Administration Guide

Novell Filr 1.0.1

May 2014

Legal Notices

Novell, Inc.
1800 South Novell Place
Provo, UT 84606
U.S.A.
www.novell.com

Online Documentation: To access the latest online documentation for this and other Novell products, see the Novell Documentation Web page (http://www.novell.com/documentation).

Novell Trademarks

Third-Party Materials

Contents

##

##

##

##

##

About This Guide

The *Novell Filr 1.0 Administration Guide* provides administration information for Novell Filr 1.0.

- Part I, “Site Setup,” on page 11
- Part II, “Site Maintenance,” on page 109
- Part III, “Interoperability,” on page 175
- Part IV, “Site Security,” on page 181
- Appendix A, “Troubleshooting the Filr System,” on page 203
- Appendix B, “Documentation Updates,” on page 207

Audience

This guide is intended for Novell Filr administrators.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation.

Documentation Updates

For the most recent version of the *Novell Filr 1.0 Administration Guide* and other documentation, visit the Novell Filr 1.0 Documentation Web site (http://www.novell.com/documentation/novell-filr1/).

Additional Documentation

You can find more information in the Novell Filr documentation, which is accessible from the Novell Filr 1.0 Documentation Web site (http://www.novell.com/documentation/novell-filr1/).

To access the *Novell Filr 1.0 User Guide* from within Filr, click the *Help* icon (question mark).

I Site Setup

After you have installed and started Novell Filr, there are administrative tasks to perform 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 as the Filr administrator you 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:

1 Logging In as the Filr Site Administrator

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

- Section 1.1, "Logging In," on page 13
- Section 1.2, "Resetting the Filr Administrator Password," on page 14

1.1 Logging In

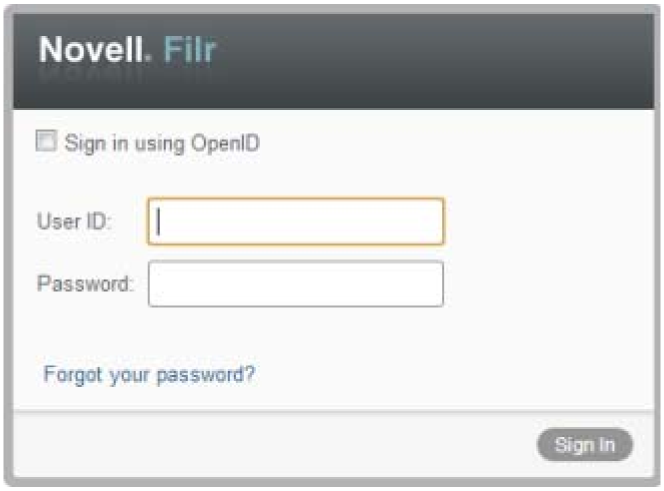
After installing and configuring Filr, you need to log in to the Filr site to perform additional administrative tasks.

1 In your Web browser, specify one of the following URLs, depending on whether or not you are using a secure SSL connection:

```
http://filr_hostname:8443
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 may not be required to enter the port number in the URL, and if you are using NetIQ Access Manager, the Filr login screen is not used. For more information about Filr configurations that affect login, see "Network Configuration" and "Changing Reverse Proxy Configuration Settings" in the *Novell Filr 1.0.1 Installation and Configuration Guide*.



2 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.

1.2 Resetting the Filr Administrator Password

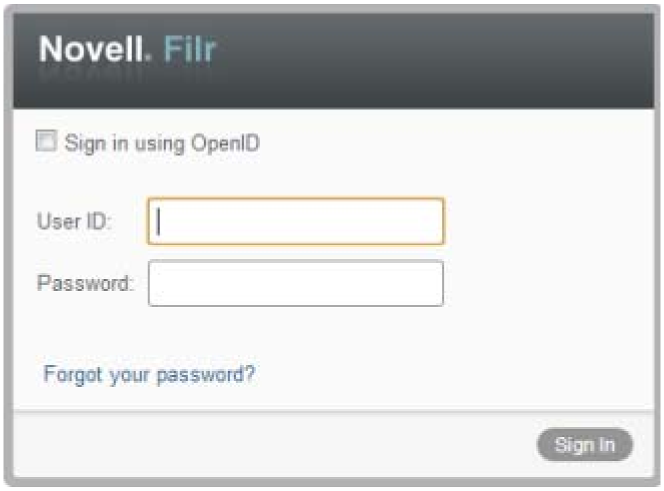
When you first install Novell Filr, the Filr administrator username is `admin` and the password is `admin`. When you first log in to the Filr site as the administrator, you should change the administrator password from the default password to a secure password of your own choosing.

1 In your Web browser, specify one of the following URLs, depending on whether or not you are using a secure SSL connection:

```
http://filr_hostname:8443
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 may not be required to enter the port number in the URL, and if you are using NetIQ Access Manager, the Filr login screen is not used. For more information about Filr configurations that affect login, see “Network Configuration” and “Changing Reverse Proxy Configuration Settings” in the *Novell Filr 1.0.1 Installation and Configuration Guide*.



2 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 Change the default administrator password to a secure password.

In the Change Password dialog box, type the `admin` in the *Current password* field, then go to the *New password* and *Confirm new password* fields and specify a new password.

2 Configuring Email Integration

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. 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 File” in “Getting Informed” in the *Novell Filr 1.0.1 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 *Novell Filr 1.0.1 Web Application User Guide*.
- Filr users can send email messages to folder contributors, as described in “Sending an Email to Folder Contributors” in the *Novell Filr 1.0.1 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 *Novell Filr 1.0.1 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 18, “Managing Email Configuration,” on page 147.

2.1 Configuring Outbound Email

During the configuration of the Filr appliance, you configured Novell Filr to communicate with your email system, as described in “Changing Outbound Email Configuration Settings” in the *Novell Filr 1.0.1 Installation and Configuration Guide*. 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 File” in the *Novell Filr 1.0.1 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 or not you are using a secure SSL connection:

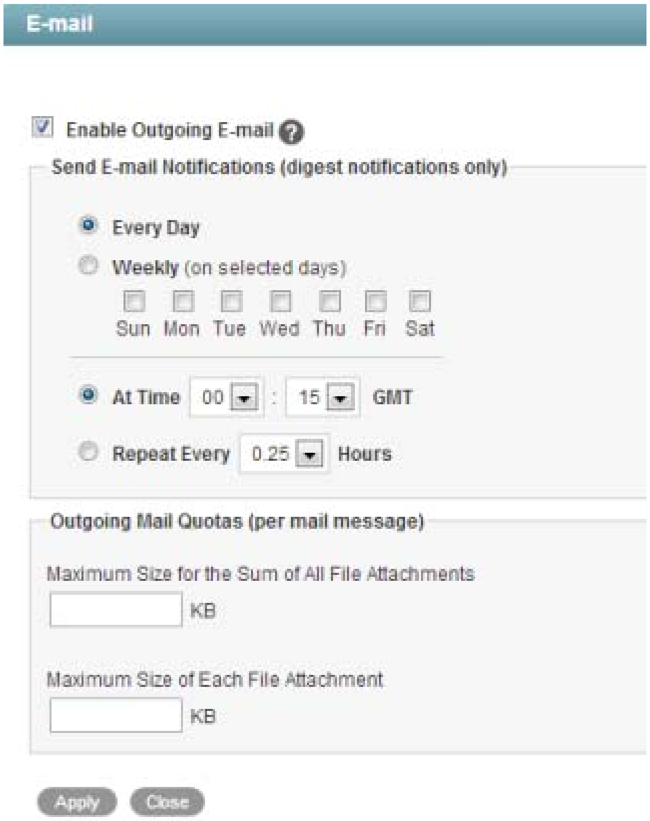
```
http://filr_hostname:8443
https://filr_hostname:8443
```

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 may not be required to enter the port number in the URL, and 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*.



E-mail

☑ Enable Outgoing E-mail

Send E-mail Notifications (digest notifications only)

● Every Day

○ Weekly (on selected days)

□ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat

● At Time 00 : 15 GMT

○ Repeat Every 0.25 Hours

Outgoing Mail Quotas (per mail message)

Maximum Size for the Sum of All File Attachments

KB

Maximum Size of Each File Attachment

KB

4 Select *Enable Outgoing Email*.

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

5 In the *Send E-mail Notifications* section, 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 File" in the *Novell Filr 1.0.1 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 *Novell Filr 1.0.1 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.

6 (Optional) To set a data quota on outgoing mail messages, 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.

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

For information about the options that users have for receiving email notifications, see “Subscribing to a Folder or File” in “Getting Informed” in the *Novell Filr 1.0.1 Web Application User Guide*.

3 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.

- Section 3.1, “Understanding Sharing,” on page 19
- Section 3.2, “Enabling Users to Share,” on page 21
- Section 3.3, “Managing Shares,” on page 24

3.1 Understanding Sharing

Sharing in Filr enables users to grant access to files and folders to other users, either internal or external to the organization. You can enable users to share the following kinds of files and folders:

- Files and folders in users’ My Files areas. This includes files and folders in users’ personal storage (if personal storage has been enabled, as described in Chapter 4, “Setting Up Personal Storage,” on page 27) and in users’ Home directories.

  Sharing of files and folders in the My Files area is enabled by default for all users after sharing is enabled for the site. You can disable sharing for files and folders in the My Files area on an individual user basis.
- Files in Net Folders (files in Net Folders are files that are synchronized to Filr from a corporate file system and that are located in the *Net Folders* tab in Filr.)

  Sharing of files in Net Folders is disabled by default after sharing is enabled for the site. You must enable sharing for each Net Folder and specify which users are allowed to share and what rights they have.

  The ability to share folders from Net Folders is not available.

If multiple users share the same item with a single user, the user who receives the share is granted the highest level of access that was shared with the user. For example, if User B shares a file with User A and that grants User A Read rights to the file, then User C shares the same file with User A and grants Read and Write rights to the file, User A has Read and Write rights to the file.

The following sections describe how sharing works in conjunction with Filr rights and file system rights. For more detailed information about how sharing works in Filr, see “Sharing through Filr” in the *How Filr Works–Overview Guide*.

- Section 3.1.1, “Users Can’t Grant Share Roles That They Don’t Have,” on page 19
- Section 3.1.2, “File System Rights Also Affect the Ability to Assign Share Roles,” on page 20

3.1.1 Users Can’t Grant Share Roles That They Don’t Have

Users with Contributor rights on folders can grant Viewer, Editor, and Contributor rights to other users as Filr system share and Net Folder share settings allow.

On the other hand, Users with Viewer rights on folders can only grant Viewer rights to other users with whom they are allowed to share.

3.1.2 File System Rights Also Affect the Ability to Assign Share Roles

Sharing of files and directories involves an additional layer that provides access and manages what those who are granted rights to share files can actually do.

For users to grant Viewer, Editor, or Contributor rights to another user, they must have the minimum rights that those roles require, as outlined in the following tables.

Table 3-1 *NSS File System Rights and Filr Roles*

Role	Minimum NSS Rights Required	Comments
Viewer	Read (R), File Scan (F)	These are the minimum file system trustee rights that users must have to view files and folders.
Editor	Read (R), Write (W), File Scan (F)	If the Write file system trustee right is added to Read and File Scan, users can then modify file content.
Contributor	Read (R), Write (W), Erase (E), Create (C), Modify, File Scan (F) or Supervisor	To perform contributor functions, 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 3-2 *NTFS Permissions and Filr Roles*

Role	Minimum NTFS Permissions Required	Comments
Viewer	`Read`, `Read & Execute`, `List Folder Content`	These are the minimum basic permissions that users must have in order to view files and folders. The default special permissions associated with these basic permissions are also required.
Editor	`Read`, `Read & Execute`, `List Folder Content`, `Write`	If the basic `Write` permission is added, users can then modify file content. The default special permissions associated with these basic permissions are also required.

Contributor	`Read`, `Read & Execute`, `List Folder Content`, `Write`, `Modify`
	or
	`Full Control`
		To perform contributor functions, users must either have the basic `Modify` permission added or they must have the basic `Full Control` permission. The default special permissions associated with these basic permissions are also required.

3.2 Enabling Users to Share

IMPORTANT: You must enable the sharing feature before any sharing can take place on the Filr system. After you enable the sharing feature, 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). You can then refine sharing rights on a user basis and set up sharing on individual Net Folders.

When you enable the sharing feature, it is best to keep the share rights fairly unrestricted (for example, give the All Internal Users group the ability to share whatever they want). You can then restrict sharing of files in the My Files area on a per-user basis, and in the Net Folder configuration, you can set the share rights to be more granular (for example, only Groups A and Groups B can share files from the Net Folder).

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 3.2.1, “Enabling Sharing for the Entire Site,” on page 22)
2. Configure sharing for individual users (as described in Section 3.2.2, “Restricting Share Rights on a User Basis,” on page 23)

   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 3.2.3, “Enabling Sharing for Specific Net Folders,” on page 24)

   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.

- Section 3.2.1, “Enabling Sharing for the Entire Site,” on page 22
- Section 3.2.2, “Restricting Share Rights on a User Basis,” on page 23
- Section 3.2.3, “Enabling Sharing for Specific Net Folders,” on page 24

3.2.1 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 restrict sharing privileges at the user level, as described in Section 3.2.2, “Restricting Share Rights on a User Basis,” on page 23.

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 or not you are using a secure SSL connection:

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

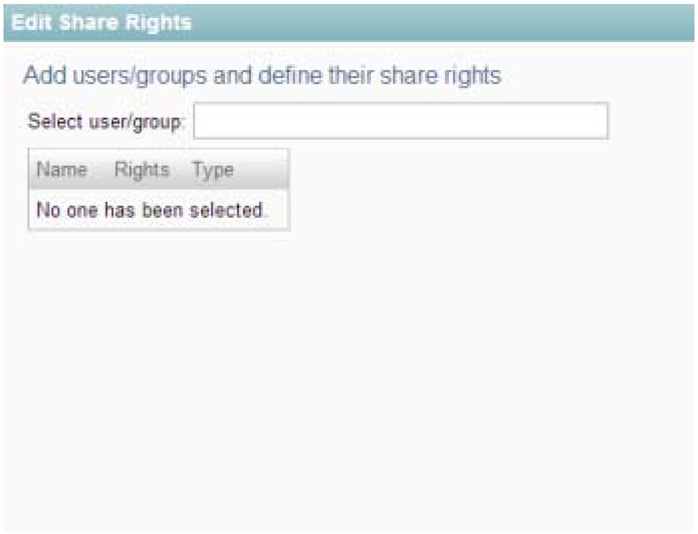
Replace *filr_hostname* with the hostname or fully qualified domain name of the Filr server that you have set up in DNS.

Depending on how you have configured your Filr system, you may not be required to enter the port number in the URL, and 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 Edit Share Rights page is displayed.



Edit Share Rights

Add users/groups and define their share rights

Select user/group:

Name	Rights	Type
No one has been selected		

4 To enable sharing for all internal users on the Filr site, go to the *Select user/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.

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.

In addition to selecting this option, you might also want to allow external users to access the Filr site with an OpenID account (Google or Yahoo), as described in Section 6.3.2, "Allowing Users to Access the Filr Site with Google and Yahoo Accounts (OpenID)," on page 63. If you do not allow this, external users must create a Filr user account in order to see items that have been shared with them.

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 *Novell Filr 1.0.1 Web Application User Guide*.

Share with the 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 6.3.1, "Allowing Guest Access to Your Filr Site," on page 61.

5 Click *OK* > *OK*.

3.2.2 Restricting Share Rights on a User Basis

After you have enabled sharing of files for the entire Filr system (as described in Section 3.2.1, "Enabling Sharing for the Entire Site," on page 22), you can restrict share rights throughout the site on the user level.

You cannot grant individual users more rights than 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 or not you are using a secure SSL connection:

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

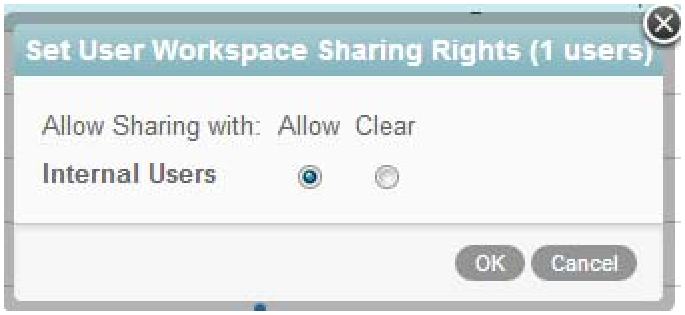
Replace `filr_hostname` with the hostname or fully qualified domain name of the Filr server that you have set up in DNS.

Depending on how you have configured your Filr system, you may not be required to enter the port number in the URL, and 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 Select the users whose sharing rights you want to manage, then click *More* > *Workspace Share Rights*.



Set User Workspace Sharing Rights (1 users)

Allow Sharing with:	Allow	Clear
Internal Users	●	○

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*.

3.2.3 Enabling Sharing for Specific Net Folders

1 Ensure that you have configured sharing as described in Section 3.2.1, “Enabling Sharing for the Entire Site,” on page 22.

2 Configure sharing for the Net Folder as described in Section 5.4, “Creating and Managing Net Folders,” on page 45 or Section 5.7, “Modifying Net Folder Connections,” on page 54 (depending on whether the Net Folder has already been created).

3.3 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 3.3.1, “Managing Shares for the Filr Site,” on page 25
- Section 3.3.2, “Managing Individual Shares,” on page 25

3.3.1 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 or not you are using a secure SSL connection:

```
http://filr_hostname:8443
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 may not be required to enter the port number in the URL, and 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 *Manage 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 username 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 filename 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. 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" in the *Novell Filr 1.0.1 Web Application User Guide*.

6 (Optional) Delete a shared item by clicking the x icon next to the share that you want to remove.

7 Click *OK*.

3.3.2 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*.

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” in the *Novell Filr 1.0.1 Web Application User Guide*.

3. (Optional) Delete a shared item by clicking the x icon next to the share that you want to remove.
4. Click *OK*.

4 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 14.2, "Creating a New Local User," on page 118) always have access to personal storage in the My Files area. Guest users who do not have a Filr user account and external users never have access to 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 *Novell Filr 1.0.1 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 *Novell Filr 1.0.1 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 you easy access to folders and files on your corporate file system. Corporate files can be files on your home drive, files on a mapped drive, or files on a remote server. Filr gives you seamless access to these files, regardless of their location. The corporate files that you have access to are defined by the Filr administrator.

  In Filr, you access these corporate files by clicking *Net Folders* in the masthead. For more information about Net Folders, see the *Novell Filr 1.0.1 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 4.1, "Understanding How Personal Storage Relates to Home Folders," on page 27
- Section 4.2, "Enabling Personal Storage for All Users," on page 28
- Section 4.3, "Enabling Personal Storage for Individual Users," on page 28

4.1 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 5.2, "Configuring Home Folders for Display in the My Files Area," on page 39.)

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 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.

4.2 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 or not you are using a secure SSL connection:

```
http://filr_hostname:8443
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 may not be required to enter the port number in the URL, and 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 users to have personal storage*, depending on whether you want users whose accounts are synchronized via LDAP to have access to the My Files area.

5 Click *OK*.

4.3 Enabling Personal Storage 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 or not you are using a secure SSL connection:

```
http://filr_hostname:8443
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 may not be required to enter the port number in the URL, and if you are using NetIQ Access Manager, the Filr login screen is not used.

2. In Filr, click the *admin* link in the upper right corner of the page, then click the *Administration Console* icon 👤.
3. Under *Management*, click *User Accounts*.

   The Manage Users page is displayed.
4. 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 *User Accounts*.

   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 *User Accounts*.

   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 global setting, then click *More > Use Global Personal Storage Setting*.

5 Setting Up Net Folders

Net Folders in Filr provide access to files on your corporate OES, Windows, or NetWare 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 5.1, “Planning Net Folder Creation,” on page 31.

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

🎬 http://www.youtube.com/watch?v=ZRNECA3iKtA

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

5.1 Planning Net Folder Creation

5.1.1 Understanding Known Issues

You should be aware of any known issues regarding Net Folders. For more information, see "Net Folder Issues (http://www.novell.com/documentation/novell-filr1/filr1_readme_novell/data/filr1_readme_novell.html#b1383h6s)" in the Novell Filr Readme (http://www.novell.com/documentation/novell-filr1/filr1_readme_novell/data/filr1_readme_novell.html).

5.1.2 Planning the Net Folder Server Proxy User

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.

- "Purpose of the Net Folder Server Proxy User" on page 32
- "Rights Requirements for the Proxy User" on page 32
- "Expected Name Format for Windows, OES, and NetWare File Servers" on page 33
- "Special Character Restrictions in Proxy Names" on page 33

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, Windows, or NetWare 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.

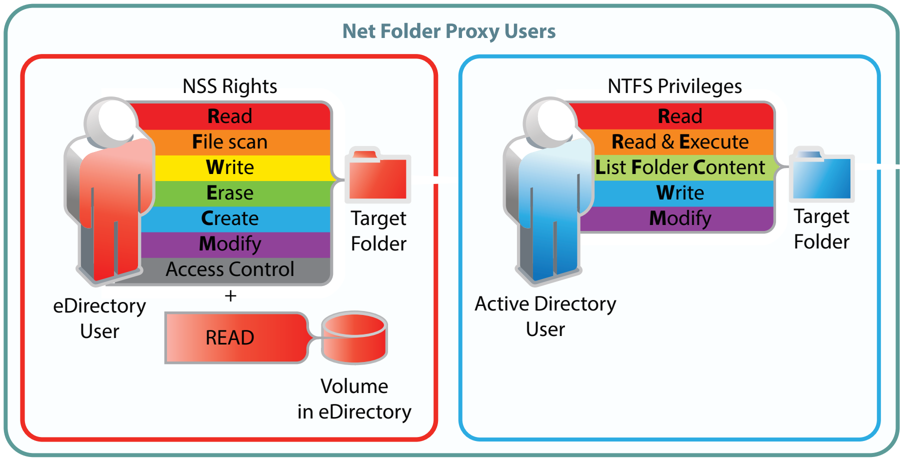
Users with native rights to files do not use the Net Folder Server proxy user.

The Net Folder Server proxy user is not the same as the LDAP proxy user used to synchronize users and groups (as described in "User DN (Proxy User for Synchronizing Users and Groups)" on page 113).

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 5-1 Net Folder Server Proxy User Rights Requirements



Expected Name Format for Windows, OES, and NetWare File Servers

The expected format for the name of the Net Folder Server proxy user differs depending on whether the proxy user is accessing an OES, Windows, or NetWare file server. Only the following syntax is supported:

OES/NetWare: `cn=admin,o=context`

Windows: `Administrator` or `cn=Administrator,cn=users,dc=domain,dc=com, domain\user, user@domain`

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

Special Character Restrictions in Proxy Names

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

5.1.3 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 34
- "Understanding Sharing Rights for Net Folders" on page 34

Understanding Access Rights for Net Folders

When you configure a Net Folder, users who already have file system rights to files and folders in the Net Folder 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 14.1, “Synchronizing Users and Groups from an LDAP Directory,” on page 111)
- 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 14.1, “Synchronizing Users and Groups from an LDAP Directory,” on page 111)
- The users are given access rights within the Net Folder, either individually or as part of a group in Filr (as described in Section 5.4, “Creating and Managing Net Folders,” on page 45)

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 who receive a share for a Net Folder might or might not have file system rights to the shared file or folder. Whether they have file system rights to the shared item affects how they can access the item in Filr. Users who do not have file system rights to a shared item can gain access to the item via the Net Folder Server proxy user. (For more information about the Net Folder proxy user, see Section 5.1.2, “Planning the Net Folder Server Proxy User,” on page 32.)

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.

5.1.4 Planning the Synchronization Method

When you synchronize files in Net Folders, only file metadata is synchronized. Whether or not the content of files is brought into Filr is determined by the index settings that you choose when creating a Net Folder, as described in Section 5.4, “Creating and Managing Net Folders,” on page 45. Files must be synchronized before they can be indexed.

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 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 all files from a given Net Folder either at a schedule that you specify 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, it is more time-consuming and resource-intensive than Just-in-Time synchronization.

For information about the time required to perform a full synchronization on a Net Folder, see Section 5.1.7, "Planning the Amount of Data to Synchronize," on page 38.

Just-in-Time synchronization: Synchronizes individual files at the time users access the files. Only files that are accessed are synchronized.

Just-in-Time synchronization 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 access them via the Filr Web application or via the Filr mobile app. This means that data users access through Filr is more accurate and processes to make the data available are less resource-intensive. However, this also means that files cannot be indexed (and therefore are not returned in searches and are not available to be synchronized via the Filr desktop application) until after users access them for the first time from the Filr Web application or from the mobile app. (For more information, see "Searchability of Data" on page 36 and "Usage of the Filr Desktop Application" on page 37.)

Just-in-Time synchronization provides two key benefits:

- Allows you to make files available to your users without needing to wait for all files within a given Net Folder to synchronize. Only those files that users want access to are synchronized. A file is synchronized to Filr at the time the user accesses the file within Filr.
- Users do not have to wait for files to synchronize based on the Net Folder synchronization schedule (which by default is every 15 minutes). Now 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.

For more detailed information about Just-in-Time synchronization, as well as how to enable it, see Section 5.6, "Enabling Just-in-Time Synchronization," on page 51.

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 5-1 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 5-1** Full Sync vs. Just-in-Time Sync*

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

- "Static versus Dynamic Data" on page 36
- "The Amount of Data" on page 36
- "Searchability of Data" on page 36
- "Usage of the Filr Desktop Application" on page 37

Static versus Dynamic Data

Whether or not 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, then use Just-in-Time synchronization thereafter.

Searchability of Data

Whether or not you want data to be immediately searchable might influence the type of synchronization method that you implement for the Net Folder because data cannot be indexed (and therefore is not returned in searches) until after the data 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 on a per-file basis only after a user accesses a file for the first time. After a file is accessed for the first time, the file is synchronized and is then 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, as described in Section 5.4, “Creating and Managing Net Folders,” on page 45.

Usage of the Filr Desktop Application

The Filr desktop application triggers Just-in-Time synchronization only for the top-level folder that the user has chosen to synchronize (not the entire folder tree), and it is triggered only when Personal Storage has been disabled. For all sub-folders, files must already be synchronized and accessible via the Filr web interface.

If your users are using the Filr desktop application, it is best to run one manual synchronization and/or enable the scheduled synchronization of the Net Folder or Net Folder Server. If you don't, the Filr desktop application might not download all of the files in the Net Folder.

5.1.5 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 5.1.4, "Planning the Synchronization Method," on page 34).
- 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 5-2, "Net Folder Synchronization Example," on page 38 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.

5.1.6 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 49.)

For more information about how to configure clustering, see "Planning a Multi-Server (Clustered) Filr Configuration" in the *Novell Filr 1.0.1 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 *Novell Filr 1.0.1 Installation and Configuration Guide*.

5.1.7 Planning the Amount of Data to Synchronize

The time required to perform a full synchronization on a Net Folder varies depending on many factors. Among those factors include:

- 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

For example, the time required to index a single Net Folder in a large Filr deployment (one Filr appliance, one database appliance, and one search index appliance) with no indexing, no active users, and no Just-in-Time synchronization is shown in the following table:

***Table 5-2** Net Folder Synchronization Example*

	Number of Files Synchronized per Minute	**Number of Files Synchronized per Hour**	**Number of Files Synchronized per Day**
Initial Synchronization:	700	42,000	1,008,000
Ongoing Synchronization:	2,300	138,000	3,312,000

5.1.8 Planning the Number of Net Folders

Depending on the number of files that exist in a volume or share on a file server, it is likely 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 5.1.4, "Planning the Synchronization Method," on page 34.)

5.1.9 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 *Novell Filr 1.0.1 Installation and Configuration Guide*.

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

5.2 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 14.1, "Synchronizing Users and Groups from an LDAP Directory," on page 111.) 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 5.2.1, "Configuring Home Folders," on page 39
- Section 5.2.2, "Editing Home Folders for Individual Users," on page 40
- Section 5.2.3, "Understanding How Home Folders Relates to Personal Storage," on page 41

5.2.1 Configuring Home Folders

- "Prerequisites" on page 39
- "Configuring Home Folders" on page 40

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 14.1, “Synchronizing Users and Groups from an LDAP Directory,” on page 111.

2 Configure the Net Folder Server, as described in Section 5.3, “Configuring and Managing Net Folder Servers,” on page 41.

> **IMPORTANT:** The Filr administrator must supply proper proxy account information for a Net Folder Server before any end user logs in to Filr. This is because Filr automatically creates 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. If you do not supply the proxy account information before the user logs in, the Home directories are not created correctly and the internal log files contain Null Pointer Exceptions.

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

Whether or not 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 4, “Setting Up Personal Storage,” on page 27.

> **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.

5.2.2 Editing Home Folders for Individual Users

After Home folders have been configured as described in Section 5.2.1, “Configuring Home Folders,” on page 39, 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 or not you are using a secure SSL connection:

```
http://filr_hostname:8443
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 may not be required to enter the port number in the URL, and 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 5.2.1, “Configuring Home Folders,” on page 39.)

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 5.4, “Creating and Managing Net Folders,” on page 45.

7 Click *OK* to save your changes.

5.2.3 Understanding How Home Folders Relates to Personal Storage

For information about how Home folders relate to Personal storage in Filr, see Section 4.1, “Understanding How Personal Storage Relates to Home Folders,” on page 27.

5.3 Configuring and Managing Net Folder Servers

- Section 5.3.1, “Configuring Net Folder Servers,” on page 41
- Section 5.3.2, “Managing Net Folder Servers,” on page 43

5.3.1 Configuring Net Folder Servers

Net Folder Servers represent a physical OES or Windows file server. Net Folder Servers are connections to specific volumes (on OES servers) and shares (on Windows 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 or not you are using a secure SSL connection:

```
http://filr_hostname:8443
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 may not be required to enter the port number in the URL, and 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*.

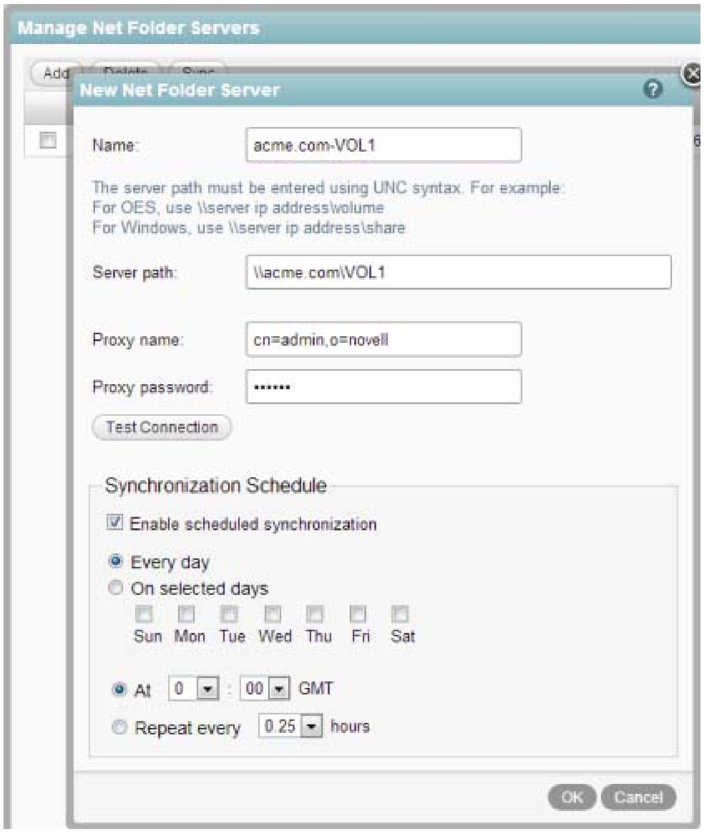
The Manage Net Folder Servers page is displayed.

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 14.1, “Synchronizing Users and Groups from an LDAP Directory,” on page 111.)

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 Section 14.1, “Synchronizing Users and Groups from an LDAP Directory,” on page 111.

To manually add a new Net Folder Server, click *Add*, then continue with Step 6.



Name: acme.com-VOL1

The server path must be entered using UNC syntax. For example:
For OES, use \\server ip address\volume
For Windows, use \\server ip address\share

Server path: \\acme.com\VOL1

Proxy name: cn=admin,o=novell

Proxy password: ••••••

Synchronization Schedule

☑ Enable scheduled synchronization

● Every day
○ On selected days
□ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat

● At 0 : 00 GMT
○ Repeat every 0.25 hours

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. 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 path: The path to the OES or Windows server.

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

The server path must be entered using UNC syntax. For example, for OES, use `\\`*`server_DNS`*`\`*`volume`*. For Windows, use `\\`*`server_DNS`*`\`*`share`*.

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.

Proxy name and password: Specify the fully qualified, comma-delimited name and password for the proxy user used to access the OES or Windows server.

IMPORTANT: Before you specify a proxy name and password for the Net Folder server, ensure that you review the information in Section 5.1.2, “Planning the Net Folder Server Proxy User,” on page 32.

Test connection: Click this button to make sure 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 "Expected Name Format for Windows, OES, and NetWare File Servers" on page 33.

Synchronization Schedule: 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 5.1.4, "Planning the Synchronization Method," on page 34). 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 5.1.5, "Planning the Synchronization Schedule," on page 37.

7 Click *OK* > *Close*.

8 For Home folders to be displayed in the My Files area for each user, ensure that you have completed the steps in Chapter 4, "Setting Up Personal Storage," on page 27.

5.3.2 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 43
- "Synchronizing a Net Folder Server" on page 44
- "Deleting a Net Folder Server" on page 44

Modifying a 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 or not you are using a secure SSL connection:

```
http://filr_hostname:8443
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 may not be required to enter the port number in the URL, and 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*.

Synchronizing a Net Folder Server

When you create a Net Folder Server, you can enable a synchronization schedule, as described in Section 5.3.1, “Configuring Net Folder Servers,” on page 41.

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 or not you are using a secure SSL connection:

```
http://filr_hostname:8443
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 may not be required to enter the port number in the URL, and 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 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 or not you are using a secure SSL connection:

```
http://filr_hostname:8443
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 may not be required to enter the port number in the URL, and 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*.

5.4 Creating and Managing Net Folders

Net Folders are connections to specific directories on OES and Windows servers. 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 5.4.1, “Creating Net Folders,” on page 45
- Section 5.4.2, “Managing Net Folders,” on page 48

5.4.1 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 5.3, “Configuring and Managing Net Folder Servers,” on page 41.

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 or not you are using a secure SSL connection:

```
http://filr_hostname:8443
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 may not be required to enter the port number in the URL, and if you are using NetIQ Access Manager, the Filr login screen is not used.

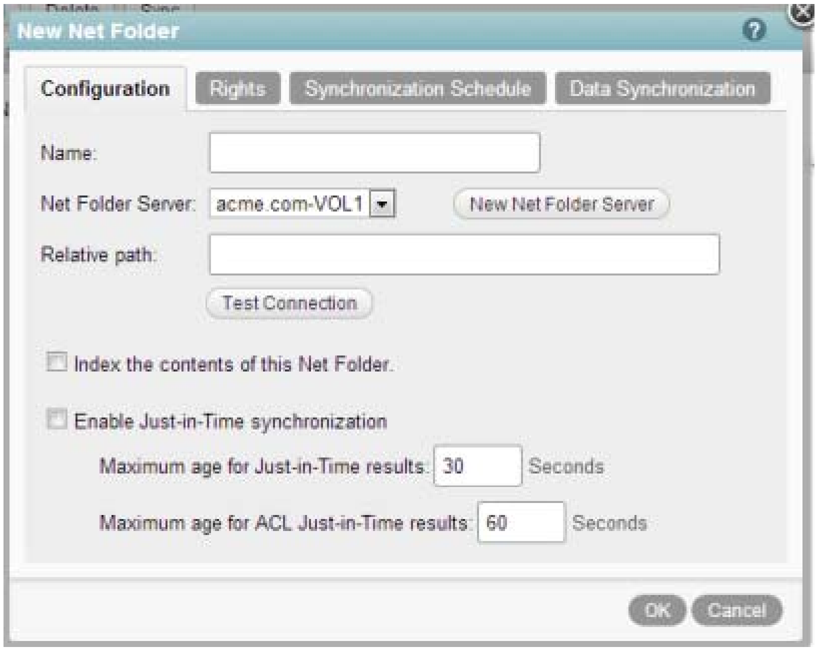
2 Click the *admin* link in the upper right corner of the page, then click the *Administration Console* icon .

3 Under *Management*, click *Net Folders*.

The Manage Net Folders page is displayed.

4 Click *Add*.

The New Net Folder dialog box is displayed.



Name:

Net Folder Server: acme.com-VOL1

Relative path:

□ Index the contents of this Net Folder.

□ Enable Just-in-Time synchronization

Maximum age for Just-in-Time results: 30 Seconds

Maximum age for ACL Just-in-Time results: 60 Seconds

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 5.3, “Configuring and Managing Net Folder Servers,” on page 41.

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.

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.

Test connection: Click this option to test the connection to the 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. 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.

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.

If indexing is turned on, you should monitor the Filr boot partition to ensure that adequate disk space continues to be available. (For information about how to use Ganglia to monitor disk space, see Section 21.1, “Monitoring Filr Performance with Ganglia,” on page 157.)

Files must first be synchronized to Filr before the indexing process can begin. For more information about the synchronization process, see Section 5.1.4, “Planning the Synchronization Method,” on page 34.

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.

There are various options for synchronizing files from a Net Folder. Before you decide on a synchronization method for a Net Folder, see Section 5.1.4, “Planning the Synchronization Method,” on page 34.

If the Net Folder you are creating contains terabytes of data, the indexing process can be lengthy if this option is selected.

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.

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.

   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 5.1.2, “Planning the Net Folder Server Proxy User,” on page 32.)

   For more information, see Section 5.1.3, “Planning Access and Sharing for Net Folders,” on page 33.

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 5.1.2, “Planning the Net Folder Server Proxy User,” on page 32.)

   For more information, see Section 5.1.3, “Planning Access and Sharing for Net Folders,” on page 33.

9. Click *OK* to save your rights changes.

10. (Optional) Click the *Synchronization Schedule* tab to create a schedule for the Net Folder synchronization. This is the synchronization between Filr and the file system server.

    Synchronizations can be scheduled only if you have configured the Net Folder to use Full Synchronization as the synchronization method (as described in Section 5.1.4, “Planning the Synchronization Method,” on page 34). 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 5.1.5, "Planning the Synchronization Schedule," on page 37.

If you already set a synchronization schedule for the Net Folder Server (as described in Section 5.3, "Configuring and Managing Net Folder Servers," on page 41), you can leave this section blank to use the Net Folder Server synchronization schedule. 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.

To set a synchronization schedule for the Net Folder:

10a Select *Enable scheduled synchronization*.

10b Select from the following synchronization options for synchronizing files between the Net Folder and the Filr site:

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.

Desktop application: If this option is selected, users can 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-filr1/filr1_qs_desktop/data/filr1_qs_desktop.html), or the Filr Desktop Application for Mac Quick Start (http://www.novell.com/documentation/novell-filr1/filr1_qs_desktopmac/data/filr1_qs_desktop.html).)

How Filr is set up to synchronize with Net Folders can affect how quickly files from the Net Folder are available to the Filr desktop application. For specific information, see "Usage of the Filr Desktop Application" on page 37 in Section 5.1.4, "Planning the Synchronization Method," on page 34.

12 Click *OK* to finish creating the Net Folder.

5.4.2 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 48
- "Synchronizing a Net Folder" on page 49
- "Deleting a Net Folder" on page 50

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 or not you are using a secure SSL connection:

```
http://filr_hostname:8443
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 may not be required to enter the port number in the URL, and 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.

5 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 5.4.1, “Creating Net Folders,” on page 45.

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 or not you are using a secure SSL connection:

```
http://filr_hostname:8443
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 may not be required to enter the port number in the URL, and 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 *Novell Filr 1.0.1 Installation and Configuration Guide*.)

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 or not you are using a secure SSL connection:

  ```
  http://filr_hostname:8443
  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 may not be required to enter the port number in the URL, and 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*.

5.5 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 3, "Setting Up Sharing," on page 19.
- 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 5.4, "Creating and Managing Net Folders," on page 45 and Section 5.7, "Modifying Net Folder Connections," on page 54.

  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 moved or renamed 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.

5.6 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 5.1.4, “Planning the Synchronization Method,” on page 34.

Just-in-Time synchronization 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 access them via the Filr Web application or via the Filr mobile app. This means that data users access through Filr is more accurate and processes to make the data available are less resource-intensive. However, this also means that files cannot be indexed (and therefore are not returned in searches and are not available to be synchronized via the Filr desktop application) until after users access them for the first time from the Filr Web application or from the mobile app. (For more information, see “Searchability of Data” on page 36 and “Usage of the Filr Desktop Application” on page 37.)

Just-in-Time synchronization provides two key benefits:

- Allows you to make files available to your users without needing to wait for all files within a given Net Folder to synchronize. Only those files that users want access to are synchronized. A file is synchronized to Filr at the time the user accesses the file within Filr.
- Users do not have to wait for files to synchronize based on the Net Folder synchronization schedule (which by default is every 15 minutes). Now 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 for the Filr system before you can enable Just-in-Time synchronization for individual Net Folders.

- Section 5.6.1, “Enabling Just-in-Time Synchronization for the Filr System,” on page 51
- Section 5.6.2, “Enabling Just-in-Time Synchronization for a Specific Net Folder,” on page 52
- Section 5.6.3, “Enabling Just-in-Time Synchronization for a Specific User’s Home Directory,” on page 53

5.6.1 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 or not you are using a secure SSL connection:

```
http://filr_hostname:8443
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 may not be required to enter the port number in the URL, and 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 *Just-In-Time Sync*.

The Just-In-Time sync page is displayed.

The following options are available:

Enable Just-in-Time synchronization for net folders: Select this option to allow Just-in-Time synchronization to be enabled for Net Folders in your Filr system.

Maximum wait time for results (in seconds): When a user clicks on a folder, the Just-in-Time operation retrieves the information 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 15 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 5.6.2, "Enabling Just-in-Time Synchronization for a Specific Net Folder," on page 52.

5.6.2 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 5.6.1, "Enabling Just-in-Time Synchronization for the Filr System," on page 51.

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 or not you are using a secure SSL connection:

```
http://filr_hostname:8443
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 may not be required to enter the port number in the URL, and 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 *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.

6 Click *OK* to save your changes.

5.6.3 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 5.6.1, "Enabling Just-in-Time Synchronization for the Filr System," on page 51.

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 or not you are using a secure SSL connection:

```
http://filr_hostname:8443
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 may not be required to enter the port number in the URL, and 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 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.

4 Under *Settings*, click *User Accounts*.

5 Click *Edit Home Folder*. (This option is displayed only if a Home folder has been configured for the user, as described in Section 5.2.1, "Configuring Home Folders," on page 39.)

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.

5.7 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 or not you are using a secure SSL connection:

```
http://filr_hostname:8443
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 may not be required to enter the port number in the URL, and 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 5.4, “Creating and Managing Net Folders,” on page 45.

5 Click *OK* to save your changes.

6 Setting Up User Access to the Filr Site

6.1 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 14.1, “Synchronizing Users and Groups from an LDAP Directory,” on page 111.
- Manually adding local users, as described in Section 6.1, “Adding New Users to Your Filr Site,” on page 55.
- Importing profile files for local users, as described in Section 14.8, “Managing Local Users and Groups by Importing Profile Files,” on page 125.

6.2 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 14.1, “Synchronizing Users and Groups from an LDAP Directory,” on page 111.

You can use existing groups or create additional groups within Filr to facilitate sharing on your Filr site. For background information on sharing, see Chapter 3, “Setting Up Sharing,” on page 19.

In addition to creating groups to assist with sharing, you might want to create groups for any of the following reasons:

- To facilitate managing data quotas, as described in Section 17.2, “Managing User Data Quotas,” on page 132.

You can create either static or dynamic groups.

6.2.1 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 14.1, “Synchronizing Users and Groups from an LDAP Directory,” on page 111.

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 or not you are using a secure SSL connection:

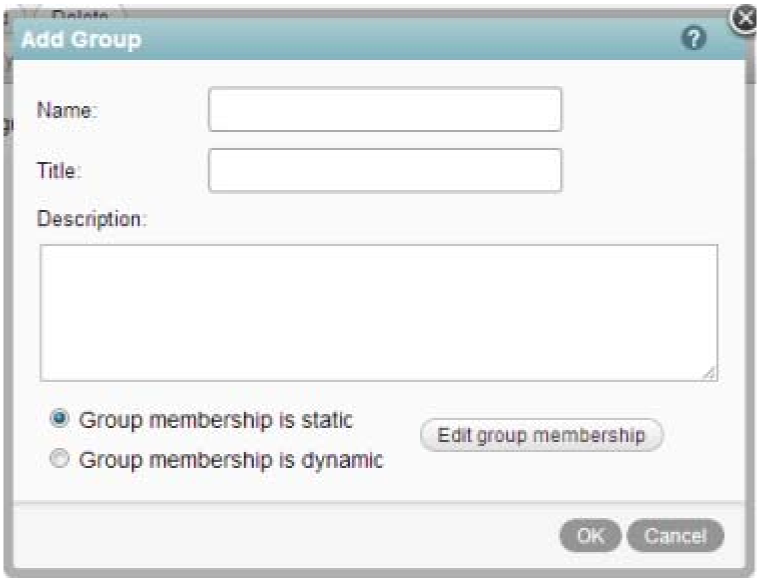
```
http://filr_hostname:8443
https://filr_hostname:8443
```

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 may not be required to enter the port number in the URL, and 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 (_).

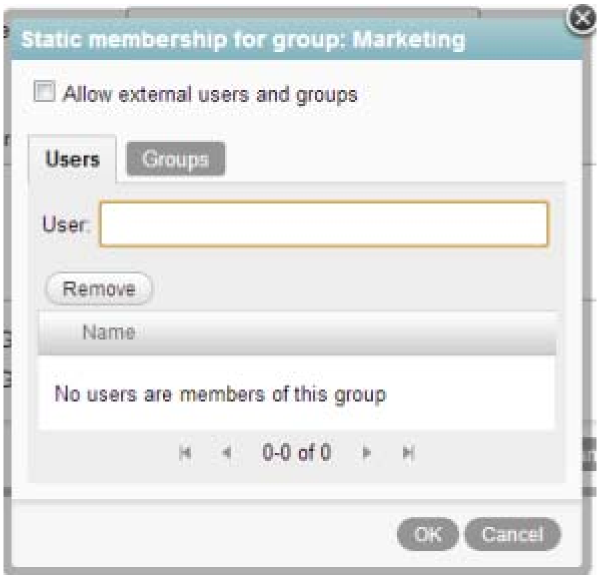
Title: Specify the group name that displays to users on the Filr site. This string can include any characters that you can type.

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*.


Static membership for group: Marketing
□ Allow external users and groups
Users
Groups
User:
Remove
Name
0-0 of 0
OK
Cancel

No users are members of this group

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.

6.2.2 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:

- “Creating Dynamic Groups within LDAP” on page 58
- “Creating Dynamic Groups within Filr” on page 58

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 Novell iManager (for more information, see the iManager Documentation (http://www.novell.com/documentation/imanager27/index.html)).

Dynamic groups created within LDAP are stored in your LDAP directory and can then be synchronized to Filr, as described in Section 14.1, "Synchronizing Users and Groups from an LDAP Directory," on page 111.

Creating Dynamic Groups within Filr

You can create dynamic groups in Filr by querying the LDAP directory.

- "Prerequisites" on page 58
- "Advantages" on page 58
- "Considerations with Multiple LDAP Sources" on page 59
- "Creating the Group" on page 59

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 "LDAP Attribute to Identify a User or Group" on page 113.

  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 14.1, "Synchronizing Users and Groups from an LDAP Directory," on page 111.

Advantages

Advantages to creating dynamic groups within Filr rather than within your LDAP directory include:

- 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 or not you are using a secure SSL connection:

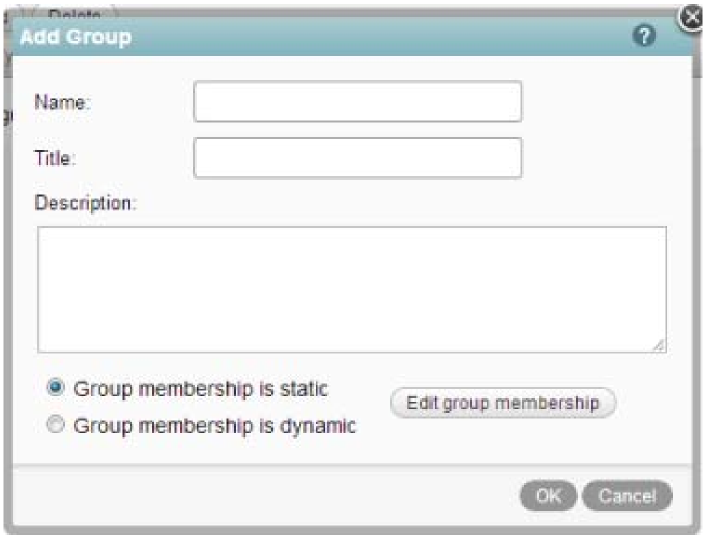
```
http://filr_hostname:8443
https://filr_hostname:8443
```

   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 may not be required to enter the port number in the URL, and 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 alphanumeric characters (a-z, A-Z, 0-9), hyphens (-), and underscores (_).

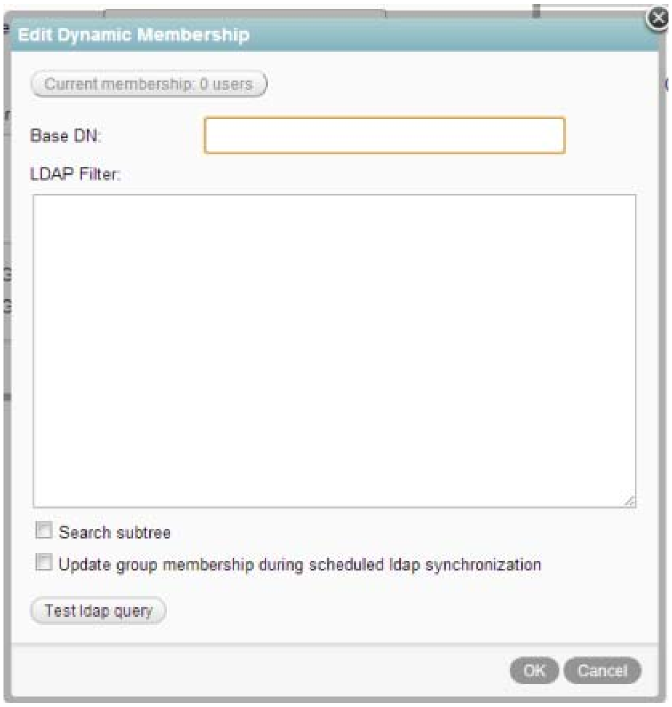
Title: Specify the group name that displays to users on the Filr site. This string can include any characters that you can type.

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*.


Edit Dynamic Membership
Current membership: 0 users
Base DN:
LDAP Filter:
□ Search subtree
□ Update group membership during scheduled ldap synchronization
Test ldap query
OK
Cancel

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 59 before proceeding.

   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 "Synchronization Schedule" on page 116.

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.

6.3 Allowing External Users Access to Your Filr Site

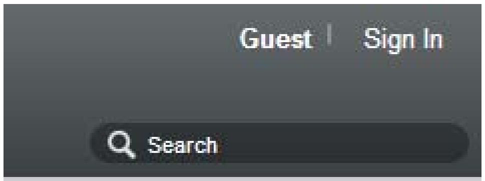
Users external to your organization can access the Filr site either as the Guest user, as a registered user (after performing an auto-registration process), or with their Google or Yahoo login (uses OpenID authentication). By default, these features are not enabled.

Users can auto-register or log in with their Google or Yahoo account only if sharing with external users has been enabled, if you have configured Filr to allow users to log in with OpenID, and if an item has been shared with them. Guest users can access the site at any time if Guest access has been enabled as described in this section.

- Section 6.3.1, “Allowing Guest Access to Your Filr Site,” on page 61
- Section 6.3.2, “Allowing Users to Access the Filr Site with Google and Yahoo Accounts (OpenID),” on page 63

6.3.1 Allowing Guest Access to Your Filr Site

When a person arrives at the Novell Filr site URL, the person is considered to be a Guest user on the site, as indicated by the username displayed in the upper right corner of the page:



This page is also the main Filr login page. Users with Filr usernames can log in to their My Files, and from there they can access any other locations where they have been granted access.

- “Guest Access Limitations” on page 61
- “Understanding the Guest User” on page 62
- “Setting Up Guest Access for the Filr Site” on page 62
- “Monitoring Guest User Access” on page 63

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 “Changing Reverse Proxy Configuration Settings” in the *Novell Filr 1.0.1 Installation and Configuration Guide*.
- 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 1.0 Mobile App Quick Start (http://www.novell.com/documentation/novell-filr1/filr1_qs_mobile/data/filr1_qs_mobile.html).

Understanding the Guest User

As the administrator, you can choose whether you want people who do not have Filr usernames 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 or not you are using a secure SSL connection:

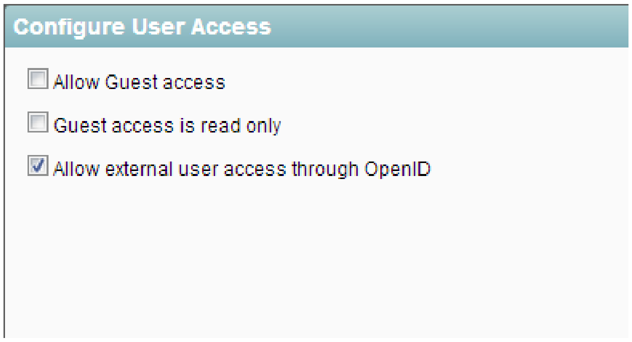
```
http://filr_hostname:8443
https://filr_hostname:8443
```

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 may not be required to enter the port number in the URL, and 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 *User Access*.



Configure User Access

□ Allow Guest access

□ Guest access is read only

☑ Allow external user access through OpenID

4 Select *Allow Guest Access*, then click *Close*.

Now 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 Ensure that users are allowed to share with the public, as described in Section 3.2, “Enabling Users to Share,” on page 21.

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 21.2.7, “User Access Report,” on page 168.

6.3.2 Allowing Users to Access the Filr Site with Google and Yahoo Accounts (OpenID)

This option allows users external to the organization who have received a shared item in Filr to log in to the Filr site using their Google or Yahoo accounts. If you do not enable this option, external users who receive a shared item must create a Filr account.

Users attempting to access the Filr site by using OpenID must have direct HTTPS access to the OpenID provider.

For more information about the user experience for external users accessing the Filr site, see “Logging in As an External User to See a Shared Item” in the *Novell Filr 1.0.1 Web Application User Guide*.

To allow external users to access the Filr site by using their Google and Yahoo accounts:

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 or not you are using a secure SSL connection:

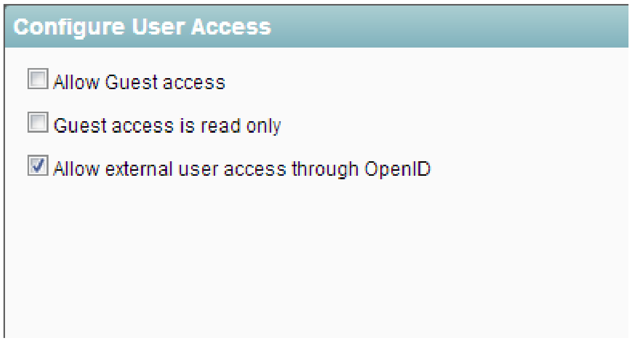
```
http://filr_hostname:8443
https://filr_hostname:8443
```

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 may not be required to enter the port number in the URL, and 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 *User Access*.



Configure User Access

☐ Allow Guest access

☐ Guest access is read only

☑ Allow external user access through OpenID

4 Select *Allow external user access through OpenID*.

5 Click *OK*.

6 Ensure that sharing with external users has been enabled, as described in Section 3.2, “Enabling Users to Share,” on page 21.

6.4 Allowing Web Crawler Access to Your Filr Site

If you allow Guest access to your Novell Filr site, as described in Section 6.3, “Allowing External Users Access to Your Filr Site,” on page 61, 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.

7 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 7.1, “Branding the Filr Site,” on page 65
- Section 7.2, “Branding the Login Dialog Box,” on page 66

7.1 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, you need to 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.

The minimum height for the Branding area is 87px. Images smaller than this are displayed in the upper-left corner of the Branding area. When images larger than 87px are used, the Branding area is expanded to accommodate the image.

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.

Images are available in the drop-down list after you upload them by clicking the *Browse* icon , as described in Step 4.

The minimum height for the Branding area is 87px. Images smaller than this are displayed in the upper-left corner of the Branding area. When images larger than 87px are used, the Branding area is expanded to accommodate the image. The width of the branding area is dynamic to account for various screen sizes. If you want your image to occupy the entire width of the Branding area and you do not want to stretch the image using the *Stretch Image* option, ensure that your image is wide enough to fill any modern screen size. (A safe estimate might be about 2,000px.) However, excess width is cut off depending on the width of the browser.

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.

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 name 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 name to the right of this field, select the new color, then click *OK*.

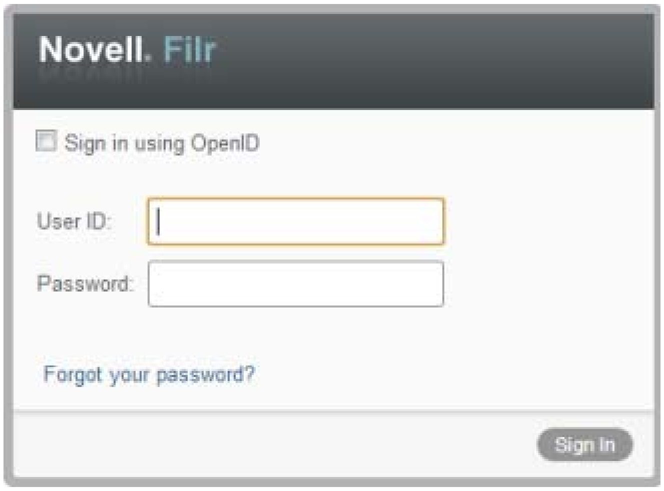
Clear branding: Click this option to clear all your current branding selections.

6 Click *OK*.

The Filr site now displays the brand that you created.

7.2 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.

   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, you need to 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.

8 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 8.1, "Configuring a Protected Resource for a Novell Filr Server," on page 69.

IMPORTANT: When you use NetIQ Access Manager with Filr, external users cannot access your Filr site. This means that the following features are not functional:

- Users are not able to share with external users, as described in "Sharing with People Outside Your Organization" in the *Novell Filr 1.0.1 Web Application User Guide*.
- Users cannot make items accessible to the public, as described in "Making Files Accessible to the Public" in the *Novell Filr 1.0.1 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 6.3.1, "Allowing Guest Access to Your Filr Site," on page 61.

For more information about external users in Filr, see Section 6.3, "Allowing External Users Access to Your Filr Site," on page 61.

8.1 Configuring a Protected Resource for a Novell Filr Server

The following sections explain how to configure the Access Gateway with a domain-base multi-homing service. The instructions assume that you have a functioning Novell Filr server on Linux and a functioning Access Manager system (3.1 SP1 IR1 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 8.1.1, "Configuring the Novell Filr Server to Trust the Access Gateway," on page 70
- Section 8.1.2, "Configuring a Reverse-Proxy Single Sign-On Service for Novell Filr," on page 70

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).

8.1.1 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 username (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 "Changing Reverse Proxy Configuration Settings" in the *Novell Filr 1.0.1 Installation and Configuration Guide*.

8.1.2 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 70
- "Configuring the Domain-Based Proxy Service" on page 70
- "Creating Policies" on page 71
- "Configuring Protected Resources" on page 72
- "Disabling a Rewriter Profile and Enabling Port Redirection" on page 74

Creating a New Reverse Proxy

Before you can configure the domain-based proxy service, you need to create a new reverse proxy. For information on how to create a reverse proxy, see "Managing Reverse Proxies and Authentication" in "Configuring the Access Gateway to Protect Web Resources" in the .

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 70.

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 you want the public to use to access your site. This DNS name must resolve to the IP address you set up as the listening address. For example, `Filr.doc.provo.novell.com`.

   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 “Changing Reverse Proxy Configuration Settings” in the *Novell Filr 1.0.1 Installation and Configuration Guide*. 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 72.

Creating Policies

There are two policies that you need to create: LDAP Identity Injection and X-Forward-Proto:

- “Creating the LDAP Identity Injection Policy” on page 71
- “Creating the X-Forward-Proto HTTP Header Policy” on page 72

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 .

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, 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/*
```

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 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 74.

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 "Configuring 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 70.)
3. Enable port redirection on the Filr server, as described in "Changing the Network Configuration Settings" in the *Novell Filr 1.0.1 Installation and Configuration Guide*.

   This allows Filr to listen on port 8443, and allows Access Manager to forward client requests to port 443.

9 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.

If you make configuration changes, users must log out of the app and log back in in order to see the changes.

9.1 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 9.2, “Configuring Mobile Device Access for Individual Users and Groups,” on page 76.

   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 downloaded: 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, then downloading the file to their mobile device via the regular Filr Web browser.

   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 1.0 Mobile App Quick Start* (http://www.novell.com/documentation/novell-filr1/filr1_qs_mobile/data/filr1_qs_mobile.html).

Interact with other applications: You must select *Allow files to be downloaded* for this option to be available. This option allows the Filr mobile app to interact with third-party applications that are also on the device. This includes:

- Open In functionality for iOS devices and the Share or Send To functionality for Android devices.

  For example, users can view a file in Filr, then open that file in a document editing application, edit the file in the document editing application, then save the file back to the Filr app.
- Cut or copy data from Filr and paste it into another application.
- Allow a third-party app to Open In or Send To Filr.
- Allow photos to be uploaded to Filr.

This setting applies to all files that users have access to, including files in Net Folders.

If you are using MobileIron to manage devices in your organization, the setting to allow Filr to interact with other applications exists both in the Filr administration console, and in the MobileIron administration console. This setting should be consistent in both locations. That is, if it is enabled in Filr, it should also be enabled in MobileIron.

The 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 iOS devices that are being managed by MobileIron are able to use Open In functionality; iOS devices that are not being managed by MobileIron, as well as all Android devices, are not able to use Open In functionality.

For more information about using MobileIron with Filr, see Section 9.3.2, “Configuring MobileIron to Manage the Filr App,” on page 78.

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*.

9.2 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 *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 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 downloaded: 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.

You can configure this setting for each Net Folder. For more information, see Step 11 in Section 5.4, “Creating and Managing Net Folders,” on page 45.

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, then downloading the file to their mobile device via the regular Filr Web browser.

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 1.0 Mobile App Quick Start* (http://www.novell.com/documentation/novell-filr1/filr1_qs_mobile/data/filr1_qs_mobile.html).

Interact with other applications: You must select *Allow files to be downloaded* for this option to be available. This option allows the Filr mobile app to interact with third-party applications that are also on the device. This includes:

- Open In functionality for iOS devices and the Share or Send To functionality for Android devices.

  For example, users can view a file in Filr, then open that file in a document editing application, edit the file in the document editing application, then save the file back to the Filr app.
- Cut or copy data from Filr and paste it into another application.
- Allow a third-party app to Open In or Send To Filr.
- Allow photos to be uploaded to Filr.

If you are using MobileIron to manage devices in your organization, the setting to allow Filr to interact with other applications exists both in the Filr administration console, and in the MobileIron administration console. This setting should be consistent in both locations. That is, if it is enabled in Filr, it should also be enabled in MobileIron.

For more information about using MobileIron with Filr, see Section 9.3.2, “Configuring MobileIron to Manage the Filr App,” on page 78.

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*.

9.3 Managing Mobile Devices

You can manage the Filr mobile app on users' mobile devices with either MobileIron or ZENworks Mobile Management (ZMM).

- Section 9.3.1, "Configuring ZMM to Manage the Filr App," on page 78
- Section 9.3.2, "Configuring MobileIron to Manage the Filr App," on page 78

9.3.1 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).

9.3.2 Configuring MobileIron to Manage the Filr App

Filr 1.0.1 provides support for managing the Filr mobile applications with MobileIron when using the Filr 1.0.2 Mobile Apps.

- "Supported Features" on page 78
- "Adding the Filr App to MobileIron" on page 79
- "Pre-Populating Fields for Filr Login" on page 81
- "Configuring Data Loss Prevention Policies" on page 82
- "Distributing the Filr App to Devices" on page 83

Supported Features

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

- "iOS Supported Features" on page 78
- "Android Supported Features" on page 79

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 setting to allow Filr to interact with other applications exists both in the Filr administration console, and in the MobileIron administration console. This setting should be consistent in both locations. That is, if it is enabled in Filr, it should also be enabled in MobileIron.

The 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 iOS devices that are being managed by MobileIron are able to use Open In functionality; iOS devices that are not being managed by MobileIron, as well as all Android devices, are not able to use Open In functionality.

For information about how to configure this option in Filr, see Section 9.1, "Configuring Mobile Device Access for All Users," on page 75 and Section 9.2, "Configuring Mobile Device Access for Individual Users and Groups," on page 76.

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 79
- "Adding the iOS Filr App" on page 80

Adding the Android Filr App

To add the Android Filr app to MobileIron, 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 (https://download.novell.com).

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, 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, 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 creating a new app configuration for iOS.

- "Modifying the Android Filr App Configuration for MobileIron" on page 81
- "Creating the iOS Filr App Configuration for MobileIron" on page 81
- "Key-Value Pairs" on page 82

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 79.
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 9-1, "Filr Key-Value Pairs," on page 82. 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 9-1, "Filr Key-Value Pairs," on page 82. 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

Table 9-1 Filr Key-Value Pairs

Key	Value
server	Specify the URL of your Filr site. For example, `filr.acme.com`.
user	Specify `$USERID$` to cause MobileIron to automatically populate the app with the users' MobileIron user ID. Alternatively, you can specify an individual user's user ID.
password (Android-only)	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 creating a new app policy for iOS.

- "Modifying the Android Filr App Policy for MobileIron" on page 82
- "Creating the iOS Filr App Policy for MobileIron" on page 82

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 79.
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 options 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.)

9.4 Understanding Filr Data Security for Mobile Devices

- Section 9.4.1, “App Security,” on page 83
- Section 9.4.2, “File Security,” on page 84

9.4.1 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.

9.4.2 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 9.1, "Configuring Mobile Device Access for All Users," on page 75.

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" (https://www.novell.com/documentation/novell-filr1/filr1_qs_mobile/data/filr1_qs_mobile.html#b141c3ul) in the *Novell Filr 1.0 Mobile App Quick Start* (http://www.novell.com/documentation/novell-filr1/filr1_qs_mobile/data/filr1_qs_mobile.html).

10 Configuring the Filr Desktop Application to Access Files

The Novell Filr desktop application enables users to work with Filr files on their personal workstations. The Novell Filr desktop application synchronizes files from the Filr server with the workstation, allowing users to manage Filr files from the file system on their computers. 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-filr1/filr1_qs_desktop/data/filr1_qs_desktop.html) and the Novell Filr Desktop Application for Mac Quick Start (http://www.novell.com/documentation/novell-filr1/filr1_qs_desktopmac/data/filr1_qs_desktop.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 10,000 total files, or to synchronize individual files that are larger than 1 GB to their workstations. (These numbers require the use of the Filr 1.0.2 desktop application.)

10.1 Planning Filr Desktop Application Usage for Your Filr Site

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. Several factors can affect the 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.
- Whether users have Home folders and how many files are in each user’s Home folder.

  Home folders are synchronized by default to each user’s workstation.
- The synchronization schedule that you specify when configuring 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 the following:

- Make 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 10.2.2, “Configuring the Filr Desktop Application for Individual Users and Groups,” on page 88.

10.2 Configuring the Filr Desktop Application for All Users or for Individual Users and Groups

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-filr1/filr1_qs_desktop/data/filr1_qs_desktop.html) and the Novell Filr Desktop Application for Mac Quick Start (http://www.novell.com/documentation/novell-filr1/filr1_qs_desktopmac/data/filr1_qs_desktop.html).

- Section 10.2.1, “Configuring the Filr Desktop Application for All Users,” on page 86
- Section 10.2.2, “Configuring the Filr Desktop Application for Individual Users and Groups,” on page 88

10.2.1 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. In the Configure Desktop Application dialog box, select *On*.
4. 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.

   NOTE: Depending on the amount of anticipated load that the Filr desktop application will put on your Filr system, you might want to make the application available to users in a staged process. For more information, see Section 10.1, “Planning Filr Desktop Application Usage for Your Filr Site,” on page 85.

You must individually enable each Net Folder to be accessed by the Filr desktop application, as described in Step 11 in Section 5.4, “Creating and Managing Net Folders,” on page 45.

Allowing access to the Filr site through the Filr desktop application can be changed on a per-user basis, as described in Section 10.2.2, “Configuring the Filr Desktop Application for Individual Users and Groups,” on page 88.

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 10.2.2, “Configuring the Filr Desktop Application for Individual Users and Groups,” on page 88.

Be deployed: Select this option to provide a link from the Filr Web client that allows users to download the desktop application. If this option is not selected, the link is not visible to users.

If this option is selected, the *Auto-update URL* field must be populated (the default configuration is to allow the Filr server to be the auto-update server).

You might want to leave this 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. However, when deploying the Filr desktop application with the `MSI` file, ensure that .NET Framework 4 or 4.5 is also installed on client workstations. If you are updating the Filr desktop application on client workstations, see Section 10.4, “Updating the Filr Desktop Application,” on page 90.

You can obtain the `MSI` file by downloading the `NovellFilrAutoUpdate.tgz` file from the Filr downloads page on Novell Downloads (https://download.novell.com); then extracting the file.

Synchronization every *xx* Minutes: Specify the interval (in minutes) for how often the Filr desktop application checks the Filr server for changes to files. 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.

Auto-update URL: The auto-update URL where the Filr desktop application can check for updates. This is the URL where the Filr desktop application download files are hosted. By default, your Filr server is set up to provide auto-update information to the Filr desktop application. The *Auto-update URL field* is populated with this information by default. The default port is 8443.

If this field is not populated, specify the following URL:

```
https://Filr_appliance_IPaddress:8443/desktopapp/
```

NOTE: When specifying the auto-update URL, consider the following:

- If your Filr system is fronted by an L4 or L10 switch, do not use the Filr server to deploy the Filr desktop application. Instead, use a separate Web server as described in Section 10.3, “Configuring a Separate Web Server to Deploy the Filr Desktop Application,” on page 89.

- If you have enabled port redirection on the Filr server, as described in “Changing the Network Configuration Settings” in the *Novell Filr 1.0.1 Installation and Configuration Guide*, ensure that either of the following requirements is met:
  - The *Auto-update URL* field contains the secure HTTP port, 8443 (or 8080 if the HTTP port is enabled)
  - A separate Web server is configured to provide auto-update information, as described in Section 10.3, “Configuring a Separate Web Server to Deploy the Filr Desktop Application,” on page 89
- To minimize load on the Filr server, you can configure a separate Web server for deploying the desktop application and to provide auto-update information. For more information, see Section 10.3, “Configuring a Separate Web Server to Deploy the Filr Desktop Application,” on page 89.

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.

5 Click *OK*.

10.2.2 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 10.2.1, “Configuring the Filr Desktop Application for All Users,” on page 86. 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 *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 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, as described in Step 11 in Section 5.4, “Creating and Managing Net Folders,” on page 45.

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*.

10.3 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 the 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.

   This compressed file contains all of the files required for installing the Filr desktop application.
3. (Conditional) If you have Windows XP workstations in your environment that will run Filr, you need to rename a couple files so that they are used instead of the default files.

   IMPORTANT: Because Microsoft .NET Framework 4.5 is not supported on Windows XP, the `NovellFilrSetup-winxp-`*`version`*`.exe` and `novellfilr/windows/x86/version-winxp.json` files are provided for organizations that have workstations that are running Windows XP. This version of Filr contains Microsoft .NET Framework 4.0 instead of 4.5.

   The only difference between this version of Filr and the version that runs Microsoft .NET Framework 4.5 is that the *Filr* tab is not available from the Windows Properties dialog box.

   3a Rename the `version.json` file to `version-x86.json` (or any other name of your choosing).

   3b Rename the `version-winxp.json` file to `version.json`.
4. (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
```

5 Configure the Filr desktop application as described in Section 10.2.1, “Configuring the Filr Desktop Application for All Users,” on page 86.

In the *Auto-update URL* 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/desktopapp/
```

```
http://web_server_DNS_or_IP/desktopapp/
```

6 Click *OK*.

10.4 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 10.4.1, “Understanding Missing Dependencies Related to Updating the Filr Desktop Application by Using the MSI File,” on page 90
- Section 10.4.2, “Updating the Filr Desktop Application on the Filr Server or on a Separate Web Server,” on page 91

10.4.1 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:

- One of the following versions of Microsoft .NET Framework, depending on whether there are workstations in your environment that are dependent on Windows XP:
  - Microsoft .NET Framework 4.5 (Applies to 64-bit Windows and Mac workstations. You should use this version if workstations in your environment are not dependent on Windows XP.)

    The ability for users to view the *Novell Filr* tab on the Windows Properties dialog (as described in “Viewing Filr Properties for a File or Folder” in the *Novell Filr Desktop Application for Windows Quick Start* (http://www.novell.com/documentation/novell-filr-1-1/filr-1-1_qs_desktop/data/filr-1-1_qs_desktop.html)) is available only with Microsoft .NET Framework 4.5.
  - Microsoft .NET Framework 4.0 (Can be used with all supported operating systems; however, because Microsoft .NET Framework 4.5 is not supported on Windows XP, this is the only option for workstations that are running Windows XP.)
- Microsoft Visual C++ 2013 Redistributable Package (Applies to all workstations except for Windows XP workstations)

IMPORTANT: Workstations running Windows XP cannot see the Novell Filr tab on the Windows Properties dialog (as described in “Viewing Filr Properties for a File or Folder” in the *Novell Filr Desktop Application for Windows Quick Start* (http://www.novell.com/documentation/novell-filr-1-1/filr-1-1_qs_desktop/data/filr-1-1_qs_desktop.html)).

This is because Microsoft .NET Framework 4.5 is not supported on Windows XP.

10.4.2 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 10.2, “Configuring the Filr Desktop Application for All Users or for Individual Users and Groups,” on page 86), or if you have configured a separate web server to deploy the Filr desktop application (as described in Section 10.3, “Configuring a Separate Web Server to Deploy the Filr Desktop Application,” on page 89), 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, except for Windows XP.

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) Now 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/
```

4 (Conditional) If you have Windows XP workstations in your environment that will run Filr, you need to rename a couple files so that they are used instead of the default files.

IMPORTANT: Because Microsoft .NET Framework 4.5 is not supported on Windows XP, the `NovellFilrSetup-winxp-`*`version`*`.exe` and `novellfilr/windows/x86/version-winxp.json` files are provided for organizations that have workstations that are running Windows XP. This version of Filr contains Microsoft .NET Framework 4.0 instead of 4.5.

The only difference between this version of Filr and the version that runs Microsoft .NET Framework 4.5 is that the *Filr* tab is not available from the Windows Properties dialog box.

4a Rename the `version.json` file to `version-x86.json` (or any other name of your choosing).

If you do not rename `version-x86.json`, Windows XP users will be prompted to upgrade the Filr desktop application, but the upgrade will fail and Windows XP users will continue to be prompted to upgrade.

4b Rename the `version-winxp.json` file to `version.json`.

10.5 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 can 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.

- Section 10.5.1, “Distributing Filr Desktop Application Traffic Separately from Other Applications,” on page 92
- Section 10.5.2, “Distributing Filr Desktop Traffic in Conjunction with Other Applications,” on page 93
- Section 10.5.3, “Load Balancer and Reverse Proxy Server Configuration,” on page 93

10.5.1 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 10.5.3, "Load Balancer and Reverse Proxy Server Configuration," on page 93.

10.5.2 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 10.5.3, "Load Balancer and Reverse Proxy Server Configuration," on page 93.

10.5.3 Load Balancer and Reverse Proxy Server Configuration

For information on how to configure a reverse-proxy server for your Filr site, see "Changing Reverse Proxy Configuration Settings" in the *Novell Filr 1.0.1 Installation and Configuration Guide*.

10.6 Managing the Filr Desktop Application

You can manage the Filr desktop application on users' workstations with client management software such as Novell ZENworks.

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 10.6.1, "Customizing the Installation for the Filr Desktop Application," on page 94
- Section 10.6.2, "Controlling Windows Explorer Restart," on page 97

10.6.1 Customizing the Installation for the Filr Desktop Application

You can customize the installation process of the Filr desktop application for your organization. You can:

- 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 94
- "Enabling Auto-Configuration" on page 95
- "Disallowing User Configuration" on page 96
- "Modifying the Filr Desktop Configuration" on page 96

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 10-1 *Default Value Configuration Options*

Windows Registry Value Name	Value Type	Mac Property Name	Value Type	Supports Env Variables	Default Value
Default Server URL	REG_SZ	FilrDefaultServerURL	string	No	https://

Windows Registry Value Name	Value Type	Mac Property Name	Value Type	Supports Env Variables	Default Value
Default Username	REG_SZ	FilrDefaultUsername	string	Yes	%USERNAME% or $USER
Default Account Name	REG_SZ	FilrDefaultAccountName	string	No	Hostname in server URL
Default Remember Password	REG_SZ (“true” or “false”)	FilrDefaultRememberPassword	<true/> or <false/>	No	false
Default Sync Dir	REG_SZ	FilrDefaultSyncDir	string	Yes	%USERNAME%\Filr or $USER\Filr
Default Start On Login	REG_SZ (“true” or “false”)	FilrDefaultStartOnLogin	<true/> or <false/>	No	true
Default Folder List	REG_MULTI_SZ	FilrDefaultFolderList	Array of strings	No	My Files Shared with Me

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 10-2 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 10-3 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 95), 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.

10.6.2 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
```

11 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 *Novell Filr 1.0.1 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 11.1.4, “Using OpenOffice as Your Document Editor for WebDAV,” on page 101.

11.1 Planning Your WebDAV Implementation

11.1.1 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/TLC (HTTPS).

  For more information, see “Choosing Basic Authentication” in the *Novell Filr 1.0.1 Installation and Configuration Guide*.

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 11.5, “Allowing Basic Authentication over an HTTP Connection on Windows 7,” on page 103. 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” in the *Novell Filr 1.0.1 Installation and Configuration Guide*.

11.1.2 Using WebDAV When Filr Is Fronted by NetIQ Access Manager

If your Filr system is fronted by either 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 “Changing Reverse Proxy Configuration Settings” in the *Novell Filr 1.0.1 Installation and Configuration Guide*, you must use basic authentication for your WebDAV implementation During the Filr appliance configuration, select *basic* when configuring WebDAV, as described in “Changing the WebDAV Authentication Configuration Settings” in the *Novell Filr 1.0.1 Installation and Configuration Guide*.

11.1.3 Meeting Filr Certificate Requirements on Windows 7

If you are using WebDAV functionality (Edit-in-Place) with Filr on Windows 7 with a secure (HTTPS) connection, you need to ensure that the Filr server certificate requirements are met. If all of the requirements are not met, various Windows 7 services fail.

The Filr server certificate requirements are:

- 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 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.

  Wildcard certificates such as `*.novell.com` are supported.

- The date range for the trusted server certificate must be valid. You cannot use an expired server certificate.

11.1.4 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.

11.2 Editing Files with Edit-in-Place Functionality

You can leverage Edit-in-Place functionality to edit files by using tools such as OpenOffice and Microsoft Office. For information on how to edit files in Filr with Edit-in-Place functionality, see "Editing Files with Edit-in-Place" in the *Novell Filr 1.0.1 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 11.1.3, "Meeting Filr Certificate Requirements on Windows 7," on page 100.

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/).

11.3 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 *Novell Filr 1.0.1 Web Application User Guide*.

When you map a Filr folder as a WebDAV folder on Windows 7, consider the following:

- When mapping a Filr folder over HTTPS, you must ensure that all Filr server certificate requirements are met, as described in Section 11.1.3, "Meeting Filr Certificate Requirements on Windows 7," on page 100.

11.4 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 11.4.1, "Administrator Configuration Responsibilities," on page 102
- Section 11.4.2, "User Configuration Responsibilities," on page 102

11.4.1 Administrator Configuration Responsibilities

1 Ensure 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.

11.4.2 User Configuration Responsibilities

Each user on his or her Windows 7 workstation 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 11.4.1, “Administrator Configuration Responsibilities,” on page 102.

11.5 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\Bas
   icAuthLevel
   ```

4. Change the value of this registry entry to `2`.
5. Navigate to the Services interface, then restart the *WebClient* service.

12 Managing Document HTML Conversions

12.1 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 *Novell Filr 1.0.1 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 12.2, “Deleting Saved Document Conversions,” on page 105.

12.2 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.

To delete all saved document conversions:

1. Purge the `/cachefilestore` directory.
2. Re-create the `/cachefilestore` directory at the same location.

12.3 Uploading TrueType 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 *Novell Filr 1.0.1 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 the Microsoft TrueType 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.

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.

13 Managing a Multiple-Language Filr Site

13.1 Accommodating Multiple Languages

13.1.1 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. Examples include:

- 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.

13.1.2 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 *Novell Filr 1.0.1 Web Application User Guide*.

II Site Maintenance

14 Managing Users

As time passes on your Novell Filr site, users come and go, resulting in the need for periodic maintenance activities.

14.1 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 (Novell 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-filr1/filr1_readme_novell/data/filr1_readme_novell.html#ble286e)” in the Novell Filr 1.0 Readme (http://www.novell.com/documentation/novell-filr1/filr1_readme_novell/data/filr1_readme_novell.html).

The following video walks you through the LDAP synchronization process:

http://www.youtube.com/watch?v=B5G84njBh64

To synchronize users and groups to the Filr site from an LDAP directory:

1 Log in to Filr as the Filr administrator.

1a Launch a web browser.

1b Specify one of the following URLs, depending on whether or not you are using a secure SSL connection:

```
http://filr_hostname:8443
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 may not be required to enter the port number in the URL, and 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*.

4 Click *Add a New LDAP Source*, then use the following sections as a reference when filling in the necessary information:

If the search context of your 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 5.3, “Configuring and Managing Net Folder Servers,” on page 41.)

- Section 14.1.1, “LDAP Connections,” on page 112
- Section 14.1.2, “LDAP Synchronization Options,” on page 116

14.1.1 LDAP Connections

You can configure one or more LDAP connections. Each connection requires the following configuration information:

- “LDAP Server” on page 112
- “User DN (Proxy User for Synchronizing Users and Groups)” on page 113
- “LDAP Attribute to Identify a User or Group” on page 113
- “LDAP Attribute Used for Filr Name” on page 114
- “User and Group Object Locations” on page 114

LDAP Server

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 hostname 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 24.2, "Securing LDAP Synchronization," on page 185 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 username and password of a user on the LDAP server who has sufficient rights to access the user information stored there.

The proxy user must have the following rights in order to view the user objects and their properties:

Directory Service	Required Rights
eDirectory	Read, Write, Erase, Create, Modify, FileScan For eDirectory, if you use a subcontainer administrator as the proxy user, the subcontainer administrator must be given the appropriate rights. (For more information about subcontainer administrators in eDirectory, see "Installing and Configuring OES as a Subcontainer Administrator" in "Preparing to Install OES 11 SP1" in the *OES 11 SP1: Installation Guide*.)
Active Directory	Modify, Read&Execute, Read, Write, ListFolderContents

You need to provide the fully qualified, comma-delimited username, along with its context in your LDAP directory tree, in the format expected by your directory service.

Directory Service	Format for the Username
eDirectory	`cn=username,ou=organizational_unit,o=organization`
Active Directory	`cn=username,ou=organizational_unit,dc=domain_component`

LDAP Attribute to Identify a User or Group

The LDAP attribute that uniquely identifies a user or group helps facilitate renaming and moving Filr users and groups 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.

To ensure that Filr modifies the existing user instead of creating a new user when the user is renamed or moved in the LDAP directory, you must specify the name of the LDAP attribute that uniquely identifies the user. The following table shows the LDAP attribute to use for your directory.

This attribute always has a unique value that does not change when you rename or move a user in the LDAP directory. If you want to map users to a different attribute, you must 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.

	eDirectory	Active Directory
Attribute to Identify a User or Group	`GUID`	`objectGUID`

LDAP Attribute Used for Filr Name

The *LDAP Attribute Used for Filr Name* setting has two purposes:

- The value is used as the Filr username 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, 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, as shown in the following table. Other LDAP directories might use the uid (unique ID) attribute, depending on the structure and configuration of the directory tree.

	eDirectory	Active Directory
Attribute Used for Filr Name	`cn` or `uid` (Depending on the structure of the LDAP directory)	`sAMAccountName`

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 *LDAP Attribute Used for Filr Name*, and then set up a separate source to the same LDAP server and use sAMAccountName as the *LDAP Attribute Used for Filr Name*.

In addition to the attributes already mentioned in this section, other LDAP attributes can be used for the *LDAP Attribute Used for Filr Name*, 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.

User and Group Object Locations

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`*

NOTE: Container names cannot exceed 128 characters. If the container name exceeds 128 characters, users are not provisioned.

To identify potential Filr users, Filr by default filters on the following LDAP directory object attributes:

- `Person`
- `orgPerson`
- `inetOrgPerson`

If you want to create Filr 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 user or group filter list if necessary. You can use the following operators in the filter:

- | OR (the default)
- & AND
- ! NOT

You can choose whether you want Filr to search for users (and optionally, groups) in containers underneath the base DN (that is, in subtrees).

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: 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`*`)`

14.1.2 LDAP Synchronization Options

The following synchronization options apply to all LDAP configurations:

- "Synchronization Schedule" on page 116
- "User Synchronization Options" on page 116
- "Group Synchronization Options" on page 117

Synchronization Schedule

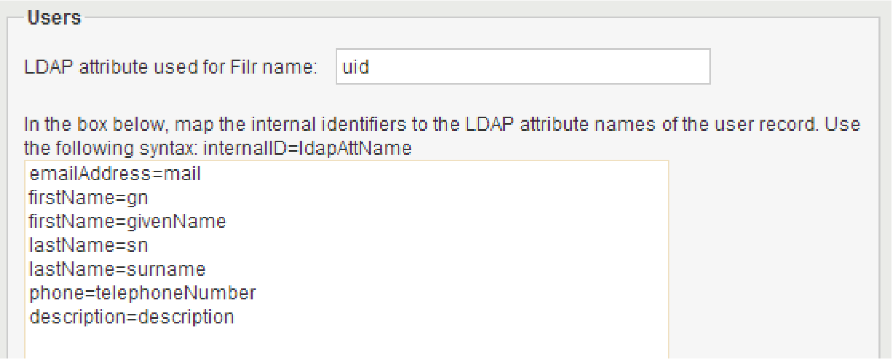
When you enable LDAP synchronization, you can set up a schedule for when it is convenient for synchronization to occur. In planning the schedule, take into account how often your LDAP directory user (and, optionally, group) information changes and the server resources required to perform the synchronization for the number of users (and, optionally, groups) that you have.

You can choose to have LDAP synchronization performed every day, or you can select specific days of the week when you want it performed (for example, on Monday, Wednesday, and Friday). You can choose to have it performed 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 performed multiple times each day (for example, every four hours). The smallest time interval you can set is .25 hours (every 15 minutes).

User Synchronization Options

The following options are available for enabling and configuring user synchronization from your LDAP directory to your Filr site:

- **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 in the *Users* section on the Configure LDAP Synchronization page.



Users

LDAP attribute used for Filr name: uid

In the box below, map the internal identifiers to the LDAP attribute names of the user record. Use the following syntax: internalID=ldapAttName

```
emailAddress=mail
firstName=gn
firstName=givenName
lastName=sn
lastName=surname
phone=telephoneNumber
description=description
```

Filr synchronizes the following attributes from the LDAP directory:

- First name
- Last name
- Phone number
- Email address
- Description

- **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.
- **Delete users that are not in LDAP:** Select this option to delete users that exist on the Filr site but do not exist in your LDAP directory.

  IMPORTANT: Before you select this option, you need to understand the following:

  - A deleted user cannot be undeleted; deleting a user is permanent and is not reversible.
  - When a user is deleted, the user's personal storage (My Files) is also deleted. As a result, all users who have access to a file or folder in the deleted user's My Files area via a share no longer have access, because the items no longer exists in the Filr system.

  Novell recommends that you leave this option deselected. Leaving this option deselected automatically disables any users in Filr who have been deleted in your LDAP directory.

  For more information about disabled users in Filr, see Section 14.7, "Disabling Filr User Accounts," on page 124.

  If you are sure that you want to automatically delete users that are not in LDAP, this option is designed to use 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 14.2, "Creating a New Local User," on page 118, and you want the LDAP synchronization process to delete the manually created users.
- **When deleting users, delete associated user workspaces and content:** Select this option to remove obsolete information along with the user accounts.
- **Use the following time zone when creating new users:** Select this option to set the time zone for user accounts that are synchronized from the LDAP directory into your Filr site. The time zone list is grouped first by continent or region, optionally by country or state, and lastly by city. Some common selections for United States time zones are:

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

- **Use the following locale when creating new users:** Select this option to set the locale for user accounts that are synchronized from the LDAP directory into your Filr site. The locale list is sorted alphabetically by language.

Group Synchronization Options

The following options are available for enabling and configuring user and group synchronization from your LDAP directory to your 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.

- **Register LDAP group profiles automatically:** Select this option to automatically add LDAP groups to the Filr site.
- **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 local groups that are not 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 Section 6.2, “Creating Groups of Users,” on page 55, and you want the LDAP synchronization process to delete the manually created groups.

14.2 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 14.1, “Synchronizing Users and Groups from an LDAP Directory,” on page 111.

To create a local Filr:

1 Log in to Filr as the Filr administrator.

  1a Launch a web browser.

  1b Specify one of the following URLs, depending on whether or not you are using a secure SSL connection:

```
http://filr_hostname:8443
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 may not be required to enter the port number in the URL, and 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 *User Accounts*.

4 Click *New*.

The User page is displayed.

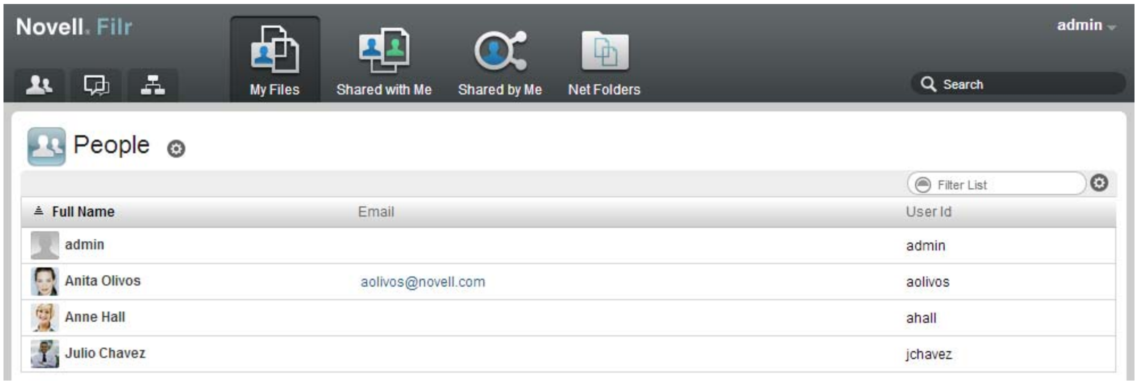
5 Provide the user’s information in the User page, then click *OK*.

14.3 Listing Filr Users

On the Novell Filr site, you can view a comprehensive list of all the Filr users.

1 Click the User List icon in the masthead.

All of the users are displayed in the main viewing window.



Full Name	Email	User Id
admin		admin
Anita Olivos	aolivos@novell.com	aolivos
Anne Hall		ahall
Julio Chavez		jchavez

You can use this page in the following ways:

- Section 14.3.1, “Navigating the User List,” on page 119
- Section 14.3.2, “Navigating to a User’s Individual Profile,” on page 119
- Section 14.3.3, “Modifying the Title,” on page 119

14.3.1 Navigating the User List

You can navigate the user list by using the filter in the upper right corner of the list.

14.3.2 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.

For information about how to navigate to a user’s My Files area, or any other area in Filr, see Chapter 16, “Managing Folders and Files,” on page 129.

14.3.3 Modifying the Title

Filr enables you to modify the name of the User List. This name is displayed when navigating the Workspace tree (as described in Section 16.1, “Navigating the Workspace Tree,” on page 129) and when performing a search.

1 Click the User List 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*.

14.4 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 or not you are using a secure SSL connection:

```
http://filr_hostname:8443
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 may not be required to enter the port number in the URL, and 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 *User Accounts*.

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

14.5 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. How you change users’ name depends on how you created the user.

- Section 14.5.1, “Renaming a Filr User from LDAP,” on page 120
- Section 14.5.2, “Renaming a Local Filr User,” on page 121

14.5.1 Renaming a Filr User from LDAP

If you are synchronizing user information from an LDAP directory, as described in Section 14.1, “Synchronizing Users and Groups from an LDAP Directory,” on page 111, 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.

14.5.2 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 121
- "Renaming Users Who Have Not Logged In to Filr" on page 121

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 👥 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*.

14.6 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 deleting it. Disabled accounts do not count as a licensed user. For information on how to disable a user, see Section 14.7, "Disabling Filr User Accounts," on page 124.

When you delete a user, the following user information is deleted and cannot be recovered:

- All profile information, including profile pictures
- Access controls to workspaces and folders

Entries and information that the user contributed are preserved even after the user is deleted.

How you delete a user depends on how you originally created the user.

- Section 14.6.1, “Deleting a Local User,” on page 122
- Section 14.6.2, “Deleting an LDAP User,” on page 123

14.6.1 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 14.6.2, “Deleting an LDAP User,” on page 123.

IMPORTANT: If you delete user accounts that were created by the LDAP synchronization process without following the instructions in Section 14.6.2, “Deleting an LDAP User,” on page 123, 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 Account: User accounts refer to the actual user object in the Filr system. When a user account is deleted, the user’s profile is deleted, and the user is cannot access the Filr system.

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 or not you are using a secure SSL connection:

```
http://filr_hostname:8443
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 may not be required to enter the port number in the URL, and 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 *User Accounts*.

4 Select the users whose accounts you want to delete, click *More*, then click one of the following options:

  Delete User Workspaces: Does not delete the user’s account, but moves the user’s workspace to the trash. The user workspace can be restored from the trash by the Filr administrator.

Purge User Workspaces: Does not delete the user’s account, but deletes and purges the user’s workspace. The user’s workspace cannot be restored. If the user logs back in, a new workspace is created as if the user is new to the Filr system.

Purge Users and their Workspaces: Deletes and purges the user’s account and the user’s workspace from the Filr system. The user no longer exists in the Filr system and cannot log in. Neither the user’s account nor the user’s workspace can be restored.

5 Click *Yes* to confirm the deletion.

14.6.2 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 14.7, “Disabling Filr User Accounts,” on page 124.

If you decide to delete Filr user accounts, it is safer to manually delete them rather than deleting them through the LDAP synchronization process. Because user accounts that are deleted cannot be recovered, you should make sure you know exactly which users you are deleting, and the only way to be sure is by manually deleting them.

- “Manually Deleting User Accounts That Are Being Synchronized through LDAP” on page 123
- “Configuring LDAP to Automatically Delete User Accounts” on page 123

Manually Deleting User Accounts That Are Being Synchronized through LDAP

The following method is the 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 14.1, “Synchronizing Users and Groups from an LDAP Directory,” on page 111.

2 In Filr, manually delete the user accounts, as described in Section 14.6.1, “Deleting a Local User,” on page 122.

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 Section 14.1.2, “LDAP Synchronization Options,” on page 116.

14.7 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 14.7.1, “Disabling a Local User Account,” on page 124
- Section 14.7.2, “Disabling an LDAP User Account,” on page 125

14.7.1 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 or not you are using a secure SSL connection:

```
http://filr_hostname:8443
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 may not be required to enter the port number in the URL, and 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 *User Accounts*.

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 or not you are using a secure SSL connection:

```
http://filr_hostname:8443
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 may not be required to enter the port number in the URL, and 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 *User Accounts*.

4 Select the user accounts that you want to enable, then click *More* > *Enable*.

14.7.2 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 14.1, “Synchronizing Users and Groups from an LDAP Directory,” on page 111.

14.8 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 or not you are using a secure SSL connection:

```
http://filr_hostname:8443
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 may not be required to enter the port number in the URL, and 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 *User Accounts*.

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*.

14.9 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

15 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 Section 6.2, “Creating Groups of Users,” on page 55.

15.1 Creating Groups

For information on how to create groups, see Section 6.2, “Creating Groups of Users,” on page 55.

15.2 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 or not you are using a secure SSL connection:

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

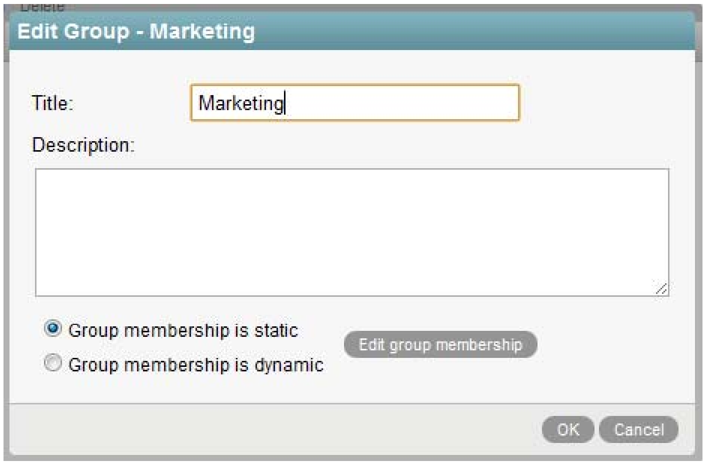
Replace `filr_hostname` with the hostname or fully qualified domain name of the Filr server that you have set up in DNS.

Depending on how you have configured your Filr system, you may not be required to enter the port number in the URL, and 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.



Title: Marketing

Description:

● Group membership is static

○ Group membership is dynamic

5 Modify the title, description, and group membership, then click *OK*.

For more information about editing static and dynamic group membership, see Section 6.2, “Creating Groups of Users,” on page 55.

15.3 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 or not you are using a secure SSL connection:

```
http://filr_hostname:8443
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 may not be required to enter the port number in the URL, and 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*.

16 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 *Novell Filr 1.0.1 Web Application User Guide*.

You can perform additional folder management tasks as the Filr administrator:

- Section 16.1, "Navigating the Workspace Tree," on page 129
- Section 16.2, "Managing Workspace Disk Space Usage," on page 129

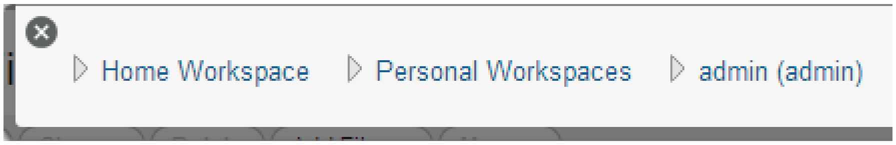
16.1 Navigating the Workspace Tree

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 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.

16.2 Managing Workspace Disk Space Usage

Disk space usage is managed on a folder basis as well as an individual user or group basis.

For more information, see Chapter 17, "Managing Disk Space Usage with Data Quotas and File Restrictions," on page 131.

17 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.

- Section 17.1, "Understanding Data Quota Behavior and Exclusions," on page 131
- Section 17.2, "Managing User Data Quotas," on page 132
- Section 17.3, "General Data Quota Management," on page 143
- Section 17.4, "Managing the File Upload Size Limit," on page 144
- Section 17.5, "Managing Quotas for Outgoing Email Messages," on page 145

17.1 Understanding Data Quota Behavior and Exclusions

- Section 17.1.1, "Understanding Default Data Quota Behavior," on page 131
- Section 17.1.2, "Understanding Data Quota Exclusions," on page 132

17.1.1 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" on page 131
- "Exceeding the High-Water Mark" on page 131

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 users exceed the data quota high-water mark, they are notified that they are approaching the data quota. Filr informs them 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 133.

17.1.2 Understanding Data Quota Exclusions

Files stored in Net Folders do not count against data quotas because they are not uploaded into the Filr site.

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.

17.2 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.

17.2.1 Planning User Data Quotas

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 17.2.2, “Setting User Data Quotas,” on page 133.

As described in “Exceeding the Data Quota” on page 131, 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 17.3.1, “Purging Deleted Files,” on page 143.

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 132.

Selecting an Appropriate High-Water Mark

The high-water mark is the percentage of the data quota when users are notified that they are approaching their data quotas. 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 132.

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 132.

17.2.2 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 134
- “Setting Data Quotas for Individual Groups” on page 135
- “Setting Data Quotas for Individual Users” on page 136

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 or not you are using a secure SSL connection:

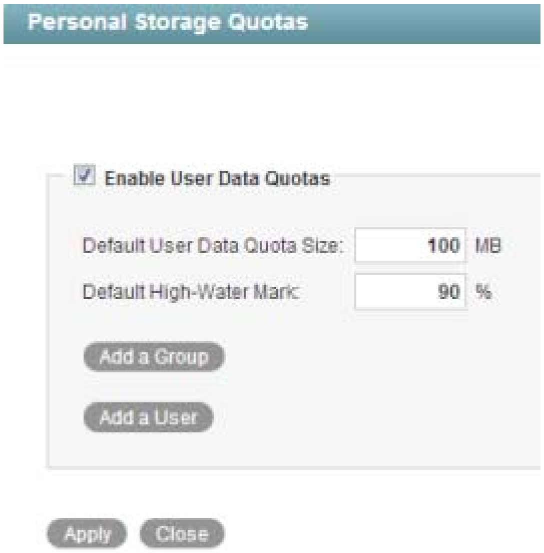
```
http://filr_hostname:8443
https://filr_hostname:8443
```

  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 may not be required to enter the port number in the URL, and 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 Quotas

☑ Enable User Data Quotas

Default User Data Quota Size: 100 MB

Default High-Water Mark: 90 %

4 Select *Enable User Data Quotas*.

5 Set the *Default User Data Quota Size* and *Default High-Water Mark* options as determined in Section 17.2.1, “Planning User Data Quotas,” on page 132.

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 or not you are using a secure SSL connection:

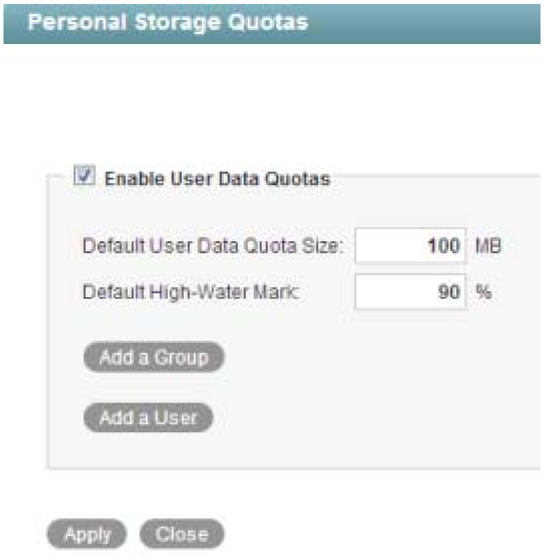
   ```
   http://filr_hostname:8443
   https://filr_hostname:8443
   ```

   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 may not be required to enter the port number in the URL, and 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 Quotas

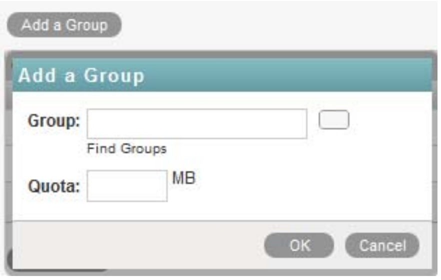
☑ Enable User Data Quotas

Default User Data Quota Size: 100 MB

Default High-Water Mark: 90 %

4 Select *Enable User Data Quotas*.

5 Click *Add a Group*.



Add a Group

Group:

Find Groups

Quota: MB

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 or not you are using a secure SSL connection:

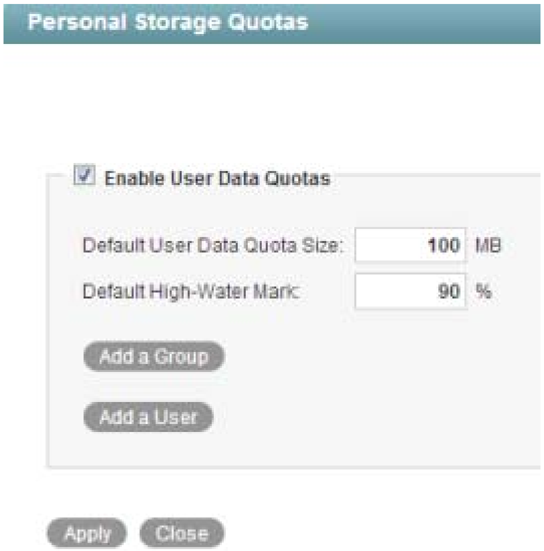
```
http://filr_hostname:8443
https://filr_hostname:8443
```

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 may not be required to enter the port number in the URL, and 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 Quotas

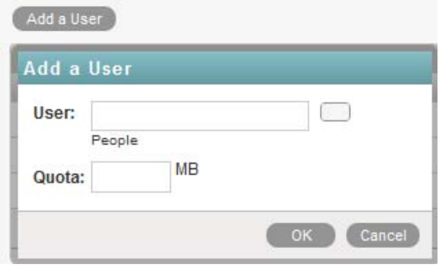
☑ Enable User Data Quotas

Default User Data Quota Size: 100 MB

Default High-Water Mark: 90 %

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.

17.2.3 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" on page 137
- "Modifying User Data Quotas for Individual Groups and Users" on page 138

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.

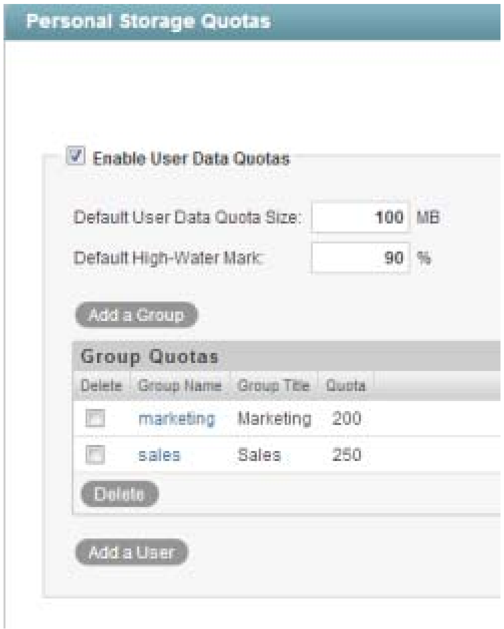
   1a Launch a web browser.

   1b Specify one of the following URLs, depending on whether or not you are using a secure SSL connection:

   ```
   http://filr_hostname:8443
   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 may not be required to enter the port number in the URL, and 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*.



☑ Enable User Data Quotas

Default User Data Quota Size: 100 MB

Default High-Water Mark: 90 %

Group Quotas

Delete	Group Name	Group Title	Quota
□	marketing	Marketing	200
□	sales	Sales	250

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 133.

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 or not you are using a secure SSL connection:

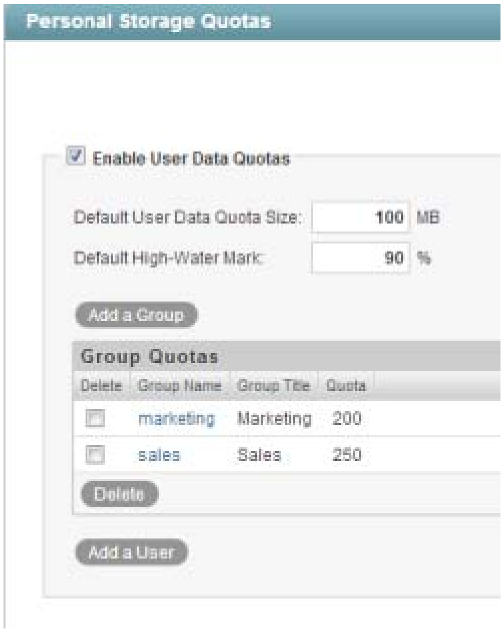
```
http://filr_hostname:8443
https://filr_hostname:8443
```

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 may not be required to enter the port number in the URL, and 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*.



☑ Enable User Data Quotas

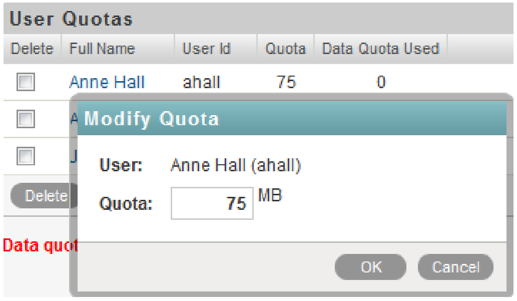
Default User Data Quota Size: 100 MB

Default High-Water Mark: 90 %

Group Quotas

Delete	Group Name	Group Title	Quota
□	marketing	Marketing	200
□	sales	Sales	250

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.



User Quotas

Delete	Full Name	User Id	Quota	Data Quota Used
□	Anne Hall	ahall	75	0
□	A			
□	J			

Modify Quota

User: Anne Hall (ahall)

Quota: 75 MB

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.

17.2.4 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 140
- “Removing User Data Quotas from Individual Groups and Users” on page 141

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 or not you are using a secure SSL connection:

```
http://filr_hostname:8443
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.

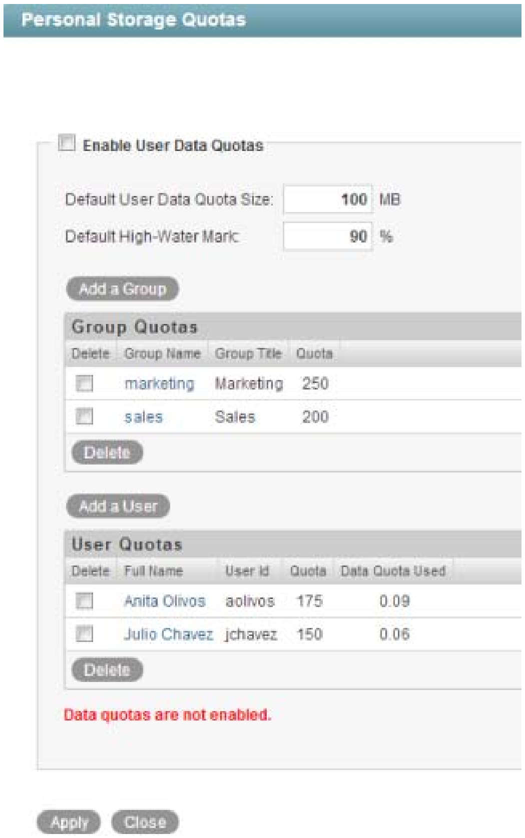
Depending on how you have configured your Filr system, you may not be required to enter the port number in the URL, and if you are using NetIQ Access Manager, the Filr login screen is not used.

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 Quotas

□ Enable User Data Quotas

Default User Data Quota Size: 100 MB

Default High-Water Mark: 90 %

Group Quotas

Delete	Group Name	Group Title	Quota
□	marketing	Marketing	250
□	sales	Sales	200

User Quotas

Delete	Full Name	User Id	Quota	Data Quota Used
□	Anita Olivos	aolivos	175	0.09
□	Julio Chavez	jchavez	150	0.06

Data quotas are not enabled.

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 or not you are using a secure SSL connection:

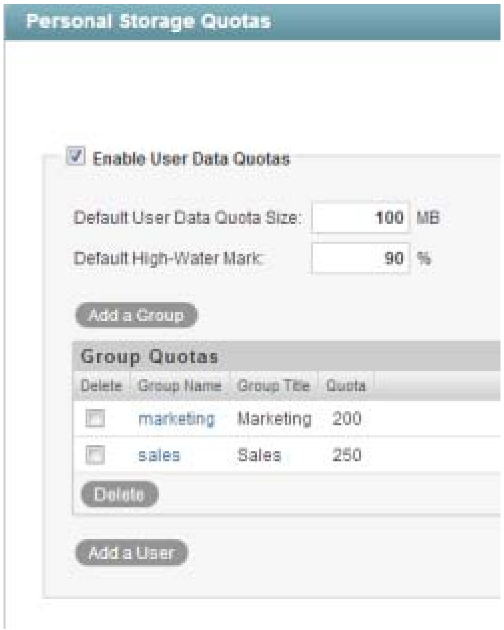
```
http://filr_hostname:8443
https://filr_hostname:8443
```

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 may not be required to enter the port number in the URL, and 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 Quotas

☑ Enable User Data Quotas

Default User Data Quota Size: 100 MB

Default High-Water Mark: 90 %

Group Quotas

Delete	Group Name	Group Title	Quota
□	marketing	Marketing	200
□	sales	Sales	250

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.

17.2.5 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” on page 142
- “Repairing a User’s Quota When a Default or Group Data Quota Is Set” on page 142

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 141.
2. Set the data quota for the user again, as described in “Setting Data Quotas for Individual Users” on page 136.

Repairing a User’s Quota When a Default or Group Data Quota Is Set

You can repair a user’s data quota when a default data quota is set, or when a group data quota is set and the user is a member of the group.

1. Set an individual data quota for the affected user, as described in “Setting Data Quotas for Individual Users” on page 136.
2. Remove the individual data quota that you just set, as described in “Removing User Data Quotas from Individual Groups and Users” on page 141.

17.2.6 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 136.

All Filr users need to manage their personal data quotas. When you have a limited allocation of disk space, you need to be aware of the amount of disk space that you have available and how to make more disk space available as you approach your quota.

For information on how to accomplish these and other important tasks as you manage your data quota, see “Managing Your Data Quota” in the *Novell Filr 1.0.1 Web Application User Guide*.

17.2.7 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 21.2.1, “Data Quota Exceeded Report,” on page 161
- Section 21.2.2, “Data Quota Highwater Exceeded Report,” on page 162

17.3 General Data Quota Management

- Section 17.3.1, “Purging Deleted Files,” on page 143

17.3.1 Purging Deleted Files

You might want to purge deleted files in order to make space available within a data quota or to recover disk space.

- “Purging Deleted Files to Create Data Quota Space” on page 143
- “Purging Deleted Files to Recover Disk Space” on page 143

Purging Deleted 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 purge the files and versions, as described in “Making Disk Space Available by Purging Deleted Items” in the *Novell Filr 1.0.1 Web Application User Guide*.

As a Filr administrator, you can purge files and versions anywhere on the Filr site in order to make space available within a user’s data quota.

Purging Deleted Files to Recover Disk Space

Whether or not disk space is recovered after you purge files using the Filr interface differs depending on whether you are purging files in Net Folders or files from a user’s personal storage in the My Files area:

- “Purging Files in Net Folders” on page 143
- “Purging Files in Personal Storage” on page 143

Purging Files in Net Folders

If you want to recover disk space on your file system, purging files in Net Folders using the Filr interface should also purge the files from the underlying file system, depending on the underlying implementation of the storage.

Purging Files in Personal Storage

If you want to recover disk space on the Filr system, you must purge the files from Filr.

For information about how to purge items, see “Making Disk Space Available by Purging Deleted Items” in the *Novell Filr 1.0.1 Web Application User Guide*.

17.4 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 17.4.1, “Modifying the File Upload Size Limit for the Filr Site,” on page 144
- Section 17.4.2, “Setting a File Upload Size Limit for Individual Users and Groups,” on page 144

17.4.1 Modifying the File Upload Size Limit for the Filr Site

You as the Filr administrator 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*.

17.4.2 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 144
- “Setting a Limit for a User” on page 145

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*.

17.5 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 2, “Configuring Email Integration,” on page 15.

18 Managing Email Configuration

After you enable email integration for the Filr site as described in Chapter 2, “Configuring Email Integration,” on page 15, you can further modify the way email is managed on the Filr site.

- Section 18.1, “Configuring Outbound Email with TLS over SMTP,” on page 147

18.1 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, as described in “Changing Outbound Email Configuration Settings” in the *Novell Filr 1.0.1 Installation and Configuration Guide*.

19 Managing the Lucene Index

For background information about the Lucene index, see “Understanding Indexing” in the *Novell Filr 1.0.1 Installation and Configuration Guide*.

- Section 19.1, “Changing Your Lucene Configuration,” on page 149
- Section 19.2, “Optimizing the Lucene Index,” on page 149
- Section 19.3, “Rebuilding the Lucene Index,” on page 151
- Section 19.4, “Performing Maintenance on a High Availability Lucene Index,” on page 152

19.1 Changing Your Lucene Configuration

You can change your Lucene Configuration settings as described in “Changing Search Index Configuration Settings” in the *Novell Filr 1.0.1 Installation and Configuration Guide*.

19.2 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.

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 19.3, “Rebuilding the Lucene Index,” on page 151.

- Section 19.2.1, “Optimizing a Single Search Index,” on page 149
- Section 19.2.2, “Optimizing the Search Index with Multiple Index Servers,” on page 150

19.2.1 Optimizing a Single Search Index

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

1a Launch a web browser.

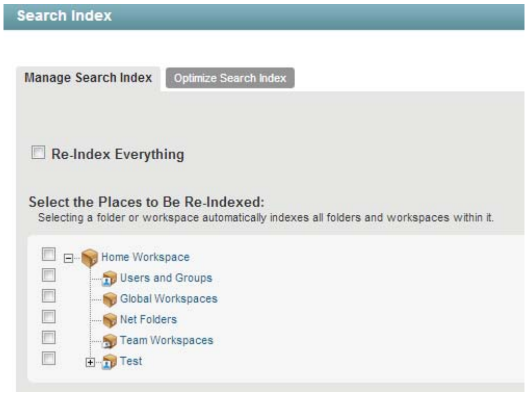
1b Specify one of the following URLs, depending on whether or not you are using a secure SSL connection:

```
http://filr_hostname:8443
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 may not be required to enter the port number in the URL, and 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*.



Search Index

Manage Search Index | Optimize Search Index

☐ Re-Index Everything

Select the Places to Be Re-Indexed:
Selecting a folder or workspace automatically indexes all folders and workspaces within it.

☐ ⊟ Home Workspace
☐ Users and Groups
☐ Global Workspaces
☐ Net Folders
☐ Team Workspaces
☐ ⊞ Test

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*.

19.2.2 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 or not you are using a secure SSL connection:

     ```
     http://filr_hostname:8443
     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 may not be required to enter the port number in the URL, and 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*.

19.3 Rebuilding the Lucene Index

The Lucene index provides access to all data in your Novell Filr site. If it 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 that they know should be available on the Filr site. If you are running multiple Lucene Index Servers, follow the instructions in Section 19.4, “Performing Maintenance on a High Availability Lucene Index,” on page 152.

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 *Novell Filr 1.0.1 Installation and Configuration Guide*.)

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

- Section 19.3.1, “Rebuilding a Single Search Index,” on page 151
- Section 19.3.2, “Rebuilding the Search Index with Multiple Index Servers,” on page 152

19.3.1 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 or not you are using a secure SSL connection:

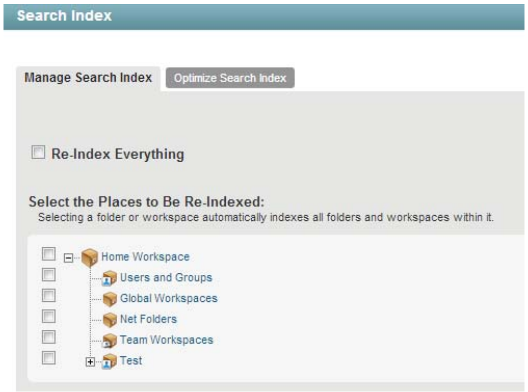
```
http://filr_hostname:8443
https://filr_hostname:8443
```

  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 may not be required to enter the port number in the URL, and 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*.



□ Re-Index Everything

Select the Places to Be Re-Indexed:
Selecting a folder or workspace automatically indexes all folders and workspaces within it.

□ Home Workspace
□ Users and Groups
□ Global Workspaces
□ Net Folders
□ Team Workspaces
□ Test

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 `ssf.log` or `ssr.log` files stating that reindexing is complete.

19.3.2 Rebuilding the Search Index with Multiple Index Servers

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

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 Section 19.4, "Performing Maintenance on a High Availability Lucene Index," on page 152.

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 Section 19.4, "Performing Maintenance on a High Availability Lucene Index," on page 152.

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 `ssf.log` or `ssr.log` files stating that reindexing is complete.

19.4 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 or not you are using a secure SSL connection:

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

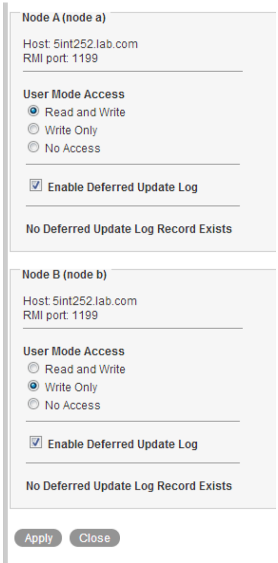
   Replace *`filr_hostname`* with the hostname or fully qualified domain name of the Filr server that you have set up in DNS.

   Depending on how you have configured your Filr system, you may not be required to enter the port number in the URL, and 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

2c In the list, locate the node that needs maintenance.

2d Make sure 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*.

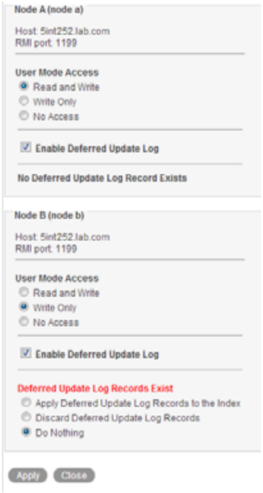
The new setting is put into effect immediately, so that the Lucene node is no longer accessible to Filr users.

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 19.3, "Rebuilding the Lucene Index," on page 151.

4 Return the out-of-date Lucene node to full service:

4a Click the *admin* link in the upper right corner of the page, then click the *Administration Console* icon.

4b Under *Search Index*, click *Nodes*.



Node A (node a)

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

User Mode Access

● Read and Write
○ Write Only
○ No Access

☑ Enable Deferred Update Log

No Deferred Update Log Record Exists

Node B (node b)

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

User Mode Access

○ Read and Write
● Write Only
○ No Access

☑ Enable Deferred Update Log

Deferred Update Log Records Exist

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

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.

20 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 inhibits your ability to update Filr in the future.

If you do use snapshots, you must remove them before updating to a new version of Filr.

- Section 20.1, "Locating Filr Data to Back Up," on page 155
- Section 20.2, "Scheduling and Performing Backups," on page 156
- Section 20.3, "Restoring Filr Data from Backup," on page 156
- Section 20.4, "Manually Restoring Individual Files," on page 156

20.1 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 20.1.1, "Filr File Repository," on page 155
- Section 20.1.2, "Filr Database," on page 155
- Section 20.1.3, "Lucene Search Index," on page 156
- Section 20.1.4, "Certificates," on page 156

20.1.1 Filr File Repository

Back up the following location on the Filr appliance:

```
/vastorage/filr/filerepository
```

For more information about the Filr file repository, see "Planning the File Repository" in the *Novell Filr 1.0.1 Installation and Configuration Guide*.

20.1.2 Filr Database

Back up the following location on the Filr appliance:

```
/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 *Novell Filr 1.0.1 Installation and Configuration Guide*.

20.1.3 Lucene Search Index

You can back up the following location on the Filr appliance:

```
/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 19.3, “Rebuilding the Lucene Index,” on page 151.

For more information about the Lucene search index, see “Search Index” in the *Novell Filr 1.0.1 Installation and Configuration Guide*.

20.1.4 Certificates

Back up the following location on the Filr appliance:

```
/vastorage/conf
```

20.2 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 one from backup can save time in case of an outage.

20.3 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.

20.4 Manually Restoring Individual Files

All Filr users can restore individual files from their personal storage if the file has been deleted but not yet purged. For information on how to do this, see “Restoring Deleted Items” in the *Novell Filr 1.0.1 Web Application User Guide*.

Unlike files from users’ personal storage, files from Net Folders cannot be restored from the Filr trash.

If a file from users’ personal storage has been deleted and also purged from the Filr site, it cannot be recovered.

21 Monitoring the Filr System

You can monitor activity on your Novell Filr site by using Filr reports and log files.

21.1 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 “Changing the Ganglia Configuration” in the *Novell Filr 1.0.1 Installation and Configuration Guide*.

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

21.1.1 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 21.1.3, “Filr Monitoring Metrics,” on page 159.

21.1.2 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 21.1.3, “Filr Monitoring Metrics,” on page 159.

   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.

21.1.3 Filr Monitoring Metrics

- “Filr Server Metrics” on page 159
- “Filr Search Metrics” on page 160

Filr Server Metrics

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.

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 Filr app server makes to the index server, because in many cases, Filr app 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 those 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).

21.2 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 filename is `report.csv`. If you create multiple reports without manually renaming them, the default filename is incremented (`report-`*`n`*`.csv`). The default location to save the report is `/tmp`.

- Section 21.2.1, “Data Quota Exceeded Report,” on page 161
- Section 21.2.2, “Data Quota Highwater Exceeded Report,” on page 162
- Section 21.2.3, “Disk Usage Report,” on page 163
- Section 21.2.4, “Email Report,” on page 164
- Section 21.2.5, “License Report,” on page 165
- Section 21.2.6, “Login Report,” on page 166
- Section 21.2.7, “User Access Report,” on page 168
- Section 21.2.8, “User Activity Report,” on page 169
- Section 21.2.9, “XSS Report,” on page 171

21.2.1 Data Quota Exceeded Report

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 17.2.2, "Setting User Data Quotas," on page 133.
- **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 17.2.2, "Setting User Data Quotas," on page 133.

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 or not you are using a secure SSL connection:

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

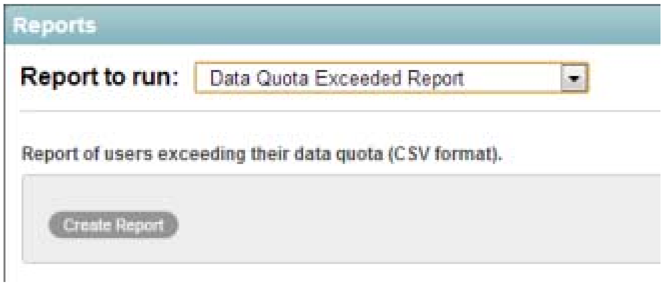
   Replace *filr_hostname* with the hostname or fully qualified domain name of the Filr server that you have set up in DNS.

   Depending on how you have configured your Filr system, you may not be required to enter the port number in the URL, and 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*.



Report to run: Data Quota Exceeded Report

Report of users exceeding their data quota (CSV format).

5 Click *Create Report* to generate the report.

   The report is launched in a spreadsheet.

21.2.2 Data Quota Highwater Exceeded Report

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 17.2.2, "Setting User Data Quotas," on page 133.
- **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 17.2.2, "Setting User Data Quotas," on page 133.

To generate the Data Quota Highwater Exceeded report:

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

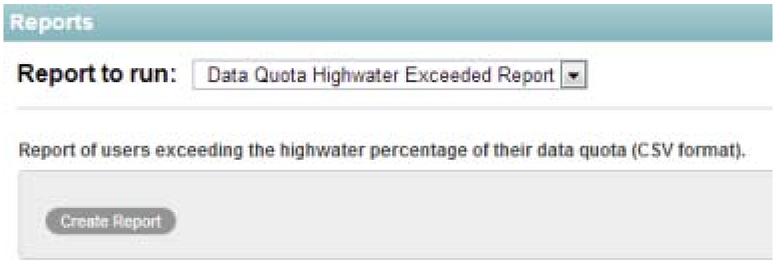
   1a Launch a web browser.

   1b Specify one of the following URLs, depending on whether or not you are using a secure SSL connection:

   ```
   http://filr_hostname:8443
   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 may not be required to enter the port number in the URL, and 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*.



Report to run: Data Quota Highwater Exceeded Report

Report of users exceeding the highwater percentage of their data quota (CSV format).

5. Click *Create Report* to generate the report.

   The report is launched in a spreadsheet.

21.2.3 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 or not you are using a secure SSL connection:

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

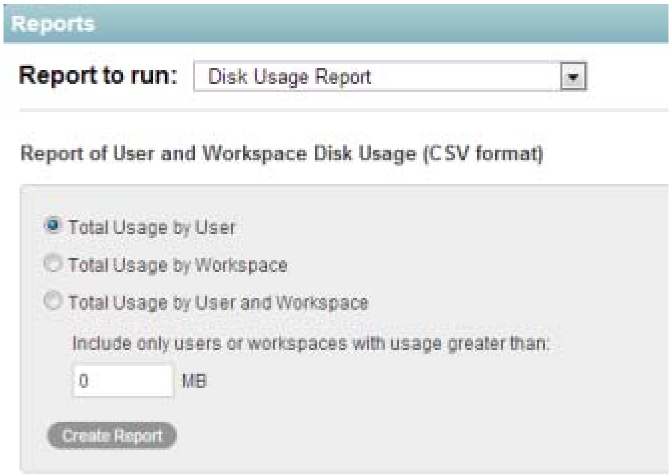
Replace `filr_hostname` with the hostname or fully qualified domain name of the Filr server that you have set up in DNS.

Depending on how you have configured your Filr system, you may not be required to enter the port number in the URL, and 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*.



Reports

Report to run: Disk Usage Report

Report of User and Workspace Disk Usage (CSV format)

● Total Usage by User
○ Total Usage by Workspace
○ Total Usage by User and Workspace

Include only users or workspaces with usage greater than: 0 MB

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.

21.2.4 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 or not you are using a secure SSL connection:

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

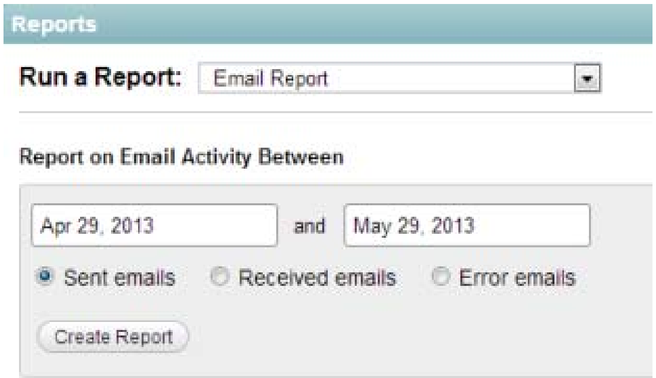
Replace `filr_hostname` with the hostname or fully qualified domain name of the Filr server that you have set up in DNS.

Depending on how you have configured your Filr system, you may not be required to enter the port number in the URL, and 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

Report on Email Activity Between

Apr 29, 2013 and May 29, 2013

● Sent emails ○ Received emails ○ Error emails

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.

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: Filename of any attachments that were included in the email message.

Errors: Any errors that are associated with the email message.

21.2.5 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 or not you are using a secure SSL connection:

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

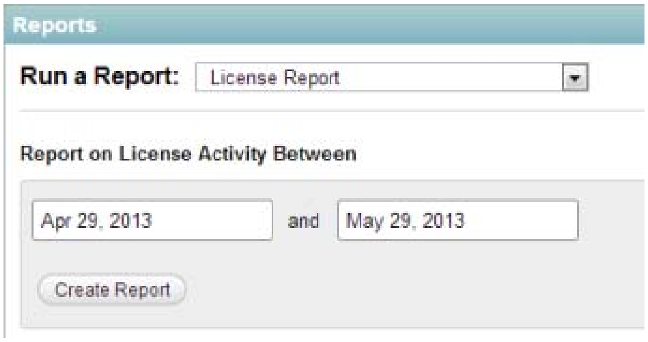
  Replace *`filr_hostname`* with the hostname or fully qualified domain name of the Filr server that you have set up in DNS.

  Depending on how you have configured your Filr system, you may not be required to enter the port number in the URL, and 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*.



Reports

Run a Report: License Report

Report on License Activity Between

Apr 29, 2013 and May 29, 2013

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, but 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.

21.2.6 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 or not you are using a secure SSL connection:

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

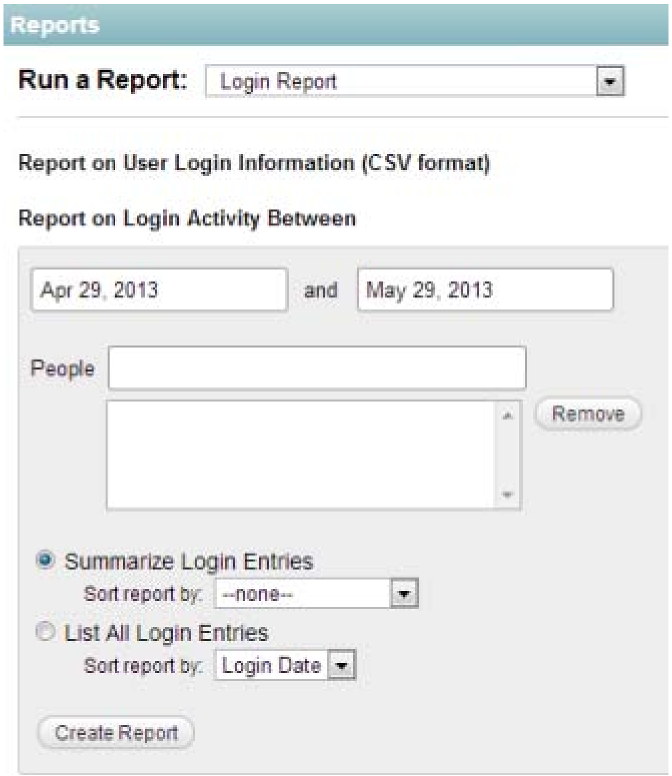
Replace `filr_hostname` with the hostname or fully qualified domain name of the Filr server that you have set up in DNS.

Depending on how you have configured your Filr system, you may not be required to enter the port number in the URL, and 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

● Summarize Login Entries

Sort report by: --none--

○ List All Login Entries

Sort report by: Login Date

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:

   - First name
   - Last name
   - Username
   - Date
   - Time

   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.

21.2.7 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 6.3, “Allowing External Users Access to Your Filr Site,” on page 61.

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 or not you are using a secure SSL connection:

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

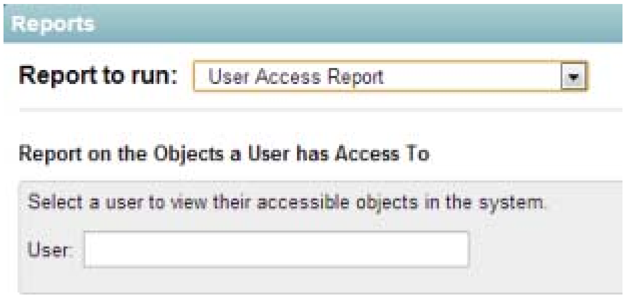
Replace `filr_hostname` with the hostname or fully qualified domain name of the Filr server that you have set up in DNS.

Depending on how you have configured your Filr system, you may not be required to enter the port number in the URL, and 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*.



Reports

Report to run: User Access Report ▾

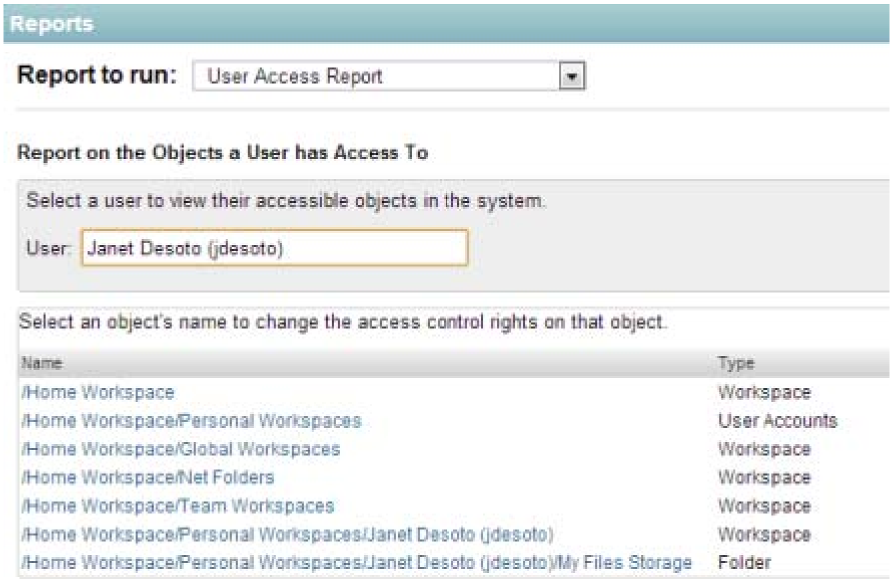
Report on the Objects a User has Access To

Select a user to view their accessible objects in the system.

User:

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.



Reports

Report to run: User Access Report

Report on the Objects a User has Access To

Select a user to view their accessible objects in the system.

User: Janet Desoto (jdesoto)

Select an object's name to change the access control rights on that object.

Name	Type
/Home Workspace	Workspace
/Home Workspace/Personal Workspaces	User Accounts
/Home Workspace/Global Workspaces	Workspace
/Home Workspace/Net Folders	Workspace
/Home Workspace/Team Workspaces	Workspace
/Home Workspace/Personal Workspaces/Janet Desoto (jdesoto)	Workspace
/Home Workspace/Personal Workspaces/Janet Desoto (jdesoto)/My Files Storage	Folder

7 (Conditional) The following steps are for informational purposes only. Novell recommends that you do not modify access controls in Filr as described below. Instead, use file system access controls.

- **7a** Click the name of a location to display the Configure Access Control page for that location.

  In this example, the Guest user has been granted Visitor access to Janet DeSoto's personal workspace.

- **7b** Select or deselect access rights as needed.
- **7c** Click *Save Changes*, then click *Close* to return to the User Access Report page
- **7d** Rerun the report to view the results of your changes.

8 (Conditional) If you want to save the user access information, select it and copy it into a text editor.

9 Click *Close* when you are finished checking user access rights.

21.2.8 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 or not you are using a secure SSL connection:

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

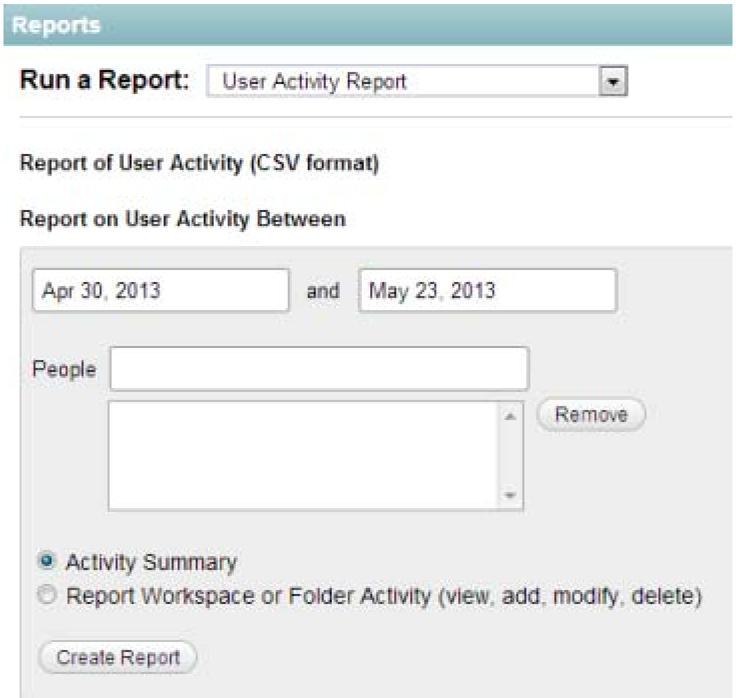
  Replace `filr_hostname` with the hostname or fully qualified domain name of the Filr server that you have set up in DNS.

  Depending on how you have configured your Filr system, you may not be required to enter the port number in the URL, and 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*.



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

● Activity Summary

○ Report Workspace or Folder Activity (view, add, modify, delete)

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:

- View
- Add
- Edit
- Delete (purge)
- Pre-Delete (delete but not purge)
- Restore (restore a deleted item that has not been purged)

Workspace or Folder Activity: Lists each individual user action and includes the following data about the action:

- User
- Activity
- Date

   - Time
   - Folder
   - Entry title
   - Entry type

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.

21.2.9 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 25.4.3, "Securing the Filr Site against XSS," on page 197.

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.

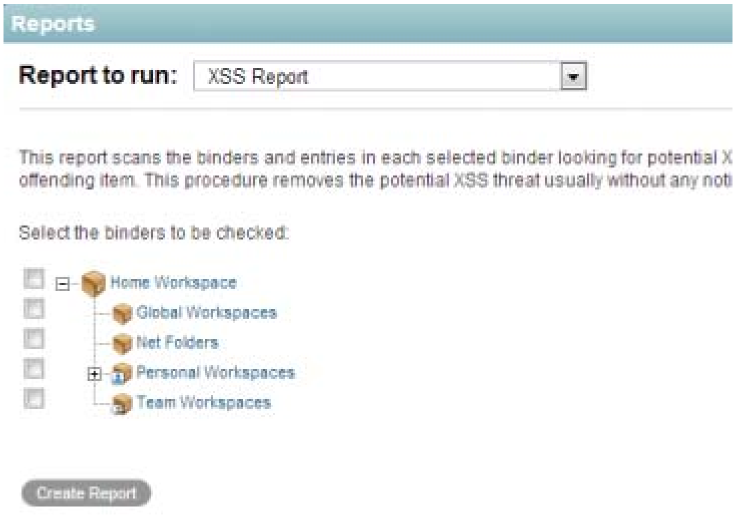
   1a Launch a web browser.

   1b Specify one of the following URLs, depending on whether or not you are using a secure SSL connection:

   ```
   http://filr_hostname:8443
   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 may not be required to enter the port number in the URL, and 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*.



Reports

Report to run: XSS Report

This report scans the binders and entries in each selected binder looking for potential X
offending item. This procedure removes the potential XSS threat usually without any noti

Select the binders to be checked:

- □ Home Workspace
- □ Global Workspaces
- □ Net Folders
- □ Personal Workspaces
- □ Team Workspaces

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).

21.3 Using the Filr Log File

- Section 21.3.1, "Filr Log File," on page 172

21.3.1 Filr Log File

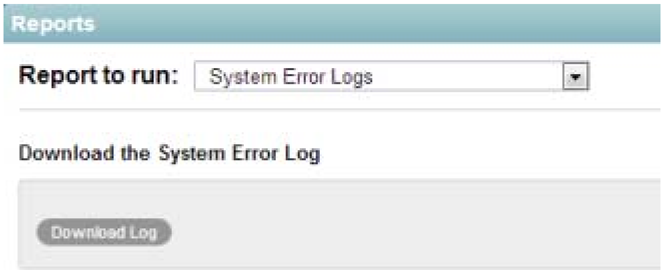
The Novell Filr log file (`ssf.log`) is available from the Filr site.

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*.



Reports

Report to run: System Error Logs

Download the System Error Log

5 Click *Download Log*.

You are prompted to open or save a file named `logfiles.zip`, which contains the current `ssf.log` file. This file contains any stack traces or warning messages because of unexpected events encountered by the Filr program.

6 Save the `ssf.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.

21.4 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 appliance shuts down.

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 an appliance shuts down because of low disk space, a message is logged to both the `/var/opt/novell/va_status` and `/var/log/messages` files.

After the appliance is shut down, you must clean up unneeded data or add additional disk space to the appliance before restarting it.

21.5 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 or not you are using a secure SSL connection:

```
http://filr_hostname:8443
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 may not be required to enter the port number in the URL, and 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 Click the information icon ⓘ.

The Filr software version and date are displayed in the Administration Information dialog box.

III 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.

- Chapter 22, “NetIQ Access Manager,” on page 177
- Chapter 23, “Novell Dynamic File Services,” on page 179

22 NetIQ Access Manager

Using Novell Filr in conjunction with NetIQ Access Manager adds enterprise-level security to your Filr system.

IMPORTANT: When you use NetIQ Access Manager with Filr, external users cannot access your Filr site. This means that the following features are not functional:

- Users are not able to share with external users, as described in “Sharing with People Outside Your Organization” in the *Novell Filr 1.0.1 Web Application User Guide*.
- Users cannot make items accessible to the public, as described in “Making Files Accessible to the Public” in the *Novell Filr 1.0.1 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 6.3.1, “Allowing Guest Access to Your Filr Site,” on page 61.

For more information about external users in Filr, see Section 6.3, “Allowing External Users Access to Your Filr Site,” on page 61.

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 8, “Allowing Access to the Filr Site through NetIQ Access Manager,” on page 69.

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 “Changing Reverse Proxy Configuration Settings” in the *Novell Filr 1.0.1 Installation and Configuration Guide*.

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” in the *Novell Filr 1.0.1 Installation and Configuration Guide*.

23 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)

IV Site Security

24 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.

- "Replacing the Self-Signed Digital Certificate for an Official Certificate" on page 183
- Section 24.2, "Securing LDAP Synchronization," on page 185
- Section 24.3, "Securing Email Transfer," on page 192
- Section 24.4, "Setting Up Filr in a DMZ," on page 192
- Section 24.5, "Filr Component Security," on page 194

24.1 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.

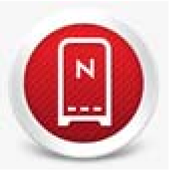
- "Using the Digital Certificate Tool" on page 183
- "Using an Existing Certificate and Key Pair" on page 184
- "Activating the Certificate" on page 185

24.1.1 Using the Digital Certificate Tool

- "Creating a New Self-Signed Certificate" on page 183
- "Getting Your Certificate Officially Signed" on page 184

Creating a New Self-Signed Certificate

1 Log in to the Novell appliance at https://*server_url*:9443, then click the Appliance Configuration icon.



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 184.

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 24.1.3, "Activating the Certificate," on page 185.

24.1.2 Using an Existing Certificate and Key Pair

When you use an existing certificate and key pair, 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 4, 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.
7. Continue with Section 24.1.3, “Activating the Certificate,” on page 185.

24.1.3 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, then clicking *View Info*.

24.2 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 generate a self-signed root certificate based on your eDirectory or Active Directory tree.

- Section 24.2.1, “Generating a Root Certificate,” on page 185
- Section 24.2.2, “Importing the Root Certificate into the Java Keystore,” on page 191

24.2.1 Generating a Root Certificate

- “Generating a Root Certificate for eDirectory” on page 185
- “Generating the Root Certificate for Active Directory” on page 186

Generating 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 self-signed certificate and click *Validate*.
8. Select the check box for the self-signed certificate and 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 filename that you can remember, such as `SelfSignCert.der`.

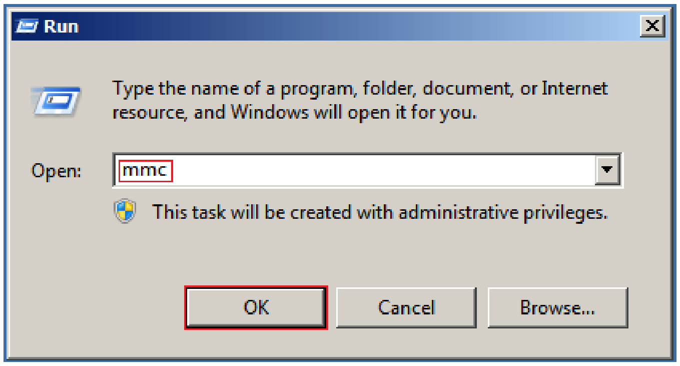
12 Click *Close* > *OK*.

13 Continue with Section 24.2.2, “Importing the Root Certificate into the Java Keystore,” on page 191.

Generating the Root Certificate for Active Directory

Generate a self-signed certificate for Active Directory:

1 On the Windows server, click *Start* > *Run*, then enter `mmc`.



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

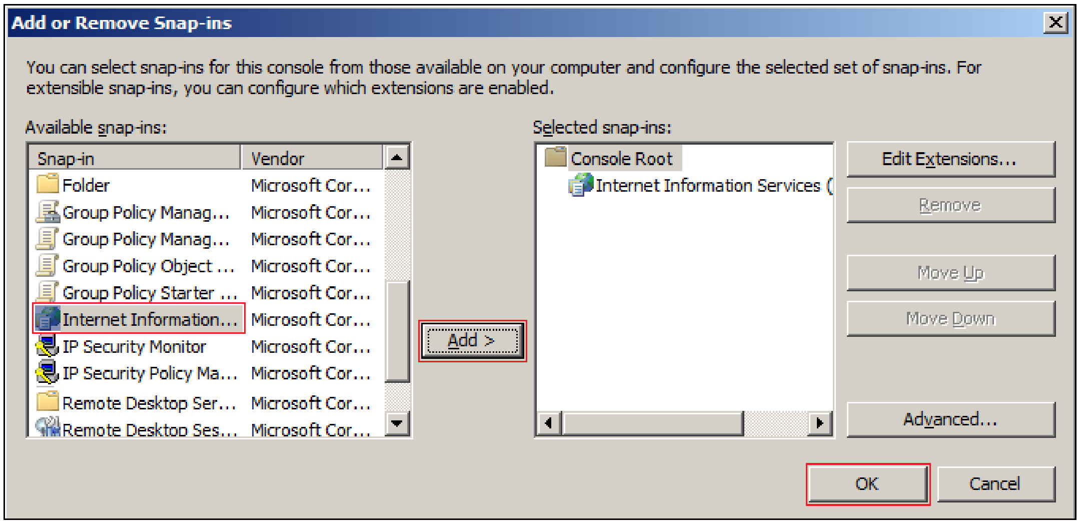
Open: mmc

This task will be created with administrative privileges.

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*.



You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

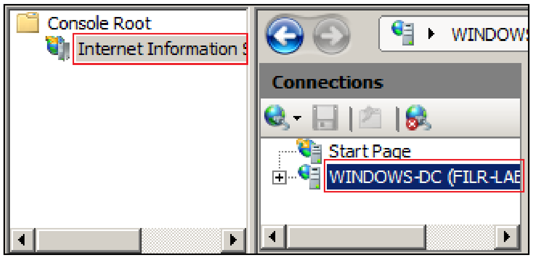
Available snap-ins:

Snap-in	Vendor
Folder	Microsoft Cor...
Group Policy Manag...	Microsoft Cor...
Group Policy Manag...	Microsoft Cor...
Group Policy Object ...	Microsoft Cor...
Group Policy Starter ...	Microsoft Cor...
Internet Information...	Microsoft Cor...
IP Security Monitor	Microsoft Cor...
IP Security Policy Ma...	Microsoft Cor...
Remote Desktop Ser...	Microsoft Cor...
Remote Desktop Ses...	Microsoft Cor...

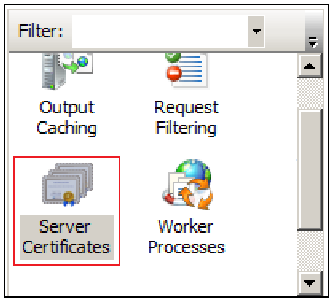
Selected snap-ins:

Console Root
Internet Information Services (

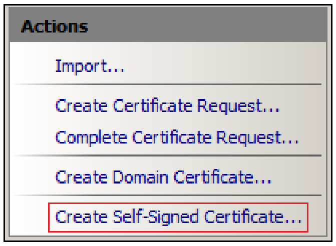
5 In the left frame, click *Internet Information Services*, then click a Windows server that Filr can connect to for synchronizing users.



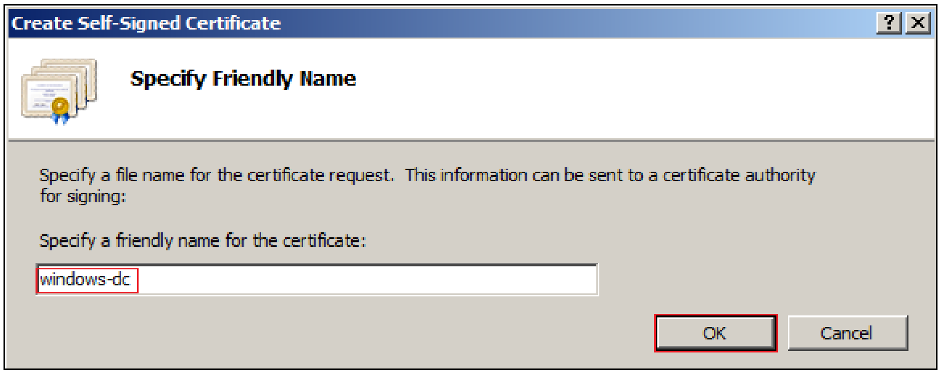
6 In the Filter list, scroll down to *Server Certificates* and double-click the icon.



7 In the *Actions* list, click *Create Self-Signed Certificate*.


Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...

8 Name the certificate with a name you can remember, such as the server name, then click *OK*.

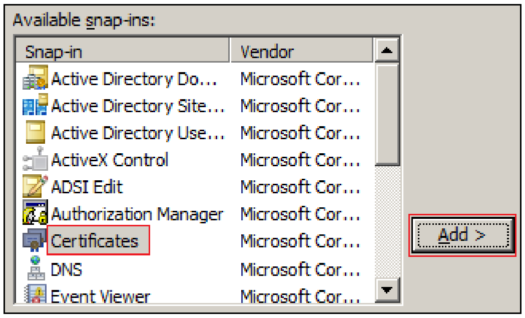


Specify a file name for the certificate request. This information can be sent to a certificate authority for signing:

Specify a friendly name for the certificate:

windows-dc

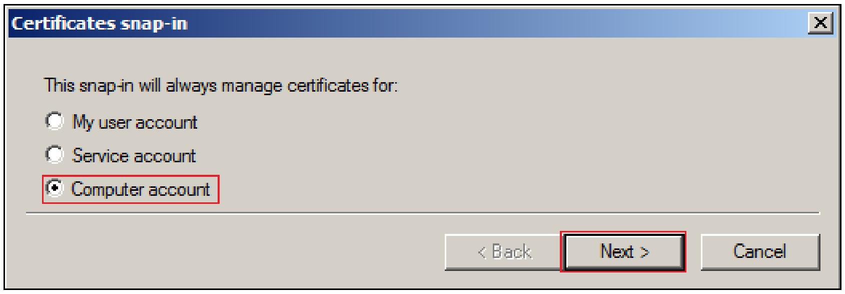
9 Type Ctrl+M, select the *Certificates* plug-in, then click *Add*.



Available snap-ins:

Snap-in	Vendor
Active Directory Do...	Microsoft Cor...
Active Directory Site...	Microsoft Cor...
Active Directory Use...	Microsoft Cor...
ActiveX Control	Microsoft Cor...
ADSI Edit	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificates	Microsoft Cor...
DNS	Microsoft Cor...
Event Viewer	Microsoft Cor...

10 Select *Computer account*, then click *Next*.



Certificates snap-in

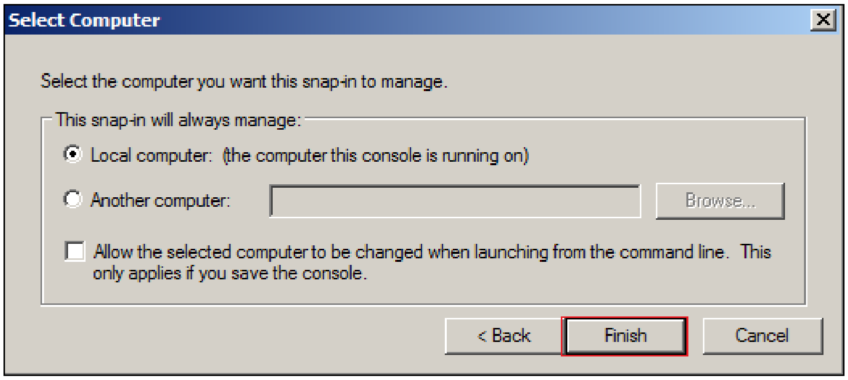
This snap-in will always manage certificates for:

○ My user account

○ Service account

● Computer account

11 Click *Finish*.



Select Computer

Select the computer you want this snap-in to manage.

This snap-in will always manage:

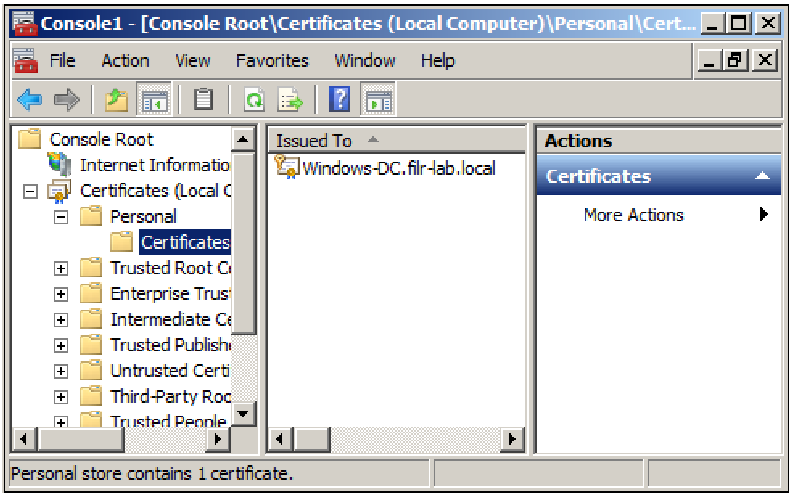
● Local computer: (the computer this console is running on)

○ Another computer:

□ Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.

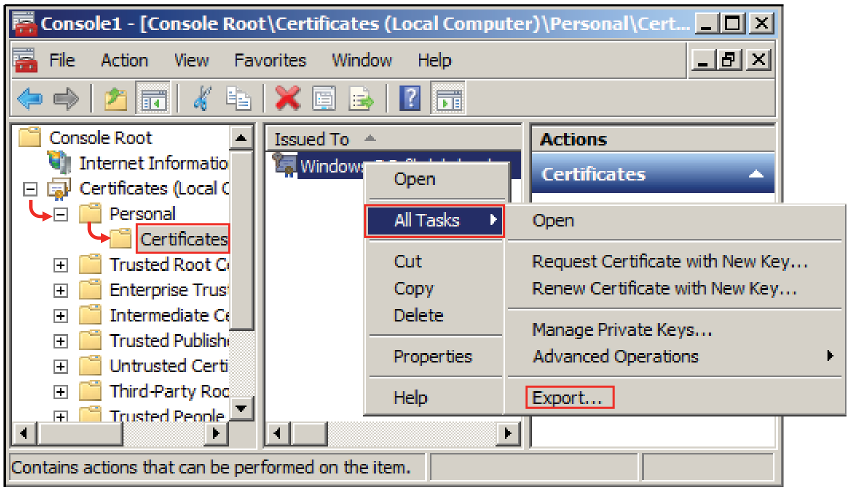
12 In the Snap-ins dialog, click *OK*.

13 In MMC, expand the *Certificates* plug-in, expand *Personal*, then click *Certificates*.



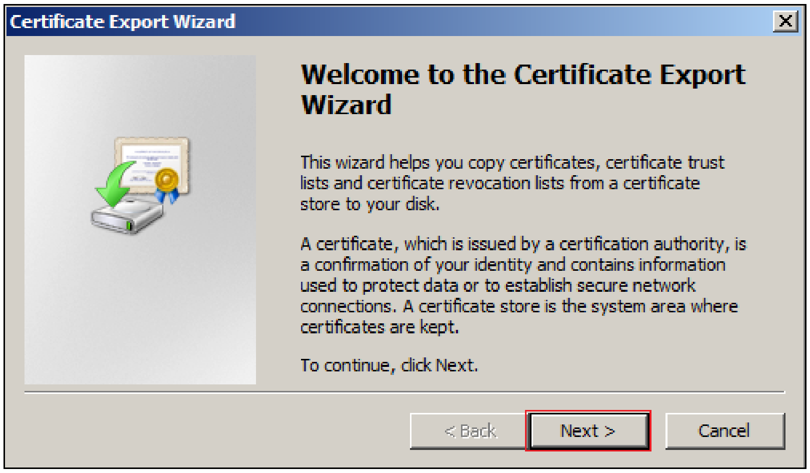
Personal store contains 1 certificate.

14 Right-click the certificate you created, select *All Tasks*, then click *Export...*.



Contains actions that can be performed on the item.

15 In the Certificate Export wizard, click *Next*.



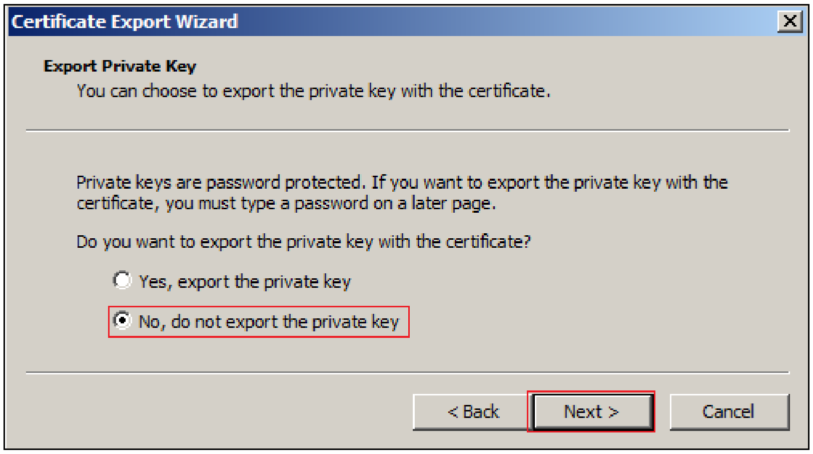
Welcome to the Certificate Export Wizard

This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

16 Ensure that *No, do not export the private key* is selected, then click *Next*.



Certificate Export Wizard

Export Private Key

You can choose to export the private key with the certificate.

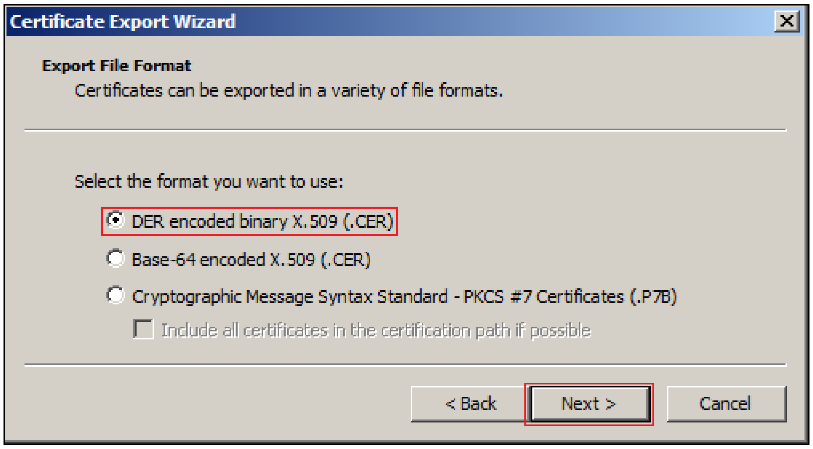
Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

Do you want to export the private key with the certificate?

○ Yes, export the private key

● No, do not export the private key

17 Ensure that *DER encoded binary* is selected, then click *Next*.



Certificate Export Wizard

Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

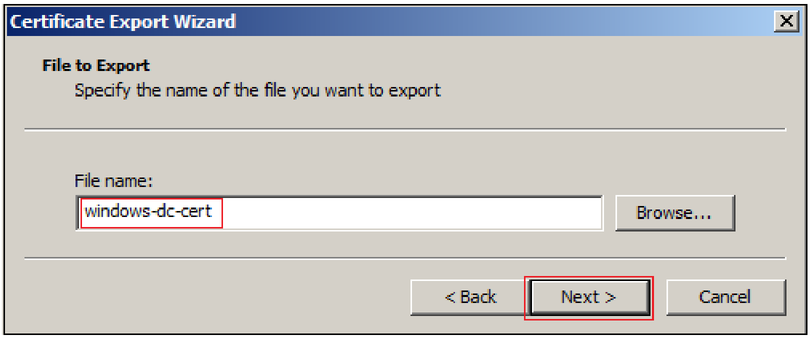
● DER encoded binary X.509 (.CER)

○ Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

□ Include all certificates in the certification path if possible

18 Name the certificate, then click *Next*.



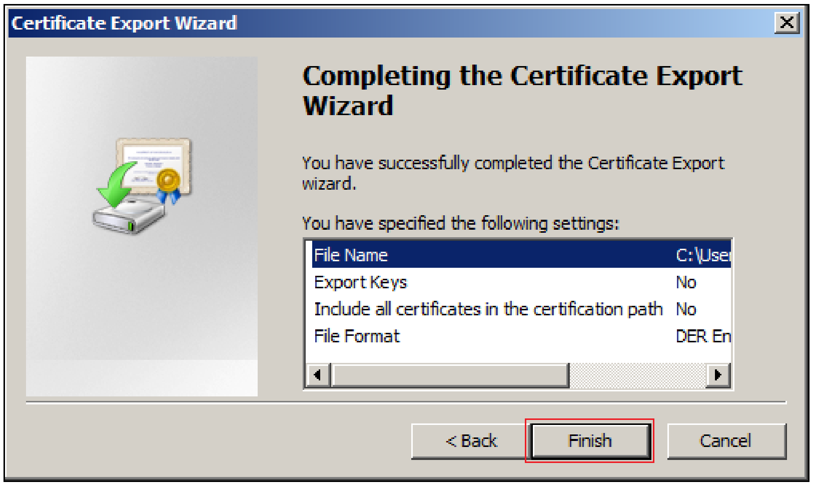
Certificate Export Wizard

File to Export

Specify the name of the file you want to export

File name: windows-dc-cert

19 Click *Finish* > *OK*.



Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

File Name	C:\Use
Export Keys	No
Include all certificates in the certification path	No
File Format	DER En

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 24.2.2, “Importing the Root Certificate into the Java Keystore,” on page 191.

24.2.2 Importing the Root Certificate into the Java Keystore

1 Navigate to the management console of your Filr 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 are now ready to configure your Filr site for secure LDAP synchronization, as described in Section 14.1, “Synchronizing Users and Groups from an LDAP Directory,” on page 111.

24.3 Securing Email Transfer

When you install Novell Filr, you can choose whether or not the Filr internal mail host uses TLS (Transport Layer Security) when it communicates with other SMTP mail hosts.![Dennis is working on how to do this]

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 24.2, "Securing LDAP Synchronization," on page 185 to set up secure SMTP for communications with your email system.

24.4 Setting Up Filr in a DMZ

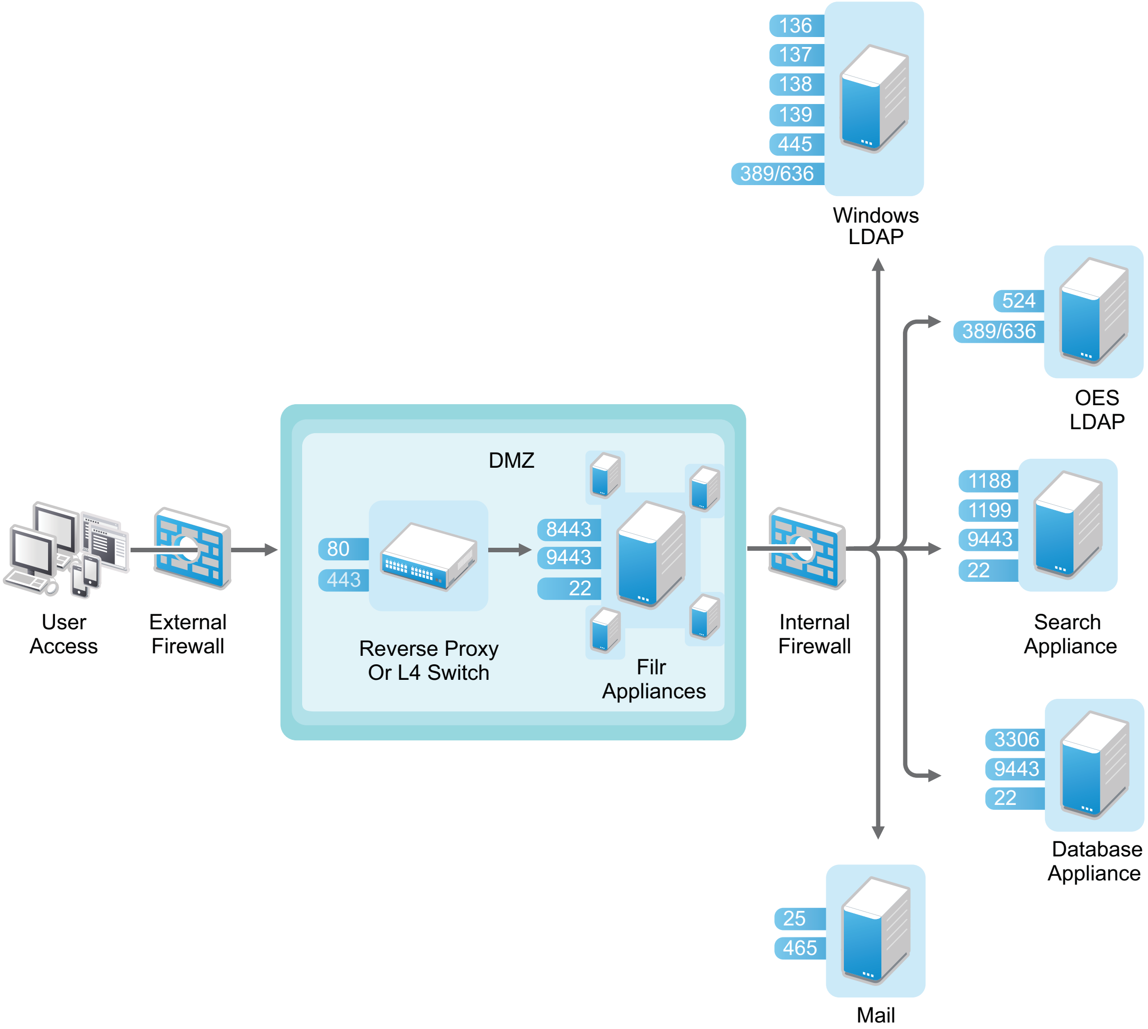
IMPORTANT: Security is a complex subject and Novell does not attempt to suggest a complete defense solution with this example. Novell recommends that you consult with your security professional to implement Filr in a DMZ.

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 6.3, "Allowing External Users Access to Your Filr Site," on page 61). 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, but 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.

The following graphic 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 24-1 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 “Changing Clustering Configuration Settings” in the *Novell Filr 1.0.1 Installation and Configuration Guide*.

For more information about port configuration in Filr, see “Port Numbers” in “Network Configuration” in the *Novell Filr 1.0.1 Installation and Configuration Guide*.

For information about setting up NetIQ Access Manager as a reverse proxy, see Chapter 22, “NetIQ Access Manager,” on page 177.

For information about configuring Apache as a load balancer, see “Configuring Apache as a Load Balancer” in the *Novell Filr 1.0.1 Installation and Configuration Guide*.

24.5 Filr Component Security

24.5.1 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.

24.5.2 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.

24.5.3 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.

25 Security Policies

25.1 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.

25.2 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 it 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.

25.3 Securing the Filr Data

- Section 25.3.1, “Understanding Administrator Access to Filr Data,” on page 196
- Section 25.3.2, “Limiting Physical Access to Filr Servers,” on page 196
- Section 25.3.3, “Protecting the Filr Database,” on page 196

25.3.1 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).

25.3.2 Limiting Physical Access to Filr Servers

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

25.3.3 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 “Database Location” in the *Novell Filr 1.0.1 Installation and Configuration Guide*. For example, for MySQL, you might add `useSSL=true&requireSSL=true` to the `options` part of the JDBC URL.

25.4 Securing the Filr Site

- Section 25.4.1, “Configuring a Proxy Server,” on page 197
- Section 25.4.2, “Setting the Filr Administrator Password,” on page 197
- Section 25.4.3, “Securing the Filr Site against XSS,” on page 197

25.4.1 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 “Changing Reverse Proxy Configuration Settings” in the *Novell Filr 1.0.1 Installation and Configuration Guide*.

25.4.2 Setting the Filr Administrator Password

The Filr site is initially installed to allow administrator access by using the username `admin` and the password `admin`. The Filr administrator password should be changed immediately after installation, as described in Section 1.2, “Resetting the Filr Administrator Password,” on page 14.

25.4.3 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 197
- “Understanding Where the Content Is Not Permitted” on page 197
- “Listing All XSS Threats in Your System” on page 197

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 197 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 21.2.9, “XSS Report,” on page 171.

25.5 Securing Filr Data on Mobile Devices

For information about data security for mobile devices, see Section 9.4, “Understanding Filr Data Security for Mobile Devices,” on page 83.

25.6 Securing the Filr Desktop Application

For information about data security for the Filr desktop application, see Chapter 10, “Configuring the Filr Desktop Application to Access Files,” on page 85.

25.7 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).

25.8 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:** User 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. Whoever has that URL can access the shared information.

25.9 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.

25.10 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.

25.11 External Users and OpenID

- External users provision themselves via a registration and validation process.
- External users’ credentials are encrypted and securely stored and protected in Filr.
- Filr also supports the OpenID authentication standard.

  OpenID users authenticate through the OpenID provider. OpenID user credentials are never stored or copied to Filr’s credential storage area.

25.12 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.

25.13 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.

25.14 Audit Trail

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

25.15 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 are:
  - **None:** No rights
  - **Viewer:** READ and VISIBILITY rights
  - **Editor:** READ, WRITE and VISIBILITY rights (WRITE include 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-folder, Filr will ensure that Tom has VISIBILITY rights to all parents up to the top level of the Net Folder or My Files container.

25.16 Anti Virus

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

25.17 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.

25.18 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.

25.19 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.

25.20 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.

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 “Changing Network Settings” in the *Novell Filr 1.0.1 Installation and Configuration Guide*.

A.2 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 “Changing the Network Configuration Settings” in the *Novell Filr 1.0.1 Installation and Configuration Guide*), 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 “Changing Reverse Proxy Configuration Settings” in the *Novell Filr 1.0.1 Installation and Configuration Guide*.

A.3 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

Error Code	Interpretation
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
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

A.4 Enabling Debug Logging

To enable debug logging for Filr:

1 In a text editor, open the `log4j.properties` file from both of the following directories:

/`opt/novell/filr/apache-tomcat/webappas/ssf/WEB-INF/`

`/opt/novell/filr/apache-tomcat/webapps/ssr/WEB-INF/`

2 Uncomment each line that 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/ssf.log` file.

B Documentation Updates

This section summarizes the changes made to the guide since the initial release of Novell Filr 1.0.

May 2014

Location	Update
Section 10.6, “Managing the Filr Desktop Application,” on page 93.	Added information about how to manage the Filr desktop application on users’ workstations with client management software such as Novell ZENworks.

April 2014

Location	Update
Chapter 7, “Setting Up Site Branding,” on page 65	Added information about pixel height and width when creating a brand.

March 2014

Location	Update
Section 10.4, “Updating the Filr Desktop Application,” on page 90	Updated section about how to update the Filr desktop application (to the Filr Desktop 1.0.2 or later) on the Filr server or on a separate web server.
Section 10.3, “Configuring a Separate Web Server to Deploy the Filr Desktop Application,” on page 89	Simplified process for making the Filr desktop application available from a separate web server.

March 2014

Location	Update
Section 9.3.1, “Configuring ZMM to Manage the Filr App,” on page 78	Updated section to include iOS support with iOS 7.1. This section links to detailed information within the ZENworks Mobile Management documentation.

January 2014

Location	Update
Section 9.3.1, “Configuring ZMM to Manage the Filr App,” on page 78	Added section about configuring ZMM to manage the Filr 1.0.3 mobile app. This section links to detailed information within the ZENworks Mobile Management documentation.

November 2013

Location	Update
Section 5.1.5, “Planning the Synchronization Schedule,” on page 37	Added section explaining the considerations to make when configuring a synchronization schedule for a Net Folder or Net Folder Server.
Chapter 5, “Setting Up Net Folders,” on page 31	Added a video explaining planning considerations for Net Folders.
“Rights Requirements for the Proxy User” on page 32	Changed format and added information for NTFS file systems.

October 2013

Location	Update
“Generating the Root Certificate for Active Directory” on page 186	Added section describing how to import the root LDAP certificate for Active Directory.
Section 9.3.2, “Configuring MobileIron to Manage the Filr App,” on page 78	Added section describing how to configure Filr with MobileIron.
Section 5.1.6, “Planning a Clustered Filr System to Support Net Folder Synchronization,” on page 37	Added section describing the benefit of setting aside a separate Filr appliance to perform Net Folder synchronization.
Section 3.1, “Understanding Sharing,” on page 19	Added information about how file system rights map to Filr rights in regard to sharing files and folders.

September 2013

Location	Update
Section 5.1.7, “Planning the Amount of Data to Synchronize,” on page 38	Added section explaining the amount of data that can be synchronized to a Net Folder in a given amount of time.