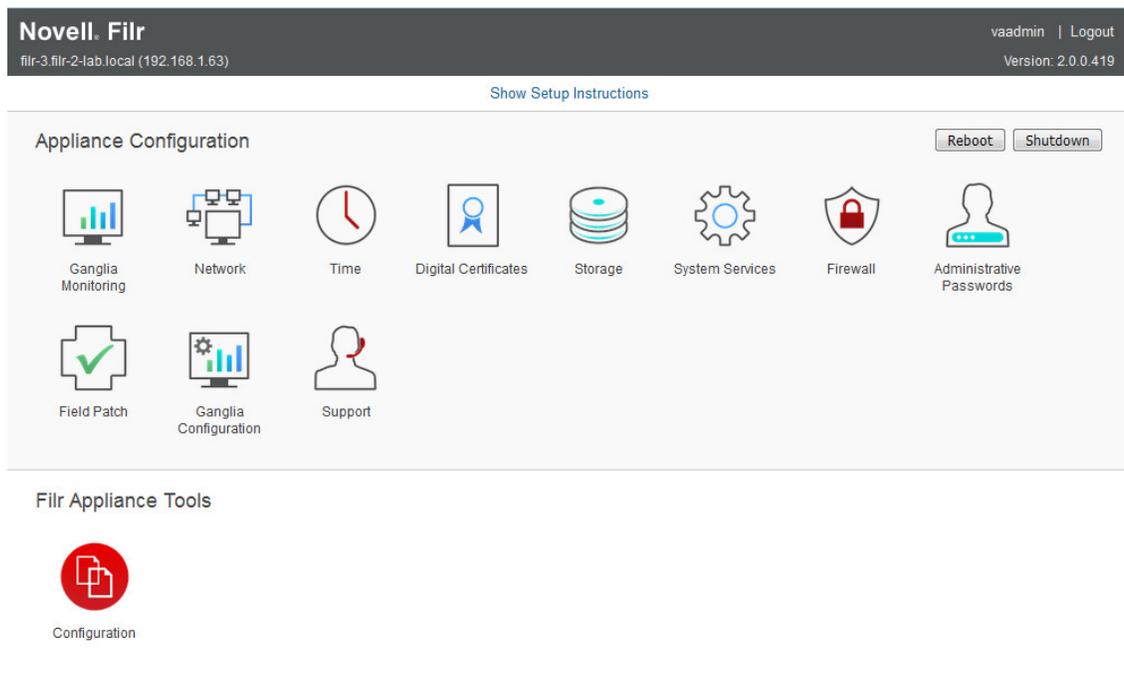
4 Click the Filr Server Configuration icon.

The Configuration page is displayed.

5 In the **Configuration** column on the left side of the page, select the setting that you want to configure.

The following configuration options are available. Click each option below for detailed information.

- Network (Section 1.2, "Network Configuration," on page 19)
- Net Folders (Section 1.3, "Net Folder Configuration," on page 23)

- Database (Section 1.4, "Database Configuration," on page 23)
- Search Appliance (Section 1.5, "Changing Your Search Index Configuration," on page 25)
- Default Locale (Section 1.6, "Language," on page 27)
- Clustering (Section 1.7, "Changing Clustering Configuration Settings," on page 28)
- Reverse Proxy (Section 1.8.3, "Changing Reverse Proxy Configuration Settings," on page 29)
- Outbound Email (Section 1.9.2, "Configuring Outbound Email Settings," on page 31)
- Requests and Connections (Section 1.10, "Changing Configuration Settings for Requests and Connections," on page 34)
- JVM Settings (Section 1.11, "Changing the JVM Configuration Settings," on page 35)
- WebDAV Authentication (Section 1.12.2, "Changing the WebDAV Authentication Configuration Settings," on page 36)
- Logging (Section 1.13, "Enabling Logging of All HTTPS Traffic," on page 37)
- HTML Viewing (Section 1.14, "Configuring Which File Formats Can Be Viewed As HTML," on page 37)
- License (Section 1.15, "Viewing and Updating the Filr License," on page 37)

6 Make any configuration changes, then click **OK**.

7 Click **Reconfigure Filr Server** for your changes to take effect.

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

1.2 Network Configuration

- Section 1.2.1, "Changing the Network Configuration Settings," on page 19
- Section 1.2.2, "Port Numbers," on page 20

1.2.1 Changing the Network Configuration Settings

The default port that is configured when you install the Filr appliance is 8443. After the initial configuration of the Filr appliance (as described in "Configuring a Small Deployment for the First Time" or "Configuring a Large Deployment for the First Time," in the *Filr 2.0: Installation and Configuration Guide*), you can make any necessary network changes.

To modify network configuration options:

1 Follow the steps in Section 1.1, "Changing Configuration Options for the Filr Appliance," on page 18.

You can modify the following configuration options:

Port Redirection: 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.

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.

For information about how to change the reverse proxy ports, see Section 1.8, "Changing Reverse Proxy Configuration Settings," on page 28.

HTTP Port: The default HTTP port is 8080. As a best practice, do not change this from the default port.

- ◆ 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).

  See Section 1.2.2, "Port Numbers," on page 20 for more information about port numbers in Filr.

Secure HTTP Port: The default secure HTTP port for Filr is 8443. As a best practice, do not change this from the default.

See Section 1.2.2, "Port Numbers," on page 20 for more information about port numbers in Filr.

Session Timeout: By default, if a user's Novell Filr 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.

Keystore File: Leave this field blank.

2 Click **OK**, then click **Reconfigure Filr Server** for your changes to take effect.

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

1.2.2 Port Numbers

Table 1-1 lists the ports that you need to take into consideration when setting up Filr. Figure 1-1 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 1-1   *Filr Port Numbers*

Port Numbers	Description
80, 443	Standard Web server ports
	For more information, see "HTTP Port:" on page 20, "Secure HTTP Port:" on page 20 and "HTTP/HTTPS Ports When You Use NetIQ Access Manager with Filr" on page 22.

Port Numbers	Description
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).
	For more information, see "HTTP Port:" on page 20, "Secure HTTP Port:" on page 20 and "HTTP/HTTPS Ports When You Use NetIQ Access Manager with Filr" on page 22.
9090, 9443	Jetty port for the appliance (Administrator Interface)
9080	Apache/HTTPD port
8005	Default shutdown port
	For an explanation of the shutdown port, see *Tomcat - Shutdown Port* (http://www.wellho.net/mouth/837_Tomcat-Shutdown-port.html).
8009	Default AJP port
	For an explanation of the Apache JServ Protocol port, see *The AJP Connector* (http://tomcat.apache.org/tomcat-6.0-doc/config/ajp.html).
22	SSH port for the appliance
111	rpcbind utility
1099	Java RMI port
4330	FAMT port
7380, 7443	Ganglia RRD-REST ports
8380, 8381	Default Jetty ports
8642, 8649, 8650, 8651, 8652	Ganglia web interface port
1199	Lucene RMI registry port
1188	Lucene server port
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

Port Numbers	Description
389	Non-secure LDAP port

Figure 1-1 *Filr Port Usage*
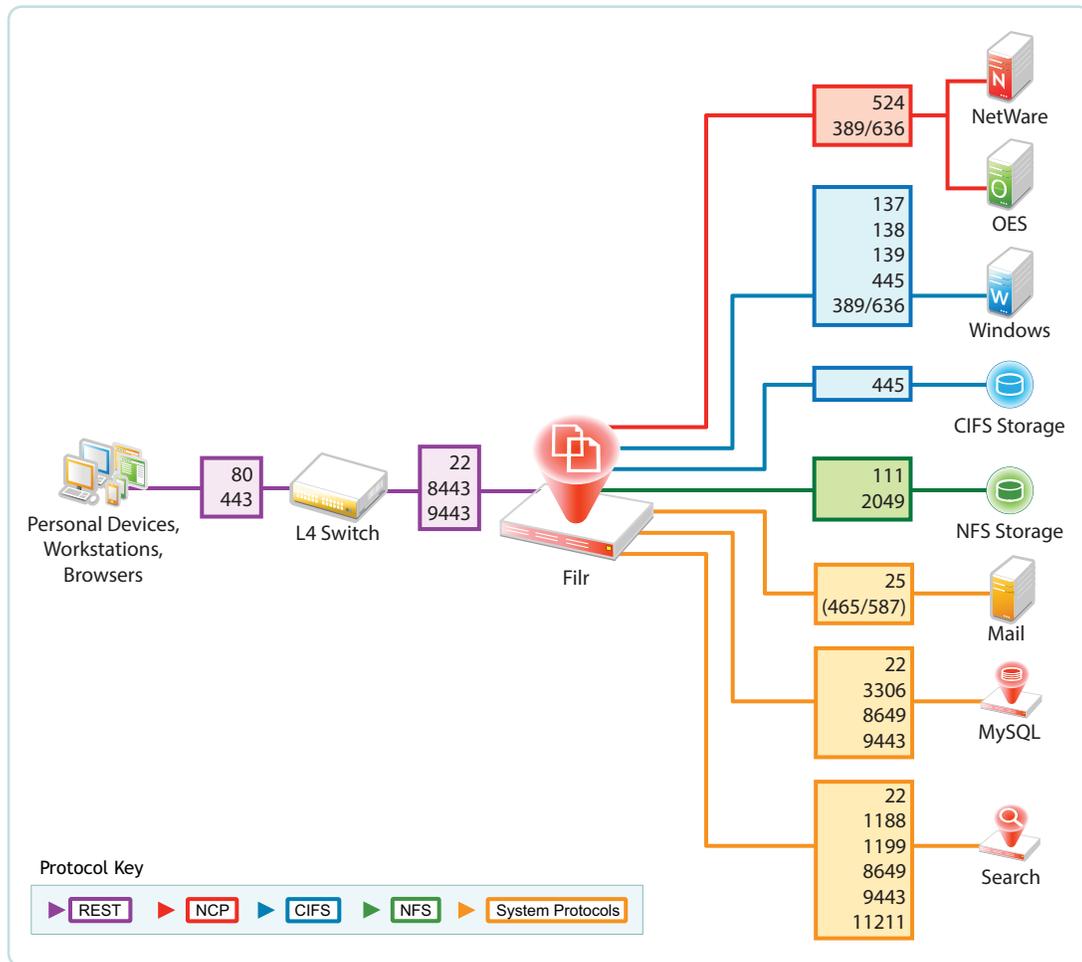
HTTP/HTTPS Ports When You Use NetIQ Access Manager with Filr

If you are fronting Filr with NetIQ Access Manager, ensure that you have configured the HTTP/
HTTPS ports.

Configuring Filr in this way configures NetIQ Access Manager to access Filr over port 80, which is the
standard port.

Port Configuration

Use the following port configuration when NetIQ Access Manager is fronting your Filr system on
Linux:

- ◆ HTTP Port: 80
- ◆ Secure HTTP Port: 443

You need to make these configuration settings in the **Reverse Proxy** section. For more information, see Section 1.8, "Changing Reverse Proxy Configuration Settings," on page 28.

1.3 Net Folder Configuration

1 Follow the steps in Section 1.1, "Changing Configuration Options for the Filr Appliance," on page 18.

You can modify the following configuration options:

The configuration options on this page affect only Full synchronizations. These settings do not affect Just-in-Time synchronizations. (For more information about the difference between Full and Just-in-Time synchronization, see Section 8.1.5, "Planning the Synchronization Method," on page 86.)

Allow Synchronization: Select this option to allow Full Synchronization for Net Folders on the appliance.

IMPORTANT: This setting must be selected for at least one Filr appliance in the cluster. If it is not, no full synchronizations can take place on the Filr system (either scheduled or manual synchronizations).

Max Simultaneous Syncs: Number of Net Folders that can be synchronized simultaneously. The default is 5.

Threads Per Sync: Number of threads that each synchronization can use. The default is 4.

For optimal performance, modify this value to be equal to the number of CPUs on the appliance, multiplied by 1.5. For example, if your appliance has 2 CPUs, change this value to 3.

The max value that you can set is the number of CPUs on the appliance multiplied by 3. For example, if your appliance has 2 CPUs, the max value is 6.

2 Click **OK**, then click **Reconfigure Filr Server** for your changes to take effect.

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

For information about how to set up Net Folders for your Filr site, see Chapter 8, "Setting Up Net Folders," on page 77.

1.4 Database Configuration

- Section 1.4.1, "Understanding Database Configuration," on page 24
- Section 1.4.2, "Changing Database Configuration Settings," on page 24
- Section 1.4.3, "Database Type," on page 25
- Section 1.4.4, "Database Location in a Small Deployment," on page 25
- Section 1.4.5, "Database Credentials," on page 25

1.4.1 Understanding Database Configuration

Novell Filr database disk space requirements are relatively modest. Files that are imported into Filr are saved in the Filr file repository.

The Filr database is primarily used for storing the following information:

- Structural information about folders and files
- Identification information about folders and files (for example, titles, descriptions, dates of creation/modification, and users associated with creation/modification)
- User profile information (for example, full name, phone number, and email address)

1.4.2 Changing Database Configuration Settings

- "Changing the Database Configuration Settings for a Small Installation" on page 24
- "Changing the Database Configuration Settings for a Large Installation" on page 24

Changing the Database Configuration Settings for a Small Installation

1. Follow the steps in Section 1.1, "Changing Configuration Options for the Filr Appliance," on page 18.

   You can modify the following configuration options:

   Database Type: Filr uses a MySQL database in a small installation. You cannot use another type of database.

   Host Name or IP Address: Host name or IP address of the MySQL appliance if MySQL is not running on the Filr appliance. In a small installation, this is `localhost`.

   Port: The JDBC URL also includes the port number on which Filr can communicate with the database server. The default port number for MySQL is 3306. Use this port number unless it is already in use by another process on the database server.

   User Name: The user name for your MySQL database. For more information, see Section 1.4.5, "Database Credentials," on page 25.

   User Password: The password for your MySQL database. For more information, see Section 1.4.5, "Database Credentials," on page 25.

2. Click **OK**, then click **Reconfigure Filr Server** for your changes to take effect.

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

Changing the Database Configuration Settings for a Large Installation

If your Filr site is configured for a large installation, it is recommended that you use your organization's existing MySQL or Microsoft SQL database as the Filr database.

Alternatively, you can use the MySQL database appliance that ships with Filr as the Filr database. You modify the configuration settings of the MySQL database appliance as described in "Configuring and Maintaining the MySQL Database Appliance" in the *Filr 2.0: Installation and Configuration Guide*.

1.4.3 Database Type

Filr can be configured to use a MySQL or Microsoft SQL database in a large deployment. In a small deployment, Filr uses a MySQL database.

1.4.4 Database Location in a Small Deployment

When you install a single virtual appliance for a small deployment, all components are on the same appliance. This is the preferable location for a small deployment. The default database name is `filr`.

Database Server	Default Location
MySQL	`/vastorage/mysql`

1.4.5 Database Credentials

The MySQL database defaults to `root` for the administrative user name.

IMPORTANT: The MySQL `root` user name is not the same as the Linux `root` user on a Linux appliance.

1.5 Changing Your Search Index Configuration

1.5.1 Understanding Indexing

The search index is responsible for indexing all data on the Filr site so that Filr users can easily use the Search feature to retrieve the information that they need. Text posted in file metadata (such as a file description) is easy to index, because the formatting is simple. However, text within a file itself arrives in many different file formats, many of which require conversion before the text in the files can be indexed. Therefore, the search index is dependent on the available file conversion technology in order to perform its indexing function. For information about the file viewers that Filr uses, see "File Viewer Information" in the *Filr 2.0: Installation and Configuration Guide*.

The search index provides additional services on your Filr site in addition to indexing. In fact, you cannot access your Filr site if the search index is not running. For this reason, Novell Filr provides multi-server configuration options.

1.5.2 Changing Search Index Configuration Settings

1 Follow the steps in Section 1.1, "Changing Configuration Options for the Filr Appliance," on page 18.

You can modify the following configuration options for the Lucene search index:

Configuration Type: Select from the following configuration types:

- ◆ **Local:** This is the default configuration type for a small Filr deployment, when the Lucene search index, the MySQL database, and the Filr software are running on the same virtual machine.
- ◆ **Server:** Select this option in a large Filr deployment when only one Lucene search index is running as a stand-alone appliance.
- ◆ **High Availability:** Select this option in a large Filr deployment when two Lucene search indexes are running as stand-alone appliances.

  For a high availability Lucene search index deployment:

  1. Specify a user name and password for the Lucene service. This user name and password applies to all Lucene search indexes in the system:

     Lucene User Name: (This option must be set in the configuration for both **Server** and **High Availability** Lucene configurations.) The default name is `lucene service` 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: (This option must be set in the configuration for both **Server** and **High Availability** Lucene configurations.) Specify the password for the Lucene user.

  2. Click **Add**, specify the information for the first Lucene index appliance, then click **OK**.

  3. Click **Add**, specify the information for the second Lucene index appliance, then click **OK**.

Name: Specify a name for the Lucene search index appliance. (This option is visible only when **Configuration Type** is set to **High Availability**.)

In a clustered Filr deployment with multiple Filr appliances, the name that you specify for a specific search index node must be the same for that same node on each Filr appliance in the cluster. For example, if from one Filr appliance you give Search Index Node A (which has the DNS name of `filr.mycompany.com`) the name `filr_index1`, then you must give Search Index Node A this same name (`filr_index1`) from each of the Filr appliances in the cluster.

Description: Specify a short description for the Lucene appliance. (This option is visible only when **Configuration Type** is set to **High Availability**.)

Host Name: This is `localhost` if your **Configuration Type** is **Local**. If your **Configuration Type** is **Server** or **High Availability**, use this field to specify the host name or IP address of the appliance where the search indexes are running. (If your **Configuration Type** is **High Availability**, click **Add** to configure multiple search indexes.)

RMI Port: When the search index is running as its own appliance, it communicates with Filr by using the RMI port. (Default 1199.) (See Remote Method Invocation (http://java.sun.com/javase/technologies/core/basic/rmi/index.jsp).) In a clustered environment where you are running multiple search index servers, ensure that each Lucene index server is running on the same ports. Novell recommends that you do not change this port from the default of 1199.

Lucene User Name: (This option must be set in the configuration for both **Server** and **High Availability** Lucene configurations.) The default name is `lucene service` 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: (This option must be set in the configuration for both **Server** and **High Availability** Lucene configurations.) Specify the password for the Lucene user.

2 Click **OK**, then click **Reconfigure Filr Server** for your changes to take effect.

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

If your Filr site is configured for a large installation (your search index is a stand-alone appliance), you can make additional configuration settings for your Lucene search index appliance, as described in "Configuring and Maintaining the Search Index Appliance" in the *Filr 2.0: Installation and Configuration Guide*.

1.5.3 Running the Search Index As Its Own Appliance

If the search index requires more memory, disk space, or CPU resources than are available on the Novell Filr appliance in a small deployment, you should configure the search index to run as a separate appliance in a large deployment. For instructions, see "Creating a Large Deployment" in the *Filr 2.0: Installation and Configuration Guide*.

1.5.4 Running Multiple Search Indexes

Because the availability of the index is critical to the functioning of the Novell Filr site, you can install multiple search indexes as multiple appliances to provide high availability. For instructions, see "Installing the Search Index Appliance" in the *Filr 2.0: Installation and Configuration Guide*.

1.6 Language

The Novell Filr installation program runs in English only. When you install the Filr software, you can set the primary language to any of the following:

- Chinese-Simplified
- Chinese Traditional
- Czech
- Danish
- Dutch
- English
- French
- German
- Hungarian
- Italian
- Japanese
- Polish
- Portuguese
- Russian
- Spanish
- Swedish

Some languages have an additional distinction by locale (the country where the language is spoken).

The language you select during installation establishes the language of the global text that displays in locations where all Filr users see it, such as in the Workspace tree when you click the Workspace tree icon :

The language you select also establishes the default interface language and locale for creating new user profiles.

1.7 Changing Clustering Configuration Settings

1 Follow the steps in Section 1.1, "Changing Configuration Options for the Filr Appliance," on page 18.

You can modify the following configuration options:

Enable Clustered Environment: Select this option to enable clustering.

JVM Route: If you plan to use Apache as the reverse proxy, add a JVM route for each filr Appliance in the Cluster. Otherwise, you can leave the JVM Route field empty. The purpose of this field is to uniquely identify each Filr Appliance to Apache.

In the **JVM Route** field, specify `worker1`. On the second Filr node, in the **JVM Route** field, specify `worker2`, and so forth for each Filr node, incrementing the JVM Route setting. Each Tomcat instance should have a unique JVM Route setting.

`worker1`, `worker2`, 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.

Hibernate Caching Provider: memcached is the only option available when configuring Filr in a clustered environment.

For more information about Memcached caching, see Memcached (http://memcached.org/).

Server Address: Each Filr server in the cluster must list all of the Lucene servers (hostname or IP address) in the cluster, with each server separated by a space. For example, *lucene_hostname1 lucene_hostname2*.

Changes made to one Filr node are immediately visible in other Filr nodes.

2 Click **OK**, then click **Reconfigure Filr Server** for your changes to take effect.

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

1.8 Changing Reverse Proxy Configuration Settings

- Section 1.8.1, "Understanding Reverse Proxy and NetIQ Access Manager," on page 29
- Section 1.8.2, "Understanding How Port Redirection Affects Reverse Proxy Settings," on page 29
- Section 1.8.3, "Changing Reverse Proxy Configuration Settings," on page 29
- Section 1.8.4, "Bypassing NetIQ Access Manager to Log In to Filr and Perform Administrative Tasks," on page 30

You might need to modify the reverse proxy configuration settings for your Filr appliance for either of the following reasons:

- When you configure a reverse proxy server, such as NetIQ Access Manager

For more information about this scenario, see Section 1.8.1, "Understanding Reverse Proxy and NetIQ Access Manager," on page 29.

 ◆ If you have enabled port redirection in your network settings page (as described in Section 1.2.1, "Changing the Network Configuration Settings," on page 19)

For more information about this scenario, see Section 1.8.2, "Understanding How Port Redirection Affects Reverse Proxy Settings," on page 29.

1.8.1 Understanding Reverse Proxy and NetIQ Access Manager

NetIQ Access Manager can provide secure single sign-on access to your Novell Filr site by functioning as a reverse proxy server. When using Access Manager with Novell Filr, Access Manager 4.1.1 or later is required and is an additional add-on product. You can download the required version of Access Manager from the NetIQ Downloads site (https://dl.netiq.com/index.jsp).

For background information about setting up NetIQ Access Manager 4.1.1, see the Access Manager 4.1 Documentation website (https://www.netiq.com/documentation/access-manager-41/). For instructions specific to Filr, see Section 12.1, "Configuring a Protected Resource for a Novell Filr Server," on page 145.

After you have configured NetIQ Access Manager, you must configure your Filr site with the IP address of one or more Access Gateway servers and with the logout URL. When you configure the Filr site to use the Access Gateway, the IP addresses that you specify are the only locations from which the Filr site accepts logins. The logout URL is the location where users find themselves when they log out of the Filr site.

When you enable the Access Gateway for use with your Filr site, all Filr users must log in through the Access Gateway. It is not possible to set up the Filr site so that some users log in through the Access Gateway and some do not.

1.8.2 Understanding How Port Redirection Affects Reverse Proxy Settings

If you have enabled the reverse proxy settings in Filr (as described in Section 1.2.1, "Changing the Network Configuration Settings," on page 19) and you have an additional reverse web proxy such as NetIQ Access Manager that is servicing Filr requests, ensure that the ports that the additional proxy connects to are the same as the ports that are configured in the Filr reverse proxy settings. (This is the **Reverse Proxy HTTP port** and the **Reverse Proxy Secure HTTP Port**.)

The reverse proxy HTTP port should be set to 80, and the reverse proxy secure HTTP port should be set to 443. If the reverse proxy ports are not correct, links that are sent from Filr in email notifications are incorrect, and users are not able to access Filr.

This issue is described in Section A.4, "Email Notification URLs Are Not Working," on page 318.

1.8.3 Changing Reverse Proxy Configuration Settings

1 Follow the steps in Section 1.1, "Changing Configuration Options for the Filr Appliance," on page 18.

You can modify the following configuration options:

Host: The host name is used to build some of the URLs that are sent in notifications. It should reflect the host used to access the Filr system from any user (either an internal or external user). It is common across all the Filr Virtual Appliances, and represents the reverse proxy or L4 device that fronts the Filr Virtual Appliance.

If Access Manager is being used to front Filr, specify the NetIQ Access Manager published DNS name for Filr application in the **Host** field.

Reverse Proxy HTTP Port: Select **Enabled** if you want to use a non-secure port for the reverse proxy. Specify the port number that you want to use. You must use port 80 if you have enabled port redirection in your network settings page.

Reverse Proxy Secure HTTP Port: Specify the port number that you want to use for the secure reverse proxy HTTP port. You must use port 443 if you have enabled port redirection in your network settings page. (Port redirection allows users to access the Filr site without specifying the port number in the URL. For information about port redirection, see Section 2.2, "Changing Network Settings," on page 39.)

Enable Access Gateway: Select this option to enable the reverse proxy Access Gateway.

Access Gateway address(es): Specify the IP address of the Access Gateway that is used for the connection to the Filr server. You must specify the IP address; host names are not supported.

If the Access Gateway is part of a cluster, add the IP address for each cluster member. Wildcards such as 164.99.*.* are allowed. Separate IP addresses with a comma. For example, 172.2.3, 172.2.4.

IMPORTANT: When you specify specific IP addresses in this option, Filr access is allowed only from the specified addresses. Also, if Authorization header credentials are not present or are incorrect, the user is prompted for login using Basic Authentication.

Logout URL: Specify the URL of the published DNS name of the reverse proxy that you have specified for the ESP, plus `/AGLogout`.

You can find the domain used for the ESP by editing the LAG/MAG cluster configuration and then clicking **Reverse Proxy / Authentication**.

For example, if the published DNS name of the proxy service that you have specified for the ESP is `esp.yoursite.com`, specify the following URL:

`https://esp.yoursite.com/AGLogout`

2 Click **OK**, then click **Reconfigure Filr Server** for your changes to take effect.

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

1.8.4 Bypassing NetIQ Access Manager to Log In to Filr and Perform Administrative Tasks

To perform administrative tasks on your Filr system, you need to log in to bypass NetIQ Access Manager and log in to Filr directly as the Filr administrator.

To allow administrator access to the Filr system when your Filr system is fronted by Access Manager:

1 Add another IP address to the **Access Gateway address(es)** field, as described in Section 1.8.3, "Changing Reverse Proxy Configuration Settings," on page 29.

2 Click **Reconfigure Filr Server** for your changes to take effect.

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

3 Access this IP address that you added in Step 1 at port 8443. For example, `172.17.2.3:8443`.

1.9 Configuring Outbound Email Services

- Section 1.9.1, "Understanding Outbound Email," on page 31
- Section 1.9.2, "Configuring Outbound Email Settings," on page 31
- Section 1.9.3, "Outbound Email Protocol," on page 33
- Section 1.9.4, "Outbound Email Host," on page 33
- Section 1.9.5, "Outbound Email Authentication," on page 33

1.9.1 Understanding Outbound Email

Your Novell Filr site can be configured to send email through an existing email system or through the included Postfix SMTP outbound mail server. The following activities generate email from the Filr site:

- Filr users can subscribe to email notifications, so that they automatically receive a message whenever content of interest changes. For more information, see "Subscribing to a Folder or Filr" in "Getting Informed" in the *Filr 2.0: Web Application User Guide*.
- Filr users can configure folders that they own to send email notifications to other users. For more information, see "Configuring Folders to Send Email Notifications to Other Users" in the *Filr 2.0: Web Application User Guide*.
- Filr users can send email messages to folder contributors, as described in "Sending an Email to Folder Contributors" in the *Filr 2.0: Web Application User Guide*.
- Filr users can send notifications when a folder of file is shared, as described in "Sharing Files and Folders" in the *Filr 2.0: Web Application User Guide*.

After installation, outbound email can be disabled, enabled and customized on the Filr site, as described in Chapter 5, "Enabling and Customizing Filr's Email Services," on page 57. However, you must configure outbound email in the Filr appliance.

1.9.2 Configuring Outbound Email Settings

1 Follow the steps in Section 1.1, "Changing Configuration Options for the Filr Appliance," on page 18.

You can modify the following configuration options:

Use Local Postfix Mail Server: Select this option to use the Postfix mail server, which is the default mail system included with Filr. To use another mail system (such as GroupWise), deselect this option, then specify the appropriate information for the protocol, host, and port of the mail system that you want to use.

Protocol: Select the type of protocol your email system uses. For more information, see Section 1.9.3, "Outbound Email Protocol," on page 33.

Host: Specify the hostname of your SMTP mail server. For more information, see Section 1.9.4, "Outbound Email Host," on page 33.

Port: The port through which Filr can connect to the SMTP mail server. The default SMTP port of 25 is typically appropriate, unless the SMTP mail server requires port 465 or 587 for SMTPS connections.

Time Zone: Select the time zone that you want Filr to use when sending email messages. When the Filr site sends email notifications for scheduled events, the messages are time-stamped according to the time zone you specify here during installation. This setting allows you to use a time zone for email notifications that is different from the time zone where the server is located. For more information, see Section 1.9.4, "Outbound Email Host," on page 33.

User Name: Specify an email address to be used when sending outbound email. Many SMTP mail hosts require a valid email address before they establish the SMTP connection.

This user name is used to authenticate to the email server (if required), and is used as the From component of email notifications that are sent from Filr.

For more information, see Section 1.9.5, "Outbound Email Authentication," on page 33.

Password: Specify a password for the user name. Some email systems also require a password. Some do not. If authentication is required, you should also provide a password. For more information, see Section 1.9.5, "Outbound Email Authentication," on page 33.

Authentication required: Select this option to require authentication.

Allow sending email to all users: Select this option to allow users to send email to the All Users group.

By default, this functionality is not enabled. On a very large Filr site, when a user sends a message to all Filr users, a very large number of email messages is generated.

Force HTTPS links: Select this option for all links contained in outbound email messages to be secure HTTP (HTTPS) instead of HTTP.

If this option is not selected, links contained in outbound email messages match the way that the user who sends the email connects to the Filr site: if the user connects via HTTP, links are HTTP. If the user connects via HTTPS, links are HTTPS.

Enable STARTTLS: Select this option to enable STARTTLS on the Filr system. Depending on how your email application is configured, you might need to configure Filr outbound email with TLS over SMTP for secure email. Novell GroupWise, for example, can be configured to require this. If you are using GroupWise or another email application that requires this type of configuration, you can configure Filr with TLS over SMTP by enabling STARTTLS.

From email address override: Specify the email address that you want to appear in the **From** address for messages sent from the Filr site.

Use from email address override for all outbound email: Select this option to always use the address that you specified in the **From email address override** field for messages sent from Filr. (For more information about the activities that generate email from Filr, see Section 1.9.1, "Understanding Outbound Email," on page 31.)

If this option is not selected and there is an email address in the **From email address override field**, the email address is used only in messages that Filr sends out as a result of a subscription (either when you subscribe to receive email notifications about a file or folder, or another user subscribes you to receive notifications).

Connection Timeout (in seconds): Specify the amount of time before the connection times out.

2 Click **OK**, then click **Reconfigure Filr Server** for your changes to take effect.

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

1.9.3 Outbound Email Protocol

Email systems communicate by using SMTP (Simple Mail Transfer Protocol). You need to determine whether the email system that you want your Filr site to communicate with is using SMTP or SMTPS (secure SMTP).

For GroupWise, you can check how the Internet Agent is configured:

1 In ConsoleOne, browse to and right-click the Internet Agent object, then click **Properties**.

2 Click **GroupWise > Network Address**.

In the **SMTP** field, if the **SSL** column displays **Disabled**, GroupWise is using SMTP. If the **SSL** column displays **Enabled**, GroupWise is using SMTPS.

3 Click **Cancel** to close the Network Address page.

If the email system requires SMTPS, see .

1.9.4 Outbound Email Host

In order to send messages to your email system, Filr needs to know the host name of your SMTP mail server.

The default SMTP port of 25 is typically appropriate, unless the SMTP mail server requires port 465 or 587 for SMTPS connections.

If you are using GroupWise, this is the host name of a server where the Internet Agent is running. GroupWise always uses port 25, even when SSL is enabled.

When the Filr site sends email notifications for scheduled events, the messages are time-stamped according to the time zone you specify here during installation. This setting allows you to use a time zone for email notifications that is different from the time zone where the server is located. The time zone list is grouped first by continent or region, optionally by country or state, and lastly by city. Common selections for United States time zones:

Time Zone	Continent/City
Pacific Time	America/Los Angeles
Mountain Time	America/Denver
Central Time	America/Chicago
Eastern Time	America/New York

1.9.5 Outbound Email Authentication

Many SMTP mail hosts require a valid email address before they establish the SMTP connection. Some email systems can construct a valid email address if you specify only a valid user name; other email systems require that you specify the full email address for successful authentication. You should provide a user name (email address) to ensure a successful connection. Email notifications from the Filr system are sent using this email address in the **From** field.

Some email systems also require a password. If authentication is required, you should also provide a password.

Consider the following tips when using GroupWise or Exchange:

- ◆ "GroupWise" on page 34
- ◆ "Exchange" on page 34

GroupWise

If you are using Novell GroupWise, the GroupWise Internet Agent does not require authentication in order to receive inbound messages. However, the /forceinboundauth startup switch is available for use in the Internet Agent startup file (`gwia.cfg`) to configure the Internet Agent to refuse SMTP connections where a valid email user name and password are not provided. The Internet Agent can accept just the user name or the full email address.

Exchange

If you are using Microsoft Exchange and 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 `ms-Exch-SMTP-Accept-Any-Sender`.

This is required because Exchange, by default, enforces that the From address of outbound emails match the exchange user who you configured for authentication, and many emails that are sent from Filr use the From address of the Filr user who is performing an action.

1.10 Changing Configuration Settings for Requests and Connections

You can configure the number of client requests and database connections that Filr is able to support.

If you have an extremely large Filr site and you need to make numerous client requests and database connections, you might see improved performance by increasing these settings.

1. Follow the steps in Section 1.1, "Changing Configuration Options for the Filr Appliance," on page 18.

   You can modify the following configuration options:

   Max Threads: The maximum number of simultaneous client request threads that Filr is able to support. The default is 250 threads.

   Max Active: The maximum number of database connections that can be allocated from this pool at the same time. The default is 300.

   Max Idle: The maximum number of database connections that can be idle in this pool at the same time. The default is 300 connections.

   Scheduler Threads: The size of thread pool used for background execution of scheduled tasks. The default is 20.

   Max REST Requests (upload/download): This is the max number of concurrent upload and download requests made by the Filr desktop and mobile applications. Specifying a max number of concurrent REST requests ensures that the Filr server does not exceed capacity. If the max number is reached and requests continue to be made, the server responds to requests when it is no longer busy. The default is 50.

2 Click **OK**, then click **Reconfigure Filr Server** for your changes to take effect.

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

1.11 Changing the JVM Configuration Settings

Depending on the amount of memory allocated to your appliance (see "Memory Requirements" in the Filr 2.0: Installation and Configuration Guide), you might need to adjust your Java heap settings as described in this section.

1 Follow the steps in Section 1.1, "Changing Configuration Options for the Filr Appliance," on page 18.

You can modify the following configuration options:

JVM Min Heap Size: The default JVM minimum heap size is 5 GB. You can increase or decrease this value as needed.

JVM Max Heap Size: The default JVM minimum heap size is 5 GB. You can increase or decrease this value as needed.

The values for the JVM heap size must end with g or m, and cannot contain fractional values. For example, if you want your JVM minimum heap size to be 1.5 GB, you must specify `1536m`.

It is recommended that the **JVM Min Heap Size** and **JVM Max Heap Size** values be the same. If the values differ, Java begins with the minimum, and if it requires more resources, proceeds up to the maximum. This process can be resource intensive and degrade system performance.

Allow generation of a system dump on a user signal: Select this option to configure Filr to generate 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.

Java Home: Displays the path to the JavaHome variable. This cannot be changed.

2 Click **OK**, then click **Reconfigure Filr Server** for your changes to take effect.

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

1.12 Changing WebDAV Authentication Configuration Settings

- Section 1.12.1, "Understanding WebDAV," on page 35
- Section 1.12.2, "Changing the WebDAV Authentication Configuration Settings," on page 36
- Section 1.12.3, "Choosing the WebDAV Authentication Method," on page 36

1.12.1 Understanding WebDAV

WebDAV is a standard collaborative editing and file management protocol. Novell Filr relies on the WebDAV protocol for Edit-in-Place to use tools such as OpenOffice and Microsoft Office to edit documents on the Filr site.

IMPORTANT: When Filr users are running Windows 7 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 Chapter 15, "Configuring Filr to Support WebDAV on Windows 7," on page 179.

1.12.2 Changing the WebDAV Authentication Configuration Settings

1. Follow the steps in Section 1.1, "Changing Configuration Options for the Filr Appliance," on page 18.

   You can modify the following configuration option:

   WebDAV authentication method: Select either **Basic** or **Digest**. The WebDAV authentication method determines how user credentials are passed from Filr to the WebDAV server. For more information, see Section 1.12.3, "Choosing the WebDAV Authentication Method," on page 36.

2. Click **OK**, then click **Reconfigure Filr Server** for your changes to take effect.

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

1.12.3 Choosing the WebDAV Authentication Method

The WebDAV authentication method determines how user credentials are passed from Filr to the WebDAV server. Filr supports two types of WebDAV authentication methods:

   ◆ "Choosing Basic Authentication" on page 36
   ◆ "Choosing Digest Authentication" on page 36

Choosing Basic Authentication

Basic authentication encodes the user name and password with the Base64 algorithm. The Base64-encoded string is unsafe if transmitted over HTTP, and therefore should be combined with SSL/TLS (HTTPS).

Digest authentication is the default. Do not select Basic authentication unless there is a specific reason for doing so.

Choosing Digest Authentication

Digest authentication 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.

Select this type of authentication when client users are using Windows 7 as their operating system and Microsoft Office as their text editor.

1.13 Enabling Logging of All HTTPS Traffic

By default, non-https logging is always enabled on the appliance. (For information about how to access the Filr log file, see Section 28.4, "Accessing the Filr Log File," on page 282.)

The option to **Enable host access logging** can be enabled in addition to regular Filr logging. When this option is enabled, a single file is generated that contains log information for all https traffic. If this file grows too large, disable this option.

To configure the Filr system to create a single log file that contains log information for all https traffic:

1 Follow the steps in Section 1.1, "Changing Configuration Options for the Filr Appliance," on page 18.

2 Select **Enable host access logging**.

3 Click **Reconfigure Filr Server** for your changes to take effect.

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

1.14 Configuring Which File Formats Can Be Viewed As HTML

Many file formats in Novell Filr can be viewed as HTML by default, as described in "Viewing the File in Your Web Browser" in the *Filr 2.0: Web Application User Guide*. File formats that can be viewed as HTML by default are: `.123, .bmp, .db, .doc, .docx, .dotm, .drw, .dxf, .htm, .html, .lwp, .odf, .odf, .odp, .ods, .odt, .pct, .ppt, .pptx, .prz, .qpw, .rtf, .sdw, .shw, .sxw, .tif, .txt, .vsd, .wpd, .xls, .xlsx, .sxi`

Some file formats, such as `.pdf` files, cannot be viewed as HTML by default. This is because the quality of these files is lessened when viewed as HTML. However, if you choose, you can enable non-default file formats, such as `.pdf` files, to be viewed as HTML.

Not all file formats can be enabled to be viewed as HTML in Filr, but many can be. If you are unsure whether Filr supports a particular file format to be viewed as HTML, try it and see.

1 Follow the steps in Section 1.1, "Changing Configuration Options for the Filr Appliance," on page 18.

2 Select **HTML Viewing**.

3 In the **Additional HTML Extensions** field, specify the extensions that you want to be able to be viewed in HTML.

4 Click **OK**.

1.15 Viewing and Updating the Filr License

You can view information about your current Filr license, as well as update your Filr license.

Filr ships with a 60-day evaluation license. You need to update this license to a full product license.

IMPORTANT: If you are running Filr in a clustered environment, you must update the license for each Filr appliance in the cluster.

The database and search index appliances do not require a license.

1 Follow the steps in Section 1.1, "Changing Configuration Options for the Filr Appliance," on page 18.

   On the License page, the **Current License Information** section displays information about your current Filr license, including the date it was issued and the number of days from the issue date that the license is valid.

2 To update your Filr license:

   2a In the **Update License** section, browse to and select a new valid `license-key.xml` file that you have previously downloaded to your workstation.

   You can obtain a new valid license key from the Novell Customer Center (NCC) (http://www.novell.com/customercenter/).

   2b Reconfigure the Filr server by clicking the **Reconfigure Filr Server** button that appears in the **Configuration** column.

2 Configuring and Maintaining the Novell Appliance

The Novell Appliance is the operating system that the Filr, MySQL, and search index applications run on. You might need to change certain configuration settings for the Novell Appliance, such as administrative passwords to the appliance, network settings, and certificate settings.

2.1 Changing Administrative Passwords

1 Log in to the Novell appliance at https://*server_url*:9443.

2 Click **Administrative Passwords**.

3 Specify new passwords for the root and vaadmin administrators.

   If you are changing the root password, you must first specify the current root password.

4 (Optional) Select or deselect **Allow root access to SSH**. When this option is selected, the root user is able to SSH to the appliance. If this option is not selected, only the vaadmin user can SSH to the appliance.

   SSH is disabled by default. For information about how to start SSH on the appliance, see Section 2.7, "Changing System Services Configuration," on page 43.

5 Click **OK**.

2.2 Changing Network Settings

1 Log in to the Novell appliance at https://*server_url*:9443.

2 Click **Network**.

3 In the **DNS Configuration** section, you can modify the name servers, search domains, and gateway settings for your Novell appliance network.

If the **Search Domains** field is left blank, it is auto-populated with the domain of the appliance hostname. For example, if the hostname of the appliance is `filr.mycompany.com`, the domain is auto-populated with `mycompany.com`.

4 In the **NIC Configuration** 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.)

    4a In the **NIC Configuration** section, click the ID of the NIC.

    4b 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

    4c Click **OK**.

5 (Optional) In the **Appliance Administration UI (port 9443) Access Restrictions** 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 any network to access the Filr site.

6 Click **OK**.

2.3 Changing Time Configuration

1 Log in to the Novell appliance at https://*server_url*:9443.

2 Click **Time**.

3 As necessary, change the following time configuration options:

NTP Server: Specify the NTP server that you want to use for time synchronization.

Region: Select the region where your Novell Appliance is located.

Time Zone: Select the time zone where your Novell Appliance is located.

4 Click **OK**.

2.4 Replacing the Self-Signed Digital Certificate for an Official Certificate

The Novell Appliance ships with a self-signed digital certificate. Instead of using this self-signed certificate, you should use a trusted server certificate that is signed by a trusted certificate authority (CA) such as VeriSign or Equifax.

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

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

NOTE: If you are using a Godaddy SSL certificate with Filr, follow the steps in "Godaddy SSL Certificates for Filr" (https://www.novell.com/communities/coolsolutions/godaddy-ssl-certificates-for-filr/) at the Novell Cool Solutions website (https://www.novell.com/communities/coolsolutions/).

2.4.1 Using the Digital Certificate Tool

Creating a New Self-Signed Certificate

1 Log in to the Novell appliance at https://*server_url*:9443.

2 Click **Digital Certificates**.

3 In the **Key Store** drop-down list, ensure that **Web Application Certificates** is selected.

4 Click **File** > **New Certificate (Key Pair)**, then specify the following information:

Alias: Specify a name that you want to use to identify and manage this certificate.

Validity (days): Specify how long you want the certificate to remain valid.

Key Algorithm: Select either **RSA** or **DSA**.

Key Size: Select the desired key size.

Signature Algorithm: Select the desired signature algorithm.

Common Name (CN): This must match the server name in the URL in order for browsers to accept the certificate for SSL communication.

Organizational Unit (OU): (Optional) Small organization name, such as a department or division. For example, Purchasing.

Organization (O): (Optional) Large organization name. For example, Novell, Inc.

City or Lacality (L): (Optional) City name. For example, Provo.

State or Province (ST): (Optional) State or province name. For example, Utah.

Two-letter Country Code (C): (Optional) Two-letter country code. For example, US.

5 Click **OK** to create the certificate.

After the certificate is created, it is self-signed.

6 Make the certificate official, as described in "Getting Your Certificate Officially Signed" on page 41.

Getting Your Certificate Officially Signed

1 On the Digital Certificates page, select the certificate that you just created, then click **File** > **Certificate Requests** > **Generate CSR**.

2 Complete the process of emailing your digital certificate to a certificate authority (CA), such as Verisign.

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

3 After you have received the official certificate and certificate chain from the CA:

3a Revisit the Digital Certificates page by clicking **Digital Certificates** from the Novell Appliance.

3b Click **File** > **Import** > **Trusted Certificate**. Browse to the trusted certificate chain that you received from the CA, then click **OK**.

3c Select the self-signed certificate, then click **File** > **Certification Request** > **Import CA Reply**.

3d Browse to and upload the official certificate to be used to update the certificate information.

On the Digital Certificates page, the name in the **Issuer** column for your certificate changes to the name of the CA that stamped your certificate.

4 Activate the certificate, as described in Section 2.4.3, "Activating the Certificate," on page 42.

2.4.2 Using an Existing Certificate and Key Pair

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

1 Go to the Digital Certificates page by clicking **Digital Certificates** from the Novell Appliance.

2 Click **File** > **Import** > **Trusted Certificate**. Browse to and select your existing certificate, then click **OK**.

3 Click **File** > **Import** > **Trusted Certificate**. Browse to your existing certificate chain for the certificate that you selected in Step 2, then click **OK**.

4 Click **File** > **Import** > **Key Pair**, then browse to and select your .P12 key pair file, specify your password if needed, then click OK.

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

5 Continue with Section 2.4.3, "Activating the Certificate," on page 42.

2.4.3 Activating the Certificate

1 On the Digital Certificates page, select the certificate that you want to make active, click **Set as Active**, then click **Yes**.

2 Verify that the certificate and the certificate chain were created correctly by selecting the certificate and clicking **View Info**.

2.5 Managing Certificates

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

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

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

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

To access the Digital Certificates tool:

1 Click **Digital Certificates** from the Novell Appliance.

2.6 Changing the Ganglia Configuration

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

1 Log in to the Novell appliance at https://*server_url*:9443.

2 Click **Ganglia Configuration**.

3 As necessary, change the following Ganglia configuration options:

Enable Full Monitoring Services: Select this option to receive and store metrics from other appliances, and to allow the Ganglia Web Interface to run on the same machine as the Filr appliance.

You might want to disable Ganglia monitoring by deselecting this option if:

- You already have a monitoring system that you plan to use for Filr.
- You plan to configure a dedicated appliance for viewing monitoring information. (You do this by selecting **Unicast** below and then specifying the DNS name or IP address of the appliance where monitoring information will be collected.)

Enable monitoring on this appliance: Select this option to enable Ganglia monitoring on this appliance.

- **Multicast:** Select this option to send monitoring information to other appliances on the network.
- **Unicast:** (Recommended) Select this option to send monitoring information to a single destination.

  Unicast mode is recommended for improving performance of the Filr system.

  Publish to: Specify the URL where Ganglia sends monitoring information when it is running in Unicast mode.

4 (Optional) Click **Reset Database** to remove all existing Ganglia metrics from this appliance.

This option is not related to the Filr database.

5 Click **OK**.

For more information about how to use Ganglia monitoring with Filr, see Section 28.1, "Monitoring Filr Performance with Ganglia," on page 265.

2.7 Changing System Services Configuration

- Section 2.7.1, "System Services and Appliance Types," on page 43
- Section 2.7.2, "Managing System Services," on page 44

2.7.1 System Services and Appliance Types

The following system services are available on the Novell appliance, depending on which appliance you are accessing.

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 Section 1.9.1, "Understanding Outbound Email," on page 31. Click **Download** to access the `mail` file.
- **Novell FAMT:** This is the Novell FAMT service that allows communication between Filr and the external OES, Windows, or NetWare file system. Click **Download** to access the `famtd.log` file.
- **MySQL:** This is the MySQL service that is running on the appliance. Click **Download** to access the `mysqld.log` file.

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

MySQL Database 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.
- **MySQL:** This is the MySQL service that is running on the appliance. Click **Download** to access the `mysqld.log` file.

2.7.2 Managing System Services

This section describes the kinds of actions you can perform in regards to these services.

Opening the Appliance Configuration Dialog

1 Log in to the Novell appliance at https://*server_url*:9443.

2 Click **System Services**.

3 You can perform various actions for system services:

Starting, Stopping, or Restarting System Services

You might want to start, stop, or restart a service. For example, you can start SSH so that you can remote into the appliance without using a VMware client.

1 Select the service that you want to start, stop, or restart.

2 Click **Action**, then click **Start**, **Stop**, or **Restart**.

3 Click **Close** to exit System Services.

Making System Services Automatic or Manual

1 Select the service that you want to make automatic or manual.

2 Click **Action**, then click **Set as Automatic**, or **Set as Manual**.

Downloading Log Files for System Services

1 In the **Log Files** column of the table, click the **download** link for the service for which you want to view log files.

The following files are available for each service:

SSH: N/A

Novell Filr: `catalina.out`, `appserver.log` (Filr appliance)

The `catalina.out` file reports all timestamps in UTC/GMT.

Jetty: `jetty.stderrout.log` (Filr, Search, and MySQL database appliances)

Postfix: `mail` (Filr appliance)

Novell FAMT: `famtd.log` (Filr appliance)

Search: `indexserver.log` (Search appliance)

MySQL: `mysqld.log` (MySQL database appliance)

Memcached: `jetty.stderrout.out` (Search appliance)

2 Click **Close** to exit System Services.

2.8 Viewing the Firewall Configuration

You can view your current firewall configuration directly from the Filr appliance:

1 Log in to the Novell appliance at https://*server_url*:9443.

2 Click **Firewall**.

Port numbers are listed with the current status of each port number. This page is not editable, but is for informational purposes.

For more information about port numbers in Filr, see Section 1.2.2, "Port Numbers," on page 20.

2.9 Managing Support Configuration Files

You can use the Novell appliance to upload configuration files to Novell Support via FTP, or to download the configuration files so that you can send them by an alternative method.

1 Log in to the Novell appliance at https://*server_url*:9443.

2 Click **Support**.

3 Select **Automatically send the configuration to Novell using FTP** to automatically send your Filr system's configuration information to Novell Support via FTP.

or

Select **Download and save the configuration file locally, then send it to Novell manually** to download your Filr system's configuration information to your management workstation. You can then send the information to Novell Support using a method of your choice.

4 Click **OK** to complete the process.

2.10 Managing Field Test Patches

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

1 Log in to the Novell appliance at https://*server_url*:9443.

2 Click **Field Test Patch**.

3 (Optional) Install a new patch:

    3a Before you can install a patch, you first need to download it from the Novell Support web site (https://www.novell.com/support/) to your management workstation.

    3b From the Field Test Patch page on the Novell appliance, click **Browse**.

    3c Browse to and select the patch that you downloaded in Step 3a.

    3d Click **Install Selected Patch**.

4 (Optional) Uninstall a patch:

    4a In the **Patch Name** column of the provided table, select the patch that you want to uninstall.

    4b Click **Uninstall Latest Patch**.

2.11 Managing Memcached (Search Index Appliance Only)

1 Log in to the Novell appliance at https://*server_url*:9443.

2 Click **Memcached**.

3 You can change the following configuration settings for Memcached:

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.

2.12 Managing Storage

Filr provides native tools to allow you to expand the storage space for the `/vastorage` and `/var` partitions. (You should have already created partitions for `/vastorage` and `/var`, as described in the *Filr 2.0: Installation and Configuration Guide*.)

1 Log in to the Novell appliance at https://*server_url*:9443.

2 Click **Storage**.

3 Use the tools provided by your virtualization platform vendor to expand the virtual disks that contain the partitions your are expanding.

4 In the provided table, select the partitions to be expanded.

5 Click **Expand partitions**.

Appliance services are stopped, the selected partitions are expanded to the size of their respective disks, and appliance services are restarted.

6 If there are any Bash console sessions open on the appliance, close them before proceeding to Step 7.

7 Reboot the appliance so the operating system can detect the disks that have been expanded.

2.13 Expanding the /var Directory

To expand the disk space available for the `/var` directory:

1 Shut down the appliance needing the expansion.

2 Add the disk space by using the hypervisor's tools.

3 Start the appliance and log in as the vaadmin user (port 9443).

4 Click **Storage**.

5 Select the devices to which you have added the disk space.

6 Click **Expand Partitions**.

2.14 Shutting Down and Restarting the Novell Appliance

You might need to shut down or restart the Novell appliance for maintenance.

1 Log in to the Novell appliance at https://*server_url*:9443.

2 Click **Reboot** or **Shutdown**.

II Setting Up the Filr Site before Users Log In

After you have installed and started Novell Filr, you need to perform several administrative tasks before your Filr site is ready for users to log in and start using Filr efficiently. Filr ships with most settings disabled by default, so you as the Filr administrator must enable each piece of functionality. This ensures that your data is not unknowingly exposed to users who do not normally have access to certain information. For example, users cannot share files until you give them the ability to do so.

Refer to the following sections to set up your Filr site:

3 Logging In as the Filr Site Administrator

After logging in to the Novell Filr site, you should reset the Filr administrator's password.

- Section 3.1, "Logging In," on page 51
- Section 3.2, "Changing the Filr Administrator User ID or Password," on page 52
- Section 3.3, "Creating Additional Filr Administrators," on page 53

3.1 Logging In

After installing and configuring Filr, you need to log in to the Filr site to perform additional administrative tasks.

1 In your web browser, specify one of the following URLs, depending on whether you are using a secure SSL connection:

   ```
   http://filr_hostname:8080
   https://filr_hostname:8443
   ```

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

   Depending on how you have configured your Filr system, you might not be required to enter the port number in the URL; if you are using NetIQ Access Manager, the Filr login screen is not used. For more information about Filr configurations that affect login, see Section 2.2, "Changing Network Settings," on page 39.

2 If this is the first time you have logged in to the Filr site, log in using `admin` as the login name and `admin` as the password.

   The Change Password dialog box is automatically displayed when you first log in to the Filr site.

   If this is not your first time logging in, log in using `admin` as the login name and your password.

3.2 Changing the Filr Administrator User ID or Password

When you first install Novell Filr, the Filr administrator user name is `admin` and the password is `admin`. When you first log in to the Filr site as the administrator, you should change the administrator password from the default password to a secure password of your own choosing.

3.2.1 Changing the Administrator Password

You can change your password to a new password at any time:

1 In your Web browser, specify one of the following URLs, depending on whether you are using a secure SSL connection:

```
http://filr_hostname:8080
https://filr_hostname:8443
```

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

Depending on how you have configured your Filr system, you might not be required to enter the port number in the URL; if you are using NetIQ Access Manager, the Filr login screen is not used. For more information about Filr configurations that affect login, see Section 2.2, "Changing Network Settings," on page 39.

2 Log in using your current user name and password.

or

If this is your first time accessing the site, log in using `admin` as the login name and `admin` as the password.

The Change Password dialog box is automatically displayed when you first log in to the Filr site.

3 Click your linked name in the upper-right corner of any Filr page.

4 Click **Change Password**.

The Change Password dialog box is displayed.

5 Specify the current password, then specify and confirm the new password.

6 Click **OK**.

3.2.2 Changing the Administrator User ID and Other Profile Information

You might want to change the administrator User ID in addition to other information on the administrator's user profile.

* **User ID:** As a security precaution, it might make sense to change the administrator's user ID from the default `admin`. The administrator user ID is used only when logging in to the Filr system.

    Changing the administrator user ID requires that you restart each Filr appliance in the Filr system in order for the change to take effect.

◆ **First Name and Last Name:** Providing a first and last name for the administrator changes the name that appears in the upper-right corner of each Filr page, as well as the name that appears in the administration console under **Administrators**.

To change the Filr administrator user ID, as well as other profile information, follow the steps in "Modifying Your Profile" in the *Filr 2.0: Web Application User Guide*.

3.3 Creating Additional Filr Administrators

Creating additional Filr administrators lets you ensure that the right people are able to access the Filr site in an administrative capacity if the need arises.

◆ Section 3.3.1, "Additional Administrators Have a Subset of Administrative Privileges," on page 53
◆ Section 3.3.2, "Creating an Administrator Group," on page 53
◆ Section 3.3.3, "Assigning Administrative Rights to a User or Group," on page 54

3.3.1 Additional Administrators Have a Subset of Administrative Privileges

Only the original (built-in) Filr administrator can add or remove site administrator rights for users and groups.

Additional Filr administrators have rights to administer the following:

◆ Users
◆ Groups
◆ Mobile Devices
◆ Net Folder
◆ Net Folder Servers

3.3.2 Creating an Administrator Group

To minimize the time-consuming indexing of the Filr site, it is most effective to create an administrator group that has administrative rights, then assign users to that group as needed. For information about how to create a group, see Chapter 9, "Creating Groups of Users," on page 115.

You can create an administration group and assign rights only to that group:

1 Log in to Filr as the Filr administrator.

   1a Launch a web browser.

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

```
http://filr_hostname:8080
https://filr_hostname:8443
```

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

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

2 Create an administration group, described in Chapter 9, "Creating Groups of Users," on page 115.

3 Assign administrator rights to that group, as described in Section 3.3.3, "Assigning Administrative Rights to a User or Group," on page 54.

4 When you want to grant administrative rights to a user, add that user to the administrator group that you created. (For information about how to add users to a group, see Section 19.2, "Modifying Groups," on page 223.)

3.3.3 Assigning Administrative Rights to a User or Group

1 Log in to Filr as the Filr administrator.

    1a Launch a web browser.

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

```
http://filr_hostname:8080
https://filr_hostname:8443
```

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

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

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

3 In the **Management** section, click **Administrators**.

4 Click **Add**, then begin typing the name of the user or group for whom you want to grant administrator rights.

5 Click the user or group name when it appears in the drop-down list.

To remove administrator rights from a user or group:

1 Select the users or groups for whom you want to remove administrator rights.

2 Click **Remove**.

4 Adding New Users to Your Filr Site

You can add new users to your Filr site in any of the following ways:

- Synchronizing from an LDAP directory, as described in Section 18.1, "Synchronizing Users and Groups from an LDAP Directory," on page 193.
- Manually adding local users, as described in Section 18.3, "Creating a New Local User," on page 206.
- Importing profile files for local users, as described in Section 18.11, "Managing Local Users and Groups by Importing Profile Files," on page 221.

5 Enabling and Customizing Filr's Email Services

Your Novell Filr site can be configured to send outbound email through an existing email system or through the included Postfix SMTP outbound mail server.

NOTE: To receive notifications, users must have a valid email address in their Filr accounts.

Filr doesn't verify that valid email addresses exist in target user accounts as a prerequisite for their being included in a notification list.

Email from the Filr site is useful for the following activities:

- Filr users can subscribe to email notifications, so that they automatically receive a message whenever content of interest changes. For more information, see "Subscribing to a Folder or Filr" in "Getting Informed" in the *Filr 2.0: Web Application User Guide*.
- Filr users can configure folders that they own to send email notifications to other users. For more information, see "Configuring Folders to Send Email Notifications to Other Users" in the *Filr 2.0: Web Application User Guide*.
- Filr users can send email messages to folder contributors, as described in "Sending an Email to Folder Contributors" in the *Filr 2.0: Web Application User Guide*.
- Filr users can send notifications when a folder or file is shared, as described in "Sharing Files and Folders" in the *Filr 2.0: Web Application User Guide*.

Initial email configuration is performed when you install Novell Filr. Additional aspects of email handling are configured on the Filr site. For information about how to further configure email settings beyond what is covered in this section, see Chapter 23, "Managing Email Configuration," on page 249.

- Section 5.1, "Enabling Outbound Email," on page 58
- Section 5.2, "Scheduling Folder Digest Emails," on page 59
- Section 5.3, "Restricting Email Attachment Size," on page 60
- Section 5.4, "Customizing Email Templates," on page 60

5.1 Enabling Outbound Email

During the configuration of the Filr appliance, you configured Novell Filr to communicate with your email system, as described in Section 1.9, "Configuring Outbound Email Services," on page 31. As a result, Filr users can send email messages to other Filr users and to anyone whose email address they know. They can also send email notifications when they create folders, add files, share files and folders, and so on.

In addition to this basic email functionality, you can configure your Filr site so that users can receive folder digests of site activity that are created and sent to the users who have subscribed to the folders. (For information about how users can subscribe to folders, see "Subscribing to a Folder or Filr" in the *Filr 2.0: Web Application User Guide*.)

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

    1a Launch a web browser.

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

```
http://filr_hostname:8080
https://filr_hostname:8443
```

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

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

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

3 Under **System**, click **Email**.

4 Select **Enable Outgoing Email**.

This option applies to all outgoing emails sent from the Filr system.

5 Click **Apply** to save the settings, then click **Close**.

5.2 Scheduling Folder Digest Emails

In addition to enabling basic email functionality, you can configure your Filr site so that users can receive folder digests of site activity that are created and sent to the users who have subscribed to the folders. (For information about how users can subscribe to folders, see "Subscribing to a Folder or Filr" in the *Filr 2.0: Web Application User Guide*.)

1 To schedule when folder digests are generated and sent, in the **Filr Administration Console > System > Email > Default Digest Schedule**, adjust the schedule of digest notifications sent from the Filr system to meet the needs of the majority of your Filr users.

Users can receive digest notifications for folders when they subscribe to a folder (as described in "Subscribing to a Folder or Filr" in the *Filr 2.0: Web Application User Guide*) or when someone configures folders to send notifications to others (as described in "Configuring Folders to Send Email Notifications to Other Users" in the *Filr 2.0: Web Application User Guide*).

Users can turn the digests on and off for individual folders, but they cannot change the email schedule that you establish.

By default, folder digests are compiled and sent daily at fifteen minutes after midnight.

2 Click **Apply** to save the settings, then click **Close**.

5.3 Restricting Email Attachment Size

1. To set a data quota on outgoing mail messages, in the **Filr Administration Console > System > Email** dialog, specify the quota limit in the **Maximum Size for the Sum of All File Attachments** and the **Maximum Size of Each File Attachment** fields.

   By default, there is no limit to the size of attached files. You can leave the fields blank to retain the default of no limit.

   To restrict any attachments from being sent, specify `0` in each field.

2. Click **Apply** to save the settings, then click **Close**.

5.4 Customizing Email Templates

Path to Configuration Dialog: Filr Administration Console > **System > Email Templates**

5.4.1 About Filr's Email Templates

Filr generates email notifications using Apache Velocity version 1.5 templates.

You can customize the following templates, beginning with the Filr 2.0 release:

Template Name	Purpose
footer.vm	Text or images applied at the end of each email
header.vm	Text or images applied at the beginning of each email
passwordChangedNotification.vm	Notification that user's password changed
publicLinkNotification.vm	Notifcation of a publicly available link to a file
selfRegistrationRequired.vm	Shared item notification to user who must register with Filr in order to view it
sharedEntryInvite.vm	Shared file invitation to an existing Filr user
sharedEntryNotification.vm	Shared file notification of change to existing Filr user
sharedFolderInvite.vm	Shared folder invitation to existing Filr user
sharedFolderNotification.vm	Shared folder notification of change to existing Filr user
style.vm	CSS style sheet for email notifications
teaming.vm	Macros that get applied to all emails

5.4.2 Tips and Documentation

The following are tips about the template files in Filr.

- Each template contains a brief explanation about what you can customize.
- Filr system-generated emails contain both text and HTML MIME parts. You can customize these independently.
- You can customize by language to localize the emails your Filr system generates.

- You can revert back to the default template by selecting a customize template in the list and then clicking the Delete button.

- Make sure you use the Velocity documentation (https://velocity.apache.org/engine/releases/velocity-1.5/user-guide.html).

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

Complete information and instructions for the Apache Velocity version 1.5 template language are available on the Apache Velocity Project website (https://velocity.apache.org/engine/releases/velocity-1.5/).

5.4.3 Modifying the Template Files

The default email templates that reside on the Filr 2.0 system cannot be changed or deleted, but you can create and deploy customized copies of them by doing the following:

1. Download a template to your local disk by clicking it in the Email Templates dialog

2. Open it in a text editor

3. Save it on your local disk.

4. Upload the customized file by dragging and dropping it into the Email Templates dialog.

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

5.4.4 A Video Walkthrough

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

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

6 Setting Up Sharing

As the Filr administrator, you need to enable sharing privileges for users on your Filr site before users are able to share files and folders. There are various sharing privileges that you can grant.

6.1 Understanding Sharing

6.1.1 My Files Sharing Vs. Net Folder Sharing

By default, users can share both files and folders in their **My Files** area; **Net Folder** sharing is limited to only files.

6.1.2 Sharing and Access Roles

When users send share invitations, they must designate the role that they want the user receiving the share to have for the file or folder being shared. The roles associated with sharing are the same as Net Folder roles.

Filr administrators who allow Net Folder sharing should understand the following foundational concepts.

- **Share Invitations Always Include a Shared-Access Role:** When users receive share invitations, they also receive one of three shared-access roles: Viewer, Editor, or Contributor. These involve the same rights as Net Folder roles.

- **Users Can't Share Roles That They Don't Have:** Users can grant only shared- access roles that either correspond to their roles or are more restrictive.

  For example, a user with the Contributor role can grant the Viewer, Editor, or Contributor shared-access role to other users as Filr system share and Net Folder share settings allow.

  On the other hand, a user with the Viewer role can only grant the Viewer shared-access role to other users.

  NOTE: Because users have all rights to their My Files area, they can share any role to a folder or file, provided that sharing is enabled on the system.

◆ **The Highest Role Wins:** If multiple users share the same item with a single user, the user receiving the share has the highest role that was granted along with the share.

   For example, if User B shares a file with User A and grants User A the Viewer role to the file, and then User C shares the same file with User A and grants the Editor role to the file, User A has Editor rights to the file.

6.1.3 Shared Access to Net Folders Is Always through a Proxy User

When Filr users access a Net Folder-based file in their Shared With Me folder, they access it through the proxy user assigned to the Net Folder where the file lives. File system rights that users do or do not have to shared items play no role when they are working within Shared with Me.

6.2 Understanding External Users

Users external to your organization can access your Filr site at no additional cost. External users in Novell Filr do not count as a licensed Filr user, but they have their own individual user account (unlike the Guest user) and can participate in Filr workspaces like any other user.

An example of an external user might be a contractor who interacts with the corporation for only a couple months a year, who needs access to the system as a defined user but does not need consistent access to the system.

External users are added to the Filr system when a workspace, folder, or entry is shared with them. You as the Filr administrator determines whether users can share externally. For information about how to enable this functionality, see Section 6.3, "Enabling Users to Share," on page 64.

6.3 Enabling Users to Share

   ◆ Section 6.3.1, "Best Practices for Setting Up Sharing," on page 64
   ◆ Section 6.3.2, "General Order for Setting Up Sharing," on page 65
   ◆ Section 6.3.3, "Enabling Sharing for the Entire Site," on page 65
   ◆ Section 6.3.4, "Restricting Personal Storage Sharing," on page 68
   ◆ Section 6.3.5, "Enabling Sharing for Specific Net Folders," on page 69

6.3.1 Best Practices for Setting Up Sharing

   ◆ **Enable Unrestricted Sharing for the Filr System:** You must enable the sharing feature before any sharing can take place on the Filr system.

   As a best practice, enable sharing in an unrestricted way. For example, give the `All Internal Users` group the ability to share.

   ◆ **If Needed, Restrict My Files Sharing:** Enabling sharing automatically lets all users share files in their My Files area, including in their Home folder and in personal storage.

   You can restrict My Files sharing on a per-user basis if desired.

   ◆ **Carefully Restrict Net Folder Sharing:** Net Folder sharing must be explicitly allowed for each Net Folder.

IMPORTANT: Make sure that only those who need to share a Net Folder's contents are granted sharing rights on that Net Folder.

For example, Group A is granted rights to share files in Net Folder A. User A (a member of Group A) then shares a file with User B (a member of Group B). Because the file contains sensitive information, User A doesn't grant User B permission to reshare the file.

As long as User B doesn't have rights to share files in Net Folder A, there is no problem.

However, if Group B also has permission to share Net Folder A's files, then User B can reshare the file even though User A assumed otherwise.

6.3.2 General Order for Setting Up Sharing

When you set up sharing for your Filr site, complete the necessary steps in the following order:

1 Set up sharing for the entire Filr site (as described in Section 6.3.3, "Enabling Sharing for the Entire Site," on page 65).

2 Configure sharing for individual users (as described in Section 6.3.4, "Restricting Personal Storage Sharing," on page 68).

After you have enabled sharing for the entire Filr system, you can fine-tune share rights throughout the site on the user level.

For example, if you want only a few groups of users to be allowed to share with external users, you first need to enable sharing to external users at the site level. After you have enabled it at the site level, you can then remove this ability from the users who you do not want to have this ability.

3 Set up sharing for specific Net Folders (as described in Section 6.3.5, "Enabling Sharing for Specific Net Folders," on page 69).

Users who are given share rights on a specific Net Folder are able to share files within that Net Folder that they have rights to at least view on the file system.

6.3.3 Enabling Sharing for the Entire Site

After you set up sharing for the entire Filr site, all users by default are granted rights to share files in the My Files area (this includes files in the Home folder and files in personal storage), with the site-wide access rights that you specify. If you want only certain users to be allowed to share files from their My Files area, you must enable sharing for the entire site as described in this section. Then you must restrict sharing privileges at the user level, as described in Section 6.3.4, "Restricting Personal Storage Sharing," on page 68.

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

    1a Launch a web browser.

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

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

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

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

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

3 Under **System**, click **Share Settings**.

The Share Settings page is displayed.
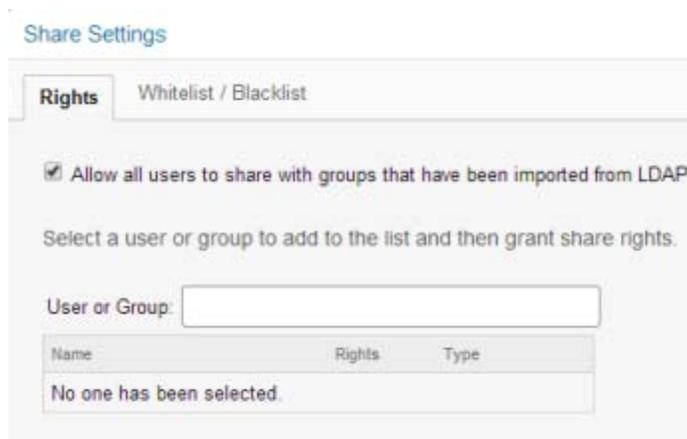
4 Select **Allow all users to share with groups that have been imported from LDAP** to enable users to share with LDAP groups.

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 (as described in "Sharing files and Folders" in the *Filr 2.0: Web Application User Guide*). All users in the LDAP group then have access to the item that was shared.

5 To enable sharing for all internal users on the Filr site, go to the **User or Group** field, begin typing `All Internal Users`, then select it when it appears in the drop-down list.

or

To enable sharing on a per-user or per-group basis, go to the **Select user/group** field, begin typing the name of the user or group for whom you want to grant share rights, then select the name when it appears in the drop-down list.

The Edit Share Rights dialog box is displayed. Select from the following options:

Re-share items: 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. The user receiving the share can share the file only if that user has been given administrative rights to share the file or folder.

IMPORTANT: When selecting this option, be aware that if one user's access rights to an item are removed, it does not remove the access rights of the user with whom the item was re-shared.

For example, suppose User A shares an item with User B and grants re-share rights. User B then shares the item with User C. If User A revokes User B's access rights to the item, User C continues to have access to the shared item.

Share with Internal users: Allows users to share items with internal users.

Share with "All Internal Users" group: Allows users to perform a mass share to all internal users by sharing with the `All Internal Users` group.

Share with External users: Allows users to share items with users external to the organization.

Users external to the organization receive an email notification with a link to the shared item, and they can then log in to the Filr site. For more information, see "Sharing with People Outside Your Organization" in the *Filr 2.0: Web Application User Guide*.

Share with Public: Allows users to make items publicly available. This means that anyone with the correct URL to the shared item can access the shared item without logging in to the Filr site.

In addition to selecting this option, you also need to enable Guest access to the Filr site if you want to allow users to share items with the public. For information about how to enable Guest access to the Filr site, see Section 10.1.1, "Allowing Guest Access to Your Filr Site," on page 123.

Share using File Link: Allows users to share a link to a file in Filr. Any user with the link can then access the file. However, the file is not displayed in the Public area, so users must have direct access to the link in order to access the file.

For more information about File Links, see "Distributing a Link to a File" in the *Filr 2.0: Web Application User Guide*.

6 (Optional) Click the **Whitelist / Blacklist** tab to configure which email addresses and domains users can share with when sharing externally.

The following options are available when configuring a whitelist or blacklist for sharing:

No restrictions: Select this option to disregard any email addresses or domains that might already exist in the **Email addresses** and **Domains** fields. Selecting this option means that users can share with any email address.

Whitelist: Select this option to allow sharing only with email addresses and domains that have been specified in the **Email addresses** and **Domains** fields.

Blacklist: Select this option to disallow sharing with any email addresses and domains that have been specified in the **Email addresses** and **Domains** fields.

Email addresses: Click **Add**, specify the email address that you want to add to the whitelist or blacklist, then click **OK**.

Repeat this process to add multiple email address.

Domains: Click Add, specify the domain that you want to add to the whitelist or blacklist (for example, `yahoo.com`), then click **OK**.

Repeat this process to add multiple domains.

Delete shares that don't meet the criteria: Select this option to delete all existing shares in the Filr system that do not match the criteria you set.

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.

7 Click **OK**.

6.3.4 Restricting Personal Storage Sharing

After you have enabled sharing of files for the entire Filr system (as described in Section 6.3.3, "Enabling Sharing for the Entire Site," on page 65), you can restrict shared-access right granting on an individual-user basis.

You cannot grant individual users more rights than are currently defined for the site-wide setting.

To restrict share rights for specific users:

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

    1a Launch a web browser.

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

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

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

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

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

3 Under **Management**, click **Users**.

4 Select the users whose sharing rights you want to manage, then click **More** > **Workspace Share Rights**.

5 Select the radio button in the **Clear** column next to the sharing right that you want to remove from the user or group, then click **OK**.

or

If you have already removed a share right and you want to add it again, select the radio button in the **Allow** column next to the sharing right that you want to add to the user or group, then click **OK**.

6.3.5 Enabling Sharing for Specific Net Folders

1 Ensure that you have configured sharing as described in Section 6.3.3, "Enabling Sharing for the Entire Site," on page 65.

2 Configure sharing for the Net Folder as described in Section 8.6, "Creating and Managing Net Folders," on page 101 or Section 8.10, "Modifying Net Folder Connections," on page 114 (depending on whether the Net Folder has already been created).

6.4 Managing Shares

As the Filr administrator, you are in control of all shared items in the Filr system. You can view who has shared items, what items have been shared, what access rights have been granted via the share, and so forth. Furthermore, you can modify share rights for existing shares or delete existing shares.

You can manage shares through a management interface, where you can filter by user, file, folder, or all shares. Or, you can manage shares for individual folders and files as you encounter them in the Filr site.

Users are not notified about changes that you make to shared items.

- Section 6.4.1, "Managing Shares for the Filr Site," on page 70
- Section 6.4.2, "Managing Individual Shares," on page 70

6.4.1 Managing Shares for the Filr Site

You can manage all active shares in the Filr system with the Manage Shares dialog box in the administration console. You can filter shares by individual users, files, or folders. Or, you can view all active shares in the Filr system.

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

   1a Launch a web browser.

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

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

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

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

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

3 Under **Management**, click **Shares**.

   The Manage Shares dialog box is displayed.

4 In the **Find share items by** drop-down list, select one of the following options by which you want to manage shares:

   User: 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: 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: 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: Displays all active shares in the Filr system.

5 (Optional) Change the access control settings, expiration date, and note for a shared item.

   For more information about these options, see "Sharing files and Folders" in the *Filr 2.0: Web Application User Guide*.

6 (Optional) Remove a user or group's access to a shared item by selecting the share that you want to remove, then clicking **Delete**.

7 Click **OK**.

6.4.2 Managing Individual Shares

As the administrator, you can manage shares for individual folders and files as you encounter them in the site.

1 In an area such as a Net Folder or in your Shared with Me area, select one or more files for which you want to manage sharing, then click **More** > **Manage Shares**.

   or

In a folder or an area such as a Net Folder or in your Shared with Me area, click the drop-down arrow ⊖ next to the file, then click **Manage Shares**

The Manage Shares dialog box is displayed.

2 (Optional) Change the access control settings, expiration date, and note for a shared item.

For more information about these options, see "Sharing files and Folders" in the *Filr 2.0: Web Application User Guide*.

3 (Optional) Remove a user or group's access to a shared item by selecting the share that you want to remove, then clicking **Delete**.

4 Click **OK**.

7 Setting Up Personal Storage

As the Filr administrator, you can enable or disable user access to personal storage. Personal storage includes all files and folders in the My Files area that are not associated with the user's Home directory if they have one.

IMPORTANT: This setting affects only users whose accounts are synchronized to your Filr system via LDAP. Users who are created locally (as described in Section 18.3, "Creating a New Local User," on page 206) always have access to personal storage in the My Files area.

Guest users and external users never have access to personal storage in the My Files area.

Filr allows you to access, share, and collaborate on files that are in two key locations:

- **My Files:** Users can upload files directly to the Filr site for personal use or to promote collaboration. Users can create folders to better organize files. For more information about how users can upload files, see "Adding Files to a Folder" in the *Filr 2.0: Web Application User Guide*.

  Files and folders that are located in a user's My Files area are visible only to that user by default. Users can make files and folders available to others by sharing them, as described in "Sharing Files and Folders"in the *Filr 2.0: Web Application User Guide*.

  Unlike Net Folders or Home folders, files in users' personal storage in the My Files area are not synchronized from an external file system.

- **Files in Net Folders:** Novell Filr gives users easy access to folders and files on the corporate file system. Corporate files can be files on a home drive, files on a mapped drive, or files on a remote server. Filr gives users seamless access to these files, regardless of their location. The corporate files that users have access to are defined by the Filr administrator.

  In Filr, users access these corporate files by clicking **Net Folders** in the masthead. For more information about Net Folders, see the *Filr 2.0: Web Application User Guide*.

You can enable or disable user access to personal storage (in the My Files area) for all users or for individual users:

- Section 7.1, "Understanding How Personal Storage Relates to Home Folders," on page 73
- Section 7.2, "Enabling Personal Storage for All Users," on page 74
- Section 7.3, "Enabling Personal Storage for Individual Users," on page 74
- Section 7.4, "Enabling Personal Storage for Individual Groups," on page 75

7.1 Understanding How Personal Storage Relates to Home Folders

Personal storage is a location in the My Files area where users can store files (files in personal storage are maintained on Filr servers; unlike Net Folders or Home folders, files in personal storage are not synchronized from an external file system). Personal storage is displayed differently depending on whether users have a Home folder enabled. If Home folders are enabled, the Home folder is displayed in each user's My Files area. (For more information about Home folders in Filr, see Section 8.4, "Configuring Home Folders for Display in the My Files Area," on page 94.)

If Personal storage is enabled and Home folders are also enabled: The Home folder is displayed in the user's My Files area at the same level of any other folder that the user decides to add to the My Files area.

If Personal storage is disabled and Home folders are enabled: The name of the Home folder is displayed at the top of the folder listing and the view lists only the content of the Home folder.

If Personal storage is enabled and Home folders are disabled: Only files that the user adds via one of the Filr clients are displayed in the My Files area.

If both Personal storage and Home folders are disabled: Users cannot see files or add files in the My Files area.

7.2 Enabling Personal Storage for All Users

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

    1a Launch a web browser.

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

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

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

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

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

3 Under **Management**, click **Personal Storage**.

4 Select or deselect **Allow LDAP users to have personal storage area**, depending on whether you want users whose accounts are synchronized via LDAP to have access to the My Files area.

5 Click **OK**.

7.3 Enabling Personal Storage for Individual Users

1 In Filr, click the **admin** link in the upper-right corner of the page, then click the **Administration Console** icon 👤.

2 Under **Management**, click **Users**.

The Manage Users page is displayed.

3 Select the check boxes next to the names of the users for whom you want to enable personal storage, then click **More** > **Enable Personal Storage**.

If you have enabled personal storage for all users or for individual users, you can disable it for specific users.

1 In Filr, click the **admin** link in the upper-right corner of the page, then click the **Administration Console** icon .

2 Under **Management**, click **Users**.

The Manage Users page is displayed.

3 Select the check boxes next to the names of the users for whom you want to disable personal storage, then click **More** > **Disable Personal Storage**.

To change individual users to use the global personal storage settings:

1 In Filr, click the **admin** link in the upper-right corner of the page, then click the **Administration Console** icon .

2 Under **Management**, click **Users**.

The Manage Users page is displayed.

3 Select the check boxes next to the names of the users for whom you want to change personal storage settings to match the default global setting, then click **More** > **Use Default Personal Storage Setting**.

7.4 Enabling Personal Storage for Individual Groups

1 In Filr, click the **admin** link in the upper-right corner of the page, then click the **Administration Console** icon .

2 Under **Management**, click **Groups**.

The Manage Groups page is displayed.

3 Select the check boxes next to the names of the groups for which you want to enable personal storage, then click **More** > **Enable Personal Storage**.

If you have enabled personal storage for all users, you can disable it for users in specific groups.

1 In Filr, click the **admin** link in the upper-right corner of the page, then click the **Administration Console** icon .

2 Under **Management**, click **Groups**.

The Manage Groups page is displayed.

3 Select the check boxes next to the names of the groups for which you want to disable personal storage, then click **More** > **Disable Personal Storage**.

To change individual users to use the global personal storage settings:

1 In Filr, click the **admin** link in the upper-right corner of the page, then click the **Administration Console** icon .

2 Under **Management**, click **Groups**.

The Manage Users page is displayed.

3 Select the check boxes next to the names of the groups for which you want to change personal storage settings to match the default global setting, then click **More** > **Use Default Personal Storage Setting**.

8 Setting Up Net Folders

Net Folders in Filr provide access to files on your corporate OES, NetWare, Windows, or SharePoint 2013 file servers by synchronizing file metadata. In essence, a Net Folder is simply a pointer or a reference to a specific folder on a specific file server.

Filr can be configured to index the content of Net Folders to make the content searchable.

IMPORTANT: Configuring Net Folders in a sub-optimal way can result in unsatisfactory performance of your Filr system. The ideal Net Folder configuration can vary greatly depending on the number of files that you want to synchronize to Filr, the frequency in which files are modified, and so forth. Before configuring Net Folders, become familiar with the various subtleties related to Net Folders, as described in Section 8.1, "Planning Net Folder Creation," on page 77.

The following video walks you through the Net Folder planning process:

   http://www.youtube.com/watch?v=En7PtGcHffA

To see other Novell Filr videos, see the Novell Filr YouTube playlist (https://www.youtube.com/playlist?list=PL8yfmcqTN8GHMg4ZYu_-72QPqD616REey).

The following sections describe the process for setting up and managing Net Folders:

8.1 Planning Net Folder Creation

8.1.1 Understanding Known Issues

Before you begin planning for and setting up Net Folders, ensure that you are aware of any known issues. For more information, see "Net Folder Issues (http://www.novell.com/documentation/novell-filr-2/filr-2-relnote/data/filr-2-relnote.html#b1383h6s)" in the *Novell Filr Readme* (http://www.novell.com/documentation/novell-filr-2/filr-2-relnote/data/filr-2-relnote.html).

8.1.2 Planning an OES 2015 NSS AD Integration

Filr 2 and NSS for AD

Beginning with OES 2015, both eDirectory and Active Directory are supported as LDAP identity sources for NSS-volume access as illustrated in Figure 8-1.

Figure 8-1 *AD Users Can Access NSS Volumes through Filr*
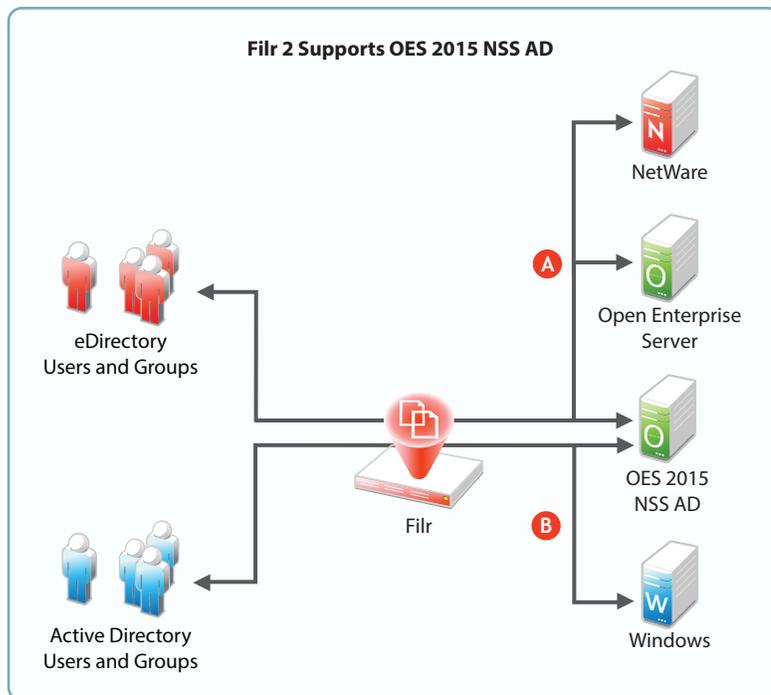
For information on installing and configuring NSS for AD, see the *OES 2015: NSS AD Deployment and Administration Guide*.

Specifying the Net Folder Proxy User

Although AD users can be granted rights to NSS volumes on properly configured OES 2015 server, the Net Folder Proxy User must be an eDirectory user that meets the qualifications outlined in Figure 8-2 on page 92.

Selecting the Correct Server Type

To accommodate NSS for AD, Filr 2 includes a new server type: Novell Open Enterprise Server (NSS for AD).

Use the following table as a guide when selecting the server type for a Net Folder Server.

Volume is Enabled for NSS AD	Protocol Used	Server Type to Select
Yes	CIFS or NCP	Novell OES (NSS for AD)
No	CIFS	Novell OES (NSS for AD)
No	NCP	Novell OES

DFS Considerations

If an NSS volume on an OES 2015 server has DFS function targets that point to an older OES server, then you must select Novell OES 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 server has DFS junctions and you are planning to select the new NSS for AD server type, you must scan the volume from iManager as instructed in "Managing Junctions" in the *OES 2015: Domain Services for Windows Administration Guide*.

8.1.3   Planning a SharePoint 2013 Integration

Filr 2.0 lets you configure Net Folders in Filr to access files in regular document libraries on a SharePoint 2013 server. When a user uploads a file to a SharePoint-configured Filr Net Folder, that file is made available on the SharePoint server as well as to any user or group who has access to the Net Folder in Filr.

- "Understanding How Filr Handles Checked Out Documents" on page 80
- "User Access Synchronization Considerations" on page 80
- "Granting Access to a Specific Folder That Has Been Shared via SharePoint" on page 80
- "Configuring Access and Sharing Rights" on page 81
- "Configuring SSL between the SharePoint Server and Filr" on page 81

Understanding How Filr Handles Checked Out Documents

SharePoint 2013 contains the following configuration option: **Require documents to be checked out before they can be edited**. When enabled, this option causes files that are uploaded to SharePoint to be uploaded in the Checked Out state, making them visible only to the person who uploaded the files. This is true regardless of the application that is used to upload (such as SharePoint web portal or One Drive).

This is also true for Filr, however, to ensure that files uploaded to the SharePoint 2013 server via a SharePoint-configured Filr Net Folder are available to all Filr users with appropriate rights to the Net Folder (through synchronization to Filr via the Filr Net Folder Server Proxy User), Filr behaves differently depending on whether the **Require documents to be checked out before they can be edited** option is enabled on the SharePoint 2013 server.

- ◆ **If Enabled:** Filr automatically checks in a minor version of the file so that the file can be seen by the Net Folder Server Proxy User, and therefore is available to Filr users with rights to the Net Folder.
- ◆ **If Disabled:** The uploaded file is immediately visible to all users who have rights to the Net Folder.

User Access Synchronization Considerations

When synchronizing user access rights information from SharePoint to Filr, consider the following:

- ◆ User access rights to files and folders within SharePoint are synchronized to Filr only for users who exist in Active Directory. Access rights for users who exist only locally on the SharePoint site are not synchronized to Filr.
- ◆ SharePoint personal sites are not currently displayed as user Home folders in Filr.

Granting Access to a Specific Folder That Has Been Shared via SharePoint

In SharePoint, if a folder has been shared with a specific group and that group does not have access to the parent directory, you must create a separate Net Folder with a relative path to the shared folder and give the group access.

If you create a Net Folder at a higher level, the group cannot access the sub-folder to which they have access because, as dictated by the SharePoint architecture, they are not able to view the parent folder.

For example, suppose Group A has access rights in SharePoint to the following folder: `http://sharepoint_site/sites/marketing/productx`. Group A does not have access rights to the `marketing` folder, only to the `productx` folder. In order for Group A to have access to the `productx` folder in Filr:

1 Create a Net Folder Server (as described in Section 8.5.1, "Configuring Net Folder Servers," on page 96) with the following server path:

   `http://sharepoint_site/sites/marketing`

2 Create a Net Folder (as described in Section 8.6.1, "Creating Net Folders," on page 102) with the following relative path:

```
productx
```

3 (Optional) You might also create another Net Folder to the `marketing` folder, and assign the appropriate set of users access to that folder. (These users would need to have access to this folder in SharePoint.)

Configuring Access and Sharing Rights

The conditions for how access rights transfer from the SharePoint site to Filr are the same as those for other types of file systems. For more information, see "Understanding Access Rights for Net Folders" on page 82.

Sharing rights are mapped from the SharePoint site to the Filr system. Filr allows users to grant Viewer, Editor, or Contributor access to the file, depending on their rights on the SharePoint site. For information about the SharePoint rights that map to these roles, "Understanding Sharing Rights for Net Folders" on page 82.

Consider the following regarding sharing:

- ◆ "Understanding How Shared Access from SharePoint Transfers to Filr" on page 81
- ◆ "Understanding How Enabling the Ability to Re-Share within Filr Can Affect SharePoint" on page 81

Understanding How Shared Access from SharePoint Transfers to Filr

If an item has been shared with a user via SharePoint, that user has access to the item within Filr within the Net Folder where the file is located. Files that are shared within SharePoint are not displayed in the Filr Shared with Me area.

Understanding How Enabling the Ability to Re-Share within Filr Can Affect SharePoint

Filr allows you to grant users with the ability to re-share items with other users who do not have access (as described in Section 6.3.3, "Enabling Sharing for the Entire Site," on page 65).

When re-sharing is enabled, users can share a file or folder and give the users they are sharing with the ability to re-share the file or folder.

IMPORTANT: Because SharePoint does not have this same capability, carefully consider whether you want to allow users to re-share items, because doing so could grant users access to items that they otherwise wouldn't have within SharePoint.

Configuring SSL between the SharePoint Server and Filr

If your SharePoint server is configured with SSL, you might need to export the SSL certificate from SharePoint and import it into Filr in order for the Net Folder Server to function properly.

After you have exported the SSL certificate and keypair from the SharePoint site, you need to import them into Filr (the certificate and key pair should be in .P12 key pair format):

1 Go to the Digital Certificates page by clicking **Digital Certificates** from the Novell Appliance.

2 Click **File** > **Import** > **Trusted Certificate**. Browse to and select your existing certificate, then click **OK**.

3 Continue with Section 31.2.3, "Activating the Certificate," on page 296.

8.1.4 Planning Access and Sharing for Net Folders

It is important that you understand what to expect when configuring access rights for Net Folders. Furthermore, the access rights that you define on a Net Folder affect how items can be accessed by users who receive shares to items in the Net Folder.

- ◆ "Understanding Access Rights for Net Folders" on page 82
- ◆ "Understanding Sharing Rights for Net Folders" on page 82

Understanding Access Rights for Net Folders

When you configure a Net Folder, users who already have rights to files and folders on the file system rights (or on the file repository in the case of SharePoint) are granted the same rights in Filr only when all of the following conditions are met:

- ◆ The users are synchronized to the Filr system via the LDAP synchronization process (as described in Section 18.1, "Synchronizing Users and Groups from an LDAP Directory," on page 193).
- ◆ If the users' file system rights are contingent on membership in a particular group on the file system, those groups are also synchronized to the Filr system via the LDAP synchronization process (as described in Section 18.1, "Synchronizing Users and Groups from an LDAP Directory," on page 193).
- ◆ The users are given access rights within the Net Folder, either individually or as part of a group in Filr (as described in Section 8.6, "Creating and Managing Net Folders," on page 101).

After you assign users rights to the Net Folder, users are granted the same level of access rights that they currently have on the file system.

If you assign users access rights within the Net Folder and those users do not already have file system rights, they are not able to see files and folders within the Net Folder.

Understanding Sharing Rights for Net Folders

- ◆ "Users Must Have File System Rights to Share from Filr" on page 82
- ◆ "Users Do Not Need File System Rights to Receive a Share" on page 85

Users Must Have File System Rights to Share from Filr

Users who share files from a Net Folder can grant Viewer, Editor, or Contributor access to the file, depending on their rights in the file system. For users to grant these rights to another user, they must have the minimum rights that those roles require, as outlined in the following tables:

Table 8-1   *NSS File System Rights Required for Net Folder Roles*

Role and Minimum NSS Rights Required	Comments
Viewer Role NSS Rights **R**ead **F**ile scan eDirectory User Target File or Folder	To view files through Filr, eDirectory users must have both `Read` and `File Scan` file system trustee rights on the target file or folder.
Editor Role NSS Rights **R**ead **F**ile scan **W**rite eDirectory User Target File or Folder	To modify file content through Filr, eDirectory users must have the `Write` file system trustee right in addition to `Read` and `File Scan`.
Contributor Role NSS Rights **R**ead **F**ile scan **W**rite **E**rase **C**reate **M**odify eDirectory User Target Folder	To perform contributor functions, eDirectory users must either have ◆ All file system trustee rights to the file or folder (except for `Access Control`) Or ◆ The `Supervisor` right to the file or folder The presence or absence of `Access Control` has no meaning in Filr because Filr cannot modify file system trustee rights. A Filr user with the `Access Control` right on the file system cannot grant *file system* access to another user through Filr. It is true that Filr users with sufficient Filr permissions can *share* access to files and folders with other users, but this is a Filr function that leverages the file system rights of Net Folder proxy users. Access to shared files and folders is independent of any file system rights that individual users have or do not have.
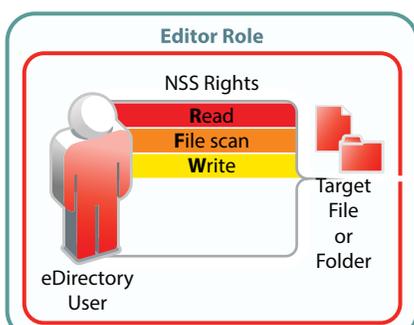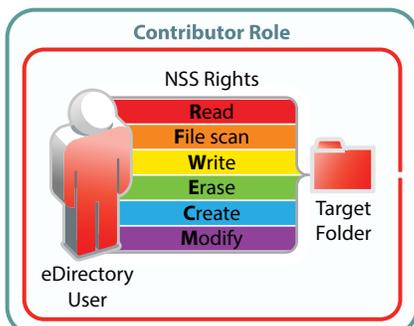
Table 8-2 *NTFS Permissions Required for Net Folder Roles*

Role and Minimum NTFS Permissions Required	Comments
Viewer Role NTFS Privileges **R**ead **R**ead & **E**xecute List Folder Content Target Folder Active Directory User	To view files and folders through Filr, Active Directory users must have `Read`, `Read & Execute`, and `List Folder Content` basic permissions on the target folder. The default special permissions associated with these basic permissions are also required.
Editor Role NTFS Privileges **R**ead **R**ead & **E**xecute List Folder Content **W**rite Target Folder Active Directory User	To modify file content through Filr, Active Directory users must have the basic `Write` permission in addition to `Read`, `Read & Execute`, and `List Folder Content` basic permissions on the target folder. The default special permissions associated with these basic permissions are also required.

Contributor Role
NTFS Privileges
Read
Read & **E**xecute
List Folder Content
Write
Modify
Target Folder
Active Directory User
The associated Special Permissions are also required.
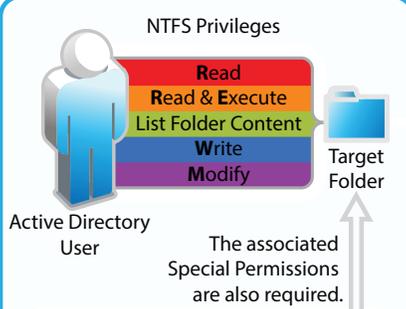 	
☐ Full control
☑ Traverse folder / execute file
☑ List folder / read data
☑ Read attributes
☑ Read extended attributes
☑ Create files / write data
☑ Create folders / append data
☑ Write attributes
☑ Write extended attributes
☐ Delete subfolders and files
☑ Delete
☐ Read permissions
☐ Change permissions
☐ Take ownership
	To perform contributor functions, users must either have
	
	◆ The basic `Full Control` permission
	
	  Or
	
	◆ The basic `Modify` permission included with the privileges required for the Editor role (`Write`, `Read`, `Read & Execute`, and `List Folder Content`)
	
	  IMPORTANT: The default special permissions associated with these basic permissions are also required as illustrated.

Table 8-3   *SharePoint Permissions Required for Net Folder Roles*

Role and Minimum SharePoint Permissions Required	Comments
Viewer Role SharePoint Permissions Use Remote Interfaces* View Items Browse User Information SharePoint Target SharePoint User	To view files and folders in SharePoint document libraries, SharePoint users must have the `Browse Directories`, `Browse User Information`, `Use Remote Interfaces*`, and `View Items` permissions in the document libraries.
Editor Role SharePoint Permissions Use Remote Interfaces* View Items Browse User Information Edit Items SharePoint Target SharePoint User	To modify file content, SharePoint users must have the `Edit` permission in addition to the permissions required for the Viewer role.
Contributor Role SharePoint Permissions Use Remote Interfaces* View Items Browse User Information Edit Items Add Items Delete Items SharePoint Target SharePoint User	To perform contributor functions, users must have the `Add Items` and `Delete Items` permissions in addition to all of the permissions required for the Viewer and Editor roles.

Users Do Not Need File System Rights to Receive a Share

Users who receive a share for a file on a Net Folder might or might not have file system rights to the shared file. Whether they have file system rights to the shared file affects how they can access the file in Filr. Users who do not have file system rights to a shared file can gain access to the file via the Net Folder Server proxy user. (For more information about the Net Folder proxy user, see Section 8.2, "Providing Net Folder Server Proxy Users," on page 91.)

Users can access shared items through the following methods from any of the Filr clients (web, desktop, or mobile), depending on their file system access rights:

- **From the Net Folders area (by navigating to the file):** Only users who have file system rights to the shared item and who have been granted access to the Net Folder in Filr. (Users are granted access to a file either through a share or from being granted access by the Filr administrator.)

◆ **In the Shared with Me area:** All users who receive a share.

8.1.5 Planning the Synchronization Method

When you synchronize files and folders in Net Folders, only file and folder metadata is synchronized. File content is only brought into Filr if you choose to have file content indexed as part of the Net Folder configuration, as described in Section 8.6, "Creating and Managing Net Folders," on page 101. File metadata must be synchronized before files can be viewed in a Filr app. When indexing is enabled for the Net Folder and the synchronization process indicates that file metadata is new or changed, the system flags the file as needing to be indexed during the next indexing cycle, which could be up to 10 minutes later.

When you configure Net Folders, you have the option to use one or both of the available synchronization methods (Full synchronization or Just-in-Time synchronization). Depending on the nature of your data, it might make sense to use full synchronization on some of your Net Folders and to use Just-in-Time synchronization on other Net Folders. You might want to use a combination of both methods of synchronization for other Net Folders.

Full synchronization: Synchronizes the metadata for all of the files and subfolders in a given Net Folder either on a set schedule or from a manual action. All files are examined for changes, and any changes are then synchronized.

This type of synchronization ensures that all files are synchronized; however, because it processes the entire Net Folder, it consumes more time and resources than Just-in-Time synchronization.

For information about the time required to perform a full synchronization on a Net Folder, see Section 8.1.8, "Planning the Amount of Data to Synchronize," on page 89.

Just-in-Time synchronization: Starts synchronizing the contents of a folder when users browse to it in a Filr app (Mobile, Web, and Desktop).

The system processes metadata for up to 5 seconds, and then the initial results are returned to the browser view. (The **Maximum wait time for results** setting in **Net Folder Global Settings** sets

If folder processing has not finished, JITS continues processing in the background until the metadata for everything in the folder is processed. If the folder contains more files and subfolders than can be processed in the initial processing period, it's possible that not all of the files and subfolders will be immediately viewable, in which case a refresh would be required.

In contrast with a full synchronization, which walks the tree until all folders and subfolders are discovered, JITS always processes only one folder at a time. Processing the contents of a subfolder requires that the user browse to that subfolder.

Just-in-Time synchronization provides two key benefits:

◆ Users can see a folder's contents without needing to wait for all of the files and subfolders within a given Net Folder to synchronize. Only those files and subfolders that users want access to are synchronized.

◆ Files and subfolders are guaranteed to be more current. What users see is not constrained by the Net Folder synchronization schedule intervals (default is every 15 minutes).

If one user edits a file and saves it, another user who views the file only a few seconds later will see the recent change.

IMPORTANT: If you are providing content indexing (searchability), there is a significant drawback to relying only on JITS for sychronization.

Content indexing can only happen after a file's metadata is synchronized and the file is marked as needing to be indexed for searchability.

Therefore, if only JITS is used, the only files that will ever have their content indexed are those that users browse to in one of the Filr apps. In that case, files that are never browsed to will not be included in content search results.

For more detailed information about Just-in-Time synchronization, as well as how to enable it, see Section 8.8, "Enabling Just-in-Time Synchronization," on page 108.

When you plan the type of synchronization method to use for a given Net Folder, consider the nature of the content you plan to synchronize and how you plan to use it after it is synchronized. Table 8-4 and the sections that follow describe which synchronization method is most suitable for certain types of content and the way you intend to use that content in Filr.

Table 8-4 *Full Sync vs. Just-in-Time Sync*

	Static Content	Dynamic Content	Large Amounts of Data	Searchability of Data
Full Synchronization	X			X
Just-in-Time Synchronization		X	X	

- ◆ "Static versus Dynamic Data" on page 87
- ◆ "The Amount of Data" on page 88
- ◆ "Searchability of Data" on page 88

Static versus Dynamic Data

Depending on whether your data never changes (static) or is constantly changing (dynamic) should influence the type of synchronization method that you implement for the Net Folder.

Full synchronization is more suited for static content, while Just-in-Time synchronization is more suited for dynamic content.

For example, a Net Folder that contains static files, such as medical records that are read-only, might be best synchronized to Filr by running one manual synchronization and disabling the scheduled synchronization as well as the Just-in-Time synchronization. The files could then be accessed via Filr without any unnecessary load being placed on the Filr system.

Conversely, a Net Folder that contains dynamic files that users actively collaborate on, such as marketing documents for a company's current products, might be best synchronized to Filr by enabling Just-in-Time synchronization. Users would then always have the latest information when they access a file.

In some cases, you might want to enable both scheduled synchronization as well as Just-in-Time synchronization. In such cases, consider also the amount of data that is located on the Net Folder.

The Amount of Data

The amount of data on the Net Folder should influence the type of synchronization method that you implement, because of the system resources that are required to perform a scheduled synchronization. If a Net Folder contains a large amount of data, a scheduled synchronization might consume a large amount of system resources more frequently than is necessary.

If you have a large amount of data but still want the data to be searchable, you might consider running one full synchronization so that you can then index the data and use Just-in-Time synchronization thereafter.

Searchability of Data

Whether you want data to be immediately searchable might influence the type of synchronization method that you implement for the Net Folder, because a file's content cannot be indexed (and therefore is not returned in searches) until after the file's metadata is synchronized.

In a full synchronization, the synchronization process begins when you configure the Net Folder. In a Just-in-Time synchronization, the synchronization process begins at a given folder when a user accesses (browses to) the folder. After a folder is accessed and if the JITS time limit for refreshing metadata has lapsed (default is 60 seconds), the file and folder metadata is synchronized and the updated files can then be indexed.

NOTE: File indexing is disabled by default. You must enable file indexing for a given Net Folder if you want the files in the Net Folder to be searchable. You enable indexing during the creation of the Net Folder Server, as described in Section 8.5, "Configuring and Managing Net Folder Servers," on page 96, or during the creation of individual Net Folders, as described in Section 8.6, "Creating and Managing Net Folders," on page 101.

8.1.6 Planning the Synchronization Schedule

You can configure Net Folders and Net Folder Servers to be synchronized at a schedule that you specify.

Synchronization in this sense means that content is simply mirrored in Filr; it is not transferred from the remote file server for replication on the Filr storage. Only metadata such as the name, path, owner, trustees, and so forth is actually stored in Filr.

Consider the following when planning the synchronization schedule:

◆ Synchronizations can be scheduled only if you have configured the Net Folder or Net Folder Server to perform full synchronization as the synchronization method (as described in Section 8.1.5, "Planning the Synchronization Method," on page 86).

◆ When a schedule is configured on a Net Folder Server, all Net Folders associated with that Net Folder Server are synchronized on the same schedule. However, if you configure a separate synchronization schedule for an individual Net Folder, this schedule is used for synchronizing the Net Folder, instead of the Net Folder Server synchronization schedule.

♦ When setting the synchronization schedule, be aware that the schedule that you choose can greatly affect system performance. Consider the information in Table 8-5, "Net Folder Synchronization Example," on page 90 and avoid the following scenarios, which can cause your Filr system to be slow or sluggish:

  ♦ You configure Net Folder synchronization schedules among various Net Folders and Net Folder Servers in such a way so that Filr is constantly synchronizing information.

  ♦ A single synchronization schedule is so frequent that a new synchronization begins as soon as the previous one finishes.

TIP: If you have a Net Folder or Net Folder Server that contains hundreds of thousands of files, consider doing only one initial Full Synchronization (if you need all of the file content to be indexed and searchable), and using Just-in-Time synchronization as the ongoing synchronization process.

8.1.7   Planning a Clustered Filr System to Support Net Folder Synchronization

Performing a full synchronization on a Net Folder can consume a significant amount of resources on your Filr appliance. If you plan to synchronize thousands of files via Net Folders, you should configure a clustered Filr system that includes multiple Filr appliances.

In a clustered environment, it is a good idea to set aside a single Filr appliance to handle the load of any manual Net Folder synchronizations. (For information about how to perform a manual synchronization on a Net Folder, see "Synchronizing a Net Folder" on page 106.)

For more information about how to configure clustering, see "Multi-Server (Clustered) Deployment" in the *Filr 2.0: Installation and Configuration Guide*.

For more information about how to set aside a Filr appliance, see "Setting Aside a Filr Appliance for Re-Indexing and Net Folder Synchronization in a Clustered Environment" in the *Filr 2.0: Installation and Configuration Guide*.

8.1.8   Planning the Amount of Data to Synchronize

The time required to perform a full synchronization on a Net Folder varies depending on many factors, including the following:

♦ The configuration of your Filr system (Large vs. Small vs. Clustered deployment)

♦ The number of active users

♦ Whether indexing is enabled (all file content is indexed and searchable, or only file metadata is synchronized)

♦ The complexity and depth of the file server's directory tree and the LDAP directory

♦ Whether Just-in-Time synchronization is enabled

♦ The database type (MySQL vs. Microsoft SQL)

♦ The file server type (OES vs. Windows vs. NetWare vs. SharePoint 2013)

♦ The number of CPUs allocated to the Filr appliance

♦ The amount of memory allocated to the Filr appliance

Net Folder Synchronization Example

The example in Table 8-5 illustrates the time required to synchronize files from five Net Folders in a large Filr deployment (one Filr appliance, one database appliance, and one search index appliance) with the following environment:

- No indexing of content
- No active users on the system
- No Just-in-Time synchronization
- 100,000 files were synchronized
- 750 sub-directories in the file system
- OES file system
- MySQL database

Table 8-5   Net Folder Synchronization Example

	Number of Files Synchronized per Second	Number of Files Synchronized per Minute	Number of Files Synchronized per Hour
Initial Synchronization:	196	11,760	705,600
Ongoing Synchronization:	952	57,120	3,427,200

8.1.9 Planning the Number of Net Folders

Unless only a small number of files exist in a volume or share on a file server, it is unwise to create a single Net Folder at the root of a volume or share. Instead, create multiple Net Folders. With multiple Net Folders created, you can be more flexible with the way you administer the Net Folders, such as the synchronization methods that you use and the rate at which you synchronize data.

For example, you can synchronize the Net Folders to Filr using different synchronization methods, depending on the nature of the data that each Net Folder contains. If the data in one Net Folder is static, you can perform a full synchronization on that Net Folder. You're then free to perform a Just-in-Time synchronization on a different Net Folder that contains more dynamic data. (For more information about the types of synchronization methods, see Section 8.1.5, "Planning the Synchronization Method," on page 86.)

8.1.10 Planning the Time Zone of the Filr Appliance to Match the Time Zone of any File Servers

The Filr appliance and any file servers that the Filr appliance connects to via a Net Folder should be synchronized to the same time and to the same time zone. You configured the time zone of the Filr appliance during the appliance installation, as described in "Installing the Filr Appliance" in the *Filr 2.0: Installation and Configuration Guide*.

If time zones are not synchronized in this way, users might see conflicting creation and modification times for files.

8.2 Providing Net Folder Server Proxy Users

It is important that you understand the purpose, rights requirements, expected user name format, and character restrictions associated with the Net Folder Server proxy user before you configure a Net Folder Server.

8.2.1 Purpose of the Net Folder Server Proxy User

The Net Folder Server proxy user is used to read, write, create, and delete files on your corporate OES, NetWare, Windows, or SharePoint 2013 file servers on behalf of users who do not have native rights to the files, but have been granted rights via a Share in Filr.

For example, User A has native Read and Write access to a file on an OES server, and User B does not have any native access to that file. User A shares the file with User B in Filr and grants User B Read access. User B can now view the file within Filr because the Net Folder Server proxy user is giving User B the ability to read it, because of the Share. If User B tries to access the same file directly from the OES server, he does not have sufficient rights.

Users with native rights to files do not use the Net Folder Server proxy user.

The Net Folder Server proxy user is not the same as the LDAP proxy user used to synchronize users and groups (as described in "Base DN:" on page 198).

8.2.2 Rights Requirements for the Proxy User

The Net Folder Server proxy user that you specify here synchronizes volume objects and file objects. Ensure that this proxy user has rights to access the files and folders for the Net Folder that will be associated to the Net Folder server. Specifically, the Net Folder Server proxy user should have the rights shown in the following graphic:

Figure 8-2   *Proxy User Rights Summary*
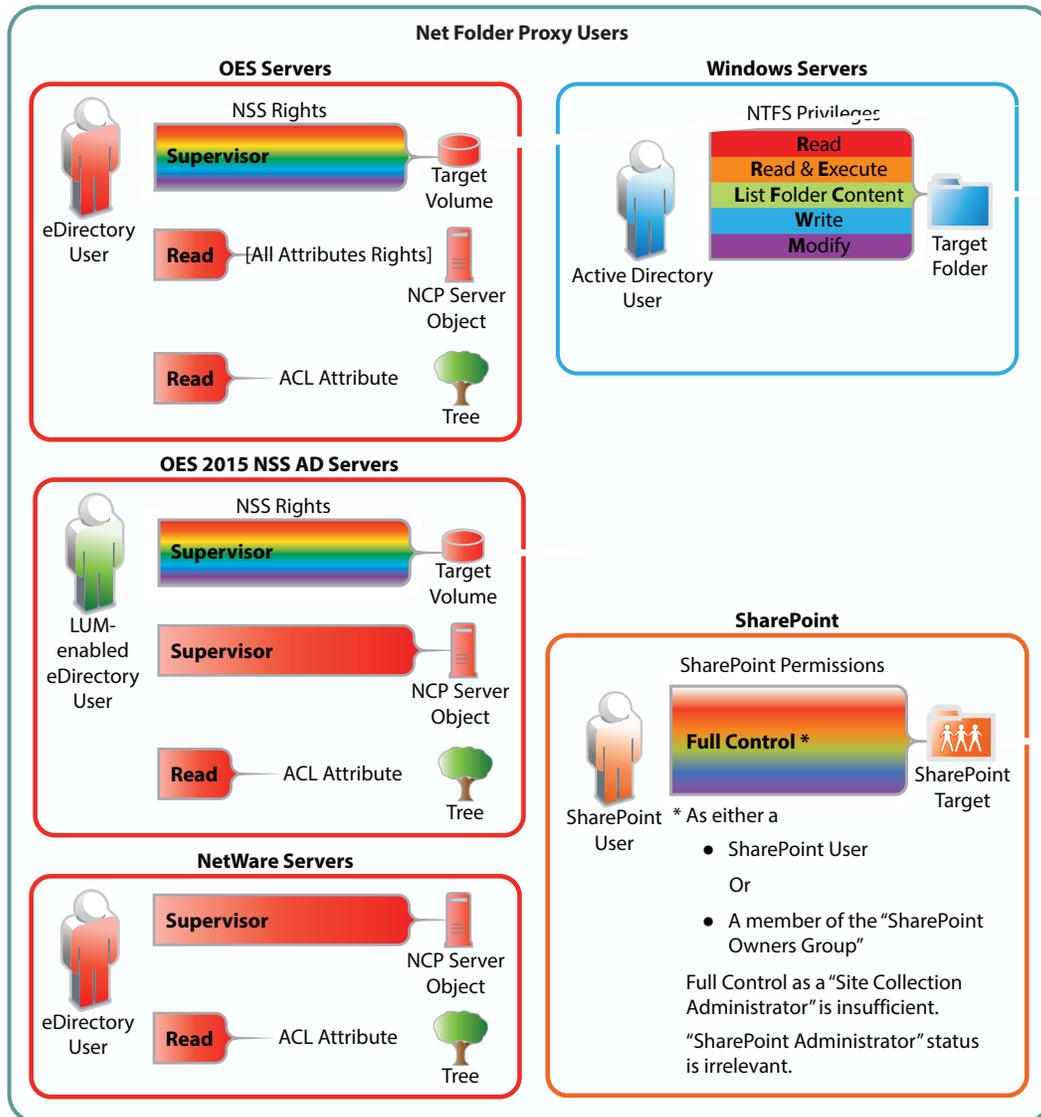
8.2.3 Requirements for Proxy User Names

Net Folder Server proxy users are key to Net Folder functionality. Ensure that you comply with the requirements in the following sections.

Platform Requirements

Name requirements differ depending on whether the proxy user is accessing an OES, OES (NSS for AD), NetWare, Windows, or SharePoint 2013 file server. Only the following syntax is supported:

- **OES/OES (NSS for AD)/NetWare:** `cn=admin,o=context`
- **Windows:** `Administrator` or `cn=Administrator,cn=users,dc=domain,dc=com,` `domain\user`, `user@domain`
- **SharePoint 2013:** `filrad\administrator`

- **DFS:** When using Distributed File System (DFS) namespaces, the proxy user name format must be `domain\user`. For example, `acme\administrator`.

Use the LDAP Browse Button

To ensure that the Net Folder Server proxy user name is formatted correctly, use the **Browse** icon next to the **Proxy** field to browse the LDAP directory (eDirectory or Active Directory) for the proxy user that you want to use.

IMPORTANT: If you are selecting the proxy user for an NSS for AD volume, be sure to select the eDirectory tree, not the AD Domain.

Special Characters and Spaces Not Supported

Proxy names that contain special characters and/or spaces are not supported. For example, `adminuser` is supported, but `@dm!n` and `admin user` are not. Other special characters that are not supported in the proxy name are `/ \ [ ] : | = , + * ? < > @ "`.

Consider Using Proxy Identities

Defining proxy user identities can greatly simplify selecting proxy users for Net Folder Servers and managing them thereafter.

8.3 Proxy User Identities

Path to Configuration Dialog: Filr Administration Console > **Management > Proxy Identities**

You can simplify the management of Net Folder Proxy Users by creating Proxy Identities for them as follows:

1 Define a proxy identity for each of your Net Folder Proxy Users.

    1a In Filr Administration Console > **Management > Proxy Identities**, click **New Proxy Identity...**

    1b Assign the identity an arbitrary name that identifies the proxy user. For example, `accounting-server-nf-proxy`.

    1c Using the LDAP browser, navigate to the user and select it.

    1d Specify and verify the user's password.

    1e Click **OK**.

2 When you configure a Net Folder Server, instead of browsing to the proxy user, you can select its associated Proxy User Identity in a drop-down list.

3 When the proxy user's password changes on the backend LDAP server, you need only change it in the Proxy User Identity dialog rather than in each Net Folder Server definition.

8.4 Configuring Home Folders for Display in the My Files Area

Most organizations using Open Enterprise Server (OES) or Windows will have user Home folders. If your organization has existing Home folders for users, the Net Folder Server will be discovered and created automatically when you provision users during the LDAP synchronization process. (For information about how to synchronize users via LDAP, see Section 18.1, "Synchronizing Users and Groups from an LDAP Directory," on page 193.) After the synchronization is complete, you are reminded to complete the Net Folder Server setup (by adding proxy credentials) when logging in to the Filr administration console.

If your organization does not currently leverage user Home folders on OES or Windows, you must first create a connection to your existing file system by creating a Net Folder Server. Then you can create a connection to specific volumes (on OES servers) and shares (on Windows servers) by creating a Net Folder.

- Section 8.4.1, "Configuring Home Folders," on page 94
- Section 8.4.2, "Editing Home Folders for Individual Users," on page 95
- Section 8.4.3, "Understanding How Home Folders Relates to Personal Storage," on page 96

8.4.1 Configuring Home Folders

- "Prerequisites" on page 94
- "Configuring Home Folders" on page 94

Prerequisites

If you are using Active Directory, the Active Directory Home folder for users must be configured as if it were on a network folder, even if the Home folder is local to the server. It cannot be configured on a local path.

To change a user's Home folder to be configured as a network folder:

1. In the Active Directory Administrative Center, access a user's profile information.
2. In the **Profile** section, in the **Home folder** area, select **Connect**.
3. Select a drive in the drop-down list, then use the **To** field to specify the path to the local directory.

   For example, `\\172.17.2.3\HOME\jchavez`

Configuring Home Folders

To configure Home Folders to be displayed in the My Files area:

1. Configure synchronization from your LDAP directory, as described in Section 18.1, "Synchronizing Users and Groups from an LDAP Directory," on page 193.
2. Configure the Net Folder Server, as described in Section 8.5, "Configuring and Managing Net Folder Servers," on page 96.

   IMPORTANT: The Filr administrator must supply proper proxy account information for Net Folder Servers that contain home directories before any end user logs in to Filr. This is because Filr automatically synchronizes the metadata for each user's Home folder using the appropriate

Net Folder Server with its associated proxy user credentials when the user logs in for the first time. See "How Filr Makes Files and Folders Visible to Users" in the *Filr 2.0: Understanding How Filr Works*.

If you do not supply the proxy account information before the user logs in, the Home directories' metadata is not synchronized correctly and the internal log files contain Null Pointer Exceptions.

Similarly, if the user Home folder is moved on the file system to a different volume or share or a different server, a new Net Folder Server is created and its metadata must be synchronized the first time the user logs in to Filr after the move.

3 (Optional) Allow users to have files and folders in personal storage in the My Files area in addition to the Home folder.

Whether users are allowed to have files in personal storage in the My Files area affects how the Home folder is displayed in the My Files area. For more information, see Chapter 7, "Setting Up Personal Storage," on page 73.

NOTE: A user's personal workspace (including the Home folder) is not displayed until the user has logged in to one of the Filr clients (web, mobile, or desktop) at least one time.

8.4.2 Editing Home Folders for Individual Users

After Home folders have been configured as described in Section 8.4.1, "Configuring Home Folders," on page 94, you can edit the Home folder settings for individual users:

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

    1a Launch a web browser.

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

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

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

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

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

3 Under **Management**, click **User Accounts**.

4 Click the drop-down arrow next to the user whose properties you want to view, then click **User Properties**.

The User Properties page is displayed.

5 Click **Edit Home Folder**. (This option is displayed only if a Home folder has been configured for the user, as described in Section 8.4.1, "Configuring Home Folders," on page 94.)

6 Make any modifications to the configuration, synchronization schedule, and data synchronization settings.

For information about each option that you can modify for Net Folders, see Section 8.6, "Creating and Managing Net Folders," on page 101.

7 Click **OK** to save your changes.

8.4.3 Understanding How Home Folders Relates to Personal Storage

For information about how Home folders relate to Personal storage in Filr, see Section 7.1, "Understanding How Personal Storage Relates to Home Folders," on page 73.

8.5 Configuring and Managing Net Folder Servers

8.5.1 Configuring Net Folder Servers

IMPORTANT: NetApp devices that are running an ONTAP version earlier than 8.3.x, must be set to communicate using SMB v1. Otherwise, the connection with Filr 2.0 will fail. See Section A.2, "NetApp Net Folder Server Test Connection Fails," on page 317.

Net Folder Servers represent a physical OES, NetWare, Windows, or SharePoint 2013 file server. Net Folder Servers are connections to specific NSS volumes (on OES and NetWare servers), shares (on Windows servers), and sites (on SharePoint 2013 servers). You can set up multiple connections to each server as needed.

You can set up each Net Folder Server to synchronize on a schedule that you specify.

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

    1a Launch a web browser.

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

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

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

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

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

3 Under **Management**, click **Net Folder Servers**.

The Manage Net Folder Servers page is displayed.

4 (Conditional) If the LDAP synchronization process for importing users contains at least one user who has a Home folder associated with them, a Net Folder Server is ready to be configured immediately after running the LDAP synchronization process. (For more information about LDAP synchronization in Filr, see Section 18.1, "Synchronizing Users and Groups from an LDAP Directory," on page 193.)

In the **Name** column, click the LDAP server name that you synchronized during the LDAP synchronization process, then skip to Step 6.

5 (Conditional) If the LDAP synchronization process for importing users does not contain at least one user who has a Home folder associated with them, you need to manually add a new Net Folder Server. Or, you can run the LDAP synchronization, as described in .

To manually add a new Net Folder Server, click **Add**.
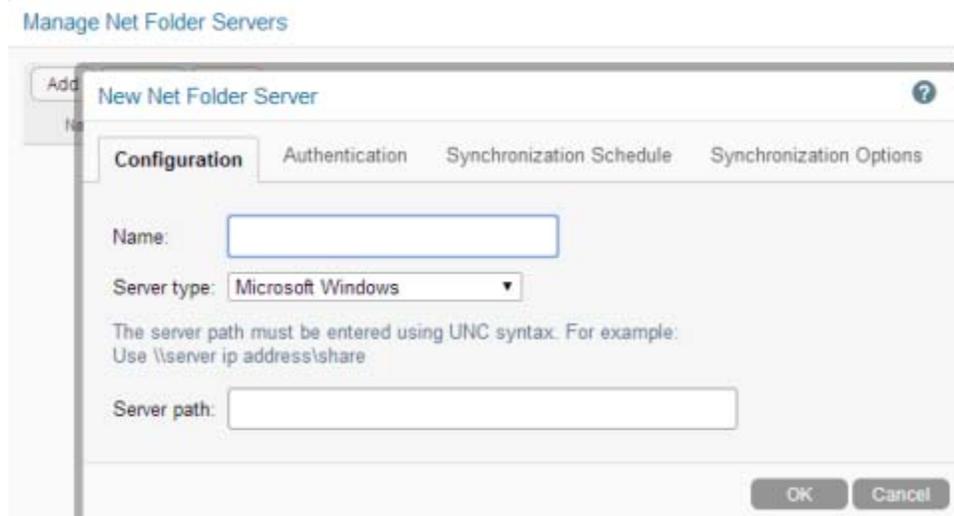
6 Whether you are adding a new Net Folder Server or configuring one that is synchronized through LDAP, you now need to configure it or finish configuring it.

On the **Configuration** tab, specify the following information:

Name: Specify a name for this Net Folder Server

This is already populated if the search context of your LDAP sync contains an OES or Windows server.

Server type: The type of file server, whether OES, OES 2015 (NSS for AD), NetWare, Windows or SharePoint 2013.

Server path: The path to the NSS volume (OES or NetWare), NSS volume on OES 2015, Windows share, or SharePoint 2013 site on the file server.

- ◆ **Windows:** The server path must be entered using UNC syntax. For example, `\\server_DNS\share`
- ◆ **OES or NetWare:** The server path must be entered using UNC syntax. For example, `\\server_DNS\volume`
- ◆ **SharePoint:** Specify the full URL to the SharePoint site. For example, `http://SharePoint_Server/site` or `https://SharePoint_Server/site`, depending on whether the SharePoint server is configured with SSL.

  If your SharePoint server is configured with SSL, you need to export the SSL certificate from SharePoint and import it into Filr in order for the Net Folder Server to function properly. For more information, see .

  Any document library within the Site Contents are in SharePoint can be synchronized to Filr.

The **Server path** field is already populated if the LDAP synchronization process for importing users contains at least one user who has a Home folder associated with them.

You can use DNS or IP address in the **Name** and **Server path** fields. DNS must be properly configured on the virtual appliance in order for it to work.

7 Click the **Authentication** tab, then specify the following information:

Proxy Identity: Specify the previously defined Proxy Identity that you created for the Net Folder Proxy User that has access to the OES, NetWare, Windows, or SharePoint 2013 server. For more information, see Section 8.3, "Proxy User Identities," on page 93.

Proxy name and password: Specify the fully qualified, comma-delimited name and password for the proxy user used to access the OES, NetWare, Windows, or SharePoint 2013 server. (You can use the **Browse** icon [⊞] next to the **Proxy** field to browse the LDAP directory for the proxy user that you want to use.)

IMPORTANT: Before you specify a proxy name and password for the Net Folder server, ensure that you review the information in Section 8.2, "Providing Net Folder Server Proxy Users," on page 91.

Test connection: Click this button to ensure that the path is accurate and that the credentials are valid, then click **OK** after the test succeeds.

Sometimes proxy users with the incorrect context pass this test. Ensure that the context for your proxy user is correct, as described in "Requirements for Proxy User Names" on page 92.

Authentication type: Select the authentication service for the file server that you are connecting to. This option corresponds with the **Server type** setting that you selected on the **Configuration** tab.

 ◆ If you selected **OES** or **NetWare** as the server type, only **Novell NMAS** is available as the authentication type.

 ◆ If you selected **OES (NSS for AD)** only **Auto Detect (Kerberos then NTLM)** is available as the authentication type.

 ◆ If you selected **Windows** as the server type, you can select either **Kerberos**, **NTLM**, or **Auto detect** as the authentication type. (Auto detect means that it tries authenticating with Kerberos first, and if that fails, authenticates with NTLM.)

NOTE: If **Kerberos** is selected as the authentication type, ensure that the DNS name server is able to resolve DNS queries for the Active Directory domains.

If the Kerberos port (port 88) is disabled on the Windows server, select **NTLM** as the authentication type.

---

8 To schedule the synchronization of the Net Folder Server, click the **Synchronization Schedule** tab, then select **Enable scheduled synchronization**.

Specify the schedule for when you want the synchronization between the file system server and Filr to occur. This becomes the default schedule for each Net Folder associated with this server.

Synchronizations can be scheduled only if you have configured the Net Folder Server to use Full Synchronization as the synchronization method (as described in Section 8.1.5, "Planning the Synchronization Method," on page 86). When setting the synchronization schedule, be aware that the schedule that you choose can greatly affect system performance.

Before you set a synchronization schedule, review the information in Section 8.1.6, "Planning the Synchronization Schedule," on page 88.

9 Click the **Synchronization Options** tab, then specify the following information:

Index the contents of Net Folders: Select this option to index all file content for each Net Folder associated with this Net Folder Server. (Before indexing can occur, file metadata must first be synchronized either via a full synchronization or Just-in-Time synchronization.)

When this option is selected, all content for each synchronized file within the Net Folders is indexed, and therefore is searched when performing a search in Filr. Deselect this option if you do not want file content to be indexed. This means that file content is not searched when

performing a search in Filr. However, file names and access controls are always indexed at the time of synchronization regardless of this setting. (For more information about content searchability, see "Searchability of Data" on page 88.)

File metadata must first be synchronized to Filr via a full synchronization or Just-in-Time synchronization before the indexing process can begin. For more information about the synchronization process, see Section 8.1.5, "Planning the Synchronization Method," on page 86.

Indexing is performed as a background process. Depending on the number of files that need to be indexed, it can take several hours or even days before all content is indexed and searchable in the Filr system.

Enable Just-in-Time synchronization: When you enable Just-in-Time synchronization, files are synchronized the moment users access them. Just-in-Time synchronization is one method that you can use to synchronize files from Net Folders to be accessed in Filr.

When enabling Just-in-Time synchronization, you can configure the following options:

- **Maximum age for Just-in-Time results (in seconds):** When a user clicks a folder or file, if it has been more than *x* seconds (x being the number that you specify) since the Just-in-Time operation retrieved information about this folder or file, it retrieves the information again. The default is 30 seconds.

- **Maximum age for ACL Just-in-Time results (in seconds):** When a user clicks a folder or file, if it has been more than x seconds (x being the number that you specify) since the Just-in-Time operation retrieved access control information about this folder or file, it retrieves the information again. The default is 60 seconds.

Allow the desktop app to trigger initial home folder sync: Select this option to ensure that user Home folders are synchronized to the Filr desktop application.

If this option is not selected, user Home folders are synchronized to the Filr desktop application only after the user logs in to Filr on the web, or after the Filr administrator triggers a full initial synchronization from the administration console (as described in "Synchronizing a Net Folder Server" on page 100).

When this option is selected, the Filr desktop application triggers a full initial synchronization of user Home folders on the Filr server. Home folder information is then synchronized to the Filr desktop application.

The following conditions must be met in order for the Filr desktop application to trigger an initial synchronization of a user's Home folder:

- The **Allow the desktop app to trigger initial home folder sync** option is selected.
- The user selects to synchronize the My Files area to the desktop application.
- The user's Home folder has not previously been synchronized to the Filr server.

10 Click **OK** > **Close**.

11 For Home folders to be displayed in the My Files area for each user, ensure that you have completed the steps in Chapter 7, "Setting Up Personal Storage," on page 73.

8.5.2 Managing Net Folder Servers

After Net Folder Servers already exist in your Filr system, you can manage them as described in this section.

- "Modifying a Net Folder Server" on page 100
- "Synchronizing a Net Folder Server" on page 100
- "Deleting a Net Folder Server" on page 101

Modifying a Net Folder Server

NOTE: You cannot modify a Net Folder Server's URL if the Net Folder Server was created automatically. Net Folder Servers are automatically created in the following scenarios:

- At the time of the LDAP synchronization (if the LDAP synchronization process for importing users contains at least one user who has a Home folder associated with them).
- When a user authenticates to Filr (if the user has a Home folder associated with them).

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

   1a Launch a web browser.

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

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

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

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

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

3 Under **Management**, click **Net Folder Servers**.

The Manage Net Folder Servers page is displayed.

4 Click the name of the Net Folder Server that you want to modify.

5 Make the desired modifications, then click **OK**.

For information about the options you can modify, see Section 8.5.1, "Configuring Net Folder Servers," on page 96.

Synchronizing a Net Folder Server

When you create a Net Folder Server, you can enable a synchronization schedule, as described in Section 8.5.1, "Configuring Net Folder Servers," on page 96.

To manually synchronize the Net Folder:

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

   1a Launch a web browser.

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

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

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

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

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

3 Under **Management**, click **Net Folder Servers**.

The Manage Net Folder Servers page is displayed.

4 Select the Net Folder Server that you want to manually synchronize, then click **Sync**.

Deleting a Net Folder Server

NOTE: Before you can delete a Net Folder Server, you must first delete any Net Folders that are associated with the Net Folder Server.

To delete a Net Folder Server after all Net Folders associated with the Net Folder Server have been deleted:

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

   1a Launch a web browser.

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

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

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

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

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

3 Under **Management**, click **Net Folder Servers**.

The Manage Net Folder Servers page is displayed.

4 Select the Net Folder Server that you want to delete, then click **Delete**.

8.6 Creating and Managing Net Folders

Net Folders are connections to specific directories on OES, NetWare, Windows, or SharePoint 2013 server. You can set up multiple connections for each Net Folder Server that you have previously configured. You can set up each Net Folder to synchronize on a schedule that you specify, independent of the schedule set for the Net Folder Server.

- Section 8.6.1, "Creating Net Folders," on page 102
- Section 8.6.2, "Managing Net Folders," on page 105

8.6.1 Creating Net Folders

Before you can create a Net Folder as described in this section, you must first create a Net Folder Server as described in Section 8.5, "Configuring and Managing Net Folder Servers," on page 96.

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

    1a Launch a web browser.

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

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

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

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

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

3 Under **Management**, click **Net Folders**.

   The Manage Net Folders page is displayed.

4 Click **Add**.

   The New Net Folder dialog box is displayed.
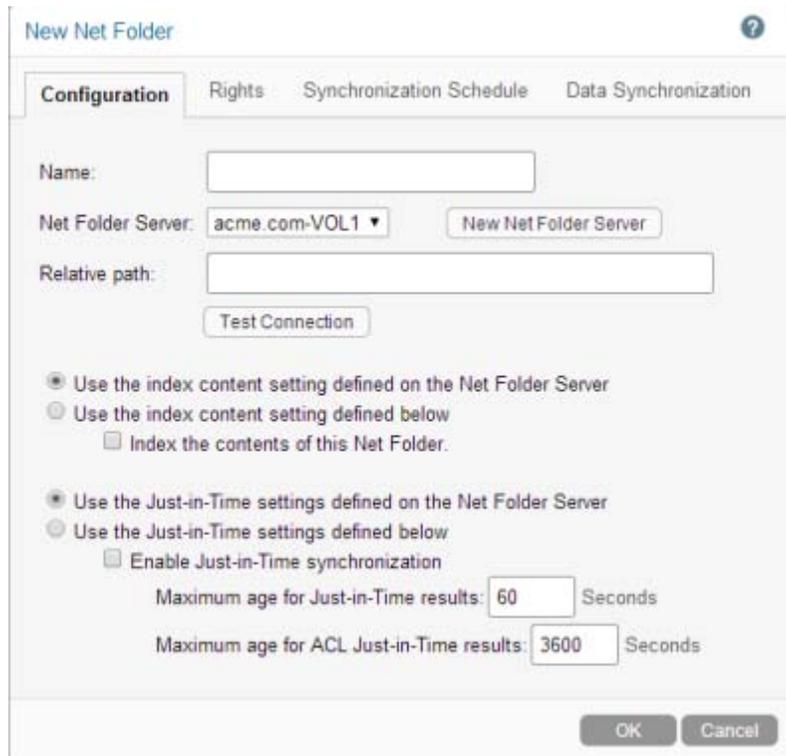
5 On the **Configuration** tab, specify the following information:

Name: Specify a name for the Net Folder. This is the name that users see when accessing the Net Folder. This can be any name you choose.

Net Folder Server: Select the Net Folder Server that the new Net Folder is associated with.

New Net Folder Server: Click this option if you have not already established a connection to a Net Folder Server, as described in Section 8.5, "Configuring and Managing Net Folder Servers," on page 96.

Relative Path: Specify the relative path to the folder on the Net Folder Server that you want this Net Folder to represent. If this field is left blank, it uses the root of the Net Folder Server. (The root of the Net Folder Server is the OES volume, the Windows share, or the SharePoint site.)

For example, if the relative path to the folder on your Net Folder Server that you want this Net Folder to represent is `\\server_address\vol1\marketing`, and `\\server_address\vol1` is the server path to your Net Folder Server, you would enter `marketing` in the **Relative Path** field for the Net Folder.

The path must be entered using UNC syntax.

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.

Test connection: Click this option to test the connection to the Net Folder.

Use the index content setting defined on the Net Folder Server: Select this option to configure this Net Folder to retain the same setting for indexing content as you selected for the Net Folder Server.

For example, if you configured the Net Folder Server to index content, select this option to index content for this Net Folder.

Use the index content setting defined below: Select this option to configure this Net Folder with a different setting for indexing content than you configured for the Net Folder Server.

For example, if you configured the Net Folder Server to not index content, but you want this Net Folder server to index content, select this option and also select the following option, **Index the contents of this Net Folder**.

- ◆ **Index the contents of this Net Folder:** When this option is selected, all content for each file within the Net Folder is indexed, and therefore is searched when performing a search in Filr. (Before indexing can occur, file metadata must first be synchronized either via a full synchronization or Just-in-Time synchronization.)

  Deselect this option if you do not want file content to be indexed. This means that file content is not searched when performing a search in Filr. However, file names and access controls are always indexed at the time of synchronization regardless of this setting. (For more information about content searchability, see "Searchability of Data" on page 88.)

  Files must first be synchronized to Filr before the indexing process can begin. For more information about the synchronization process, see Section 8.1.5, "Planning the Synchronization Method," on page 86.

  Indexing is performed as a background process. Depending on the number of files that need to be indexed, it can take several hours or even days before all content is indexed and searchable in the Filr system.

Use the Just-in-Time settings defined on the Net Folder Server: Select this option to configure this Net Folder to retain the same setting for Just-in-Time synchronization as you selected for the Net Folder Server.

For example, if you configured the Net Folder Server to use Just-in-Time synchronization, select this option to use Just-in-Time synchronization for this Net Folder.

Use the Just-in-Time settings defined below: Select this option to configure this Net Folder with different Just-in-Time synchronization settings than you configured for the Net Folder Server.

For example, if you configured the Net Folder Server to not use Just-in-Time synchronization, but you want this Net Folder server to use Just-in-Time synchronization, select **Enable Just-in-Time synchronization**. You can also modify synchronization options.

- **Enable Just-in-Time synchronization:** When you enable Just-in-Time synchronization, files are synchronized the moment users access them. Just-in-Time synchronization is one method that you can use to synchronize files from Net Folders to be accessed in Filr.

  When enabling Just-in-Time synchronization, you can configure the following options:

  - **Maximum age for Just-in-Time results (in seconds):** When a user clicks a folder or file, if it has been more than *x* seconds (x being the number that you specify) since the Just-in-Time operation retrieved information about this folder or file, it retrieves the information again. The default is 60 seconds.

  - **Maximum age for ACL Just-in-Time results (in seconds):** When a user clicks a folder or file, if it has been more than x seconds (x being the number that you specify) since the Just-in-Time operation retrieved access control information about this folder or file, it retrieves the information again. The default is 3600 seconds (1 hour).

There are various options for synchronizing files from a Net Folder. Before you decide on a synchronization method for a Net Folder, see Section 8.1.5, "Planning the Synchronization Method," on page 86.

6 Click the **Rights** tab, then use the **User or Group** field to 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:

- Individual users (either imported from the LDAP directory or that have been created in Filr)
- Groups (either imported from the LDAP directory or that have been created in Filr)
- Organization Units (when using eDirectory as the LDAP directory)

After you specify the user, group, or Organization Unit and select it, the Grant Rights dialog box is displayed.

7 In the Grant Rights dialog box, select **Allow access to the Net Folder**.

Users are granted the same level of access rights that they currently have on the file system. Users who have rights on the file system do not have access to the same files through Filr until this option is selected for them. If you select this option for users who do not currently have access rights on the file system, these users cannot see files within the Net Folder, but they are able to see the folder names. (This access is obtained via the Net Folder Server Proxy user. For more information about the Net Folder Server proxy user, see Section 8.2, "Providing Net Folder Server Proxy Users," on page 91.)

For more information, see Section 8.1.4, "Planning Access and Sharing for Net Folders," on page 82.

8 Select whether you want the users or groups that you specified in Step 6 to be able to share with internal users, external users, and the public, and whether you want to allow them to give users that they share with the ability to re-share items.

Users who receive a share for a Net Folder do not have file system rights to the shared item. This means they can access the shared item only in the Shared with Me area through one of the Filr clients (web, desktop, or mobile); they cannot access the shared item directly through a mapped drive on the file system nor can they access the shared item from the Net Folders area

through one of the Filr clients. This is because the Net Folder proxy user is used to grant the user access to an item through a share. (For more information about the Net Folder proxy user, see Section 8.2, "Providing Net Folder Server Proxy Users," on page 91.)

For more information, see Section 8.1.4, "Planning Access and Sharing for Net Folders," on page 82.

9 Click **OK** to save your rights changes.

10 (Optional) Click the **Synchronization Schedule** tab to configure the synchronization between the Net Folder and the file system server.

Specify the following information for the synchronization schedule:

Use the synchronization schedule defined on the Net Folder Server: If you already set a synchronization schedule for the Net Folder Server (as described in Section 8.5, "Configuring and Managing Net Folder Servers," on page 96), and if you want the Net Folder to use that same schedule, select this option. If you select this option, skip to Step 11.

Use the synchronization schedule defined below: Select this option to create an independent synchronization schedule for the Net Folder. (If you do set a synchronization schedule for the Net Folder, this schedule is used for synchronizing the Net Folder, instead of the Net Folder Server synchronization schedule.)

Synchronizations can be scheduled only if you have configured the Net Folder to use Full Synchronization as the synchronization method (as described in Section 8.1.5, "Planning the Synchronization Method," on page 86). When setting the synchronization schedule, be aware that the schedule that you choose can greatly affect system performance.

Before you set a synchronization schedule, review the information in Section 8.1.6, "Planning the Synchronization Schedule," on page 88.

- **Enable scheduled synchronization:** Select this option to enable the synchronization, then select from the following synchronization options:
  - **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.

11 (Optional) Click the **Data Synchronization** tab to configure whether the Net Folder is synchronized with the Filr desktop application.

Specify the following information:

Desktop application: Select this option to allow users to access files on the Net Folder via the Filr desktop application. (For more information about the Filr desktop application, see the Filr Desktop Application for Windows Quick Start (http://www.novell.com/documentation/novell-filr-2/filr-2-qs-desktop/data/filr-2-qs-desktop.html) or the Filr Desktop Application for Mac Quick Start (https://www.novell.com/documentation/novell-filr-2/filr-2-qs-desktopmac/data/filr-2-qs-desktopmac.html).)

12 Click **OK** to finish creating the Net Folder.

8.6.2 Managing Net Folders

After Net Folders already exist in your Filr system, you can manage them as described in this section.

- "Modifying a Net Folder" on page 106
- "Synchronizing a Net Folder" on page 106

Modifying a Net Folder

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

    1a Launch a web browser.

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

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

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

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

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

3 Under **Management**, click **Net Folders**.

The Manage Net Folders page is displayed.

4 (Optional) To filter the list of Net Folders, specify the name of a Net Folder in the **Filter List** field.

5 (Optional) To display user Home directories in the list of Net Folders, click the drop-down arrow next to the **Filter List** field, then select **Show Home Directories**.

6 Click the name of the Net Folder that you want to modify.

7 Make the desired modifications, then click **OK**.

Synchronizing a Net Folder

When you create a Net Folder, you can enable a synchronization schedule, as described in Section 8.6.1, "Creating Net Folders," on page 102.

To manually synchronize the Net Folder:

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

    1a Launch a web browser.

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

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

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

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

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

3 Under **Management**, click **Net Folders**.

The Manage Net Folders page is displayed.

4 Select the Net Folder that you want to manually synchronize, then click **Sync**.

In a clustered environment, it is a good idea to dedicate a single Filr appliance to handle the load of any manual Net Folder synchronizations. (For information about how to dedicate a Filr appliance, see "Setting Aside a Filr Appliance for Re-Indexing and Net Folder Synchronization in a Clustered Environment" in the *Filr 2.0: Installation and Configuration Guide*.)

Viewing the Synchronization Status of a Net Folder

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

1a Launch a web browser.

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

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

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

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

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

3 Under **Management**, click **Net Folders**.

The Manage Net Folders page is displayed.

4 In the **Sync status** column, the synchronization status is displayed. You can click the icon for more detailed status information.

Deleting a Net Folder

To delete a Net Folder, and thereby delete access to files from the Net Folder from within Filr:

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

1a Launch a web browser.

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

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

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

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

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

3 Under **Management**, click **Net Folders**.

The Manage Net Folders page is displayed.

4 Select the Net Folder that you want to delete, then click **Delete**.

8.7 Setting Up Sharing for Net Folders

To allow users to share files that are located in a Net Folder, you as the Filr administrator must give users the proper share rights when setting up the net folder or when modifying the Net Folder's configuration. Ensure that:

- Users who you want to be allowed to view files (and by extension, receive shared items) for files in the Net Folder have been given the **Allow Access to the Net Folder** right. For information about how to give users this right, see Chapter 6, "Setting Up Sharing," on page 63.

- Users who you want to be allowed to share files that are located in the Net Folder have been given one of the appropriate Share rights (located on the **Rights** tab when creating or modifying a Net Folder), as described in Section 8.6, "Creating and Managing Net Folders," on page 101 and Section 8.10, "Modifying Net Folder Connections," on page 114.

When you create a Net Folder, you specify which users you want to be allowed to access files on the Net Folder. Users who already have file system rights to files have the same rights to these files in Filr. Users who do not have file system rights to files are not able to see the files and folders unless items have been shared with them. It is up to you as the Filr administrator whether users with native rights are allowed to share these files with others.

IMPORTANT: If a user moves or renames a file directly from the file server (instead of using a Filr client to do the move or rename), any shares that are associated with that file in Filr are removed. This means that users who gained access to a file via a share in Filr no longer have access to the file if the file was renamed or moved from the file server. Additionally, the file is not displayed in users' Shared by Me and Shared with Me views.

If this situation occurs, files must be re-shared in Filr.

8.8 Enabling Just-in-Time Synchronization

You can enable Just-in-Time synchronization for a given Net Folder in addition to or in place of full synchronization. Before you decide on a synchronization method for a Net Folder, see Section 8.1.5, "Planning the Synchronization Method," on page 86.

Just-in-Time synchronization (JITS) is one method that you can use to synchronize files from Net Folders to be accessed in Filr. When you enable Just-in-Time synchronization, files are synchronized the moment users browse to the folder where they are located. This means that the files and folders that users see in Filr are guaranteed to be more current and that processes to make the files and folders available for viewing and access are less resource-intensive.

Just-in-Time synchronization provides two key benefits:

- Users can see a folder's contents without needing to wait for all of the files and subfolders within a given Net Folder to synchronize. Only those files and subfolders that users want access to are synchronized.

- Files and subfolders are guaranteed to be more current. What users see is not constrained by the Net Folder synchronization schedule intervals (default is every 15 minutes).

  If one user edits a file and saves it, another user who views the file only a few seconds later will see the recent change.

You must enable Just-in-Time synchronization in the Net Folder Settings dialog before you can enable Just-in-Time synchronization for individual Net Folders.

8.8.1 Enabling Just-in-Time Synchronization for the Filr System

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

  1a Launch a web browser.

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

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

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

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

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

3 Under **Management**, click **Net Folder Settings**.

The Net Folder Global Settings page is displayed.

The following options for configuring Just-in-Time synchronization are available:

Enable Just-in-Time synchronization of Net Folders: Select this option to allow Just-in-Time synchronization to be enabled for Net Folders in your Filr system. You can enable or disable Just-in-Time synchronization on specific Net Folder Servers or Net Folders.

- **Maximum wait time for results (in seconds):** When a user clicks on a folder, the Just-in-Time operation retrieves the associated metadata for *x* seconds (x being the number that you specify). If the operation has not completed its work within *x* seconds, it returns to the user the work it has done up to that point, and the work continues in the background. The default is 5 seconds.

4 Click **OK**.

5 Enable Just-in-Time synchronization for each Net Folder where you want this type of synchronization to occur, as described in Section 8.8.3, "Enabling Just-in-Time Synchronization for a Specific Net Folder," on page 111.

8.8.2 Enabling Just-in-Time Synchronization for a Net Folder Server

Just-in-Time synchronization settings that are set for specific Net Folder Servers are not active until Just-in-Time synchronization has been enabled at the system level, as described in Section 8.8.1, "Enabling Just-in-Time Synchronization for the Filr System," on page 109.

By default, Just-in-Time synchronization settings are applied to all Net Folders associated with the Net Folder Server.

To enable Just-in-Time synchronization for a specific Net Folder Server:

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

    1a Launch a web browser.

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

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

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

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

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

3 Under **Management**, click **Net Folder Servers**.

    The Manage Net Folder Servers page is displayed.

4 Click the name of the Net Folder Server where you want to enable Just-in-Time synchronization.

5 On the **Synchronization Options** tab, select **Enable Just-in-Time synchronization**, then specify the following options:

    Maximum age for Just-in-Time results (in seconds): When a user clicks a folder or file, if it has been more than *x* seconds (x being the number that you specify) since the Just-in-Time operation retrieved information about this folder or file, it retrieves the information again. The default is 60 seconds.

    Maximum age for ACL Just-in-Time results (in seconds): When a user clicks a folder or file, if it has been more than x seconds (x being the number that you specify) since the Just-in-Time operation retrieved access control information about this folder or file, it retrieves the information again. The default is 3600 seconds (1 hour).

6 Click **OK** to save your changes.

8.8.3 Enabling Just-in-Time Synchronization for a Specific Net Folder

Just-in-Time synchronization settings that are set for specific Net Folders are not active until Just-in-Time synchronization has been enabled at the system level, as described in Section 8.8.1, "Enabling Just-in-Time Synchronization for the Filr System," on page 109.

To enable Just-in-Time synchronization for a specific Net Folder:

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

    1a Launch a web browser.

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

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

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

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

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

3 Under **Management**, click **Net Folders**.

    The Manage Net Folders page is displayed.

4 Click the name of the Net Folder where you want to enable Just-in-Time synchronization.

5 On the **Configuration** tab, select **Use the Just-in-Time settings defined below**, then specify the following options:

    Enable Just-in-Time synchronization: When you enable Just-in-Time synchronization, files are synchronized the moment users access them. Just-in-Time synchronization is one method that you can use to synchronize files from Net Folders to be accessed in Filr.

    When enabling Just-in-Time synchronization, you can configure the following options:

       ◆ **Maximum age for Just-in-Time results (in seconds):** When a user clicks a folder or file, if it has been more than *x* seconds (x being the number that you specify) since the Just-in-Time operation retrieved information about this folder or file, it retrieves the information again. The default is 60 seconds.

       ◆ **Maximum age for ACL Just-in-Time results (in seconds):** When a user clicks a folder or file, if it has been more than x seconds (x being the number that you specify) since the Just-in-Time operation retrieved access control information about this folder or file, it retrieves the information again. The default is 3600 seconds (1 hour).

6 Click **OK** to save your changes.

8.8.4 Enabling Just-in-Time Synchronization for a Specific User's Home Directory

Just-in-Time synchronization settings that are set for specific user's Home directory are not active until Just-in-Time synchronization has been enabled at the system level, as described in Section 8.8.1, "Enabling Just-in-Time Synchronization for the Filr System," on page 109.

To enable Just-in-Time synchronization for a specific user's Home directory:

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

    1a Launch a web browser.

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

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

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

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

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

3 Under **Management**, click **Users**.

4 Click the drop-down arrow next to the user whose properties you want to view, then click **User Properties**.

    The User Properties page is displayed.

5 Click **Edit Home Folder**. (This option is displayed only if a Home folder has been configured for the user, as described in Section 8.4.1, "Configuring Home Folders," on page 94.)

6 On the **Configuration** tab, select **Enable Just-in-Time synchronization**, then specify the following options:

    Maximum age for Just-in-Time results (in seconds): When a user clicks a folder or file, if it has been more than *x* seconds (x being the number that you specify) since the Just-in-Time operation retrieved information about this folder or file, it retrieves the information again. The default is 30 seconds.

    Maximum age for ACL Just-in-Time results (in seconds): When a user clicks a folder or file, if it has been more than x seconds (x being the number that you specify) since the Just-in-Time operation retrieved access control information about this folder or file, it retrieves the information again. The default is 60 seconds.

7 Click **OK** to save your changes.

8.9 Setting Global Net Folder Configuration Options

To modify global configuration options that affect all Net Folders in your Filr system:

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

   1a Launch a web browser.

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

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

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

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

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

3 Under **Management**, click **Net Folder Settings**.

The Net Folder Global Settings page is displayed.

The following options are available:

Enable Just-in-Time synchronization of Net Folders: Select this option to allow Just-in-Time synchronization to be enabled for Net Folders in your Filr system. You can enable or disable Just-in-Time synchronization on specific Net Folder Servers or Net Folders.

   ◆ **Maximum wait time for results (in seconds):** When a user clicks on a folder, the Just-in-Time operation retrieves the associated metadata for *x* seconds (x being the number that you specify). If the operation has not completed its work within *x* seconds, it returns to the user the work it has done up to that point, and the work continues in the background. The default is 5 seconds.

For more detailed information about configuring Just-in-Time synchronization at a global level, see Section 8.8.1, "Enabling Just-in-Time Synchronization for the Filr System," on page 109. For more generic information about Just-in-Time synchronization, as well as how to enable it for specific Net Folders, see Section 8.8, "Enabling Just-in-Time Synchronization," on page 108.

Use directory rights in addition to file system rights: When this option is selected, Filr consults eDirectory for user and group rights information when accessing files and folders on the file system via a Net Folder. Users and groups who have inherited Supervisor rights on the NCP server object (and therefore have implicit rights on the volume) in eDirectory are considered as trustees.

This option is enabled by default. You might want to disable this option if no users are inheriting Supervisor rights from eDirectory. If users are inheriting Supervisor rights from eDirectory, disabling this option might affect users' ability to access certain files.

Changes made to this option take effect at the system level the next time the 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 *xx* Minutes: Specify the frequency that the Filr server checks the rights information from the OES file system and from eDirectory. (The option **Use directory rights in addition to file system rights** must be selected in order for Filr to check the rights information from eDirectory.)

The default for refreshing cached rights information is every 5 minutes.

Rights information is available in Filr only after one of the following occurs since the last successful cache refresh:

- Someone triggers Just-in-Time synchronization on the folder.
- A Full (manual) synchronization is triggered on the folder.

  For information about how to perform a manual synchronization, see "Synchronizing a Net Folder" on page 106 and "Synchronizing a Net Folder Server" on page 100.

- A scheduled synchronization is triggered on the folder.

IMPORTANT: The **Refresh cached rights information every xx Minutes** option affects only OES file systems; NetWare, Windows, and SharePoint file systems are not affected.

With **NetWare** file systems, rights information is refreshed every 60 minutes.

With **Windows** and **SharePoint** file systems, rights information is refreshed by Full (manual) synchronizations, scheduled synchronizations, and JITS operations if enabled.

In light of this, managing Net Folder synchronization options is critical to Filr being able to reflect users' current rights. It is also inevitable that Net Folder users might not see rights changes immediately reflected by Filr.

4 Click **OK**.

8.10 Modifying Net Folder Connections

You can modify the connection settings for a Net Folder after the Net Folder has been created. You can modify configuration settings, rights that users have in the Net Folder, the synchronization schedule, and whether the Net Folder can be accessed via the Filr desktop application and the Filr mobile app.

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

   1a Launch a web browser.

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

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

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

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

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

3 Under **Management**, click **Net Folders**.

   The Manage Net Folders page is displayed.

4 Click the name of the Net Folder that you want to modify.

   For information about each option that you can modify for Net Folders, see Section 8.6, "Creating and Managing Net Folders," on page 101.

5 Click **OK** to save your changes.

9 Creating Groups of Users

This section describes how to create groups within Filr. You can also synchronize groups of users from your LDAP directory to your Novell Filr site, as described in Section 18.1, "Synchronizing Users and Groups from an LDAP Directory," on page 193.

You might want to create groups for any of the following reasons:

 ◆ To facilitate sharing on your Filr site. For background information on sharing, see Chapter 6, "Setting Up Sharing," on page 63.
 ◆ To facilitate managing data quotas, as described in Section 22.2, "Managing User Data Quotas," on page 234.

You can create either static or dynamic groups.

 ◆ Section 9.1, "Creating Static Groups," on page 115
 ◆ Section 9.2, "Creating Dynamic Groups," on page 117

9.1 Creating Static Groups

Static groups are groups whose membership does not change based on LDAP queries.

This section describes how to create static groups directly from Filr. Alternatively, you can synchronize static groups to Filr from your LDAP directory as described in Section 18.1, "Synchronizing Users and Groups from an LDAP Directory," on page 193.

To create static groups in Filr:

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

   1a Launch a web browser.

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

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

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

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

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

3 Under **Management**, click **Groups**, then click **Add**.

4 Fill in the following fields:

Name: Specify the unique name under which the group is stored in the Filr database. You can use only alphanumeric characters (a-z, A-Z, 0-9), hyphens (-), and underscores (_).

This is the name that appears to users in Filr.

You can modify the name completion settings (the group name that is displayed when users are specifying the group, such as in the Share dialog) to use the Title instead of the Name.

For more information about modifying the name completion settings, see Section 19.5, "Managing How Group Names Are Displayed during Name Completion," on page 225.

Title: Enter a descriptive group title. This string can include any characters that you can type.

You can modify the name completion settings (the group name that is displayed when users are specifying the group, such as in the Share dialog) to use the Title instead of the Name.

For more information about modifying the name completion settings, see Section 19.5, "Managing How Group Names Are Displayed during Name Completion," on page 225.

Description: Describe what the members of this group have in common.

5 Select **Group membership is static**.

This means that group membership does not change based on LDAP queries.

6 Click **Edit group membership**.

7 Select **Allow external users and groups** if you want to allow external users and groups to be members of the group that you are creating.

8 Click the **Users** or **Groups** tab, depending on whether you want to add users or groups to the group that you are creating.

9 In the **User** or **Group** field, specify the name of the user or group that you want to add to the group that you are creating, then click the name of the user or group when it appears in the drop-down list.

10 Repeat Step 8 and Step 9 to add multiple users and groups to the group that you are creating, then click **OK** when you have finished adding users and groups.

11 Click **OK** to create the group.

After you have created one or more small groups, you can use the **Groups** field to create larger groups from smaller groups.

9.2 Creating Dynamic Groups

Groups based on LDAP queries are dynamic because they can be configured to have their membership updated when the information in the LDAP directory changes.

Creating groups based on LDAP queries is a quick way to create Filr groups that consist of users who match specific criteria. You can create dynamic groups as described in the following sections:

- Section 9.2.1, "Creating Dynamic Groups within LDAP," on page 118
- Section 9.2.2, "Creating Dynamic Groups within Filr," on page 118

9.2.1 Creating Dynamic Groups within LDAP

Depending on the LDAP directory that you are using, you might be able to create dynamic groups within your LDAP directory. For example, you can create dynamic group objects in eDirectory with NetIQ iManager (for more information, see the iManager Documentation (https://www.netiq.com/documentation/imanager27/)).

Dynamic groups created within LDAP are stored in your LDAP directory and can then be synchronized to Filr, as described in Section 18.1, "Synchronizing Users and Groups from an LDAP Directory," on page 193.

9.2.2 Creating Dynamic Groups within Filr

You can create dynamic groups in Filr by querying the LDAP directory.

- "Prerequisites" on page 118
- "Advantages" on page 118
- "Considerations with Multiple LDAP Sources" on page 119
- "Creating the Group" on page 119

Prerequisites

- 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 197.

  The Filr process that creates a dynamic group uses the LDAP configuration settings in Filr to authenticate to the LDAP directory server. 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 Section 18.1, "Synchronizing Users and Groups from an LDAP Directory," on page 193.

Advantages

Advantages to creating dynamic groups within Filr rather than within your LDAP directory include the following:

- Allows the Filr administrator to control group membership without having direct access to the group object in the LDAP user store.
- Your LDAP directory might not support dynamic groups.
- You do not want dynamic groups to sync to applications other than Filr that are leveraging your LDAP directory.

Considerations with Multiple LDAP Sources

Consider the following if your Filr site is configured with multiple LDAP sources:

* You should not create dynamic groups in Filr if the base DN that you define for the dynamic group does not exist in each LDAP source. This is because 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.

Creating the Group

To create the dynamic group within Filr:

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

   1a Launch a web browser.

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

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

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

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

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

3 Under **Management**, click **Groups**, then click **Add**.

4 Fill in the following fields:

Name: Specify the unique name under which the group is stored in the Filr database. You can use only alphanumeric characters (a-z, A-Z, 0-9), hyphens (-), and underscores (_).

This is the name that appears to users in Filr.

You can modify the name completion settings (the group name that is displayed when users are specifying the group, such as in the Share dialog) to use the Title instead of the Name.

For more information about modifying the name completion settings, see Section 19.5, "Managing How Group Names Are Displayed during Name Completion," on page 225.

Title: Enter a descriptive group title. This string can include any characters that you can type.

You can modify the name completion settings (the group name that is displayed when users are specifying the group, such as in the Share dialog) to use the Title instead of the Name.

For more information about modifying the name completion settings, see Section 19.5, "Managing How Group Names Are Displayed during Name Completion," on page 225.

Description: Describe what the members of this group have in common.

5 Select **Group membership is dynamic**.

This means that group membership is based on an LDAP query that you will define in this procedure.

6 Click **Edit group membership**.
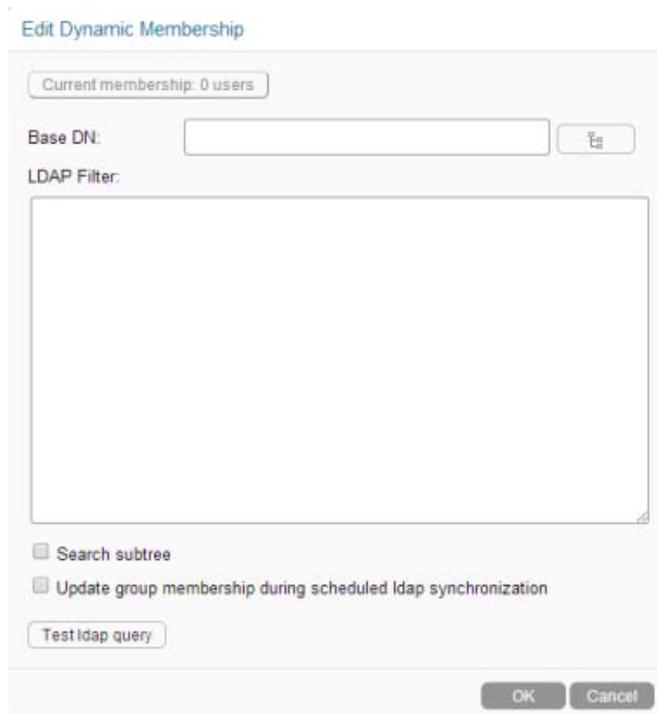
7 Specify the following options:

Base DN: Specify the base DN where you want to start your search.

If you have multiple LDAP sources, see "Considerations with Multiple LDAP Sources" on page 119 before proceeding.

TIP: You can use the **Browse** icon [icon] next to the **Base DN** field to browse the LDAP directory for the base DN that you want to use.

LDAP Filter: Specify the filter criteria.

For example, to search for all users located in Utah, specify `(st=Utah)`.

Search subtree: Select this option if you want to also search for matches in subtrees of the base dn you are currently searching.

Update group membership during scheduled ldap synchronization: Select this option to update the membership of this group during each scheduled LDAP synchronization. Group membership is updated based on changes that might have occurred in the LDAP directory.

For information on how to set the LDAP synchronization schedule, see "Configuring the Synchronization Schedule" on page 204.

8 (Optional) Click **Test ldap query** to test the results of your LDAP query.

This process can take several minutes, depending on the size of your LDAP directory.

9 Click **OK** > **OK** to create the group.

10 Configuring User Access to the Filr Site

10.1 Allowing External Users Access to Your Filr Site

Users external to your organization can access the Filr site either as the Guest user or as a registered user (after performing an auto-registration process). By default, these features are not enabled.

- Section 10.1.1, "Allowing Guest Access to Your Filr Site," on page 123

10.1.1 Allowing Guest Access to Your Filr Site

When guest access is enabled on the Filr site (as described in this section), and users enter the Filr site as the Guest user, the person is considered to be a Guest user on the site. This is indicated by the user name displayed in the upper-right corner of the page:
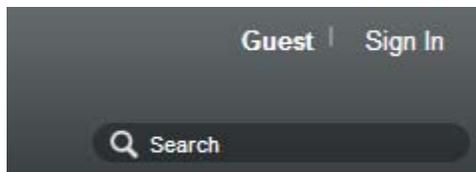
- "Guest Access Limitations" on page 123
- "Understanding the Guest User" on page 124
- "Setting Up Guest Access for the Filr Site" on page 124
- "Monitoring Guest User Access" on page 125

Guest Access Limitations

Guest access to the Filr site is not possible in the following situations:

- If you are using NetIQ Access Manager to provide single sign-on functionality.

  For more information about NetIQ Access Manager, see Section 1.8, "Changing Reverse Proxy Configuration Settings," on page 28.

- If users are using the Filr mobile app. For guest users to access the Filr site, they must access the full user interface from a browser.

  For more information about using the Filr mobile app, see the *Novell Filr Mobile App Quick Start*.

Understanding the Guest User

As the administrator, you can choose whether you want people who do not have Filr user names to be able to access information on the Filr site as the Guest user.

For example, a government organization such as a city might give Filr user accounts only to key city knowledge workers. However, it is critical that other city workers and regular citizens also access the site to see a listing of upcoming events, read city news, report complaints, and so forth. As a Filr administrator, you can allow guests to access Filr as the Guest User.

When people visit your Filr site as the Guest user, they are presented with the following user experience:

- Any user who knows the Filr site URL can access the Filr site as the Guest User and is immediately taken to the **Shared with Me** tab where they see all files and folders that are shared with the public.

- If a Guest user uses the Search feature, the only information returned is information that the Guest user has been granted access to see.

Setting Up Guest Access for the Filr Site

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

   1a Launch a web browser.

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

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

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

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

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

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

4 Select **Allow Guest Access**.

Guest access means that when users without a user account access the root page of your Filr site and the login dialog box is displayed, they can click **Enter as guest** on the login dialog box to enter the Filr site as the Guest user. Only items that have been shared with the public are available to the Guest user.

If an item is shared with the public, recipients of that shared item are given the URL to the shared item, and no login is required.

5 (Optional) Select **Guest access is read only** if you do not want the Guest user to be allowed to add files or make comments on files.

6 Click **OK**.

7 Ensure that users are allowed to share with the public, as described in Section 6.3, "Enabling Users to Share," on page 64.

If no items have been shared with the public, the guest user does not have access to any files.

Monitoring Guest User Access

As the Filr site administrator, you can create a report of all locations on the Filr site that the Guest user can access. For instructions, see Section 28.2.10, "User Access Report," on page 277.

10.2 Allowing Web Crawler Access to Your Filr Site

If you allow Guest access to your Novell Filr site, as described in Section 10.1, "Allowing External Users Access to Your Filr Site," on page 123, you can provide Internet search engines (such as Google) with the Filr permalinks for folders that you want to make publicly available on the Internet. A Filr permalink is the complete URL that someone outside of your Filr site and outside of your organization, such as a web crawler (http://en.wikipedia.org/wiki/Web_crawler), could use to access a specific location on your Filr site.

1 To determine the permalink of a folder, click **Permalinks** at the bottom of a folder page.

10.3 Disabling User Access to the Filr Site on the Web

If you want users to have access to the Filr system only through the Filr desktop application or through the Filr mobile app, you can disable users' ability to access the Filr site via a web browser.

You can restrict access to the Filr site on the web for all users, or for specific users and groups. Alternatively, you can disable access to the site for all users and then enable access for specific users and groups.

- Section 10.3.1, "Disabling Access for All Users," on page 126
- Section 10.3.2, "Disabling or Enabling Access for Individual Users," on page 126
- Section 10.3.3, "Disabling or Enabling Access for Individual Groups," on page 127

10.3.1 Disabling Access for All Users

Disabling access as described in this section disables access to Filr on the web for all users in the Filr system, except for the Filr administrator.

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

   1a Launch a web browser.

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

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

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

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

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

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

4 Select **Disable web access**.

5 Click **OK**.

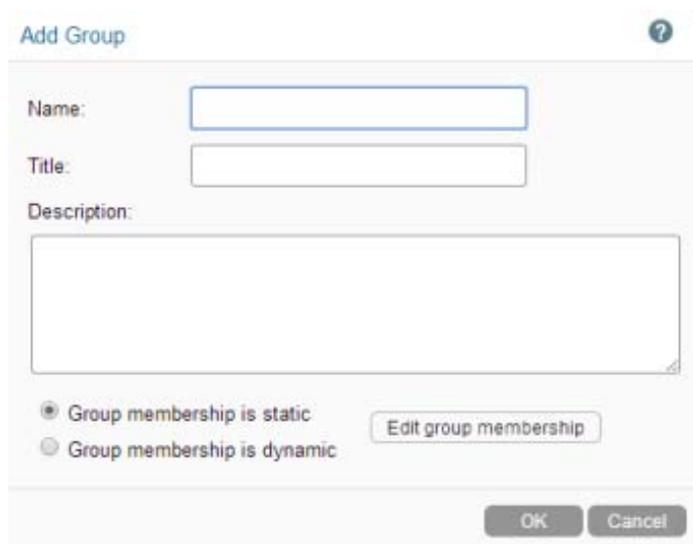## 10.3.2 Disabling or Enabling Access for Individual Users

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

   1a Launch a web browser.

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

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

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

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

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

3 Under **Management**, click **Users**.

The Manage Users page is displayed.

4 (Conditional) If you have not disabled access for all users (as described in Section 10.3.1, "Disabling Access for All Users," on page 126), you can disable access for an individual user by clicking the drop-down arrow next to the user's name and then clicking **Disable Web Access for this User**.

or

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

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

or

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

10.3.3 Disabling or Enabling Access for Individual Groups

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

1a Launch a web browser.

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

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

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

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

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

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

The Manage Groups page is displayed.

4 (Conditional) If you have not disabled access for all users (as described in Section 10.3.1, "Disabling Access for All Users," on page 126), you can disable access for users who belong to an individual group by clicking the drop-down arrow next to the group name and then clicking **Disable Web Access for Users in this Group**.

or

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

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

or

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

10.4 Disabling Downloads from the Filr Site on the Web

You can disable the ability for users to download files from the Filr site on the web. If you do not disable downloads as described in this section, users can download files to their personal workstations, as described in "Downloading Files" in the *Filr 2.0: Web Application User Guide*.

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

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

10.4.1 Disabling Downloads for All Users

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

1a Launch a web browser.

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

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

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

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

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

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

Configure Web Application

☐ Allow Guest access

☐ Guest access is read only

☐ Disable file downloads

☐ Disable web access

4 Select **Disable file downloads**.

5 Click **OK**.

10.4.2 Disabling or Enabling Downloads for Individual Users

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

    1a Launch a web browser.

    1b Specify one of the following URLs, depending on whether you are using a secure SSL connection:
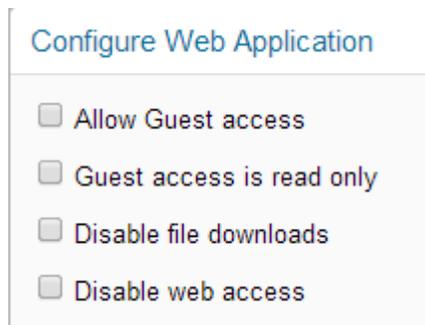
```
http://Filr_hostname:8080
https://Filr_hostname:8443
```

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

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

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

3 Under **Management**, click **Users**.

   The Manage Users page is displayed.

4 (Conditional) If you have not disabled downloads for all users (as described in Section 10.4.1, "Disabling Downloads for All Users," on page 128), you can disable downloads for an individual user by clicking the drop-down arrow next to the user's name and then clicking **Disable File Downloads for this User**.

   or

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

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

or

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

10.4.3 Disabling or Enabling Downloads for Individual Groups

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

   1a Launch a web browser.

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

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

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

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

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

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

The Manage Groups page is displayed.

4 (Conditional) If you have not disabled access for all users (as described in Section 10.4.1, "Disabling Downloads for All Users," on page 128), you can disable access for users who belong to an individual group by clicking the drop-down arrow next to the group name and then clicking **Disable Web Access for Users in this Group**.

or

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

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

or

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

10.5 Configuring Single Sign-On with NetIQ Access Manager

For information about how to configure NetIQ Access Manager to provide single sign-on functionality in Filr, see Section 1.8, "Changing Reverse Proxy Configuration Settings," on page 28.

10.6 Configuring Single Sign-On with KeyShield

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

10.6.1 Prerequisites

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

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

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

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

1 If the connectors your users will use are not listed, click the bar below the already-allowed connectors.

2 Select the connectors for your users, then click **OK**.
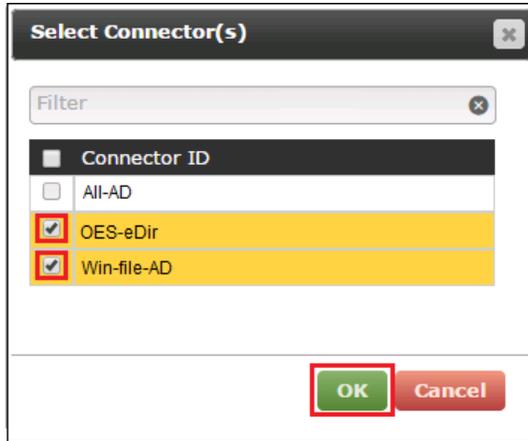
10.6.3   Configuring Filr for KeyShield SSO Support

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

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

For example `https:192.168.30.150:8443`

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

2 In the new browser session, log in to Filr as an administrator.

3 Click the admin link in the upper-right corner of the page, then click the Administration Console

icon .

4 In the left frame, click **KeyShield SSO**.
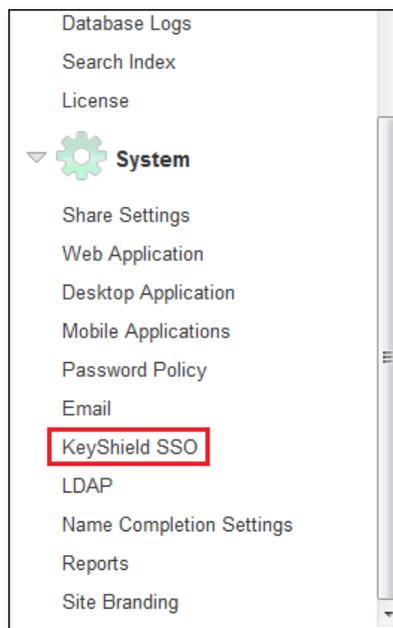
5 In the KeyShield SSO Configuration dialog, click **Enable KeyShield SSO**.

6 In the **KeyShield Server URL** field, type the access URL for the KeyShield server:

`https://ks-server-dns-name_or_ip-address:ks-server-https-port/`

For example,

7 Switch to the KeyShield browser-based console, toggle open the API Key, then select and copy the key to your clipboard.

8 Switch to the Filr Administration panel and paste the API Key into the **API Authorization** field.

9 The **HTTP Connection Timeout** controls how long the Filr Appliance will wait for a response from the KeyShield server before prompting users for their login credentials.

Novell doesn't recommend changing this value unless the connection between the Filr Appliance and the KeyShield SSO server doesn't facilitate a quick response. For example the appliance and server are connected over a WAN.

10 In the Connector Names field, type the names of each KeyShield SSO connector that Filr users will connect through.

11 Continue with the next section, "KeyShield Attribute Alias Support."

10.6.4   KeyShield Attribute Alias Support

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

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

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

A Filr Example

1. Jane Smith logs in through KeyShield's SSO service using jsmith (her UID in LDAP) as her Username.

2. Jane then launches Filr.

   Unfortunately, the Filr administrator who configured the LDAP import, specified CN as the LDAP username attribute and JaneSmith was impoted as Jane's Filr username.

3. When Filr tries to authenticate Jane Smith, KeyShield doesn't find her as an authenticated user and the attempt fails.

Jane is then prompted to log in to Filr.

4. To fix the mismatch of LDAP attributes, Jane's KeyShield administrator adds `x-filr = cn` as an **Attribute Alias** in Keyshield.

5. Jane's Filr administrator adds `x-filr` as the **Username Attribute Alias** in Filr.

6. The next time Jane launches Filr after signing in through KeyShield' SSO service, KeyShield verifies to Filr that JaneSmith is authenticated and no additional login is required.

Configuring Attribute Alias Support

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

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

`x-filr = cn`

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

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

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

3 Continue with "Configuring Two-Factor Authentication."

10.6.5 Configuring Two-Factor Authentication

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

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

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

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

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

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

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

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

1 If you want to configure two-factor authentication for your KeyShield 6.1 SSO service, select the options and specify the text accordingly.

2 Click **Test Connection**.

Because the Filr appliance doesn't yet have the KeyShield SSO SSL certificate in its keystore, the test fails.

3 Continue with

10.6.6 Downloading and Installing the KeyShield SSO SSL Certificate

1 Open a third browser session and access the Filr appliance on port 9443:

`https://`*`filr-ip-address-or-dns-name`*`:9443`

For example `https:192.168.30.150:9443`

2 Log in as `vaadmin`.

3 Switch to the KeyShield browser-based console and under General/Web Interface, click Edit.

4 Click the **Download** button for the **HTTPS Keystore**.
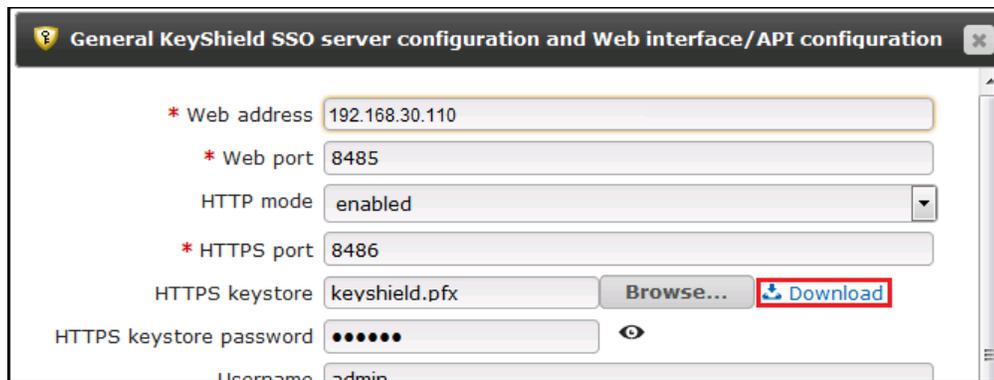
5 Save the `Keyshield.cer` file on the workstation running the browser.

6 Switch to the browser session opened in and click the **Appliance Configuration** icon.

7 Click the **Digital Certificates** icon.
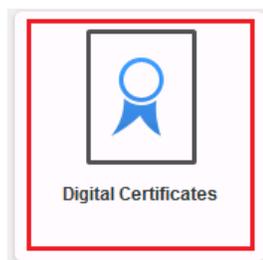
8 Click **File > Import > Trusted Certificate**.
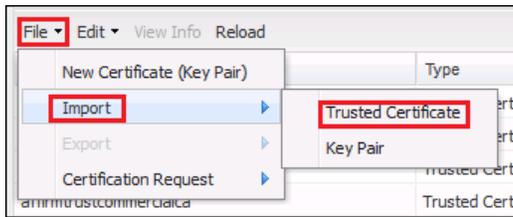
9 Click **Browse**, then browse to the location where you saved the `Keyshield.cer` file and click **Open**.
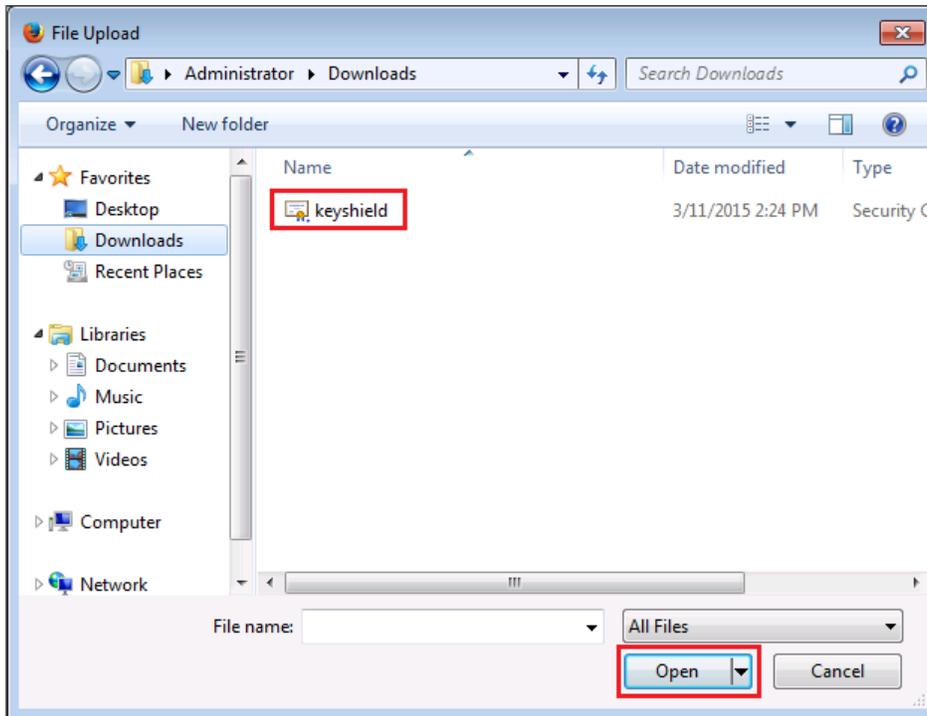
10 Click **OK** to import the certificate file.
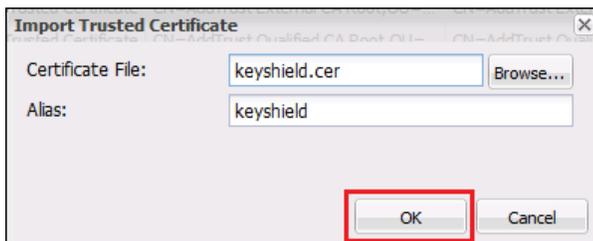
11 Acknowledge the message about restarting the appliance by clicking **OK**.

12 Click the back arrow in the browser, then select **Reboot**.

13 After the system restarts, continue with the next section, Testing the KeyShield SSO Configuration.

10.6.7   Testing the KeyShield SSO Configuration

1 Switch back to the Filr administration console (port 8443).

2 Click **Test Connection**.

The test should succeed.

3 Click **OK** to finalize the configuration and complete the Keyshield SSO integration.

11 Setting Up Site Branding

You can brand your Filr site to display a corporate logo on the login dialog box before users log in. You can also display a corporate brand on each Filr page after users log in.

- Section 11.1, "Branding the Filr Site," on page 141
- Section 11.2, "Branding the Login Dialog Box," on page 142

11.1 Branding the Filr Site

You can brand your Novell Filr site to match your corporate brand. When you add a site-wide brand to your Filr site, the brand is displayed on every Filr page. You can create your brand by adding an image, by creating the brand in HTML using CSS styles, or by using a combination of both.

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

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

   The Administration page is displayed.

3 In the **System** section, click **Site Branding**.

   The Site Branding dialog box is displayed.

4 (Conditional) If you have not done so already, upload to Filr any images that you want to use in your site branding:

   4a Click any **Browse** icon on the Site Branding page to browse to and upload your image to Filr to be used in the site branding.

      The Add File Attachment dialog box is displayed.

   4b (Optional) Click **Add file** if you want to upload multiple images to the Filr site. After images are uploaded to the Filr site, they can then be used in the site branding.

   4c Browse to and select the images that you want to upload.

   4d Click **OK** to exit the Add File Attachment dialog box.

5 Specify the following information to create your desired brand:

   Use Branding Image: Select this option if you want to use the drop-down list to select an existing image for the branding foreground, such as a company name. To have no branding image, select **None** in the drop-down list. (**Powered by Novell Filr** is displayed in the upper-right corner below each user's name.)

   Images are available in the drop-down list after you upload them by clicking the **Browse** icon , as described in Step 4.

   Use Advanced Branding: Select this option, then click **Edit Advanced** if you want to create a brand that includes advanced features, such as HTML. You can create your brand in HTML by using CSS styles and copying them into the HTML editor by clicking **HTML** in the Edit Advanced Branding dialog box. (**Powered by Novell Filr** is displayed in the upper-right corner below each user's name.)

   Background Image: Use the drop-down list to select an existing image. The background image is displayed behind your branding image or your advanced branding.

TIP: Buttons in the header (such as My Files, and Shared with Me) display better when your background image is a medium to darker color. Lighter images make it more difficult to see the buttons.

Images are available in the drop-down list after you upload them by clicking the **Browse** icon [icon], as described in Step 4.

Stretch Image: Stretches the image to occupy the entire branding area.

If you stretch your background image, the image overrides any background color that you have set.

Background Color: Adds a background color that occupies the entire branding area. To change the background color, click the color picker icon [icon] to the right of this field, select the new color, then click **OK**.

If you added a background image and stretched the image, the background color is not displayed.

Text Color: Changes the text color of the workspace name in the upper-right corner of the branding area. To change the text color, click the color picker icon [icon] to the right of this field, select the new color, then click **OK**.

Clear branding: Click this option to clear all your current branding selections.

6 Click **OK**.

The Filr site now displays the brand that you created.

11.2 Branding the Login Dialog Box

You can change the image that is used in the login dialog box that users see before they log in to the Novell Filr site.

To re-brand the login dialog box to contain a custom image:

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

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

The Administration page is displayed.

3 In the **System** section, click **Site Branding**.

The Site Branding dialog box is displayed.

4 (Conditional) If you have not done so already, upload to Filr any images that you want to use in your site branding:

    4a Click the **Browse** icon to browse to and upload your image to Filr to be used in the site branding.

        The Add File Attachment dialog box is displayed.

    4b (Optional) Click **Add file** if you want to upload multiple images to the Filr site. After images are uploaded to the Filr site, they can then be used in the site branding.

    4c Browse to and select the images that you want to upload.

        The suggested image size to use in the login dialog box is width: 400px, height: 60 px.

    4d Click **OK** to exit the Add File Attachment dialog box.

5 In the **Sign In Dialog Image** section, in the **Current image** drop-down list, select the file that you want to use for branding the login dialog box.

12 Allowing Access to the Filr Site through NetIQ Access Manager

To allow access to the Filr site through NetIQ Access Manager, you need to make configuration changes in NetIQ Access Manager to configure a protected resource for a Novell Filr server as described in Section 12.1, "Configuring a Protected Resource for a Novell Filr Server," on page 145.

IMPORTANT

NetIQ Access Manager cannot grant external users access through the generated URL links that Filr includes in email notifications. This means that the following features are not functional for external or Guest users:

- Users are not able to share with external users, as described in "Sharing with People Outside Your Organization" in the *Filr 2.0: Web Application User Guide*.

  A possible work-around for this issue is documented in TID 7014912 (https://www.novell.com/support/kb/doc.php?id=7014912).

- Users are not able to share a File Link with external users, as described in "Distributing a Link to a File" in the *Filr 2.0: Web Application User Guide*.

- Users cannot make items accessible to the public, as described in "Making Files Accessible to the Public" in the *Filr 2.0: Web Application User Guide*.

  This means that public users cannot access the Filr site as the Guest user. For more information about the Guest user, see Section 10.1.1, "Allowing Guest Access to Your Filr Site," on page 123.

For more information about external users in Filr, see Section 10.1, "Allowing External Users Access to Your Filr Site," on page 123.

12.1 Configuring a Protected Resource for a Novell Filr Server

The following sections explain how to configure the Access Gateway with a domain-based multi-homing service. The instructions assume that you have a functioning Novell Filr server on Linux and a functioning Access Manager system (4.1.1 or higher) with a reverse proxy configured for SSL communication between the browsers and the Access Gateway.

The Filr server needs to be configured to trust the Access Gateway to allow single sign-on with Identity Injection and to provide simultaneous logout. You also need to create an Access Gateway proxy service and configure it.

- Section 12.1.1, "Configuring the Novell Filr Server to Trust the Access Gateway," on page 146
- Section 12.1.2, "Configuring a Reverse-Proxy Single Sign-On Service for Novell Filr," on page 146

For information on other possible Access Gateway configurations, see "Teaming 2.0: Integrating with Linux Access Gateway" (http://www.novell.com/communities/node/9580/teaming-20-integration-linux-access-gateway).

12.1.1 Configuring the Novell Filr Server to Trust the Access Gateway

To use Novell Filr as a protected resource of an Access Gateway and to use Identity Injection for single sign-on, the Filr server needs a trusted relationship with the Access Gateway. With a trusted relationship, the Filr server can process the authorization header credentials. The Filr server accepts only a simple user name (such as user1) and password in the authorization header.

To configure a trusted relationship and simultaneous logout, specify the reverse proxy configuration settings for your Filr appliance, as described in Section 1.8, "Changing Reverse Proxy Configuration Settings," on page 28.

12.1.2 Configuring a Reverse-Proxy Single Sign-On Service for Novell Filr

To configure a reverse-proxy single sign-on service for Filr, complete the following tasks:

- "Creating a New Reverse Proxy" on page 146
- "Configuring the Domain-Based Proxy Service" on page 146
- "Creating Policies" on page 147
- "Creating a Word Rewriter Profile for Each Filr Host" on page 148
- "Configuring Protected Resources" on page 148
- "Disabling a Rewriter Profile and Enabling Port Redirection" on page 150

Creating a New Reverse Proxy

Before you can configure the domain-based proxy service, you need to create a new reverse proxy. For information, see "Managing Reverse Proxies and Authentication" in the NetIQ Access Manager 4.1 Administration Guide.

Configuring the Domain-Based Proxy Service

1 In the Administration Console, click **Devices** > **Access Gateways** > **Edit**, then click the name of the reverse proxy that you created in "Creating a New Reverse Proxy" on page 146.

2 Click the reverse proxy link that you have previously created. In the **Reverse Proxy List**, click **New**, then fill in the following fields:

- **Proxy Service Name:** Specify a display name for the proxy service that the Administration Console uses for its interfaces.

- **Published DNS Name:** Specify the DNS name that you want the public to use to access your site. This DNS name must resolve to the IP address that you set up as the listening address. For example, `Filr.doc.provo.novell.com`.

   IMPORTANT: To avoid incomplete logout problems, you must also create a an **Additional Strings to Replace** entry for each Filr appliance that points to this DNS name.

   See "Creating a Word Rewriter Profile for Each Filr Host" on page 148.

- **Web Server IP Address:** Specify the IP address of the Filr server.

- **Host Header:** Select the **Forward received host name**.

- ◆ **Web Server Host Name:** Because of your selection in the **Host Header** field, this option is dimmed.

3 Click **OK**.

4 Click the newly added proxy service, then select the **Web Servers** tab.

5 Configure the **Connect Port** to match the **Reverse Proxy Secure HTTP Port** setting that you configured from the Filr appliance, as described in Section 1.8, "Changing Reverse Proxy Configuration Settings," on page 28. This will be either port 443 or 8443.

6 When using SSL, select **Use SSL** in the Access Manager configuration, then select one of the following:

- ◆ **Any in reverse proxy store:** Select this option if your Filr and Access Manager servers are in separate geographical locations, or if you want added security within your local network.
- ◆ **Do not verify:** Select this option if your Filr and Access Manager servers are part of the same local network.

7 Click **TCP Connect Options**.

8 Click **OK**.

9 Continue with "Configuring Protected Resources" on page 148.

Creating Policies

You need to create two policies: LDAP Identity Injection and X-Forward-Proto:

- ◆ "Creating the LDAP Identity Injection Policy" on page 147
- ◆ "Creating the X-Forward-Proto HTTP Header Policy" on page 148

Creating the LDAP Identity Injection Policy

1 In the Administration Console, click **Policies > Policies**.

2 Select the policy container, then click **New**.

3 Specify `ldap_auth` as the name for the policy, select **Access Gateway: Identity Injection** for the type, then click **OK**.

4 (Optional) Specify a description for the injection policy. This is useful if you plan to create multiple policies to be used by multiple resources.

5 In the **Actions** section, click **New**, then select **Inject into Authentication Header**.

6 Fill in the following fields:

User Name: If users are provisioned with `cn` or `uid` attributes, select **Credential Profile**, then select **LDAP Credentials:LDAP User Name**. In the **Refresh Data Every** drop-down, select **Session**.

or

If users are provisioned with mail attributes, select **LDAP Attribute**, then select **mail**. In the **Refresh Data Every** drop-down, select **Session**.

Password: Select **Credential Profile**, then select **LDAP Credentials:LDAP Password**.

7 Leave the default value for the **Multi-Value Separator**, which is comma.

8 Click **OK**.

9 To save the policy, click **OK**, then click **Apply Changes**.

For more information on creating such a policy, see "Configuring an Authentication Header Policy" in the .

Creating the X-Forward-Proto HTTP Header Policy

When communicating over HTTPS from the browser to Access Manager, and over HTTP from Access Manager to Filr, the X-Forwarded-Proto is a best practice.

1 In the Administration Console, click **Policies > Policies**.

2 Select the policy container, then click **New**.

3 Specify `x-forward` as the name for the policy, select **Access Gateway: Identity Injection** for the type, then click **OK**.

4 (Optional) Specify a description for the injection policy. This is useful if you plan to create multiple policies to be used by multiple resources.

5 In the **Actions** section, click **New**, then select **Inject into Custom Header**.

6 Fill in the following fields:

Custom Header Name: Specify `X-Forward-Proto` as the name.

Value: Select **String Constant** in the drop-down, then specify `https`.

7 Leave the other settings at the defaults.

8 Click **OK**.

9 To save the policy, click **OK**, then click **Apply Changes**.

For more information on creating such a policy, see "Configuring an Authentication Header Policy" in the .NetIQ Access Manager 4.1 Administration Guide

Creating a Word Rewriter Profile for Each Filr Host

Due to a security fix in Filr 2.0 and later, when users log out of Filr, they are taken to the Filr DNS name rather than the NAM host. This results in a condition where it appears that they are logged out although they actually are not.

To avoid these incomplete login conditions, create a word rewriter for each Filr host that points to the DNS name of the NAM host.

The NetIQ Access Manager Best Practices Guide contains pertinent rewriter examples in a section that deals with SharePoint. See Table 3-2 in the above-mentioned guide and also refer to the instructions associated with the table.

Configuring Protected Resources

You need to create two protected resources, one for HTML content and a public protected resource:

1 Create a protected resource for HTML content:

  1a In the **Protected Resource List**, click **New**, specify `Basic auth with redirection` for the name, then click **OK**.

  1b (Optional) Specify a description for the protected resource. You can use it to briefly describe the purpose for protecting this resource.

  1c Click the **Edit** icon ✎ next to the **Authentication Procedure** drop-down list.

  1d Create a new authentication procedure by clicking **New**, specifying a name for the authentication procedure, and then clicking **OK**.

  1e In the dialog box that is displayed, fill in the following fields.

    Contract: Select the **Secure Name/Password - Form** contract.

Non-Redirected Login: Select this option.

Realm: Specify a name that you want to use for the Filr server. This name does not correspond to a Filr configuration option. It appears when the user is prompted for credentials.

Redirect to Identity Server When No Authentication Header is Provided: Select this option.

1f Click **OK** twice.

1g In the **URL Path List**, add the following paths for HTML content:

```
/*
/ssf/*
/ssf/s/readFile/share/*
```

1h On the configuration page for the protected resource, select the authentication procedure that you just created from the **Authentication Procedure** drop-down list, then click **OK**.

2 Create a public protected resource for Web Services:

NetIQ Access Manager is not designed to protect certain public resources. You must complete the following steps to allow these resources to be protected by the Filr server itself, rather than by NetIQ Access Manager.

2a In the **Protected Resource** List, click **New**, specify `public` for the name, then click **OK**.

2b (Optional) Specify a description for the protected resource. You can use it to briefly describe the purpose for protecting this resource.

2c For the **Authentication Procedure**, select **None**.

2d Click **OK**.

2e In the **URL Path List**, remove the `/*` path and add the following paths:

For public content:

```
/ssf/atom/*
/ssf/ical/*
/ssf/ws/*
/ssf/rss/*
/ssr/*
/rest/*
/rest
/
/dave/*
/my_files/*
/net_folders/*
/shared_with_me
/desktopapp/*
```

The `/ssf/rss/*` path enables non-redirected login for RSS reader connections.

Filr provides authentication for all of the paths listed above.

2f Click **OK**.

3 Assign the X-Forward-Proto Header policy to both protected resources that you created:

3a Click **Access Gateways** > **Edit** > **[Name of Reverse Proxy]** > **[Name of Proxy Service] > Protected Resources**.

3b For each Filr protected resource, click the **Identity Injection** link, select the **x-forward** policy that you created, click **Enable**, then click **OK**.

3c Click **OK.**

4 Assign the Identity Injection policy to the HTML protected resource that you created, specifically, **Basic auth with redirection**.

    4a Click **Access Gateways** > **Edit** > **[Name of Reverse Proxy]** > **[Name of Proxy Service] > Protected Resources**.

    4b For each Filr protected resource, click the **Identity Injection** link, select the **ldap_auth** policy that you created, click **Enable**, then click **OK**.

    4c Click **OK.**

5 To save the configuration changes, click **Devices** > **Access Gateways**, then click **Update**.

6 In the **Protected Resource List**, ensure that the protected resources that you created are enabled.

7 To apply your changes, click **Devices** > **Access Gateways**, then click **Update**.

8 Continue with "Disabling a Rewriter Profile and Enabling Port Redirection" on page 150.

Disabling a Rewriter Profile and Enabling Port Redirection

NOTE: If you have changed the Filr and Access Manager ports from their defaults (8443 for Filr and 443 for Access Manager), you cannot disable the rewriter profile and enable port redirection as described in this section. Instead, you must configure a rewriter profile in Access Manager, as described in "Creating or Modifying a Rewriter Profile" in the .

To disable the HTML Rewriter and enable port redirection:

1 In the Proxy Service List in Access Manager, ensure that the HTML Rewriter is disabled.

2 Under the **Web Servers** tab, ensure that the Connect Port has been modified to port 443. (This matches the configuration that you made in Step 5 in "Configuring the Domain-Based Proxy Service" on page 146.)

3 Enable port redirection on the Filr server, as described in Section 1.2.1, "Changing the Network Configuration Settings," on page 19.

This allows Filr to listen on port 8443, and allows Access Manager to forward client requests to port 443.

13 Configuring Mobile Device Access to the Filr Site

Filr provides the capability for users to access Filr content via the Filr mobile app on a mobile device.

You can enable this functionality for all users in the Filr system, or for individual users and groups. By default, this functionality is not enabled.

In addition to enabling mobile device access for the Filr site, Filr also provides native controls to limit certain actions that users might perform within the Filr mobile app that are related to security. For example, you can restrict users from cutting or copying data and pasting it into another app. If you are using Filr in conjunction with an MDM solution, such as ZENworks Mobile Management, settings made within the MDM solution override any setting made within the Filr administration console.

If you make configuration changes, users must log out of the app and log in again in order to see the changes.

13.1 Configuring Mobile Device Access for All Users

To customize the mobile experience for all users in your Filr system:

1 In Filr, click the **admin** link in the upper-right corner of the page, then click the **Administration Console** icon 🔲.

2 Under **System**, click **Mobile Applications**.

The Configure Mobile Applications dialog box is displayed.

3 As necessary, configure Filr to allow the Filr mobile app to support the following features.

Most of the following options can be changed on a per-user basis, as described in Section 13.2, "Configuring Mobile Device Access for Individual Users and Groups," on page 153.

Access Filr: Allows users to access the Filr site through the Filr mobile app.

Cache the user's password: Allows users to 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: Allows users to download files from Filr to the mobile device. Downloaded files can then be viewed in offline mode by accessing the **Downloads** section in the app.

This setting applies to all files that users have access to, including files in Net Folders.

You should be aware that even if this option is disabled, users can still work around this by accessing Filr from a web browser on their device and then downloading the file to their mobile device via the regular Filr web browser.

In order for files to remain secure after they are downloaded, users are responsible for configuring their mobile device to encrypt files, as described in "Encrypting Downloaded Files" in the "Novell Filr Mobile App Quick Start".

Force PIN Code: Forces users who are running the version 2.0 and later mobile 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 "Novell Filr Mobile App Quick Start."

Cut/Copy: Allows users to cut or copy data from the Filr mobile app so that the data can be pasted into third-party applications.

Screen capture: Allows users to take a screen capture while inside the Filr application.

This option controls the ability to take screen captures on Android devices only. Users can always take screen captures on iOS devices.

Disable applications on rooted or jail-broken devices: Disables users' ability to run the Filr mobile app on devices that have been rooted or jail-broken.

Open in: This option controls users' ability to use Open In functionality for iOS devices and the Share or Send To functionality for Android devices. This functionality allows users to open files from the Filr app into third-party applications.

For example, users can view a file in Filr, open that file in a document editing application, edit the file in the document editing application, and then save the file back to the Filr app.

This setting applies to all files that users have access to, including files in Net Folders.

Select from the following options:

* **Disabled:** Disables users' ability to open files from the Filr app into third-party applications.
* **All applications:** Allows users to open files from the Filr app into any third-party application.
* **Whitelist:** Allows you to specify which third-party applications users can open files into.

  If you select this option, you need to provide the Android package name or the iOS bundle ID for the applications that you want to allow:

  Click **Add**, specify the Android package name or iOS bundle ID, then click **OK**.

  For example, the bundle ID for the Pages app on iOS is `com.apple.iwork.pages`.

  The package name for the Gallery app on Android is `com.google.android.gallery3d`.

TIP: An easy way to find the package name for an Android app is to install the `Package Name Viewer` app from the Google Play store. This app displays the package name for each app that is currently installed on the device.

To find the bundle ID for an iOS app:

1. (Conditional) If the app for which you want to location the bundle ID has not yet been synchronized to iTunes from your device, you must sync the device with iTunes.

2. In your iTunes library on your Mac or PC, open the `Mobile Applications` folder.

   On a Mac, this is usually in your Home directory, at the following location: `~/Music/iTunes/Mobile Applications/`

   On Windows 7, this is usually at the following location: `C:\Users\`*username*`\My Music\iTunes\Mobile Applications/`

3. In the `Mobile Applications` folder, locate the app for which you want the bundle ID.

4. Create a copy of the file, and re-save the copy as a `.zip` file.

5. Unzip the newly created `.zip` file.

   You now see a folder by the name of the application name.

6. Locate the `iTunesMetadata.plist` file within the folder and open it in a text editor.

7. Locate the `softwareVersionBundleid` key within the file.

   The string value below this key is the bundle ID.

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

For more information about using MobileIron with Filr, see Section 13.3.3, "Configuring MobileIron to Manage the Filr App," on page 158.

Synchronize every *xx* Minutes: Specify the interval (in minutes) for how often content is synchronized between Filr servers and the Filr mobile app. This lets you control the amount of load the Filr mobile app puts on the Filr server.

4 Click **OK**.

13.2 Configuring Mobile Device Access for Individual Users and Groups

To customize the mobile experience for individual users and groups in your Filr system:

1 In Filr, click the **admin** link in the upper-right corner of the page, then click the **Administration Console** icon.

2 Under **Management**, click **Users**.

The Manage Users page is displayed.

3 Select the check boxes next to the names of the users or groups for whom you want to configure the Filr mobile app, then click **More** > **Mobile Application Settings**.

The **Configure User Mobile Application Settings** page is displayed.

4 To change the mobile app settings for the selected users to be different from the global settings, select **Use user settings to allow mobile applications to**, then choose from the following options:

Access Filr: Allows users to access the Filr site through the Filr mobile app.

Cache the user's password: Allows users to 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: Allows users to download files from Filr to the mobile device. Downloaded files can then be viewed in offline mode by accessing the **Downloads** section in the app.

This setting applies to all files that users have access to, including files in Net Folders.

Be aware that even if this option is disabled, users can still work around this by accessing Filr from a web browser on their device and then downloading the file to their mobile device via the regular Filr web browser.

In order for files to remain secure after they are downloaded, users are responsible for configuring their mobile device to encrypt files, as described in "Encrypting Downloaded Files" in the "Novell Filr Mobile App Quick Start".

Force PIN Code: Forces users running version 2.0 and later mobile apps to have a 4-digit access code set on their device for accessing Filr, as described in "Configuring a 4-Digit Passcode" in the "Novell Filr Mobile App Quick Start."

Cut/Copy: Allows users to cut or copy data from the Filr mobile app so that the data can be pasted into third-party applications.

Screen capture: Allows users to take a screen capture while inside the Filr application.

This option controls the ability to take screen captures on Android devices only. Users can always take screen captures on iOS devices.

Disable applications on rooted or jail-broken devices: Disables users' ability to run the Filr mobile app on devices that have been rooted or jail-broken.

Open in: This option controls users' ability to use Open In functionality for iOS devices and the Share or Send To functionality for Android devices. This functionality allows users to open files from the Filr app into third-party applications.

For example, users can view a file in Filr, open that file in a document editing application, edit the file in the document editing application, and then save the file back to the Filr app.

This setting applies to all files that users have access to, including files in Net Folders.

Select from the following options:

- **Disabled:** Disables users' ability to open files from the Filr app into third-party applications.

- **All applications:** Allows users to open files from the Filr app into any third-party application.

- **Whitelist:** Allows you to specify which third-party applications users can open files into.

  If you select this option, you need to provide the Android package name or the iOS bundle ID for the applications that you want to allow:

  Click **Add**, specify the Android package name or iOS bundle ID, then click **OK**.

  For example, the bundle ID for the Pages app on iOS is `com.apple.iwork.pages`.

  The package name for the Gallery app on Android is `com.google.android.gallery3d`.

  TIP: An easy way to find the package name for an Android app is to install the `Package Name Viewer` app from the Google Play store. This app displays the package name for each app that is currently installed on the device.

  To find the bundle ID for an iOS app:

  1. (Conditional) If the app for which you want to location the bundle ID has not yet been synchronized to iTunes from your device, you must sync the device with iTunes.

  2. In your iTunes library on your Mac or PC, open the `Mobile Applications` folder.

     On a Mac, this is usually in your Home directory, at the following location: `~/Music/iTunes/Mobile Applications/`

     On Windows 7, this is usually at the following location: `C:\Users\`*username*`\My Music\iTunes\Mobile Applications/`

  3. In the `Mobile Applications` folder, locate the app for which you want the bundle ID.

  4. Create a copy of the file, and re-save the copy as a `.zip` file.

  5. Unzip the newly created `.zip` file.

     You now see a folder by the name of the application name.

  6. Locate the `iTunesMetadata.plist` file within the folder and open it in a text editor.

7. Locate the `softwareVersionBundleid` key within the file.

The string value below this key is the bundle ID.

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

For more information about using MobileIron with Filr, see Section 13.3.3, "Configuring MobileIron to Manage the Filr App," on page 158.

5 Click **OK**.

If you have set individual and group settings for the Filr mobile app, you can change those settings back to the global settings for the individual users and groups.

1 In Filr, click the **admin** link in the upper-right corner of the page, then click the **Administration Console** icon 👤.

2 Under **Management**, click **User Accounts**.

The Manage Users page is displayed.

3 Select the check boxes next to the names of the users or groups for whom you want to configure the mobile app, then click **More** > **Mobile Application Settings**.

The **Configure User Mobile Application Settings** page is displayed.

4 To change the desktop application settings back to the global settings for the selected users, select **Use global settings**.

5 Click **OK**.

13.3 Managing Mobile Devices

You can manage the Filr application on users' mobile devices with either MobileIron or ZENworks Mobile Management (ZMM).

- Section 13.3.1, "Key-Value Pairs," on page 155
- Section 13.3.2, "Configuring ZMM to Manage the Filr App," on page 158
- Section 13.3.3, "Configuring MobileIron to Manage the Filr App," on page 158
- Section 13.3.4, "Managing Mobile Devices with Filr," on page 164

13.3.1 Key-Value Pairs

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

Depending on your MDM solution, the key-value pairs listed here might not be necessary for setting configuration options. For example, if you are using MobileIron as your MDM solution, you can set configuration options for opening into third-party apps by using the MobileIron interface.

Table 13-1 *Filr Key-Value Pairs*

Key	Value
server	Specify the URL of your Filr site. For example, `filr.acme.com`.
username	Specify `$USERID$` to cause MobileIron to automatically populate the app with the user's MobileIron user ID
	Alternatively, you can specify an individual user's user ID.
password	Specify `$PASSWORD$` to cause MobileIron to automatically populate the app with the user's MobileIron password.
	Alternatively, you can specify an individual user's password.
allowOpenIn	Specify `1` as the value if you have disabled Open In or Send To support for the mobile apps in the Filr administration console, but you want to allow the Filr secure app to integrate with other secure apps.
	A value of `1` indicates that users can open Filr files into any secure app.
	A value of `2` allows you to designate specific apps that users can open Filr files into. You do this by creating a whitelist of apps using the `openInWhitelist` key.

Key	Value
openInWhitelist	Specify 1 as the value if you want to allow the Filr secure app to integrate with only the specific secure apps that you designate. To designate apps for the whitelist, specify the applications' bundle ID (for iOS apps) and package name (for Android apps) in a comma-delimited list.
	In order for the openInWhitelist values to be recognized, the value for the allowOpenIn key must be set to 2.
	An easy way to find the package name for an Android app is to install the Package Name Viewer app from the Google Play store. This app displays the package name for each app that is currently installed on the device.
	To find the bundle ID for an iOS app:
	1. (Conditional) If the app for which you want to location the bundle ID has not yet been synchronized to iTunes from your device, you must sync the device with iTunes.
	2. In your iTunes library on your Mac or PC, open the Mobile Applications folder.
	On a Mac, this is usually in your Home directory, at the following location: ~/Music/iTunes/ Mobile Applications/
	On Windows 7, this is usually at the following location: C:\Users*username*\My Music\iTunes\Mobile Applications/
	3. In the Mobile Applications folder, locate the app for which you want the bundle ID.
	4. Create a copy of the file, and re-save the copy as a .zip file.
	5. Unzip the newly created .zip file.
	You now see a folder by the name of the application name.
	6. Locate the iTunesMetadata.plist file within the folder and open it in a text editor.
	7. Locate the softwareVersionBundleid key within the file.
	The string value below this key is the bundle ID.
allowCutCopy	Specify 1 as the value if you want users to be able to copy information from the Filr app and paste it into other apps.

13.3.2 Configuring ZMM to Manage the Filr App

> **IMPORTANT:** ZENworks Mobile Management (ZMM) can be used with the iOS and Android Filr mobile apps with the following version requirements:
>
> - **Android requirements:** Filr mobile app 1.0.3 or later with Android 2.3 or later.
> - **iOS requirements:** Filr mobile app 1.0.4 or later with iOS 7.1 or later.

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

13.3.3 Configuring MobileIron to Manage the Filr App

MobileIron Environment Support

The Filr 2.0 mobile apps have been validated in the following MobileIron environments:

- Sentry-AppTunneling
- MobileIron 7.5 AppConnect

Device-Specific Support Information

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

iOS Supported Features

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

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

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

For information about how to configure this option in Filr, see Section 13.1, "Configuring Mobile Device Access for All Users," on page 151 and Section 13.2, "Configuring Mobile Device Access for Individual Users and Groups," on page 153.

Android Supported Features

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

Adding the Filr App to MobileIron

- "Adding the Android Filr App" on page 159
- "Adding the iOS Filr App" on page 160

Adding the Android Filr App

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

1 Download the `.apk` file for the Filr mobile app from the Novell downloads site.

2 Upload the file to MobileIron.

   2a In the MobileIron Admin Portal, click the **Apps** tab.

   2b On the **App Distribution Library** tab, in the **Select Platform** drop-down list, select the platform for the app that you want to add. For example, if you are uploading the Filr mobile app for Android, select **Android**.

   2c Click **Add App**.

      The Add App Wizard is displayed.

   2d Click **Next**, then specify the following information:

      Distribution Type: Select **In-house App**.

      Silently Install: If your device supports a silent install, you can select **Yes**. If the device does not support a silent install or you are unsure, select **No**.

      App Upload: Browse to and select the `.apk` file that you downloaded in Step 1.

   2e Click **Next**, then specify the following information:

      App Name: `Novell Filr` is already specified for you. This cannot be changed.

      Display Version: The version is already specified for you. This cannot be changed.

      Code Version: The version is already specified for you. This cannot be changed.

      Description: Specify a short description for the app.

      Override URL: For information about this feature, see the blue information icon next to this field.

      Featured: Select whether you want to feature this app.

      Category: Select the category that most closely matches the app. You can add a new category as described in the dialog box.

   2f Click Next, then click **Browse** to upload any screen shots that you have for the app.

The mandatory image size is displayed in the dialog box.

    2g Click **Finish** to close the Add App Wizard.

3 Apply the Android label to your application:

    3a From the **App Distribution Library** tab on the **Apps** tab, select the Novell Filr app that you just created, then click **Actions** > **Apply To Label**.

        The Apply To Label dialog box is displayed.

    3b Select the **Android** label, then click **Apply** > **OK**.

Adding the iOS Filr App

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

1 Import the app from the Apple Appstore.

    1a In the MobileIron Admin Portal, click the **Apps** tab.

    1b On the **App Distribution Library** tab, in the **Select Platform** drop-down list, select **iOS**.

    1c Click **App Store Import**.

        The App Store Search dialog box is displayed.

    1d In the **App Name** field, type `Novell Filr`.

    1e In the **App Store** field, select the country appropriate to your location.

    1f Click **Search**.

    1g Click **Import** next to the Novell Filr app, then click **OK** after it is imported.

    1h Close the App Store Search dialog box.

    1i From the **App Distribution Library** tab on the **Apps** tab, click the **Edit** icon next to the Novell Filr app that you just imported.

        The Edit App for iOS dialog box is displayed.

    1j Make any desired changes to the app details and icon, then click **Save**.

2 Apply the iOS label to your application:

    2a From the **App Distribution Library** tab on the **Apps** tab, select the Novell Filr app that you just created, then click **Actions** > **Apply To Label**.

        The Apply To Label dialog box is displayed.

    2b Select the **iOS** label, then click **Apply** > **OK**.

Pre-Populating Fields for Filr Login

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

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

- "Modifying the Android Filr App Configuration for MobileIron" on page 161
- "Creating the iOS Filr App Configuration for MobileIron" on page 161
- "Key-Value Pairs" on page 161

Modifying the Android Filr App Configuration for MobileIron

1 In the MobileIron Admin Portal, click the **Policies & Configs** tab.

2 On the **Configuration** tab, in the **Name** column, click the name of the Filr configuration for the Filr app that you uploaded, as described in "Adding the Android Filr App" on page 159.

3 Click **Edit**.

The Modify AppConnect App Configuration dialog is displayed.

4 Specify the following information:

Name: Provide a name for the configuration, or keep the default.

Description: (Optional) Provide a description for the configuration, or keep the default.

Application: Select `Novell Filr` from the drop-down list.

5 In the **App-specific Configurations** section, keep or remove the key-value pairs that are shown in Table 13-2, "Filr Key-Value Pairs," on page 162. Key-value pairs that remain in the table represent the information that will be pre-populated for Filr login.

6 Click **Save**.

Creating the iOS Filr App Configuration for MobileIron

1 In the MobileIron Admin Portal, click the **Policies & Configs** tab.

2 On the Configuration tab, click **Add New** > **AppConnect** > **Configuration**.

The New AppConnect App Configuration dialog box is displayed.

3 Specify the following information:

Name: Provide a name for the configuration, such as `Filr iOS Configuration`.

Description: (Optional) Provide a description for the configuration.

Application: Specify the Filr iOS bundle ID, which is `com.novell.vibefilr`.

4 In the **App-specific Configurations** section, click the **Plus** icon to add a new field to the key-value pair table; you can then specify the key-value pair to be included in the configuration. The key-value pairs that you can add are shown in Table 13-2, "Filr Key-Value Pairs," on page 162. Key-value pairs that you add to the table represent the information that will be pre-populated for Filr login.

5 Click **Save**.

Key-Value Pairs

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

Table 13-2 *Filr Key-Value Pairs*

Key	Value
server	Specify the URL of your Filr site. For example, `filr.acme.com`.
username	Specify `$USERID$` to cause MobileIron to automatically populate the app with the user's MobileIron user ID.
	Alternatively, you can specify an individual user's user ID.
password	Specify `$PASSWORD$` to cause MobileIron to automatically populate the app with the user's MobileIron password.
	Alternatively, you can specify an individual user's password.

Configuring Data Loss Prevention Policies

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

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

Modifying the Android Filr App Policy for MobileIron

1 In the MobileIron Admin Portal, click the **Policies & Configs** tab.

2 In the **Name** column, click the name of the Filr policy for the Filr app that you uploaded, as described in "Adding the Android Filr App" on page 159.

3 Click **Edit**.

The Modify AppConnect App Container Policy dialog is displayed.

4 Specify the following information:

Name: Provide a name for the policy, or keep the default.

Description: (Optional) Provide a description for the policy, or keep the default.

Application: Select `Novell Filr` from the drop-down list.

5 In the **Data Loss Prevention Policies** section, you can change the following configuration option for Android devices:

Screen Capture: Allow users to take a screen capture from within any AppConnect app (including Filr).

6 Click **Save**.

Creating the iOS Filr App Policy for MobileIron

1 In the MobileIron Admin Portal, click the **Policies & Configs** tab.

2 On the Configuration tab, click **Add New** > **AppConnect** > **Container Policy**.

   The New AppConnect App Configuration dialog box is displayed.

3 Specify the following information:

   Name: Provide a name for the policy, such as `Filr iOS Policy`.

   Description: (Optional) Provide a description for the policy.

   Application: Specify the Filr iOS bundle ID, which is `com.novell.vibefilr`.

4 In the **Data Loss Prevention Policies** section, you can change the following configuration options for iOS devices:

   Print: This setting is not honored in the Filr app. There is no printing ability from within the Filr app.

   Copy/Paste To: This setting is ignored in this release of the Filr mobile app. Copy/Paste functionality is included in the Open In setting. In other words, you must disable Open In in order to disable Copy/Paste.

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

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

5 Click **Save**.

Distributing the Filr App to Devices

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

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

Preventing Frequent Prompts for a Passcode

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

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

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

13.3.4 Managing Mobile Devices with Filr

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

For more information, see Chapter 20, "Managing Mobile Devices," on page 227.

13.4 Understanding Filr Data Security for Mobile Devices

- Section 13.4.1, "App Security," on page 164
- Section 13.4.2, "File Security," on page 164

13.4.1 App Security

On Android devices, the application itself and cached content are stored on internal storage. Internal storage on Android devices is always secure (unless the device has been rooted contrary to manufacturer recommendations). iOS devices do not have a concept of external storage, so data within the application is always secure.

13.4.2 File Security

Files that are downloaded or opened in third-party apps are by nature less secure than files that remain within the app. On Android devices, downloaded files are stored on the device's external storage.

It is up to you as the Filr administrator to decide whether to allow users to download files and open them in third-party applications, as described in Section 13.1, "Configuring Mobile Device Access for All Users," on page 151.

In order for downloaded files to remain secure, users should configure their devices to encrypt files. However, not all devices support file encryption. For information about how to enable file encryption on iOS and Android devices, see "Encrypting Downloaded Files" in the *Novell Filr Mobile App Quick Start*.

14 Setting Up the Filr Desktop Application

The Novell Filr desktop application enables you to work with Filr files on your personal computer. The Novell Filr desktop application synchronizes files from the Filr server with your personal workstation, allowing you to manage Filr files from the file system on your computer. For more information about the Novell Filr desktop application, see the *Novell Filr Desktop Application for Windows Quick Start* (http://www.novell.com/documentation/novell-filr-2/filr-2-qs-desktop/data/filr-2-qs-desktop.html#bwrk0ll) and the *Novell Filr Desktop Application for Mac Quick Start* (http://www.novell.com/documentation/novell-filr-2/filr-2-qs-desktopmac/data/filr-2-qs-desktopmac.html).

As a Filr administrator, you must enable file synchronization for the Filr desktop application in order for users to take advantage of this functionality. There are also optional administrative procedures that you might want to perform when configuring the Filr desktop application.

If you make configuration changes, users must log out of the application and log in again in order to see the changes.

IMPORTANT: For optimal performance, users should not configure the Filr desktop application to synchronize more than 35,000 total files, or to synchronize individual files that are larger than 5 GB to their workstations.

14.1 Planning Filr Desktop Application Usage for Your Filr Site

14.1.1 Understanding System Load

Depending on your environment and the settings that you choose for the Filr desktop application, the Filr desktop application can put a significant load on your Filr system.

Factors that affect the Filr load:

- The number of users in your Filr system
- The number of files that users plan to synchronize to their workstations with the Filr desktop application

If your environment is such that the Filr desktop application is likely to place significant load on your Filr system, consider making the Filr desktop application available to only a few hundred users to begin with. After the initial group of users have synchronized all files to their workstations and Filr is running smoothly, make the application available to another set of users. Continue this process until all users in your system are using the Filr desktop application.

For information about how to make the Filr desktop application available to only a subset of users, see Section 14.2.2, "Configuring the Filr Desktop Application for Individual Users and Groups," on page 168.

14.1.2 Understanding Rights Requirements for Installation

Administrator privileges are required when installing the Filr desktop application on user workstations (either through client management software or directly).

14.2 Enabling Desktop Application Access for Users

The Filr desktop application allows users to synchronize their Novell Filr files with their personal computers. You can enable this functionality for all users in the Filr system, or for individual users and groups. By default, this functionality is not enabled.

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

Users need to download, install, and configure the Filr desktop application on their personal computers. For more information, see the *Novell Filr Desktop Application for Windows Quick Start* (http://www.novell.com/documentation/novell-filr-2/filr-2-qs-desktop/data/filr-2-qs-desktop.html) and the *Novell Filr Desktop Application for Mac Quick Start* (https://www.novell.com/documentation/novell-filr-2/filr-2-qs-desktopmac/data/filr-2-qs-desktopmac.html).

- Section 14.2.1, "Configuring the Filr Desktop Application for All Users," on page 166
- Section 14.2.2, "Configuring the Filr Desktop Application for Individual Users and Groups," on page 168

14.2.1 Configuring the Filr Desktop Application for All Users

To customize the desktop application experience for your Filr system:

1 In Filr, click the **admin** link in the upper-right corner of the page, then click the **Administration Console** icon .

2 Under **System**, click **Desktop Application**.

3 As necessary, configure Filr to allow the Filr desktop application to support the following features:

Access Filr: Allows users to access the Filr site through the Filr desktop application.

You must individually enable each Net Folder to be accessed by the Filr desktop application. For information about how to enable Net Folders to be accessed by the Filr desktop application, see Step 11 in Section 8.6, "Creating and Managing Net Folders," on page 101.

Allowing access to the Filr site through the Filr desktop application can be changed on a per-user basis, as described in Section 14.2.2, "Configuring the Filr Desktop Application for Individual Users and Groups," on page 168.

Cache the user's password: Allows users to enable the **Remember password** option on the **Account Information** page in the Novell Filr Console.

This option can be changed on a per-user basis, as described in Section 14.2.2, "Configuring the Filr Desktop Application for Individual Users and Groups," on page 168.

Be deployed: Select this option to make the Filr desktop application available to users. If this option is selected, users can download the Filr desktop application as described in "Downloading and Installing the Filr Desktop Application (http://www.novell.com/documentation/novell-filr-2/filr-2-qs-desktop/data/filr-2-qs-desktop.html#bwrk0ll)" in the *Novell Filr 2.0 Desktop Application for Windows Quick Start* (http://www.novell.com/documentation/novell-filr-2/filr-2-qs-desktop/data/filr-2-qs-desktop.html#bwrk0ll) or the *Novell Filr 2.0 Desktop Application for Mac Quick Start* (http://www.novell.com/documentation/novell-filr-2/filr-2-qs-desktopmac/data/filr-2-qs-desktopmac.html). If this option is not selected, the link to download the Filr desktop application is not visible to users.

After you select this option, select from the following methods of deploying the Filr desktop application:

- ◆ **Deploy files contained locally:** Select this option to use the Filr server for deploying the Filr desktop application.

  If you select this option, no other configuration is necessary for making the Filr desktop application available to users to download.

- ◆ **Deploy files accessed via a URL to another location:** (Recommended) Select this option if you want to configure a separate web server to deploy the Filr desktop application. Deploying the desktop application in this way minimizes load on the Filr server.

  Select this option if your Filr system is fronted by an L4 or L10 switch.

  For information about how to set up a separate web server to deploy the application, see Section 14.3, "Configuring a Separate Web Server to Deploy the Filr Desktop Application," on page 169.

  If this option is selected, the available field must be populated with the URL of the web server that you configure for deploying the desktop application.

NOTE: You might want to leave the **Be deployed** option deselected if you plan to deploy the Filr desktop application to user workstations by using client management software such as Novell ZENworks. The `.msi` file is available to you if you are planning to deploy the Filr desktop application by using ZENworks.

For more information about how to deploy Filr by using the `.msi` file, see Section 14.6, "Customizing and Modifying the Desktop Application," on page 173.

Synchronization every *xx* Minutes: Specify the interval (in minutes) for how often the Filr desktop application checks the Filr server for changes to **Available Offline** files. The default is every 15 minutes. This means that 15 minutes after one synchronization ends, another begins. This lets you control the amount of load that the Filr desktop application puts on the Filr server.

Changes made in the desktop application are automatically synchronized to the server regardless of this setting.

Maximum file size that can be synchronized: Specify the maximum file size (in MB) that can be synchronized between the Filr desktop application and the Filr server.

4 Click **OK**.

14.2.2 Configuring the Filr Desktop Application for Individual Users and Groups

Individual user and group settings override global settings. This section describes how to customize the desktop application experience for individual users and groups on your Filr system.

To make the desktop application available to only a subset of users in your system, configure the application for all users, as described in Section 14.2.1, "Configuring the Filr Desktop Application for All Users," on page 166, then restrict access to the users and groups who should not have access to the application, as described in this section.

1. In Filr, click the **admin** link in the upper-right corner of the page, then click the **Administration Console** icon .

2. Under **Management**, click **Users**.

   The Manage Users page is displayed.

3. Select the check boxes next to the names of the users or groups for whom you want to configure the Filr desktop application, then click **More** > **Desktop Application Settings**.

   The **Configure Desktop Application** page is displayed.

4. To change the desktop application settings for the selected users to be different from the global settings, select **Use user settings to allow the desktop application to**, then choose from the following options:

   Access Filr: Allows users to access the Filr site through the Filr desktop application.

   You must individually enable each Net Folder to be accessed by the Filr desktop application. For information about how to enable Net Folders to be accessed by the Filr desktop application, see Step 11 in Section 8.6, "Creating and Managing Net Folders," on page 101.

   Cache the user's password: Allows users to enable the **Remember password** option on the **Account Information** page in the Novell Filr Console.

5. Click **OK**.

If you have set individual and group settings for the Filr desktop application, you can change those settings back to the global settings for the individual users and groups.

1. In Filr, click the **admin** link in the upper-right corner of the page, then click the **Administration Console** icon .

2. Under **Management**, click **User Accounts**.

   The Manage Users page is displayed.

3. Select the check boxes next to the names of the users or groups for whom you want to configure the Filr desktop application, then click **More** > **Desktop Application Settings**.

   The **Configure Desktop Application** page is displayed.

4. To change the desktop application settings back to the global settings for the selected users, select **Use global settings**.

5. Click **OK**.

14.3 Configuring a Separate Web Server to Deploy the Filr Desktop Application

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

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

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

2. Download and extract the `NovellFilrAutoUpdate.tgz` file onto the web server. (You can download the `NovellFilrAutoUpdate.tgz` file from the Filr downloads page on the Novell Downloads site (https://download.novell.com).)

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

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

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

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

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

   - From a browser

     For example:

     `http://`*`web_server_address`*`/desktopap/novellfilr/`*`windows`*`/`*`x64`*`/version.json`

   - From a command line

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

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

4. Configure the Filr desktop application as described in Section 14.2.1, "Configuring the Filr Desktop Application for All Users," on page 166.

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

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

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

5. Click **OK**.

14.4   Updating the Filr Desktop Application

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

- Section 14.4.1, "Understanding Missing Dependencies Related to Updating the Filr Desktop Application by Using the MSI File," on page 170
- Section 14.4.2, "Updating the Filr Desktop Application on the Filr Server or on a Separate Web Server," on page 170

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

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

- Microsoft .NET Framework 4.5 (Applies to 64-bit Windows and Mac workstations.)

  You can download Microsoft .NET Framework 4.5 from the Microsoft .NET Downloads page (http://www.microsoft.com/net/downloads).

- Microsoft Visual C++ 2013 Redistributable Package (Applies to all workstations)

  You can download the redistributable package from the Microsoft Download Center (https://www.microsoft.com/en-us/download/details.aspx?id=40784).

14.4.2   Updating the Filr Desktop Application on the Filr Server or on a Separate Web Server

If you have configured your Filr system to deploy the Filr desktop application (as described in Section 14.2, "Enabling Desktop Application Access for Users," on page 166), or if you have configured a separate web server to deploy the Filr desktop application (as described in Section 14.3, "Configuring a Separate Web Server to Deploy the Filr Desktop Application," on page 169), you can replace the Filr desktop application download files on the Filr back end so that users are prompted to update the Filr desktop application on their individual workstations.

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

To download the Filr desktop application:

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

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

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

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

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

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

```
mv novellfilr novellfilr.bak
```

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

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

```
tar xvzf NovellFilrAutoUpdate.tgz
```

You can download the `NovellFilrAutoUpdate.tgz` file from the Novell Downloads site (download.novell.com).

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

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

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

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

```
chown -R wwwrun:www novellfilr/
```

```
chmod -R g-w novellfilr/
```

```
chmod -R o-rwx novellfilr/
```

14.5 Distributing the Filr Desktop Application Synchronization Traffic

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

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

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

14.5.1 Distributing Filr Desktop Application Traffic Separately from Other Applications

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

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

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

For specific information on how to configure the load balancer or reverse proxy server, see Section 14.5.3, "Load Balancer and Reverse Proxy Server Configuration," on page 172.

14.5.2 Distributing Filr Desktop Traffic in Conjunction with Other Applications

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

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

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

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

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

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

For specific information on how to configure the load balancer or reverse proxy server, see Section 14.5.3, "Load Balancer and Reverse Proxy Server Configuration," on page 172.

14.5.3 Load Balancer and Reverse Proxy Server Configuration

For information on how to configure a reverse-proxy server for your Filr site, see Section 1.8, "Changing Reverse Proxy Configuration Settings," on page 28.

14.6 Customizing and Modifying the Desktop Application

You can manage the Filr desktop application on users' workstations with client management software such as Novell ZENworks.

When following the instructions in this section, you must use the `.msi` file, which is bundled in the `NovellFilrAutoUpdate.tgz` file, and is available at the Novell Downloads site (https://download.novell.com/).

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

- Microsoft .NET Framework 4.5 (Applies to 64-bit Windows and Mac workstations.)

  You can download Microsoft .NET Framework 4.5 from the Microsoft .NET Downloads page (http://www.microsoft.com/net/downloads).

- Microsoft Visual C++ 2013 Redistributable Package (Applies to all workstations)

  You can download the redistributable package from the Microsoft Download Center (https://www.microsoft.com/en-us/download/details.aspx?id=40784).

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

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

- Section 14.6.1, "Customizing the Installation for the Filr Desktop Application," on page 173
- Section 14.6.2, "Controlling Windows Explorer Restart," on page 176

14.6.1 Customizing the Installation for the Filr Desktop Application

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

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

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

The following sections describe how to make these customizations.

- "Configuring Default Values" on page 174
- "Enabling Auto-Configuration" on page 175
- "Disallowing User Configuration" on page 175
- "Modifying the Filr Desktop Configuration" on page 176

Configuring Default Values

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

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

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

`\\HKLM\Software\Novell\Filr`

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

`/Applications/Novell Filr/Contents/Info.plist`

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

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

Table 14-1   Default Value Configuration Options

Windows Registry Value Name	Value Type	Mac Property Name	Value Type	Supports Env Variables	Default Value
Default Server URL	REG_SZ	FilrDefaultServer URL	string	No	https://
Default Username	REG_SZ	FilrDefaultUsern ame	string	Yes	%USERNAME% or $USER
Default Account Name	REG_SZ	FilrDefaultAccou ntName	string	No	Hostname in server URL
Default Remember Password	REG_SZ ("true" or "false")	FilrDefaultReme mberPassword	<true/> or <false/>	No	false
Default Sync Dir	REG_SZ	FilrDefaultSyncD ir	string	Yes	%USERNAME% \Filr or $USER\Filr
Default Start On Login	REG_SZ ("true" or "false")	FilrDefaultStartO nLogin	<true/> or <false/>	No	true

Enabling Auto-Configuration

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

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

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

   `\\HKLM\Software\Novell\Filr`

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

   `/Applications/Novell Filr/Contents/Info.plist`

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

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

Table 14-2   Auto-Configuration Options

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

Disallowing User Configuration

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

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

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

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

   `\\HKLM\Software\Novell\Filr`

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

   `/Applications/Novell Filr/Contents/Info.plist`

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

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

Table 14-3 *Disallow User Configuration Options*

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

Modifying the Filr Desktop Configuration

If you have configured the Filr desktop application with auto-configuration (as described in "Enabling Auto-Configuration" on page 175), you can modify the configuration settings:

1 Change the options in the registry or .plist file, then restart the Filr desktop application.

   When the Filr desktop application starts, it detects that the default settings have changed and applies the new settings.

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

14.6.2 Controlling Windows Explorer Restart

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

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

- No UI ("msiexec /qn")

  Windows Explorer is never restarted when using this option.
- Basic UI ("msiexec /qb")
- Reduced UI ("msiexec /qr")
- Full UI ("msiexec /qf" or simply "msiexec", since this is the default)

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

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

14.7 Controlling File Downloads by the Filr Desktop Applications

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

14.7.1 Why File-Download Control Is Important

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

14.7.2 How File-Download Control Works

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

NOTE: for more information regarding the user experience, see "Preventing Application-Driven Downloads From Filling Up the Local Disk" in the *Desktop Quick Start for Windows* and the *Desktop Quick Start for Mac*.

- **No Restrictions:** All applications, including antivirus scanners and backup software, are allowed to download files to the workstation's local disk.

- **Blacklists (default):** Filr ships with two administrator-configurable application blacklists (one each for Windows and Mac). Blacklisted applications are blocked from downloading files through Filr. All unlisted applications are allowed to download.

  When an application that is blacklisted attempts to download files, a system alert displays stating that the download is blocked by an administrative setting.

- **Whitelists:** Filr also lets administrators create whitelists that identify the only approved-to-download applications.

  When an application that is not whitelisted attempts to download files, a system alert displays stating that the download is blocked by an administrative setting.

- **Blacklist and Whitelist:** The final option is to use both lists. Blacklisted applications are always blocked; whitelisted applications are always allowed.

  Filr notifies users when unidentified applications try to download files, and it adds the application to a list of blocked applications. Users can allow downloading by the applications through their Filr console.

14.7.3 Managing File Downloading

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

1 Log in to the Filr administration console and navigate to **System** > **Desktop Application > Application Whitelist/Blacklist**.

2 Review the list of applications that are blocked by default for the desktop platforms (Windows and Mac) that your organization uses.

3 If you want to only block certain applications from downloading files through Filr, ensure that the applications are listed in the appropriate Windows and Mac blacklists.

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

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

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

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

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

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

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

5 If you want a flexible approach that allows downloading by specified applications, blocks downloading by other applications, and lets users deny or approve download requests by unlisted applications, then deploy both a whitelist and a blacklist.

6 Periodically review and update your file-download strategy. Make sure that new antivirus and backup software is included. Consult with users about applications that they have allowed or blocked, and consider adding these to your lists as applicable.

15 Configuring Filr to Support WebDAV on Windows 7

WebDAV is a standard collaborative editing and file management protocol. Novell Filr relies on the WebDAV protocol to edit files, as described in "Editing Files with Edit-in-Place" in the *Filr 2.0: Web Application User Guide*.

If your Filr users are running a supported client operating system other than Windows 7, editing files works without any problems. Windows 7 must be configured to use a self-signed certificate in order to work with WebDAV.

The information in this section assumes that your environment requires the use of Microsoft Office. If your environment does not require the use of Microsoft Office, see Section 15.1.4, "Using OpenOffice as Your Document Editor for WebDAV," on page 181.

- Section 15.1, "Planning Your WebDAV Implementation," on page 179
- Section 15.2, "Editing Files with Edit-in-Place Functionality," on page 181
- Section 15.3, "Mapping a Filr Folder as a WebDAV Folder," on page 181
- Section 15.4, "Configuring Windows 7 to Use a Self-Signed Certificate with Filr," on page 181
- Section 15.5, "Allowing Basic Authentication over an HTTP Connection on Windows 7," on page 183

15.1 Planning Your WebDAV Implementation

- Section 15.1.1, "Understanding the Different Types of WebDAV Authentication Methods," on page 179
- Section 15.1.2, "Using WebDAV When Filr Is Fronted by NetIQ Access Manager," on page 180
- Section 15.1.3, "Meeting Filr Certificate Requirements on Windows 7," on page 180
- Section 15.1.4, "Using OpenOffice as Your Document Editor for WebDAV," on page 181

15.1.1 Understanding the Different Types of WebDAV Authentication Methods

Novell Filr supports the following WebDAV authentication methods:

- **Basic Authentication:** The user name and password are encoded with the Base64 algorithm. The Base64-encoded string is unsafe if transmitted over HTTP, and therefore should be combined with SSL/TLS (HTTPS).

  For more information, see "Choosing Basic Authentication" on page 36.

  If you plan to use Basic authentication over a non-secure connection (HTTP), you need to modify the registry on each Windows 7 client workstation, as described in Section 15.5, "Allowing Basic Authentication over an HTTP Connection on Windows 7," on page 183. The registry modification allows users to use WebDAV with Microsoft Office 2007. However, Microsoft Office 2010 is not supported.

◆ **Digest Authentication:** Applies MD5 cryptographic, one-way hashing with nonce values to a password before sending it over the network. This option is more safe than Basic Authentication when used over HTTP.

   For more information, see "Choosing Digest Authentication" on page 36.

15.1.2 Using WebDAV When Filr Is Fronted by NetIQ Access Manager

If your Filr system is fronted by NetIQ Access Manager, you must use the designated WebDAV authentication method:

Product Fronting Filr	Designated Authentication Method
NetIQ Access Manager	If your Filr installation is fronted by NetIQ Access Manager, as described in Section 1.8, "Changing Reverse Proxy Configuration Settings," on page 28, you must use basic authentication for your WebDAV implementation.
	During the Filr appliance configuration, select **basic** when configuring WebDAV, as described in Section 1.12, "Changing WebDAV Authentication Configuration Settings," on page 35.

15.1.3 Meeting Filr Certificate Requirements on Windows 7

If you are using WebDAV functionality with Filr on Windows 7 with a secure (HTTPS) connection, ensure that the Filr server certificate requirements are met. If all of the requirements are not met, various Windows 7 services fail.

Filr server certificate requirements:

   ◆ You must use a trusted server certificate that is accepted by Windows 7. This server certificate must be signed by a trusted certificate authority (CA) such as VeriSign or Equifax.

   NOTE: You can use a self-signed certificate only if the certificate is imported into the Trusted Root Certification Authorities store on each Windows 7 client computer.

   ◆ The trusted server certificate must be issued to a name that exactly matches the domain name of the URL that you are using it for. This means that it must match the URL of your Filr site.

   ◆ The date range for the trusted server certificate must be valid. You cannot use an expired server certificate.

   ◆ The Windows 7 system must be adjusted to enable FIPS-compliant algorithms for encryption, hashing, and signing, unless you are using Novell Access Manager 4.1.1 or later.

      1. From the Start menu, type **Local Security Policy**, then press Enter.

      2. Expand **Local Policies**, then select **Security Options**.

      3. Enable the following setting:

         System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing.

15.1.4 Using OpenOffice as Your Document Editor for WebDAV

If your environment does not require the use of Microsoft Office, you might consider migrating users to OpenOffice 3.1 or later as their document editor. Using OpenOffice 3.1 or later provides seamless integration between the WebDAV server and Filr, regardless of which operating system is being used.

15.2 Editing Files with Edit-in-Place Functionality

IMPORTANT: Due to security concerns about the NPAPI cross platform plug-in architecture, Google's Chrome browser version 45 and later and Microsoft's Edge browser have discontinued support for the Java browser plug-in. Because Filr's Edit-in-Place functionality relies on the plug-in, Edit-in-Place is no longer supported in these browsers.

Novell anticipates that other browser vendors might also discontinue support for the Java browser plug-in in the near future.

If you are using a browser that still supports the NPAPI plug-in architecture, you can leverage Edit-in-Place functionality. For information on how to edit files in Filr with Edit-in-Place functionality, see "Editing Files with Edit-in-Place" in the *Filr 2.0: Web Application User Guide*.

If you are using Edit-in-Place functionality over HTTP, no additional setup is required. However, if you are using Edit-in-Place functionality over HTTPS on Windows 7, ensure that you have met the Filr server certificate requirements, as described in Section 15.1.3, "Meeting Filr Certificate Requirements on Windows 7," on page 180.

For more information about editing Filr documents in Microsoft Office with Windows 7, see "TID 7006717: Document editing failure with Windows 7 and Microsoft Office" in the Novell Support Knowledgebase (http://www.novell.com/support/kb/).

15.3 Mapping a Filr Folder as a WebDAV Folder

Mapping a Novell Filr folder as a WebDAV folder on the client computer allows access to Filr files from a WebDAV-compliant file navigation tool such as Windows Explorer or Nautilus. For information on how to map a Filr folder, see "Adding Files to a Folder through WebDAV" in the *Filr 2.0: Web Application User Guide*.

When you map a Filr folder as a WebDAV folder on Windows 7, ensure that all Filr server certificate requirements are met, as described in Section 15.1.3, "Meeting Filr Certificate Requirements on Windows 7," on page 180.

15.4 Configuring Windows 7 to Use a Self-Signed Certificate with Filr

Configuring Windows 7 to use a self-signed certificate with Novell Filr is a two-step process. The first step is accomplished by the Filr administrator on the Filr server, and the second step is accomplished by each Filr user on his or her Windows 7 workstation.

- Section 15.4.1, "Administrator Configuration Responsibilities," on page 182
- Section 15.4.2, "User Configuration Responsibilities," on page 182

15.4.1   Administrator Configuration Responsibilities

1 Ensure that the following prerequisites are met in order to configure Windows 7 to use a self-signed certificate with Filr:

- ◆ The self-signed server certificate must be issued to a name that exactly matches the domain name of the URL that you use it for. This means that it must match the URL of your Filr site.
- ◆ The date range for the trusted server certificate must be valid. You cannot use an expired server certificate.

15.4.2   User Configuration Responsibilities

Each Windows 7 workstation user must import the self-signed certificate of the Filr server into the **Trusted Root Certification** Authorities store.

In a controlled corporate environment where the system administrator sets up each client workstation before use, this certificate can be preinstalled on each Windows 7 workstation. This can minimize end-user error and frustration.

1 Launch the Internet Explorer browser.

2 Click **Tools** > **Internet Options** to display the Internet Options dialog box.

3 Click the **Security** tab, then select **Trusted sites**.

4 Click **Sites**.

5 In the **Add this website to the zone** field, specify the URL of the Filr web site, then click **Add** > **Close**.

6 Browse to your Filr site.

7 (Conditional) If a prompt displays indicating that there is a problem with this web site's security certificate, complete the following steps:

7a Click **Continue to this website (not recommended)**.

7b Click **Certificate Error** at the right of the address bar, then click **View certificates**.

7c Click **Install Certificate**, then click **Next** in the wizard.

7d Select **Place all certificates in the following store**.

7e Click **Browse**, browse to and select **Trusted Root Certification Authorities**, then click **OK**.

7f In the wizard, click **Next**, then click **Finish**.

7g (Conditional) If a Security Warning dialog box displays, click **Yes**.

7h Click **OK** to close the Certificate Import Wizard.

7i Click **OK** to close the Certificate window.

7j Shut down all instances of the Internet Explorer browser, then restart the browser.

7k Browse to the Filr site. You should no longer see the certificate error message.

If you continue to see the certificate error message, the server's self-signed certificate might not match the site URL, as described in Section 15.4.1, "Administrator Configuration Responsibilities," on page 182.

15.5 Allowing Basic Authentication over an HTTP Connection on Windows 7

You can modify the Windows registry to allow Basic authentication to WebDAV over an HTTP connection. This registry change allows users to use Microsoft Office 2007 on the Windows 7 operating system, but does not allow them to use Microsoft Office 2010. Microsoft Office 2010 is not supported with Basic Authentication over an HTTP connection.

To modify the Windows registry:

1 On each Windows 7 workstation, click **Start** > **Run**, then specify `regedit` in the **Open** field.

2 Click **OK**.

3 In the Registry Editor window, navigate to the following registry entry:

`\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlset\services\WebClient\Parameters\BasicAuthLevel`

4 Change the value of this registry entry to `2`.

5 Navigate to the Services interface, then restart the **WebClient** service.

16 Managing HTML Renderings of Documents

Filr caches document HTML conversions by default. Because of this, you need to understand what document HTML conversions are and how to delete them if they begin consuming large amounts of disk space. Also, you can install additional fonts on the Filr server to improve HTML rendering.

- Section 16.1, "Understanding Document HTML Conversions," on page 185
- Section 16.2, "Manually Deleting Saved Document Conversions," on page 185
- Section 16.3, "Installing Additional Fonts to Improve Document HTML Rendering," on page 186

16.1 Understanding Document HTML Conversions

Filr converts documents to HTML to enable users to quickly view documents without the need of a separate editing or viewing application. (For information about how users can view files in HTML, see "Viewing the File in Your Web Browser" in the *Filr 2.0: Web Application User Guide*.)

Document conversions are saved and stored in the Filr cache store, in the `/cachefilestore` directory. After a document conversion has been saved, Filr does not need to convert the document to HTML the next time a user views the file in HTML, if the file has not been changed since it was last converted. This process of saving and re-using HTML conversions places less load on the Filr system.

To conserve disk space, the contents of the `/cachefilestore/converted_html_files` directory are deleted when the Filr appliance is restarted at a time when the `/cachefilestore/converted_html_files` directory exceeds 10 GB. If the Filr appliance is restarted and the contents of the `/cachefilestore/converted_html_files` directory do not exceed 10 GB, the contents of the directory are not deleted.

For information about how to manually delete document conversions, see Section 16.2, "Manually Deleting Saved Document Conversions," on page 185.

16.2 Manually Deleting Saved Document Conversions

You might want to delete saved document conversions if your Filr system is running out of disk space or if existing document conversions become out of date or corrupted for any reason. After the document conversions have been deleted, they are re-created the next time a document is viewed in HTML.

Document conversions are automatically deleted when the Filr appliance is restarted at a time when the `/cachefilestore/converted_html_files` directory exceeds 10 GB, as described in Section 16.1, "Understanding Document HTML Conversions," on page 185.

To manually delete all saved document conversions:

1 Purge the `/cachefilestore` directory.

2 Re-create the `/cachefilestore` directory at the same location.

16.3 Installing Additional Fonts to Improve Document HTML Rendering

Users can view files in an HTML view either from the Filr web client (as described in "Viewing the File in Your Web Browser" in the *Filr 2.0: Web Application User Guide*) or from the Filr mobile app. This is often the easiest way for users to view a file in Read-Only mode.

To improve the way fonts are displayed when they are rendered into HTML, you can install additional fonts on your Filr server.

IMPORTANT: The fonts that you apply will get overwritten when you update your Filr system. You must re-apply the fonts as described in this section after you update Filr.

You can upload Microsoft TrueType fonts as well as fonts for viewing Asian characters.

16.3.1 Uploading Microsoft TrueType Fonts to the Filr Server

1 Log in as `root` to the Filr command prompt.

2 Type the following command to navigate to the `fonts` directory, then press Enter:

```
cd /filrinstall/fonts
```

3 Install the supported RPM files by typing the following command, then press Enter:

```
rpm -ivh *.rpm
```

The RPM files are now installed on the Filr server.

4 Run the script to retrieve the fonts by typing the following command, then press Enter:

```
sh fetchmsttfonts-11.1-5.7.10-fetchmsttfonts.sh.txt
```

The fonts are downloaded from Sourceforge and installed on your Filr server.

16.3.2 Uploading Chinese Fonts to the Filr Server

1 Log in as `root` to the Filr command prompt.

2 Launch YaST2 control center by typing the following command:

```
YaST2
```

3 Under **System**, select **Language**, then press Enter.

4 On the Languages page, tab down to the **Secondary Languages** section, then scroll to and select **Traditional Chinese**.

5 Select **OK**.

6 Configure a software repository that has access to a SLES 11 server. For example, you can insert a SLES 11 SP3 DVD into the workstation where Filr is running, or point to a URL of a SLES 11 SP3 repository.

   6a In the YaST2 control center, under **Software**, select **Software Repositories**.

   6b Select **Add**, then select the method by which you want to connect to the repository.

   For example, select **DVD** if you want to insert a SLES 11 SP3 DVD into the workstation.

7 In the YaST2 control center, under **Software**, select **Software Management**.

8 Search for `MozillaFirefox-translations`, then install this package.

9 Verify that the following packages were installed:

```
FZFangSong
FZHeiTi
FZKaiTi
FZSongTi
ttf-arphic-gbsn00lp
ttf-arphic-gkai00mp
ttf-arphic-ukai
ttf-arphic-uming
yast2-trans-zh_CN
kde3-i18n-zh_CN
kde4-l10n-zh_CN
libreoffice-help-zh-CN
libreoffice-l10n-zh-CN
sles-installquick_zh_CN
translation-update-zh_CN
```

17 Managing a Multiple-Language Filr Site

◆ Section 17.1, "Accommodating Multiple Languages," on page 189

17.1 Accommodating Multiple Languages

◆ Section 17.1.1, "Understanding the Filr Site Default Language," on page 189
◆ Section 17.1.2, "Changing the Default Language on the Login Page," on page 189

17.1.1 Understanding the Filr Site Default Language

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

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

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

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

17.1.2 Changing the Default Language on the Login Page

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

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

1 Navigate to the Guest profile.

2 On the Profile page, click **Edit**.

   The User page is launched.

3 In the **Locale** drop-down list, select the language that you want to be displayed on your login page.

   Users who log in as Guest view the Filr site in the language that you select.

4 Click **OK**.

Each Filr user can change the language on a per-user basis by changing the **Locale** setting in the user profile, as described in "Modifying Your Profile" in the *Filr 2.0: Web Application User Guide*.

III Maintaining the Filr Site

18 Managing Users

As time passes on your Novell Filr site, users come and go, resulting in the need for periodic maintenance activities.

18.1 Synchronizing Users and Groups from an LDAP Directory

Unless you are planning a very small Novell Filr site, the most efficient way to create Filr users is to synchronize initial user information from your network directory service (NetIQ eDirectory, Microsoft Active Directory, or other LDAP directory service) after you have installed the Filr software. Over time, you can continue to synchronize user information from the LDAP directory to your Filr site.

IMPORTANT: The following limitations apply when synchronizing user information to Filr from an LDAP directory service:

- Filr performs one-way synchronization from the LDAP directory to your Filr site. If you change user information on the Filr site, the changes are not synchronized back to your LDAP directory.
- Filr does not support multi-value attributes. If your LDAP directory contains multi-value attributes, Filr recognizes only the first attribute. For example, if your LDAP directory contains multiple email addresses for a given user, only the first email address is synchronized to Filr.
- Users that are imported to Filr via LDAP are always authenticated to Filr via the LDAP source. If the LDAP source is unavailable for any reason, the LDAP-imported users cannot log in to Filr.

For information about known issues with LDAP synchronization in Filr, see "LDAP Synchronization Issues (http://www.novell.com/documentation/novell-filr-2/filr-2-relnote/data/filr-2-relnote.html#ble286e)" in the *Novell Filr 2.0 Release Notes* (http://www.novell.com/documentation/novell-filr-2/filr-2-relnote/data/filr-2-relnote.html).

Table 18-1 shows user synchronization rates based on samples from test labs at Novell. Results may vary depending on hardware, LDAP server, database, and network topology.

Table 18-1 *LDAP Synchronization Performance Rate Samples*

Number of Users Synchronized	Time Required to Complete Synchronization
1,000	20 seconds
2,500	44 seconds
10,000	2 minutes
20,000	5 minutes
50,000	13 minutes

To synchronize users and groups from LDAP:

1 Log in to Filr as the Filr administrator.

    1a Launch a web browser.

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

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

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

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

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

3 Under **System**, click **LDAP**.

- Section 18.1.1, "Configuring an LDAP Connection," on page 194
- Section 18.1.2, "Configuring LDAP Synchronization," on page 201
- Section 18.1.3, "Restricting Local User Accounts from Logging In," on page 204
- Section 18.1.4, "Previewing and Running the LDAP Synchronization," on page 205
- Section 18.1.5, "Viewing Synchronization Results," on page 206
- Section 18.1.6, "Deleting an LDAP Configuration," on page 206

18.1.1 Configuring an LDAP Connection

You can configure one or more LDAP connections to your directory.

You should never configure multiple LDAP connections to point to the same location on the same LDAP directory. If you need a failover solution, you should use a load balancer.

To configure an LDAP connection:

1 On the LDAP Configuration page, click the **LDAP Servers** tab.

2 To create a new LDAP connection, click **Add**.

or

To modify an existing LDAP connection, click the URL of the connection in the **Server URL** column of the provided table.

3 On the LDAP Server Configuration dialog box, specify the information on each tab, as described in the following sections:

◆ "Server Information" on page 195

◆ "Users" on page 198

◆ "Groups" on page 200

Server Information

1 On the **LDAP Servers** tab, click Add.

The LDAP Server Configuration dialog box is displayed.

2 Specify the following information on the **Server Information** tab:

IMPORTANT: When modifying an existing LDAP connection, do not modify the LDAP server URL. Doing so can lead to synchronized users being disabled or deleted.

LDAP Server URL: In order to synchronize initial user information, Filr needs to access an LDAP server where your directory service is running. You need to provide the host name of the server, using a URL with the following format:

```
ldap://hostname
```

If the LDAP server requires a secure SSL connection, use the following format:

```
ldaps://hostname
```

If the LDAP server is configured with a default port number (389 for non-secure connections or 636 for secure SSL connections), you do not need to include the port number in the URL. If the LDAP server uses a different port number, use the following format for the LDAP URL:

```
ldap://hostname:port_number
ldaps://hostname:port_number
```

If the LDAP server requires a secure SSL connection, additional setup is required. You must complete the steps in Section 31.3, "Securing LDAP Synchronization," on page 296 to import the root certificate for your LDAP directory into the Java keystore on the Filr server before you configure Filr for LDAP synchronization.

User DN (proxy user for synchronizing users and groups): Filr needs the user name and password of a user on the LDAP server who has sufficient rights to access the user information stored there:

Directory Service	Required Rights
eDirectory	◆ [All Attribute Rights] - Compare & Read ◆ [Entry Rights] - Browse (on the container containing the users that need to be imported into Filr)
Active Directory	Any authenticated user can be used as the proxy user as long as there are no read restrictions in place on the Organizational Unit (OU) that contains the users Required rights if OU read restrictions are in place: ◆ Read (on the Organizational Unit containing the users that need to be imported into Filr) Ensure that **This object & all descendant objects** is selected in the **Security** tab under the advanced options.

You need to provide the fully qualified, comma-delimited user name, along with its context in your LDAP directory tree, in the format expected by your directory service.

Directory Service	Format for the User Name
eDirectory	`cn=username,ou=organizational_unit,o=organization`
Active Directory	`cn=username,ou=organizational_unit,dc=domain_component`

Password: Password for the User DN.

Directory Type: The directory type that you are connecting to. Select **eDirectory** or **Active Directory**.

GUID attribute: Depending on the directory type that you chose, this field is populated with the name of the LDAP attribute that uniquely identifies a user or group. For eDirectory, this value is GUID. For Active Directory, this value is objectGUID. This attribute always has a unique value that does not change when you rename or move a user in the LDAP directory. It ensures that Filr modifies the existing user instead of creating a new user when the user is renamed or moved in the LDAP directory.

If this attribute is not set and you rename or move a user in the LDAP directory, Filr assumes that the new name (or the new location of the same name) represents a new user, not a modified user, and creates a new Filr user.

For example, suppose you have a Filr user named William Jones. If William changes his name to Bill, and you make that change in the LDAP directory, Filr creates a new user named Bill Jones.

If you want to map users to a different attribute, select **Other** in the drop-down list, specify the name of the LDAP attribute, then click **OK**. Before you do this, ensure that the attribute that you use is a binary attribute. For example, the cn attribute cannot be used because it is not a binary attribute.

Create Users As: Specify whether you want Filr to treat the users as Internal or External.

Filr account name attribute: The attribute you choose here depends on the directory type you selected in the **Directory type** drop-down list. If you selected **eDirectory** in the **Directory type** drop-down list, you see **cn** and **Other** as options for this attribute. If you selected **Active Directory** or **Other** in the **Directory type** drop-down list, you see **sAMAccountName**, **cn**, and **Other** as options for this attribute. If you select **Other** as the value for this attribute, you are prompted to enter the name of the LDAP attribute. The value of the attribute that you enter is used for the Filr account name.

The Filr account name attribute has two purposes:

- ◆ Used as the Filr user name when the user is first provisioned from LDAP. The value of this attribute must be unique.

- ◆ During Filr login, Filr uses this attribute to locate the user in the LDAP directory and then tries to authenticate as that user.

LDAP directories differ in the LDAP attribute used to identify a User object. Both eDirectory and Active Directory might use the cn (common name) attribute. A more sure alternative for Active Directory is to use the sAMAccountName attribute. Other LDAP directories might use the uid (unique ID) attribute, depending on the structure and configuration of the directory tree.

You might need to consult with your directory administrator in order to determine which attribute is best to use. In some cases where not all users are imported successfully, you might need to set up two LDAP sources pointing to the same LDAP server and have each source use a different value for the **LDAP Attribute Used for Filr Name**. For example, set up one LDAP source and use cn as the **Filr account name attribute**. Then set up a separate source to the same LDAP server and use 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 on User objects could be used to enable Filr users to log in to the Filr site by using their email addresses.

NOTE: Because the login name becomes part of the user's workspace URL, the at sign (@) in the email address is replaced with an underscore (_) in the workspace URL because @ is not a valid character in a URL.

3 Continue with .

Users

1 On the LDAP Server Configuration page, click the **Users** tab, then click **Add**.

The LDAP Search dialog box is displayed.

2 Specify the following information n the LDAP search dialog box:

Base DN: Filr can find and synchronize initial user information from User objects located in one or more containers in the LDAP directory tree. A container under which User objects are located is called a base DN (distinguished name). The format you use to specify a base DN depends on your directory service.

Directory Service	Format for the User Container
eDirectory	`ou=organizational_unit,o=organization`
Active Directory	`ou=organizational_unit,dc=domain_component`

Container names cannot exceed 128 characters. If the container name exceeds 128 characters, users are not provisioned.

TIP: You can use the **Browse** icon 🗃️ next to the **Base DN** field to browse the LDAP directory for the base DN that you want to use.

Filter: To identify potential Filr users, Filr by default filters on the following LDAP directory object attributes:

* `Person`
* `orgPerson`
* `inetOrgPerson`

You can add attributes to the user or group filter list if necessary. You can use the following operators in the filter:

* | OR (the default)
* & AND
* ! NOT

You might find it convenient to create a group that consists of all the users that you want to set up in Filr, regardless of where they are located in your LDAP directory. After you create the group, you can use the following filter to search for User objects that have the specified group membership attribute:

IMPORTANT: If you create a filter to search for a specific group to find users, users that are located in any sub-groups to that group are not synchronized.

When synchronizing against Active Directory, you can create a filter that synchronizes users in sub-groups by using the following rule object identifier (OID):

`<attribute name>:<matching rule OID>:=<value>`

Be sure to include the parentheses in your filter.

Directory Service	Filter to search for User objects
eDirectory	`(groupMembership=cn=`*`group_name`*`,ou=`*`organizational_unit`*`,o=`*`organization`*`)`
Active Directory	`(memberOf=cn=`*`group_name`*`,ou=`*`organizational_unit`*`,dc=`*`domain_component`*`)`

Search subtree: Select whether you want Filr to search for users in containers underneath the base DN (that is, in subtrees).

Home Directory Net Folder Configuration: Select from the following options for creating Home directories for users in the Filr system:

For more information about Home directories, see Section 8.4, "Configuring Home Folders for Display in the My Files Area," on page 94.

* **Use the following custom criteria:** Select this option to specify the Net Folder Server and path where user Home directory information is located.

  In the **Net Folder Server** field, select the Net Folder Server that will be used with the Home directory Net Folders that will be created automatically when a user logs in. If you have not already created Net Folder Servers, or if you need to create a new one, click **Create Net Folder Server**. For information about how to create a Net Folder Server, see Section 8.5, "Configuring and Managing Net Folder Servers," on page 96.

  In the **Relative path** field, specify the path that points to user home directories on the selected server.

You must use a replaceable parameter in the **Relative path** field. Replaceable parameters are entered by using the following syntax: `%attributeName%`. Replaceable parameters are evaluated dynamically each time a user logs in to Filr, and are replaced with the value of the given LDAP attribute. For example, if each users' Home directory is associated with the `cn` value in the LDAP directory, specify the following in the **Relative path** field: `Home\%cn%`.

The server path must be entered using UNC syntax.

- ◆ **Use the LDAP Home directory attribute:** Select this option to use the LDAP Home directory attribute. This attribute is detected 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, a Net Folder Server is ready to be configured immediately after running the LDAP synchronization process. (For more information about configuring the Net Folder Server, see Section 8.5, "Configuring and Managing Net Folder Servers," on page 96.)

- ◆ **Use the specified LDAP attribute:** Select this option to specify the name of the LDAP attribute that contains the home directory information. The attribute must be of type String. The attribute must contain a string that is a UNC path, with one of the following forms:

  `\\server\volume\path`

  `\\server\share\path`

  `\\server\share`

- ◆ **Don't create a Home directory Net Folder:** 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.

3 Click **OK**.

4 Continue with "Groups" on page 200.

Groups

1 On the LDAP Server Configuration page, click the **Groups** tab, then click **Add**.

The LDAP Search dialog box is displayed.
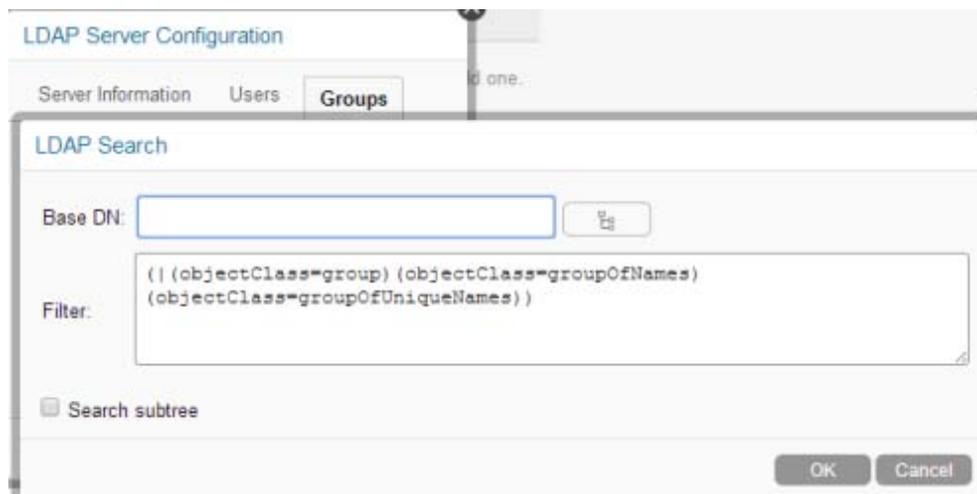
2 Specify the following information on the LDAP Search dialog box:

Base DN: Filr can find and synchronize initial user information from group objects located in one or more containers in the LDAP directory tree. A container under which User objects are located is called a base DN (distinguished name). The format you use to specify a base DN depends on your directory service.

Directory Service	Format for the User Container
eDirectory	`ou=organizational_unit,o=organization`
Active Directory	`ou=organizational_unit,dc=domain_compone` `nt`

Container names cannot exceed 128 characters. If the container name exceeds 128 characters, users are not provisioned.

TIP: You can use the **Browse** icon ⬚ next to the **Base DN** field to browse the LDAP directory for the base DN that you want to use.

Filter: To import groups based on information in your LDAP directory, Filr filters on the following LDAP directory object attributes:

- `group`
- `groupOfNames`
- `groupOfUniqueNames`

You can add attributes to the group filter list if necessary. You can use the following operators in the filter:

- | OR (the default)
- & AND
- ! NOT

IMPORTANT: Be sure to include the parentheses in your filter.

Directory Service	Filter to search for Group objects
eDirectory	`(groupMembership=cn=group_name,ou=organiza` `tional_unit,o=organization)`
Active Directory	`(memberOf=cn=group_name,ou=organizational_` `unit,dc=domain_component)`

Search subtree: Select whether you want Filr to search for groups in containers beneath the base DN (that is, in subtrees).

3 Click **OK**, then click **OK** again to save the LDAP server configuration.

4 Continue with .

18.1.2 Configuring LDAP Synchronization

When you configure LDAP synchronization, you configure user synchronization options, groups synchronization options, and the synchronization schedule.

NOTE: Because the synchronization options apply to all LDAP configurations for the Filr system, you cannot have customized synchronization settings for each LDAP configuration.

Configuring User Synchronization Options

1 On the LDAP Configuration page, click the **User Settings** tab.

2 Specify the following information for enabling and configuring user synchronization from your LDAP directory to your Filr site:

Register LDAP user profiles automatically: Select this option to automatically add LDAP users to the Filr site. However, workspaces are not created until users log in to the Filr site for the first time.

Synchronize user profiles: Select this option to synchronize user information whenever the LDAP directory information changes after initial Filr site setup. The attributes that are synchronized are the attributes that are found in the map box on the **Server Information** tab on the LDAP Server Configuration page.

Filr synchronizes the following attributes from the LDAP directory:

- First name
- Last name
- Phone number

- Email address
- Description

For user accounts provisioned from LDAP that are no longer in LDAP: Because deleting user accounts cannot be undone, Novell recommends that you leave **Disable account** selected.

For more information about disabled users in Filr, see Section 18.8, "Disabling Filr User Accounts," on page 213.

Select **Delete account** only if you are certain that you want to delete users that exist on the Filr site but do not exist in your LDAP directory. If you do decide to delete user accounts, you can select the option **Also delete associated user workspaces and content** to remove obsolete information along with the user accounts.

IMPORTANT: A deleted user cannot be undeleted; deleting a user is permanent and is not reversible.

If you are sure that you want to automatically delete users that are not in LDAP, this option is designed to be used under the following conditions:

- You have deleted users from your LDAP directory and you want the LDAP synchronization process to also delete them from Filr.
- In addition to the users synchronized from LDAP, you create some Filr users manually, as described in Section 18.3, "Creating a New Local User," on page 206, and you want the LDAP synchronization process to delete the manually created users.

Use the following when creating new users

- **Time Zone:** 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.

  Common selections for United States time zones:

Time Zone	Continent/City
Pacific Time	America/Los Angeles
Mountain Time	America/Denver
Central Time	America/Chicago
Eastern Time	America/New York

- **Locale:** 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.

3 Continue with "Configuring Group Synchronization Options" on page 203.

Configuring Group Synchronization Options

1 On the LDAP Configuration page, click the **Groups** tab.

2 Specify the following information for enabling and configuring user and group synchronization from your LDAP directory to your Filr site:

Register LDAP group profiles automatically: Select this option to automatically add LDAP groups to the Filr site.

Synchronize group profiles: Select this option to synchronize group information, such as the group description, to the Filr site whenever this information changes in LDAP.

Synchronize group membership: Select this option so that the Filr group includes the same users (and possibly groups) as the group in your LDAP directory. If you do not select this option, and you make changes to group membership in the LDAP directory, the changes are not reflected on your Filr site.

If users have rights to files on your OES or Windows file systems through group membership, you must select this option to synchronize group membership to Filr. If you do not synchronize group membership, users who have access rights to files through membership in a group might not have the appropriate access rights in Filr.

Delete groups that were provisioned in LDAP but are no longer in LDAP: Select this option to delete groups that exist on the Filr site but do not exist in your LDAP directory. Use this option under the following conditions:

- You have deleted groups from your LDAP directory and you want the LDAP synchronization process to delete them from Filr as well.

- In addition to the groups synchronized from LDAP, you create some Filr groups manually, as described in Chapter 9, "Creating Groups of Users," on page 115, and you want the LDAP synchronization process to delete the manually created groups.

3 Continue with "Configuring the Synchronization Schedule" on page 204.

Configuring the Synchronization Schedule

This section describes how to set a schedule for the LDAP synchronization.

When planning the schedule, take into account how often your LDAP directory user (and, optionally, group) information changes and the server resources required to perform the synchronization for the number of users (and, optionally, groups) that you have.

1 On the LDAP Configuration page, click the **Synchronization Schedule** tab.

2 Select **Enable schedule** to enable a schedule for the LDAP synchronization to occur.

3 Select whether to run the LDAP synchronization every day, or select specific days of the week when you want it run (for example, on Monday, Wednesday, and Friday).

   You can choose to have it run once a day at a specified time (for example, at 2:00 a.m.), or you can set a time interval, so that it is run multiple times each day (for example, every four hours). The smallest time interval you can set is .25 hours (every 15 minutes).

4 (Conditional) If you want to restrict local users from logging in to the Filr site, continue with Section 18.1.3, "Restricting Local User Accounts from Logging In," on page 204.

5 Continue with Section 18.1.4, "Previewing and Running the LDAP Synchronization," on page 205.

18.1.3 Restricting Local User Accounts from Logging In

By default, Filr allows locally created users to log in the Filr site. This section describes how to configure Filr to allow only users that are synchronized via LDAP to log in.

1 On the LDAP Configuration page, click the **Local User Accounts** tab.

2 Leave **Allow log in for local user accounts (i.e. user accounts not in LDAP)** to allow users who you have created locally to log in to the Filr site.

   For more information about creating users, see Section 18.3, "Creating a New Local User," on page 206.

3 Continue with Section 18.1.4, "Previewing and Running the LDAP Synchronization," on page 205.

18.1.4 Previewing and Running the LDAP Synchronization

Before you run the LDAP synchronization, it is a good idea to preview the synchronization so that you are aware what changes will occur when you run the live synchronization.

- ◆ "Previewing LDAP Synchronization" on page 205
- ◆ "Running the LDAP Synchronization" on page 205

Previewing LDAP Synchronization

After you have configured the LDAP connection, you can see a preview of what the synchronization results will be. This allows you to see beforehand the users and groups that will be added or deleted, as well as the users that will be disabled, before you run the actual synchronization.

To preview the LDAP synchronization:

1 On the LDAP Configuration page, click the **LDAP Servers** tab, then click **Preview sync**.

Users and groups that will be modified by running the LDAP sync are shown, along with information about how they will be modified (whether they will be added, modified, deleted, or disabled).

2 (Optional) Specify a user or group in the **Filter List** field to filter the list of users and groups to be synchronized.

or

Click the drop-down arrow next to the **Filter List** field, then select the type of users or groups that you want to display, then click **OK**. (For example, select to display added users, modified users, modified groups, and so forth.)

3 After you review the results of the synchronization, click **Close**, then continue with "Running the LDAP Synchronization" on page 205.

Running the LDAP Synchronization

After you have run the preview of the LDAP synchronization (as described in "Running the LDAP Synchronization" on page 205), you are ready to run the live synchronization.

1 On the LDAP Configuration page, click the **LDAP Servers** tab, then click **Sync All**.

Users and groups that have been modified by running the LDAP sync are shown, along with information about how they have been modified (whether they were added, modified, deleted, or disabled).

2 (Optional) Specify a user or group in the **Filter List** field to filter the list of users and groups to be synchronized.

or

Click the drop-down arrow next to the Filter List field, then select the type of users or groups that you want to display. (For example, select to display added users, modified users, modified groups, and so forth.)

3 Click **Close**.

18.1.5 Viewing Synchronization Results

You can view the synchronization results of the most recent LDAP synchronization for the current browser session. If you perform a synchronization, log out of Filr, and then log in again, you cannot view the results of the LDAP synchronization for your previous session.

To view the results for a previous synchronization:

1 On the LDAP Configuration page, click the **LDAP Servers** tab.

2 Click **Show sync results**.

18.1.6 Deleting an LDAP Configuration

IMPORTANT: If you delete an LDAP configuration and you have selected the option to delete user accounts that are provisioned from LDAP that are no longer in LDAP, all users that were synchronized to the Filr site through that LDAP configuration are deleted from the Filr site. (For more information about the configuration option concerning user accounts provisioned from LDAP, see "Configuring User Synchronization Options" on page 202.)

---

1 On the LDAP Configuration page, click the **LDAP Servers** tab.

2 Select the LDAP configuration that you want to delete, then click **Delete**.

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

Path to Configuration Dialog: Filr Administration > Console**Management > Default User Settings**

By default, the locale setting for newly created non-LDAP and external users is `English (US)` and the time zone is set to `Greenwich Mean Time (GMT)`.This dialog lets you change the defaults.

You specify the default locale and time zone for LDAP users when you configure LDAP synchronization.

18.3 Creating a New Local User

You can manually create users on the Filr site, rather than synchronizing user information from an LDAP directory. Users created in this way are local users, and are not added to your LDAP directory. For more information about synchronizing users with an LDAP directory, see Section 18.1, "Synchronizing Users and Groups from an LDAP Directory," on page 193.

To create a local Filr user:

1 Log in to Filr as the Filr administrator.

1a Launch a web browser.

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

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

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

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

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

3 In the **Management** section, click **Users**.

4 Click **New**.

The User page is displayed.

5 Provide the user's information in the User page, then click **OK**.

18.4 Listing Filr Users

On the Novell Filr site, you can view a comprehensive list of all the Filr users.

1 Log in to Filr as the Filr administrator.

    1a Launch a web browser.

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

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

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

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

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

3 In the **Management** section, click **Users**.

All users in the Filr site are displayed.

You can use this page in the following ways:

18.4.1 Filtering Users

You can filter the user list in the following ways: by specifying a name in the **Filter List** field in the upper-right corner.

- Specify a name in the **Filter List** field in the upper-right corner, then press Enter.

- Click the drop-down arrow next to the **Filter List** field, then select from the following options (by default, all options are selected):
  - **Show Internal Users:** Shows internal Filr users.
  - **Show External Users:** Shows external Filr users.
  - **Show Disabled Users:** Shows users that have been disabled.
  - **Show Enabled Users:** Shows users that are enabled.
  - **Show Administrators:** Shows users that have Administrative rights.
  - **Show Users That Are Not Administrators:** Shows users that do not have Administrative rights.

18.4.2 Navigating to a User's Individual Profile

You can use the user list to navigate to a user's individual profile.

1 In the user list, in the **Full Name** column, click the name of the user whose profile you want to navigate to, then click **Profile**.

For information about how to navigate to a user's My Files area, or any other area in Filr, see Chapter 21, "Managing Folders and Files," on page 231.

18.4.3 Adding Local Users

A local user is a Filr user who is not added to your LDAP directory. You can use the Users page to add new local users to your Filr site.

For information about how to add local users, see Section 18.3, "Creating a New Local User," on page 206.

18.5 Viewing User Properties

User properties show you important information about any user in your Filr system, such as profile, account, Home directory, data quota, sharing, and Net Folder information.

To view user properties:

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

    1a Launch a web browser.

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

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

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

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

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

3 Under **Settings**, click **Users**.

4 Click the drop-down arrow next to the user whose properties you want to view, then click **User Properties**.

18.6 Renaming a Filr User

Novell Filr users are identified by name (first, middle, last) and by user ID. User names are used to identify personal profiles. User IDs are used for logging in. You can change users' names, but not their user IDs. The way you change a user's name depends on how you created the user.

- Section 18.6.1, "Renaming a Filr User from LDAP," on page 209
- Section 18.6.2, "Renaming a Local Filr User," on page 209

18.6.1 Renaming a Filr User from LDAP

If you are synchronizing user information from an LDAP directory, as described in Section 18.1, "Synchronizing Users and Groups from an LDAP Directory," on page 193, you change a user's first, middle, or last name by updating it in the LDAP directory. The updated information then synchronizes to the Filr site according to the schedule you have established for LDAP synchronization. If you change a user's first, middle, or last name by updating information on the Filr site, the change is not synchronized back to the LDAP directory, so the two sources of user information can be out of sync.

18.6.2 Renaming a Local Filr User

If you manually create Filr users on the Filr site, rather than synchronizing user information from an LDAP directory, you can change users' names (first, middle, last) on the Filr site.

When a user logs in to the Filr site for the first time, the user's personal profile is created. Before a user logs in, he or she does not have a personal profile. Filr enables site administrators to manually rename both types of users.

- "Renaming Users Who Have Logged In to Filr" on page 209
- "Renaming Users Who Have Not Logged In to Filr" on page 210

NOTE: Filr does not allow you to change a user ID after the user account has been created.

Renaming Users Who Have Logged In to Filr

To rename a user who has previously logged in to the Filr site and therefore has a personal profile:

1 Navigate to the user's personal profile.

2 Click **Edit** on the Profile page.

The User page is displayed.

3 Modify the **First Name**, **Middle Name**, and **Last Name** fields as desired.

4 Click **OK**.

Renaming Users Who Have Not Logged In to Filr

To rename a user who has not previously logged in to the Filr site and therefore does not have a personal profile:

1 Click the User List icon ![icon] in the masthead.

2 Click the name of the user who you want to rename, then click **Modify**.

The User page is displayed

3 Modify the **First Name**, **Middle Name**, and **Last Name** fields as desired.

4 Click **OK**.

18.7 Deleting a Filr User

When users no longer need access to your Novell Filr site, you have two options to revoke their access to the Filr site: disabling or deleting their Filr user accounts.

IMPORTANT: Novell recommends that you disable user accounts instead of deleting them. When you delete a user account, the account can never be re-activated. If there is the slightest possibility that the user might return to your Filr site, disable the user account rather than delete it. Disabled accounts do not count as a licensed user. For information on how to disable a user, see Section 18.8, "Disabling Filr User Accounts," on page 213.

The you delete a user depends on how you originally created the user:

- Section 18.7.1, "Deleting a Local User," on page 210
- Section 18.7.2, "Deleting an LDAP User," on page 212
- Section 18.7.3, "Recovering User Workspaces from the Trash," on page 213

18.7.1 Deleting a Local User

Any user account that has been created manually (not created by the LDAP synchronization process) can be deleted as described in this section. To delete a user account that was created by the LDAP synchronization process, see Section 18.7.2, "Deleting an LDAP User," on page 212.

Users must have logged in to the Filr site at least one time in order to delete the user workspace. However, you can delete the user object in conjunction with the user workspace at any time (users do not need to have logged in).

IMPORTANT: If you delete user accounts that were created by the LDAP synchronization process without following the instructions in Section 18.7.2, "Deleting an LDAP User," on page 212, new users with the same name are created the next time the users log in or the next time the LDAP synchronization occurs.

When deleting local users, you should be familiar with the following terms:

User Workspaces: User workspaces are a physical location in the Filr system where information related to the user is stored. When a user's workspace is deleted, all information within the user's My Files area is deleted. The user, however, can still access the Filr system.

User Object: User objects refer to the actual user in the Filr system. When a user object is deleted, the user's profile is deleted, and the user cannot access the Filr system.

When you delete a **user object**, the following user information is deleted and cannot be recovered:

- All profile information, including profile pictures (User Object)
- Access controls to workspaces and folders (User Object)

When you delete a **user workspace**, the following user information is deleted and cannot be recovered:

- Files added to the user's Personal Storage area (User Workspace)
- Shares made to other users from the Personal Storage area (User Workspace)

To delete local users (the user workspace only or the user workspace and the user account):

1 Log in to Filr as the Filr administrator.

   1a Launch a web browser.

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

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

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

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

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

3 In the **Management** section, click **Users**.

4 Select the users whose accounts you want to delete, then click **Delete**.

The Delete Users dialog box is displayed.

Depending on whether users who are being deleted have Home folders, you can select from the following options:

If users being deleted do not have Home folders, the following options are displayed:

- **Move user workspaces to trash:** Moves user workspaces to the trash. Does not delete the user objects. You can restore the user workspaces from the trash, as described in .

- **Delete user workspaces:** Does not delete the user objects, but deletes the user workspaces. The user workspaces cannot be restored. If the user logs back in, a new workspace is created as if the user is new to the Filr system.

  - **Delete user objects:** Deletes the user objects and the user workspaces from the Filr system. The users no longer exist in the Filr system and cannot log in. Neither the user objects nor the user workspaces can be restored.

If all users being deleted have Home folders, the following option is displayed:

- **Delete all selected user objects:** Deletes the user objects and the user workspaces from the Filr system. The users no longer exist in the Filr system and cannot log in. Neither the user objects nor the user workspaces can be restored. If the user logs back in to Filr, a new workspace is created as if the user is new to the Filr system.

If some users being deleted have Home folders and others do not, the following options are displayed:

- ◆ **Move local user workspaces with only Personal Storage to the trash and delete others:** Moves user workspaces that contain no Home folder to the trash. Deletes user workspaces that do contain a Home folder. Does not delete the user objects. You can restore user workspaces that were moved to the trash, as described in Section 18.7.3, "Recovering User Workspaces from the Trash," on page 213.

  - ◆ **Delete user objects whose workspaces are deleted:** Deletes the user objects that are associated with the user workspaces that are being deleted. The users no longer exist in the Filr system and cannot log in. Neither the user objects nor the user workspaces can be restored.

- ◆ **Delete all user workspaces:** Deletes all user workspaces, regardless of whether user workspaces contain a Home folder. Does not delete the user objects. The user workspaces cannot be restored. If the user logs back in, a new workspace is created as if the user is new to the Filr system.

  - ◆ **Delete user objects:** Deletes the user objects and the user workspaces from the Filr system. The users no longer exist in the Filr system and cannot log in. Neither the user objects nor the user workspaces can be restored.

5 Click **Yes** to confirm the deletion.

18.7.2 Deleting an LDAP User

User accounts can be synchronized to the Filr site with an LDAP directory. Although you can delete Filr user accounts, Novell recommends that you disable them, as described in Section 18.8, "Disabling Filr User Accounts," on page 213.

If you decide to delete Filr user accounts, it is safer to manually delete than to delete them through the LDAP synchronization process. Because user accounts that are deleted cannot be recovered, ensure that you know exactly which users you are deleting; the only way to be sure is to manually delete them.

- ◆ "Manually Deleting User Accounts That Are Being Synchronized through LDAP" on page 212
- ◆ "Configuring LDAP to Automatically Delete User Accounts" on page 213

Manually Deleting User Accounts That Are Being Synchronized through LDAP

The following method is preferred for deleting user accounts from the Filr site if the accounts are being synchronized from an LDAP directory:

1 In your LDAP directory, modify the User objects that you want to delete from the Filr site so that the User objects no longer match the LDAP synchronization criteria that you previously set.

For information about setting LDAP synchronization criteria, see Section 18.1, "Synchronizing Users and Groups from an LDAP Directory," on page 193.

2 In Filr, manually delete the user accounts, as described in Section 18.7.1, "Deleting a Local User," on page 210.

Configuring LDAP to Automatically Delete User Accounts

IMPORTANT: Although it is possible to configure LDAP synchronization to automatically delete Filr users and workspaces, this should be avoided because it might result in unwanted deletion of users. For example, if the LDAP context is entered incorrectly and none of the users match the incorrect LDAP context, all of the users are permanently deleted.

For more information about how to configure the LDAP synchronization to automatically delete Filr users and workspaces, see "For user accounts provisioned from LDAP that are no longer in LDAP:" on page 203.

18.7.3 Recovering User Workspaces from the Trash

If you have deleted user workspaces, you can restore the workspaces from the trash.

IMPORTANT: It is not possible to restore user objects that have been deleted. This section describes how to restore user workspaces. The process for deleting user workspaces and/or user objects is described in Section 18.7.1, "Deleting a Local User," on page 210.

1 Log in to Filr as the Filr administrator.

   1a Launch a web browser.

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

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

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

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

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

3 In the **Management** section, click **Users**.

4 Click the **Trash** icon , located in the upper-right corner of the page.

5 Select the user's workpsace and My Files Storage folder (if applicable) that you want to restore, then click **Restore**.

18.8 Disabling Filr User Accounts

Novell recommends that you disable user accounts instead of deleting them. When you delete a user account, the account can never be re-activated. If there is the slightest possibility that the user might return to your Filr site, disable the user account rather than delete it.

Disabled accounts do not count as a licensed user.

The way to disable a user account differs depending on whether the user was created in Filr or in an LDAP directory and then synchronized to Filr.

- Section 18.8.1, "Disabling a Local User Account," on page 214
- Section 18.8.2, "Disabling an LDAP User Account," on page 215

18.8.1 Disabling a Local User Account

1 Log in to Filr as the Filr administrator.

   1a Launch a web browser.

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

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

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

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

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

3 In the **Management** section, click **Users**.

4 Select the user accounts that you want to disable, then click **More** > **Disable**.

Names of disabled users are displayed in grey.

To enable local user accounts after they have been disabled:

1 Log in to Filr as the Filr administrator.

   1a Launch a web browser.

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

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

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

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

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

3 In the **Management** section, click **Users**.

4 Select the user accounts that you want to enable, then click **More** > **Enable**.

18.8.2 Disabling an LDAP User Account

If users are being synchronized from an LDAP directory, you must disable the accounts directly from the LDAP directory. User accounts that are disabled in the LDAP directory are disabled in Filr at the next LDAP synchronization.

For more information about LDAP synchronization in Filr, see Section 18.1, "Synchronizing Users and Groups from an LDAP Directory," on page 193.

18.9 Limiting User Visibility

Path to Configuration Page: Filr Administration Console > **Management** > **Limit 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.

- Section 18.9.1, "User-Visibility Is Either Restricted or Not," on page 215
- Section 18.9.2, "How User-Visibility Limitations Work," on page 215
- Section 18.9.3, "Creating User Visibility Limitations," on page 220

18.9.1 User-Visibility Is Either Restricted or Not

From a user-visibility standpoint, there are only two conditions:

Limited Visibility: A user account has a user-visibility limitation applied; therefore, the user can see only other members of the groups it belongs to.

Unlimited Visibility: Either the user's account has no user-visibility limitation applied, or an override is in place. In both cases, the user can see all other users on the system.

NOTE: Group visibility cannot be restricted; all groups are visible to all users.

18.9.2 How User-Visibility Limitations Work

1. In the default state, there are no user-visibility limitations in Filr.

No User-Visibility Limitations

By default, all Filr users can see and collaborate with all other Filr users.

| User A | User B | User C |

| User D | User E | User X |
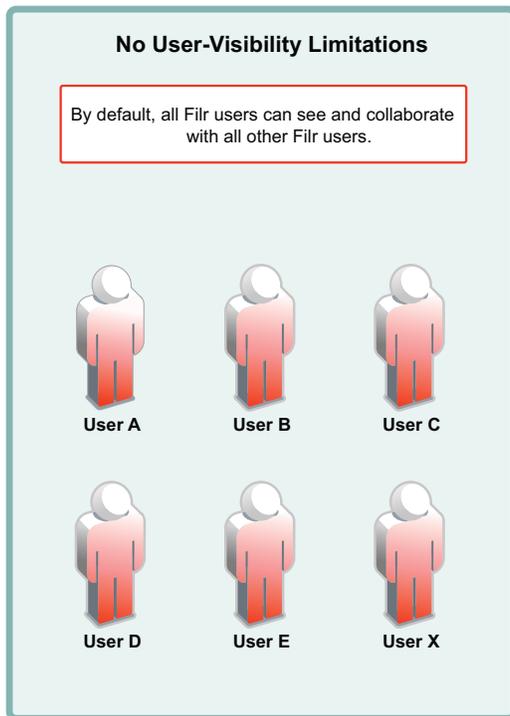
2. User-visibility functionality relies on group membership.

   In the figure below

   - ◆ Group A contains User A
   - ◆ Group B contains User A and User B.
   - ◆ Group C contains User C and User X.
   - ◆ Users D and E are not members of a group.

User-Visibility Limitations Leverage Group Membership

User-visibility limitations require that those being limited are members of one or more groups.

Group A   Group B   Group C

User A   User B   User C   User X

User D   User E
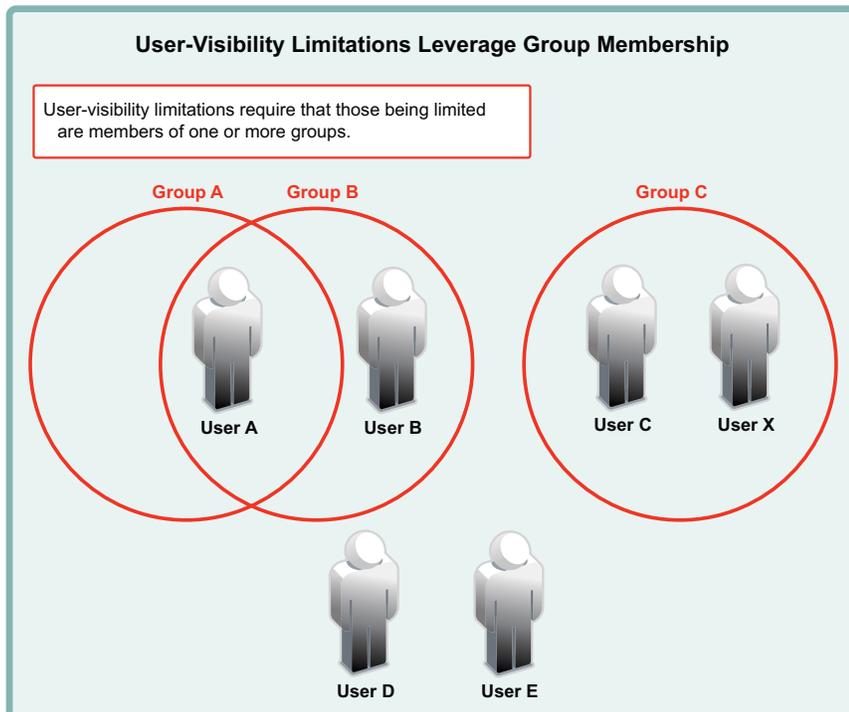
3. Filr admins apply user-visibility limitations to groups. Users within the affected groups can then only see other members of the groups that they belong to.

   For example, after a user-visibility limitation is applied to Group A, User A can only see User B. (User B's ability to see other users is not affected because User B is not in Group A.)

A User-Visibility Limitation on Group A Applies to Only User A

User A can only see users in the groups that it belongs to--User B in this case.

Group A	Group B		Group C	
User A	User B		User C	User X

User D   User E
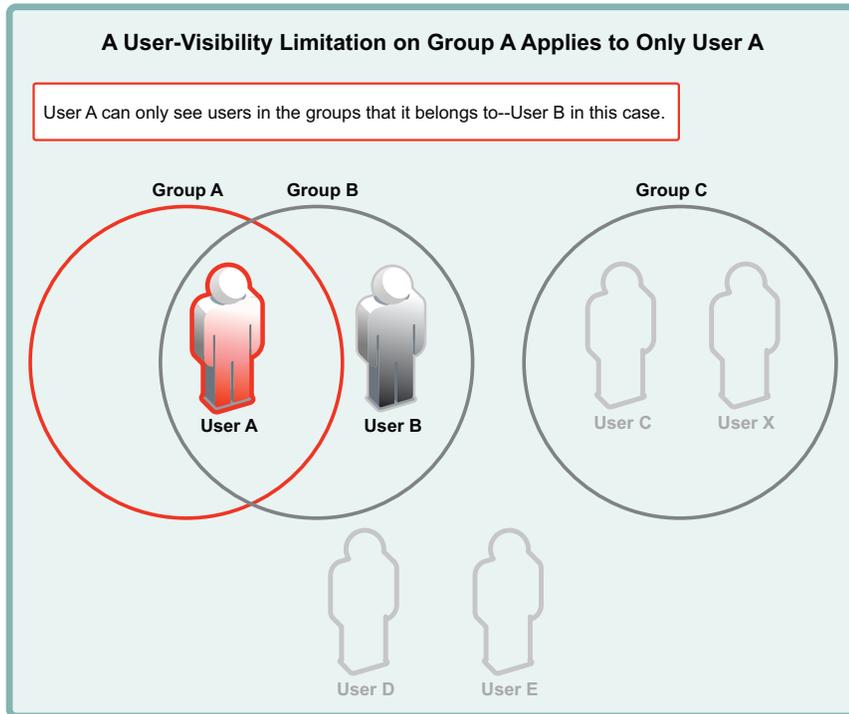
4. You cannot restrict group visibility.

User-Visibility Limitations Don't Block Group Visibility

User A can see Group C but not who is in Group C.

Group A	Group B		Group C	
User A	User B		User C	User X

User D   User E
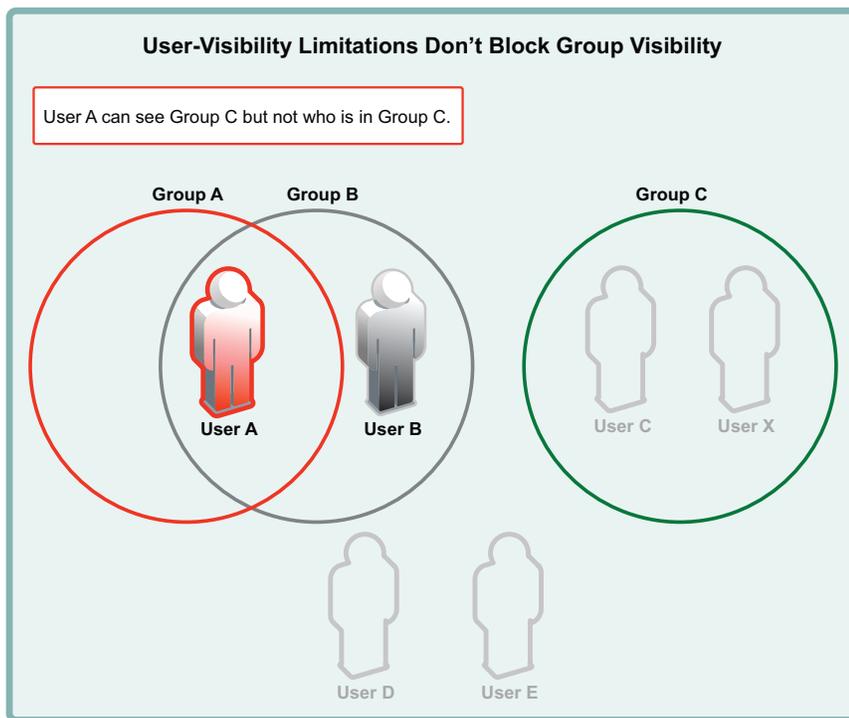
5. You can apply user-visibility limitations to individual users.

   For example, an administrator might restrict User C rather than Group C. User C could then only see User X. (User X, on the other hand, could still see all users on the system.)

User-Visibility Limitations Can be Directly Applied to Users

User C can only see User X. (User X can still see everyone.)

Group A   Group B   Group C

User A   User B   User C   User X

User D   User E
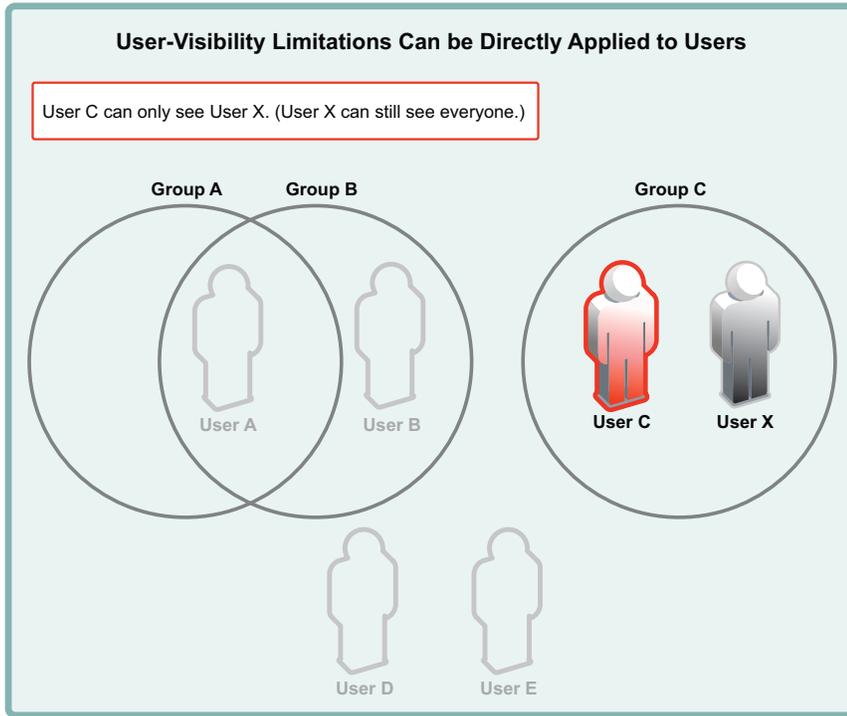
6. A user with user-visibility limitations applied who is not a member of a group, cannot see any other users on the system. Of course, the user can still see all groups, but not being able to see user comments, etc. inhibits effective collaboration through Filr.

Limiting a Non-Group Member Severly Limits Collaboration

Limiting User D's Visibility hides all other users.

Group A   Group B   Group C

User A   User B   User C   User X

User D   User E
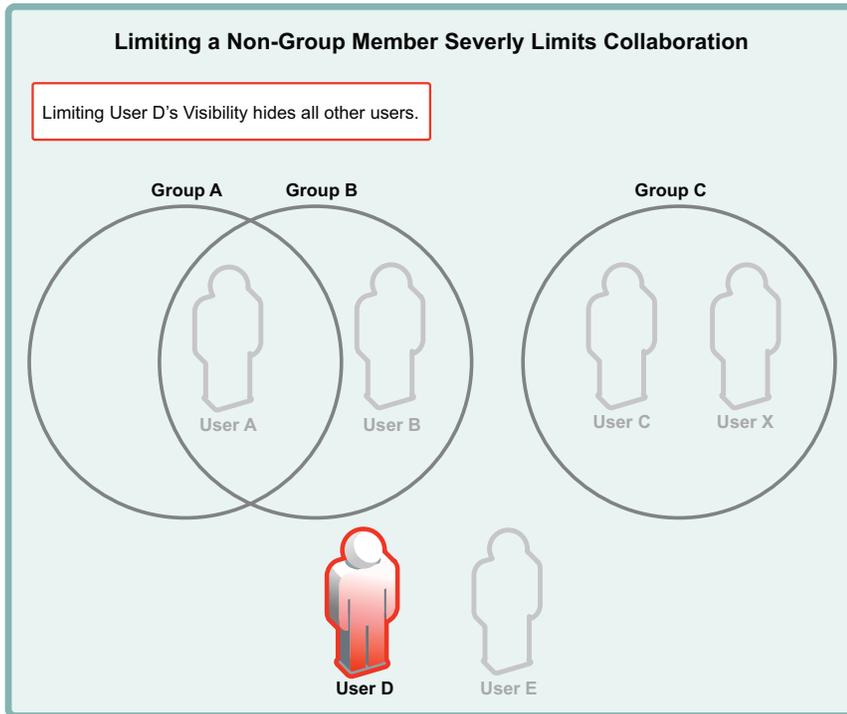
7. Adding a user to a group immediately applies the group's visibility limitations.

   For example, if User E is added to Group A, its user-visibility is immediately limited to seeing only User A.

Adding a User to a Group Applies the Limitations Set on the Group

After User E is added to Group A, it can only see User A.

Group A   Group B

User E   User A   User B

Group C

User C   User X

User D
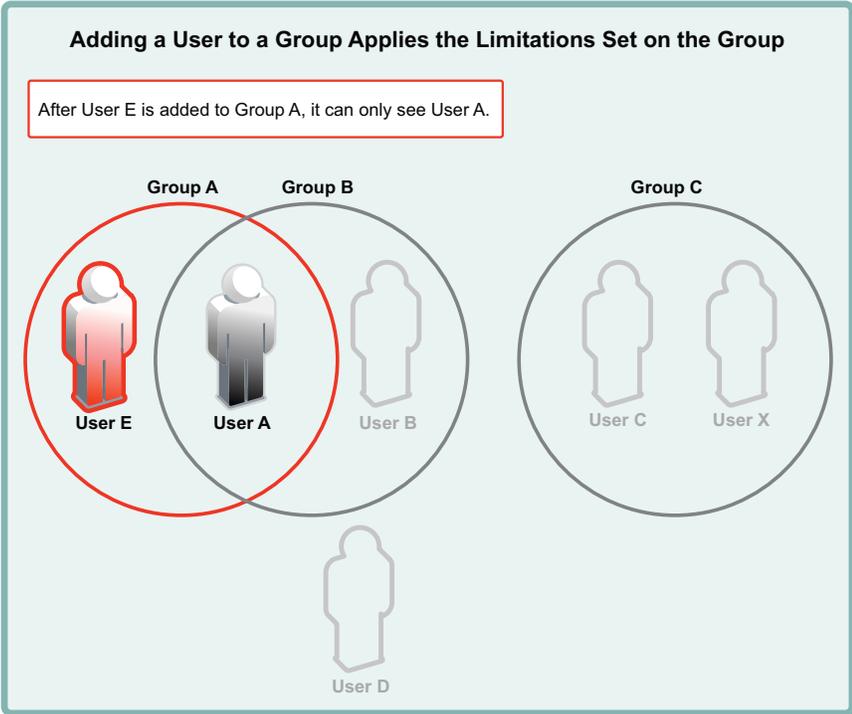
8. Applying an override to a user account lifts all user-visibility limitations from that user account.

Limitations Can Be Overridden

After an override is applied to its user account, User A can see all other users.

Group A   Group B

User E   User A   User B

Group C

User C   User X

User D
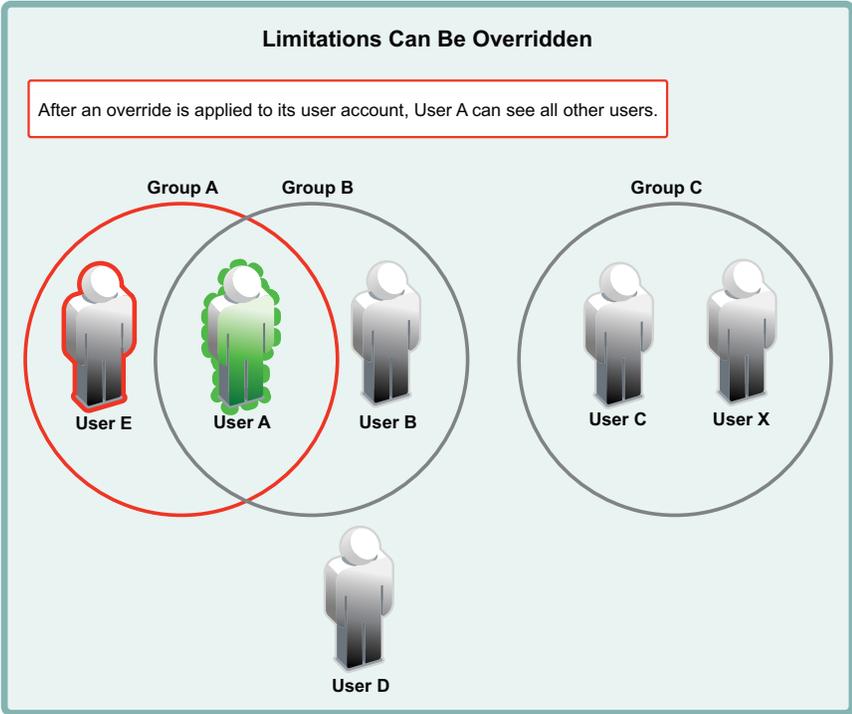
9. Applying new user-visibility limitations doesn't affect overrides. User B is now restricted, but User A can still see all other users.

New Limitations Don't Affect Overrides

With an override in place, User A is unaffected by a new limitation on Group B. (Of course, User B can now see only User A.)

Group A   Group B   Group C

User E   User A   User B   User C   User X

User D
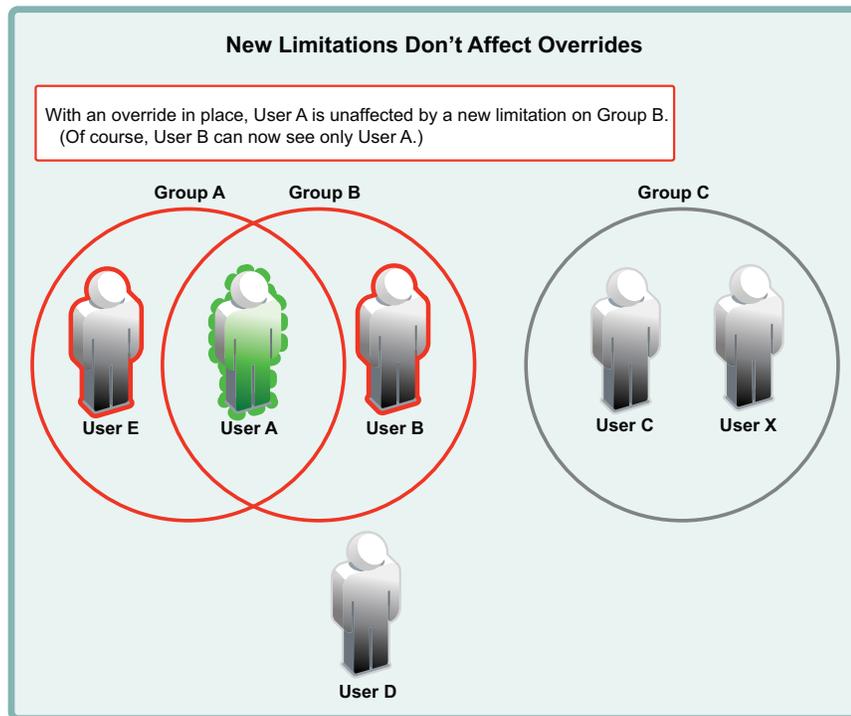
18.9.3 Creating User Visibility Limitations

For administrative efficiency and as a best practice, user-visibility limitations are usually applied to one or more groups.

Most organization choose to limit visibility at the group level and then manage exceptions by creating overrides for individual users. However, limitations can be applied to individual users if needed.

1   After reading the previous sections, identify the groups whose users require and/or will benefit from having user-visibility limitations set.

2   Identify group users who will need to be able to collaborate and share on a system-wide basis and will therefore need overrides.

3   Log in as a Filr administrator, open the Filr Administration Console > **Management** > **Limit User Visibility**.

4   Use the **Add Limitation** button to add user-visibility limitations to the groups (or users) identified.

5   Use the **Add Override** as needed.

6   If you need to remove a limitation, select the line to be removed and use the **Remove Visibility Settings** button to remove the setting from the list.

18.10 Adding or Removing Administrator Rights for a User

As described in Section 3.3, "Creating Additional Filr Administrators," on page 53, you can grant administrative privileges to a user.

To add or remove administrator rights to a user on the Manage Users page:

1 Select the users for whom you want to add or remove administrator rights.

2 Click **More** > **Add Administrator Rights** or **Remove Administrator Rights**.

18.11 Managing Local Users and Groups by Importing Profile Files

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 when you are not using LDAP.

You can perform the following actions:

 • Create or modify users
 • Delete users
 • Create or modify groups

To manage local users and groups by importing profile files:

1 Log in to Filr as the Filr administrator.

    1a Launch a web browser.

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

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

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

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

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

3 In the **Management** section, click **Users**.

4 Click **Import Profiles**.

5 Click **Choose File**, then navigate to and select the file that contains user or group profile information in XML format.

Ensure that the format of your file matches the format that is shown in the provided sample file. To view the provided sample file, click **View a Sample File** in the **Import Files** tab.

6 Click **OK**.

18.12 Understanding the XSS Security Filter

Cross-site scripting (XSS) is a client-side computer attack that is aimed at Web applications. Because XSS attacks can pose a major security threat, Novell Filr contains a built-in security filter that protects against XSS vulnerabilities.

The XSS security filter protects the Filr site from XSS in two key areas:

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

18.13 Modifying the Title of the People Page

Filr enables you to modify the name of the People page. (This is an alternate way of viewing users in your Filr system.) This name is displayed when navigating the Workspace tree (as described in Section 21.1, "Navigating the Workspace Tree," on page 231) and when performing a search.

1 Click the People icon in the masthead.

2 Click the Configure icon next to the folder name, then click **Rename Workspace**.

3 In the **New Name** field, specify a new name for the workspace, then click **OK**.

19 Managing Groups

Creating groups is a useful way to manage and maintain users throughout your Filr site. For more information about why it is important to create groups, see Chapter 9, "Creating Groups of Users," on page 115.

- Section 19.1, "Creating Groups," on page 223
- Section 19.2, "Modifying Groups," on page 223
- Section 19.3, "Deleting Groups," on page 224
- Section 19.4, "Adding or Removing Administrator Rights for a Group," on page 225
- Section 19.5, "Managing How Group Names Are Displayed during Name Completion," on page 225

19.1 Creating Groups

For information on how to create groups, see Chapter 9, "Creating Groups of Users," on page 115.

19.2 Modifying Groups

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

　1a Launch a web browser.

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

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

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

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

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

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

4 Click the name of the group that you want to modify.

5 Modify the title, description, and group membership, then click **OK**.

For more information about editing static and dynamic group membership, see Chapter 9, "Creating Groups of Users," on page 115.

19.3 Deleting Groups

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

   1a Launch a web browser.

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

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

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

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

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

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

4 Select the group that you want to delete, then click **Delete**.

19.4 Adding or Removing Administrator Rights for a Group

As described in Section 3.3, "Creating Additional Filr Administrators," on page 53, you can grant administrative privileges to a group.

To add or remove administrator rights to a group on the Manage Groups page:

1 Select the groups for which you want to add or remove administrator rights.

2 Click **More** > **Add Administrator Rights** or **Remove Administrator Rights**.

19.5 Managing How Group Names Are Displayed during Name Completion

Certain fields throughout the Filr site employ name completion (or Type-to-Find) functionality. For example, when you share an item in Filr and you begin typing the name of a user or group in the **Share with field**, names of users or groups that match what you have typed so far appear in a drop-down list.

In the Type-to-Find drop-down list, Filr includes the group name or group title, as well as secondary information about the group (either the group description or the Fully Qualified DN). This secondary information helps distinguish between multiple groups that have the same name.

Filr allows you to determine the way group names are displayed in this Type-to-Find drop-down list.

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

    1a Launch a web browser.

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

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

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

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

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

3 Under **System**, click **Name Completion Settings**.

The following options are available:

Primary display text: Select **Name** or **Title**. Name represents the name of the group as it appears in Filr. Title represents the title as it appears in the LDAP directory.

Secondary display text: Select **Description** or **Fully Qualified DN**. Description represents the description of the group as it appears in Filr. Fully Qualified DN represents the Fully Qualified Domain Name as it appears in the LDAP directory.

4 Click **OK**.

20 Managing Mobile Devices

Filr provides native mobile device management functionality, directly from the Filr Administration Console.

You can perform the following tasks:

- Section 20.1, "Viewing Device Information," on page 227
- Section 20.2, "Wiping All Data from a Device," on page 228
- Section 20.3, "Deleting a Mobile Device," on page 228

20.1 Viewing Device Information

You can view all devices (and device owners) that have accessed your Filr system, as well as valuable information about the device and login history.

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

   1a Launch a web browser.

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

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

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

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

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

3 To view all mobile devices in the Filr system, under **Management**, click **Mobile Devices**.

   The Manage Mobile Devices page is displayed.

   or

   To view all mobile devices belonging to a specific user, under **Management**, click **Users**, then click the icon in the mobile device column 1 (the number in the icon represents the number of devices that belong to the user).

   The following information is displayed about each mobile device that has accessed the Filr system:

- **Description:** The name given to the device by the device owner, the type of device (such as iPhone), and the operating system on the device.
- **User:** The name of the Filr user who owns the device.
- **Last login:** The date and time when the device was last used to log in to the Filr system.

- **Wipe scheduled:** Whether a wipe has been scheduled to occur to remove all Filr data from the device.
- **Last wipe:** The last time Filr data was wiped from the device.

20.2 Wiping All Data from a Device

You might want to wipe all Filr data from a device in the even that it is lost or stolen.

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

1a Launch a web browser.

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

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

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

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

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

3 To view all mobile devices in the Filr system, under **Management**, click **Mobile Devices**.

The Manage Mobile Devices page is displayed.

or

To view all mobile devices belonging to a specific user, under **Management**, click **Users**, then click the icon in the mobile device column 1 (the number in the icon represents the number of devices that belong to the user).

4 Select the mobile device that you want to wipe, then click **Wipe** > **Schedule Devices to be Wiped**.

The device will be wiped at the next synchronization (by default, synchronization occurs every 15 minutes). You can change the synchronization schedule as described in Section 13.1, "Configuring Mobile Device Access for All Users," on page 151.

5 (Optional) To cancel the wipe from taking place, click **Yes** in the **Wipe scheduled** column.

20.3 Deleting a Mobile Device

You can delete a mobile device so that it is no longer displayed on the Manage Mobile Devices page. (The app is still available on the device.) If the device accesses the Filr site again, the device is re-added to the Manage Mobile Devices page.

IMPORTANT: If the device was lost or stolen, you should wipe the device before deleting it (as described in Section 20.2, "Wiping All Data from a Device," on page 228), because deleting a device does not cause the Filr data to be removed from the device.

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

    1a Launch a web browser.

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

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

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

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

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

3 To view all mobile devices in the Filr system, under **Management**, click **Mobile Devices**.

The Manage Mobile Devices page is displayed.

or

To view all mobile devices belonging to a specific user, under **Management**, click **Users**, then click the icon in the mobile device column `1` (the number in the icon represents the number of devices that belong to the user).

4 Select the mobile device that you want to delete, then click **Delete** > **Yes**.

21 Managing Folders and Files

As an administrator for Novell Filr, you can perform management functions on all Filr folders. For information on how to perform general folder management functions, such as creating a folder, deleting a folder, moving a folder, and so forth, see "Managing and Using Folders" in the *Filr 2.0: Web Application User Guide*.

You can perform additional folder management tasks as the Filr administrator:

21.1 Navigating the Workspace Tree

You can use the Workspace Tree to navigate to any location on the Filr site. The Workspace Tree displays the path of all of the workspaces and folders that contain the place you are currently viewing, without leaving the current page.

This is the only way to navigate to another user's My Files area.

Only the Filr administrator has access to the Workspace Tree.

1 Click the **Workspace Tree** icon ![workspace tree icon] in the upper-left corner of any Filr page.

2 Navigate to and click the linked name of the desired location in the Workspace Tree.

3 (Optional) To navigate to a user's My Files area, click a folder within that user's personal workspace.

21.2 Managing Workspace Disk Space Usage

Disk space usage is managed on a folder basis as well as on an individual user or group basis.

For more information, see Chapter 22, "Managing Disk Space Usage with Data Quotas and File Restrictions," on page 233.

21.3 Restoring Files and Folders from the Trash

You can view all items that have been sent to the trash and restore them to their previous location.

IMPORTANT: Only items from a user's My Files area (Personal Storage) that were moved to the trash are able to be restored from the trash. Items that were permanently deleted from a user's My Files area cannot be restored. Items deleted from a Net Folder are never sent to the trash, and cannot be restored.

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

   1a Launch a web browser.

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

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

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

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

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

3 Under **Management**, click **Users**.

   The Manage Users page is displayed.

4 Click the **Trash** icon 🗑, located in the upper-right corner of the page.

5 Select the items that you want to restore, then click **Restore**.

22 Managing Disk Space Usage with Data Quotas and File Restrictions

As time passes, your Novell Filr site occupies more and more disk space as users post files. As the Filr administrator, you can impose limits on the amount of data that is uploaded into the Filr site.

Only files count toward the data quota. Folders that do not contain files do not count toward the data quota. Files that are located in Net Folders do not count toward the data quota.

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

22.1 Understanding Data Quota Behavior and Exclusions

22.1.1 Understanding Default Data Quota Behavior

The following sections describe the default behavior for how user data quotas work after they have been enabled.

Exceeding the Data Quota

Filr users are strictly held to the data quota that you set. If a user who is approaching his or her data quota tries to upload a file to the Filr site and that file exceeds the user's data quota, Filr rejects the upload attempt and the entry is lost. This is also true with data quotas that are set on folders.

Exceeding the High-Water Mark

When a user exceeds the data quota high-water mark, a warning message is displayed on the user's profile page informing the user that he or she is approaching the data quota. Filr displays how many kilobytes of disk space are still available.

For more information on selecting an appropriate high-water mark, see "Selecting an Appropriate High-Water Mark" on page 235.

22.1.2 Understanding Data Quota Exclusions

Files that are located in Net Folders do not count against data quotas because they are not uploaded into the Filr site. Only files in users' Personal Storage count against data quota.

Folders that do not contain files do not count toward the data quota.

22.2 Managing User Data Quotas

Each user's data quota establishes how much disk space the user's files can occupy in the Filr site. Folders that do not contain files do not count toward a user's data quota.

By default, users are not limited in the disk space that their files occupy in the Filr site. As the Filr administrator, you can decide when limiting users' disk space usage becomes appropriate.

- Section 22.2.1, "Planning User Data Quotas," on page 234
- Section 22.2.2, "Setting User Data Quotas," on page 236
- Section 22.2.3, "Modifying User Data Quotas," on page 239
- Section 22.2.4, "Removing User Data Quotas," on page 242
- Section 22.2.5, "Repairing a User's Data Quota," on page 244
- Section 22.2.6, "Managing Your Personal Data Quota," on page 245
- Section 22.2.7, "Monitoring User Data Quotas," on page 245

22.2.1 Planning User Data Quotas

- "Understanding User Data Quota Priority" on page 234
- "Selecting the Default User Data Quota for All Users" on page 235
- "Selecting an Appropriate High-Water Mark" on page 235
- "Determining Data Quotas for Specific Users" on page 235
- "Determining Data Quotas for Specific Groups" on page 235

Understanding User Data Quota Priority

Because users can have multiple data quotas assigned to them (either individually, through group membership, or through the site-wide default), Filr prioritizes the existing data quotas and uses only one for each individual Filr user. If users have multiple data quotas that pertain to them, the priority level is as follows:

1. **User Quota:** A quota that is set for an individual user overrides the site-wide default quota and any other quotas that are associated with any groups where the user is a member.
2. **Group Quota:** A quota that is set for an individual group overrides the site-wide default quota. This pertains to all users who are members of that group.

   When a user is a member of multiple groups that have data quotas associated with them, the user is given the highest data quota. For example, if a Filr user is a member of Group A, Group B, and Group C, and the data quotas for each of these groups is 10, 20, and 30, the Filr user's data quota is 30.
3. **Site-Wide Default:** The site-wide default quota is used for all Filr users who have not been assigned individual quotas, and who are not associated with any groups where a quota has been set.

Selecting the Default User Data Quota for All Users

When you enable the data quota feature, the initial default data quota is 100 MB. This means that each Filr user can upload 100 MB of files and attachments to the Filr site.

When you select the default data quota for your Filr site, consider the size of your Filr site, the number of Filr users, the amount of available disk space, and so on. You can override the default data quota on a per-user and per-group basis, as described in Section 22.2.2, "Setting User Data Quotas," on page 236.

As described in "Exceeding the Data Quota" on page 233, when a user adds enough files and attachments to exceed the data quota, the user can no longer attach files or create versions until existing files have been deleted and purged to free up storage space.

For information about purging deleted files to make storage space available, see Section 22.3.1, "Permanently Deleting Files from the Trash," on page 245.

For information about which data quota is used when users have multiple data quotas that pertain to them, see "Understanding User Data Quota Priority" on page 234.

Selecting an Appropriate High-Water Mark

The high-water mark is the percentage of the data quota that must be reached before the user is made aware that he or she is approaching the data quota (a warning message is displayed on the user's profile page). The default high-water mark is 90% of a user's data quota.

This high-water mark also applies to data quotas that are set on workspaces and folders.

Determining Data Quotas for Specific Users

If there is a user in your Filr site who needs either a higher or lower data quota than the site-wide default, you can assign that user an individual user data quota.

When you set data quotas for specific users, remember that individual user data quotas override the default user data quota, as well as quotas that are assigned to any groups where the user is a member, as described in "Understanding User Data Quota Priority" on page 234.

Determining Data Quotas for Specific Groups

When you set data quotas for specific groups, remember that group data quotas override the default site-wide data quota, but do not override individual user quotas, as described in "Understanding User Data Quota Priority" on page 234.

22.2.2 Setting User Data Quotas

You can set data quotas for the entire Filr site, for individual groups, and for individual users.

- "Setting a Default Data Quota" on page 236
- "Setting Data Quotas for Individual Groups" on page 237
- "Setting Data Quotas for Individual Users" on page 238

Setting a Default Data Quota

When you set a default data quota, the quota applies to all Filr users who have not been assigned individual quotas, and who are not associated with any groups where a quota has been set.

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

    1a Launch a web browser.

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

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

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

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

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

3 Under **Management**, click **Personal Storage**.

4 Select **Enable User Data Quotas**.

5 Set the **Default User Data Quota Size** and **Default High-Water Mark** options as determined in Section 22.2.1, "Planning User Data Quotas," on page 234.

6 Click **Apply** > **Close** to save the user data quota settings.

Setting Data Quotas for Individual Groups

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

    1a Launch a web browser.

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

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

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

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

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

3 Under **Management**, click **Personal Storage Quotas**.

4 Select **Enable User Data Quotas**.

5 Click **Add a Group**.

6 In the **Group** field, start typing the name of the group for which you want to set a quota, then click the group name when it appears in the drop-down list.

Repeat this process to add additional groups for which you want to assign the same data quota.

7 In the **Quota** field, specify the disk space limit for the group.

8 Click **OK**, then click **Apply** > **Close** to save the user data quota settings.
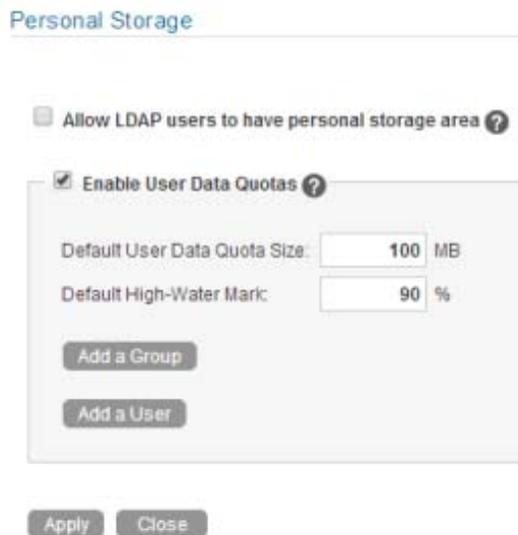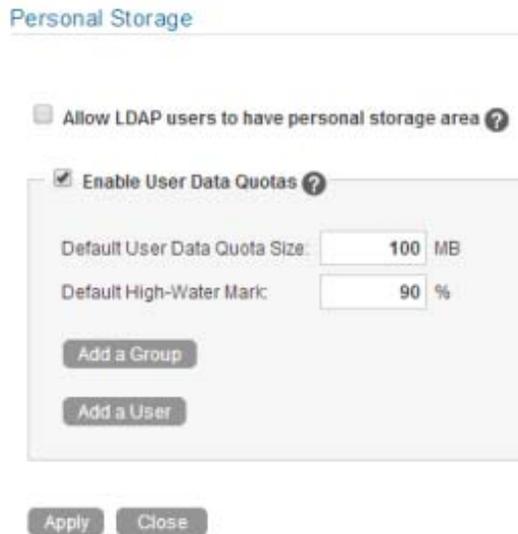
Setting Data Quotas for Individual Users

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

   1a Launch a web browser.

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

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

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

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

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

3 Under **Management**, click **Personal Storage Quotas**.

4 Select **Enable User Data Quotas**.

5 Click **Add a User**.

6 In the **User** field, start typing the name of the user for which you want to set a quota, then click the user's name when it appears in the drop-down list.

Repeat this process to add additional users for which you want to assign the same data quota.

7 In the **Quota** field, specify the disk space limit for the user.

8 Click **OK**, then click **Apply** > **Close** to save the user data quota settings.

22.2.3 Modifying User Data Quotas

Filr enables you to modify data quotas that you have previously set. You can modify data quotas for your entire Filr site, or modify data quotas for individual groups and users.

Modifying User Data Quotas for the Entire Filr Site

Filr enables you to easily modify the site-wide default user data quota.

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

    1a Launch a web browser.

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

```
http://Filr_hostname:8080
https://Filr_hostname:8443
```
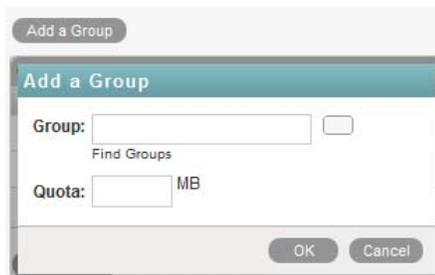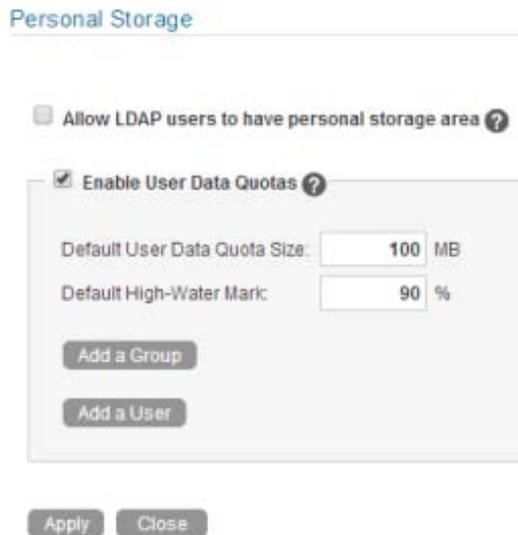
       Replace `Filr_hostname` with the host name or fully qualified domain name of the Filr server that you have set up in DNS.

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

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

3 Under **Management**, click **Personal Storage Quotas**.

4 In the **Default User Data Quota Size** field, delete the existing quota and specify the new quota.

You can also modify the default high-water mark in the **Default High-Water Mark** field. For more information about the high-water mark, see "Selecting an Appropriate High-Water Mark" on page 235.

5 Click **Apply** > **Close** to save the user data quota settings.

Modifying User Data Quotas for Individual Groups and Users

Filr enables you to easily modify individual group and user data quota settings that you have previously set.

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

   1a Launch a web browser.

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

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

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

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

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

3 Under **Management**, click **Personal Storage Quotas**.

4 In the **Group Quotas** table or **User Quotas** table, click the group name or user name that represents the group or user whose quota you want to modify.

5 In the **Quota** field, delete the existing quota and specify a new quota.

6 Click **OK**, then click **Apply** > **Close** to save the user data quota settings.

22.2.4 Removing User Data Quotas

Filr enables you to disable data quotas that you have previously set. You can disable data quotas for your entire Filr site, or remove data quotas from individual groups and users.

- "Disabling User Data Quotas for the Entire Filr Site" on page 242
- "Removing User Data Quotas from Individual Groups and Users" on page 243

Disabling User Data Quotas for the Entire Filr Site

If you decide that you no longer need to impose limits on the amount of data that users are permitted to upload into the Filr site, you can disable the data quota feature. Disabling the data quota feature enables all Filr users to upload as much data to the Filr site as they want.

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

    1a Launch a web browser.

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

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

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

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

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

3 Under **Management**, click **Personal Storage Quotas**.

    The Data Quotas and File Upload Limits page is displayed.

4 Deselect **Enable User Data Quotas**, then click **Apply**.

Personal Storage

☐ Allow LDAP users to have personal storage area ❔

☐ Enable User Data Quotas ❔

Default User Data Quota Size: [100] MB
Default High-Water Mark: [90] %

[Add a Group]

Group Quotas

Delete	Group Name	Group Title	Quota
☐	marketing	Marketing	200
☐	sales	Sales	250

[Delete]

[Add a User]

User Quotas

Delete	Full Name	User Id	Quota	Data Quota Used
☐	Anita Olivos	aolivos	175	0
☐	Julio Chavez	jchavez	150	0

[Delete]

Data quotas are not enabled.

[Apply] [Close]

Data quotas are no longer enabled for your Filr site.

Removing User Data Quotas from Individual Groups and Users

You can remove data quotas that you have previously set for individual groups and users. Users are held to the site-wide data quota default setting if they do not have an individual quota defined for them and they are not members of any groups where a group quota has been assigned.

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

    1a Launch a web browser.

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

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

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

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

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

3 Under **Management**, click **Personal Storage Quotas**.

Personal Storage

☐ Allow LDAP users to have personal storage area ❓

☑ Enable User Data Quotas ❓

Default User Data Quota Size: [100] MB

Default High-Water Mark: [90] %

[Add a Group]

Group Quotas

Delete	Group Name	Group Title	Quota
☐	marketing	Marketing	200
☐	sales	Sales	250

[Delete]

[Add a User]

[Apply] [Close]

4 In the **Group Quotas** table or **User Quotas** table, select the check box next to the group or user whose quota you want to remove.

5 Click **Delete**, then click **Apply** > **Close** to save the user data quota settings.

22.2.5 Repairing a User's Data Quota

It is possible for a user's data quota calculation to become inaccurate if errors occur during processing that is related to a user's file handling. If this happens and a user's quota calculation is inaccurate, you can repair the data quota:

Repairing a User's Quota When an Individual Data Quota Is Set

You can repair a user's data quota when an individual data quota is set on the user.

1 Remove the data quota that is set on the user, as described in "Removing User Data Quotas from Individual Groups and Users" on page 243.

2 Set the data quota for the user again, as described in "Setting Data Quotas for Individual Users" on page 238.

Repairing a User's Quota When a Default or Group Data Quota Is Set

You can repair a user's data quota when a default data quota is set, or when a group data quota is set and the user is a member of the group.

1 Set an individual data quota for the affected user, as described in "Setting Data Quotas for Individual Users" on page 238.

2 Remove the individual data quota that you just set, as described in "Removing User Data Quotas from Individual Groups and Users" on page 243.

22.2.6 Managing Your Personal Data Quota

NOTE: As a Filr administrator, you are also held to a data quota if quotas are enabled. If you want to assign yourself a larger quota than the site-wide default, you can add an individual quota for yourself, as described in "Setting Data Quotas for Individual Users" on page 238.

All Filr users need to manage their personal data quotas. When you have a limited allocation of disk space, you need to be aware of the amount of disk space that you have available and how to make more disk space available as you approach your quota.

For information on how to accomplish these and other important tasks as you manage your data quota, see "Managing Your Data Quota" in the *Filr 2.0: Web Application User Guide*.

22.2.7 Monitoring User Data Quotas

You can monitor which users in the Filr site have exceeded or are close to exceeding their data quotas by generating the following reports:

- Section 28.2.2, "Data Quota Exceeded Report," on page 269
- Section 28.2.3, "Data Quota Highwater Exceeded Report," on page 270

22.3 General Data Quota Management

- Section 22.3.1, "Permanently Deleting Files from the Trash," on page 245

22.3.1 Permanently Deleting Files from the Trash

You might want to permanently delete files in order to make space available within a data quota or to recover disk space.

- "Permanently Deleting Files to Create Data Quota Space" on page 245
- "Permanently Deleting Files to Recover Disk Space" on page 246

Permanently Deleting Files to Create Data Quota Space

When users delete files or file versions, the disk space occupied by the deleted files and versions counts against the data quotas until users permanently delete the files and versions, as described in "Making Disk Space Available by Deleting Trashed Items" in the *Filr 2.0: Web Application User Guide*.

As a Filr administrator, you can permanently delete files and versions anywhere on the Filr site in order to make space available within a user's data quota.

Permanently Deleting Files to Recover Disk Space

Whether disk space is recovered after you permanently delete files using the Filr interface differs depending on whether you are deleting files in Net Folders or files from a user's personal storage in the My Files area:

- "Permanently Deleting Files in Net Folders" on page 246
- "Permanently Deleting Files in Personal Storage" on page 246

Permanently Deleting Files in Net Folders

If you want to recover disk space on your file system, permanently deleting files in Net Folders using the Filr interface should also delete the files from the underlying file system, depending on the underlying implementation of the storage.

Permanently Deleting Files in Personal Storage

If you want to recover disk space on the Filr system, you must permanently delete the files from Filr.

For information about how to purge items, see "Making Disk Space Available by Deleting Trashed Items" in the *Filr 2.0: Web Application User Guide*.

22.4 Managing the File Upload Size Limit

The file upload size limit conserves disk space on your Novell 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.

Browsers also impose limits on the size of files that can be uploaded. This limit differs depending on which browser you are using to run Filr.

- Section 22.4.1, "Modifying the File Upload Size Limit for the Filr Site," on page 246
- Section 22.4.2, "Setting a File Upload Size Limit for Individual Users and Groups," on page 247

22.4.1 Modifying the File Upload Size Limit for the Filr Site

As the Filr administrator, you can increase or decrease the file upload size limit for the Filr site. Workspace and folder owners can set a file upload size limit for their own workspaces and folders, but the limit in individual workspaces and folders cannot exceed what you set for the Filr site.

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

2 Under **Management**, click **File Upload Limits**.

3 In the **Default File Upload Size Limits** field, specify the new file upload size limit.

4 Click **Apply** > **Close**.

22.4.2 Setting a File Upload Size Limit for Individual Users and Groups

You can assign a file upload size limit to individual users and groups that is different from the site-wide file upload size limit. For example, if the file upload size limit for your Filr site is 2 GB, but your Marketing team often uploads large files, you can give the `Marketing` group a file upload size of 3 GB.

- "Setting a Limit for a Group" on page 247
- "Setting a Limit for a User" on page 247

Setting a Limit for a Group

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

2 Under **Management**, click **File Upload Limits**.

3 In the **File Upload Size Limits** section, click **Add a Group**.

4 Specify the following information:

   Group: Begin typing the group name for which you want to set a file upload size limit, then click the name when it appears in the list.

   File Size Limit: Specify the new file size limit for the group.

5 Click **OK**.

Setting a Limit for a User

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

2 Under **Management**, click **File Upload Limits**.

3 In the **Default File Upload Size Limits** section, click **Add a User**.

4 Specify the following information:

   User: Begin typing the user name for which you want to set a file upload size limit, then click the name when it appears in the list.

   File Size Limit: Specify the new file size limit for the user.

5 Click **OK**.

22.5 Managing Quotas for Outgoing Email Messages

You can set data quotas on the amount of content users can send on email messages that are sent from the Filr system.

For information about how to do this, see Chapter 5, "Enabling and Customizing Filr's Email Services," on page 57.

23 Managing Email Configuration

After you enable email integration for the Filr site as described in Chapter 5, "Enabling and Customizing Filr's Email Services," on page 57, you can further modify the way email is managed on the Filr site.

 ◆ Section 23.1, "Configuring Outbound Email with TLS over SMTP," on page 249

23.1 Configuring Outbound Email with TLS over SMTP

Depending on how your email application is configured, you might need to configure Filr outbound email with TLS over SMTP for secure email. Novell GroupWise, for example, can be configured to require this. If you are using GroupWise or another email application that requires this type of configuration, you can configure Filr with TLS over SMTP by using STARTTLS.

NOTE: During the Filr appliance configuration, when configuring Outbound email, ensure that you have selected **SMTP** in the **Protocol** drop-down list, and that **Enable STARTTLS** is selected, as described in Section 1.9, "Configuring Outbound Email Services," on page 31.

---

24 Viewing the Filr License

Path: **https://DNS_or_IP:8443 > Administration Console > Management > License**

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

2. Under **Management**, click **License**.

   The Filr license is displayed.

3. (Conditional) If you have updated your Filr license and the contents of the new license are not being displayed, click **Reload Filr License**.

You update the Filr license from the Filr appliance management console, as described in Section 1.15, "Viewing and Updating the Filr License," on page 37.

25 Managing the Lucene Index

For background information about the Lucene index, see Section 1.5.1, "Understanding Indexing," on page 25.

- Section 25.1, "Changing Your Lucene Configuration," on page 253
- Section 25.2, "Optimizing the Lucene Index," on page 253
- Section 25.3, "Rebuilding the Lucene Index," on page 255
- Section 25.4, "Performing Maintenance on a High Availability Lucene Index," on page 257

25.1 Changing Your Lucene Configuration

You can change your Lucene Configuration settings as described in Section 1.5.2, "Changing Search Index Configuration Settings," on page 25.

25.2 Optimizing the Lucene Index

If you notice that search performance in Novell Filr is becoming slower over time, you might want to optimize your Lucene index.

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

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

Optimizing the Lucene index does not repair a damaged or out-of-date index. To repair a damaged or out-of-date index, you must rebuild the index, as described in Section 25.3, "Rebuilding the Lucene Index," on page 255.

- Section 25.2.1, "Optimizing a Single Search Index," on page 253
- Section 25.2.2, "Optimizing the Search Index with Multiple Index Servers," on page 254

25.2.1 Optimizing a Single Search Index

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

   1a Launch a web browser.

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

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

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

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

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

3 Under **Management**, click **Search Index**.

4 Click the **Optimize Search Index** tab.

5 Select **Run Immediately** if you want to run the optimization right now.

6 Select **Run at Scheduled Time**, then specify the days and times that you want the optimization to occur.

7 Click **OK**.

25.2.2 Optimizing the Search Index with Multiple Index Servers

1 Log in to the Filr site as the Filr administrator.
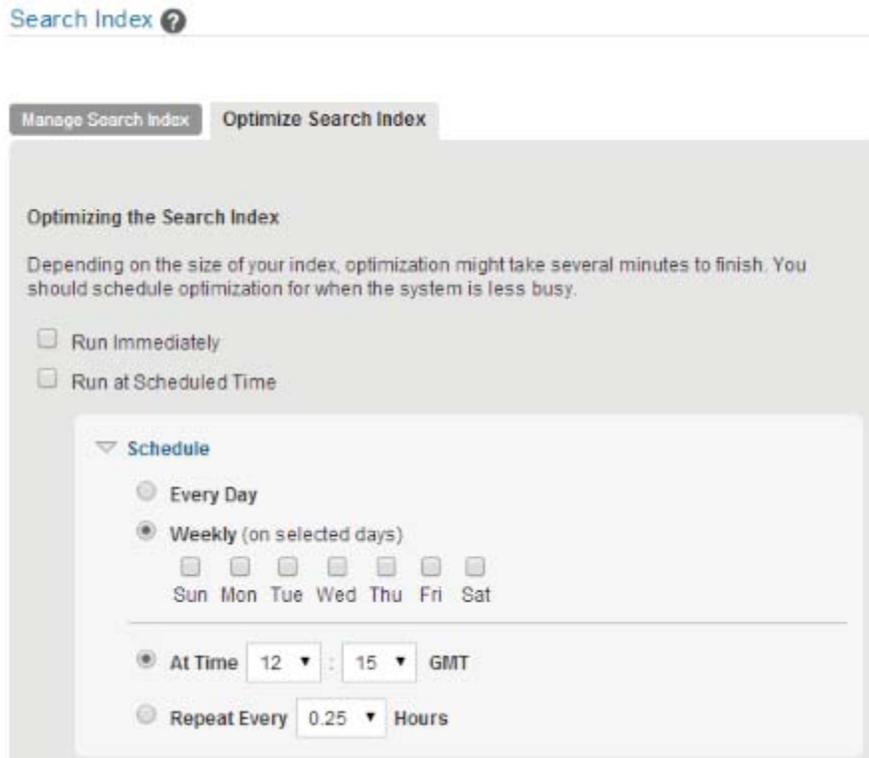
   1a Launch a web browser.

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

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

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

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

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

3 In the **Search Index** section, click **Index**.

4 Click the **Optimize Search Index** tab.

5 Select **Run Immediately** if you want to run the optimization right now.

6 Select **Run at Scheduled Time**, then specify the days and times that you want the optimization to occur.

7 Select each node that you want to optimize.

8 Click **OK**.

25.3 Rebuilding the Lucene Index

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

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

Users might first notice a problem with the Lucene index if they cannot find information or people that they know should be available on the Filr site. If you are running multiple Lucene Index Servers, follow the instructions in Section 25.4, "Performing Maintenance on a High Availability Lucene Index," on page 257.

Rebuilding the Lucene search index can consume a significant amount of resources on your Filr appliance. In a clustered environment, it is a good idea to set aside a single Filr appliance to handle the load of rebuilding the search index. (For information about how to set aside a Filr appliance, see "Setting Aside a Filr Appliance for Re-Indexing and Net Folder Synchronization in a Clustered Environment" in the *Filr 2.0: Installation and Configuration Guide*.)

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

## 25.3.1 Rebuilding a Single Search Index

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

1a Launch a web browser.

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

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

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

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

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

3 In the **Management** section, click **Search Index**.
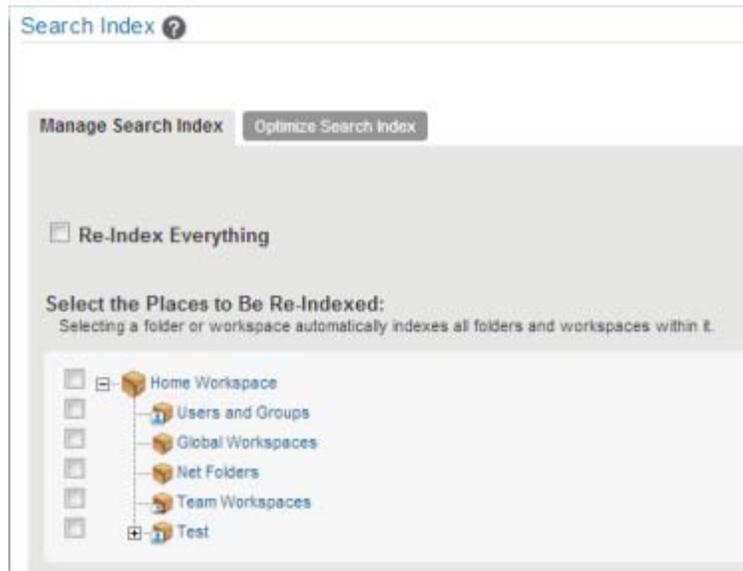
4 To reindex the entire Filr site, select **Re-Index Everything**.

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

or

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

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

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

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

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

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

For information about how to access the `appserver.log` file, see .

25.3.2 Rebuilding the Search Index with Multiple Index Servers

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

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

For information about how to take a node out of service, see .

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

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

For information about how to put a node back into service, see .

4 Repeat this process for the second search index node.

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

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

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

For information about how to access the `appserver.log` file, see .

25.4 Performing Maintenance on a High Availability Lucene Index

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

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

  1a Launch a web browser.

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

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

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

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

2 Take the Lucene node that needs maintenance out of service:

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

  2b Under **Search Index**, click **Nodes**.

Node A (node a)

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

User Mode Access
- ⦿ Read and Write
- ◯ Write Only
- ◯ No Access

☑ Enable Deferred Update Log

No Deferred Update Log Record Exists

Node B (node b)

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

User Mode Access
- ◯ Read and Write
- ⦿ Write Only
- ◯ No Access

☑ Enable Deferred Update Log

No Deferred Update Log Record Exists

Apply   Close

2c In the list, locate the node that needs maintenance.

2d Ensure that **Enable Deferred Update Log** is selected.

2e In the **User Mode Access** box, change **Read and Write** to one of the following options, depending on the type of maintenance that you want to perform:

- **Write Only:** Select this option if you are performing a re-index on the search index node.

- **No Access:** Select this option if you are performing other types of maintenance on the search index node, such as upgrading it, adding more disk space or memory, and so forth.

  Selecting this option ensures that no data is written to the index while the maintenance is being performed.

2f Click **Apply**, then click **Close**.

The new setting is put into effect immediately, so that the Lucene node is no longer accessible to Filr users.

3 Perform the needed maintenance on the Lucene node. For example, for information about how to perform a re-index on the node, see Section 25.3, "Rebuilding the Lucene Index," on page 255.

4 Return the out-of-date Lucene node to full service:

  4a Click the **admin** link in the upper-right corner of the page, then click the **Administration Console** icon.

  4b Under **Search Index**, click **Nodes**.

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

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

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

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

  4d Click **Close**.

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

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

26 Managing Database Logs for the Audit Trail

Filr allows you to determine the frequency with which audit trail entries and are deleted from the Filr system.

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

   1a Launch a web browser.

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

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

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

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

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

3 Under **Management**, click **Database Logs**.

4 In the **Manage Database Logs** section, the following options are available:

   Automatically Delete Audit Trail Entries Older Than *xx* Days: Specify the maximum number of days to keep audit trail log entries before they are deleted. The default is 183 days (6 months). The allowed minimum is 30 days.

   Audit trail entries are used to build the Activity and Login reports. Removing older entries limits the possible time span for these reports. (For more information about these reports, see Section 28.2, "Monitoring Filr by Generating Reports," on page 269.)

   The Filr desktop application relies on audit trail data when doing full synchronizations.

5 Click **OK**.

27 Backing Up Filr Data

Reliable backups are critical to the stability of your Novell Filr site.

IMPORTANT: Do not use VMware snapshots as a backup method for Filr. Doing so creates problems when managing the system disk and inhibits your ability to update Filr in the future.

- Section 27.1, "Locating Filr Data to Back Up," on page 263
- Section 27.2, "Scheduling and Performing Backups," on page 264
- Section 27.3, "Restoring Filr Data from Backup," on page 264
- Section 27.4, "Manually Restoring Individual Files and Folders," on page 264

27.1 Locating Filr Data to Back Up

In order to keep adequate backups of your Novell Filr data, you must back up the following types of data:

- Section 27.1.1, "Filr File Repository," on page 263
- Section 27.1.2, "Filr Database," on page 263
- Section 27.1.3, "Lucene Search Index," on page 264
- Section 27.1.4, "Certificates," on page 264

27.1.1 Filr File Repository

Back up the following location on the Filr appliance. In a large deployment, back up this location on each Filr appliance in the cluster.

```
/vastorage/filr/filerepository
```

For more information about the Filr file repository, see "Planning the File Repository" in the *Filr 2.0: Installation and Configuration Guide*.

27.1.2 Filr Database

Back up the following location on the Filr appliance (in a small deployment) or on the MySQL database appliance (in a large deployment):

```
/vastorage/mysql
```

Specifically, you should back up the following databases: `filr`, `information_schema`, `mysql`

Refer to the database backup method information (http://dev.mysql.com/doc/refman/5.0/en/backup-methods.html) in the MySQL documentation.

For more information about the Filr database, see "Filr Database" in the *Filr 2.0: Installation and Configuration Guide*.

27.1.3 Lucene Search Index

You can back up the following location on the Filr appliance (in a small deployment) or the Lucene search index appliance (in a large deployment):

```
/vastorage/conf
```

The Lucene search index does not need to be backed up because it can be rebuilt at any time. For information about how to rebuild the Lucene search index, see Section 25.3, "Rebuilding the Lucene Index," on page 255.

For more information about the Lucene search index, see "Search Index" in the *Filr 2.0: Installation and Configuration Guide*.

27.1.4 Certificates

Back up the following location on the Filr appliance. In a large deployment, back up this location on each Filr appliance in the cluster.

```
/vastorage/conf
```

27.2 Scheduling and Performing Backups

You do not need to bring your Novell Filr site down in order to perform backups. You might want to back up the Filr file repository and the Filr database every night, perhaps doing a full backup once a week and incremental backups on other days. You can back up the Lucene index whenever it is convenient. You can always reindex the Filr site in order to re-create the Lucene index, but being able to restore content from a backup can save time in case of an outage.

27.3 Restoring Filr Data from Backup

If you need to restore your Novell Filr site from a backup, restoring the same backup version for both the file repository and the database creates a Filr site that is consistent within itself but might be missing information that was added after the backups were created. If you lose the file repository but not the database, you can restore the backed-up file repository and keep the more current database, but some files are missing from the file repository.

27.4 Manually Restoring Individual Files and Folders

Files and folders from users' My Files area (personal storage) that were moved to the trash and were not permanently deleted can be restored from the trash. Unlike files from users' personal storage, files from Net Folders cannot be restored from the Filr trash.

The Filr administrator can view all items that were moved to the trash and restore them to their previous location, as described in Section 21.3, "Restoring Files and Folders from the Trash," on page 231.

Individual Filr users can restore items from the trash, as described in "Restoring Items from the Trash" in the *Filr 2.0: Web Application User Guide*.

28 Monitoring the Filr System

You can monitor activity on your Novell Filr site by using Filr reports and log files.

- Section 28.1, "Monitoring Filr Performance with Ganglia," on page 265
- Section 28.2, "Monitoring Filr by Generating Reports," on page 269
- Section 28.3, "Managing Product Improvement," on page 281
- Section 28.4, "Accessing the Filr Log File," on page 282
- Section 28.5, "Understanding Disk Usage Checks," on page 283
- Section 28.6, "Checking the Filr Site Software Version," on page 283

28.1 Monitoring Filr Performance with Ganglia

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

For information about how to configure Ganglia for your environment, including changing from multicast mode to unicast mode, see Section 2.6, "Changing the Ganglia Configuration," on page 43.

NOTE: Setting Ganglia hosts to unicast mode can help to improve overall performance of the Filr system.

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

- Section 28.1.1, "Viewing Metrics for an Individual Node," on page 265
- Section 28.1.2, "Viewing Metrics for Multiple (Clustered) Filr Nodes," on page 266
- Section 28.1.3, "Filr Monitoring Metrics," on page 267

28.1.1 Viewing Metrics for an Individual Node

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

1. In a small installation, log in to the Filr appliance.

   or

   In a large installation, log in to either the Filr appliance, search index appliance, or database appliance.

   Use the following URL for each appliance: https://*server_url*:9443.

2. Click the **Ganglia** icon.

An overview is displayed of all the nodes in the cluster, including information such as CPU utilization, memory, load, and so forth.

3 In the **Grid-Node** drop-down list, select a node that you want to monitor.

or

Scroll to the bottom of the page and click a node.

For a list of available metrics, see Section 28.1.3, "Filr Monitoring Metrics," on page 267.

28.1.2 Viewing Metrics for Multiple (Clustered) Filr Nodes

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

1 In a small installation, log in to the Filr appliance.

or

In a large installation, log in to either the Filr appliance, search index appliance, or database appliance.

Use the following URL for each appliance: https://*server_url*:9443.

2 Click the **Ganglia** icon.

An overview is displayed of all the nodes in the cluster, including information such as CPU utilization, memory, load, and so forth.

3 Click the **Aggregate Graphs** tab.

4 Specify the appropriate information for the following fields to create the aggregate graph:

Title: The title that appears on the aggregate graph after it is created.

Vertical (Y-Axis) label: The label that appears for the graph's Y-axis after the graph is created.

Limits: Defines the lower and upper limits of the Y-axis. (The Y-scale of the graph.)

Host Regular expression: Specify the nodes in the cluster that you want to compare. Nodes must be separated by a vertical bar (|). For example, `node1|node2`.

Metric Regular expression: Specify the name of the metric that you want to view. For example, typing `FILR_Unique_Users` displays information about the number of unique logged in users. As you type, matching metric names that you can choose from are displayed. (You can also see the metric name to specify in this field by clicking on the **Main** tab and looking in the upper-left corner of each metric graph.)

For a list of available metrics, see Section 28.1.3, "Filr Monitoring Metrics," on page 267.

Graph Type: Select whether you want a line or stacked graph to be created.

Legend options: Select whether to show or hide the legend.

5 Click **Create Graph**.

6 (Optional) To save this graph for future use, click **Direct Link to this aggregate graph**, then save the resulting URL.

28.1.3   Filr Monitoring Metrics

- "Filr Server Metrics" on page 267
- "Filr Search Metrics" on page 268

Filr Server Metrics

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

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

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

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

Sessions: Number of valid sessions in memory.

Peak Sessions: Peak number of valid sessions in memory.

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

These users might not be currently logged in.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Represents only those requests that resulted in a conversion.

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

Represents only those requests that resulted in a conversion.

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

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

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

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

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

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

Filr Search Metrics

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

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

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

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

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

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

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

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

28.2 Monitoring Filr by Generating Reports

Most Novell Filr reports are created in CSV format, so that you can import them into a spreadsheet and easily manipulate the data to suit your needs. The default CSV file name is `report.csv`. If you create multiple reports without manually renaming them, the default file name is incremented (`report-n.csv`). The default location to save the report is `/tmp`.

28.2.1 Credits Report

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

28.2.2 Data Quota Exceeded Report

NOTE: This report is generated only when data quotas are enabled.

The Data Quota Exceeded report lists individual users who have exceeded the data quota. The report provides a spreadsheet with the following information for each user:

- **Data Quota Used (MB):** Displays the amount of disk space the user is currently using.
- **Data Quota:** Displays the user's individual quota if one has been set.

For information on how to set a quota for individual users, see Section 22.2.2, "Setting User Data Quotas," on page 236.

 * **Max Group Quota (MB):** Displays the largest data quota for any group that the user is a member of. Users are assigned the highest of all data quotas for any group for which they are a member.

 * **Default Data Quota (MB):** Displays the site-wide default quota.

   For information on how to set a default data quota, see Section 22.2.2, "Setting User Data Quotas," on page 236.
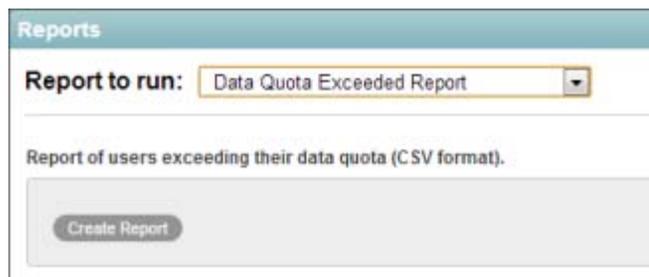
To generate the Data Quota Exceeded report:

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

   1a Launch a web browser.

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

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

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

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

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

3 Under **System**, click **Reports**.

4 In the **Report to run** drop-down list, select **Data Quota Exceeded Report**.

5 Click **Create Report** to generate the report.

   The report is launched in a spreadsheet.

28.2.3 Data Quota Highwater Exceeded Report

NOTE: This report is generated only when data quotas are enabled.

The Data Quota Highwater Exceeded report lists individual users who have exceeded the data quota high-water mark. The report provides the following information for each user:

 * **Data Quota Used (MB):** Displays the amount of disk space the user is currently using.

 * **Data Quota (MB):** Displays the user's individual quota if one has been set.

For information on how to set a quota for individual users, see Section 22.2.2, "Setting User Data Quotas," on page 236.

 * **Max Group Quota (MB):** Displays the largest data quota for any group that the user is a member of. Users are assigned the highest of all data quotas for any group for which they are a member.
 * **Default Data Quota (MB):** Displays the site-wide default quota.

   For information on how to set a default data quota, see Section 22.2.2, "Setting User Data Quotas," on page 236.
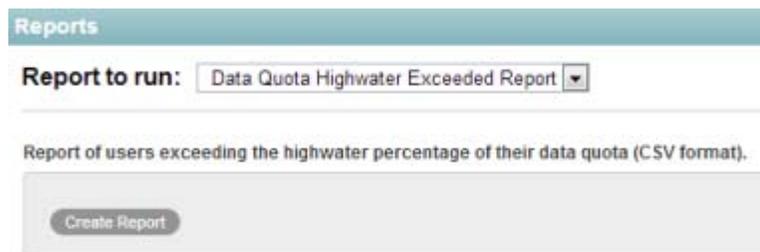
To generate the Data Quota Highwater Exceeded report:

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

   1a Launch a web browser.

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

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

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

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

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

3 Under **System**, click **Reports**.

4 In the **Report to run** drop-down list, select **Data Quota Highwater Exceeded Report**.

Reports

Report to run: Data Quota Highwater Exceeded Report

Report of users exceeding the highwater percentage of their data quota (CSV format).

Create Report

5 Click **Create Report** to generate the report.

The report is launched in a spreadsheet.

28.2.4 Disk Usage Report

The Disk Usage report lists the amount of disk space for workspaces on the Filr site by user, by workspace, or by both. In addition, you can restrict the reporting to only those workspaces that exceed a specified number of megabytes.

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

   1a Launch a web browser.

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

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

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

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

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

3 Under **System**, click **Reports**.

4 In the **Report to run** drop-down list, select **Disk Usage Report**.

5 Select the type of Disk Usage report that you want to generate:

Total Usage by User: Lists all Filr users whose disk space usage is above the amount specified in the **Usage Greater Than** field.

Total Usage by Workspace: Lists all workspaces where disk space usage is above the amount specified in the **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: Specify the number of megabytes above which you want to list disk space usage. This eliminates smaller disk space usages from the report.

6 Click **Create Report** to generate the Disk Usage report.

7 Select a text editor to view the report in, then click **OK**.

For a short report, you might obtain the information you need by viewing the CSV file.

8 (Optional) Save the CSV file with a meaningful name in a convenient location, then retrieve it into a spreadsheet program for further examination.

9 Click **Close** when you are finished checking disk space usage.

28.2.5 Email Report

The Email Report lists mail messages that have been sent from and into the Filr site. It also lists email errors that have been encountered.

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

    1a Launch a web browser.

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

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

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

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

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

3 Under **System**, click **Reports**.

4 In the **Report to run** drop-down list, select **Email Report**.

> **Reports**
>
> **Run a Report:** Email Report ▾
>
> *Reports may be truncated if too large.*
>
> **Report on Email Activity Between**
>
> Mar 9, 2014   and   Apr 10, 2014
>
> ◉ Sent emails   ○ Received emails   ○ Error emails
>
> Create Report

5 Specify the date range for the Email report.

6 Select whether you want a report on email that was sent from Filr or email errors that occurred.

Because Filr cannot currently be configured to receive email messages, the option **Received emails** is not a valid option.

7 Click **Create Report**.

The report contains the following information:

Send Date: Date when the email was sent.

From Address: Address that the email was sent from. This is the email address that the user has defined in his or her user profile.

To Address: Address that the email was sent to.

Type: This is the action that caused the message to be sent. For example, `sendMail` indicates that an item was shared.

Status: Status of the message, such as Sent or Received.

Subject Line: Subject line of the message.

Attached Files: File name of any attachments that were included in the email message.

Errors: Any errors that are associated with the email message.

28.2.6   External User Report

Lists information about the external users you include, such as the date on which their account was created.

28.2.7   License Report

The License report lists information about your Filr license, as well as information about the number of users in your Filr site and how many of those users have accessed the site.

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

   1a Launch a web browser.

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

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

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

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

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

   3 Under **System**, click **Reports**.

   4 In the **Report to run** drop-down list, select **License Report**.

   5 Specify the date range for the License report, then click **Create Report**.

   The License report lists the following information:

   ◆ Filr version

- License key type
- Date the license key was issued
- Date range when the license key is valid
- Maximum number of logged-in users during the date range
- Current active user count
- List of dates in the date range with the following user license information:
  - **Local Users:** The user account was created within Filr, and is not being synchronized from an LDAP directory.
  - **Users Synchronized from LDAP:** The user account was created from an LDAP source. (Only synchronized accounts that are not marked as Deleted or Disabled are counted.)
  - **Users Who Used Filr During the Previous 365 Days:** Users who have logged in at least once in the past year.

The Filr software does not limit the number of Filr users that you can create. However, sites where Filr licenses have been purchased and the Filr software installed are periodically audited against their purchased number of licenses.

6 Click **Close** when you are finished reviewing the License report.

28.2.8 Login Report

The Login report lists the Filr users who have logged in to the Filr site during a specified period of time. In addition, it can include a dated list of every login by each user.

Logins are recorded only for the web application. Logins via the desktop application and mobile app are not recorded.

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

   1a Launch a web browser.

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

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

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

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

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

3 Under **System**, click **Reports**.

4 In the **Report to run** drop-down list, select **Login Report**.

Reports

Run a Report: Login Report

Report on User Login Information (CSV format)

Report on Login Activity Between

Apr 29, 2013   and   May 29, 2013

People

Remove

○ Summarize Login Entries
Sort report by: --none--

○ List All Login Entries
Sort report by: Login Date

Create Report

5 Specify the date range for the Login report.

6 Leave the **People** field blank to list all user logins.

or

In the **People** field, start typing the first name of a Filr user, then in the drop-down list of names that match what you have typed, select a user whose logins you want to be reported. Repeat this process to include multiple users in the report.

7 Select the type of Login report that you want to generate.

Summarize Login Entries: Lists how many times the selected users have logged into the Filr site. In the **Sort Report By** drop-down list, select **User**, **Last Login**, or **Number of Logins** to organize the data.

List All Login Entries: Lists each individual user login and includes the following data about the action:

  ◆ User (first name, last name, and user ID)
  ◆ Account type
  ◆ Login date and time
  ◆ IP address

In the **Sort report by** drop-down list, select **Login Date** or **User** to organize the data in the way that is most helpful to you.

8 Click **Create Report** to generate the Login report.

9 Select a text editor to view the report in, then click **OK**.

For a short report, you might obtain the information you need by viewing the CSV file.

10 (Optional) Save the CSV file with a meaningful name in a convenient location, then retrieve it into a spreadsheet program for further examination.

28.2.9 System Error Logs Report

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

28.2.10 User Access Report

The User Access report lists the locations on the Filr site where a specified user has access rights. In addition, you can view, and if necessary, change or remove the access rights for any location. This report is especially useful on Filr sites where Guest user access has been granted, as described in Section 10.1, "Allowing External Users Access to Your Filr Site," on page 123.

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

    1a Launch a web browser.

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

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

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

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

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

3 Under **System**, click **Reports**.

4 In the **Report to run** drop-down list, select **User Access Report**.

5 Start typing the first name of a Filr user.

6 In the drop-down list of names that match what you have typed, select the user whose site access you want to be reported.

7 Click **Close** when you are finished checking user access rights.

28.2.11 User Activity Report

The User Activity report lists how many times specified users have viewed, added, modified, or deleted content on the Filr site during a specified period of time. In addition, it can include the date and time of each action, along with the location of the action.

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

   1a Launch a web browser.

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

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

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

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

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

3 Under **System**, click **Reports**.

4 In the **Report to run** drop-down list, select **User Activity Report**.

Reports

Run a Report: User Activity Report

Report of User Activity (CSV format)

Report on User Activity Between

Apr 30, 2013   and   May 23, 2013

People

Remove

◉ Activity Summary
◯ Report Workspace or Folder Activity (view, add, modify, delete)

Create Report

---

5 Specify the date range for the User Activity report.

6 Leave the **Select User** field blank to list all user activity.

or

In the **Select User** field, start typing the first name of a Filr user.

In the drop-down list of names that match what you have typed, select a user whose activity you want to be reported. Repeat this process to include additional users.

7 Select the type of User Activity report that you want to generate.

Activity Summary: Lists how many times the selected users have performed the following actions in the Filr site:

- User
- View
- 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
- Delete shares

Workspace or Folder Activity: Lists each individual user action and includes the following data about the action:

- User
- Activity type

- Count
- Activity date and time
- Folder
- Entry title
- Entry type
- Share Recipient
- Recipient Type
- Share Role

8 Click **Create Report** to generate the User Activity report.

9 Select a text editor to view the report in, then click **OK**.

For a short report, you might obtain the information you need by viewing the CSV file.

10 (Optional) Save the CSV file with a meaningful name in a convenient location, then retrieve it into a spreadsheet program for further examination.

28.2.12 XSS 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, Novell Filr contains a built-in security filter that protects against XSS vulnerabilities. For more general information about XSS, see Section 32.4.3, "Securing the Filr Site against XSS," on page 309.

The XSS report in Filr enables you to remove potentially harmful XSS threats from your Filr site.

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

   1a Launch a web browser.

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

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

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

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

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

3 Under **System**, click **Reports**.

4 In the **Report to run** drop-down list, select **XSS Report**.
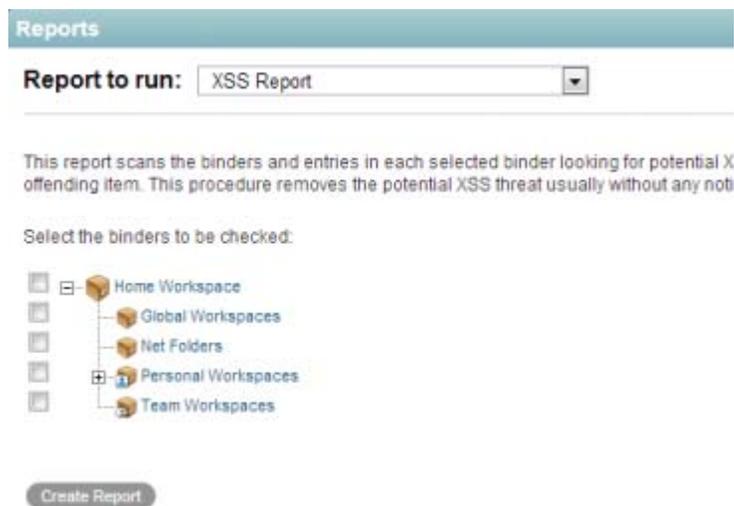
5 Select the directories (subdirectories are included) for which you want to generate the report, then click **Create Report**.

> **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 Novell Filr" in the Novell Support Knowledgebase (http://www.novell.com/support).

28.3 Managing Product Improvement

Path to Configuration Dialog: Filr Administration Console > **Management > 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.

> **IMPORTANT:** Novell collects nothing that identifies your organization, your data, or your users.

28.3.1 Accessing the Product Improvement Dialog

You can see what is collected, and you can modify, disable, or re-enable the data collection system by using the Product Improvement dialog.

1 Open the Filr Administration Console as the Admin user.

2 Click **Product Improvement**.

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

After the initial run, a **View the information collected** link displays in the dialog that lets you download the `.json` file created by the collection process.

To see the information collected, open the downloaded file in an application such as WordPad.

28.3.2 About the Data That Is Collected for Product Improvement

As already mentioned, Novell collects nothing that identifies your organization, your data, or your users.

The items in the `.json` file are mostly self-explanatory, but the following points might be helpful to understanding file content.

The data is divided in three sections:

- **Installation Identifier:** This is a unique string generated for each appliance. Its sole purpose is to let Novell track usage and statistics for a specific appliance over time.
- **Tier 1:** This section includes the product, version and build, license type, and number of users.
- **Tier 2:** This section includes additional information about the installation, most of which is self-explanatory.
    - 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 `admin`, `_filesyncagent`, and so on.
    - The group count numbers do not include system groups, such as `allusers`, `allextusers`, and so on.
    - `workspaceCount` does not include system workspaces, such as the `/Home` workspace and so on.
    - The numbers in `fileCounts` and `folderCounts` in the `netFolder` 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 `other`.

28.3.3 How Novell Receives Product Improvement Data

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

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

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

28.4 Accessing the Filr Log File

The Novell Filr log file (`appserver.log`) is available from the Filr site.

1 Log in as the Filr site administrator.

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

3 Under **System**, click **Reports**.

4 In the **Report to run** drop-down list, select **System Error Logs**.
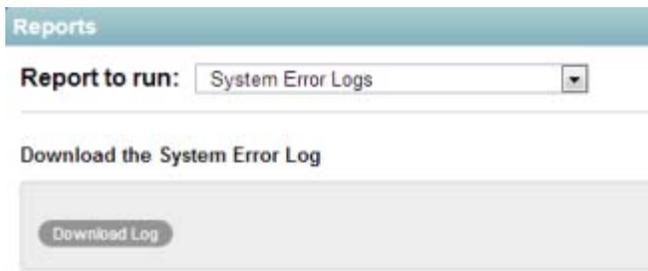
5 Click **Download Log**.

You are prompted to open or save a file named `logfiles.zip`, which contains the current `appserver.log` file. This file contains any stack traces or warning messages because of unexpected events encountered by the Filr program.

6 Save the `appserver.log` file to a convenient location on the Filr server.

This file is helpful when you need assistance resolving a problem with your Filr site.

28.5 Understanding Disk Usage Checks

Each hour, Filr checks the amount of disk space that is being used on the system drive for a given appliance. If disk usage reaches 90% capacity or greater on the system drive for any appliance, the Filr and FAMT services are stopped.

Following are the scripts that are used to monitor disk usage for each type of appliance:

* **Filr Appliance:** `/etc/cron.hourly/filr-diskcheck.sh`
* **Search Index Appliance:** `/etc/cron.hourly/lucene-diskcheck.sh`
* **Database Appliance:** `/etc/cron.hourly/mysql-diskcheck.sh`

When the Filr and FAMT services are stopped because of low disk space, a message is logged to both the `/var/opt/novell/va_status` and `/var/log/messages` files.

After the services are stopped, you must clean up unneeded data or add additional disk space to the appliance before restarting the services.

28.6 Checking the Filr Site Software Version

To display the version number and software date of the Novell Filr software:

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

   1a Launch a web browser.

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

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

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

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

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

The Filr software version and date are displayed.

IV Interoperability

Novell Filr can be used in conjunction with various other software products. By incorporating these products into your Filr system, you can add functionality, increase security, and maximize the value of Filr.

29 NetIQ Access Manager

Using Novell Filr in conjunction with NetIQ Access Manager adds enterprise-level security to your Filr system.

Only a version of Access Manager that supports Transport Layer Security (TLS) can be used when using Access Manager with Filr. For information about which versions of Access Manager support TLS and how to enable it, see *Enabling Transport Layer Security 1.1 and 1.2 for Access Manager* (https://www.netiq.com/documentation/netiqaccessmanager4/enable_tls_nam40/data/enable_tls_nam40.html#).

IMPORTANT

NetIQ Access Manager cannot grant external users access through the generated URL links that Filr includes in email notifications. This means that the following features are not functional for external or Guest users:

- Users are not able to share with external users, as described in "Sharing with People Outside Your Organization" in the *Filr 2.0: Web Application User Guide*.

  A possible work-around for this issue is documented in TID 7014912 (https://www.novell.com/support/kb/doc.php?id=7014912).

- Users are not able to share a File Link with external users, as described in "Distributing a Link to a File" in the *Filr 2.0: Web Application User Guide*.

- Users cannot make items accessible to the public, as described in "Making Files Accessible to the Public" in the *Filr 2.0: Web Application User Guide*.

  This means that public users cannot access the Filr site as the Guest user. For more information about the Guest user, see Section 10.1.1, "Allowing Guest Access to Your Filr Site," on page 123.

For more information about external users in Filr, see Section 10.1, "Allowing External Users Access to Your Filr Site," on page 123.

Before internal users can access your Filr site through NetIQ Access Manger, you must first configure specific protected resources in Access Manager to be public, as described in Chapter 12, "Allowing Access to the Filr Site through NetIQ Access Manager," on page 145.

Furthermore, you can configure NetIQ Access Manager to work with Novell Filr in the following way:

- Configure NetIQ Access Manager to provide single sign-on access to the Filr site.

  For more information, see Section 1.8, "Changing Reverse Proxy Configuration Settings," on page 28.

When you set up NetIQ Access Manager to work with Filr, ensure that you specify the correct HTTP/HTTPS port numbers during the configuration of the Filr appliance, as described in "HTTP/HTTPS Ports When You Use NetIQ Access Manager with Filr" on page 22.

30 Novell Dynamic File Services

You can manage your Novell Filr files by leveraging the functionality of Novell Dynamic File Services. Novell Dynamic File Services is an information life-cycle management technology that uses a policy-based approach for relocating files between two paths located on different storage devices. You can use Dynamic File services to better manage your premium storage for Filr by offloading large or seldom used files to a secondary storage location. Dynamic File Services provides a merged view of the data to the Filr application, which allows its users to transparently access their files without being aware of where they are physically stored.

For information on how to configure Filr with Novell Dynamic File Services, see "Setting Up a Merged View for Collaboration Applications: Novell Teaming" in the *Dynamic File Services Administration Guide* (http://www.novell.com/documentation/dynamic_file_services/dynamic_admin_win/data/teaming.html).

V **Site Security**

31 Security Administration

SSL (Secure Socket Layer) and TLS (Transport Layer Security) can be used to secure the connections between your Novell Filr site and other network services.

- Section 31.1, "Dealing with Security Scan Results," on page 293
- Section 31.2, "Replacing the Self-Signed Digital Certificate for an Official Certificate," on page 294
- Section 31.3, "Securing LDAP Synchronization," on page 296
- Section 31.4, "Securing Email Transfer," on page 302
- Section 31.5, "Security against Brute-Force Attacks with CAPTCHA," on page 303
- Section 31.6, "Securing User Passwords," on page 303
- Section 31.7, "If You Use eDirectory Universal Passwords," on page 303
- Section 31.8, "Restricting SSH Access for the Root User," on page 304
- Section 31.9, "Setting Up Filr in a DMZ," on page 304
- Section 31.10, "Filr Component Security," on page 306

31.1 Dealing with Security Scan Results

Running regular security scans on your network is critical to security administration. As exemplified in Chapter 32, "Security Policies," on page 307, security is a top priority for the Filr development team.

Occasionally, reputable security scanning software reports risks that the Filr team considers to be less significant than reported. The following are specific examples:

- **PHP as a Security Vulnerability:** Although in many cases the presence of PHP scripts is a legitimate concern, in the case of Filr, there is no PHP access without first authenticating through port 9443. Since access through port 9443 is secure by definition, Filr's PHP implementation is secure.

- **Diffie-Hellman 1024 Keys:** If you run a Nessus or equivalent security scan, you might receive a report of "Medium Risk" associated with Diffie-Hellman 1024-bit keys.

  The Filr team is aware of this and is considering increasing the key size in a future release. At this time, however, the team does not feel that this is a significant threat to Filr installations; breaking 1024-bit keys requires computing resources that only a nation-state would have at its disposal.

  If you are concerned or feel that your organization might be vulnerable to nation-state attacks, you can specify a stronger key through the Java security policy.

31.2 Replacing the Self-Signed Digital Certificate for an Official Certificate

The Novell Appliance ships with a self-signed digital certificate. Instead of using this self-signed certificate, you should use a trusted server certificate that is signed by a trusted certificate authority (CA) such as VeriSign or Equifax.

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

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

NOTE: If you are using a Godaddy SSL certificate with Filr, follow the steps in "Godaddy SSL Certificates for Filr" (https://www.novell.com/communities/coolsolutions/godaddy-ssl-certificates-for-filr/) at the Novell Cool Solutions web site (https://www.novell.com/communities/coolsolutions/).

31.2.1 Using the Digital Certificate Tool

Creating a New Certificate

1 Log in to the Novell Appliance at https://*server_url*:9443.

2 Click **Digital Certificates**.

3 In the **Key Store** drop-down list, ensure that **Web Application Certificates** is selected.

4 Click **File** > **New Certificate (Key Pair)**, then specify the following information:

Alias: Specify a name that you want to use to identify and manage this certificate.

Avoid using periods (.) in the Alias name, because doing so can result in unpredictable behavior with some browsers when importing trusted certificates.

Validity (days): Specify how long you want the certificate to remain valid.

Key Algorithm: Select either **RSA** or **DSA**.

Key Size: Select the desired key size.

Signature Algorithm: Select the desired signature algorithm.

Common Name (CN): This must match the server name in the URL in order for browsers to accept the certificate for SSL communication.

Organizational Unit (OU): (Optional) Small organization name, such as a department or division. For example, Purchasing.

Organization (O): (Optional) Large organization name. For example, Novell, Inc.

City or Lacality (L): (Optional) City name. For example, Provo.

State or Province (ST): (Optional) State or province name. For example, Utah.

Two-letter Country Code (C): (Optional) Two-letter country code. For example, US

5 Click **OK** to create the certificate.

After the certificate is created, it is self-signed.

6 Make the certificate official, as described in "Getting Your Certificate Officially Signed" on page 295.

Getting Your Certificate Officially Signed

1 On the Digital Certificates page, select the certificate that you just created, then click **File** > **Certificate Requests** > **Generate CSR**.

2 Complete the process of emailing your digital certificate to a certificate authority (CA), such as Verisign.

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

3 After you have received the official certificate and certificate chain from the CA:

3a Revisit the Digital Certificates page by clicking **Digital Certificates** from the Novell Appliance.

3b Click **File** > **Import** > **Trusted Certificate**. Browse to the trusted certificate chain that you received from the CA, then click **OK**.

3c Select the certificate that you created in "Creating a New Certificate" on page 294, then click **File** > **Certification Request** > **Import CA Reply**.

3d Browse to and upload the official certificate to be used to update the certificate information.

On the Digital Certificates page, the name in the **Issuer** column for your certificate changes to the name of the CA that stamped your certificate.

4 Activate the certificate, as described in Section 31.2.3, "Activating the Certificate," on page 296.

31.2.2   Using an Existing Certificate and Key Pair

When you use an existing certificate and key pair (such as in the case of a wildcard certificate), use a .P12 key pair format.

1 If your certificate is not yet in .P12 key pair format, you can use openSSL to convert it. For example, run the following command from a Linux command prompt:

```
openssl pkcs12 -export in mycert.pem -inkey mykey.pem -out mycert.p12
```

2 Go to the Digital Certificates page by clicking **Digital Certificates** from the Novell Appliance.

3 In the **Key Store** drop-down list, select **Web Application Certificates**.

4 Click **File** > **Import** > **Trusted Certificate**. Browse to and select your existing certificate, then click **OK**.

5 Click **File** > **Import** > **Trusted Certificate**. Browse to your existing certificate chain for the certificate that you selected in Step 2, then click **OK**.

6 Click **File** > **Import** > **Key Pair**, then browse to and select your .P12 key pair file, specify your password if needed, then click OK.

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

7 Continue with Section 31.2.3, "Activating the Certificate," on page 296.

31.2.3 Activating the Certificate

1 On the Digital Certificates page, in the **Key Store** drop-down list, select **Web Application Certificates**.

2 Select the certificate that you want to make active, then click **Set as Active**, then click **Yes**.

3 Verify that the certificate and the certificate chain were created correctly by selecting the certificate and clicking **View Info**.

31.3 Securing LDAP Synchronization

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

 ◆ Section 31.3.1, "Exporting a Root Certificate," on page 296
 ◆ Section 31.3.2, "Importing the Root Certificate into the Java Keystore," on page 302

31.3.1 Exporting a Root Certificate

 ◆ "Exporting a Root Certificate for eDirectory" on page 296
 ◆ "Exporting the Root Certificate for Active Directory" on page 296

Exporting a Root Certificate for eDirectory

1 Launch and log in to iManager for your tree.

2 Click **Directory Administration**.

3 Click **Modify Object**.

4 Click the magnifying glass icon to browse to and select the "*Tree Name* CA" object in the Security container of the eDirectory tree.

5 Click **OK**.

6 Click the **Certificates** tab.

7 Select the check box for the root certificate (this is not the certificate titled **Self Signed Certificate**, but rather the root certificate), then click **Validate**.

8 Select the check box for the root certificate, then click **Export**.

9 Deselect **Export private key**, then click **Next**.

10 Click **Save the exported certificate**, then select **File in binary DER format**.

11 Save the file to a location where it can be accessed later and with a file name that you can remember, such as `SelfSignCert.der`.

12 Click **Close** > **OK**.

13 Continue with Section 31.3.2, "Importing the Root Certificate into the Java Keystore," on page 302.

#### Exporting the Root Certificate for Active Directory

**1** On the Windows server, click **Start > Run**, then enter `mmc`.
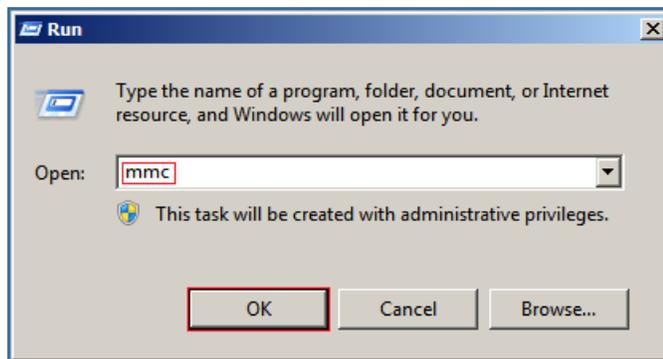
2 In MMC, type `Ctrl+M`.

3 If the **Internet Information Services (IIS) Manager** snap-in is not installed on your Windows server, install it.

4 With IIS selected, click **Add**, then click **OK**.
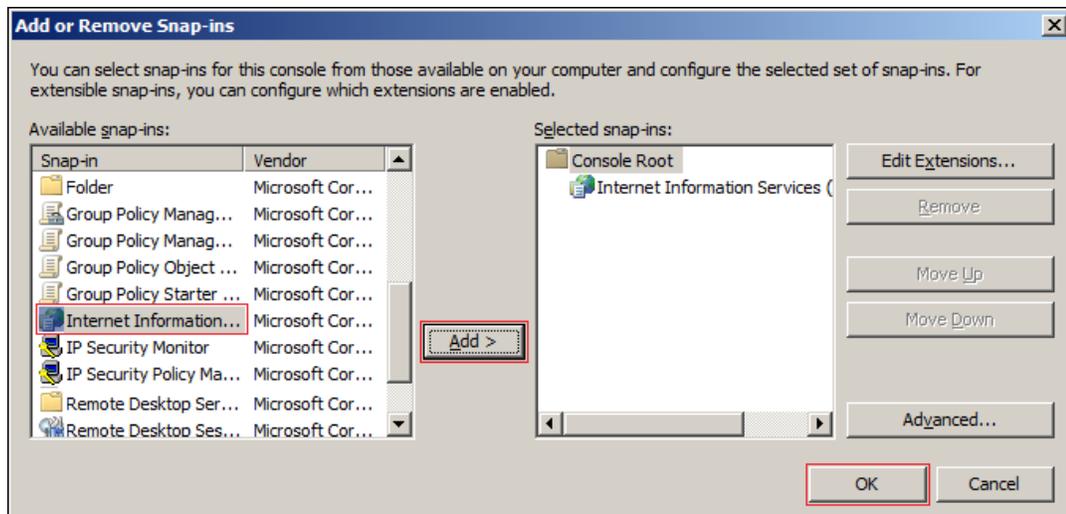
5 In the left frame, click **Internet Information Services**, then click a Windows server that Filr can connect to for synchronizing users.
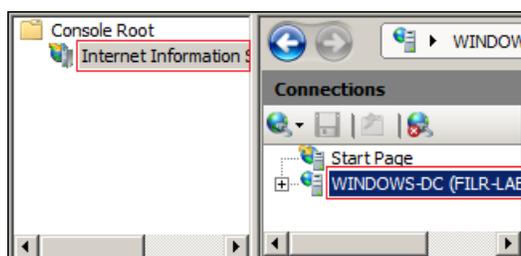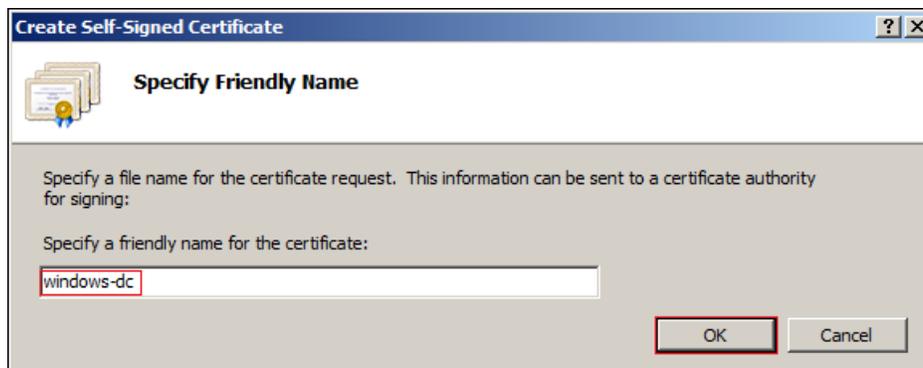

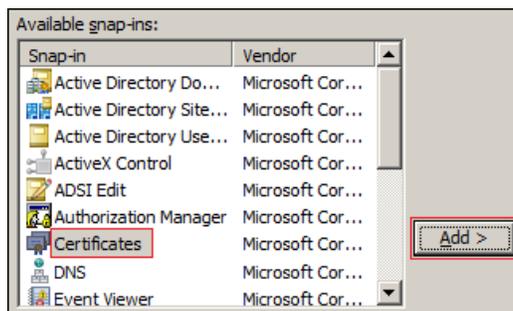**6** In the Filter list, scroll down to **Server Certificates** and double-click the icon.
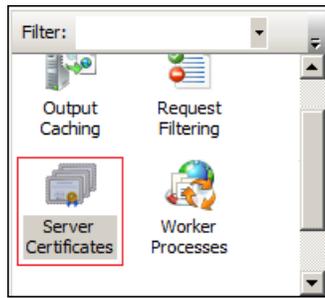
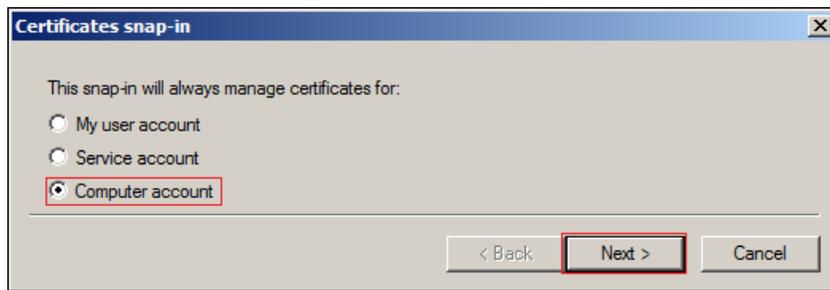**7** In the **Actions** list, click **Create Self-Signed Certificate**.

8 Name the certificate with a name you can remember, such as the server name, then click **OK**.
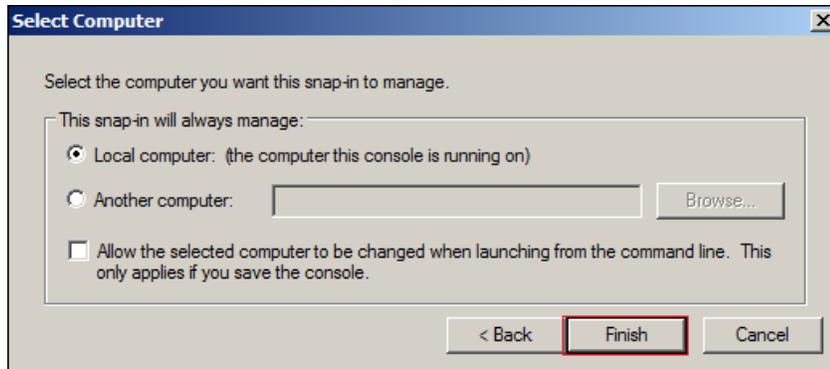

9 Type Ctrl+M, select the **Certificates** plug-in, then click **Add**.

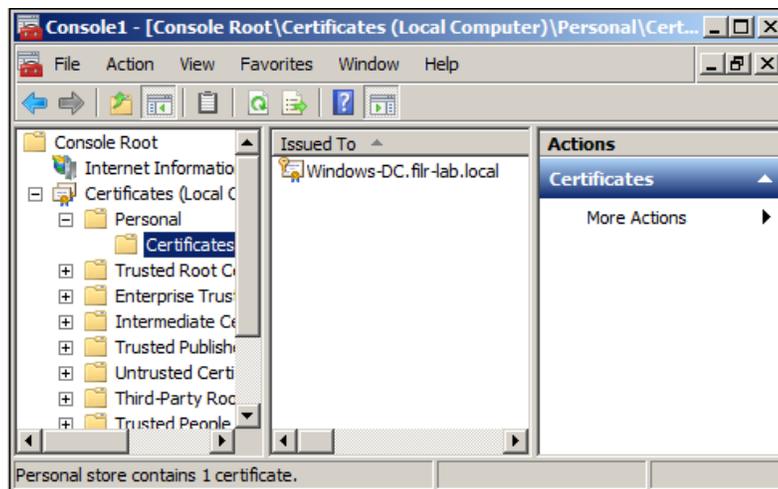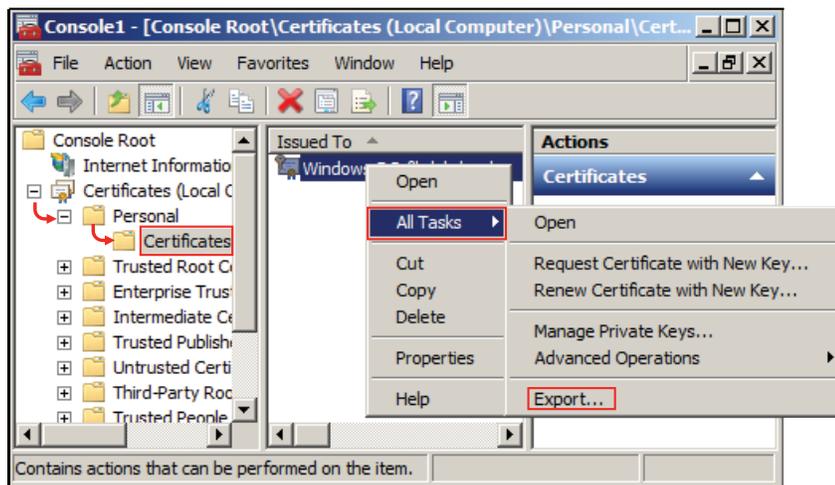**10** Select **Computer account**, then click **Next**.

11 Click **Finish**.

12 In the Snap-ins dialog, click **OK**.

13 In MMC, expand the **Certificates** plug-in, expand **Personal**, then click **Certificates**.

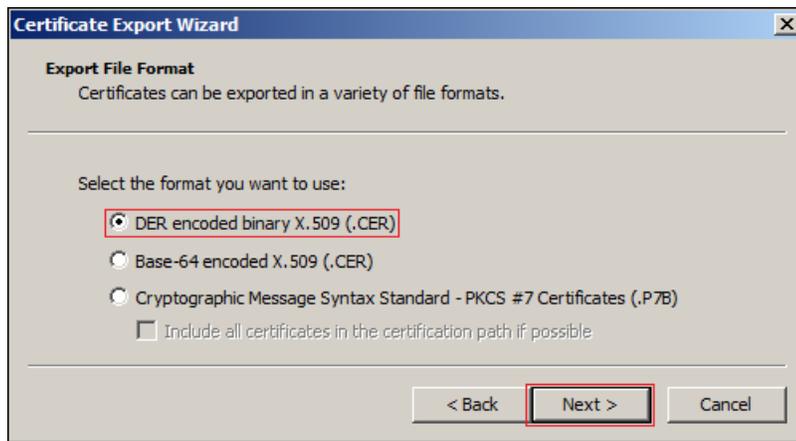**14** Right-click the certificate you created, select **All Tasks**, then click **Export....**.

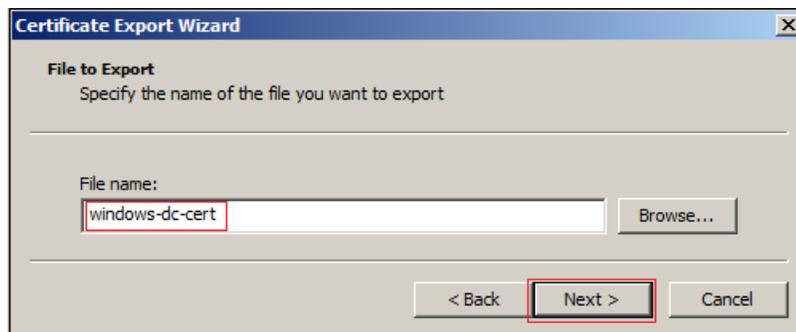**15** In the Certificate Export wizard, click **Next**.

16 Ensure that **No, do not export the private key** is selected, then click **Next**.

17 Ensure that **DER encoded binary** is selected, then click **Next**.

18 Name the certificate, then click **Next**.

19 Click **Finish > OK**.

The certificate is saved in `C:\Users\`*`Your-User-Name`*.

20 Ensure that the certificate is accessible from your management browser.

21 Continue with Section 31.3.2, "Importing the Root Certificate into the Java Keystore," on page 302.

31.3.2 Importing the Root Certificate into the Java Keystore

1 Navigate to the management console of your Novell Appliance:

`https://ip_address:9443`

2 Click the **Appliance System Configuration** icon.

The Novell Appliance Configuration page is displayed.

3 Click **Digital Certificates**.

4 In the **Key Store** drop-down list, select **JVM Certificates**.

5 Click **File** > **Import** > **Trusted Certificate**.

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

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

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

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

8 Click **OK**.

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

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

You can restart the Filr service as described in Section 2.7, "Changing System Services Configuration," on page 43.

You are now ready to configure your Filr site for secure LDAP synchronization, as described in Section 18.1, "Synchronizing Users and Groups from an LDAP Directory," on page 193.

31.4 Securing Email Transfer

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

If your Filr site needs to send email messages to an email system that requires secure SMTP (SMTPS), the Filr site must have the same type of root certificate that is required for secure LDAP (LDAPS). If you have not already set up secure LDAP for your Filr site, follow the instructions in Section 31.3, "Securing LDAP Synchronization," on page 296 to set up secure SMTP for communications with your email system.

31.5 Security against Brute-Force Attacks with CAPTCHA

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

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

31.6 Securing User Passwords

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.

When you enable password complexity checking in Filr, Filr requires that passwords:

- 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:
    - A lower-case character
    - An upper-case character
    - A number
    - One of the following symbols: ~ @ # $ % ^ & * ( ) - + { } [ ] | \ ? / , . < >

To enable password policy checking on the Filr site:

1 Log in to the Filr site as the Filr administrator.
2 Click the **admin** link in the upper-right corner of the page, then click the **Administration Console** icon .
3 Under **System**, click **Password Policy**.
4 Select **Enable Password Complexity Checking for Local and External Users**, then click **OK**.

31.7 If You Use eDirectory Universal Passwords

If you use Universal Passwords and eDirectory LDAP is not NMAS-aware, users are able to log in to Filr with case-insensitive passwords even though the passwords are actually case sensitive. For example, they can log in with 'novell1!' when their password is 'Novell1!'

In addition to the security concern, when users log in with the incorrect case, they cannot upload any files.

To prevent users from logging in to Filr with an incorrect password, set eDirectory LDAP to be NMAS-aware by following the instructions in this TID (https://www.novell.com/support/kb/doc.php?id=3307424).

31.8 Restricting SSH Access for the Root User

By default, the root user is able to SSH to each appliance in the Filr system. You can disable this access on each appliance so that only the vaadmin user can SSH to the system.

For information about how to disable SSH access for the root user, see Section 2.1, "Changing Administrative Passwords," on page 39.

31.9 Setting Up Filr in a DMZ

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

To provide an additional level of security, you can set up Filr in a DMZ. You might want to consider setting up Filr in a DMZ especially if you are planning to allow external users to access the Filr system (as described in Section 10.1, "Allowing External Users Access to Your Filr Site," on page 123). It is most secure to restrict external user access to Filr appliances that are located in the DMZ, rather than allowing external users access to a Filr appliance behind the internal firewall.

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

Figure 31-1 illustrates a basic setup with Filr running in a DMZ, including information about the ports that you need to open for the firewalls and for communication between the various servers.

Figure 31-1 *Filr in a DMZ*
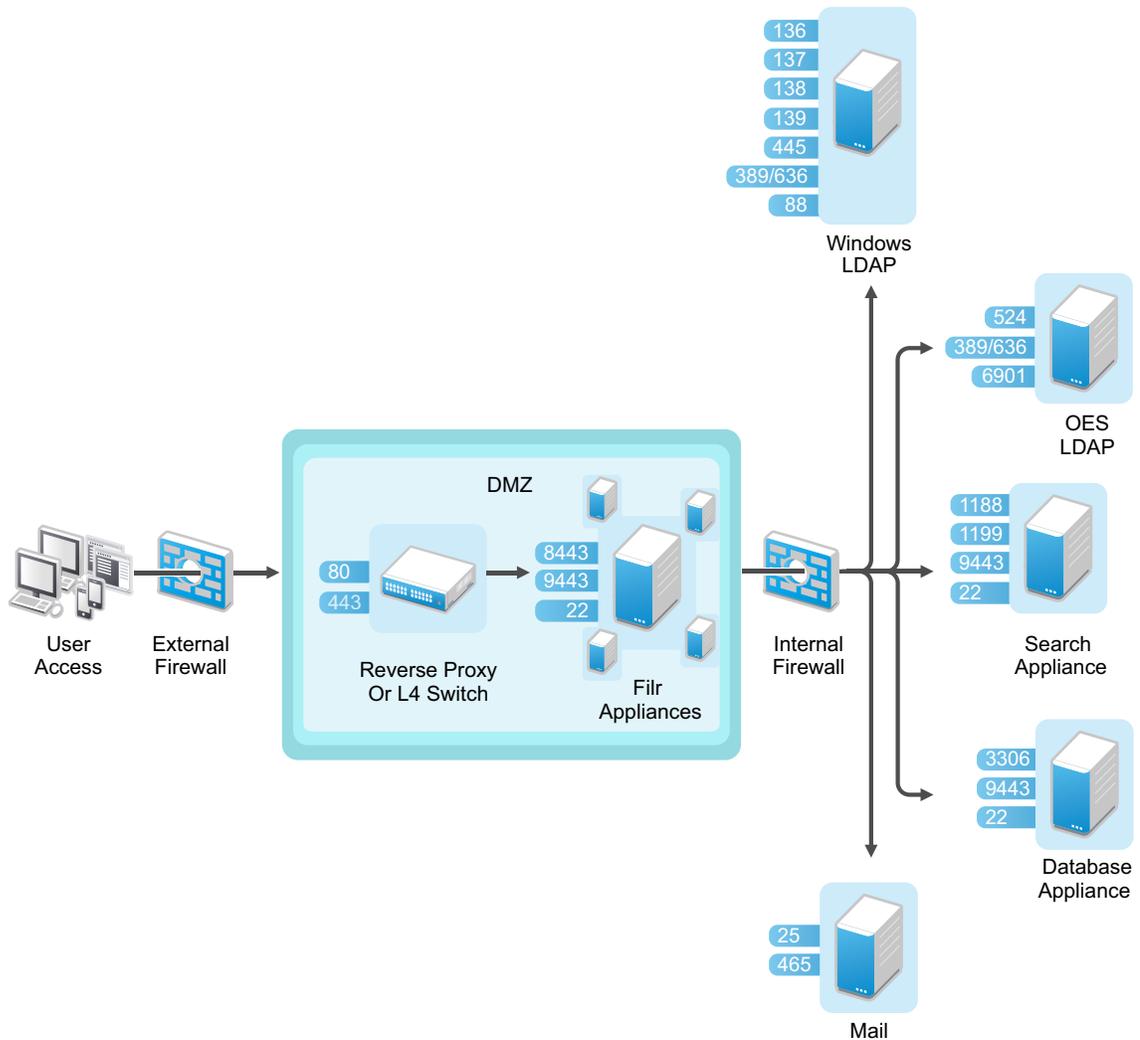
Only traffic destined to the DMZ is allowed through the front-end firewall, and only traffic from the DMZ to the internal network is allowed through the back-end firewall.

In a clustered environment, it is also possible for some of the Filr appliances in the cluster to run behind the internal firewall while others run in the DMZ. Doing so can result in performance benefits for internal users. Setting up Filr in this way requires that you use memcached caching. For more information about configuring memcached caching, see Section 1.7, "Changing Clustering Configuration Settings," on page 28.

For more information about port configuration in Filr, see Section 1.2.2, "Port Numbers," on page 20.

For information about setting up NetIQ Access Manager as a reverse proxy, see Chapter 29, "NetIQ Access Manager," on page 287.

31.10 Filr Component Security

31.10.1 Filr Software Security

The Filr software is a customized version of Apache Tomcat. The version of Apache used for the Filr software contains all security fixes and patches that were available when Filr was released.

31.10.2 Filr Database Security

The Filr database is a MySQL database built with SuSE Studio, and contains all security fixes and patches that were available when Filr was released.

31.10.3 Filr Search Index Security

The Filr search index is a Lucene search index. It contains all security fixes and patches that were available when Filr was released.

32 Security Policies

32.1 Why 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.

32.2 Out of the Box, Filr Is Locked Down

- Client access is only allowed using REST over SSL (HTTPS), using unique self-signed certificates for each instance.
- All access through Filr is turned off by default.
- All Filr sharing is off by default.
- User provisioning can be done via LDAP over SSL (LDAPS).

- Filr supports replacing self-signed certificates with certificates that have been signed by a trusted certificate authority (CA).
- All security-related credentials and passwords are encrypted with unique 2048-bit keys.
- Communication between virtual machines is authenticated and encrypted.

32.3 Securing the Filr Data

32.3.1 Understanding Administrator Access to Filr Data

The Filr administrator can see all files and folders:

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

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

32.3.2 Limiting Physical Access to Filr Servers

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

32.3.3 Protecting the Filr Database

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

Support for this is highly dependent on the database client drivers and JDBC connector support, and on how you are configuring your database client and server certificates. You should check with your database vendor on how to set up SSL connections on both the client and server sides of the connection. You might need to modify the JDBC URL when configuring the Filr appliance, as described in Section 1.4.4, "Database Location in a Small Deployment," on page 25. For example, for MySQL, you might add useSSL=true&requireSSL=true to the options part of the JDBC URL.

32.4 Securing the Filr Site

32.4.1 Configuring a Proxy Server

Your Novell Filr system should be located behind your firewall. If Filr users want to access the Filr site from outside your firewall, you should set up a proxy server outside your firewall to provide access. You can use NetIQ Access Manager to protect your Filr site, as described in Section 1.8, "Changing Reverse Proxy Configuration Settings," on page 28.

32.4.2 Setting the Filr Administrator Password

The Filr site is initially installed to allow administrator access by using the user name `admin` and the password `admin`. The Filr administrator password should be changed immediately after installation, as described in Section 3.2, "Changing the Filr Administrator User ID or Password," on page 52.

32.4.3 Securing the Filr Site against XSS

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, Novell Filr contains a built-in security filter that protects against XSS vulnerabilities. This security filter is enabled by default.

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

- "Understanding What Content Is Not Permitted" on page 309
- "Understanding Where the Content Is Not Permitted" on page 309
- "Listing All XSS Threats in Your System" on page 309

Understanding What Content Is Not Permitted

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

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

Understanding Where the Content Is Not Permitted

The type of content discussed in "Understanding What Content Is Not Permitted" on page 309 is filtered by Filr in the following areas:

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

Listing All XSS Threats in Your System

Filr enables you to run an XSS report that lists XSS threats that are contained in your Filr system. For more information, see Section 28.2.12, "XSS Report," on page 280.

32.5 Securing Filr Data on Mobile Devices

For information about data security for mobile devices, see Section 13.4, "Understanding Filr Data Security for Mobile Devices," on page 164.

32.6 Securing the Filr Desktop Application

For information about data security for the Filr desktop application, see Chapter 14, "Setting Up the Filr Desktop Application," on page 165.

32.7 Certificates

 ◆ All communication with Filr appliances is done using certificates.

 ◆ Self-signed certificates are used by default.

 ◆ You can import your own trusted CA certificates so that clients configured to trust these certificates do not get a certificate warning.

 ◆ Filr appliances use the same certificate for all services on the appliance (VA Admin, Web Application, Apache, Tomcat, Jersey/Jetty).

32.8 Sharing

 ◆ Sharing is turned off by default.

 ◆ Sharing controls must be configured for files in the My Files area (includes users' personal storage and Home directories) and for Net Folders.

   ◆ Sharing for files in the My Files area can be configured on a global level for all users or for individual users or groups.

   ◆ Even if sharing is turned on for a given user or group, it must also be turned on at every Net Folder and for each user for files in their Home folder.

 ◆ My Files vs. Net Folders

   ◆ **My Files:** Filr expects that you want users to be able to share their own files and folders.

     After sharing is enabled at the global level, users can share files and folders in their **My Files** area by default (includes users' personal storage and Home directories).

   ◆ **Net Folders:** Filr expects that you do not want users sharing files in **Net Folders** unless they are specifically authorized to do so.

     Sharing is enabled at the global level for **Net Folders**. However, users cannot share the files in any Net Folder until you specifically turn sharing on for them at the Net Folder level (either individually or as part of a group).

     Folders within Net Folders cannot be shared.

 ◆ Sharing privileges are granular:

   ◆ **Share Internal:** Users can share only with internal users (provisioned and administrator-created local users).

   ◆ **Share External:** Users can share with external users. These are users that have been invited via an email notification to provision themselves as users in Filr based on their email address identity.

- **Share public:** Users can share with the public. No authentication is required. The URL that is shared in public sharing can be forwarded, posted, emailed, tweeted, blogged, and disseminated in any way. Anyone who has that URL can access the shared information.

32.9 Comments

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

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

32.10 LDAP-Provisioned Users and Local Users

- Filr supports authentication using IDs and credentials that are validated with the LDAP identity source from which they were provisioned. The credentials from these LDAP providers are cached within Filr, but they are never really synchronized from the LDAP provider.
- Local users that are not provisioned via LDAP have their local credentials stored in Filr. These credentials are secured, encrypted, and protected.

32.11 Proxy Users

- Filr uses administrator-created proxy users for communicating with LDAP providers and Net Folder servers.
- LDAP proxy users must have sufficient rights to read user and group objects from the desired contexts within LDAP providers.
- Net Folder proxy users must have full rights to the file server volumes or shares that contain the Net Folders.
- Proxy users' identities and credentials are secured, encrypted, and protected in Filr.

32.12 File Servers

- Filr honors and respects all trustee rights, file attributes, and folder attributes on all targeted file systems.
- Filr never changes any rights or attributes on targeted file systems.

- The only time file system rights are effectively bypassed is when a Filr user shares a file or folder with another user. In this case, the proxy user's rights are used on behalf of the user receiving the share.

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

32.13 Audit Trail

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

32.14 Simplified Rights Model

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

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

    IMPORTANT: Folders only, not Files.

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

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

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

32.15 Antivirus

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

32.16 Backup and Restore

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

32.17 NESSUS Scans

- The Filr development team runs NESSUS scans on all Filr code and fixes all reported problems.

  This means that no unexpected ports are open and all open ports are protected according to industry standards.

32.18 Coverity

- The Filr development team runs all Filr code through Coverity.

  Coverity not only checks for memory leaks and possible bugs using stack code analysis techniques, but it also helps developers identify security vulnerabilities, such as buffer over-runs.

32.19 Encryption

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

VI Appendixes

- ◆
- ◆

A Troubleshooting the Filr System

A.1 Unable to Connect to the Filr Site (HTTP 500 Error)

Problem: You see an HTTP 500 error when trying to connect to the Filr site.

To fix this problem, ensure that your DNS server is properly configured and that your Filr server is directed at the proper DNS server.

For information about how to configure Filr to point to your DNS server, see Section 1.2.1, "Changing the Network Configuration Settings," on page 19.

A.2 NetApp Net Folder Server Test Connection Fails

Problem: Clicking the **Test Connection** option when creating a Net Folder Server for a NetApp device causes the following error to be logged in `/var/opt/novell/filr/log/smbclient.log.`: `Could not retrieve case sensitivity flag: NT_STATUS_REVISION MISMATCH`.

NetApp ONTAP versions earlier than 8.3.*x* have only limited support for the SMB v2 protocol. Nevertheless, NetApp sets the default protocol level to SMB v2.

If your NetApp devices are running an ONTAP version earlier than 8.3.*x*, you must set the protocol level to SMB v1. Filr 2.0 will then use SMB v1 for connecting and communicating with the devices.

A.3 Previously Available Files and Folders Disappear

Problem: Filr users (desktop, mobile, and web) are suddenly unable to see files and folders that were previously visible.

This happens when the metadata index no longer contains information for the objects that have disappeared, either because the Search server goes down, or because the index itself changes (for example, during a rebuild).

To understand how the index affects object availability and how to prevent file/folder disappearance, see "Filr Search Appliance—Accessibility, and Searchability" in the *Filr 2.0: Understanding How Filr Works*.

A.4 Email Notification URLs Are Not Working

The network and reverse proxy settings that you configure after installing Filr affect how email notification URLs are constructed. If you have configured port redirection and have failed to verify the reverse proxy ports, email notifications from Filr can be constructed in such a way that users who click on the email notification URL are not able to access the Filr site.

When port redirection is enabled (as described in Section 1.2.1, "Changing the Network Configuration Settings," on page 19), ensure that the reverse proxy ports are set to 80 for the HTTP port and to 443 for the secure HTTP port. For information about how to change the reverse proxy ports, see Section 1.8, "Changing Reverse Proxy Configuration Settings," on page 28.

A.5 eDirectory Users Can Log In But Cannot Upload Files

See Section 31.7, "If You Use eDirectory Universal Passwords," on page 303.

A.6 FAMT Error Codes

When errors occur in the FAMT component of Filr, an error code is displayed. These codes can be helpful for diagnosing problems with FAMT. The following table lists the possible error codes and a brief interpretation.

Error Code	Interpretation
0	FAMT_SUCCESS
1	FAMT_FAILURE
2	FAMT_NO_MEMORY
3	FAMT_OPEN_FILE_FAIL
4	FAMT_GET_FILE_SIZE_FAIL
5	FAMT_READ_FILE_FAIL
6	FAMT_WRITE_FILE_FAIL
7	FAMT_SOCKET_WRITE_FAIL
8	FAMT_LOGIN_FAILED
9	FAMT_GET_FILE_INFO_FAIL
10	FAMT_CREATE_FILE_FAILED
11	FAMT_PATH_NOT_FOUND
12	FAMT_CONFLICT
13	FAMT_SHARING_VIOLATION

Error Code	Interpretation
14	FAMT_ALREADY_EXIST
15	FAMT_NO_CONTENT
16	FAMT_REQUIRED_AUTH
17	FAMT_UNDEFINED_VOLUME
18	FAMT_INVALID_PARAMETERS
19	FAMT_ADD_TRUSTEE_FAILED
20	FAMT_MAP_OBJ_TOID_FAIL
21	FAMT_ACCESS_VIOLATION
22	FAMT_GET_RIGHTS_FAILED
23	FAMT_LOCK_NOT_EXIST
24	FAMT_RESOURCE_BUSY
25	FAMT_DUP_ENTRY
26	FAMT_SERVER_DOWN
27	FAMT_PATH_TOO_LONG
100	FAMT_XML_PARSING_FAILED

A.7 Enabling Debug Logging

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

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

A.7.1 Enabling Debug Logging for Filr

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

1 In a text editor, open the `log4j.properties` file from both of the following directories:

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

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

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

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

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

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

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

A.7.2 Enabling Debug Logging for FAMT

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

Setting Debug Logging for FAMT

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

`/opt/novell/filr/bin`

2 Set the FAMT log level as follows:

`./famtconfig -s loglevel 4`

or

To view the current log level:

`./famtconfig -g loglevel`

Viewing FAMT Log Files

1 Change to the following location on the Filr server:

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

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

Clearing FAMT Log Files

1 Run the following command to clear the log files:

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

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

A.7.3 Configuring Debug Logging for SMB Communications

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

Beginning with Filr 2.0, a log file named `smbclient.log` is available for capturing SMB/CIFS communications with Net Folders on Windows and Novell OES servers (including OES for NSS AD).

The path to the log file is `/var/opt/novell/filr/log/smbclient.log`.

About the smbclient.log File

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

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

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

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

Changing the Debug Level

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

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

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

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

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

3 Save the smb.conf file.

4 Restart famtd by entering the following command:

   `# rcnovell-famtd restart`

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

A.8 Using VACONFIG to Modify Network Information

The easiest way to update the configuration information for the appliance (such as the IP address, host name, and so forth) after Filr is already installed is to use the VACONFIG utility from the appliance command prompt:

1 In the vSphere client, select the Filr appliance, then click the **Console** tab.

2 From the command prompt, log in to the appliance.

3 Type `vaconfig`, then press Enter.

4 In the VACONFIG utility, select **Configure**, then press Enter.

5 Press the Tab key until the IP address is selected, then modify the IP address as desired.

6 Select **Next**, then press Enter.

A.9 Accessing Filr Log Files

You can access log files for Filr, Jetty, Postfix, and Novell FAMT.

1 Log in to the Novell appliance at https://*server_url*:9443.

2 Click **System Services**.

3 In the **Log Files** column of the table, click the **download** link for the service for which you want to view log files.

For more detailed information about these services, see Section 2.7, "Changing System Services Configuration," on page 43.

The following files are available for each service:

Novell Filr: `catalina.out`, `appserver.log` (Filr appliance)

The `catalina.out` file reports all timestamps in UTC/GMT.

Jetty: `jetty.stderrout.log` (Filr, Search, and MySQL database appliances)

Postfix: `mail` (Filr appliance)

Novell FAMT: `famtd.log` (Filr appliance)

Search: `indexserver.log` (Search appliance)

MySQL: `mysqld.log` (MySQL database appliance)

Memcached: `jetty.stderrout.out` (Search appliance)

4 Click **Close** to exit System Services.

B
 Documentation Updates

The following changes have been made to this guide since the initial release of Novell Filr 2.0.

Date	Section	Additional Information
1 April 2016	Section A.2, "NetApp Net Folder Server Test Connection Fails," on page 317.	Title change from Net Folder to Net Folder Server; spelling correction of NetApp in body.
31 March 2016	Table 14-1 on page 174	Removed Default Folder List entry because it is no longer supported with new files-on-demand functionality.
16 March 2016	Section 31.1, "Dealing with Security Scan Results," on page 293	
	"Creating a Word Rewriter Profile for Each Filr Host" on page 148	