Configuring FTP Access

You can access data using the FTP/SFTP protocol.

This document will guide you in the procedures for configuring FTP/SFTP access.

Overview of Configuring FTP/SFTP Access

In order to access data using the FTP/SFTP protocol, the following steps are necessary:

- Create a CIFS or NFS volume. See “Adding a CIFS or NFS Volume” on page 2.
- Enable the FTP protocol on the volume. See “Enabling the FTP Protocol on a Volume” on page 4.
- (Optional) Configure FTP settings. See “Configuring FTP Settings (optional)” on page 6.
- Add a new FTP/SFTP directory. See “Adding FTP Directories for a Volume” on page 7.
- (Optional) Create a permission group that has storage access. See “Adding a Permission Group with Storage Access (optional)” on page 14.
- (Optional) Create a user in a permission group that has storage access. See “Adding Users (optional)” on page 16. Active Directory and LDAP users can log in for FTP access just as they do for CIFS access. Also, if anonymous access is enabled, you don't need a specific group or user.
- Access files using the FTP/SFTP protocol. See “Accessing Data using the FTP/SFTP Protocol” on page 19.

  Note: *See www.nasuni.com/support/documentation for all Nasuni documentation.*

Adding a CIFS or NFS Volume

This section explains how to add a new CIFS or NFS volume.

> ***Note:*** *This is an abbreviated procedure. See the Nasuni Filer Administration Guide for the complete procedure.*

To add a new CIFS or NFS volume, follow these steps:

1. Click **Volumes**, then click **All Volumes** from the list.

   > ***Note:*** *If this Nasuni Filer is under Nasuni Management Console control, this page is not available on the Nasuni Filer. Instead, use the Nasuni Management Console to view information or perform actions.*

2. Click **Add New Volume**. The **Add New Volume** page appears.

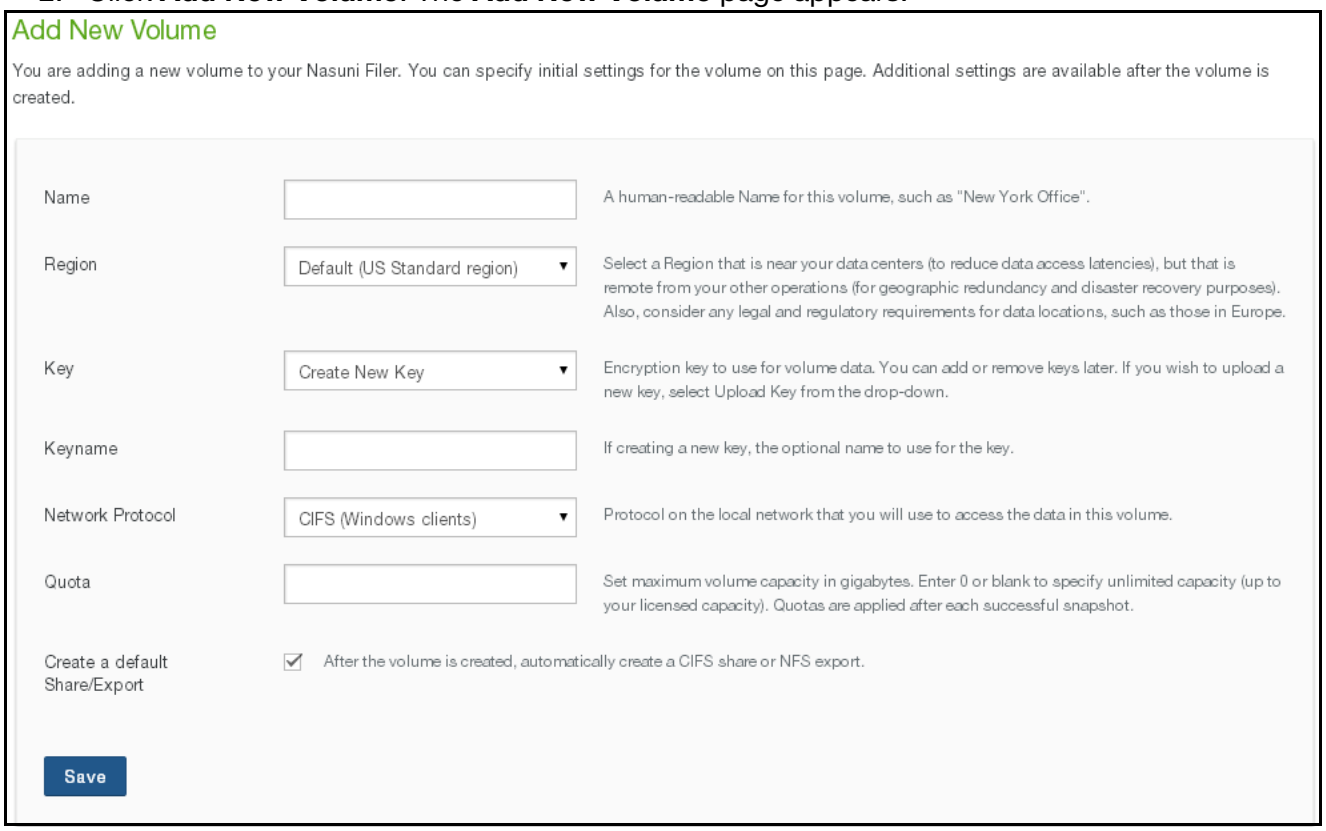

Figure 1-1: Add New Volume page.

3. Enter or select information for **Name**, **Region**, encryption key, and **Quota**.

4. From the **Network Protocol** drop-down list, select a network protocol on your network. This is the protocol you use to access files on a volume. Your choices are:

   - **CIFS (Windows clients)**: This protocol allows Windows users to share files across a network. The CIFS protocol is used on other operating systems besides Windows, including UNIX, Linux, and Mac OSX.
   - **NFS (Unix clients)**: This protocol allows UNIX users to access and share file systems across a computer network using UNIX and Linux.

     Note: *You can enable FTP/SFTP access to a CIFS volume or an NFS volume after the volume is created. See* *"You can add up to 150 permission groups to which you can assign users. For each group, you can specify exactly which actions the users in that group have permission to perform. You can associate Active Directory and LDAP domain groups with a permission group." on page 14.*

5. For CIFS and NFS volumes only, to automatically create a CIFS share or an NFS export for the new volume, leave the **Create a default Share/Export** check box selected.
6. For CIFS volumes only, if the Nasuni Filer is configured for Active Directory or LDAP authentication, the **CIFS-Specific Properties** area appears. Enter or select values to configure the CIFS volume.
7. Click **Save**.

   A message appears telling you that the new volume creation is complete. Click **x** to close the message box. The new volume appears on the Home page under Volumes.

Enabling the FTP Protocol on a Volume

You can assign CIFS, NFS, and FTP protocols to existing CIFS and NFS volumes. This enables you to allow access to data using multiple protocols. This might be helpful for simplifying access by users or applications.

> ***Tip:*** *You cannot assign multiple protocols to a volume to which a volume running a pre-6.0 version is connected. Update the connected volume to version 6.0 or later first, then perform a snapshot for the volume.*
>
> ***Note:*** *If this volume has Remote Access enabled and other volumes connect to this volume, the connected volumes inherit the same protocols as this volume. If these protocols change, the connected volumes inherit the changed protocols. This can take some time. You can refresh the volume connections in order to inherit the changed protocols immediately. The connected Nasuni Filer must be running version 6.0 or later software in order to connect to a remote volume that has multiple protocols defined.*
>
> ***Warning:*** *Protocols work in parallel. Enabling an additional protocol to an original protocol does not affect the original protocol. However, writing data to the volume using one protocol can affect the permissions or other metadata used by another protocol. This can inadvertently affect permissions in unexpected ways.*

To enable the FTP protocol for a CIFS or NFS volume, follow these steps:

1. Click **Volumes**, then select a CIFS or NFS volume from the list.

   > ***Note:*** *If this Nasuni Filer is under Nasuni Management Console control, this page is not available on the Nasuni Filer. Instead, use the Nasuni Management Console to view information or perform actions.*

2. Select **Volume Protocols** from the **Properties** drop-down list. The **Enabled Volume Protocols** page appears.

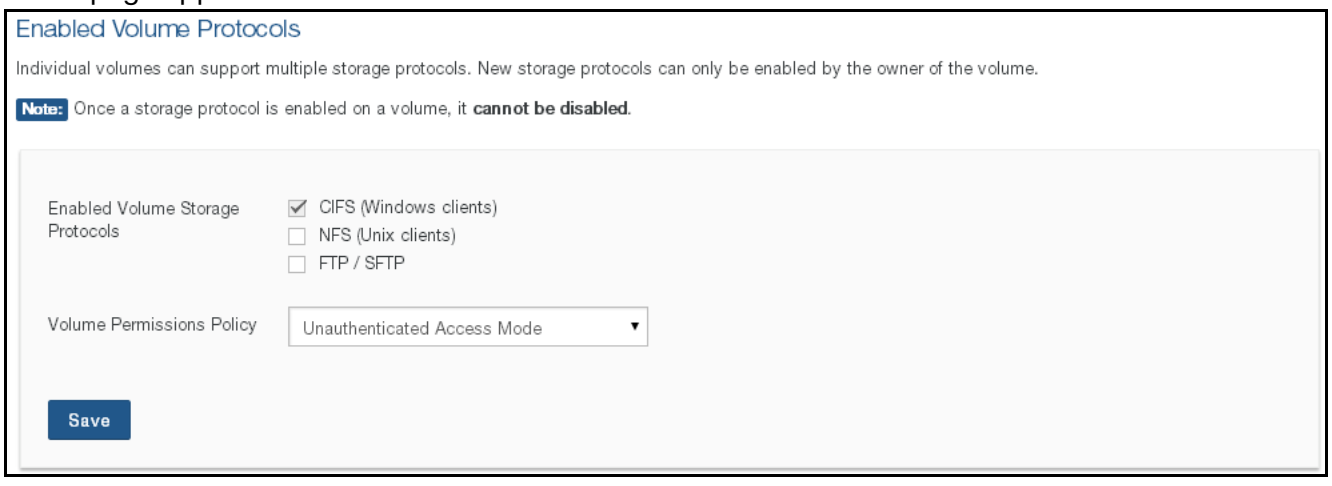

Figure 1-2: Enabled Volume Protocols page.

   The currently enabled protocols for the volume are selected.

3. Select **FTP/SFTP**.

   > ***Warning:*** *After enabling a protocol, you cannot disable that protocol.*

4. From the **Volume Permissions Policy** drop-down list, select one of the following:
    - **UNIX/NFS Permissions Only Mode**: Default mode for NFS volumes. Recommended for primary or heavy NFS use. Not recommended for Windows users. Only the traditional UNIX mode bits control permissions (chmod). Windows can view permissions as access control lists (ACLs), but cannot add or remove access control entries (ACEs). Windows CIFS users can change permissions using the Security tab of the Windows Properties dialog box.
    - **NTFS Compatible Mode**: Default mode for CIFS volumes on Nasuni Filers joined to Active Directory. This mode is required for multiple protocol support, such as NFS or FTP/SFTP protocols, as well as CIFS/SMB. NFS and FTP/SFTP protocols cannot see all NTFS permissions and do not obey all access rules in NTFS permissions. NFS and FTP/SFTP protocols obey only the POSIX access control list (ACL) component of inheritance rules. A high level of Windows compatibility is supported through the CIFS/SMB protocol, with some limitations.
    - **NTFS Exclusive Mode**: Optional mode for CIFS volumes on Nasuni Filers joined to Active Directory. Recommended for CIFS volumes that do not require mixed mode access, because multiple protocols, such as NFS or FTP/SFTP, are not supported. Produces full NTFS permissions, as supported on CIFS/SMB. Windows clients obey inheritance rules. This policy has the greatest Windows compatibility.

      Important: *You cannot switch from NTFS Exclusive Mode to NTFS Compatible Mode.*

      Important: *Volumes in NTFS Exclusive Mode do not support multiple protocols.*
    - **POSIX Mixed Mode**: Default mode for CIFS volumes on Nasuni Filers joined to LDAP. Recommended for combined CIFS and FTP/SFTP volumes, with light NFS use. Also recommended for CIFS-only volumes with Linux or Mac clients, with UNIX extensions enabled. Access control lists (ACLs) are supported entirely through POSIX ACLs. Windows clients receive mapping of POSIX ACLs to NTFS ACLs. However, the mappings are not as complete as mappings done for NTFS Compatible Mode. NFS clients cannot view the ACLs.
      The NFSv4 protocol automatically translates the underlying ACLs to NFSv4 ACLs. The common tools for managing POSIX ACLs are not supported on NFSv4. To manage ACLs using NFSv4, you must use the NFSv4 ACL tools. Not all Nasuni Filers support NFSv4. You can check whether NFSv4 is supported on the NFS Status page (Nasuni Filers) or the Exports page (NMC).
    - **Unauthenticated Access Mode**: Default mode for CIFS volumes on Nasuni Filers that are not joined to Active Directory or to LDAP. Recommended for CIFS Public-mode volumes. For CIFS clients, this mode acts as an open share. For all other protocols, this mode acts identically to POSIX Mixed Mode.

    -
5. Click **Save**.
   The FTP/SFTP protocol is enabled.

Configuring FTP Settings (optional)

You can view and configure FTP/SFTP settings for the Nasuni Filer. These advanced features of the FTP/SFTP protocol apply to all volumes on the Nasuni Filer.

To configure FTP settings, follow these steps:

1. Click **Configuration**, then select **FTP Settings**. The **General FTP Settings** page appears.

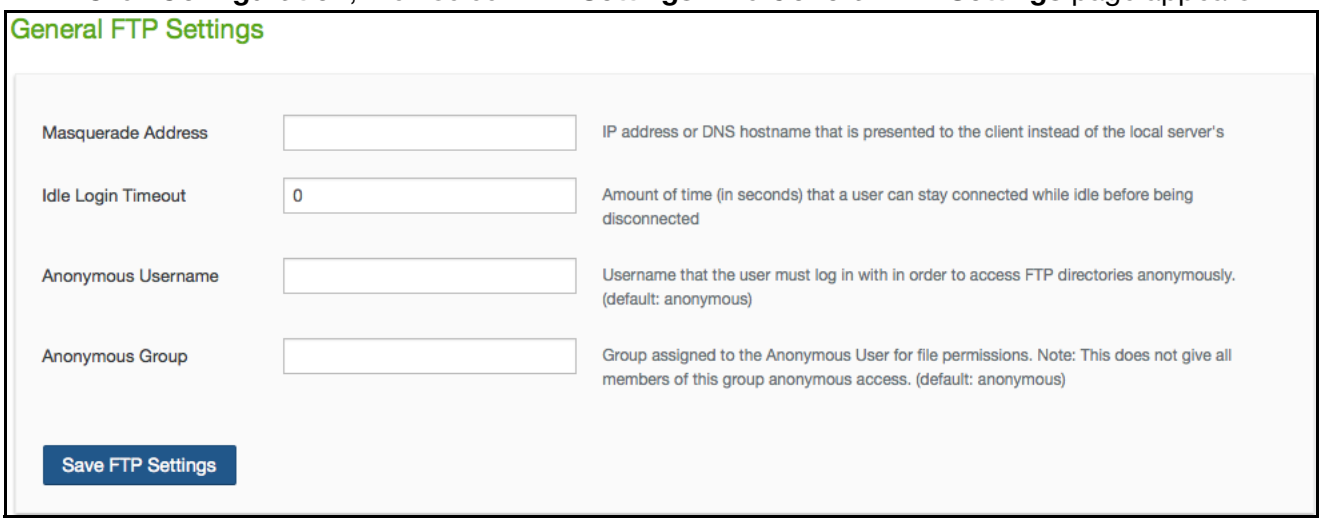

Figure 1-3: General FTP Settings page.

> ***Note:*** *If this Nasuni Filer is under Nasuni Management Console control, this page is not available on the Nasuni Filer. Instead, use the Nasuni Management Console to view information or perform actions.*

2. Optionally, in the **Masquerade Address** text box, type an IP address (not a DNS hostname) to present to the client instead of the local server's IP address or DNS hostname.
3. Optionally, in the **Idle Login Timeout** text box, type the time in seconds to wait before closing an idle connection. Zero (0) means never close an idle connection.
4. Optionally, in the **Anonymous Access Username** text box, type the username that the user must log in with in order to access any FTP/SFTP directory anonymously. Default: `anonymous`. The username is case sensitive.
5. Optionally, in the **Anonymous Access Group** text box, type the group associated with the Anonymous Access Username.
6. Click **Save FTP Settings** to save your settings.

Adding FTP Directories for a Volume

You can create, view, edit, and delete FTP/SFTP directories for volumes that have the FTP protocol enabled. This enables you to allow FTP/SFTP access to directories and files without adding new users.

To create a new FTP/SFTP directory for a volume, follow these steps:

1. On the **FTP Directories** page for a volume, click **Add New FTP Directory**. The **Add FTP Directory / Edit Settings** page appears.

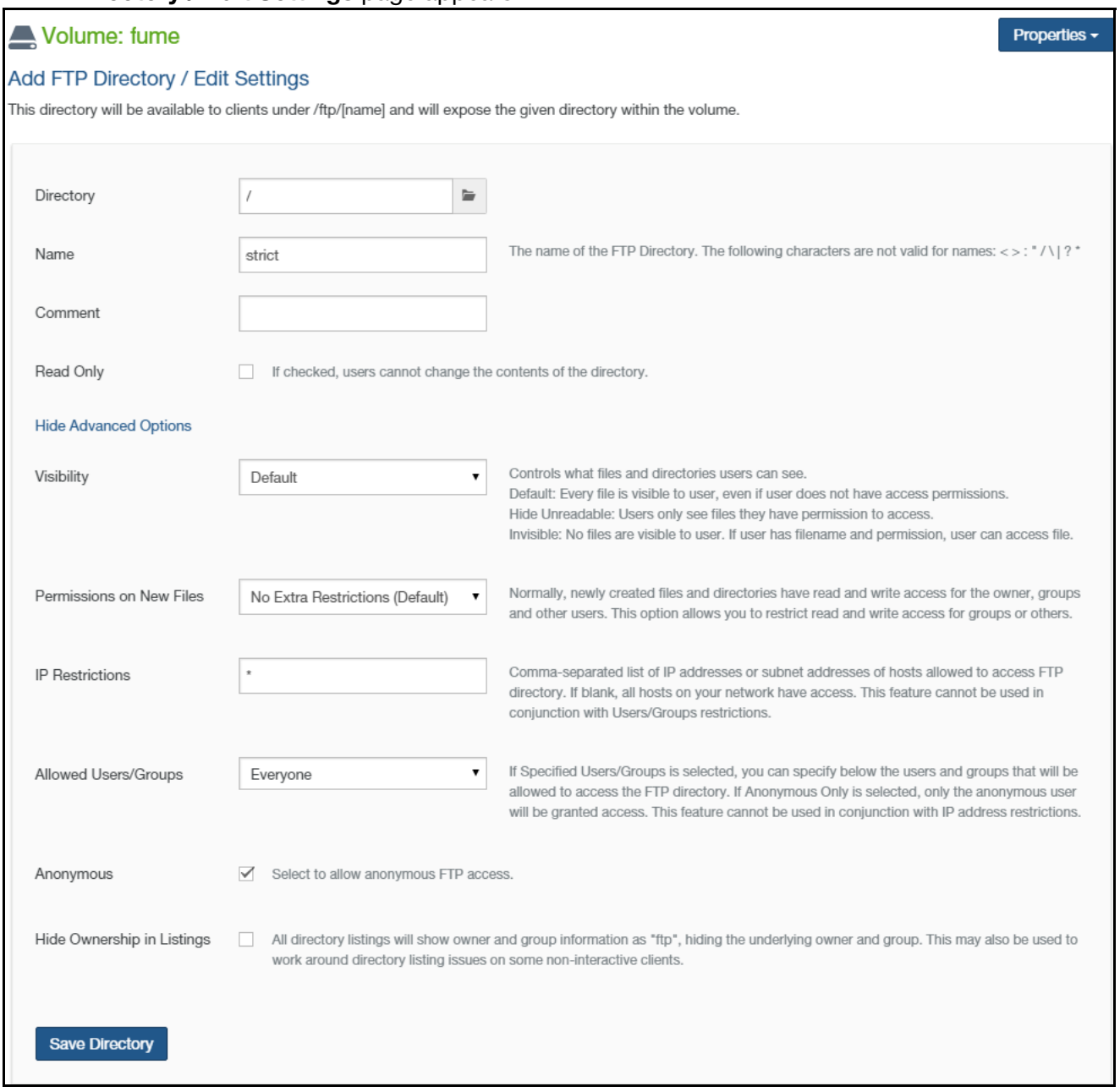

Figure 1-4: Add FTP Directory / Edit Settings page.

2. Click the **Directory** text box and navigate to the directory you want to access using FTP/SFTP.

3. In the **Name** text box, enter a name for this FTP/SFTP directory. The following characters are not valid for FTP/SFTP directory names:

   ```
   < > : " / \ | ? *
   ```

   Tip: *For Windows uses, see Naming Files, Paths, and Namespaces.*

4. Optionally, enter a descriptive comment in the **Comment** text box.
5. If you want the FTP/SFTP directory to be read-only, select the **Read Only** check box. This means that users can access the FTP/SFTP directory, but only have read-only rights and therefore cannot make changes to any of the files or directories in the FTP/SFTP directory.
6. From the **Visibility** drop-down list, select the visibility of the new FTP/SFTP directory. Your choices are:
   - **Default**: Every file is visible to the user. However, even if a file is visible to the user, the user might not be able to access the file because of permissions.
   - **Hide Unreadable**: Files that the user does not have permission to access are not visible to the user.
   - **Invisible**: No files are visible to the user. However, if a user has the filename of a file, and the appropriate permission, the user can access the file.
7. To control the permissions on new files in this FTP/SFTP directory, there are several choices, which use umask settings to represent read, write, and execute permissions for the user, the group, and others. Select one of the following choices from the **Permissions on New Files** drop-down menu:
   - **No Extra Restrictions (Default)**: The owner, the group, and all others have all permissions for all files in this FTP/SFTP directory. This is a umask setting of 000, which, for a requested permission of 777, produces 777.
   - **Read-Only Others**: The owner and the group have all permissions for all files in this FTP/SFTP directory. Others can only read all files in this FTP/SFTP directory. This is a umask setting of 002, which, for a requested permission of 777, produces 775.
   - **Read-Only Groups and Others**: The owner has all permissions for all files in this FTP/SFTP directory. The group and others can only read all files in this FTP/SFTP directory. This is a umask setting of 022, which, for a requested permission of 777, produces 755.
   - **Restrict Others**: The owner and the group have all permissions for all files in this FTP/SFTP directory. Others have no permissions for all files in this FTP/SFTP directory. This is a umask setting of 006, which, for a requested permission of 777, produces 771.
   - **Restrict Groups and Others**: The owner has all permissions for all files in this FTP/SFTP directory. The group and others have no permissions for all files in this FTP/SFTP directory. This is a umask setting of 066, which, for a requested permission of 777, produces 711.
   - **Read-Only Groups, Restrict Others**: The owner has all permissions for all files in this FTP/SFTP directory. The group can only read all files in this FTP/SFTP directory. Others have no permissions for all files in this FTP/SFTP directory. This is a umask setting of 026, which, for a requested permission of 777, produces 751.

8. To control which hosts are allowed to connect to this FTP/SFTP directory, in the **IP Restrictions** text box, enter a comma-separated list of the IP addresses or subnet addresses of the hosts that are allowed to access this FTP/SFTP directory. If you leave this field blank, all hosts on your network have access to this FTP/SFTP directory without restrictions.

   Note: *You cannot use IP Restrictions in conjunction with Allowed Users/Groups in step 9 on page 9.*

9. To control the users and groups that have access to the FTP/SFTP directory, from the **Allowed Users/Groups** drop-down list, select one of the following choices.

   - **Everyone**: Allows all users and groups to access the FTP/SFTP directory.
   - **Anonymous Only**: Allows only the anonymous user to access the FTP/SFTP directory. This selection is only available if **Anonymous** is enabled, as in step 10 on page 12.
   - **Specific Users/Groups**: Allows you to specify the users and groups that have access to this FTP/SFTP directory. The **Allowed Groups** and **Allowed Users** areas appear.

     Note: *You cannot use Allowed Users/Groups in conjunction with IP Restrictions in step 8 on page 9.*

   Tip: *A user can access the FTP/SFTP directory if the user is accessing the FTP/SFTP directory from one of the allowed hosts and is either one of the allowed users or a member of one of the allowed groups.*

   Tip: *To specify users or groups, the users or groups must have Storage Access enabled.*

   a. To add one group, follow these steps:

      i. In the **Allowed Groups** area, click **Add One**. The **Name** search box appears.

Figure 1-5: Add One Name search box.

      ii. Enter a partial or complete group name, then click **Search** . The **Select Group** dialog box appears, containing the partial or complete group name.

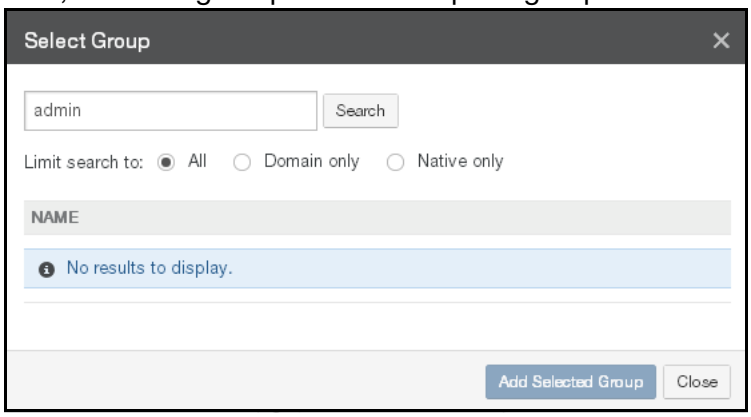

Figure 1-6: Select Group dialog box.

iii. To control the range of the search, select one of the following:

- **All**: To search through all groups.
- **Domain only**: To search though domain groups only.
- **Native only**: To search through native groups only.

iv. Click **Search**. A list of groups that match your search appears. Select the group to define access for, then click **Add Selected Group**. The selected group appears in the **Allowed Groups** area.

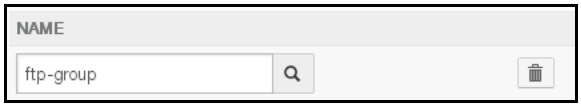

Figure 1-7: Allowed Groups area.

b. To add more than one group, follow these steps:

i. In the **Allowed Groups** area, click **Add Many**. The **Select Groups** dialog box appears.

ii. In the **Search** text box, enter a partial or complete group name.

iii. To control the range of the search, select one of the following:

- **All**: To search through all groups.
- **Domain only**: To search though domain groups only.
- **Native only**: To search through native groups only.

iv. Click **Search**. A list of groups that match your search appears.

v. Select the groups to define access for, then click **Add Selected Groups**. The selected groups appear in the **Allowed Groups** area.

c. To delete a group from the **Allowed Groups** list, click **Delete** next to the group name. The group is deleted from the list.

d. To add one user, follow these steps:

i. In the **Allowed Users** area, click **Add One**. The **Name** search box appears.

Figure 1-8: Add One Name search box.

ii. Enter a partial or complete user name, then click **Search** . The **Select User** dialog box appears, containing the partial or complete user name.

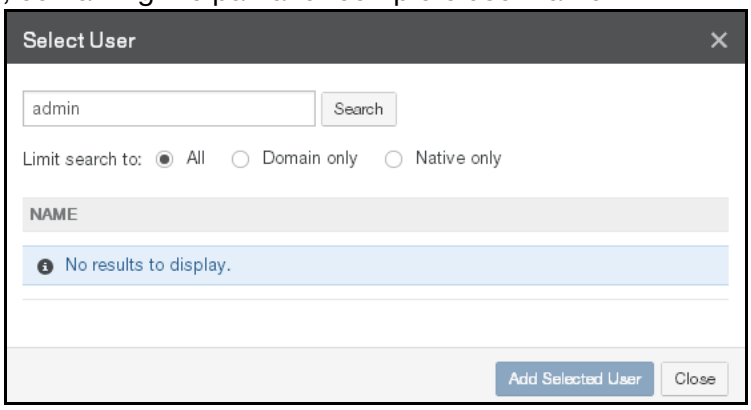

Figure 1-9: Select User dialog box.

iii. To control the range of the search, select one of the following:

- **All**: To search through all users.
- **Domain only**: To search though domain users only.
- **Native only**: To search through native users only.

iv. Click **Search**. A list of users that match your search appears. Select the user to define access for, then click **Add Selected User**. The selected user appears in the **Allowed Users** area.

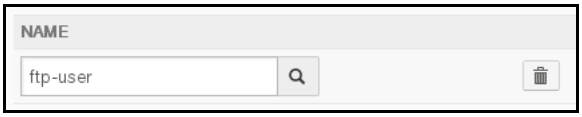

Figure 1-10: Allowed Users area.

e. To add more than one user, follow these steps:

i. In the **Allowed Users** area, click **Add Many**. The **Select Users** dialog box appears.

ii. In the **Search** text box, enter a partial or complete user name.

iii. To control the range of the search, select one of the following:

- **All**: To search through all users.
- **Domain only**: To search though domain users only.
- **Native only**: To search through native users only.

iv. Click **Search**. A list of users that match your search appears.

v. Select the users to define access for, then click **Add Selected Users**. The selected users appear in the **Allowed Users** area.

f. To delete a user from the **Allowed Users** list, click **Delete** next to the user name. The user is deleted from the list.

10. To allow anonymous FTP access, select the **Anonymous** check box.

    Tip: *If anonymous FTP access is enabled, any user can access the FTP/SFTP directory.*

11. To hide ownership details in directories, select **Hide Ownership in Listings**. This can enhance security.

12. To accept your selections, click **Save Directory**.

    The FTP/SFTP directory is created and appears in the list of FTP/SFTP directories. The FTP/SFTP directory is available to users.

    Alternatively, to exit this screen without creating an FTP/SFTP directory, click the **Reset** button.

Viewing FTP directories

To view existing FTP/SFTP directories for a volume, follow these steps:

1. Click **Volumes**, then select a volume that has the FTP protocol enabled from the list.

   Note: *If this Nasuni Filer is under Nasuni Management Console control, this page is not available on the Nasuni Filer. Instead, use the Nasuni Management Console to view information or perform actions.*

2. The **Volume** properties page appears. Select **FTP Directories** from the **Properties** drop-down list. The **FTP Directories** page appears.

Figure 1-11: FTP Directories page.

For each FTP/SFTP directory, the following information is displayed:

- **Name**: The name of the FTP/SFTP directory.
- **Path**: The path to the FTP/SFTP directory.

Editing FTP directories

To edit the selected FTP/SFTP directory, click **Edit Directory**, then follow the steps of “Adding FTP Directories for a Volume” on page 7.

Deleting FTP directories

To delete the selected FTP/SFTP directory access point (not the data), follow these steps:

1. Click **Volumes**, then select a volume that has the FTP protocol enabled from the list.

   Note: *If this Nasuni Filer is under Nasuni Management Console control, this page is not available on the Nasuni Filer. Instead, use the Nasuni Management Console to view information or perform actions.*

2. The **Volume** properties page appears. Select **FTP Directories** from the **Properties** drop-down list. The **FTP Directories** page appears.

Figure 1-12: FTP Directories page.

3. For the FTP/SFTP directory you want to delete, click **Delete Directory**.

   The **Confirm Directory Delete** dialog box appears.

4. Click **Confirm Delete**. The FTP/SFTP directory is removed.

Adding a Permission Group with Storage Access (optional)

You can add up to 150 permission groups to which you can assign users. For each group, you can specify exactly which actions the users in that group have permission to perform. You can associate Active Directory and LDAP domain groups with a permission group.

To add a permission group, follow these steps:

1. Click **Configuration**, then select **Users/Groups** from the drop-down list. The **Filer Users and Groups Overview** page appears.

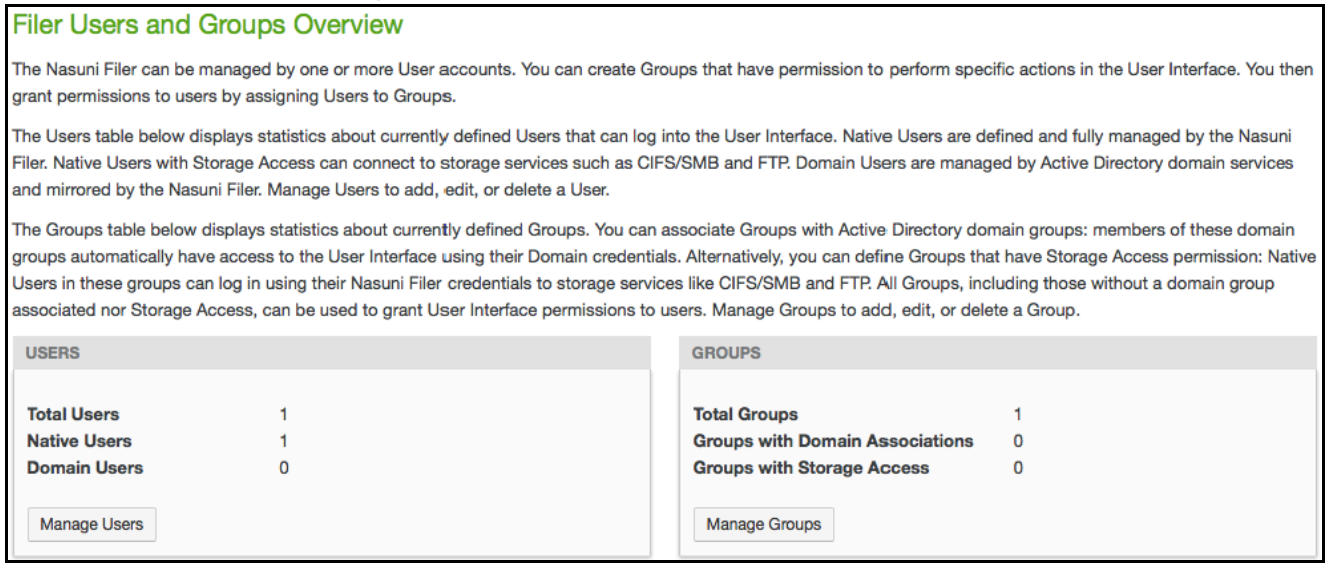

Figure 1-13: Filer Users and Groups Overview page.

> ***Note:*** *If this Nasuni Filer is under Nasuni Management Console control, this page is not available on the Nasuni Filer. Instead, use the Nasuni Management Console to view information or perform actions.*

2. On the **Filer Users and Groups Overview** page, click **Manage Groups**. The **Filer Groups** page appears.

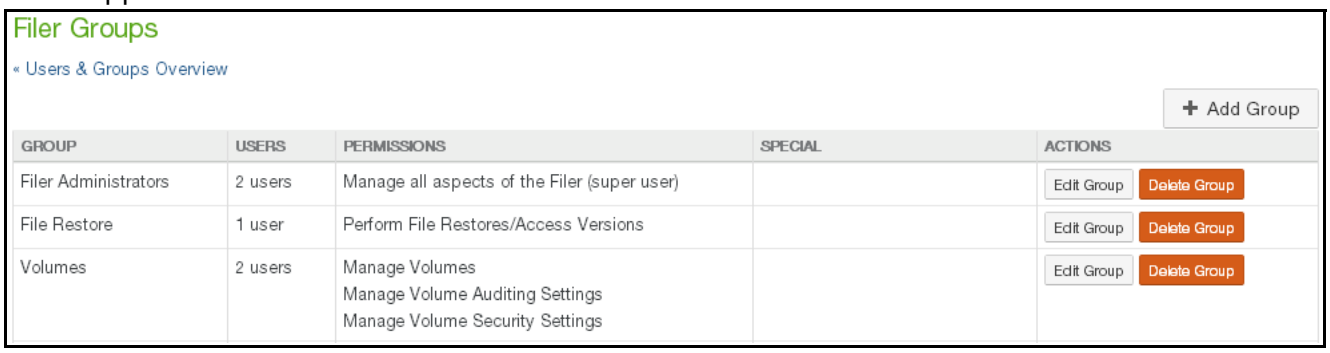

Figure 1-14: Filer Groups page.

3. Click **Add Group**. If there are already 150 groups, you must delete an existing group before you can add a new group. The **Add New Group** dialog box appears.

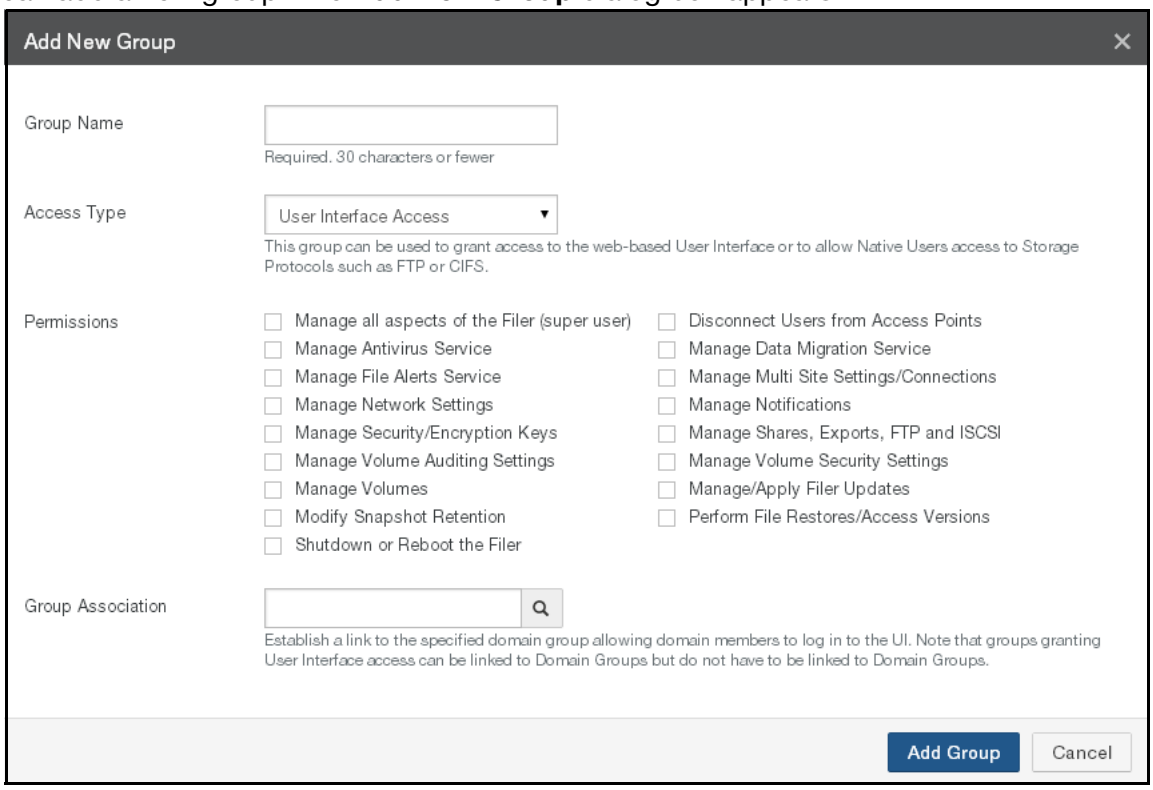

Figure 1-15: Add New Group dialog box.

4. In the **Group Name** text box, enter the name for this group. The Group Name can have up to 30 characters, including letters, digits, and symbols.
5. From the **Access Type** drop-down list, select **Storage Access**.

   Note: *Storage Access does not grant any access to the Nasuni Filer user interface.*

   Note: *If you select Storage Access, you cannot enter a Group Association.*

6. To accept your selections, click **Add Group**.
   The permission group is added with the selected permissions.

Adding Users (optional)

You can add up to 150 users. For each user, you can specify which permission groups that user belongs to. If this Nasuni Filer is joined to Active Directory or LDAP, you can also add domain users.

> ***Note:*** *Adding a domain group allows all Active Directory or LDAP users in that group to access the user interface. You do not need to explicitly add those users.*

1. Click **Configuration**, then select **Users/Groups** from the drop-down list. The **Filer Users and Groups Overview** page appears.

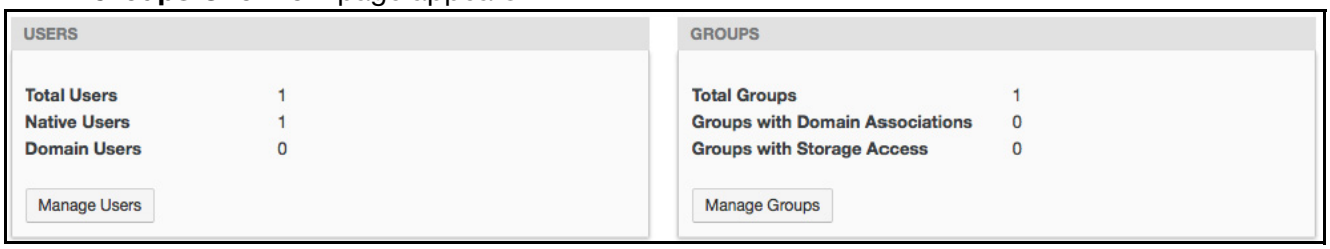

Figure 1-16: Filer Users and Groups Overview page.

> ***Note:*** *If this Nasuni Filer is under Nasuni Management Console control, this page is not available on the Nasuni Filer. Instead, use the Nasuni Management Console to view information or perform actions.*

2. On the **Filer Users and Groups Overview** page, click **Manage Users**. The **Filer Users** page appears.

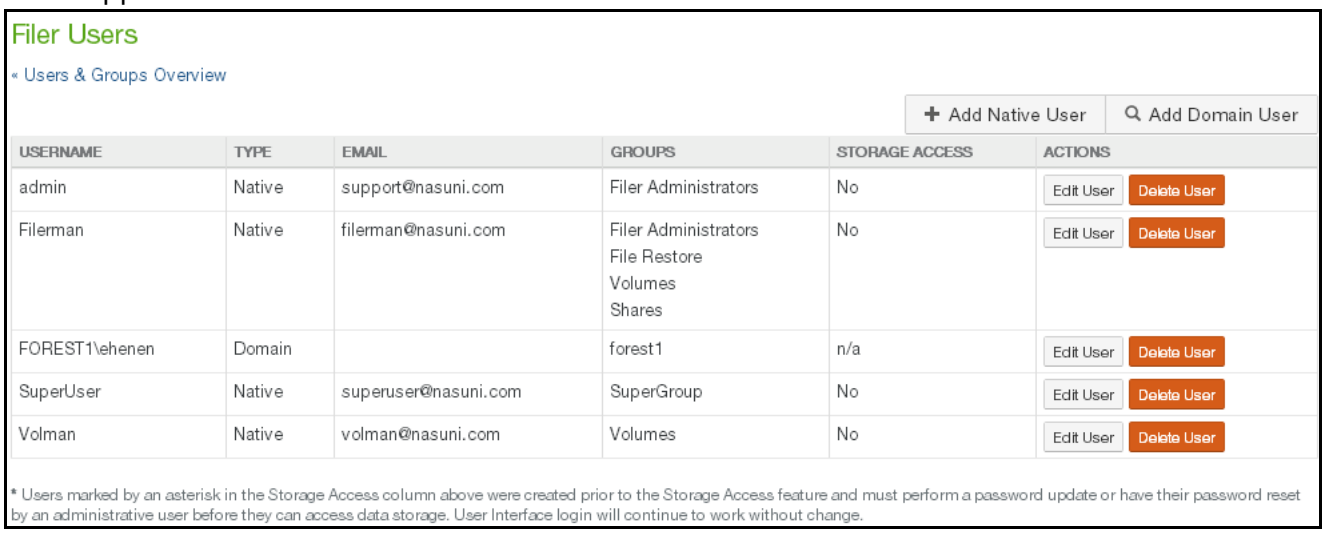

Figure 1-17: Filer Users page.

3. Click **Add Native User**. If there are already 150 users, you must delete an existing user before you can add a new user. The **Add Native User** dialog box appears.

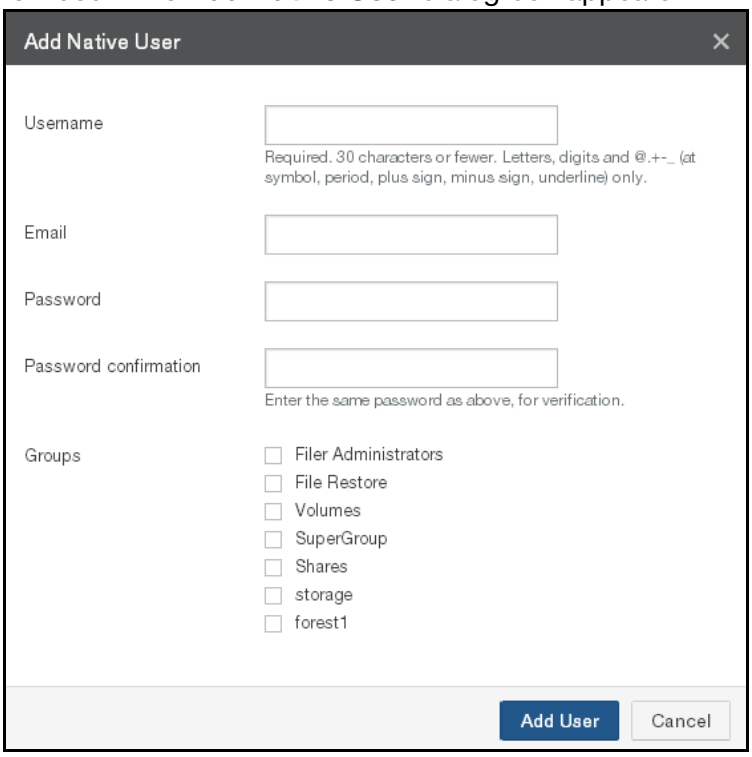

Figure 1-18: Add Native User dialog box.

a. In the **Username** text box, enter the name for this user. The Username can have up to 30 characters, including letters, digits, and the following symbols:

@ . + - _ (at symbol, period, plus sign, minus sign, underline)

b. In the **Email** text box, enter the email address for this user.

c. In the **Password** text box, enter the password for this user. Enter the same password in the **Password confirmation** text box. An indicator of password strength appears. Although password strength is not enforced, you should use strong passwords.

d. In the **Groups** list, for each of the permission groups, select or clear the check box for granting membership to the permission group.

e. To accept your selections, click **Add User**.

The user is added with membership in the selected groups.

4. If the Nasuni Filer is joined to Active Directory or LDAP Directory Services, to add a domain user, click **Add Domain User**. If there are already 150 users, you must delete an existing user before you can add a new user. The **Add Domain User** dialog box appears.

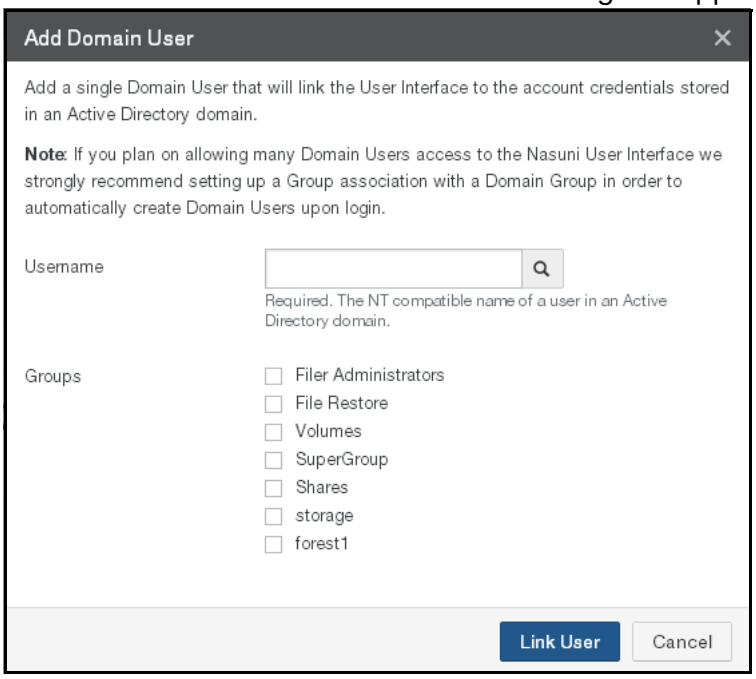

Figure 1-19: Add Domain User dialog box.

Note: *Adding a domain group allows all Active Directory or LDAP users in that group to access the user interface. You do not need to explicitly add those users. You only need to add Active Directory or LDAP users individually if you do not want to grant access to the entire group.*

a. In the **Username** text box, enter the name of a user in an Active Directory or LDAP domain. For Active Directory domains, the Username must be NT-compatible. The Username can have up to 30 characters, including letters, digits, and the following symbols:
@ . + - _ (at symbol, period, plus sign, minus sign, underline)

b. In the **Groups** list, for each of the permission groups, select or clear the check box for granting membership to the permission group.

c. To accept your selections, click **Link User**.

The user is added with membership in the selected groups.

Accessing Data using the FTP/SFTP Protocol

If the FTP/SFTP protocol has been enabled for a volume, and FTP/SFTP directories have been added to a volume, you can use FTP/SFTP commands and various applications to access that data.

To access data using FTP commands, use commands such as these:

1. Enter the following FTP command:

   ```
   ftp <filer DNS | filer IP>
   ```

   where `<filer DNS | filer IP>` is the DNS or IP address or hostname of the Nasuni Filer.

2. When prompted, enter a valid username and password for that Nasuni Filer.

   Note: *This user must belong to a permission group that has Storage Access enabled. See "Adding a Permission Group with Storage Access (optional)" on page 14.*

3. Navigate to the directory using a command of the form:

   ```
   cd /<ftp_directory>/<folder_name>
   ```

   where `<ftp_directory>` is the name of the FTP directory and `<folder_name>` is the name of the folder that the FTP access is defined for.

Alternatively, follow these steps:

1. Enter the following on the address bar of your Web browser:

   ```
   ftp://<user_name>@<filer>/<ftp_directory>/<folder_name>
   ```

   where
   `<user_name>` is the username of the user. This user must belong to a permission group that has Storage Access enabled. See *"Adding a Permission Group with Storage Access (optional)" on page 14*.
   `<filer>` is the IP address or hostname of the Nasuni Filer.
   `<ftp_directory>` is the name of the FTP directory.
   `<folder_name>` is the name of the folder that FTP access is defined for.

   Note: *If you are not logging in anonymously, you still must specify a username in the URL, such as `ftp://username@ftp.server.hostname`. This is true even if Anonymous access is not enabled.*

2. When prompted, enter a valid username and password for that Nasuni Filer.

   Note: *This user must belong to a permission group that has Storage Access enabled. See "Adding a Permission Group with Storage Access (optional)" on page 14.*

3. A display of the FTP/SFTP directory appears. You can then navigate this directory to access folders and files.

FTP Status

You can view FTP/SFTP directories for volumes that have the FTP/SFTP protocol enabled. You can also view the status of FTP/SFTP clients.

Viewing FTP directories and FTP clients

To view FTP/SFTP directories, follow these steps:

1. Click **Status,** then select **FTP Status** from the list. The **FTP Directories** page displays a list of FTP/SFTP directories for volumes that have the FTP protocol enabled. A list of any FTP/SFTP clients also appears.

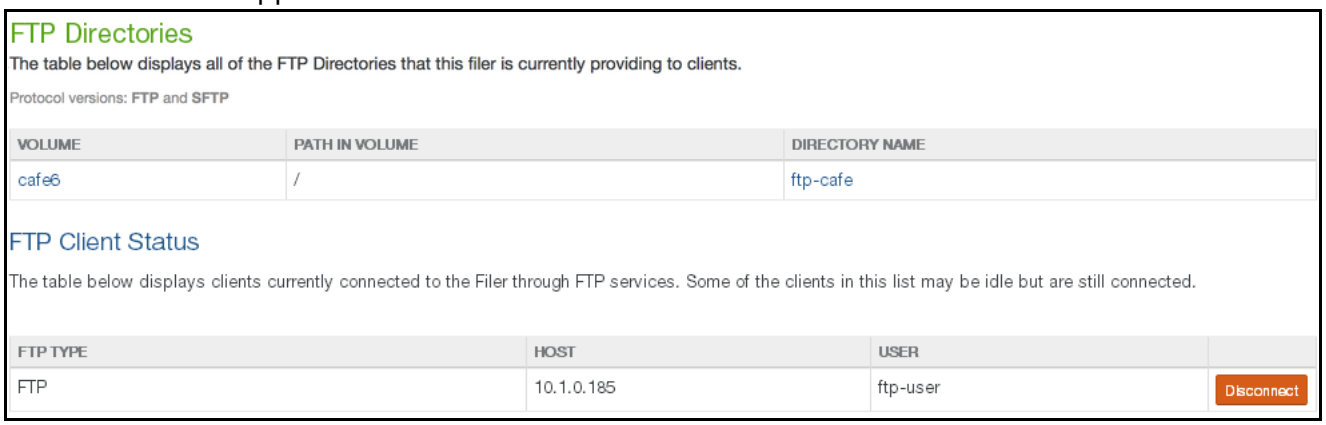

Figure 1-20: FTP Directories page.

The following information is displayed:

- **Protocol version**: The supported versions of the FTP/SFTP protocol.
- **FTP Directories**: A table displays, for each FTP/SFTP directory, the following:
  - **Volume**: The volume for the FTP/SFTP directory. Clicking this link opens either the **FTP Directories** page for this volume (see "Viewing FTP directories" on page 12), if this Nasuni Filer is not under the control of the Nasuni Management Console, or the **Home** page, if this Nasuni Filer is under the control of the Nasuni Management Console.
  - **Path**: The path to the FTP/SFTP directory.
  - **Directory Name**: The name of the FTP/SFTP directory. Clicking this link opens either the **Add FTP Directory / Edit Settings** page for this volume (see "Editing FTP directories" on page 12), if this Nasuni Filer is not under the control of the Nasuni Management Console, or the **Home** page, if this Nasuni Filer is under the control of the Nasuni Management Console.
- **FTP Client Status**: A table displays, for each FTP/SFTP client, the following:
  - **FTP Type**: The type of FTP/SFTP client: FTP or SFTP.
  - **Host**: The host of the FTP/SFTP client.
  - **User**: The name of the user using the FTP/SFTP client. This user must belong to a permission group that has Storage Access enabled. See "Adding a Permission Group with Storage Access (optional)" on page 14.

Disconnecting FTP clients

To disconnect an FTP/SFTP client, follow these steps:

1. Click **Status,** then select **FTP Status** from the list. The **FTP Directories** page displays a list of FTP/SFTP clients.

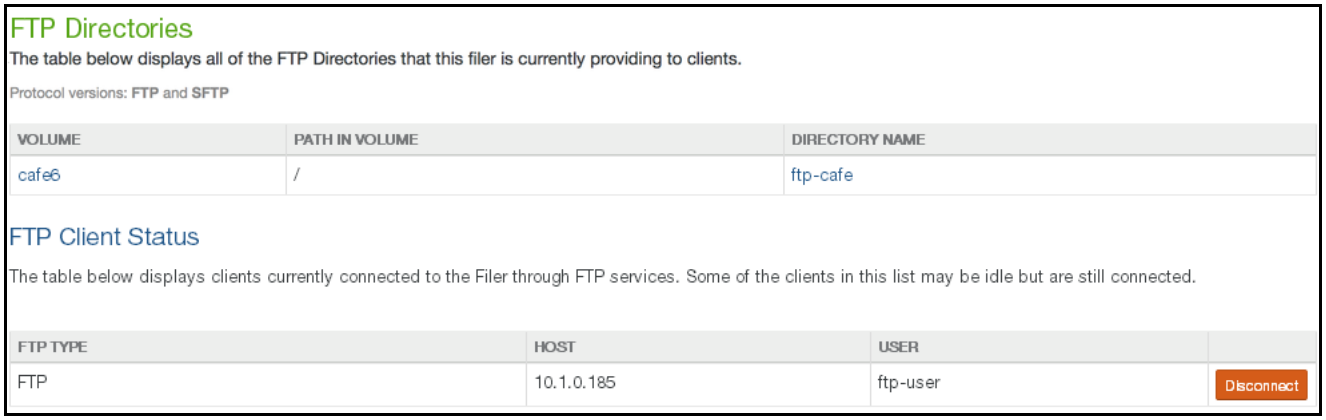

Figure 1-21: FTP Directories page.

2. Select a client from the list of clients, then click **Disconnect**. The **Disconnect Client** dialog box appears.
3. Click **Disconnect Client**.
   The client is disconnected. The message “Client was disconnected from the Filer” appears. Click **x** to close the message box.

Nasuni Corporation | One Marina Park Drive, Boston, MA 02210 | 1.857.444.8500 | www.nasuni.com