Micro Focus Storage Manager 5.3 for eDirectory

Administration Guide

June 1, 2020

Legal Notices

Condrey Corporation makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Condrey Corporation reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Condrey Corporation makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Condrey Corporation reserves the right to make changes to any and all parts of the software at any time, without obligation to notify any person or entity of such revisions or changes. See the Software EULA for full license and warranty information with regard to the Software.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export, or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. Condrey Corporation assumes no responsibility for your failure to obtain any necessary export approvals.

Condrey Corporation
122 North Laurens St.
Greenville, SC 29601
U.S.A.
http://condrey.co

For information about Micro Focus legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see https://www.microfocus.com/about/legal.

Third Party Systems

The software is designed to run in an environment containing third party elements meeting certain prerequisites. These may include operating systems, directory services, databases, and other components or technologies. See the accompanying prerequisites list for details.

The software may require a minimum version of these elements in order to function. Further, these elements may require appropriate configuration and resources such as computing, memory, storage, or bandwidth in order for the software to be able to perform in a way that meets the customer requirements. The download, installation, performance, upgrade, backup, troubleshooting, and management of these elements is the responsibility of the customer using the third party vendor’s documentation and guidance.

Third party systems emulating any these elements must fully adhere to and support the appropriate APIs, standards, and protocols in order for the software to function. Support of the software in conjunction with such emulating third party elements is determined on a case-by-case basis and may change at any time.

Contents

About This Guide

This administration guide is written to provide network administrators the conceptual and procedural information for managing user and collaborative storage by using Micro Focus Storage Manager for eDirectory.

Audience

This guide is intended for network administrators who manage user and collaborative network storage resources.

Feedback

We want to hear your comments and suggestions about this guide and the other documentation included with this product. Please use the User Comment feature at the bottom of each page of the online documentation, or go to www.novell.com/documentation/feedback.html and enter your comments there.

Documentation Updates

For the most recent version of the *Micro Focus Storage Manager 5.3 for eDirectory Administration Guide*, visit the Micro Focus Storage Manager Web site (http://www.novell.com/documentation/storagemanager5/index.html).

Additional Documentation

For additional Micro Focus Storage Manager documentation, see the following guide at the Micro Focus Storage Manager Documentation Web site (http://www.novell.com/documentation/storagemanager5/index.html):

- *Micro Focus Storage Manager 5.3 for eDirectory Installation Guide*

1 What's New

Micro Focus Storage Manager 5.3 for eDirectory provides new features and product enhancements. A summary of some of the more notable new features and enhancements follows.

1.1 New in Version 5.3

Support for Open Enterprise Server 2018 SP2

Storage Manager 5.3 for eDirectory has been updated and thoroughly tested to support the storage capabilities and features of Open Enterprise Server 2018 SP2.

Updates to Engine, Agent, and Event Monitor

Updates include consolidation of native code, product updates for the current build system, and TLS updates for security.

Updates to the Admin Client Interface

Some minor interface changes were made to the Admin Client with the objectives of making the interface more user friendly and more consistent with current product sets. Updates were also made to third-party libraries. In cleaning up the code base, some legacy code was removed.

1.2 New in Version 5.0

Re-branded Administrative Interface

The Storage Manager administrative interface has been re-branded. Based on this re-branding, some filenames and paths have been updated.

2 Overview

Micro Focus Storage Manager introduces management and structure to an unmanaged and unstructured network storage system. In the process, it automates the full life cycle management of user and group storage. Leveraging directory services (commonly referred to as “the directory”), Storage Manager automates a comprehensive set of storage management tasks based on events, identity, and policies.

The Directory

NetIQ eDirectory stores the identity information about the users and groups that Micro Focus Storage Manager manages. When Storage Manager is installed, it adds or modifies user and group attributes so that they can be managed through Storage Manager.

Events

When a user or group is created, moved, renamed, or deleted, it is known as a directory “event.”

Policies

Policies within Storage Manager indicate what storage-specific actions to enact when an event in eDirectory takes place. These actions include creating user storage when a new user is added to eDirectory, moving storage when a user is moved from one organizational unit or group to another, and archiving or deleting storage when a user is removed.

Micro Focus Storage Manager for eDirectory lets you create the following types of policies:

User Home Folder: Manages home folders for users who access their storage from an assigned user workstation.

Container: Manages the users located in an organizational unit.

Group: Manages the users that are members of a group.

Auxiliary: Manages additional storage that you can create automatically in association with a User Home Folder policy.

Engine

The Engine performs actions based on events in eDirectory and the defined Storage Manager policies. These include provisioning, moving, grooming, deleting, renaming, and vaulting in the file system. There is only a single Engine per directory tree.

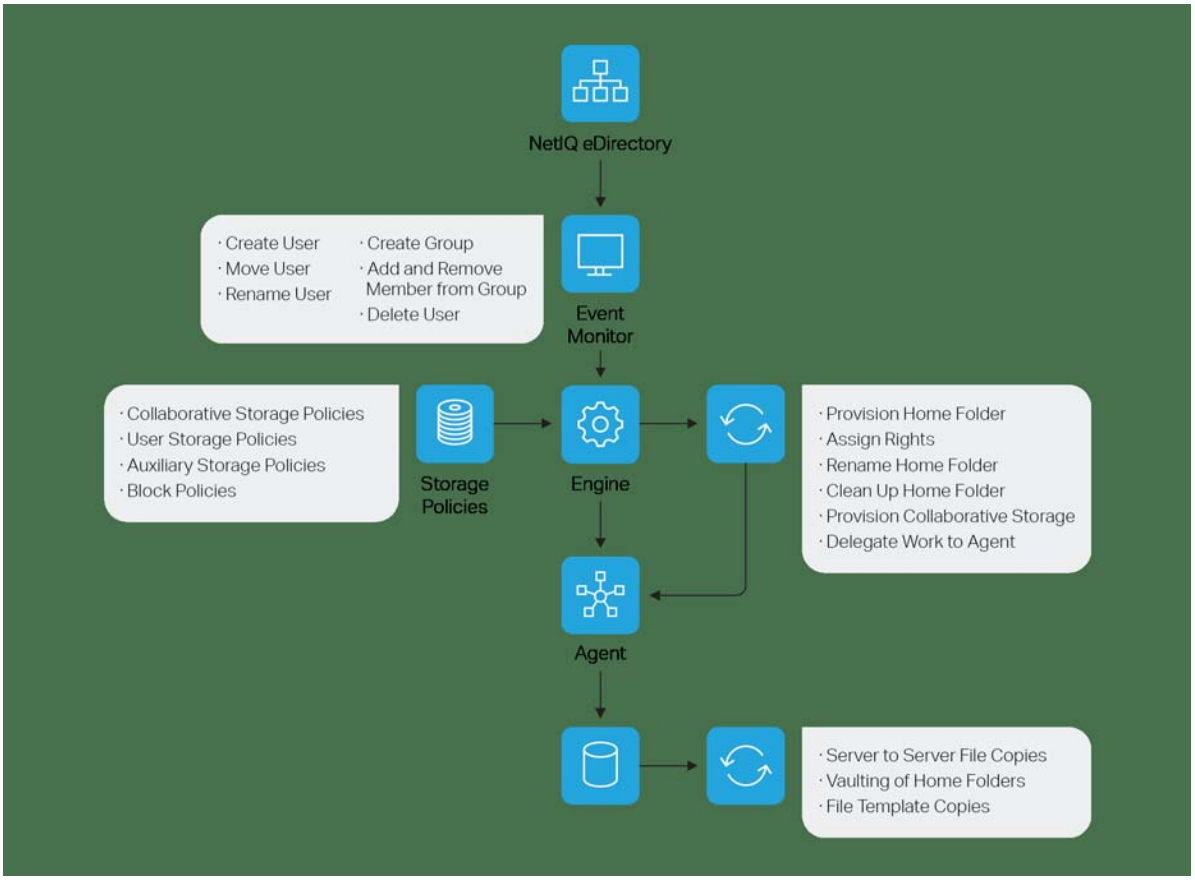
Event Monitor

The Event Monitor monitors changes to eDirectory based on create, move, rename, and delete events. Event monitors should be configured to monitor at least one server per eDirectory partition ring that you care about. That is, servers that hold a replica for each eDirectory partition that contains objects that you wish to receive event data about and for which Storage Manager will consequently manage storage.

NOTE: As a best practice, install two Event Monitors per replica ring.

Agent

Agents perform copying, moving, grooming, deleting, and vaulting through directives from the Engine. For optimum performance, Agents should be installed on all servers with storage managed by Micro Focus Storage Manager.



3 Using the Admin Client

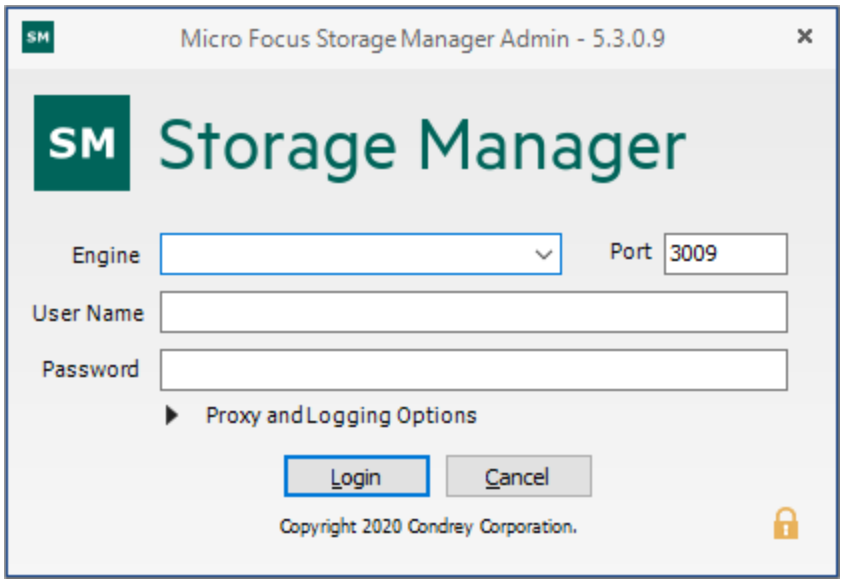
The Admin Client is the administrative interface for Micro Focus Storage Manager for eDirectory. All management tasks run from this easy-to use Windows application. The Admin Client is built from the Microsoft .NET Framework and is run from a Windows workstation or server.

Procedures for installing the Admin Client are included in "Installing and Configuring the Admin Client " of the *Micro Focus Storage Manager 5.3 for eDirectory Installation Guide*. If you have not yet installed the Admin Client, go to that guide to install it before proceeding with this section.

3.1 Launching the Admin Client

1 Double-click the Storage Manager 5.3 Admin icon from the Windows desktop.

An authentication dialog box appears.



2 In the **Engine** field, specify the DNS name or IP address where the Engine service is installed.

3 In the **Port** field, specify the secure port number.

The default setting is 3009.

4 Specify the username.

You must specify the username in fully distinguished username format.

5 Specify the password.

The user must be a member of the SMAdmins group to be able to log in.

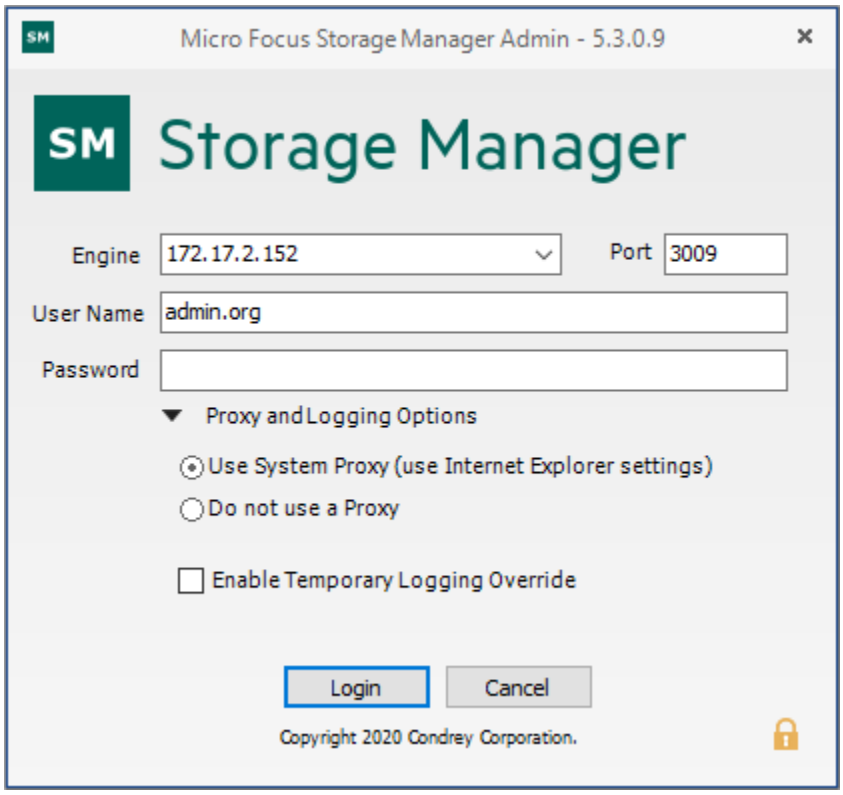
6 Click **Login**.

3.1.1 Overriding Proxy Settings at Login

As a .NET application, the Admin Client is managed by the proxy configurations and exceptions of Microsoft Internet Explorer. If you do not have an exception in your proxy settings to allow for the Admin Client, the Admin Client application might not launch.

Try to launch the Admin Client using the default setting first. If you are unable to log in, use the following procedures:

1 Repeat Step 1 on page 13 through Step 5, then click the **Proxy and Logging Options** button to expand the authentication dialog box.



2 Select **Do not use a Proxy**.

3 Click **Login**.

3.1.2 Enabling Temporary Logging Override

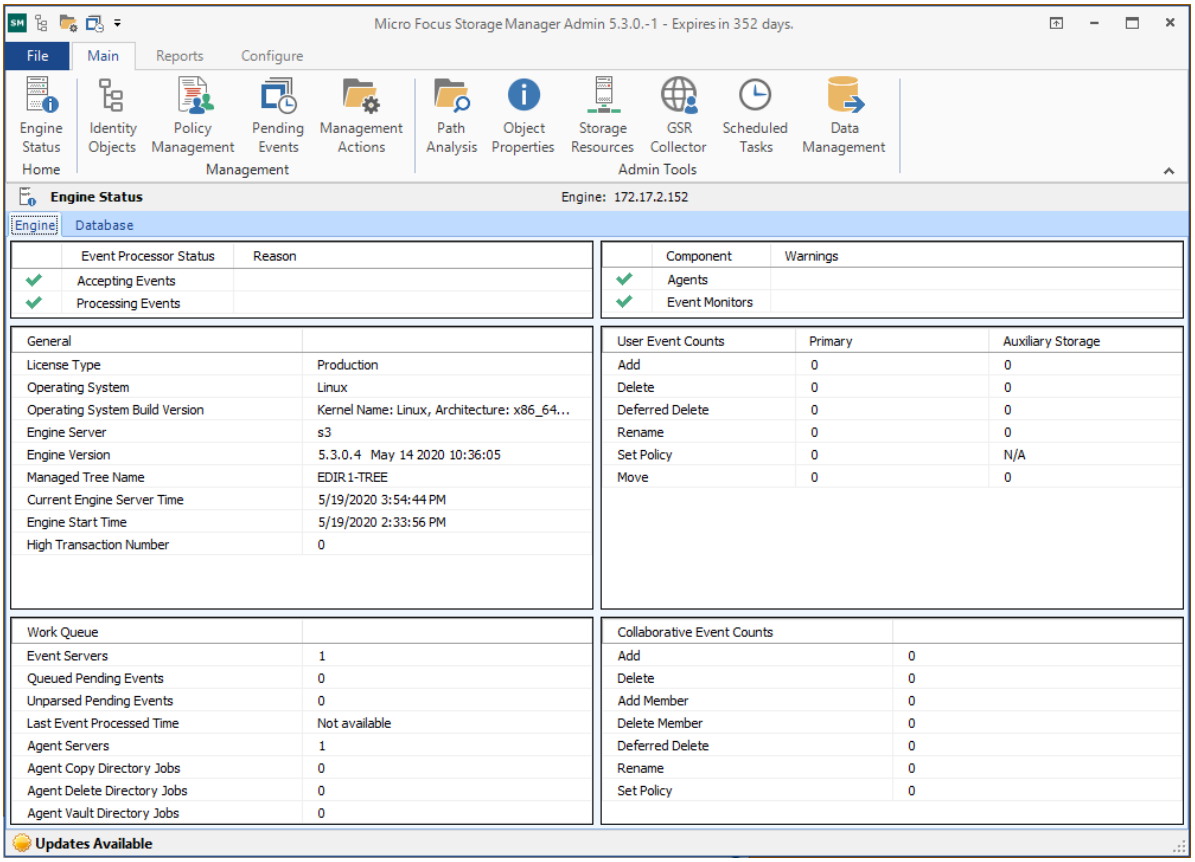
Selecting **Enable Temporary Logging Override** indicates that you want Storage Manager to override any logging configuration settings you have set for the Engine and the Agent in the Admin Client, and to create log files during this session. The data contained in the log files might be useful for troubleshooting.

The **Enable Temporary Logging Override** option overrides the currently set logging option for the Admin Client, and temporarily enables debug logging. The log can be found in the `%AppData%\Roaming\Micro Focus\Storage Manager\Admin` folder.

3.2 Using the Admin Client Interface

The Admin Client interface has three tabs: **Main**, **Reports**, and **Configure**. Clicking each tab displays an associated toolbar directly below the tabs. The toolbar is divided into sections based on the actions that are available. Clicking a tool displays data or an interface for performing a management task.

The default display is the Engine Status page, which is discussed in detail in the Reference chapter of this guide.



All other Storage Manager tools are covered in the other sections of this guide.

4 Managing Existing User Storage

Because Micro Focus Storage Manager for eDirectory is deployed into an existing Micro Focus Open Enterprise Server network with users, groups, and containers already established in eDirectory, your principle focus should be to start managing the storage that is assigned to these users. This process involves several tasks:

- Running reports to determine the status of your user storage
- Creating policies that standardize the storage allocation, quota, rights, and more
- Managing the users through Manage Operations
- Testing these policies to verify that they are working as desired

By completing this section, you not only put your existing users' storage into a managed state and set it up for ongoing management through Storage Manager for eDirectory, but you also learn the basic procedures for reporting and for setting user policies.

After completing the procedures in this section, refer to the remainder of the *Micro Focus Storage Manager 5.3 for eDirectory Administration Guide* for more detailed content on these tasks as well as many others.

4.1 Running the GSR Collector

The Global Statistics Reporting (GSR) Collector collects data for general statistics, presents historical data, reports on anomalies such as potential orphaned home folders, and catalogs managed storage movement.

As the first step in managing your existing user storage through Storage Manager, you should run the GSR Collector. Depending on the size of your network, running the GSR Collector might be resource intensive and can take some time to complete. After you run the GSR Collector the first time, you should schedule it to run at a regularly scheduled time, preferably after regular business hours.

1. Launch the Admin Client.
2. In the **Main** tab options, click **GSR Collector**.
3. Click **Run Collector**.

4.2 Viewing Anomaly Reports

The GSR Collector can generate anomaly reports to identify issues that might need to be addressed before you create storage policies. The anomaly report, which is generated through data collected by the GSR Collector, lists potential problems according to seven different categories:

Tab Name	Explanation
Orphan Candidates	Lists home directories that are not currently assigned to a User object in eDirectory.
Name Mismatch	Lists cases where a username and the associated home directory name do not match. This is frequently the case when a User object is renamed, but the corresponding home directory is not.
Path Overlap	List home directories that are parent paths of other user home directories. For example, a user's home directory attribute in eDirectory is set to VOL1:\HOME\USERS instead of VOL1:\HOME\USERS\JBANKS. This is a potential conflict because if you move an object that resides in the first path, it moves all users below the user.
Duplicate Storage Pointer	Lists users that have identical home directory paths.
Missing Primary Folders	Lists users who do not have assigned home directories.
Other Missing Folders	Lists users that have auxiliary storage assigned, but the storage is not yet created.
Objects Not Managed	Lists objects in eDirectory whose managed path is populated with a value but are not managed through Storage Manager.

1. In the Admin Client, click the **Reports** tab.
2. Click **Anomaly Reports**.
3. Click the tab for the category you want to view.

   At this point, because none of your existing users are being managed through Storage Manager, each user in eDirectory should be listed when you click the **Objects Not Managed** tab. Additionally, you might notice other potential problems by viewing data categorized through the other tabs.

4.3 Running Consistency Check Reports on Existing Storage

When Storage Manager for eDirectory is installed, you need to analyze and correct any issues that might exist in the current user storage environment. Issues might include missing storage quotas, inconsistent home folder attributes, inconsistent home folder rights, missing home folders, and inconsistent file paths. Storage analysis begins by running consistency check reports on existing user storage prior to creating and implementing storage policies.

In addition to reporting on storage issues, consistency check reports let you review current quota assignments and can help you in designing and planning storage policies.

1. In the Admin Client, click the **Main** tab.
2. Click **Identity Objects**.
3. In the left pane, browse through the directory tree so that an organizational unit with the users for whom you want to generate the consistency check report is displayed in the right pane.
4. In the right pane, right-click the container and select **User Actions > Consistency Check**.
5. Click **Run** and view the results in the bottom panel.
6. Click **Expand** to expand the view.

   Because none of the users are currently managed through Storage Manager for eDirectory, each user has a Management status of Not Managed. Additionally, there are no established storage quotas and there might be inconsistent directory attributes, rights, flags, and file paths, along with various warnings or errors that you can mouse over to view the specifics.

   To export a consistency check report for printing, see Section 9.2.1, “Consistency Check Reports,” on page 103.

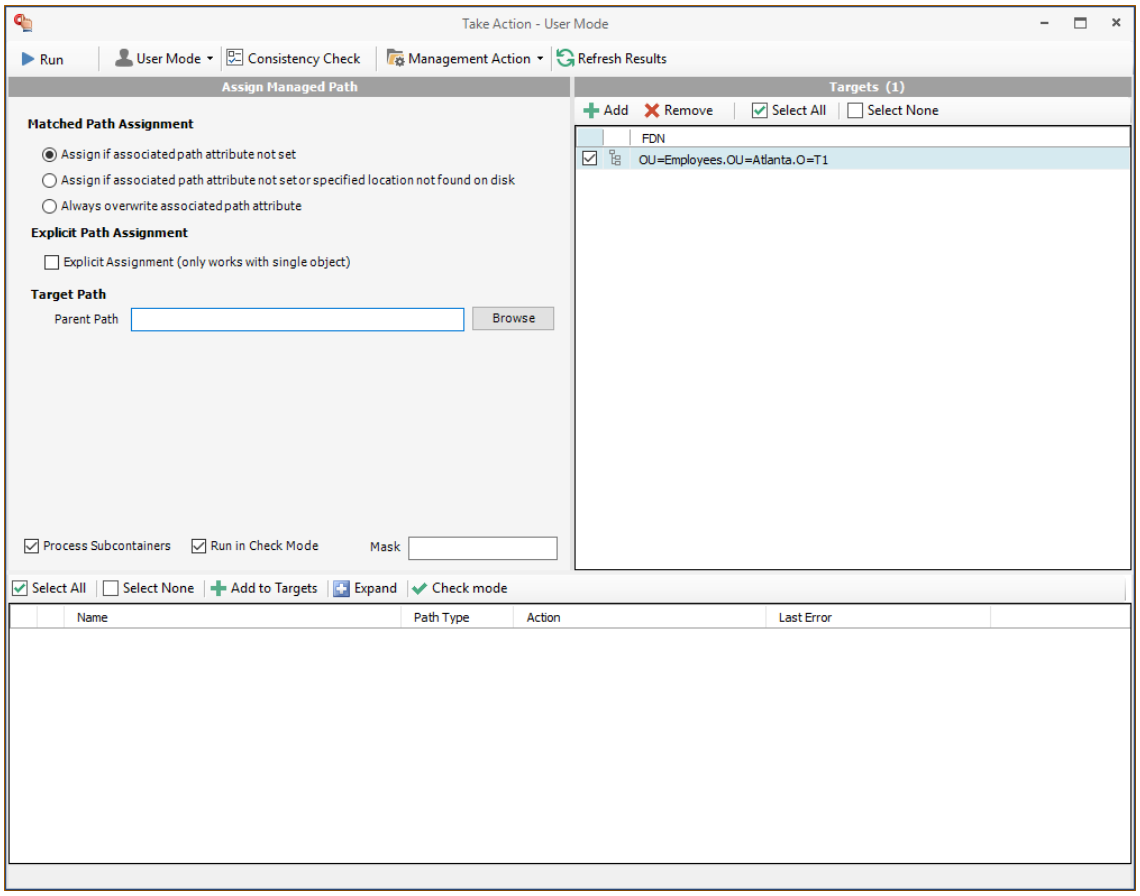
4.4 Assigning Missing Home Folder Attributes

The consistency check report’s **DS Path** column indicates the path (also referred to as “attributes”) of the user’s assigned home folder. If no path is indicated, it is because the home folder attribute is not set in eDirectory.

Storage Manager for eDirectory allows you to populate any missing home folder attributes or correct attributes that are not configured correctly. You do this by selecting a path and looking for a match on each user’s ID. You also have the option to overwrite an existing attribute based on a match found.

If no home folder exists for the user, Storage Manager for eDirectory can create one automatically when the target path for the home folder is indicated in the policy. For more information, see Section 4.5, “Standardizing User Home Folder Attributes,” on page 21.

1. In the Admin Client, click the **Main** tab.
2. Click **Identity Objects**.
3. In the left pane, browse through the tree so that an organizational unit with users that need home folder attributes appears in the right pane.
4. In the right pane, select the desired container.
5. Click **User Actions > Assign Managed Path**.



6 In the Matched Path Assignment portion of the window, make sure the **Assign if Home Directory attribute not set** option is selected.

7 Click **Browse**, use the Path Browser dialog box to browse to the path where your user home folders in the selected organizational unit reside, then click **OK**.

   The selected path appears in the **Parent Path** field.

8 Verify that the **Run in Check Mode** check box is selected.

   Check mode allows you to view the results of the action, without actually making changes.

9 Click **Run**.

10 Click **Expand** to expand the view.

   Storage Manager for eDirectory summarizes any problems it can resolve in the **Action** column.

11 Click **Collapse**.

12 If you approve of the actions Storage Manager for eDirectory took in Check mode, deselect **Run in Check Mode** and click **Run**.

13 Run a new consistency check report by selecting the organizational unit you selected in Step 3 on page 19, clicking **Consistency Check**, then clicking **Run**.

14 Observe that all users now have home directory attributes listed in the **DS Path** column.

4.5 Standardizing User Home Folder Attributes

As a best practice, you should have all of your user home folder attributes set to a path that ends with the user's home folder name, rather than the parent path. For example, instead of user EBROWN having a home folder attribute of VOL2:\USERS, it should be set to VOL2:\USERS\EBROWN.

Storage Manager for eDirectory lets you easily standardize home folder attributes by overwriting attributes linked to the parent path.

1. In the Admin Client, click the **Main** tab.
2. Click **Identity Objects**.
3. In the left pane, browse through the tree so that a container with users that need standard home folder attributes appears in the right pane.
4. In the right pane, right-click the desired organizational unit and select **User Actions > Assign Managed Path**.
5. Select the **Always overwrite Managed Path attribute** option.
6. Click **Browse**, use the Path Browser dialog box to browse to the path where you want all home folders in the selected container to reside, then click **OK**.
7. Verify that the **Run in Check Mode** check box is selected.
8. Click **Run**.
9. Click **Expand Results** to expand the view.

   Storage Manager for eDirectory summarizes any problems it can resolve in the **Action** column. Resulting home folder attributes that will be created are displayed as "Match found. Managed path would be set."
10. Click **Collapse**.
11. If you approve of the actions Storage Manager for eDirectory took in check mode, deselect **Run in Check Mode** and click **Run**.
12. Run a new consistency check report by selecting the organizational unit you selected in Step 4, clicking **Consistency Check**, then clicking **Run**.
13. Observe that all users who did not previously have proper home folder attributes, now do.

4.6 Creating a Blocking Policy

Storage Manager for eDirectory provides the ability to create "blocking policies" that block other Storage Manager for eDirectory policies from affecting members of organizational units, members of groups, or even individual users. For example, you might have proxy users such as a BACKUP PROXY or VIRUS SCAN PROXY who do not need a home folder. Or, you might have an organizational unit within an organizational unit whose members you do not want to be assigned home folders.

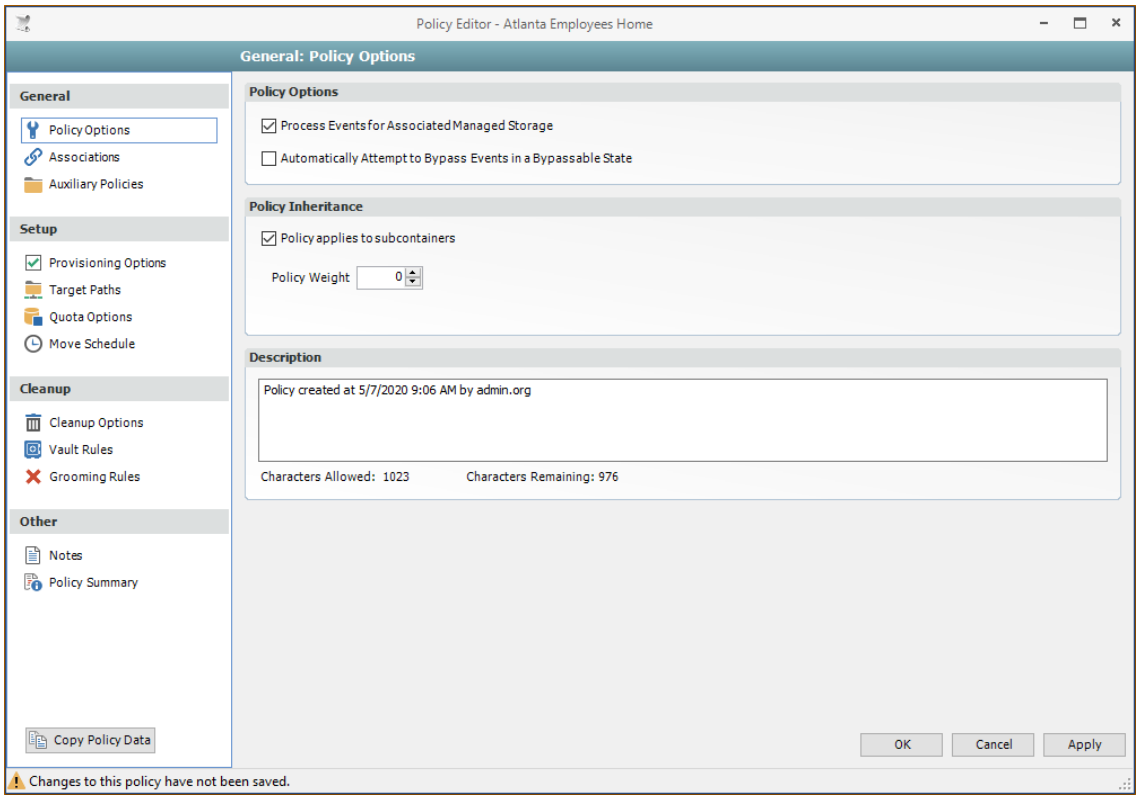
Creating a blocking policy is as easy as creating a group, adding the users you want to block from a policy to the group, and then using the Admin Client to create the blocking policy and associate it to the group.

NOTE: Blocking policies can be assigned to users, groups or containers.

IMPORTANT: Before proceeding, you should create a group in eDirectory whose members you want to block from the effects of any Storage Manager for eDirectory policies that you create.

1. In the Admin Client, click the **Main** tab.
2. Click **Policy Management**.
3. From the **Manage** drop-down menu, select **New > User Home Folder**.
4. Specify a descriptive name in the **Name** field, such as “Block Policy,” leave the **User** option selected, then click **OK**.

   The Policy Options page appears.



5. Deselect the **Process Events for Associated Managed Storage** check box.

   A description at the right of the check box indicates that the policy is now a blocking policy.
6. In the left pane, click **Associations**.
7. Click the + sign.
8. Browse down and locate the user, group, or container that you want to block from the effects of Storage Manager for eDirectory policies, then drag it to the **Selected Items** pane.
9. Click **OK** to save the setting.
10. Click **OK** to save the block policy.

4.7 Creating a User Home Folder Policy

A policy is the means by which Storage Manager for eDirectory provisions, manages, deletes, and archives storage. The parameters within the policy dictate where user storage is created, what rights are granted, what quota to assign, what to do when a user is deleted, and much more.

IMPORTANT: Only one policy of the same type can be associated with a volume, container, group, or user.

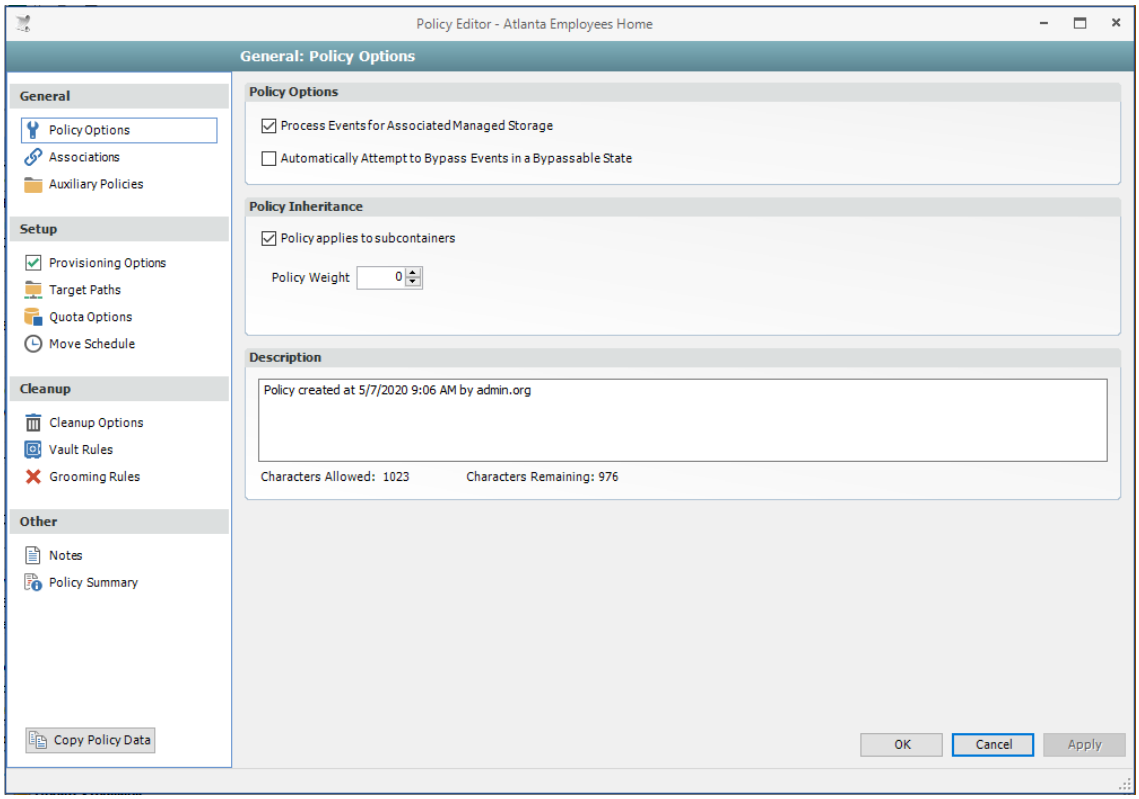
1 In the Admin Client, click the **Main** tab.

2 Click **Policy Management**.

3 From the In **Manage** drop-down menu, select **New > User Home Folder**.

4 Specify a descriptive name for the policy, then click **OK**.

The Policy Options page appears.



5 Set the Policy Options specifications for the policy:

5a If you want the container's subcontainers to inherit the policy settings, leave the **Policy applies to subcontainers** check box selected. Otherwise, deselect it.

5b If you will have users that are members of multiple groups, which means they could be affected by multiple policies, use the **Policy Weight** field to indicate a weight for this policy.

When multiple policies pertain to a user, Storage Manager for eDirectory uses the highest weight number to determine which policy to apply.

6 Set the associations:

6a In the left pane, click **Associations**.

6b Click **Add**.

6c Browse to and locate the organizational unit, Group object, or User object you want the policy applied to, then drag it to the Selected Items pane.

6d Click **OK**.

7 Set the provisioning specifications:

7a In the Folder Properties region, specify the settings you want for the rights to be applied to network home folders that are created through this policy. Select the **Policy-Defined Default Attributes** check box, to activate additional check boxes.

7b In the Template Folder region, click the **Browse** button to locate and place a path to a template directory that can be copied into each home folder.

For more information on templates, see Step 3 on page 34.

7c In the Home Folder region, leave the **Set target path server as Default Server** check box selected.

8 Set the target paths:

8a In the left pane, click **Target Paths**.

8b Click **Add**, browse to the volume or folder where you want your home folders to reside, right-click and choose **Select** to add the target path to the Selected Paths pane.

8c Click **OK**.

8d If you want to set the location of home directories among different paths, repeat Step 8b to include all the paths you want.

8e If you have multiple paths listed, select a distribution method from the **Distribution** drop-down list.

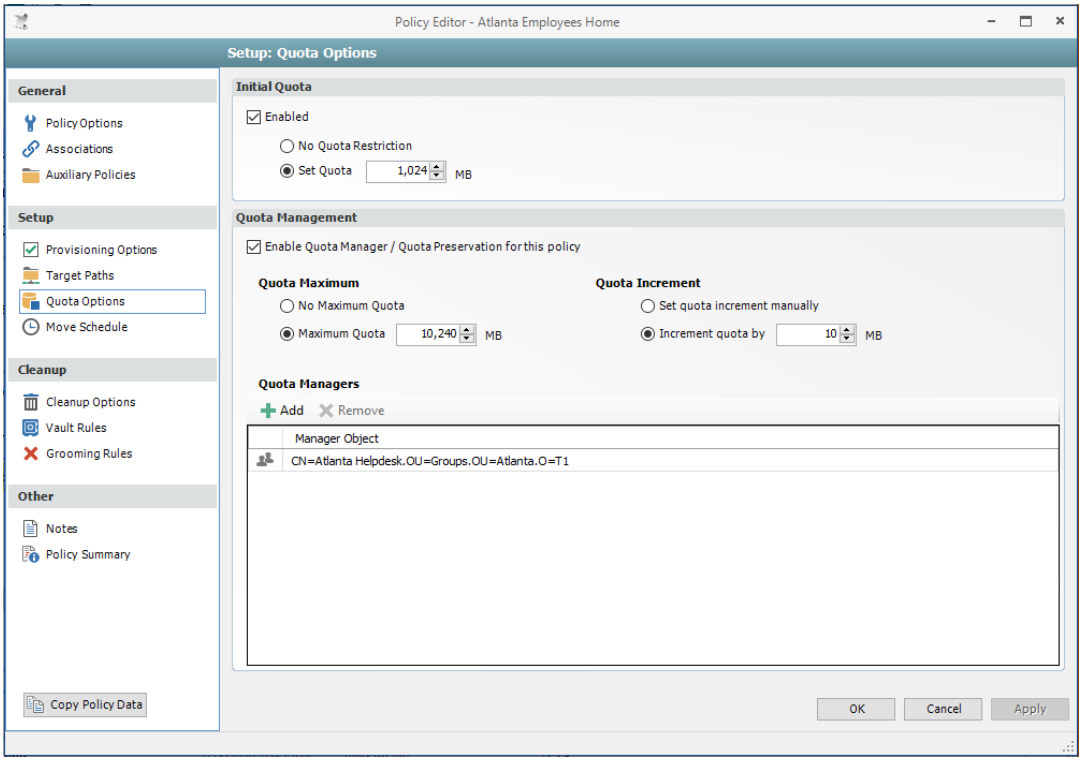
For an explanation of storage distribution, see Section 5.4.4, “Setting Target Paths,” on page 35.

8f Leave the other fields as they are currently set.

8g Click **Apply** to save your settings.

9 Set the directory quota options:

9a In the left pane, click **Quota Options**.



9b In the Initial Quota region, specify the amount of initial directory storage space to be allocated to all users associated with this policy.

9c (Optional) In the Quota Management region, click the **Enable Quota Manager / Quota Preservation for this Policy** check box, to display additional options.

9d Select one of the following Quota Maximum options:

- Use the **No Maximum Quota** option to specify that the users managed by this policy will be granted additional directory storage quota when they need more.
- Use the **Maximum Quota** field to specify the maximum amount of storage that is allocated to a user. This allocation comes through the quota increment settings below.

9e (Optional) Select one of the following Quota Increment options:

- Select the **Set quota increment manually** option to allow users who are designated as quota managers to set directory quotas manually.
- Select the **Increment quota by** option to indicate the size in MB for each new allocation of additional storage quota.

9f Click **Apply** to save your settings.

10 Set the move schedule:

10a In the left pane, click **Move Schedule**.

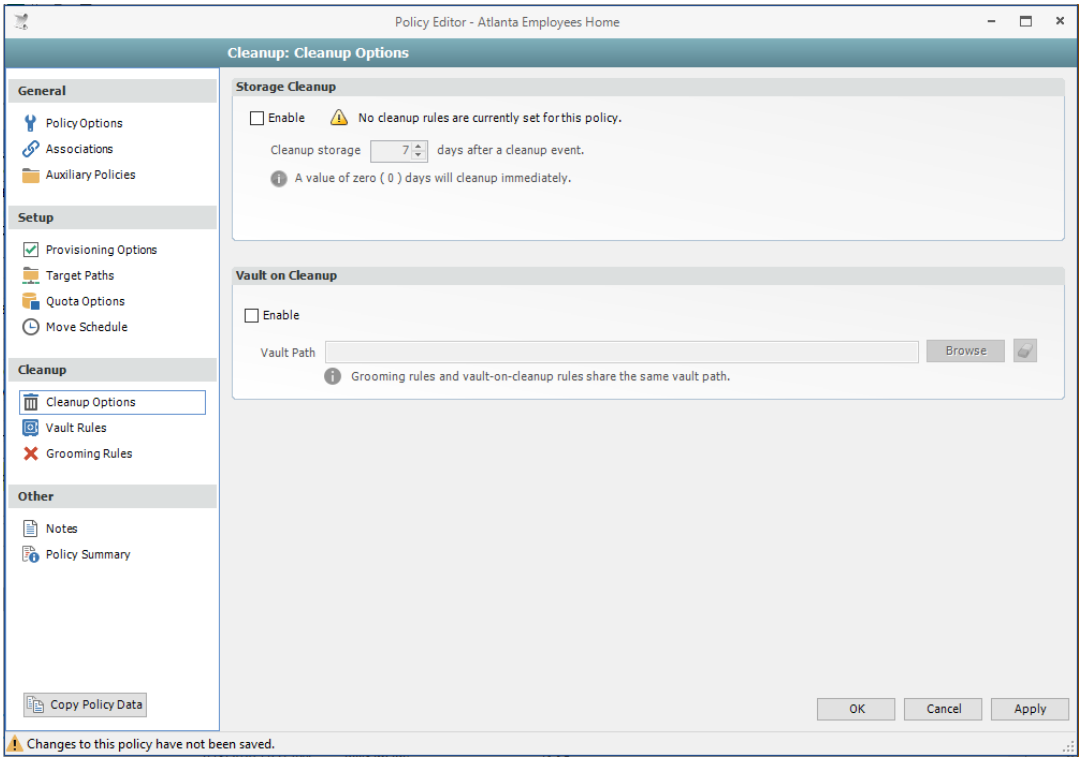
10b Specify the hours when Storage Manager for eDirectory can perform data migrations.

For more information on data migrations, see Section 5.4.6, “Setting the Move Schedule,” on page 38.

10c Click **Apply** to save the settings.

11 Set the cleanup options:

11a In the left pane, click **Cleanup Options**.



11b In the Storage Cleanup region, select the **Enable** check box to indicate if you want user storage associated with this policy deleted when a user is removed from eDirectory.

If you select the check box, you can specify the number of days a user home folder and its contents will remain before it is deleted.

11c If you want user storage associated with this policy vaulted, in the Vault on Cleanup region, select the **Enable** check box and use the **Browse** button to indicate a path to the vault location.

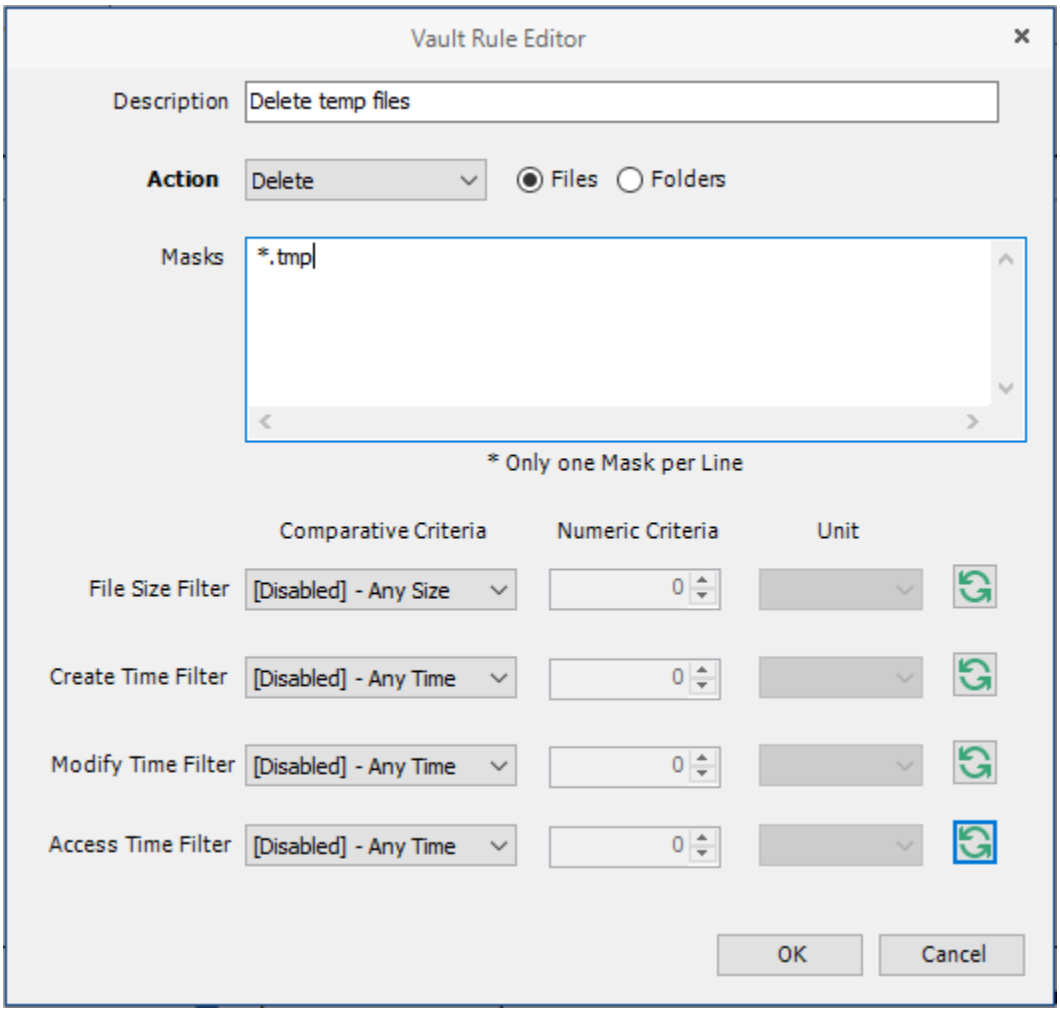
11d Click **Apply** to save your settings.

If you have both Storage Cleanup and Vault on Cleanup enabled, Storage Manager for eDirectory vaults the data and then deletes it after the specified period of time. If you have Vault on Cleanup but not Storage Cleanup enabled, Storage Manager for eDirectory vaults the data immediately and never cleans it up.

12 Set the vault rules:

12a In the left pane, click **Vault Rules**.

12b Click the **Add** to create vault rules.



For example, in the rule above, all `.tmp` files are deleted prior to their home folder being vaulted. When the specified number of days in the **Cleanup storage after** field has passed, the home folder is deleted from the specified vault location.

12c Click **Apply** to save your settings.

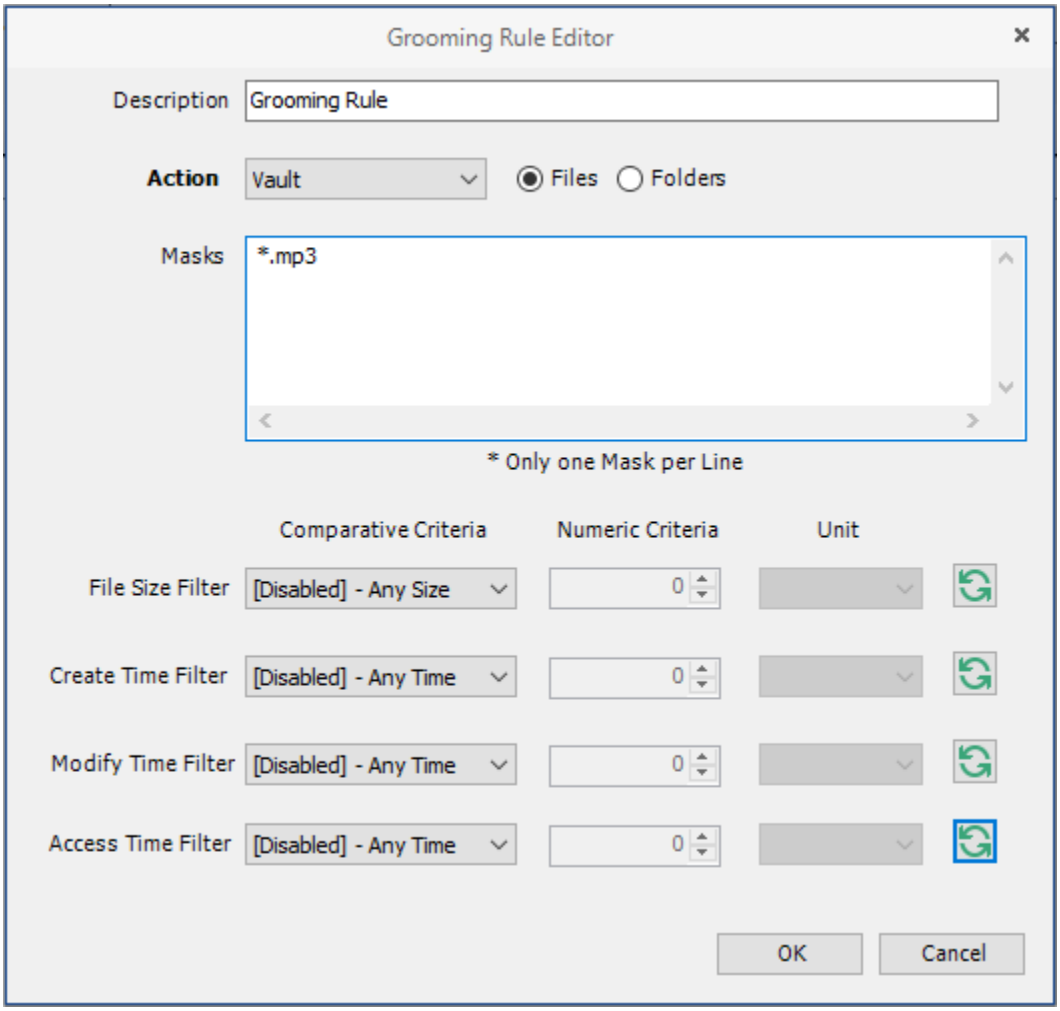
13 Set the grooming rules:

13a In the left pane, click **Grooming Rules**.

13b Click **Add**.

13c Select either **Vault** or **Delete** from the **Action** drop-down menu to specify whether to vault or delete a particular type of file.

13d In the **File Name Mask** field, indicate the type of file for which this grooming rule will take action. For example, `*.mp3` and `*.mp4`.



To narrow the scope of the grooming rule, you can use the filter settings in the lower portion of the dialog box.

For example, if you select **Greater than** from the **File Size Filter** drop-down menu, enter 2 as the Numeric Criteria, and select **MBs** as the Unit setting, the grooming rule in this example vaults all MP3 files greater than 2 MB. Setting additional filters narrows the scope of the grooming action even more.

13e Click **OK** to save the grooming rule.

13f Repeat Step 13a through Step 13e to create additional grooming rules.

13g Click **Apply** to apply the grooming rules.

14 Click **OK** to save the policy settings.

4.8 Removing a Preexisting Process for Creating User Home Folders

When you create and configure a policy, it is important to understand that Storage Manager for eDirectory is now set up to provision and manage all new users that are created in the associated container.

If you have a network tool such as ConsoleOne or iManager creating home folders when a new user is added to the container or group associated with a policy, you need to remove the setting that creates the home folder.

You might also need to notify anyone who previously managed storage for those users that are now being managed by Storage Manager for eDirectory, to cease any manual storage management tasks such as home folder creation, renames, moves, etc., and let Storage Manager for eDirectory now manage the user storage.

4.9 Testing the User Home Folder Policy

You should now create a test user to confirm that Storage Manager for eDirectory will provision and deprovision the test user's home folder according to the policy rules that you created.

1. Using ConsoleOne or iManager, create a new user such as TESTUSER in the organizational unit associated with the policy you configured in Section 4.7, "Creating a User Home Folder Policy," on page 22.
2. In the Admin Client, click the **Main** tab.
3. Click **Path Analysis**.
4. In the left pane, browse down to the location where the new home folder for the new TESTUSER is located.
5. Select the TESTUSER home folder, then select **Folder Trustees**.

   This displays the View Trustees page.
6. Verify that the rights that you set in Step 7a on page 24 are those that you set in the policy.
7. Click **OK** to close the View Trustees page.
8. Click **Quota**.

   This displays the View Quota dialog box.
9. Verify that the quota specifications that you set in Step 9 on page 24 are those that you set in the policy.
10. Click **OK** to close the View Quota dialog box.

4.10 Performing a Consistency Check

Performing a follow-up consistency check allows you to verify that other policy specifications that you established in the user home folder policy are being enacted.

1. In the Admin Client, click the **Main** tab.
2. Click **Identity Objects**.
3. In the left pane, browse to select the organizational unit associated with the policy that you created earlier.
4. Select the **Filters** check box that is associated with Users.

5 In the right pane, locate and right-click TESTUSER, then select **User Actions > Consistency Check.**

The Take Action – User Mode page appears.

6 Click **Process Selected Targets**.

7 Verify that the settings for the home directory attribute (DS Path), Flags, Rights, and Quota are what you established when you configured the policy. Additionally, verify that the Management status is set to “Managed” and that the Mgmt Path and DS Path match (a check mark in the **Paths Match** column indicates a match).

4.11 Testing a Rename Event

This procedure lets you verify that a user’s home folder attribute is updated following a rename event.

1 Use iManager or ConsoleOne to rename the user from the suggested TESTUSER name to a name such as TESTUSER2.

2 In the Admin Client, while you are still displaying the users through the Identity Objects page, click **Refresh** to refresh the screen and see the renamed user.

3 Right-click the renamed user and select **User Actions > Consistency Check**.

4 Verify that the home folder and the directory attribute have been updated in the **DS Path** and **Mgmt Path** columns.

4.12 Testing a Cleanup Rule

This procedure lets you verify that Storage Manager for eDirectory cleans up a user’s storage according to the user home folder policy that you created earlier.

1 Use iManager or ConsoleOne to delete TESTUSER2.

2 If you chose to delay the cleanup of user storage for a set amount of days in Step 11b on page 26, open the Admin Client, click the **Main** tab **> Pending Events > Deferred** to view any information indicating the deferred number of days for the storage cleanup.

3 Click **Path Analysis**.

4 In the left pane, browse to the location where the TESTUSER2 resided and verify that the folder has been deleted.

5 (Conditional) If you set your policy to vault deleted storage, browse to the location in the left pane where you chose to vault deleted storage in Step 11c on page 26 and verify that TESTUSER2 was vaulted:

5a If you set your policy to delay the cleanup of user storage for a set amount of days in Step 11b on page 26, click **Pending Events** to view details on deferred action.

5b Right-click the listed deferred action, then select **Properties**. In the Properties dialog box, then verify that the **Next Eligible Time** displays a date that corresponds to the number of days you set in your policy for the deleted storage to be cleaned up.

5c Click **OK** to close the dialog box.

6 Because this is a test user, perform the storage cleanup immediately by once again right-clicking the listed deferred action and selecting **Make Eligible**.

7 Click **Path Analysis** and browse to the location in the left pane where you viewed the vaulted storage, then verify that the storage has been cleaned up.

4.13 What's Next

Now that you have created and tested a User Home Folder policy, you can create User Home Folder policies for the users in other containers or groups. You can do so based on the overview and procedures you were given in this chapter, or you can review Chapter 5, "Managing User Home Folders," on page 31, which provides a more comprehensive discussion of performing user-based storage tasks in the Admin Client.

When you have a better understanding of the user-based storage capabilities in Storage Manager for eDirectory, you can proceed to have Storage Manager for eDirectory manage your collaborative-based storage. Refer to Chapter 7, "Managing Collaborative Storage," on page 63 for a comprehensive discussion and procedures for performing collaborative storage tasks.

5 Managing User Home Folders

5.1 Overview

In Chapter 4, “Managing Existing User Storage,” on page 17, you created and configured a blocking policy and a User Home Folder policy to put your existing storage in a managed state. In this section you will learn in greater detail about how to create and configure User Home Folder policies, along with other policies associated with user storage. These include:

- User policies
- Auxiliary storage policies

5.2 User Policies

User policies automate the provisioning, ongoing management, and disposition of network user home folders. A user policy can be associated with the following eDirectory objects:

- Organization
- Organizational Unit
- Group
- User

If you associate a user policy to an Organization object or Organizational Unit object, the policy affects all users that reside in those areas of the directory, unless it is specifically blocked through a blocking policy. If you associate the policy to a group, it affects all members of the group.

Standard directory inheritance applies to policy associations. This means that if you assign a policy to an Organization object but there is a policy at an Organizational Unit object the policy associated with the Organizational Unit object will be the active policy for the user. The policy that is most directly associated to the user takes precedence.

NOTE: Although creating a user policy for an individual User object is possible, it is somewhat impractical and should only be done in rare circumstances.

User policies are stored in a database that is created during the Engine installation.

5.3 Setting Up a Vaulting Location

Vaulting is the process of saving the contents of a user's home folder after the user's User object has been removed from eDirectory. If your user storage policies are to include vaulting rules, you must first set up a storage location where the policy will vault the storage.

5.4 Creating a User Home Folder Policy

Prior to creating the user policy, you must determine if the policy should pertain to the members of the organization, organizational unit, or a group.

1. Launch the Admin Client.
2. In the **Main** menu, click **Policy Management**.
3. From the **Manage** drop-down menu, select **New > User Home Folder.**
4. Specify a descriptive name in the **Name** field and click **OK**.

   The Policy Options page appears.
5. Continue with Section 5.4.1, "Setting Policy Options," on page 32.

5.4.1 Setting Policy Options

Settings within Policy Options let you indicate how to apply the policy, set policy inheritance and policy weight, and write an expanded policy description.

1. In the Policy options region, fill in the following fields:

   Process Events for Associated Managed Storage: Select this check box to apply the settings in this policy to all users within the container where this policy is assigned. Deselect this check box to create a blocking policy that can be applied to a specific user, group, or container. For more information on blocking policies, see Section 4.6, "Creating a Blocking Policy," on page 21.

   Automatically Attempt to Bypass Events in Bypassable State: Select this check box to allow Storage Manager for eDirectory to automatically attempt to address any pending events that can bypass administrative action.

   Be careful when considering applying this setting to a policy. Doing so has the potential to make incorrect associations and, thus, grant a user access to a folder that he or she shouldn't have. For example, suppose Tom Smith and Tammy Smith are in the same container and managed by the same policy, and that there is a home folder already created named TSMITH. Storage Manager for eDirectory might consider this a bypassable event and, if this check box is selected, might associate the home folder to Tammy Smith, when it should belong to Tom Smith.
2. In the Policy Inheritance region, fill in the following fields:

   Policy applies to subcontainers: Select this check box to have this policy inherited for all containers that reside within the organization or organizational unit where this policy is assigned.

   Policy Weight: When a user is a member of multiple groups and each group has a separate effective policy, Storage Manager for eDirectory uses this setting to determine which policy to apply. Storage Manager for eDirectory applies the policy with the largest numerical weight.

   In the case where multiple policies have the same weight, the event will go into a pending state indicating that multiple polices have the same weight and one must be changed in order for the event to process.

3 In the text field in the Description region, specify a description of the policy you are creating.

4 Proceed with Section 5.4.2, “Setting Associations,” on page 33.

5.4.2 Setting Associations

The Associations page is where you assign the policy you are creating to a container, Group object, or—if you are creating a blocking policy—a User, Group, or Container object.

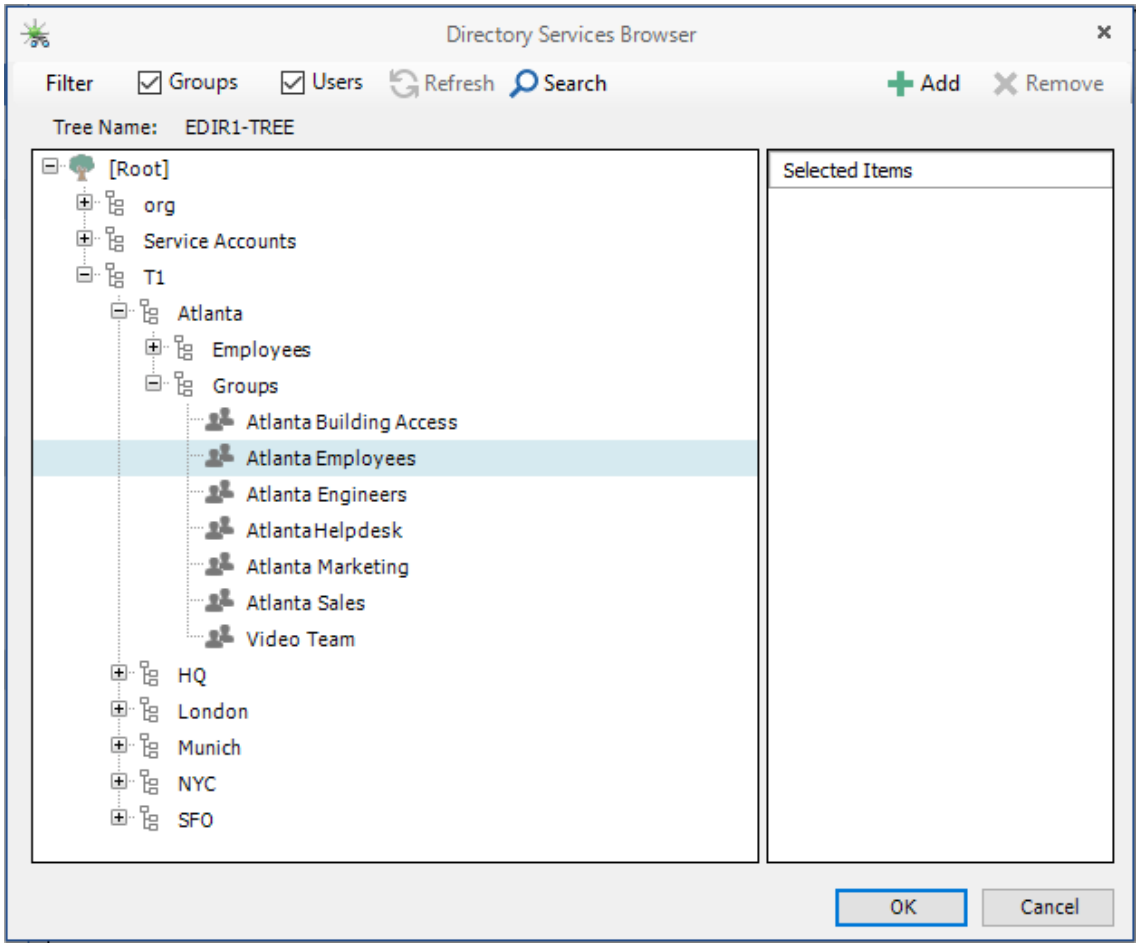
1 In the left pane, click **Associations**.

2 Click **Add** to bring up the Object Browser.

3 If you plan to assign the policy to a User object, select the **Users** check box in the Filter region of the Object Browser.

4 Browse through the directory structure and select the container, Group object, or User object you want to associate the policy to.

A policy can be assigned to multiple organizational units, groups, and users.



5 Drag the object to the Selected Items pane, then click **OK**.

The Object Browser is closed and the object is displayed in fully distinguished name format in the right pane of the window. For example, Atlanta Employees.Groups.Atlanta.T1.

6 Click **OK** to close the Object Browser.

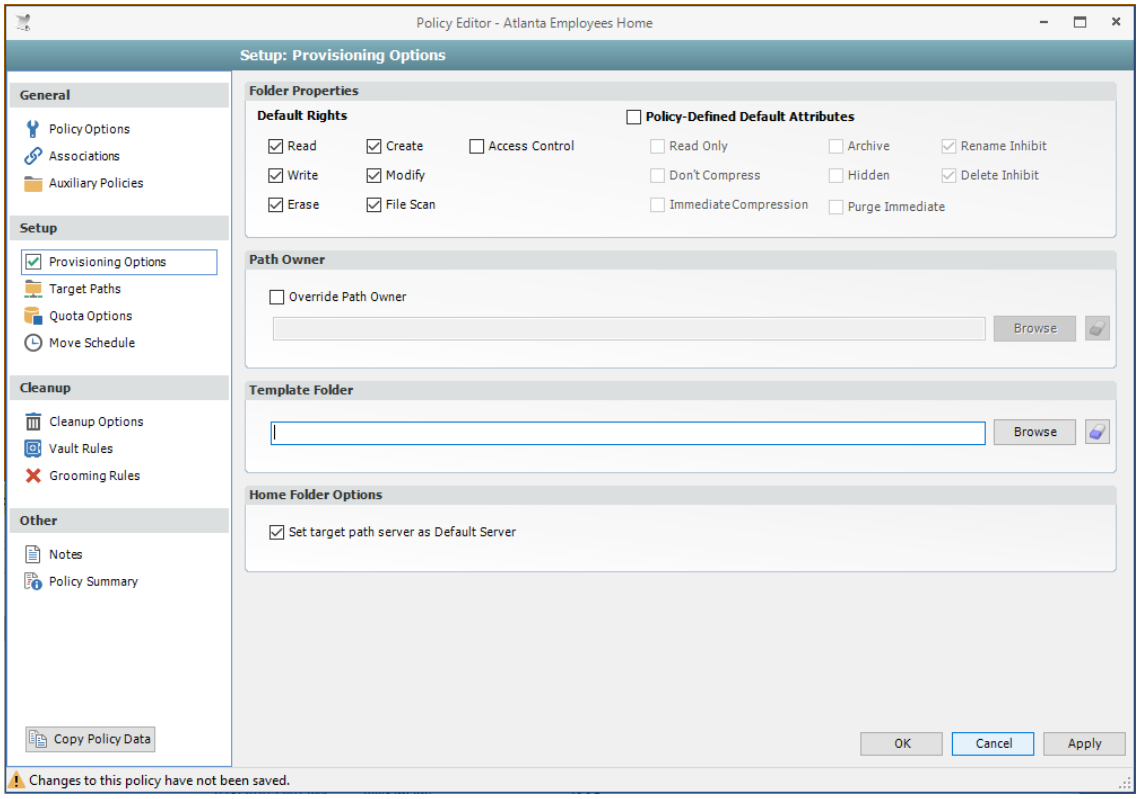
7 Proceed with Section 5.4.3, “Provisioning Options,” on page 34.

5.4.3 Provisioning Options

The Provisioning Options page is where you indicate home folder rights, home folder attributes, the location of a template for provisioning folder structure and content in a home folder when it is created, and more.

1 In the left pane, click **Provisioning Options**.

The following page appears:



2 In the Folder Properties region, specify the following settings:

Default Rights: By default, Storage Manager for eDirectory grants the user all file rights to the home folder except for Access Control. Granting Access Control is not recommended because it provides administrator rights to the home folder, and enables the user to rename and delete the folder.

Policy Defined Default Attributes: Select this check box to enable the **Archive**, **System**, and **Hidden** check boxes, which provide the user the ability to set these attributes for the home folder. For example, if you wanted home folders to be hidden from view, you could enable the Hidden attribute by selecting the **Hidden** check box.

3 (Optional) To have subfolders and documents provisioned in the home folder when it is created, use an existing file path as a template.

For example, if you wanted each home folder to have an HR subfolder with some HR documents inside, click **Browse** to locate and select the HR folder in the file system.

Everything beneath the selected folder is copied into the user's home folder.

4 In the Home Folder Options region, leave the **Set target path server as Default Server** check box selected so that during login, Storage Manager for eDirectory will connect to the target server and reduce unwanted authentications to other servers.

5 Proceed with Section 5.4.4, “Setting Target Paths,” on page 35.

5.4.4 Setting Target Paths

The Target Paths page is where you set the paths to the server volumes where user home folders will be hosted.

1 In the left pane, click **Target Paths**.

2 In the Target Placement region, fill in the following fields:

Distribution: If you create more than one target path for a policy, you can indicate any of the following options:

- **Random:** Distributes storage randomly among the number of target paths.
- **Actual Free Space:** Distributes the creation of user home folders according to volumes with the largest amount of absolute free space. For example, if you have two target paths listed, target path 1 has 15 GB of free space, and target path 2 has 10 GB, the home folders are created using target path 1.
- **Percentage Free Space:** Distributes the creation of user home directories to volumes with the largest percentage of free space. For example, if you have two target paths listed, target path 1 is to a 10 TB volume that has 30 percent free space and target path 2 is to a 500 GB volume with 40 percent free space, the home directories are created using target path 2, even though target path 1 has more absolute available disk space. You should be cautious when using this option with target paths to volumes of different sizes.

Leveling Algorithm: Use this option to structure the home folders so that they are categorized by the first or last letter of a username through a subordinate folder. For example, if you choose **First Letter**, and the **Leveling Length** field is set to 1, a user named BSMITH has a home folder located in a path such as `\\S2\HOME\B\BSMITH`.

If you choose **Last Letter**, and the **Leveling Length** field is set to 1, the same user has a home folder located in a path such as `\\S2\HOME\H\BSMITH`.

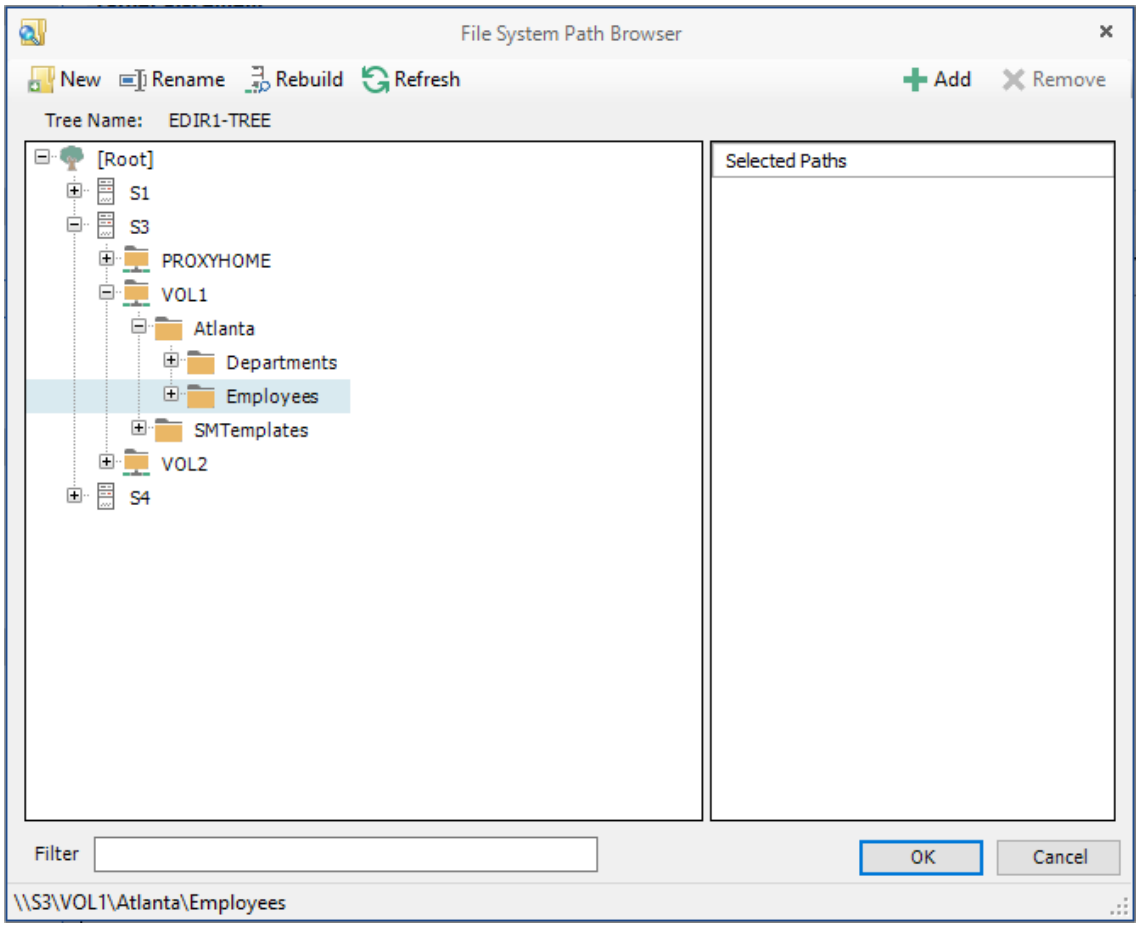
The **Last Letter** means the last character of the attribute Storage Manager for eDirectory uses to create storage.

The **Leveling Length** field allows you to enter up to 4 characters. This makes it so that you can organize home folders by year. For example, if your **Leveling Algorithm** setting is **Last Letter**, and the **Leveling Length** setting is 4, a user named BMITH2020 has a home folder located in a path such as `\\S3\HOME\2020\BSMITH2020`.

Maximum Unreachable Paths: If you have a substantial number of target paths listed on this page, this field lets you indicate the number of target paths Storage Manager for eDirectory accesses to attempt to create a home folder before it suspends the attempt.

3 For each target path that you want to establish, click **Add** to access the Path Browser.

4 Browse to the location of the target path you want and click **Add** to add the target path to the Selected Paths pane.



5 Click **Apply** to save your settings.

6 Proceed to Section 5.4.5, “Setting Quota Options,” on page 36.

5.4.5 Setting Quota Options

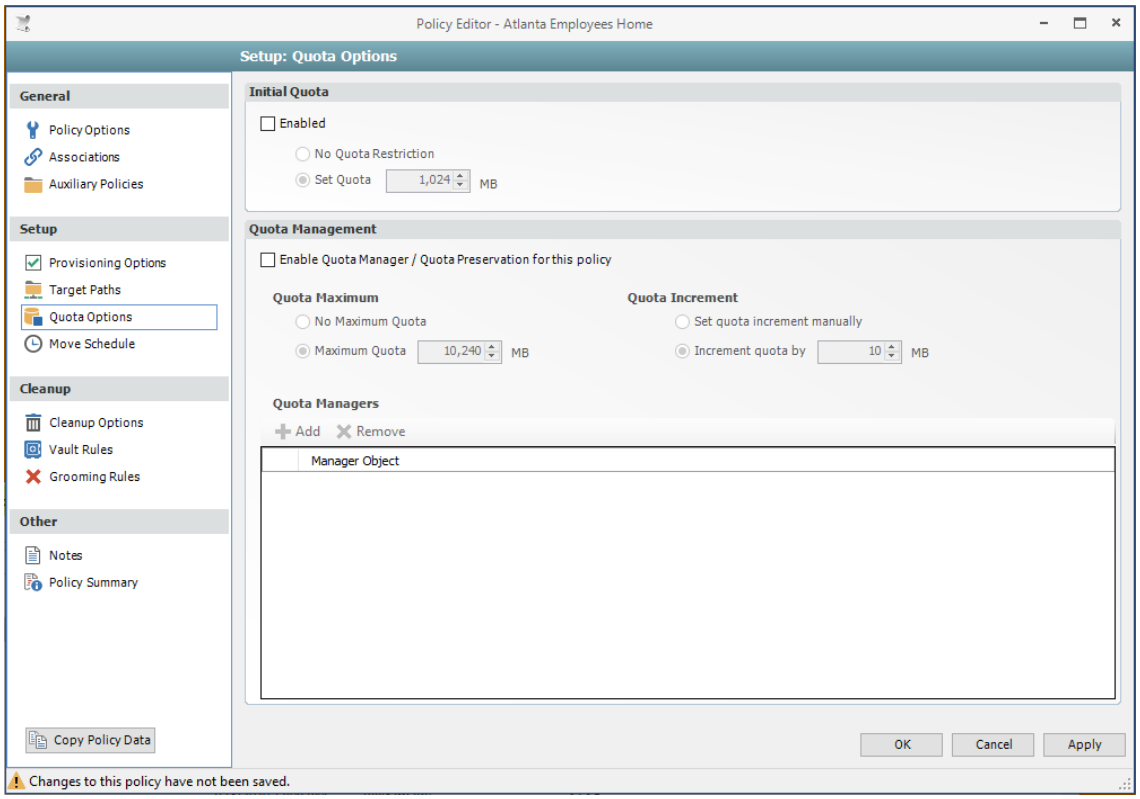
This page lets you establish user storage quotas. Until quota management is established, users have unlimited storage disk space for their home folders.

Storage Manager 5.3 for eDirectory policies manage directory quota, rather than volume quota.

This page is also where you establish quota management settings for quota managers. A quota manager is a specified user or group—for example, a help desk administrator or technical support rep—who is granted the ability to increase a user’s quota, without having rights to the file system. Quota management actions are performed through Quota Manager, which is a separate Web browser-based management interface. For more information on Quota Manager, see Chapter 8, “Using Quota Manager,” on page 81.

1 In the left pane, click **Quota Options**.

The following page appears:



2 Select the **Enabled** check box to enable quota management.

3 In the **MB** field, specify the initial storage quota for the user home folders.

4 Set up quota managers for this policy by filling in the following fields:

Enable Quota Manager / Quota Preservation for this Policy: Select this check box to enable the Quota Management region of the page and to enable quota preservation.

Quota preservation preserves the home folder quota settings for users that are moved. For example, if a user is moved from the Sales organizational unit to the Marketing organizational unit, if the user's quota allocation for the policy that applies to Sales were higher than the quota allocation for the policy that applies to Marketing, the quota allocations from the policy associated with the Sales policy are preserved for the user.

Quota Maximum: Indicate whether the users associated with this policy will have a maximum quota setting. If so, indicate the maximum quota.

Quota Increment: Indicate whether quota managers will set the quota manually or in set increments. If you use manual increments, the quota manager can increase the quota in any increment until it meets the maximum quota setting. If you establish set increments, the quota manager can only increase the quota by the increment setting.

Quota Managers: Click **Add** and use the Object Browser to browse to and select a user you want to serve as a quota manager by dragging the User object over to the right pane. Repeat this for each user you want to establish as a quota manager.

5 Click **Apply** to save your settings.

6 Proceed with Section 5.4.6, "Setting the Move Schedule," on page 38.

5.4.6 Setting the Move Schedule

This page lets you use a grid to specify when data can be moved during data movement operations.

By default, all days and times are available for data movement. If data movement during regular business hours creates unacceptable network performance, you can choose to move data after regular business hours.

1. In the left pane, click **Move Schedule**.
2. In the Data Move Schedule grid, click the squares for the day and hour you want to disable for data movement.
3. Click **Apply** to save your settings.
4. Proceed with Section 5.4.7, “Setting Cleanup Options,” on page 38.

5.4.7 Setting Cleanup Options

This page lets you enable and specify cleanup rules for the policy. Options for cleanup include deleting a home folder after a set number of days following the removal of a User object from eDirectory, or vaulting (rather than deleting) the home folder.

1. In the left pane, click **Cleanup Options**.
2. Enable storage cleanup by filling in the following fields:

   Enable: Select this check box to enable storage cleanup rules.

   Cleanup storage: Specify the number of days a user home folder remains after the associated User object is removed from eDirectory.
3. Enable vault on cleanup by filling in the following fields:

   Enable: Select this check box to enable vault on cleanup rules.

   Vault Path: Click **Browse** to browse and select the volume where you want the cleaned-up user home folders to be vaulted.

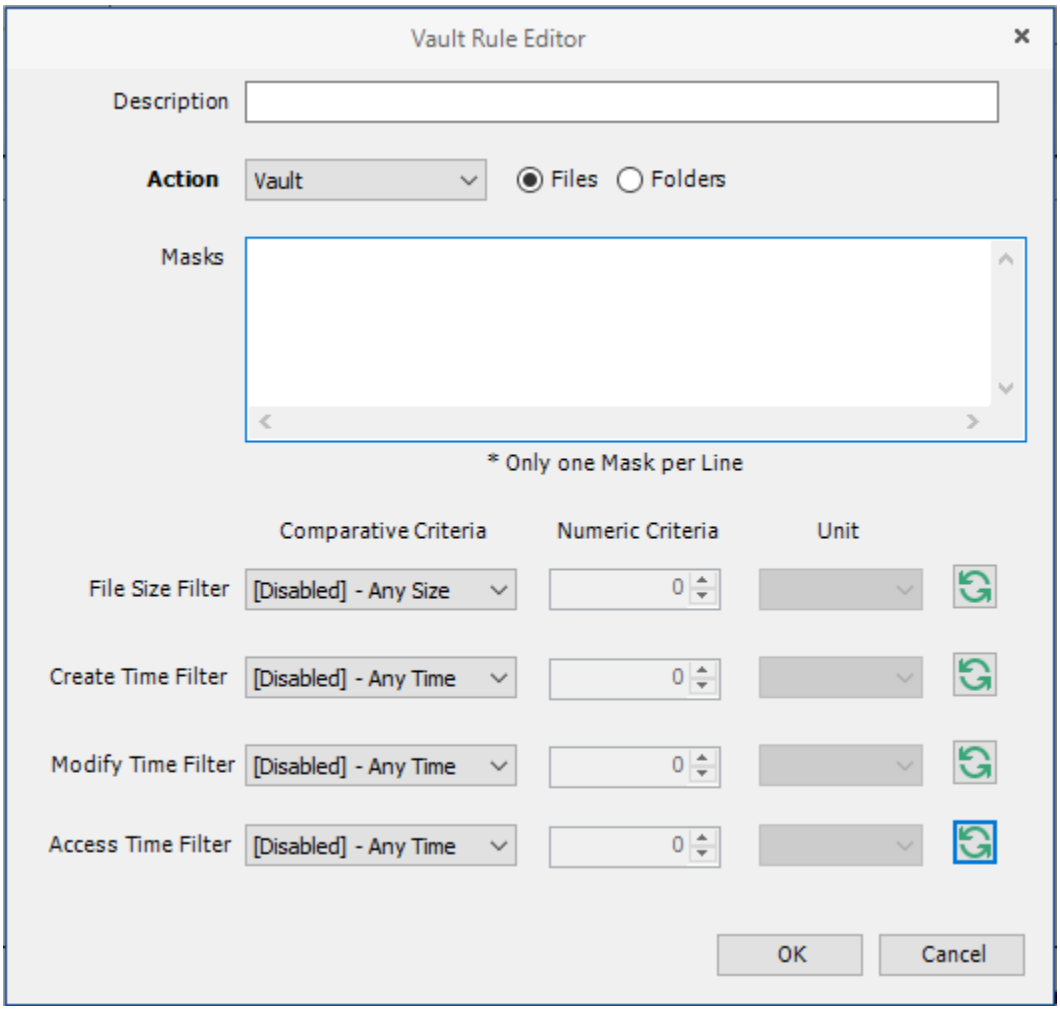
   When you indicate this path, it also appears in the **Vault Path** field of the Grooming Rules page, because grooming rules and vault on cleanup rules share the same vault path.
4. Click **Apply** to save the settings.
5. Proceed with Section 5.4.8, “Setting Vault Rules,” on page 38.

5.4.8 Setting Vault Rules

When a User object is removed from eDirectory, you can have Storage Manager for eDirectory vault the contents of the user’s home folder from a primary storage device to a less expensive secondary storage device. Storage Manager for eDirectory lets you specify what to vault or delete through vault rules. For example, before vaulting a user’s home folder, you might want to remove all `.tmp` files. Or, you might want to vault only the user’s `My Documents` folder and nothing else in the home folder. You accomplish all of this through settings in the Vault Rules Editor.

1. In the left pane, click **Vault Rules**.

   The **Vault Path** field displays the vault path that you established when you set up cleanup rules.
2. Click **Add** to bring up the Vault Rules Editor.



3 In the **Description** field, specify a description of the vault rule.

For example, “Files to delete before vaulting,” or “Files to vault.”

4 Fill in the following fields:

Action: Select whether this vault rule will delete or vault files.

If you select **Vault**, only the files or folders that you list in the **Masks** text box are vaulted and the remainder of the home folder contents is deleted. Conversely, if you select **Delete**, only the files or folder that you list in the **Masks** text box is deleted and the remainder is vaulted.

Files: If the vault rule you are creating will vault or delete content at the file level, leave the **File** option selected.

Folders: If the vault rule you are creating will vault or delete content at the folder level, select the **Folders** option.

Selecting **Folders** disables the filter settings in the lower portion of the Vault Rules Editor.

Masks: List the files or folders you want to be vaulted or deleted, according to what is indicated in the **Action** drop-down menu.

File or folder names can contain an asterisk.

5 (Conditional) If the vault rule you are creating is specific to files, complete the applicable filter settings.

Leaving the setting as **[Disabled]-Any Size**, vaults or deletes all file types listed in the **Mask** text box according to what is indicated in the **Action** drop-down menu. Choosing any of the other options from the drop-down menu lets you indicate files to delete or vault according to size, when created, when last modified, and when last accessed.

6 Click **OK** to save the vault rule.

7 If necessary, create any needed additional vault rules by repeating the procedures above.

8 Proceed with Section 5.4.9, “Setting Grooming Rules,” on page 40.

5.4.9 Setting Grooming Rules

Grooming rules in Storage Manager for eDirectory specify the file types that you do not want network users storing in their home folders. Examples of these might be MP3 and MP4 files, MOV files, and many others. You specify in the grooming rule whether to delete or vault a groomed file.

Grooming takes place as a Management Action that is run by the administrator. A Management Action is a manual action that is enacted through the Admin Client. For more information, see Section 9.1.4, “Management Actions,” on page 88.

1 In the left pane, click **Grooming Rules**.

The **Vault Path** field displays the vault path that you established when you set up cleanup rules.

2 Click **Add** to bring up the Grooming Rules Editor.

3 In the **Description** field, enter a description of the grooming rule.

For example, “Files to groom in Henderson OU.”

4 Fill in the following fields:

Action: Select whether this grooming rule will delete or vault groomed files.

Files: If the grooming rule you are creating will vault or delete content at the file level, leave the **File** option selected.

Folders: If the grooming rule you are creating will vault or delete content at the folder level, select the **Folders** option.

Masks: List the files or folders you want to be vaulted or deleted, according to what is indicated in the **Action** drop-down menu.

File or folder names can contain an asterisk.

5 (Conditional) If the grooming rule you are creating is specific to files, complete the applicable filter settings.

Leaving the setting as **[Disabled]-Any Size**, vaults or deletes all file types listed in the **Mask** text box according to what is indicated in the **Action** drop-down menu. Choosing any of the other options from the drop-down menu lets you indicate files to delete or vault according to size, when created, when last modified, and when last accessed.

6 Click **OK** to save the grooming rule.

7 Click **Apply** to save your settings.

8 Proceed with Section 5.4.10, “Notes,” on page 40.

5.4.10 Notes

The Notes page lets you enter up to 64,000 characters of notes for the policy you are creating. A practical use of this page is to provide a better description of the policy.

5.4.11 Policy Summary

The Policy Summary page displays a summary of the policy settings in HTML format. The Policy Summary page provides an easy way to view all of the policy settings in a single page.

5.5 Using a Policy to Manage Inactive Users

When a user leaves an organization, many organizations choose to make the User object inactive, rather than immediately delete the User object. This provides the organization an indefinite amount of time to review and determine what to do with the contents of the user's home folder before finally deleting the User object.

In Storage Manager for eDirectory, you can easily create an Inactive Users policy that has all home folder property rights removed and apply it to an organizational unit set up specifically for inactive users. When the User object is moved to the organizational unit, the access rights for that user are immediately removed.

5.5.1 Creating an Inactive Users Organizational Unit

1. In the Admin Client, click the **Main** tab.
2. Click **Identity Objects**.
3. In the left pane, browse to where you want to create an inactive users organizational unit.
4. Right-click and select **Create OU**.
5. Give the object a descriptive name, such as "Inactive Users" and click **OK**.
6. Click **Refresh** to view the new organizational unit.

5.5.2 Creating an Inactive Users Folder

1. On a network volume, create a folder to store inactive user home folders.
2. Give the folder a descriptive name, such as "Inactive Users."

5.5.3 Creating an Inactive Users Policy

1. In the Admin Client, click **Policy Management**.
2. From the **Manage** drop-down menu, select **Create Policy > Create User Home Folder Policy.**
3. Specify a descriptive name in the **Name** field and click **OK**.

   The Policy Options page appears.
4. Continue with Section 5.5.4, "Setting an Inactive Users Policy Associations," on page 42.

5.5.4 Setting an Inactive Users Policy Associations

1. In the left pane, click **Associations**.
2. Click **Add**, then browse to and select the inactive users organizational unit you created in Step 5 on page 41.
3. Click **Add** to add the inactive users organizational unit to the Selected Items panel.
4. Click **OK** to save the setting.
5. Proceed with Section 5.5.5, “Setting Inactive Users Policy Provisioning Options,” on page 42.

5.5.5 Setting Inactive Users Policy Provisioning Options

1. In the left pane, click **Provisioning Options.**
2. In the Folder Properties region of the page, deselect each of the rights check boxes.

   This assures that User objects placed in the inactive users organizational unit do not have access rights to home folders.
3. Click **OK** to save the setting.
4. Proceed with Section 5.5.6, “Setting Inactive Users Policy Target Paths,” on page 42.

5.5.6 Setting Inactive Users Policy Target Paths

1. In the left pane, click **Target Paths**.
2. Click **Add**, then browse to and select the inactive users folder that your created in Section 5.5.2, “Creating an Inactive Users Folder,” on page 41.
3. Click **Add** to add the inactive users folder to the Selected Items panel.
4. Click **OK** to save the setting.
5. Proceed with Section 5.5.7, “Setting Inactive Users Policy Cleanup Options,” on page 42.

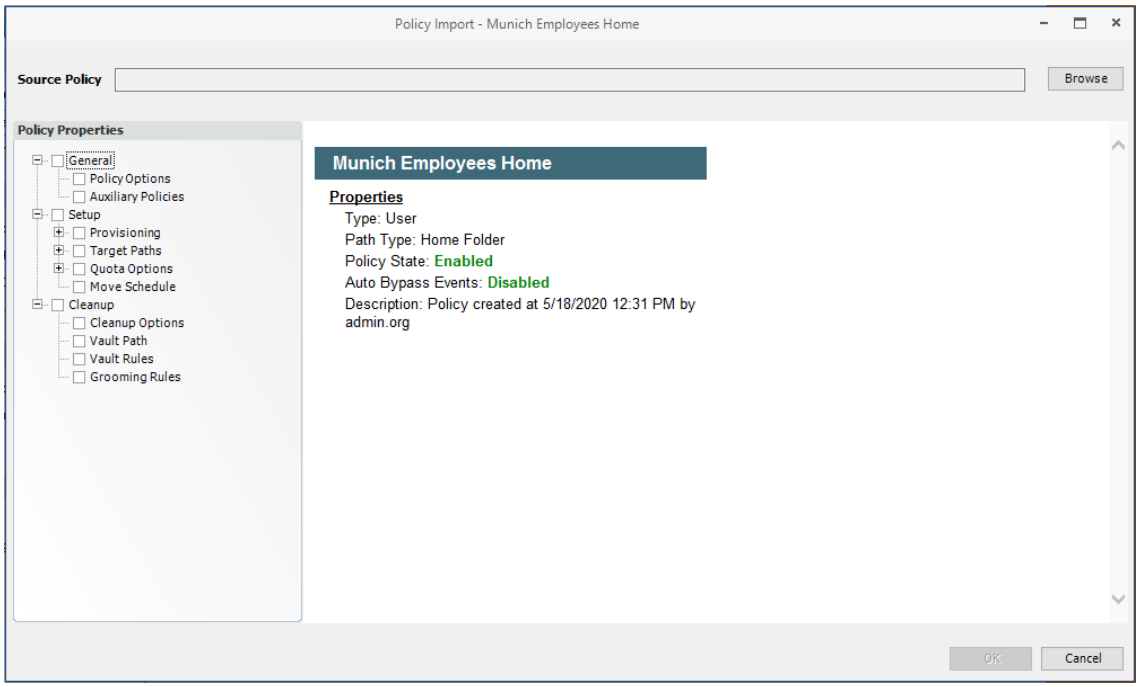
5.5.7 Setting Inactive Users Policy Cleanup Options

1. In the left pane, click **Cleanup Options.**
2. In the Storage Cleanup region, select the **Enable** check box.
3. In the **Cleanup storage** field, specify the number of days you want an inactive user’s home folder to remain before it is removed from the target path for this policy.
4. Click **Apply** to save the settings.

5.6 Copying Policy Data

Copy Policy Data allows you to copy all or a portion of the policy settings of one policy into another policy.

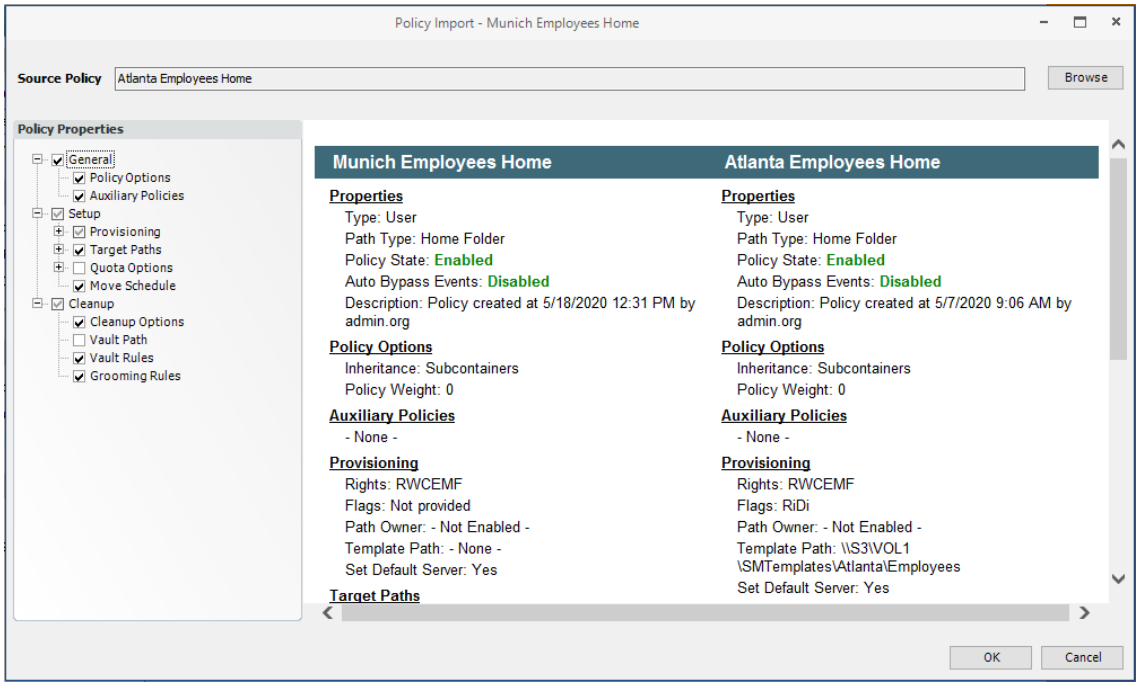
1. In the Admin Client, click the **Main** tab.
2. Click **Policy Management**.
3. While creating a new policy or editing an existing policy, click **Copy Policy Data** in the left pane of the Policy Editor dialog box.



4 Click the **Browse** button. In the Policy Selector dialog box, select the policy from which you want to copy policy settings, then click **OK**.

The dialog box is updated to list the name of the policy from which you are copying settings.

5 In the Policy Properties region, click the settings from the policy you want to copy.



6 When you are finished selecting the setting to copy, click **OK**.

5.7 Using a Policy to Manage Auxiliary Storage

Auxiliary storage allows administrators to create a policy that creates auxiliary storage folders when a new user is created. This auxiliary storage can even be invisible to the user for whom it was created.

For example, an organization's HR department might keep an individual folder for each user in the organization. With auxiliary user storage enabled, this folder can be created when the user joins the company and Storage Manager for eDirectory creates and provisions his or her home folder. The user never sees the auxiliary storage.

Additionally, the auxiliary storage can be as large as the policy specifies. This means that even though the user's home directory might have 500 MB, the auxiliary storage could be as small as the HR department needed it to be for storing HR-specific documents about the user. In fact, the policy can dictate that the auxiliary storage is provisioned with needed HR documents at the time the auxiliary storage is created.

Of course, you can configure auxiliary user storage so that a user can access it. For example, you might want to have a separate storage folder for application-specific files. It is important to remember that auxiliary storage is simply another home folder for a user. To provide access to this storage, you need to provide some sort of mapping for the user to get automated access to it.

There is no limit to the number of auxiliary folders that can be created. Auxiliary folders can be created in volumes that differ from the location of the user's home folder.

Storage Manager's life cycle management capabilities easily manage auxiliary storage to the specific needs of the organization. For example, if a user transfers from one city to another and the user home folder is moved to a new Organizational Unit object as a result, the policy can dictate what becomes of the auxiliary storage including moving it, moving it and adjusting the quota settings, leaving it where it currently is, etc. For more information on moving Auxiliary storage, see Section 5.7.4, “Establishing Auxiliary Purpose Mappings,” on page 47.

5.7.1 Creating an Auxiliary Storage Policy

1. In the Admin Client, click **Policy Management**.
2. From the **Manage** drop-down menu, select **New > Auxiliary**.
3. Specify a descriptive name in the **Name** field, such as “HR-AUX,” and click **OK**.

   The Policy Options page appears.
4. Proceed with “Setting Auxiliary Storage Policy Options” on page 44.

Setting Auxiliary Storage Policy Options

1. Leave the **Process Events for Associated Managed Storage** check box selected.
2. Proceed with “Enabling Auxiliary Storage Extended Options” on page 45.

Enabling Auxiliary Storage Extended Options

Auxiliary storage extended options help other tools identify the auxiliary storage policy through additional attributes.

1. In the left pane, click **Extended Options**.
2. Click the **Enable** check box.
3. In the **Tag** field, enter a descriptive string for the auxiliary storage.

   Micro Focus recommends that once you have made an entry in the **Tag** field, that you do not change it. If the value of the **Tag** field is changed after some users have already had their auxiliary storage provisioned via that policy, the new tag value does not automatically get propagated to those users. Only users who get storage provisioned *after* the change in the tag value will get the new tag value.
4. In the **Description** field, specify a description of the auxiliary storage policy.
5. Click **Apply** to save your settings.
6. Proceed with "Setting Auxiliary Storage Provisioning Options" on page 45.

Setting Auxiliary Storage Provisioning Options

Before setting the provisioning options, you need to decide whether the user should have rights to auxiliary storage.

Additionally, if you are going to provision auxiliary storage folders with a certain structure or with specific documents, you need to place them somewhere in the file system so you can use them as a template. For example, if the HR department wants the auxiliary storage folder to have an Annual Reviews folder and an Insurance Forms folder, you need to set these up in the file system before proceeding.

1. In the left pane, click **Provisioning Options**.
2. Do one of the following:
   - If you do not want the associated user to have access to the auxiliary storage folder, deselect all of the Default Rights check boxes.
   - If you want the associated user to have access to the auxiliary storage folder, select the appropriate rights from the Default Rights check boxes.
3. In the Template Folder region, click the **Browse** button, and then specify the template path in the Path Browser dialog box.
4. Click **Apply** to save your settings.

Setting Additional Auxiliary Storage Options

1. Select the additional options that you want to use in the Auxiliary Storage policy.

   Auxiliary Storage Target Paths: You need to specify the location where the auxiliary storage folders are to be located. For example, if these were HR Department folders, they would probably be located on a network volume specific to the HR Department.

   The fields presented on the Target Paths page are identical to those presented when you create a User Home Folder policy. For an explanation of the page along with procedures for setting target paths, see Section 5.4.4, "Setting Target Paths," on page 35.

   Auxiliary Storage Quota Options: You need to specify the quota for the auxiliary storage folder associated with a user. In many cases, such as the HR Department example, this folder can be much smaller that the home folder.

The fields presented on the Quota Options page are identical to those presented when you create a User Home Folder policy. For an explanation of the page, along with procedures for setting quota options, see Section 5.4.5, “Setting Quota Options,” on page 36.

Auxiliary Storage Move Schedule: The fields presented on the Move Schedule page are identical to those presented when you create a user home folder policy. For an explanation of the page, along with procedures for setting the move schedule, see Section 5.4.6, “Setting the Move Schedule,” on page 38.

Auxiliary Storage Cleanup Options: The fields presented on the Cleanup Options page are identical to those presented when you create a User Home Folder policy. For an explanation of the page, along with procedures for setting cleanup options, see Section 5.4.7, “Setting Cleanup Options,” on page 38.

Auxiliary Storage Vault Rules: The fields presented on the Vault Rules page are identical to those presented when you create a User Home Folder policy. For an explanation of the page, along with procedures for setting vault rules, see Section 5.4.8, “Setting Vault Rules,” on page 38.

Auxiliary Storage Grooming Rules: The fields presented on the Grooming Rules page are identical to those presented when you create a user home folder policy. For an explanation of the page, along with procedures for setting grooming rules, see Section 5.4.9, “Setting Grooming Rules,” on page 40.

2 Proceed with Section 5.7.2, “Linking a User Home Folder Policy to an Auxiliary Storage Policy,” on page 46.

5.7.2 Linking a User Home Folder Policy to an Auxiliary Storage Policy

This procedure connects the Auxiliary Storage policy with an existing User Home Folder policy. All new users that are added to a group or organizational unit associated with the linked user home folder policy will also have auxiliary storage created. To provide existing users with auxiliary storage, see Section 5.7.3, “Provisioning Auxiliary Storage for Existing Users,” on page 46.

1 In the Admin Client, click the **Main** tab.
2 Click **Policy Management**.
3 In the list of policies, double-click the policy you want to link to the auxiliary storage policy.
4 In the left pane of the Policy Editor, click **Auxiliary Policies**.
5 Click **Add**. In the Policy Selector dialog box, select the Auxiliary Storage policy, then click **OK**.
6 Click **OK** to exit the Policy Editor.

5.7.3 Provisioning Auxiliary Storage for Existing Users

This procedure lets Storage Manager for eDirectory manage an existing second user home folder by classifying the second home folder as an auxiliary storage folder and managing it through an auxiliary storage policy. In the process, Storage Manager for eDirectory corrects any potential problems.

1 In the Admin Client, click the **Main** tab.
2 Click **Policy Management**.
3 Select the auxiliary storage policy linked to the User Home Folder policy of the users for whom you want to create auxiliary storage.
4 In the **Actions** drop-down menu, select **Assign Auxiliary Attributes**.
5 Verify that the **Assign using value in policy is Auxiliary Attribute is not set** option is selected.

This option uses the defined auxiliary storage policy path and looks for a folder that matches the common name of all users defined within the policy. If a match is found, the Auxiliary Storage Attribute is set and the users are cataloged and managed by the Auxiliary Storage policy.

6 Verify that the **Run in Check Mode** check box is selected and click **Run**.

Run in Check Mode allows you to view the results of an action without actually making changes.

7 Click **Expand** to see the results.

Note that the Auxiliary Attribute is set for each folder that matches a User object.

8 Click **Collapse**.

9 Deselect **Run in Check Mode** and click **Run** to set the Auxiliary Attribute.

10 From the **Actions** drop-down menu, select **Apply Quota**.

11 Select **Set quota for all directories. Overwrite any existing quota assignments except where the existing quota is larger than the quota defined in the policy.**

12 Select **Run in Check Mode** and click **Run** to view the results.

13 Deselect **Run in Check Mode**, then click **Run** to put auxiliary storage into effect for existing users.

5.7.4 Establishing Auxiliary Purpose Mappings

Auxiliary purpose mappings are the means of moving a user's auxiliary storage when a user is moved in eDirectory. For example, if a user were moved from the Atlanta container to the Detroit container, and the two container's Auxiliary storage policies were part of the same Auxiliary purpose mapping, the user's Auxiliary storage would move to the Detroit Auxiliary storage location.

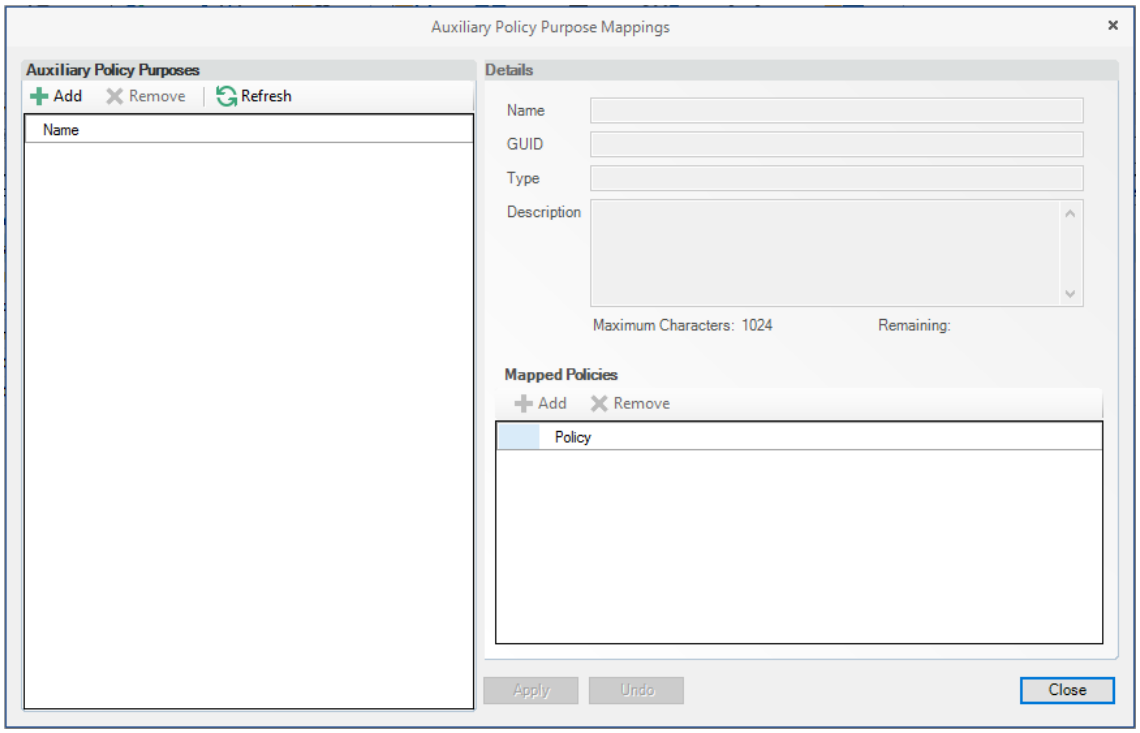
WARNING: If there is no established Auxiliary purpose mapping between the source and destination container, the user's auxiliary storage is deleted once the user is moved.

---

1 In the Admin Client, click the **Main** tab.

2 Click **Policy Management.**

3 From the **Manage** drop-down menu, select **Auxiliary Purpose Mappings**.



4 Click **Add**.

5 Give the new Auxiliary purpose mapping a descriptive name.

For example, “HR.”

6 Click **OK**.

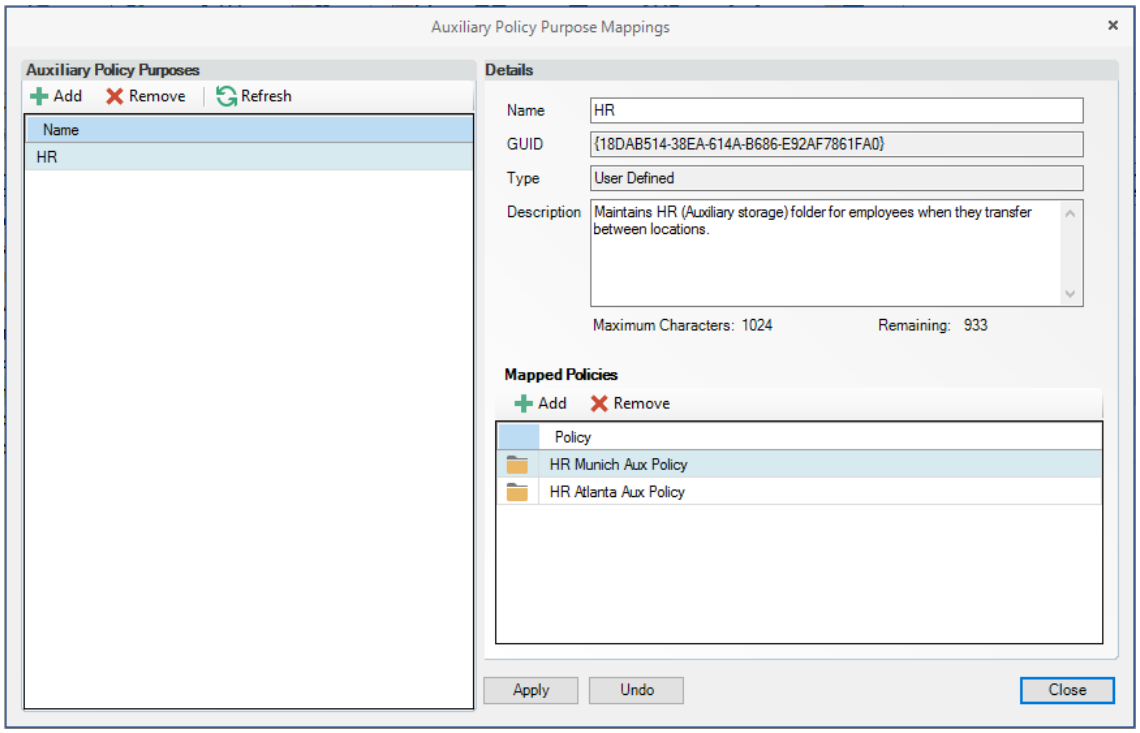
7 In the Mapped Policies region, click **Add**.

8 From the Policy Selector dialog box, hold down the Control key to select each of the Auxiliary storage policies you want associated with the Auxiliary purpose mapping.

Using the example above, you would select the Auxiliary storage policy for the Atlanta container, the Detroit container, and any others you want included.

9 Click **OK**.

10 In the **Description** field, specify the details of the Auxiliary storage purpose mapping.



11 Click **Apply**.

12 Click **Close**.

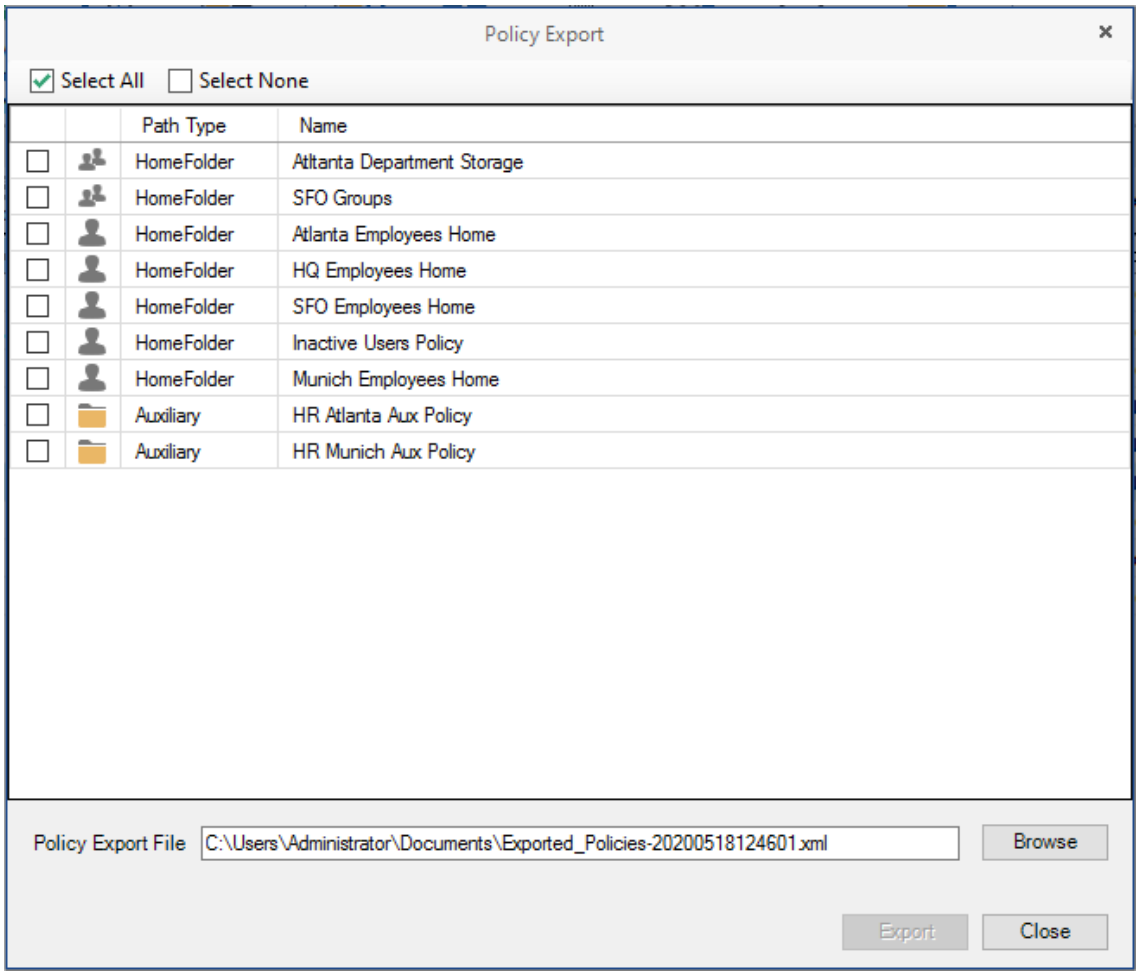
5.8 Exporting Policies

Storage Manager for eDirectory provides the ability to export policies so that they can be imported later. For example, many customers first evaluate Storage Manager for eDirectory in a lab environment and create a large number of policies in the process. You can export these policies and later import them into the production environment. All exported policies are saved in a single XML file.

1 In the Admin Client, click the **Main** tab.

2 Click **Policy Management**.

3 From the **Manage** drop-down menu, select **Export Policies**.



4 Select the check boxes of those policies you want to export

5 Accept the default export filename or indicate a new one in the **Policy Export File** field.

6 Accept the default path of the file or browse to select a new path.

7 Click **Export**.

8 After you are notified that the policies have been exported, click **Close**.

5.9 Importing Policies

Previously exported policies are imported by using the Import Policies feature.

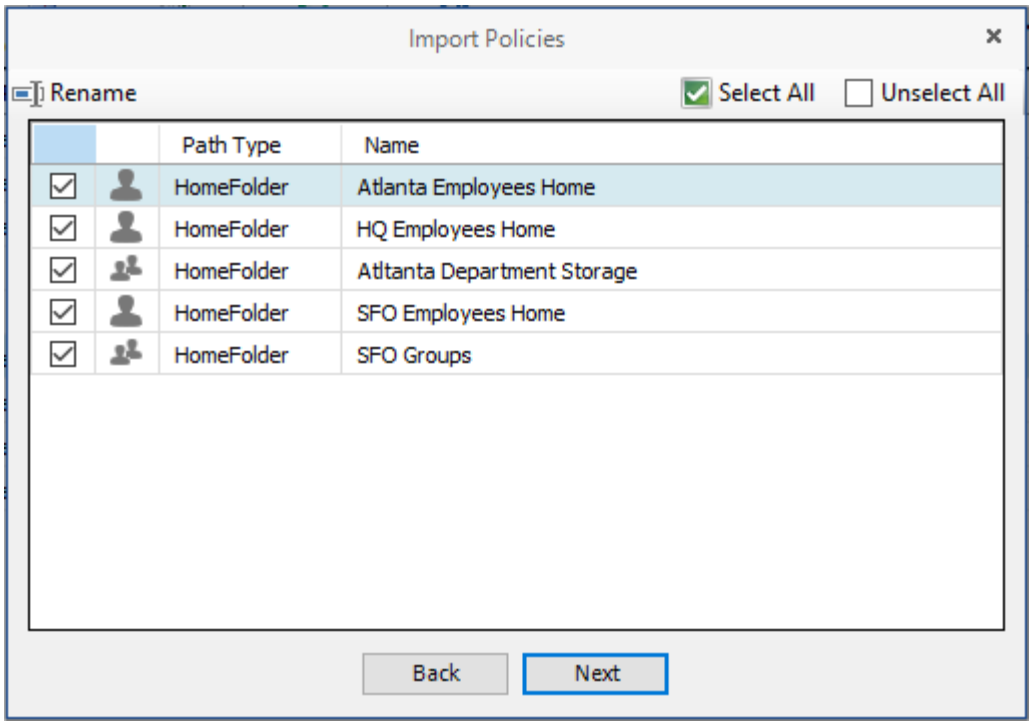
1 In the Admin Client, click the **Main** tab.

2 Click **Policy Management**.

3 From the **Manage** drop-down menu, select **Import Policies**.

4 Browse to select the saved export file.

5 Click **Next**.



6 Verify that the check box for each policy you want to import is selected.

7 Click **Next**.

A status page appears indicating what policies were imported and when the import process is complete.

8 Click **Close**.

6 Managing Existing Collaborative Storage

This section includes the procedures for using Storage Manager for eDirectory to manage the managed paths that are assigned to Group objects or containers in eDirectory.

In a Storage Manager for eDirectory environment, group-based or container-based storage is referred to as “collaborative storage,” because Storage Manager for eDirectory, through its collaborative policies, provides the means of creating storage folders where members can easily collaborate through a single project folder, or even through a structured project folder where all members have personal subfolders.

Similar to Chapter 4, “Managing Existing User Storage,” on page 17, this section provides the basic procedures for managing collaborative storage, which includes associating groups and containers with shared storage, and setting the target path, quota rules, and grooming rules.

This section does not provide procedures for establishing a structured project folder with personal subfolders, which are enabled through template creation and Dynamic Template Processing. For a comprehensive discussion on managing collaborative storage, including Dynamic Template Processing, see Chapter 7, “Managing Collaborative Storage,” on page 63.

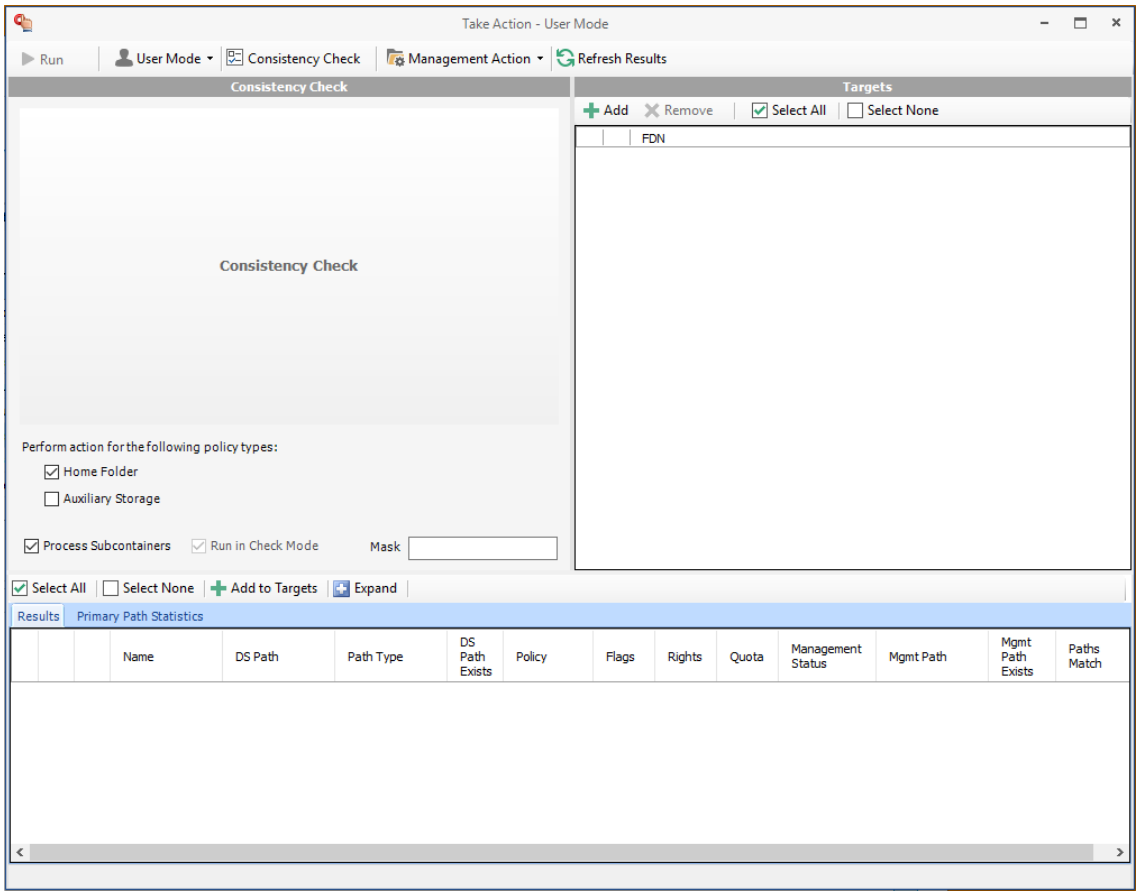
This process for managing existing storage and creating personal subfolders involves several tasks:

6.1 Assigning a Managed Path to Existing Group-based or Container-based Storage

A collaborative managed path attribute is created by Storage Manager for eDirectory when the eDirectory schema is extended. The attribute is used to associate a Group or container object with a managed path.

In this procedure, you assign a managed path to a Group or container object that has existing collaborative storage and then assign the storage path.

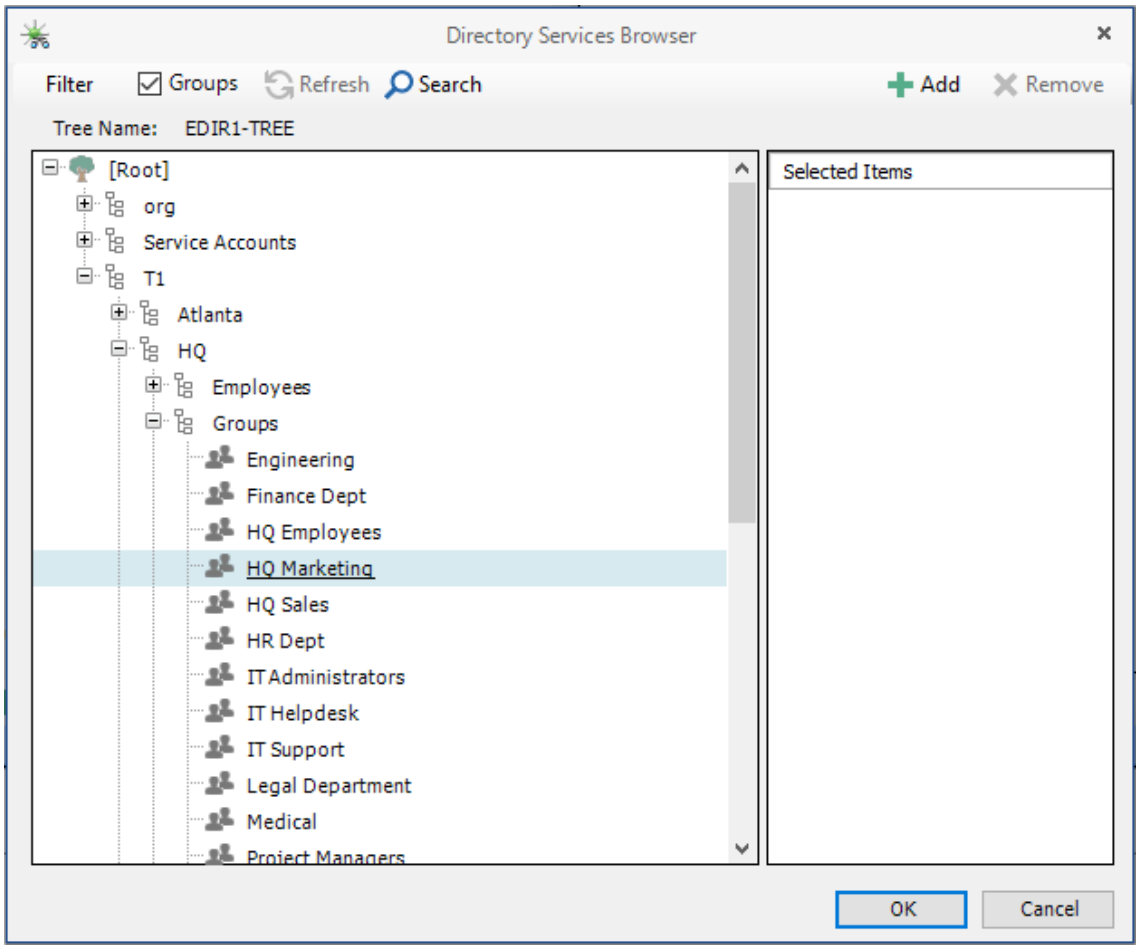
1. In the Admin Client, click the **Main** tab.
2. Click **Management Actions**.



3 Use the menu to replace **User Mode** with **Group Mode** or **Container Mode**.

4 In the Targets region, click **Add**.

5 Browse to locate and select the container or group you want to associate to a group storage area, then click **Add**.



6 Click **OK**.

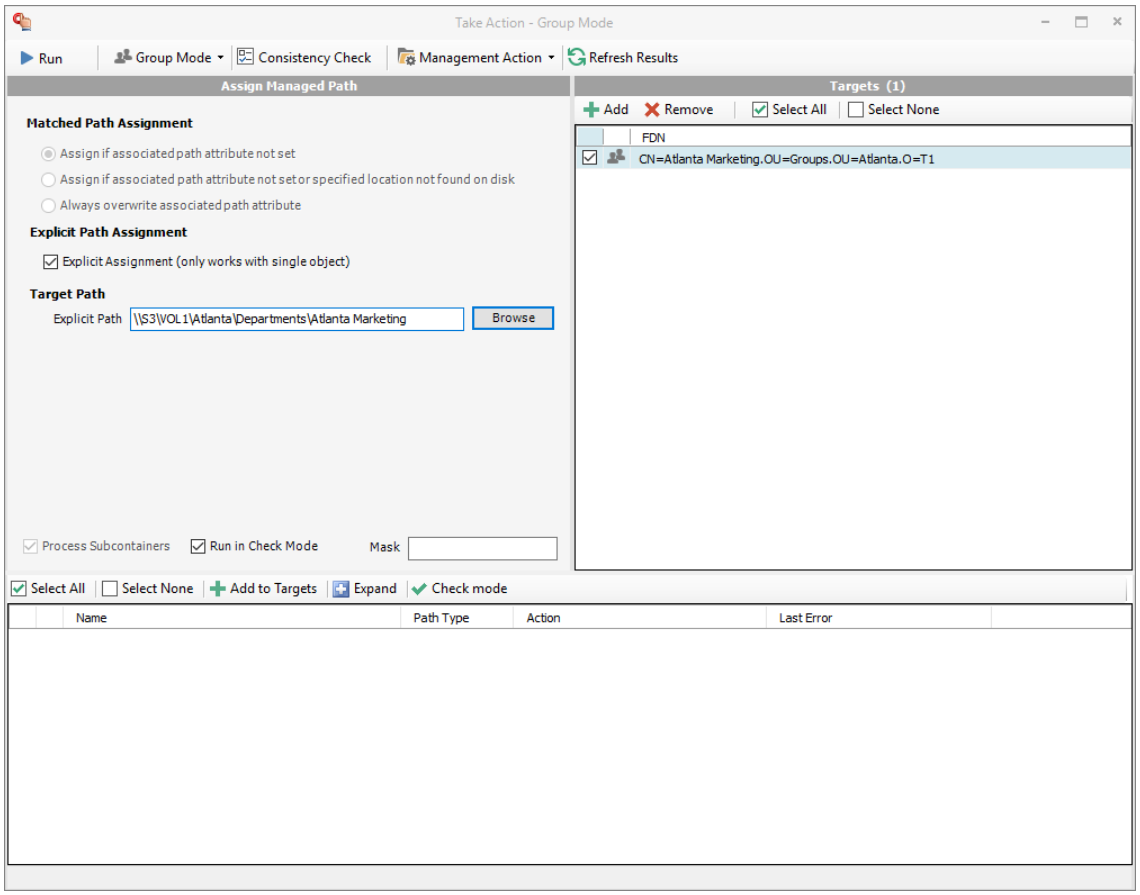
7 Click **Management Action** > **Assign Managed Path**.

8 Select the **Explicit Assignment** check box.

9 Click **Browse**, then locate and select the group storage folder you want to manage through Storage Manager.

10 Verify that the **Run in Check Mode** check box is selected.

11 Click **Run**.



12 Deselect **Run in Check Mode**, then click **Run**.

13 Observe in the bottom portion of the page that the managed path has been set.

14 Continue with Section 6.2, “Creating a Collaborative Storage Policy,” on page 56.

6.2 Creating a Collaborative Storage Policy

After you assign a managed path, the next step is to create a collaborative storage policy for the group or container you selected in Step 5 on page 54. In this procedure, the Collaborative Storage policy will apply to the Group object. However, a Collaborative Storage policy can apply to a Group's parent container thus making it applicable to all existing and new groups located therein.

1 In the Admin Client, click the **Main** tab.

2 Click **Policy Management**.

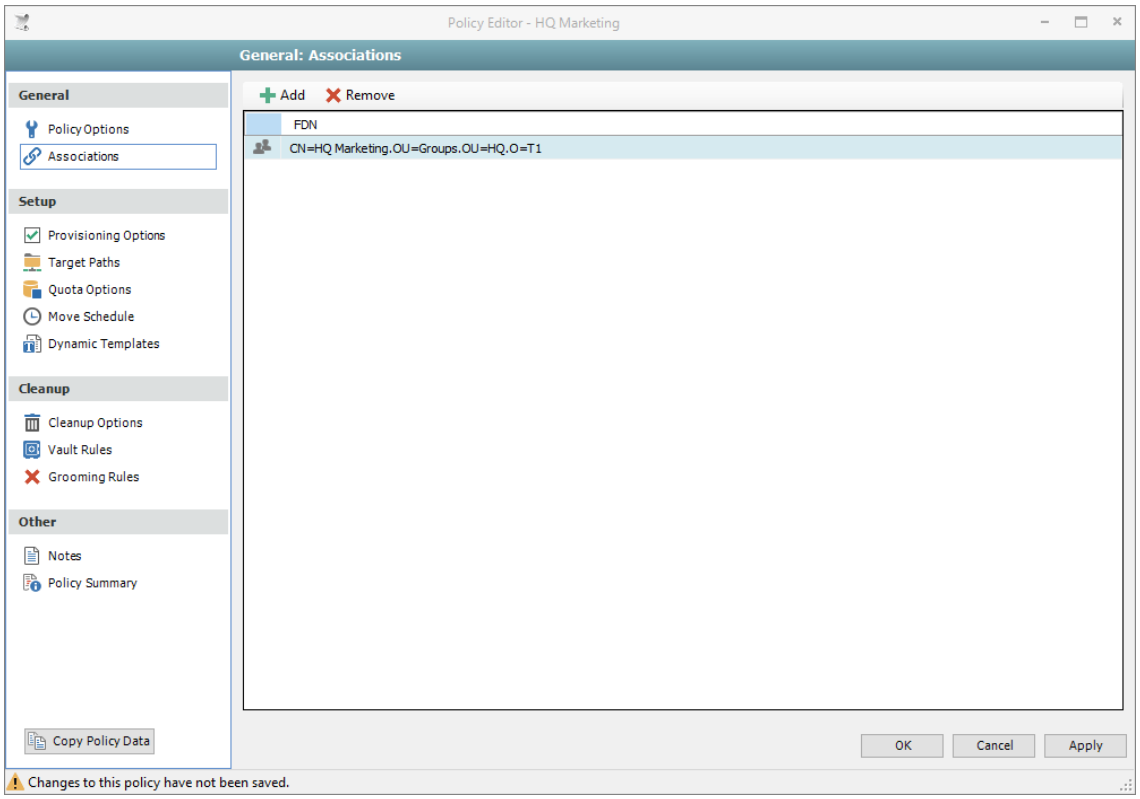
3 From the **Manage** drop-down menu, select **Create Policy** > **Create Group Policy**.

4 Specify a descriptive name for the new policy and click **OK**.

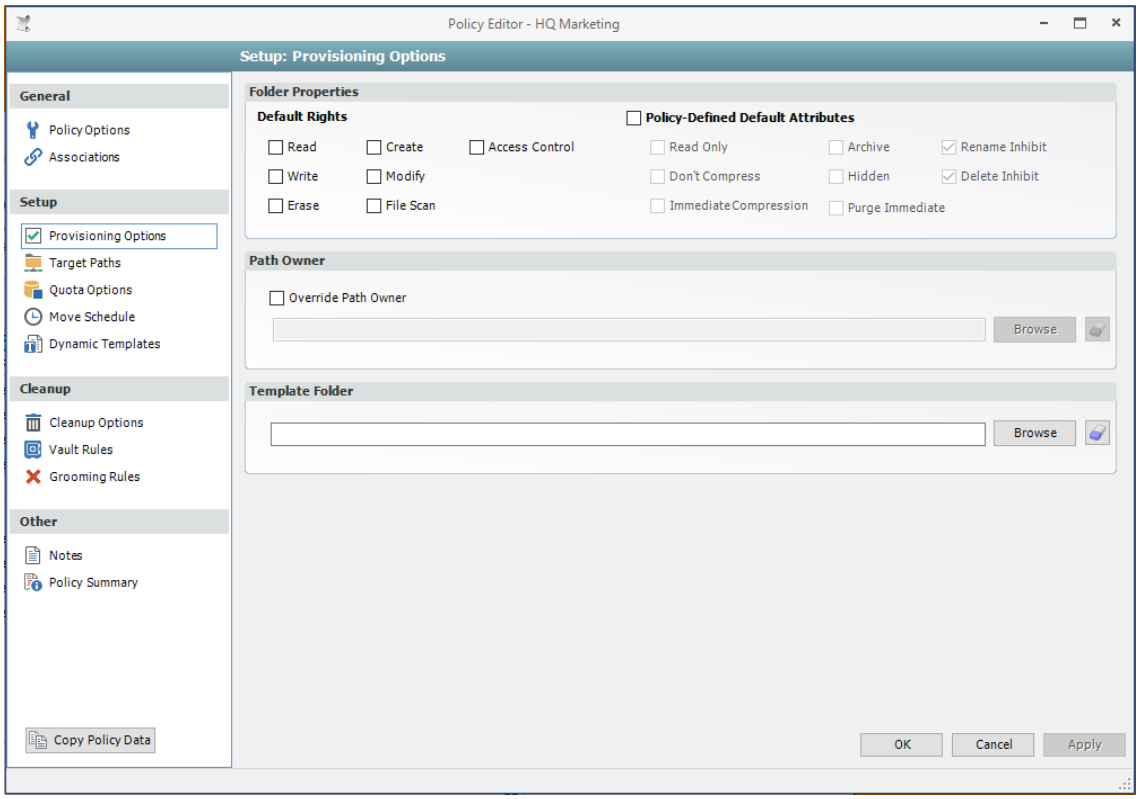
5 In the left panel, click **Associations**.

6 At the top of the right pane, click **Add** and browse to select the group or container that you selected in Step 5 on page 54.

7 Click **Add**, then click **OK**.



8 In the left panel, click **Provisioning Options**.



9 In the Default Rights region, specify the rights that you want the managed object to have to the collaborative managed path.

10 In the Policy-Defined Default Attributes region, select the **Policy-Defined Default Attributes** check box.

This enables the Rename Inhibit and Delete Inhibit attributes—which in most cases you should leave selected.

11 (Conditional) From the other attributes in this region, select any additional attributes you want to apply.

12 In the left panel, select **Target Paths**, then click **Add**.

13 Browse to and select the parent of the folder you selected in Step 9 on page 55.

14 Click **Add**, then click **OK**.

15 In the left panel, select **Quota Options**.

16 In the Initial Quota region, select the **Enabled** check box and specify the amount of initial quota you want assigned to the collaborative storage folder.

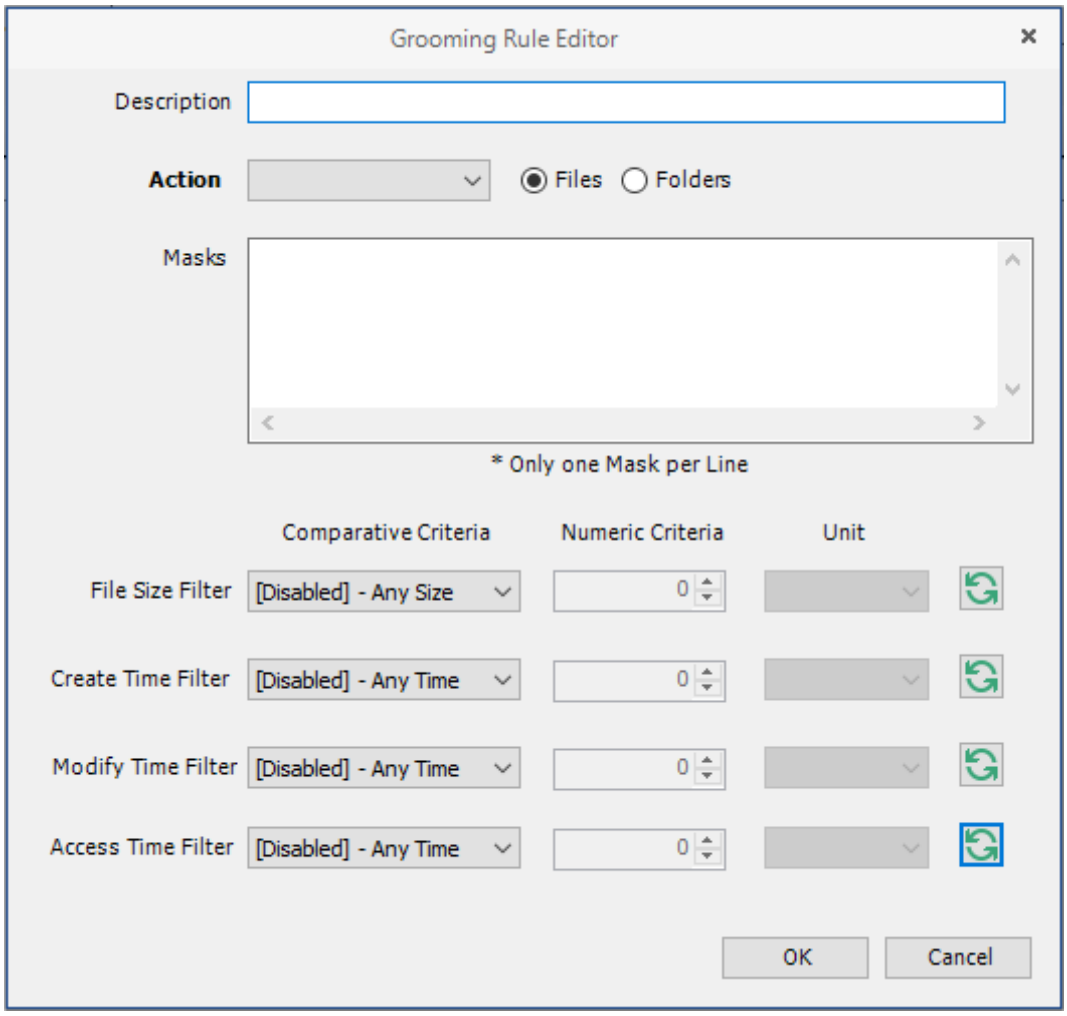
17 (Conditional) If you want to set specifications for a quota manager, select **Enable Quota Manager / Quota Preservation for this policy** and set quota maximums, increments, and managers.

18 In the left pane, select **Grooming Rules**.

19 Browse to select the folder where you want to vault the files that will be groomed.

If the folder does not exist, you can right-click to create the folder.

20 Click **OK** to save the vault path, then click **Add**.



21 In the Grooming Rule Editor dialog box, indicate the files that Storage Manager for eDirectory will groom from the collaborative storage pertaining to this policy.

For information on each of the fields in this dialog box, refer to Section 5.4.9, “Setting Grooming Rules,” on page 40.

22 Click **OK** to save the grooming rule.

23 Continue with Section 6.3, “Performing Management Actions,” on page 59.

6.3 Performing Management Actions

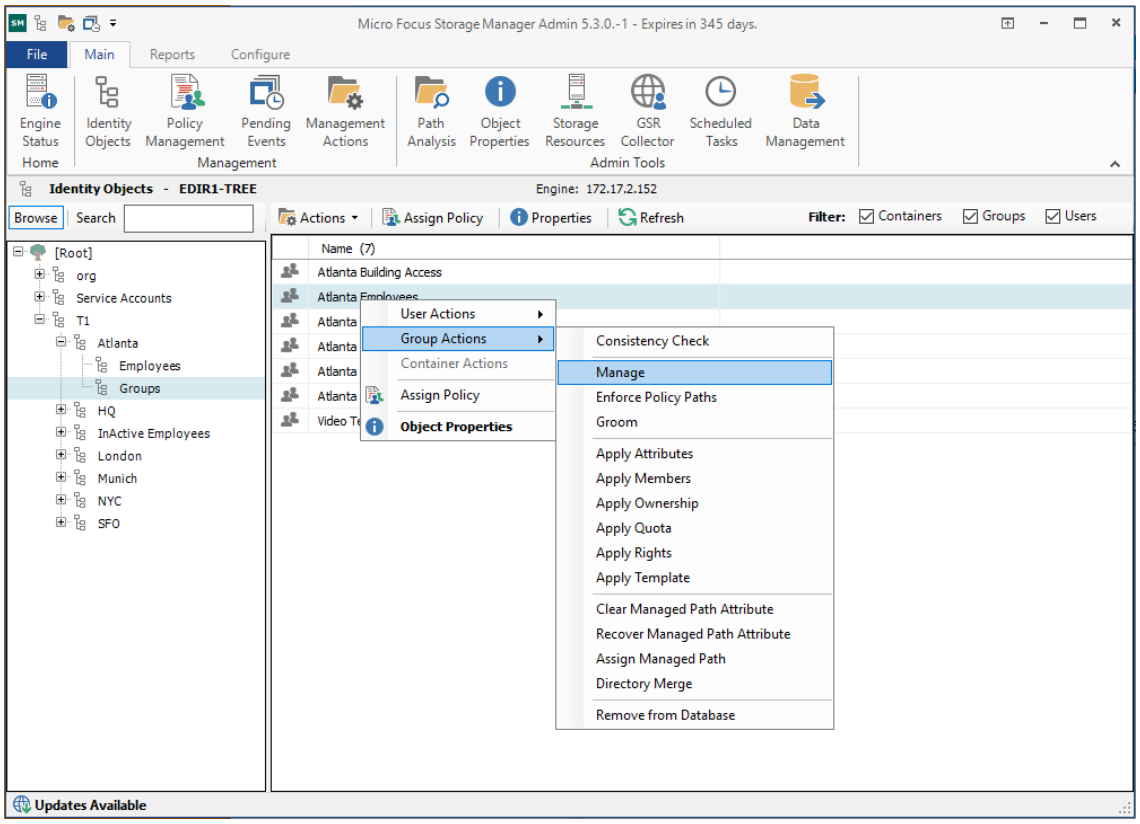
This procedure manages and creates collaborative storage for groups through Dynamic Template Processing. For more information on Dynamic Template Processing, see Chapter 7, “Managing Collaborative Storage,” on page 63.

1 In the Admin Client, click the **Main** tab.

2 Click **Identity Objects**.

3 Browse to and select the group or container that you specified in Step 5 on page 54.

4 Right-click the group or container and select **Group Actions** > **Manage**.



5 Verify that **Run in Check Mode** is selected, then click **Run**.

6 Verify that the following message appears in the lower panel of the window:

```
Catalog Existing Managed Path Location.
```

7 Deselect the **Run in Check Mode** check box, then click **Run**.

8 From the **Management Action** menu, select **Apply Attributes**.

9 Select the **Use policy definitions** check box.

10 Select the **Run in Check Mode** check box, then click **Run**.

11 Verify that the following message appears in the lower panel of the window:

```
Apply attributes will be applied for object.
```

12 Deselect the **Run in Check Mode** check box, then click **Run**.

13 From the **Management Action** menu, select **Apply Quota**.

14 Verify that the **Set quota for directories that do not have quota defined** option is selected.

15 Select the **Run in Check Mode** check box, then click **Run**.

16 Verify that the following message appears in the lower panel of the window:

```
Apply quota will be scheduled for object.
```

17 Deselect the **Run in Check Mode** check box, then click **Run**.

18 From the **Management Action** menu, select **Apply Rights**.

19 Select the **Run in Check Mode** check box, then click **Run**.

20 Verify that the following message appears in the lower panel of the window:

```
Apply rights will be scheduled for object.
```

21 Deselect the **Run in Check Mode** check box, then click **Run**.

22 From the **Management Action** menu, select **Groom**.

23 Select the **Run in Check Mode** check box, then click **Run**.

24 Verify that the following message appears in the lower panel of the window:

```
Groom scheduled for object.
```

25 Deselect the **Run in Check Mode** check box, then click **Run**.

6.4 Editing Collaborative Storage Policies

In this section, you created a basic collaborative storage policy designed to manage a non-structured storage folder. If you decide later that you want to edit the policy to adjust the quota, modify the target path, or even structure the group or container managed path with personal folders for each group or container member, you can easily do so.

For more comprehensive information on collaborative storage policies, including their ability to create structured group-based or container-based storage folders through Dynamic Template Processing, see Chapter 7, “Managing Collaborative Storage,” on page 63.

7 Managing Collaborative Storage

Collaborative storage is a shared storage area where a group of people in an organization can collaborate by accessing the same collaborative storage. For example, a cross-functional project team in an organization might need a collaborative storage area where all members could access and submit project files.

Storage Manager for eDirectory lets you easily create collaborative storage areas through collaborative storage policies that you can assign to Group objects or to an organizational unit (also known as a container). You can structure the collaborative storage in one of two ways:

- Creating a single project folder where all project members have access and have the same rights.
- Creating a project folder with a specified owner. The project folder has subfolders for each of the members of the group. This configuration is done through Dynamic Template Processing. For more information on Dynamic Template Processing, see Setting Group Policy Dynamic Template Processing.

Storage Manager works with eDirectory to ensure that only members of the Group object have access to collaborative storage. As new members are added to the group, they are automatically granted access to the collaborative storage. As members are removed, they no longer have access to the collaborative storage.

In cases where personal folders are issued through Dynamic Template Processing, when a user is removed from the group, the personal folder is renamed to *username*`#removed#`, leaving the file content in the storage location, but making the former group member unable to access the files within.

In this chapter, you will learn how to create collaborative storage policies. These include:

- Group-based collaborative policies
- Container-based collaborative policies

7.1 Creating Collaborative Storage Objects in eDirectory

For Storage Manager for eDirectory to manage collaborative storage, it must have the following Group objects located in eDirectory:

- -MEMBER-
- -OWNER-
- -GROUP-

These objects are needed for assigning rights to the collaborative storage template folders (that you will create later) for the group members, the manager, and the group itself.

IMPORTANT: You only need to create these objects in one container.

---

1. Using iManager or ConsoleOne, create a new Group object and name it -MEMBER-.
2. Repeat Step 1to create a -OWNER- Group object and a -GROUP- Group object.

   These three objects are used to automatically set rights for the collaborative storage. Make sure you name the objects exactly as indicated. The object names can either be uppercase or lowercase.

7.2 Understanding Collaborative Storage Template Folders

When you created user home folder policies in Chapter 5, “Managing User Home Folders,” on page 31, a field in the Provisioning Options page let you indicate the path to a template for provisioning folder structure and content in the home folder.

For collaborative storage management, you can also indicate a template path for provisioning and folder structure within the collaborative managed path. When Storage Manager for eDirectory creates a collaborative managed path for a group, it examines the policy to determine if a template has been defined and, if so, copies the contents of the template directory along with all attributes, trustee assignments, and quotas.

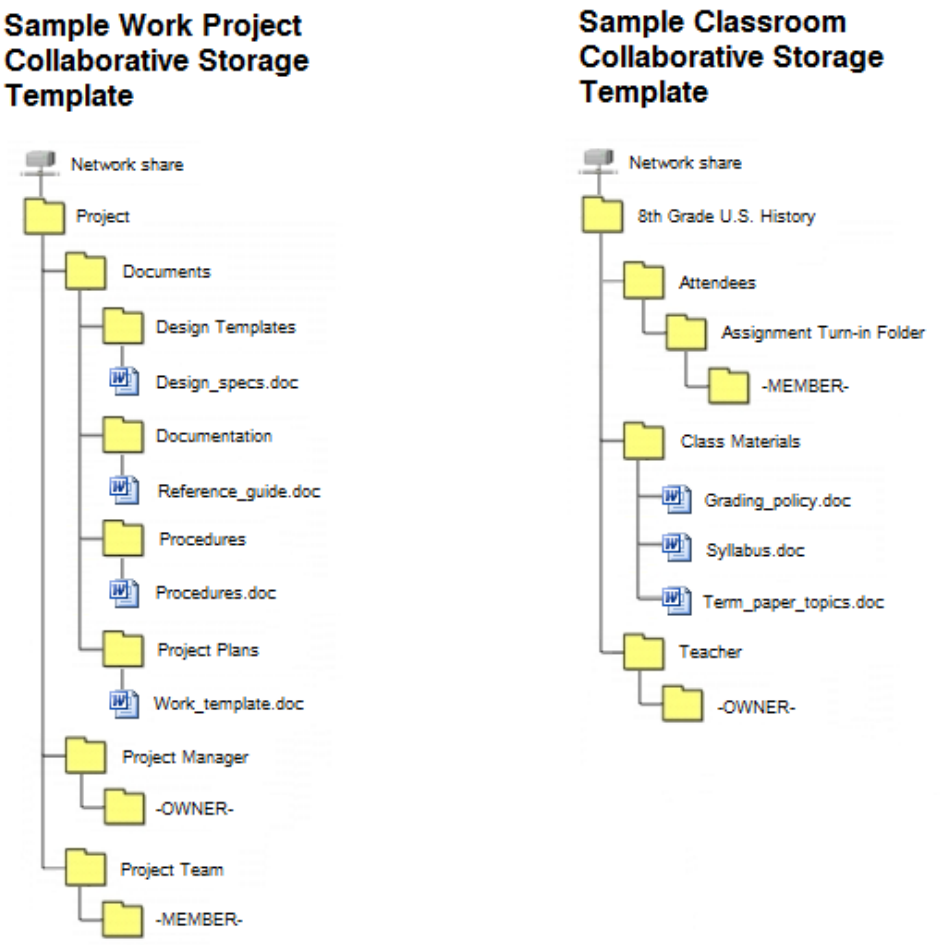
Unlike user home folders, collaborative disk space managed by Storage Manager for eDirectory is dynamic in that the member attributes of Group objects are monitored so that the addition and deletion of members can have a direct impact on the structure of the individual file system of a group as well as the rights given within the structure.

7.3 Determining How You Want to Structure Your Collaborative Storage

Your collaborative storage area should be structured so that it optimally serves the needs of your collaborative users. The collaborative storage needs of a cross-functional team at an architectural firm would be quite different from a junior high school history class.

Two sample designs are shown below.

Figure 7-1 *Sample Collaborative Storage Templates*



In the template structures above, both have -OWNER- and -MEMBER- folders. This means that there is a personal folder created for the designated manager of the group, along with personal folders created for each member of the group.

In order for those folders to be created and managed properly, the -OWNER- and -MEMBER- folders must not exist in the same folder.

In the project collaborative storage template, all members can see the contents of each member's folder—except for the designated manager's folder. In the classroom template, class members cannot see the contents of other classmate's folders because members have rights only to their personal folders.

7.4 Creating a Collaborative Storage Template

1. On a network volume, create a file structure for a group for which you will provide collaborative storage.
2. Place any documents you want available to the group in the appropriate folders.

7.5 Setting Up Security for a Collaborative Storage Template

Properly setting security and rights for collaborative storage in eDirectory can be potentially confusing. For this reason, we are providing an example of the correct way to set up security for a collaborative storage template.

The example provided is for a school class where the instructor is using a collaborative storage folder as the means of distributing assignments to students, as well as the means of retrieving assignments that the students turn in. The students cannot see the personal folders of the other students.

The file structure above is a common structure that can be used as a template for collaborative storage in an academic setting. By establishing the correct permissions, the course instructor can be established as the owner with full control of the collaborative storage area. Students can be provided with personal folders for retrieving and turning in assignments.

The diagram below shows the security permissions that must be established.

Figure 7-2 *Common Academic Setting Collaborative Storage Template Structure*

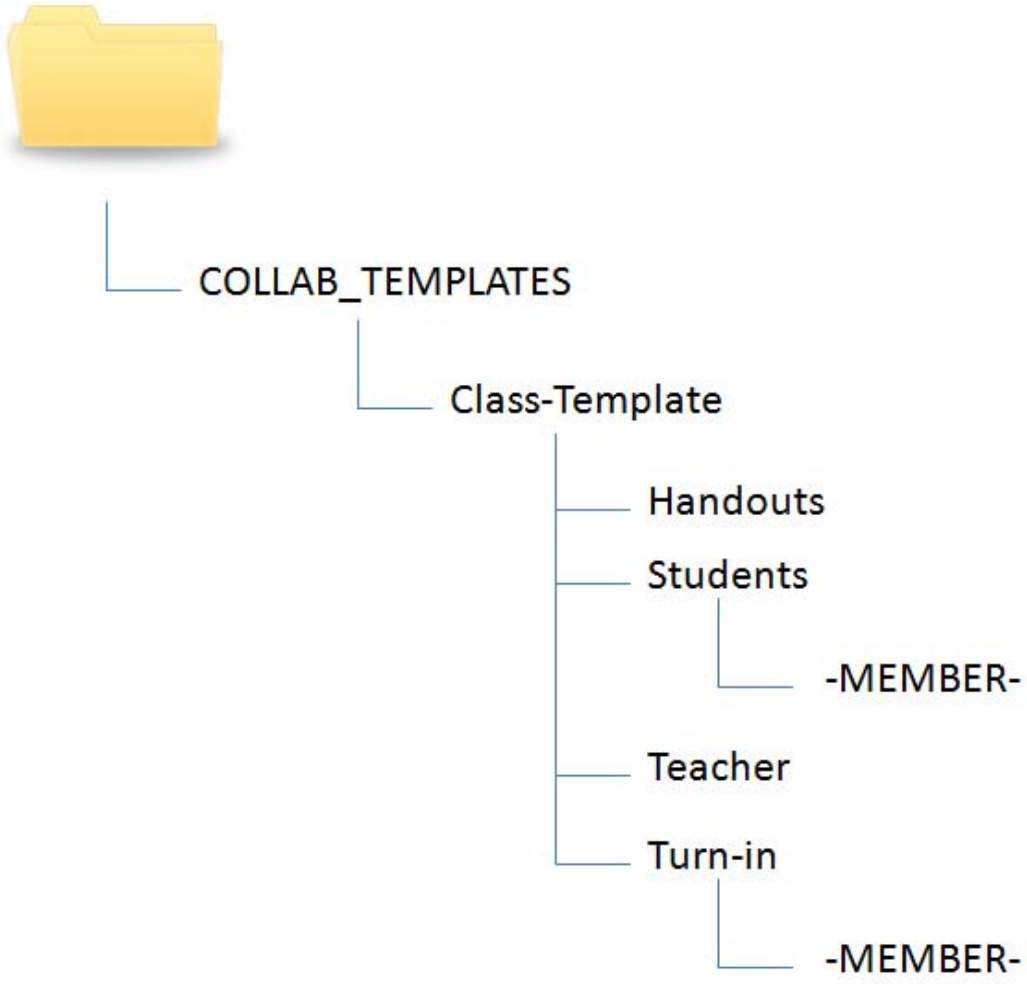
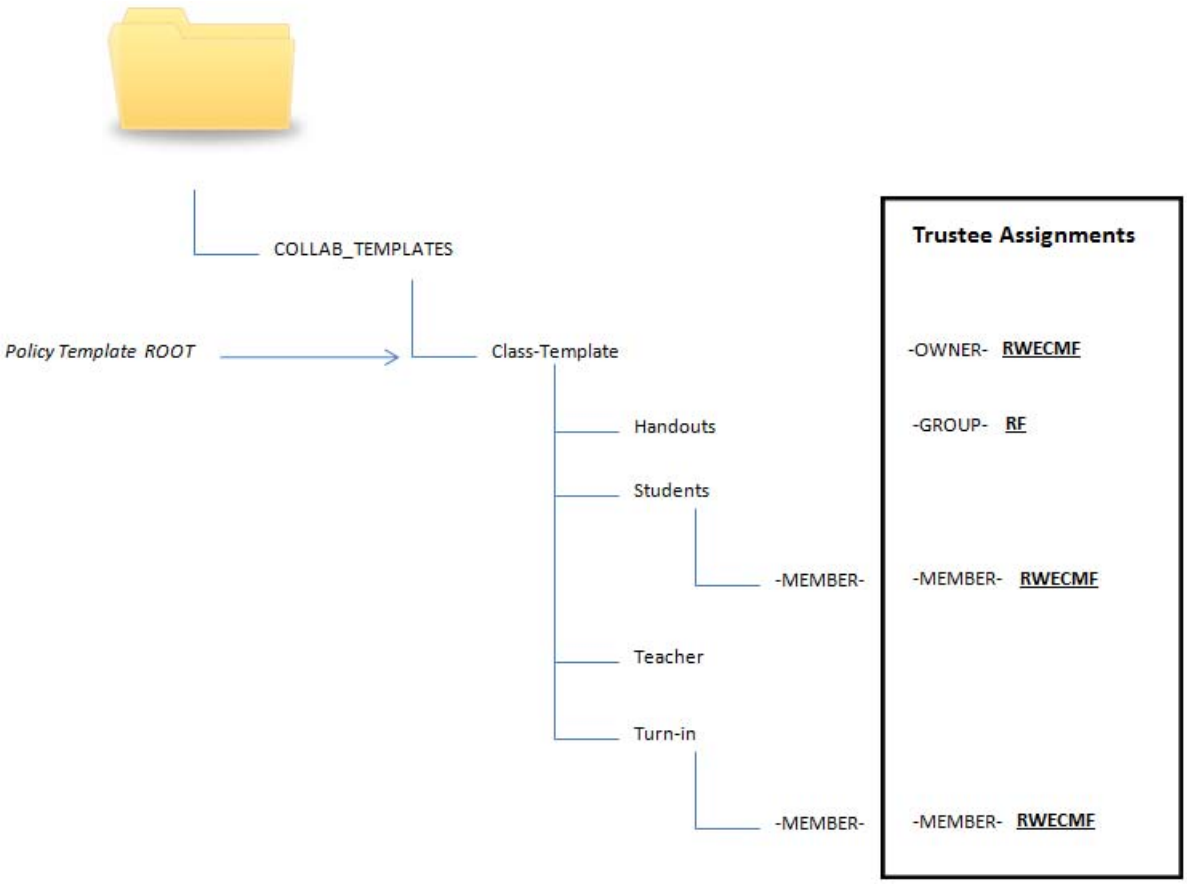


Figure 7-3 *Security Permissions for Each Folder in the Sample Template*



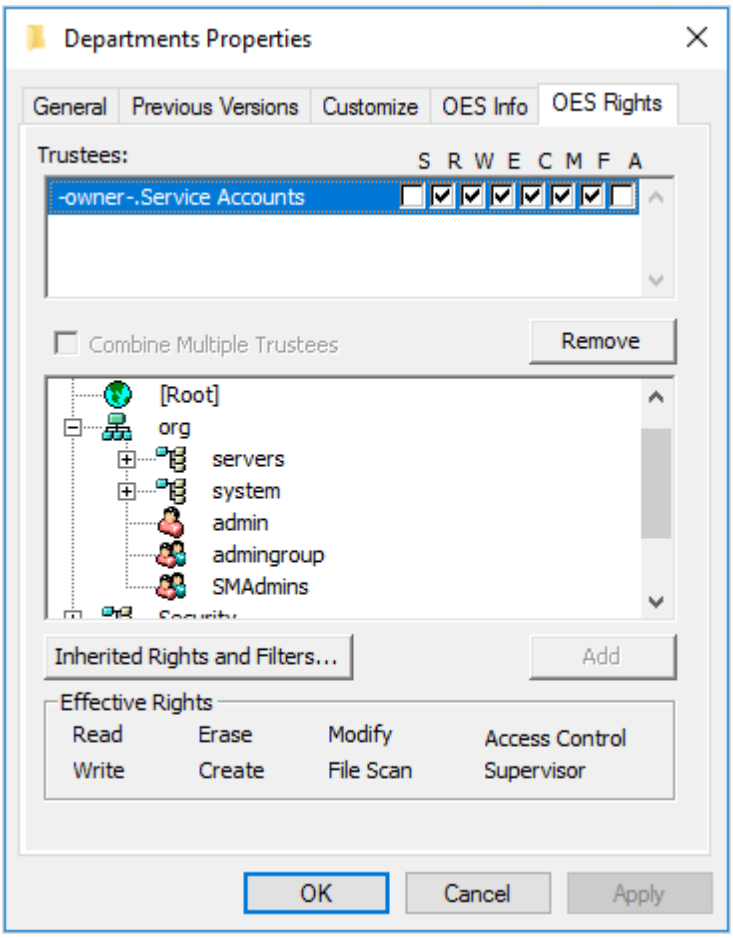
The diagram above shows the trustee assignments that must be established for each of the folders in the template structure. For example, the -OWNER- object must be given RWECMF rights to the Class-Template folder.

7.5.1 Establishing Trustee Rights

If you have the Client for OES installed, you can establish the trustee rights specified for each of the folders in Figure 7-3 on page 67 through Windows Explorer.

1. Log in through the Client for OES.
2. Launch Windows Explorer.
3. Right-click the Class Template folder and select **Trustee Rights**.

   A dialog box appears.
4. In the dialog box, browse to the -OWNER- object and grant him trustee RWECMF rights.



5 Click **OK**.

6 Repeat Step 2 through Step 5 to establish the remaining trustees and rights as specified in Figure 7-3 on page 67.

7.6 Understanding Collaborative Storage Policies

Before setting up collaborative storage policies, you need to understand the two types of collaborative storage policies and the differences between the two.

- A Group Collaborative Storage policy creates storage for a group when a Group object is created in an organizational unit where the policy is associated. For example, if a cross-functional team named HEALTHFAIR2014 is created in an organizational unit associated with the Group Collaborative Storage policy, the collaborative storage area is created when the group is created.
- A Container Collaborative Storage policy grants access to collaborative storage when a new User object is added to an organizational unit where the policy is associated. For example, if user BSMITH is added to an organizational unit that had an associated Container policy, BSMITH is granted access to the collaborative storage area. Furthermore, if the template associated with the policy is structured with a -MEMBER- Group object, the user is given a personal storage area within the collaborative storage area.

7.7 Creating a Group Collaborative Storage Policy

1. Launch the Admin Client.
2. In the **Main** menu, click **Policy Management**.
3. From the **Manage** drop-down menu, select **Create Policy > Create Group Policy**.
4. Specify a name in the **Name** field.

   The Policy Options page appears.
5. Continue with Section 7.7.1, “Setting Group Policy Options,” on page 69.

7.7.1 Setting Group Policy Options

Settings within Policy Options let you indicate how the policy is applied, set policy inheritance, and write an expanded policy description.

NOTE: Group policies in Storage Manager for eDirectory are completely independent of Microsoft Group policies.

---

1. Leave the **Process Events for Associated Managed Storage** check box selected.

   This indicates that you want the settings in this policy to be applied to all groups within the domain or organizational unit where this policy is assigned. Deselecting this check box indicates that you want to create a Blocking policy that can be applied to a specific group. For more information on blocking policies, see Section 4.6, “Creating a Blocking Policy,” on page 21.
2. Do one of the following:
   - If you are assigning this policy to a container rather than a group, and you want the settings to apply to subcontainers, leave the **Policy applies to subcontainers** check box selected.
   - If you are assigning this policy to a container, and you do not want the settings to apply to subcontainers, deselect the **Policy applies to subcontainers** check box.
3. In the Description region, use the text field to specify a description of the policy you are creating.
4. Click **OK** to save your settings.
5. Proceed with Section 7.7.2, “Setting Group Policy Associations,” on page 69.

7.7.2 Setting Group Policy Associations

The Associations page is where you assign the collaborative policy you are creating to a domain, organizational unit, or Group object.

1. In the left pane, click **Associations**.
2. Click **Add** to bring up the Object Browser.
3. Browse through the directory structure and select the organizational unit or Group object you want to associate the policy to.
4. Drag the object to the Selected Items pane and click **OK**.

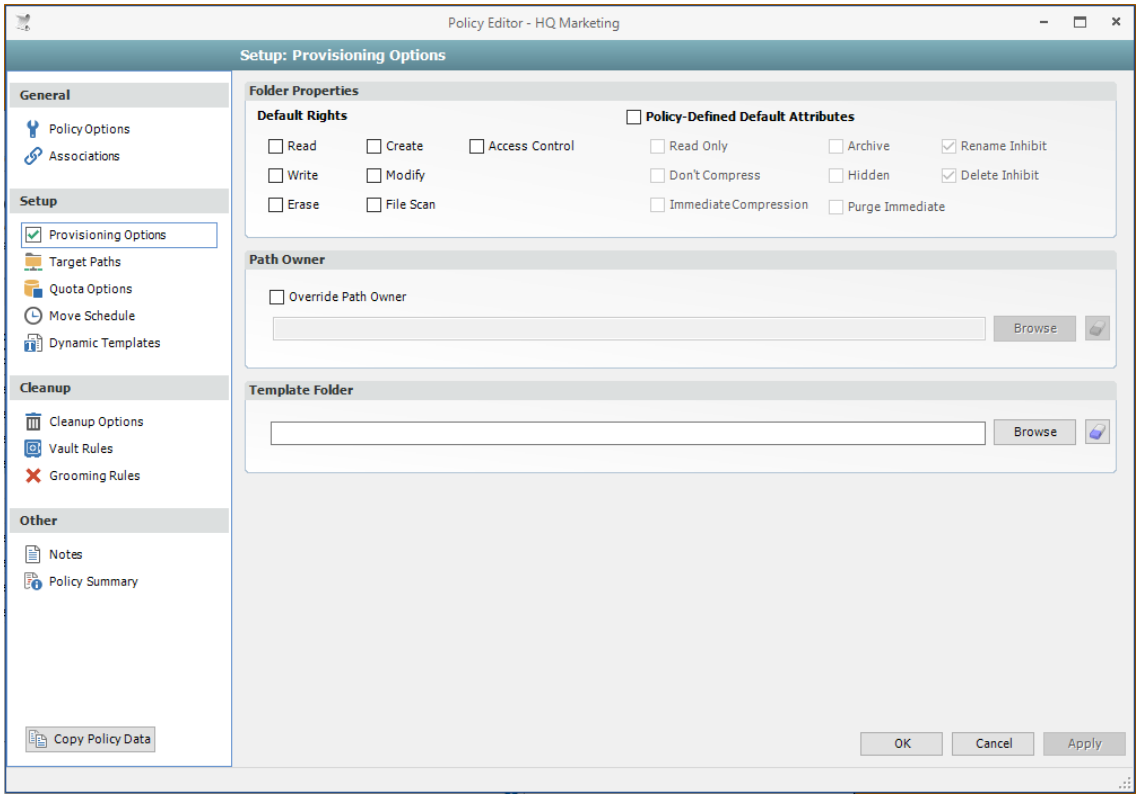
   The Object Browser is closed and the object is displayed in fully qualified name format in the right pane of the window. For example, `CN=HQ Marketing.OU=Groups,OU=HQ.O=T1`.
5. Click **OK** to close the Object Browser.
6. Click **Apply** to save your settings.
7. Proceed with Section 7.7.3, “Setting Group Policy Provisioning Options,” on page 70.

7.7.3 Setting Group Policy Provisioning Options

The Provisioning Options page is where you indicate collaborative storage rights, the location of a template for provisioning the collaborative storage folder structure and content in a managed path when it is created, and more.

1 In the left pane, click **Provisioning Options**.

The following page appears:



2 In the Folder Properties region, deselect all rights.

If you chose to create a collaborative storage temple, the rights will be applied from the template that you created in Section 7.4, “Creating a Collaborative Storage Template,” on page 65.

3 (Conditional) If you want to override the path owner, select the **Override Path Owner** check box.

4 In the field below the **Override Path Owner** check box, browse to indicate a path owner (that is, the owner of the group’s managed path).

5 In the Template Folder region, click the **Browse** button and locate the folder structure that you created in Section 7.4, “Creating a Collaborative Storage Template,” on page 65.

6 Select the topmost folder in the folder structure and click **OK**.

For example, if you had a structure similar to the Sample Classroom Collaborative Storage Template in Figure 7-1 on page 65, you would select “8th Grade U.S. History.”

7 Click **Apply** to save your settings.

8 Proceed with Section 7.7.4, “Setting Group Policy Target Paths,” on page 71.

7.7.4 Setting Group Policy Target Paths

The Target Paths page is where you set the paths to where the collaborative storage area for this policy will be hosted.

1. In the left pane, click **Target Paths**.
2. In the Target Placement region, fill in the following fields:

   Random: Distributes storage randomly among the number of target paths.

   Actual Free Space: Distributes the creation of collaborative storage folders according to volumes with the largest amount of absolute free space. For example, if you have two target paths listed, target path 1 has 15 GB of free space, and target path 2 has 10 GB, the collaborative storage folders are created using target path 1.

   Percentage Free Space: Distributes the creation of collaborative storage folders to volumes with the largest percentage of free space. For example, if you have two target paths listed and target path 1 is to a 10 TB drive that has 30 percent free space, and target path 2 is to a 500 GB drive with 40 percent free space, the collaborative storage folders are created using target path 2, even though target path 1 has more absolute available disk space. You should be cautious when using this option with target paths to volumes of different sizes.

   Leveling Algorithm: Use this option to structure the home folders so that they are categorized by the first or last letter of a username through a subordinate folder. For example, if you choose **First Letter**, and the **Leveling Length** field is set to 1, a user named BSMITH has a home folder located in a path such as `\\S2\HOME\B\BSMITH`.

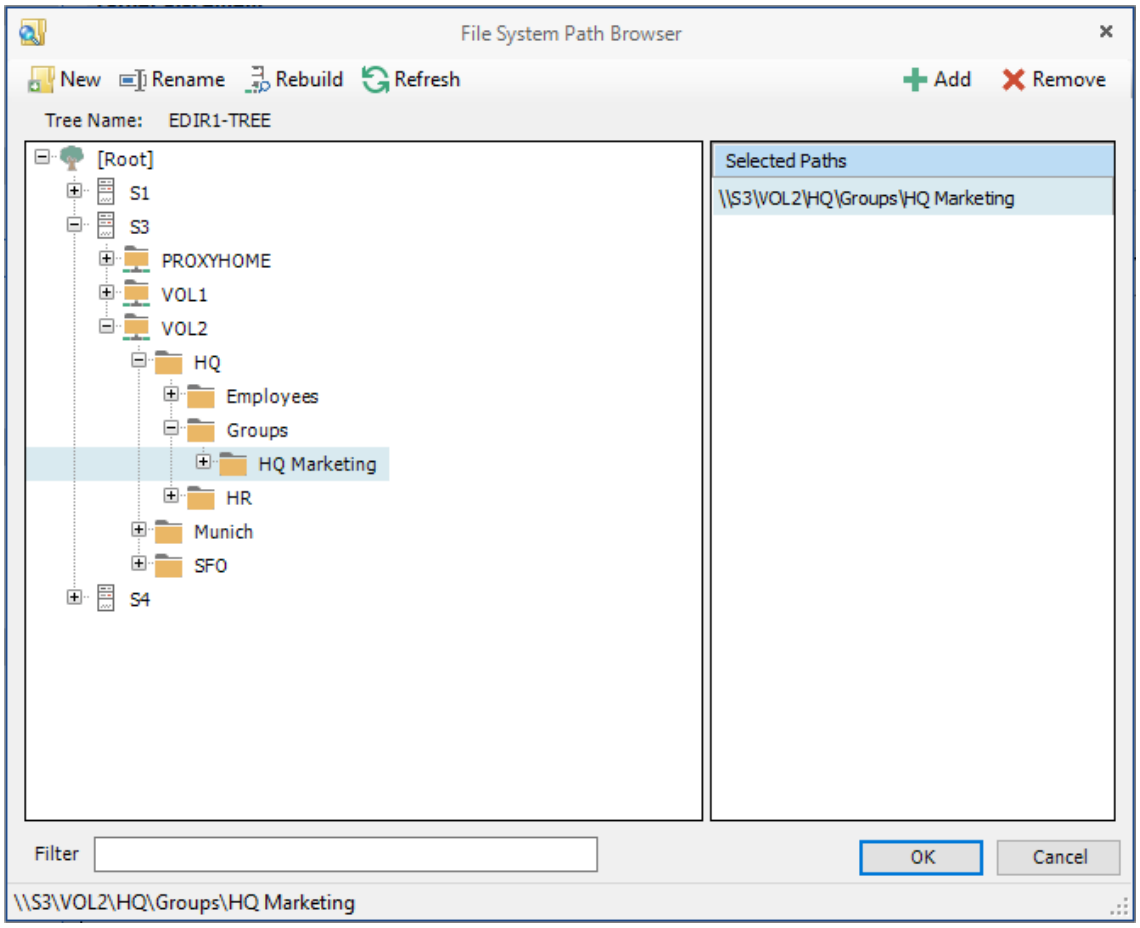
   If you choose **Last Letter**, and the **Leveling Length** field is set to 1, the same user has a home folder located in a path such as `\\S2\HOME\H\BSMITH`.

   The **Last Letter** means the last character of the attribute Storage Manager for eDirectory uses to create storage.

   The **Leveling Length** field allows you to enter up to 4 characters. This makes it so that you can organize home folders by year. For example, if your **Leveling Algorithm** setting is **Last Letter**, and the **Leveling Length** setting is 4, a user named BMITH2020 has a home folder located in a path such as `\\S3\HOME\2020\BSMITH2020.`

   Maximum Unreachable Paths: If you have a substantial number of target paths listed on this page, this field lets you indicate the number of target paths Storage Manager for eDirectory accesses to attempt to create a home folder before it suspends the attempt.

   For example, suppose you have 100 target paths and you're using Random Distribution and the **Maximum Unreachable Paths** setting is 20. Storage Manager for eDirectory will try 20 of those 100 paths before the event will become a pending event. A path can be unreachable for any error condition. For example: the server is down or the share is not available.
3. For each target path that you want to establish, click **Add** to access the Path Browser.
4. Browse to the location of the target path you want and click Add to add the target path to the Selected Paths pane.



5 Click **OK** to save the path.

6 Click **Apply** to save your settings.

7 Proceed to Section 7.7.5, “Setting Group Policy Quota Options,” on page 72.

7.7.5 Setting Group Policy Quota Options

This page lets you establish storage quota for the collaborative storage folder. Until quota management is established, a collaborative storage area has unlimited storage. Quota management for collaborative storage applies to:

- The quota for the entire storage folder
- Quotas for personal folders in the collaborative storage folder

---

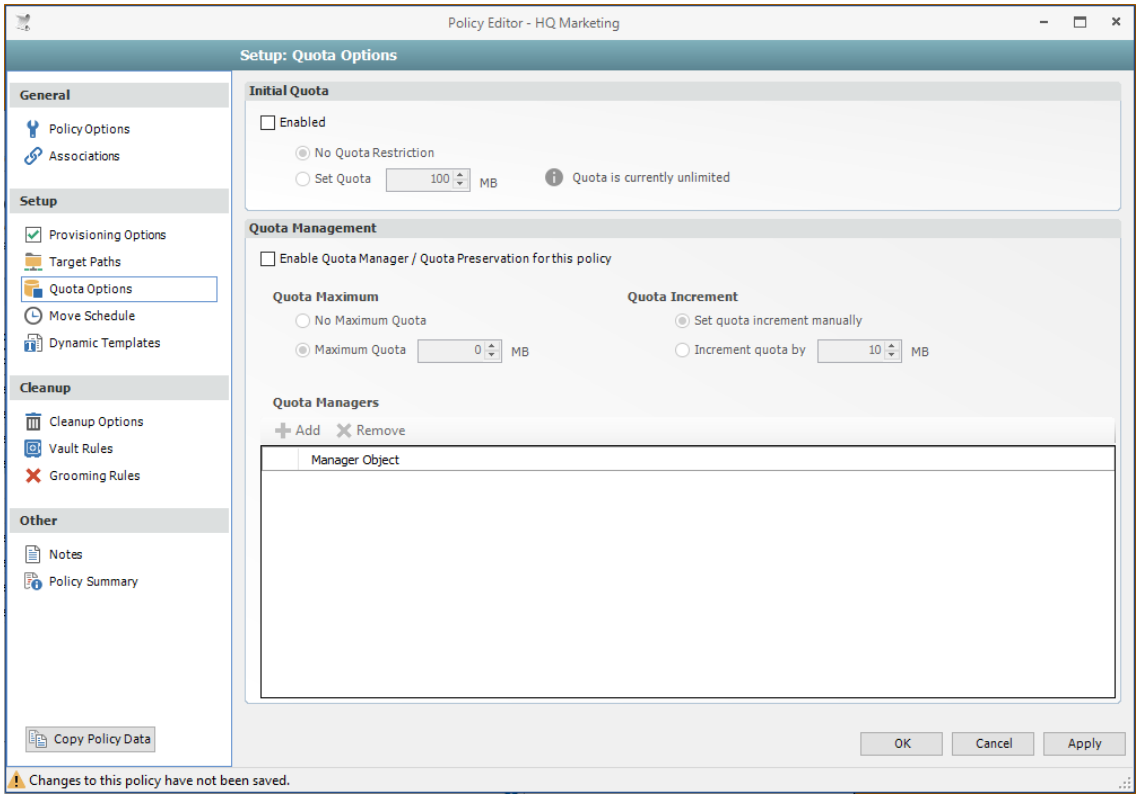
NOTE: In order for the quota to be managed on a personal folder, you must also manage the quota on the -OWNER- or -MEMBER- folder. You can set this in the template through the properties of each folder.

The Quota Options page is also where you establish quota management settings for quota managers. A quota manager is a specified user—for example, a help desk administrator or technical support rep, who is granted the ability to increase quotas without having rights to the file system.

Quota management actions are performed through Quota Manager, which is a separate Web browser-based management interface. For more information on Quota Manager, see Chapter 8, “Using Quota Manager,” on page 81.

1 In the left pane, click **Quota Options**.

The following page appears:



2 Select the **Enabled** check box to enable quota management.

3 In the **MB** field, specify the initial storage quota for the collaborative storage folders.

4 Set up quota managers for this policy by filling in the following fields:

Enable Quota Manager / Quota Preservation for this Policy: Select this check box to enable the Quota Management region of the page.

Quota Maximum: Indicate whether the users managed by this policy will have a maximum quota setting. If so, indicate the maximum quota.

Quota Increment: Indicate whether quota managers will set quotas manually or in set increments. If you select manual increments, the quota manager can increase the quota in any increment until it meets the maximum quota setting. If you select set increments, the quota manager can only increase the quota by the increment setting.

Quota Managers: Click **Add** and use the Object Browser to browse to and select a user you want to be a quota manager, then drag the User object to the right pane. Repeat this for each user you want to be a quota manager.

5 Click **Apply** to save your settings.

6 Proceed with Section 7.7.6, “Setting the Group Policy Move Schedule,” on page 74.

7.7.6 Setting the Group Policy Move Schedule

This page lets you use a grid to specify when collaborative storage data can be moved during data movement operations.

By default, all days and times are available for data movement. You might decide that data movement during regular business hours creates unacceptable network performance, and choose to move data after regular business hours.

NOTE: The collaborative storage folder will not move if there are any open files. Until the folder can be moved, the Move event will be listed as a pending event.

---

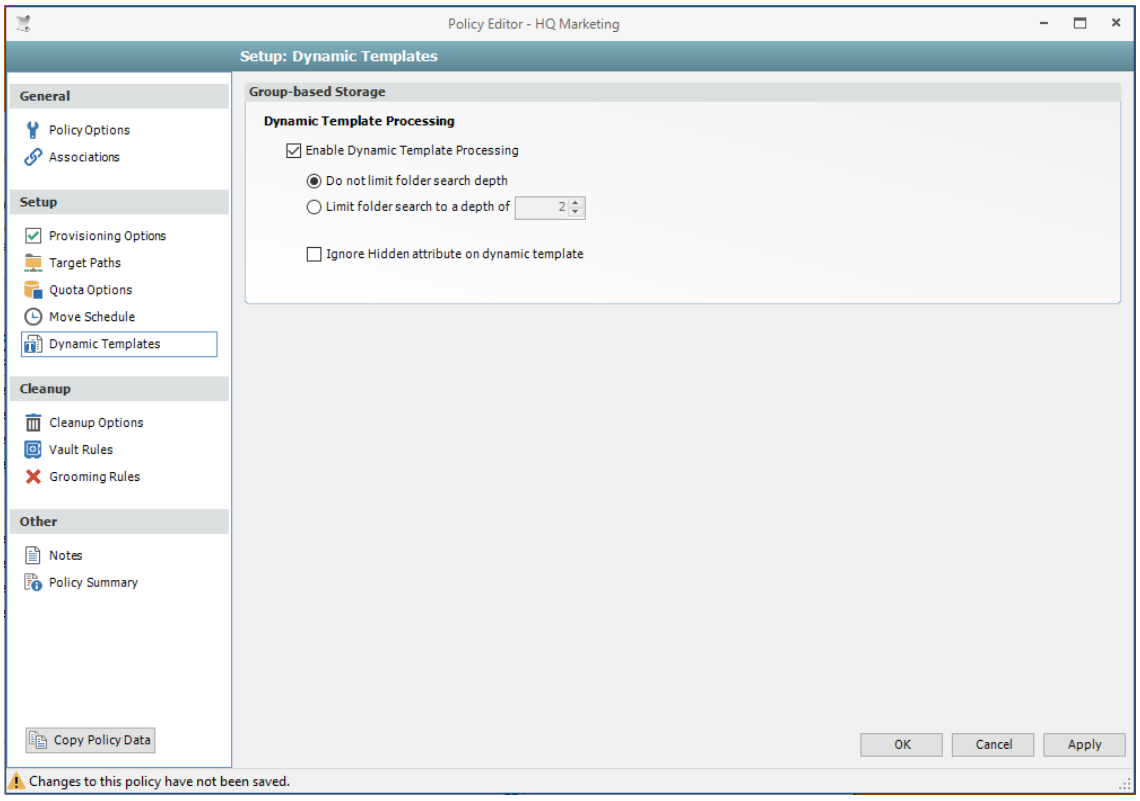
1. In the left pane, click **Move Schedule**.
2. In the Data Move Schedule grid, click the squares for the day and hour you want to disable for data movement.
3. Click **Apply** to save your settings.
4. Proceed with Section 7.7.7, “Setting Group Policy Dynamic Template Processing,” on page 74.

7.7.7 Setting Group Policy Dynamic Template Processing

Dynamic Template Processing is the term used in Storage Manager for eDirectory for creating personal folders in a collaborative storage folder. If Dynamic Template Processing is enabled, creating a -MEMBER- Group object in the collaborative storage file structure automates the creation of a user’s personal folder when he or she is added to the group.

1. In the left pane, click **Dynamic Templates**.

   The following screen appears:



2 Do one of the following:

- If the folder structure in your collaborative storage template includes a `-MEMBER-` folder, Storage Manager for eDirectory can create personal folders within the collaborative storage folder. Leave the **Enable Dynamic Template Processing** check box selected and proceed with Step 3.
- If your collaborative storage template does not include a -MEMBER- folder, Storage Manager for eDirectory does not create personal folders within the collaborative storage folder. Deselect the **Enable Dynamic Template Processing** check box and proceed with Section 7.7.8, “Setting Group Policy Cleanup Options,” on page 75.

3 Choose one of the following options:

- **Do not limit folder search depth:** The Engine searches through the collaborative storage folder looking for -GROUP-, -OWNER-, and -MEMBER- folders. Depending on the number of folders in the collaborative storage folder, this can take significant time. It is therefore best to not select this option.
- **Limit folder search to a depth of:** If you know the maximum level where the -MEMBER- folder is structured in your collaborative storage template, you can select this option and indicate the level.

  For example, in the Sample Classroom Collaborative Storage Template in Figure 7-1 on page 65, the -MEMBER- folder is located four levels down.

4 Indicate whether to hide the folders named -MEMBER, -OWNER-, and -GROUP-, objects by selecting the **Ignore hidden attribute on dynamic template** check box to hide the objects.

  Hiding the folders might prevent the folders from being deleted by users who don’t know why they are there.

5 Click **Apply** to save your settings.

6 Proceed with Section 7.7.8, “Setting Group Policy Cleanup Options,” on page 75.

7.7.8 Setting Group Policy Cleanup Options

This page lets you enable and specify cleanup rules for the Group policy. Options for cleanup include deleting a collaborative storage folder after a set number of days following the removal of the associated Group object from eDirectory, or vaulting (rather than deleting) the collaborative storage folder.

1 In the left pane, click **Cleanup Options.**

2 Enable storage cleanup by filling in the following fields:

  Enable: Select this check box to enable storage cleanup rules.

  Cleanup storage: Specify the number of days a collaborative storage folder remains after the associated Group object is removed from eDirectory.

3 Enable vaulting on cleanup by filling in the following fields:

  Enable: Select this check box to enable vaulting on cleanup rules.

  Vault Path: Click **Browse** to browse and select the path where you want the collaborative storage folders vaulted after cleanup.

  When you indicate this path, it also appears in the **Vault Path** field of the Grooming Rules page, because grooming rules and vault on cleanup rules share the same vault path.

4 Click **Apply** to save the settings.

5 Proceed with Section 7.7.9, “Setting Group Policy Vault Rules,” on page 76.

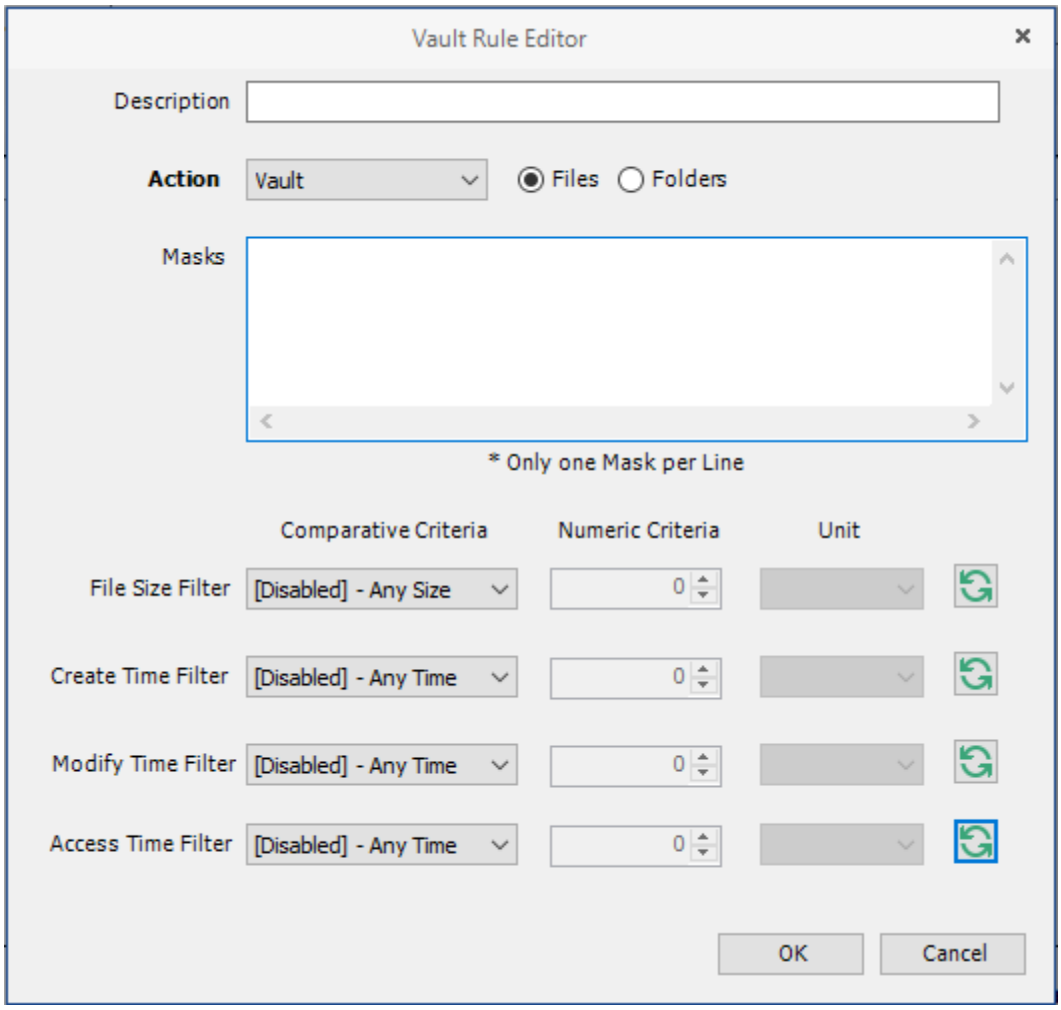
7.7.9 Setting Group Policy Vault Rules

When a Group object is removed from eDirectory, you can have Storage Manager for eDirectory vault the contents of the associated collaborative storage folder from a primary storage device to a less expensive secondary storage device. Storage Manager for eDirectory lets you specify what to vault or delete by using vault rules. For example, you might want to remove all `.tmp` files before vaulting the collaborative storage folder. Or, you might want to vault only a single folder, such as Final Proposal and nothing else in the other folders. You accomplish all of this through settings in the Vault Rules Editor.

1 In the left pane, click **Vault Rules**.

The **Vault Path** field displays the vault path that you established when you set up collaborative storage cleanup rules.

2 Click **Add** to bring up the Vault Rules Editor.



3 In the **Description** field, specify a description of the vault rule.

For example, “Files to delete before vaulting,” or “Files to vault.”

4 Fill in the following fields:

Action: Select whether this vault rule deletes or vaults.

Be aware that if you select **Vault**, only the files or folders that you list in the **Masks** text box are vaulted and the remainder of the home folder content is deleted. Conversely, if you select **Delete**, only the files or folders that you list in the **Masks** text box are deleted, and everything else is vaulted.

Files: If the vault rule you are creating will vault or delete content at the file level, leave the **File** option selected.

Folders: If the vault rule you are creating will vault or delete content at the folder level, select the **Folders** option.

Selecting **Folders** disables the filter settings in the lower portion of the Vault Rules Editor.

Masks: List the files or folders you want to be vaulted or deleted, according to what is indicated in the **Action** drop-down menu.

File or folder names can contain an asterisk.

5 (Conditional) If the vault rule you are creating is specific to files, complete the applicable filter settings.

Leaving the setting as **[Disabled]-Any Size** vaults or deletes all file types listed in the **Mask** text box, according to what is indicated in the **Action** drop-down menu. Choosing any of the other options from the drop-down menu lets you indicate files to delete or vault according to size, when created, when last modified, and when last accessed.

6 Click **OK** to save the vault rule.

7 If necessary, create any needed additional vault rules by repeating the procedures above.

8 Proceed with Section 7.7.10, “Setting Group Policy Grooming Rules,” on page 77.

7.7.10 Setting Group Policy Grooming Rules

Grooming rules in Storage Manager for eDirectory specify the file types that you do not want network users storing in their home folders or collaborative storage areas. Examples of these might be `.mp3` and `.mp4` files, `.mov` files, and many others. You use the Grooming rule to specify whether to delete or vault a groomed file.

Grooming takes place as a Management Action that is run by the administrator. A Management Action is a manual action that is enacted through the Admin Client. For more information, see Section 9.1.4, “Management Actions,” on page 88.

1 In the left pane, click **Grooming Rules**.

The **Vault Path** field displays the vault path that you established when you set up cleanup rules.

2 Click **Add** to bring up the Grooming Rules Editor.

3 In the **Description** field, specify a description of the grooming rule.

For example, “Files to groom in Community Outreach Group.”

4 Fill in the following fields:

Action: Select whether this grooming rule will delete or vault groomed files.

Files: If the grooming rule you are creating will vault or delete content at the file level, leave the **File** option selected.

Folders: If the grooming rule you are creating will vault or delete content at the folder level, select the **Folders** option.

Selecting Folders disables the filter settings in the lower portion of the Grooming Rules Editor.

Masks: List the files or folders you want to be vaulted or deleted, according to what is indicated in the **Action** drop-down menu.

File or folder names can contain an asterisk.

5 (Conditional) If the grooming rule you are creating is specific to files, complete the applicable filter settings.

Leaving the setting as **[Disabled]-Any Size** vaults or deletes all file types listed in the **Mask** text box, according to what is indicated in the **Action** drop-down menu. Choosing any of the other options from the drop-down menu lets you indicate files to delete or vault according to size, when created, when last modified, and when last accessed.

6 Click **Apply** to save the grooming rule.

7.8 Creating a Container Collaborative Storage Policy

1 In the Admin Client, click the **Main** tab.

2 Click **Policy Management**.

3 From the **Manage** drop-down menu, select **Create Policy > Create Container Policy**.

4 Specify a name in the **Name** field.

The Policy Options page appears.

5 Continue with Section 7.8.1, “Setting Container Policy Options,” on page 78.

7.8.1 Setting Container Policy Options

Settings within Policy Options let you indicate how the policy is applied and lets you write an expanded policy description.

1 Leave the **Process Events for Associated Managed Storage** check box selected.

In this example, the Collaborative Storage policy will apply to a container object. However, it could apply to the parents’ container thus making it applicable to all existing and new containers located therein. Deselecting this check box indicates that you want to create a Blocking policy. For more information on blocking policies, see Section 4.6, “Creating a Blocking Policy,” on page 21.

2 In the Description region, specify a description of the policy you are creating in the text field.

3 Click **Apply** to save your settings.

4 Select the options and setting that you want to policy to use:

Container Policy Associations: The Associations page is identical to the Association page presented when you create a Group policy. For an explanation of the page, along with procedures for setting associations, see Section 7.7.2, “Setting Group Policy Associations,” on page 69.

Container Policy Provisioning Options: The fields presented on the Provisioning Options page are identical to those presented when you create a Group policy. For an explanation of the page, along with procedures for setting provisioning options, see Section 7.7.3, “Setting Group Policy Provisioning Options,” on page 70.

Container Policy Target Paths: The fields presented on the Target Paths page are identical to those presented when you create a Group policy. For an explanation of the page, along with procedures for setting target paths, see Section 7.7.4, “Setting Group Policy Target Paths,” on page 71.

Container Policy Quota Options: The fields presented on the Quota Options page are identical to those presented when you create a Group policy. For an explanation of the page, along with procedures for setting quota options, see Section 7.7.5, “Setting Group Policy Quota Options,” on page 72.

Container Policy Move Schedule: The fields presented in the Move Schedule page are identical to those presented when you create a Group policy. For an explanation of the page, along with procedures for setting the move schedule, see Section 7.7.6, “Setting the Group Policy Move Schedule,” on page 74.

Container Policy Dynamic Template Processing: The fields presented on the Dynamic Templates page are identical to those presented when you create a Group policy. For an explanation of the page, along with procedures for setting the move schedule, see Section 7.7.7, “Setting Group Policy Dynamic Template Processing,” on page 74.

Container Policy Cleanup Options: The fields presented on the Cleanup Options page are identical to those presented when you create a Group policy. For an explanation of the page, along with procedures for setting cleanup options, see Section 7.7.8, “Setting Group Policy Cleanup Options,” on page 75.

Container Policy Vault Rules: The fields presented on the Vault Rules page are identical to those presented when you create a Group policy. For an explanation of the page, along with procedures for setting vault rules, see Section 7.7.9, “Setting Group Policy Vault Rules,” on page 76.

Container Policy Grooming Rules: The fields presented on the Grooming Rules page are identical to those presented when you create a Group policy. For an explanation of the page, along with procedures for setting grooming rules, see Section 7.7.10, “Setting Group Policy Grooming Rules,” on page 77.

5 Click **Apply** to save your settings.

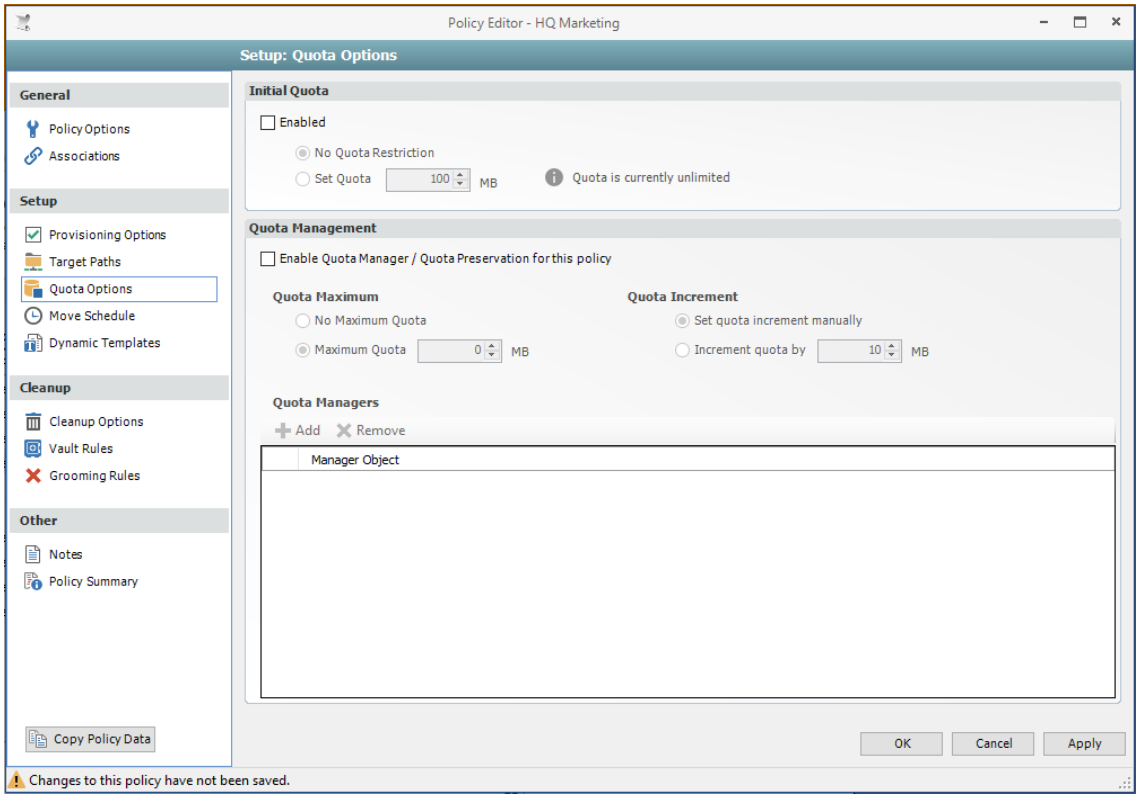
8 Using Quota Manager

Quota Manager is a separate management interface for designated users such as help desk administrators or support personnel, to increase user home folder or collaborative storage areas without needing rights to the file system.

Quota Manager can also provide storage information such as the total number of files and file types in a managed path. With this type of information, the help desk or support rep can make suggestions for freeing up space in the managed path rather than simply granting additional storage quota.

8.1 Quota Management Prerequisites

1 Using the Admin Client, verify that all of the policies managing the users for whom you want to manage quotas through Quota Manager have the **Enable Quota Manager** check box selected, with a Quota Maximum and/or Quota Increment setting.

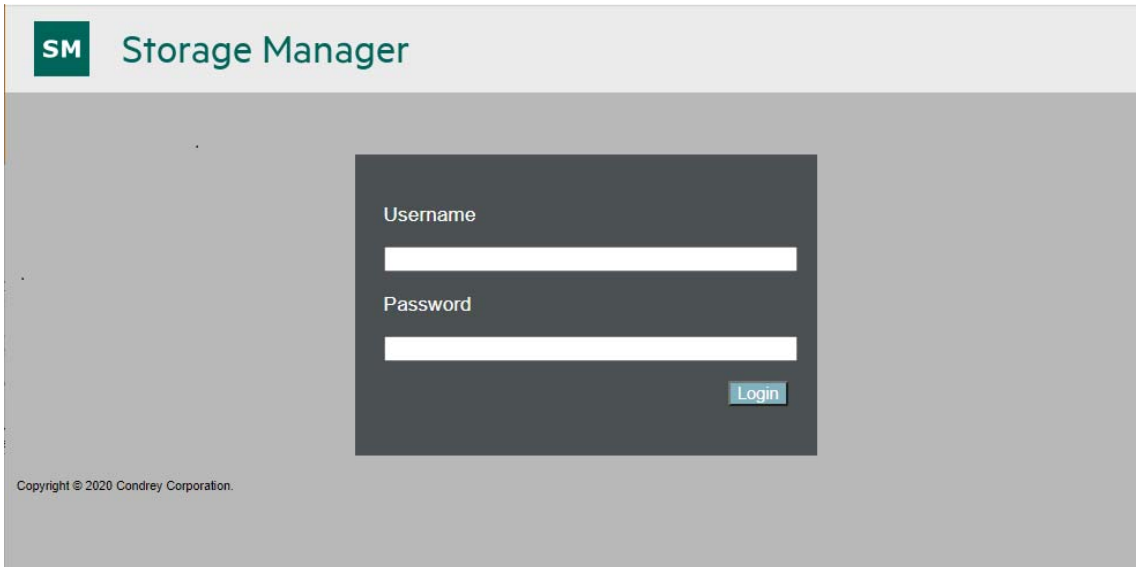


2 Verify that you have users or groups listed in the list box in the Quota Managers region of the page.

8.2 Managing Quotas Through Quota Manager

1. Launch a Web browser.
2. Enter the following address: https://*ip-address-or-dns-name-of-engine-server*:3009/qm
3. (Conditional) If a message appears informing you that the connection is not trusted, proceed by adding the security exception and downloading the certificate.

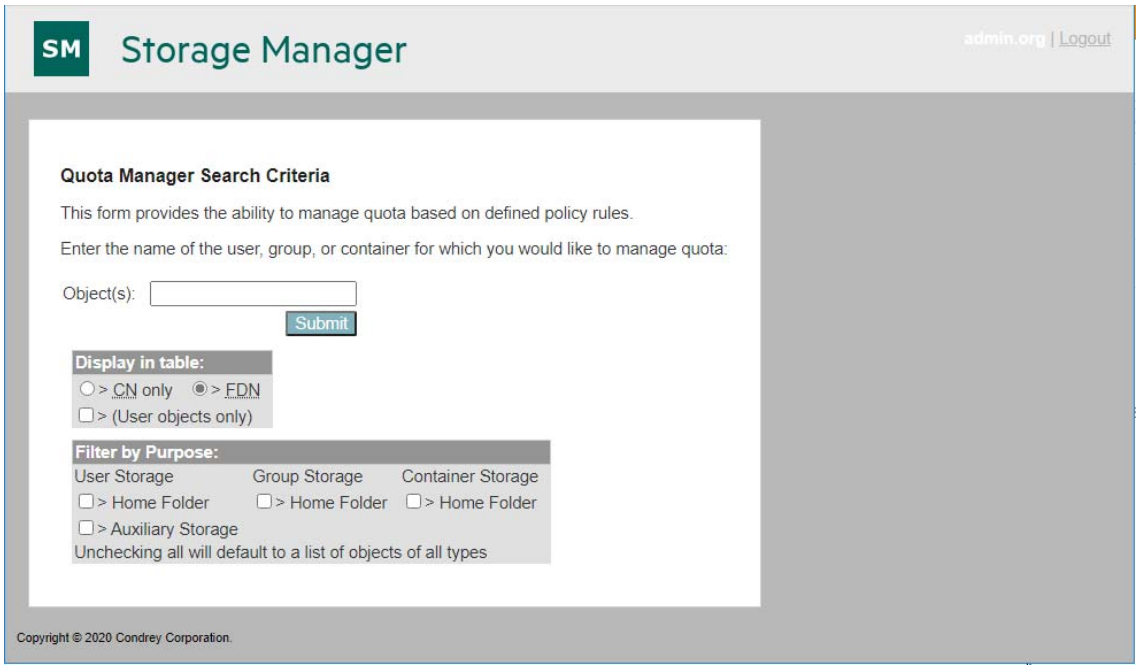
   The following screen appears:



4. Enter a username and password and click **Login**.

   The username and password must correspond to user that has been designated as quota manager either directly or through a group association.

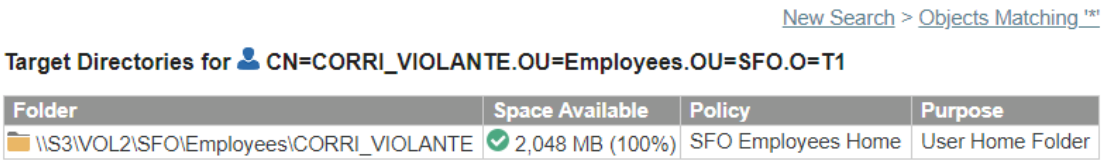
   If a user is enabled as a quota manager through eDirectory rights rather than through designation in the policy, the user must log in using a fully distinguished name.



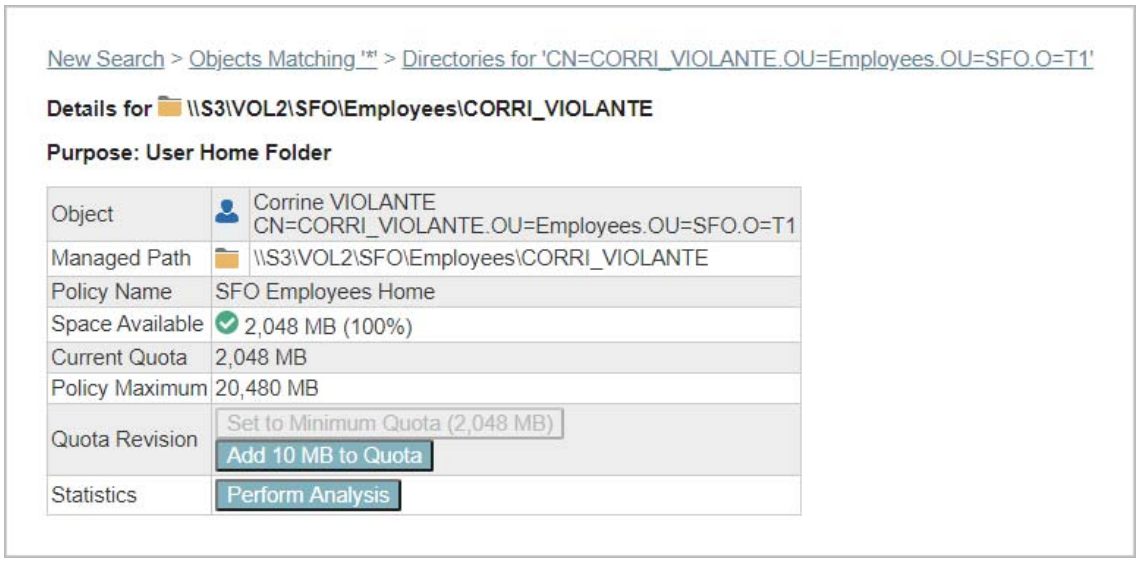
5 In the **Object(s)** field, specify a User or Group object name, or use an asterisk (*).
In large networks, building a list through the asterisk can be time consuming.

6 Specify your display and filter preferences in the corresponding regions.

7 Click **Submit**.



8 Click the User object you want to manage.



9 Add or remove a quota or perform a storage analysis by using the buttons provided.

8.3 Understanding Quota Manager Status Indicators

Quota Manager uses three different status indicators to show the current storage quota status for a user home directory or collaborative storage directory.

	Object FDN	Full Name	Folder	Space Available	Policy	Purpose
	CN=Adam James.OU=Employees.OU=Atlanta.O=T1	Adam James	\\S3\VOL1\Atlanta\Employees\Adam James	6 MB (22%)	Atlanta Employees Home	User Home Folder
	CN=Alicia Nance.OU=Employees.OU=Atlanta.O=T1	Alicia Nance	\\S3\VOL1\Atlanta\Employees\Alicia Nance	0 MB (1%)	Atlanta Employees Home	User Home Folder
	CN=Amanda Cox.OU=Employees.OU=HQ.O=T1	Amanada Cox	\\S3\VOL2\HQ\Employees\Amanda Cox	200 MB (100%)	HQ Employees Home	User Home Folder

Red: Denotes one of the following conditions:

- Quota usage has exceeded 90 percent.
- The SM Engine is unable to contact the server containing the volume.
- The volume does not support quota management.
- The home directory does not exist.
- The server containing the volume gave an Access Denied error, indicating that either remote storage management is not configured or enabled for the SM Engine, or that the firewall disallows remote storage management.

Yellow: Denotes that the quota usage has exceeded 75 percent.

Green: Denotes that quota usage is under 75 percent and that there are none of the problems specified above.

9 Reference

This section presents the tabs and tools in the Admin Client in a reference format. All of the tools are covered as they are presented in the Admin Client interface, beginning with the **Main** tab.

9.1 Main Tab

The **Main** tab provides access to all of the active management interfaces for Storage Manager for eDirectory. You use the **Main** tab to create, edit, deploy, and analyze Storage Manager for eDirectory policies.

9.1.1 Start Page

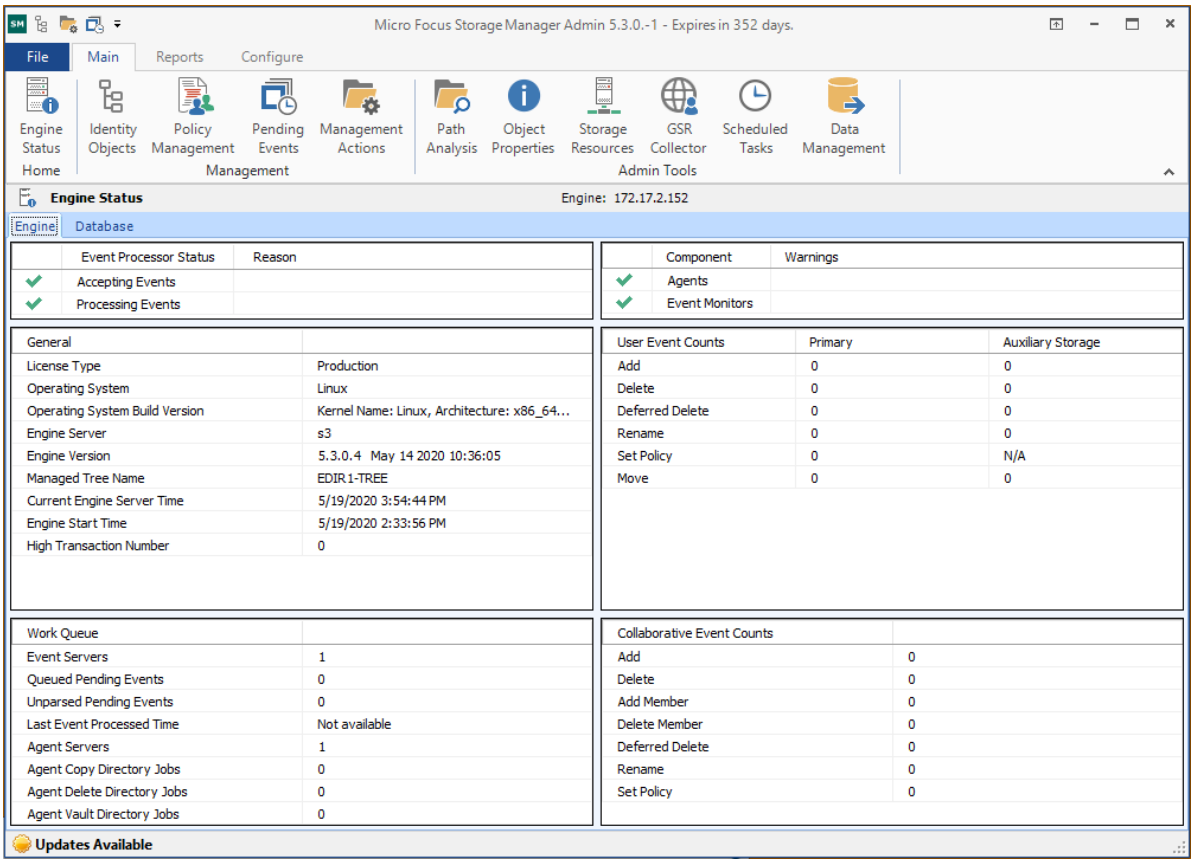
The left panes of the Start Page tool display an at-a-glance view of the management status of user storage, collaborative storage, and users and groups that have managed storage. The right pane displays links to resources and product news.

9.1.2 Engine Status

The Engine Status page provides an overview of the current status of the Engine through the **Engine** tab. If you are not seeing Storage Manager for eDirectory enact actions after events in eDirectory take place, viewing whether the Engine is processing and accepting events through this page is a good first step in troubleshooting.

Expanded details pertaining to events are detailed in different regions of the page. The General region provides general details including naming and version numbers. The User Event Counts region displays user storage actions. The Work Queue region provides details on actions yet to be completed. The Collaborative Event Counts region provides collaborative storage actions.

Figure 9-1 *Engine Status Page*



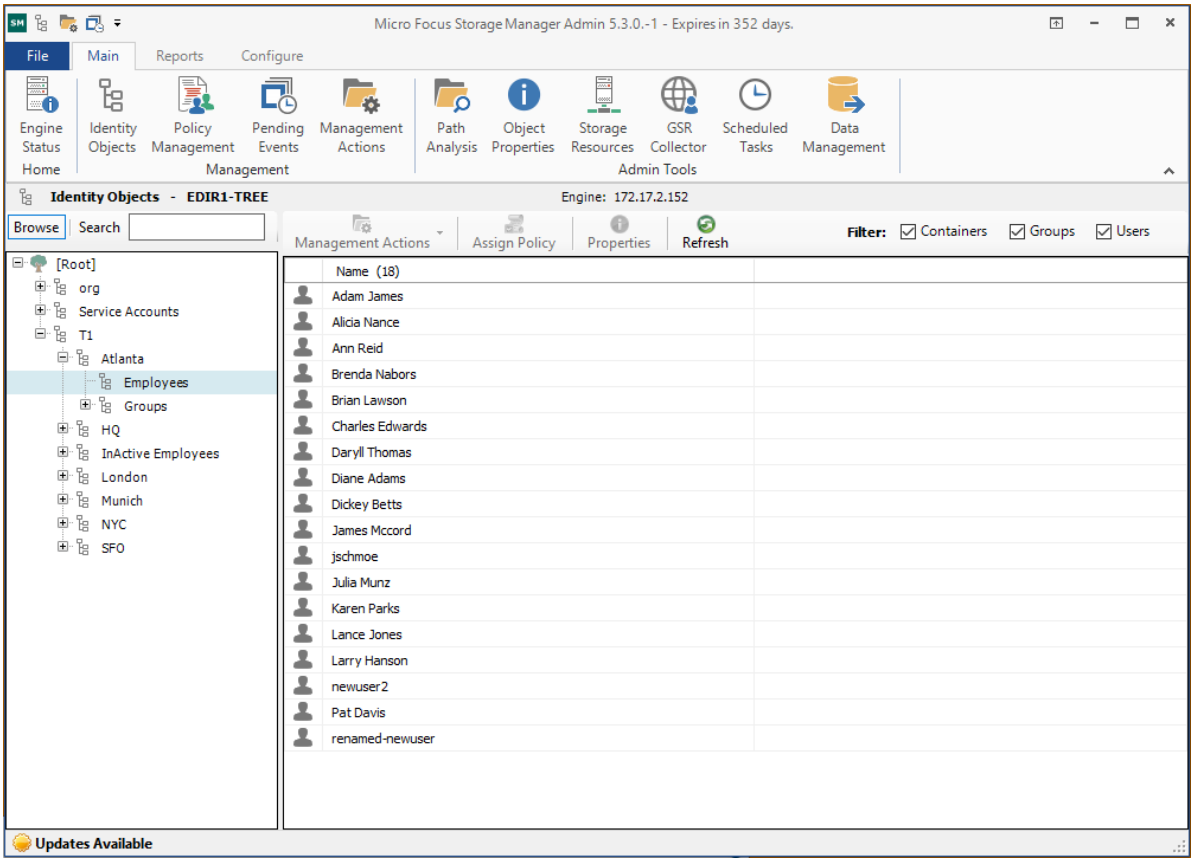
If you have Micro Focus File Reporter installed in your network, you can click the **File Reporter Integration** tab to view the status of the integration between Storage Manager for eDirectory and File Reporter.

NOTE: File Reporter reports on Storage Manager for eDirectory policies through a plug-in installed in the Admin Client. The plug-in allows administrators to create detailed, policy- based storage reports by reporting on the target paths associated with Storage Manager for eDirectory policies.

9.1.3 Identity Objects

The Identity Objects tool lets you manage the associations between Storage Manager for eDirectory policies and eDirectory objects such as organizational units, groups and users. This includes creating organizational units, setting context, viewing properties, performing Management Actions, and assigning policies.

Figure 9-2 *Identity Objects Page*



Left Pane

Use the left pane to browse and select organizational units in the directory. Right-clicking an organizational unit in the left pane lets you take additional actions:

- Create an organizational unit (OU)
- Set the directory context in the left pane to display the hierarchy from the root or from the selected organizational unit

Right Pane

Use the right pane to view the objects within a selected organizational unit as well as view properties, perform Management Actions, and assign policies. The right pane displays containers, groups, and users, according to what you have selected in the Filter check boxes.

IMPORTANT: When you perform actions in the right pane, it is important that you know whether you are performing management specific to users, groups, or containers.

9.1.4 Management Actions

In managing user and collaborative storage with Storage Manager for eDirectory, there are cases when you need to retroactively apply policies, rights, attributes, and quotas to existing user storage, or perform some administrative corrective action or operation on a large set of users, groups, or containers.

In Storage Manager for eDirectory, performing these types of operations is collectively referred to as performing a Management Action, and is done through the Identity Objects page by right-clicking the object and selecting **Management Action**, or clicking the **Management Actions** drop-down menu.

You can perform a Management Action on an organizational unit, a Group object, or a User object. Management Action operations on a Group object apply to users who are members of the group. Management Action operations on an organizational unit apply to users in the organizational unit, and optionally to all subordinate organizational units.

IMPORTANT: The Management Actions vary based on whether the selected mode is **User**, **Group**, or **Container**. For example, if **Group** mode is selected, the Management Action will be performed for collaborative storage processing using Dynamic Template processing. If **Collaborative** mode is selected, the Management Action will be performed for container based collaborative storage.

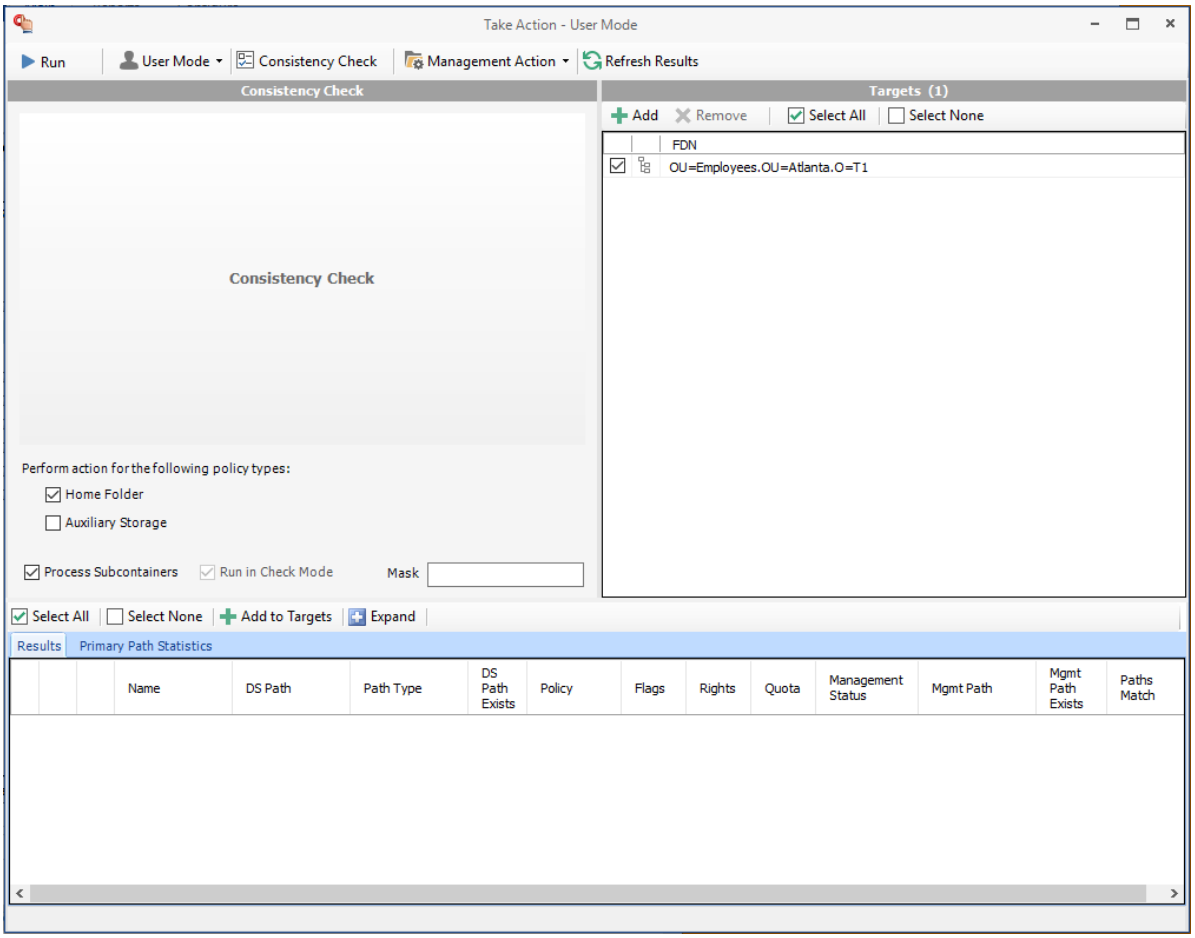
Storage Manager for eDirectory analyzes each User object independently, regardless of whether the Management Action is initiated via organizational unit, Group objects, or User objects.

- “Management Actions Dialog Box” on page 88
- “Available Management Actions” on page 90
- “Assign Policy” on page 94
- “Object Properties” on page 95

Management Actions Dialog Box

Whenever you initiate a Management Action, you work in a dialog box similar to the one below. A description of the components follows the graphic.

Figure 9-3 *Management Actions Dialog Box*



Run: Clicking this button executes the Management Action.

Mode: This drop-down menu lets you indicate if the Management Action is to apply to User, Group, or Container policy.

Consistency Check: This button lets you perform a consistency check before determining what Management Actions to perform. You can also use the **Consistency Check** button to view the results after you perform a Management Action.

Management Action: This drop-down menu lets you change from one Management Action to another while you are in the dialog box.

Refresh Results: This button refreshes the results displayed in the bottom pane of the dialog box.

Top Left Pane: The fields, options, and check boxes in this region vary based on the Management Action you are performing. In some cases, there is nothing in this region, because there are no settings to create. This region includes some powerful options for Management Actions, including the following:

- Process Subcontainers
- Run in Check Mode
- Mask

When you perform a Management Action on a container, Storage Manager for eDirectory applies the action to all subcontainers. If you do not want the action applied to subcontainers, you can deselect the **Process Subcontainers** check box.

The **Run in Check Mode** check box lets you view the potential outcome of performing a Management Action before you actually perform the action. The action is evaluated and all tasks associated with the action are listed. We recommend that you perform all Management Actions in check mode and observe the outcomes before actually performing a Management Action.

For Management Actions performed on organizational units or Group objects, you can enter a search filter in the **Mask** field to limit the number of objects that Storage Manager for eDirectory analyzes. You can enter standard wild card characters with multiple strings separated by the "|" character.

Top Right Pane: This part of the dialog box lets you add, delete, or select objects to which the Management Action applies.

Bottom Pane: This part of the dialog box displays the results after the Management Action has taken place. To expand the viewable area, click **Expand**.

Available Management Actions

Consistency Check

This Management Action notifies you of inconsistencies or potential problems pertaining to user and group storage being managed through Storage Manager for eDirectory. These potential problems might be missing storage quotas, inconsistent directory attributes, missing and inconsistent managed paths, and more.

In addition to reporting on storage issues, consistency check reports let you review current quota assignments and can help you with the design and planning of storage policies. In Section 4.3, "Running Consistency Check Reports on Existing Storage," on page 19, you ran a consistency check before creating your first primary user policy to help you determine how to configure the policy.

Manage

This Management Action catalogs objects in Storage Manager for eDirectory, putting them in a managed state.

If the existing objects already have established managed paths, attributes, and rights, Storage Manager for eDirectory does not change these settings, nor does it enforce policy paths, grooming, and quota management. If you need to change attributes and rights, or enforce policy paths, grooming, and quotas, you can do so through the specific Management Actions.

If these existing objects do not have established managed paths, Manage creates the managed paths and sets the rights, attributes, quotas, etc. according to the policies that apply to the objects.

Enforce Policy Paths

This Management Action moves data to where the policy's target path specifies. If you decide to move your user home folders from one location to another, you can simply change the target path in the policy and then run Enforce Policy Paths to move the home folders.

The **Enable pre-stage data copy** option lets you copy data without alerting you to failures if there are files open. When a user is moved in Active Directory and the policy dictates that the home folder is to be moved to a new target path, this option allows for all closed files to be moved. At a later time, you can go back and run an Enforce Policy Path Management Action without the **Enable pre-stage data copy** check box selected, to move the files that were previously open.

Groom

This Management Action carries out file grooming according to the file grooming specifications in the applied policy.

Apply Attributes

This Management Action lets you apply file system attributes. If you decide to modify the file system attributes in a policy, you can select **Apply Attributes** to immediately apply the new attributes for all of the affected objects.

If you cataloged existing objects with existing managed paths through Manage, the attributes for the managed path are not modified once the object's managed path attribute is cataloged (see Manage above). If you want to modify the original attributes of the managed path, you can do so through the settings in the in the left pane of the Apply Attributes dialog box.

Apply Home Drive

When the **Home Folder** check box is selected, this Management Action changes the home drive letter for the user that is assigned under eDirectory, to the drive letter that is specified in the Storage Manager for eDirectory policy.

NOTE: The new drive letter does not take effect until the user logs out and then logs in again.

Apply Members

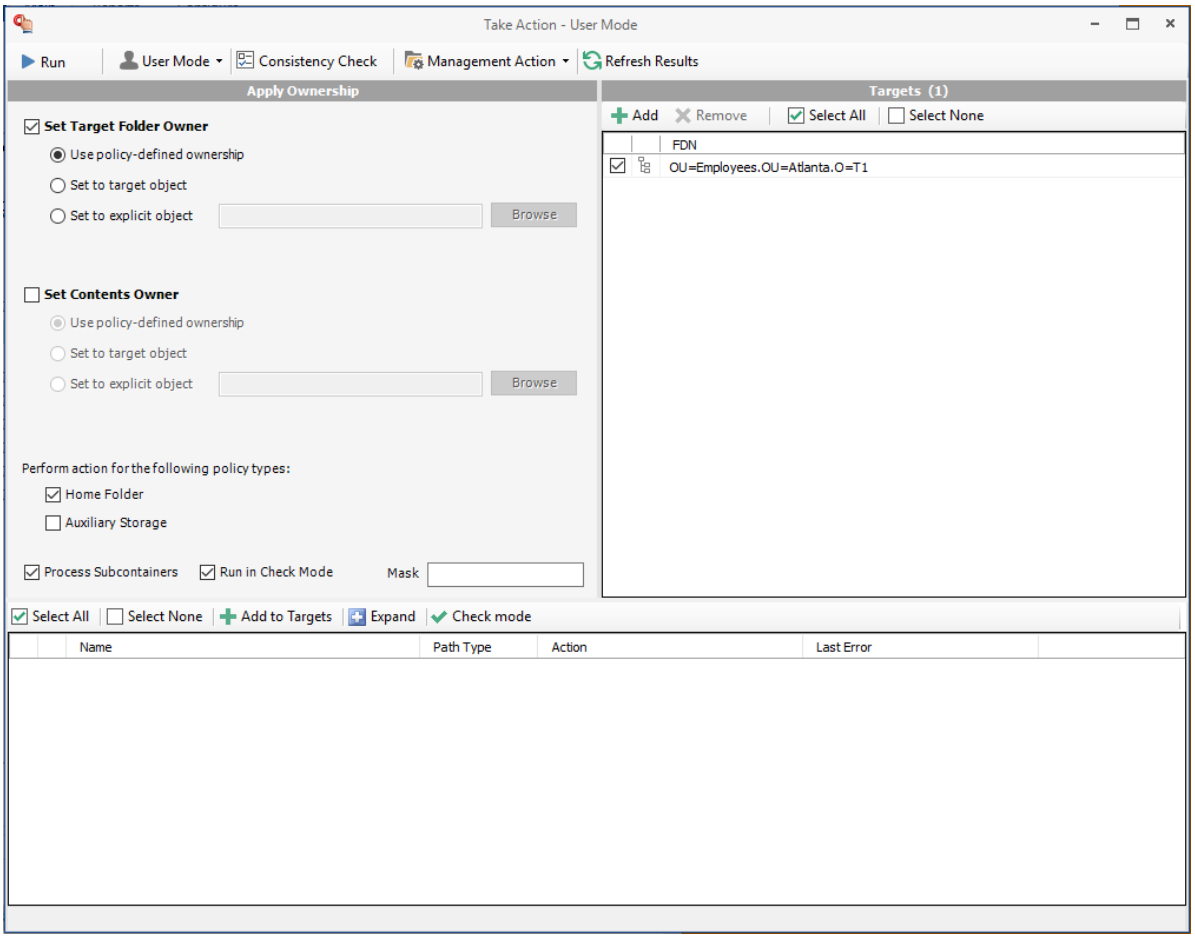
This Management Action is included to create the owner folder and personal folders in a collaborative storage area, where these folders did not exist previously. You must first modify the collaborative storage template in the policy to include -OWNER- and -MEMBER-. For more information, see Chapter 7, “Managing Collaborative Storage,” on page 63.

If you do have personal folders in the collaborative storage area and you later change the rights on -MEMBER-, you use the Apply Members Management Action to enforce the new rights.

Apply Ownership

This Management Action lets you set ownership of the home folder and home folder contents.

Figure 9-4 *Apply Ownership Management Action Page*



NOTE: The ownership specifications you make on the page shown above are applied to folders and files that exist at the time the Management Action takes place. The ownership of files and folders that are created later is not affected by this action. For example, if a user's home folder is moved due to an Enforce Policy Path action, the ownership of the user’s home folder will be determined by the settings in the policy.

Set Target Folder Owner: Select this check box to specify that the ownership applies only to the home folder and not to any subfolders.

Use policy-defined ownership: This option sets the home folder owner according to the specified owner in the **Path Owner** field of the policy.

Set to target object: When this option is selected, each of the selected users' home folders is set to have that user object as the owner.

Set to explicit object: This option lets you browse to select a specific owner for the home folder.

Set Contents Owner: Select this check box to specify that the ownership applies to the subfolders and files contained in the home folder.

Use policy-defined ownership: This option sets the home folder contents owner according to the specified owner in the **Path Owner** field of the policy.

Set to target object: When this option is selected, each of the selected users' home folders is set to have that user object as the owner.

Set to explicit object: This option lets you browse to select a specific owner for the contents of the home folder.

Perform action for the following policy types: Specify the policy types you want this Management Action to apply to.

Process Subcontainers: Selecting this option specifies that you want the settings on this page to apply to users that reside in the subcontainers within the container where this policy is applied.

Run in check mode: Selecting this check box lets you view the potential outcome of performing a Management Action before you actually perform it. The action is evaluated and all tasks associated with the action are listed. We recommend that you perform all Management Actions in check mode and observe the outcomes before actually performing a Management Action.

Mask: For Management Actions performed on organizational units or Group objects, you can enter a search filter in the **Mask** field to limit the number of objects that Storage Manager for eDirectory analyzes. You can enter standard wild card characters with multiple strings separated by the "|" character.

Apply Quota

This Management Action lets you apply managed path quotas. If you decide to modify the quota settings in a policy, you can select **Apply Quota** to immediately apply the new quota setting to all of the affected users.

If you cataloged existing network users with existing home folders through Manage, there might be no quota settings for the user home folders. Or, the quota settings might be inconsistent with those specified in the policy. If you want to establish or reset the quota for the home folder, you can do so through the settings in the left pane of the Apply Quota dialog box.

Apply Rights

This Management Action lets you apply file system rights. If you decide to modify the file system rights in a policy, you can select **Apply Rights** to immediately apply the new rights for all of the affected users.

Apply Template

This Management Action lets you apply a template specifying how to provision user or collaborative storage. If you decide to modify the template in a policy, you can select **Apply Template** to immediately apply the new template structure to all of the affected users. This can be especially

useful if you need to quickly provision a new subfolder with a document, such as a new health benefits document for all employees. All you need to do is modify the template to include the new subfolder and document inside the subfolder and then use Apply Template to provision it to everyone.

If you cataloged existing network users with existing home folders through Manage, the file structure created by the template is not modified after the user and his or her associated home folder are cataloged (see Manage above). If you want to modify the original file structure for the home folder, you can do so through the settings in the in the left pane of the Apply Template dialog box.

Clear Managed Path Attribute

This Management Action allows removes the managed path attribute so you can create a new one. Administrators might find this useful when users have invalid values for their home folder attributes and want to start over by creating new ones.

Recover Managed Path Attribute

If the attribute for a user home folder ever becomes corrupted, this Management Action can be used to recover an uncorrupted version of the attribute from the Storage Manager for eDirectory database.

Assign Managed Path

You can use this Management Action to assign an attribute to a user folder.

Directory Merge

This Management Action lets you merge contents of one home folder with those of another. This is especially useful if a user leaves an organization and you want to transition the files from the former user to another user. Another example might be if a user has two home folders and you want to merge the contents into one.

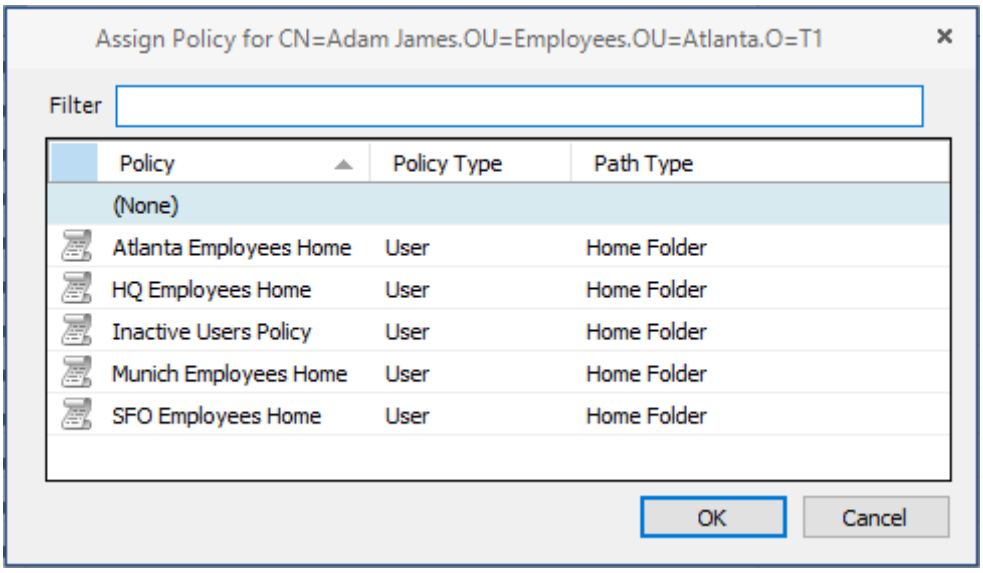
Remove from Database

This Management Action removes object from the Storage Manager for eDirectory database and makes the object unmanaged.

Assign Policy

Lets you easily assign a User, Group, or Organizational Unit object a policy while you are in the Identity Objects page. If an effective policy is already assigned to one of these objects, you can assign a new policy, replacing the effective policy with an assigned policy.

Figure 9-5 *Policy Selector Dialog Box*



The **Filter** field filters policy names as you type.

Object Properties

You can easily view an expanded set of object properties in the Identity Objects page by right-clicking an object in the right pane and selecting **Object Properties**.

The five tabs display the following information:

Properties: Displays eDirectory values and Engine database values. If you are working with a Support representative to resolve a problem, you might need to provide information from this screen.

Effective Policies: Lists all of the effective policies for the selected object. An effective policy is a policy that affects a user either directly through association or inheritance by membership in a organization, container, or group.

Associated Policies: Lists all of the associated policies for an object. An associated policy is an explicitly assigned policy associated with a container, group, or user.

Transactions: Shows pending events for the selected object. If there are many pending events, but you only want to see those pertaining to a particular user, you can see the pending events for the User object.

History: Shows a history of move and rename events that pertain to the selected User object.

Having historical information can be beneficial for a number of reasons. One in particular is for restoring files. Suppose a project manager was working on a project three years ago and then the company decided to discontinue funding the project. After one year, the project manager decided to delete the project files from her personal folder. Now suppose that two years later, a new executive in the organization wants to renew the project. To locate the original project files from backed up storage would be quite time consuming, but by viewing the information in the History tab, you could easily find the original location of the backed up home folder, if it was moved, and if so, where it was moved to, so that you could retrieve the project files.

9.1.5 Policy Management

The Policy Management page displays all policies, along with a summary of policy details. When you select a policy, applicable tools in the toolbar are activated. A summary of the toolbar follows.

NOTE: All of these tools are also accessible by right-clicking a selected policy.

Manage: Lets you create any of the following policies:

- User Home Folder policy
- Group policy
- Container policy
- Auxiliary policy

Rename Policy: Lets you rename the selected policy.

Delete Policy: Lets you delete the selected policy.

Edit Policy: Brings up the Policy Editor, where you can edit the selected policy.

Import Policies: Provides the ability to import policies that were previously exported through the Export Policies menu option.

NOTE: Policy associations are not imported. After policies are imported, you need to associate the policies to containers or groups.

For more information on importing policies, see Section 5.9, “Importing Policies,” on page 50.

Export Policies: Provides the ability to export policies so that they can be imported later. For example, many customers first evaluate Storage Manager for eDirectory in a lab environment and create a large number of policies in the process. You can export these policies and later import them into the production environment. For more information, see Section 5.8, “Exporting Policies,” on page 49.

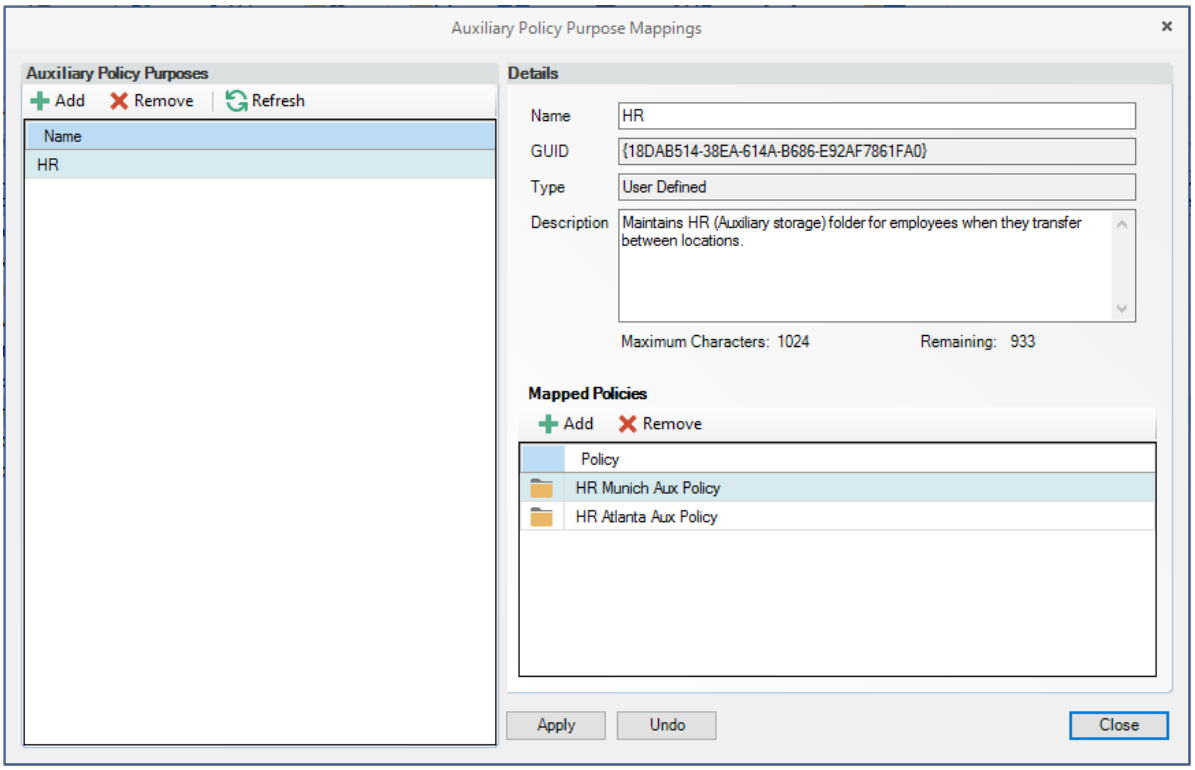
Import Upgraded Policies: Provides the ability to import policies migrated from a Storage Manager 2.5*x* Engine after the Admin Client Setup Wizard has been run. This feature is provided in case you chose not to import the policies when you ran the Setup Wizard.

Actions for Auxiliary Policies: Provides menu options that are applicable to Auxiliary policies. To activate this menu, click an Auxiliary policy. Menu options include **Manage**, **Groom, Apply Attributes**, **Apply Quota**, **Apply Rights**, and **Assign Auxiliary Attributes**.

Auxiliary Purpose Mappings: Auxiliary policy mappings give you the ability to specify a purpose or classification for auxiliary storage policies. For example, you might want to create an HR purpose for all of the auxiliary storage policies that create HR folders for employees. With each of the auxiliary storage policies that create HR folders assigned the same purpose, it makes it possible for Storage Manager for eDirectory to make intelligent decisions for auxiliary storage when a user is moved.

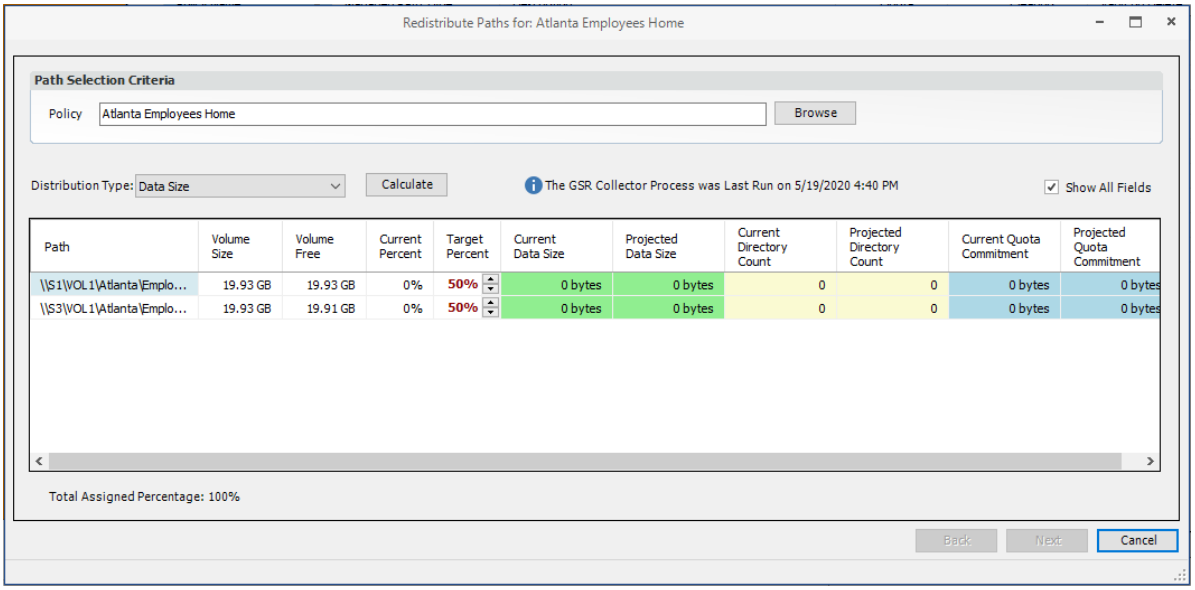
For example, if a user in the Detroit office transfers to the Dallas office, and the user has a home folder and an auxiliary storage folder in the Detroit office’s HR department, you want to migrate both the home folder and the auxiliary storage folder to correct locations in Dallas. Having the Detroit auxiliary storage policy and the Dallas auxiliary storage policy identified with the same HR purpose, ensures that the user moved from Detroit to Dallas, will have his auxiliary storage properly established with the move.

Figure 9-6 *Auxiliary Purpose Mappings Dialog Box*



Redistribute Policy Paths: Allows you to define additional target paths in the policy and then redistribute or load-balance the data among the various paths.

Figure 9-7 *Redistribute Policy Paths Dialog Box*



Using the Redistribute Policy Paths dialog box, you can redistribute the user and collaborative storage across the target paths associated with a policy.

NOTE: The data displayed in the dialog box is taken from the most recent report from the GSR Collector.

Use the **Distribution Type** drop-down menu to view your data distribution according data size, directory count, and quota commitment.

Click **Next** to view the current locations of the home folders and collaborative storage folders, and the location where Storage Manager for eDirectory proposes to redistribute the folders. If you want, you can deselect a folder for distribution by deselecting the check box corresponding to the folder. You can also indicate a new target path for the folder by clicking in the **Target Policy Path** column and selecting a new target path.

Clicking **Submit** begins the process of redistributing the folders.

Report on Policy Paths: If your network includes Micro Focus File Reporter, this button is the means of Micro Focus File Reporter reporting on Storage Manager for eDirectory policy paths.

This capability is particularly powerful because it allows you to specify the target paths where user and collaborative storage resides on the network. Because network user and collaborative home folders tend to be the source of most of the stale, redundant, and non-work-related file types, the Policy Path Reporter can quickly and easily be the means of generating reports on the storage areas that you care about most. For procedures, refer to the *Micro Focus File Reporter 3.6 Administration Guide*.

Refresh: Refreshes the list of policies.

NOTE: Refreshing locks the database during the refresh operation. For best performance, do not refresh more than is necessary.

Reload Policy Cache: Reloads your policies from the database. For example, you can use this tool if you have a policy that is not displayed in the list.

Check Boxes: The Admin Client shows only the policy types that are checked.

Filter: Filters policy names as you type.

9.1.6 Pending Events

This page displays a list of pending events for the Engine. All of the pending events are listed with details on the status of those events. Some events process very quickly and might actually be completed before they can be viewed in the list. Other events might remain in the queue for a long time, waiting for some condition to be met before they can be completed.

Clicking a listed event or events activates the toolbar. The toolbar has the following options:

Properties: Displays event properties such as FDN, ID, Action, and Current Status.

Make Eligible: If an event is deferred, you can click this option to make the event eligible immediately.

Defer: If an event is eligible, you can click this option to manually defer it to a specific date. The chosen deferral date is displayed in a **Notes** field. You can also enter any notes explaining the reason you are deferring the event. Text from the **Notes** field is also displayed in the **Deferred Notes** field of the Properties dialog box.

Bypass: Lets you bypass the status that is holding up the event.

Abort: Lets you terminate the selected event or events.

WARNING: Aborting events should only be used when really necessary, as they can leave your managed objects in an unknown state. Use aborts carefully! Be sure to only highlight the events needing to be cleared. All selected, eligible, events will be aborted. When aborting events, be sure to do extra checking of data before trying to act on objects again. Do frequent consistency checks before moves. Watch for things like home directories set to PROXYHOM. You may need to make some manual corrections before initiating further operations.

Refresh: Refreshes the event list.

Previous/Next: The arrows let you move forward or back in the event list according to the **Events Per Page** setting.

Events Per Page: Indicates the number of events you want displayed on each page.

NOTE: These settings are persisted across Engine restarts. Therefore, if you stop processing and restart the Engine or the server hosting the Engine reboots for some reason, event processing will remain off until you turn it back on.

- **Accepting:** A green check mark indicates that Storage Manager for eDirectory is accepting events to process. You can stop accepting events to process by clicking this button. You are prompted to enter text in a field indicating your reason for stopping the acceptance of events. The text you enter is recorded on the Engine Status page.
- **Processing:** A green check mark indicates that Storage Manager for eDirectory is processing events. You can stop processing events by clicking this button. You are prompted to enter text in a field indicating your reason for stopping the processing of events. The text you enter is recorded on the Engine Status page.

9.1.7 Path Analysis

The Path Analysis page shows a tree view of your network storage and provides various storage reports. These reports are a quick way to determine the trustees of a volume or folder, the number of files and file types in a given folder, whether a quota is assigned to a folder and if so, how much, and the trustees of individual files.

NOTE: Whether managed by Storage Manager for eDirectory or not, all of the storage visible in the left panel is eligible for path analysis.

Use the left pane to browse and select network volumes and folders. Use the right pane to view the files within a selected folder.

Clicking a volume or folder in the left pane activates the toolbar. Options are also available by right-clicking a volume or folder. The toolbar has the following options:

Path Analysis A drop-down menu with the following options:

- **Quota:** Indicates if a quota is set for a folder, the quota size, and the amount of free space remaining in the folder.

- **File Types:** Categorizes the content of the selected folder by displaying the various file types, the total number of each file type, and the total size of each file type. For example, to know if a user is storing non-work related files in his or her home folder and the total size of these files, you could use this feature to quickly determine this information.
- **Trustees**: Opens the View Trustees dialog box, which lists all users and objects that have any type of rights to the selected volume, folder, or file. The View Trustees dialog box also indicates the rights that each of these users and objects have as well as how these rights are obtained.

Path Management: A drop-down menu with the following options:

- **Create Folder:** Lets you create a new folder within a selected folder.
- **Rename Folder:** Lets you rename a selected folder.
- **Delete Folder:** Lets you delete a selected folder.

Rebuild: Rebuilds your storage resource list. You might need to do this to display the storage resource list structure after it has been modified.

Refresh: Refreshes the view within the Path Analysis page.

9.1.8 Object Properties

You can display the object properties through the Identity Objects page, and you can also display them through the Object Properties page.

Use the **Browse** button to select an object from the Object Browser to place the fully distinguished name of the object in the **FDN** field, then click **Submit**. The five tabs display the following information:

Properties: Displays eDirectory values and Engine database values. If you are working with a Micro Focus Support representative to resolve a problem, you might need to provide information from this page.

Effective Policies: Lists all of the effective policies for the selected object. An effective policy is a policy that affects a user either directly through association or inheritance by membership in a container or group.

Associated Policies: Lists all of the associated policies for an object. An associated policy is an explicitly assigned policy associated with a container, group, or user.

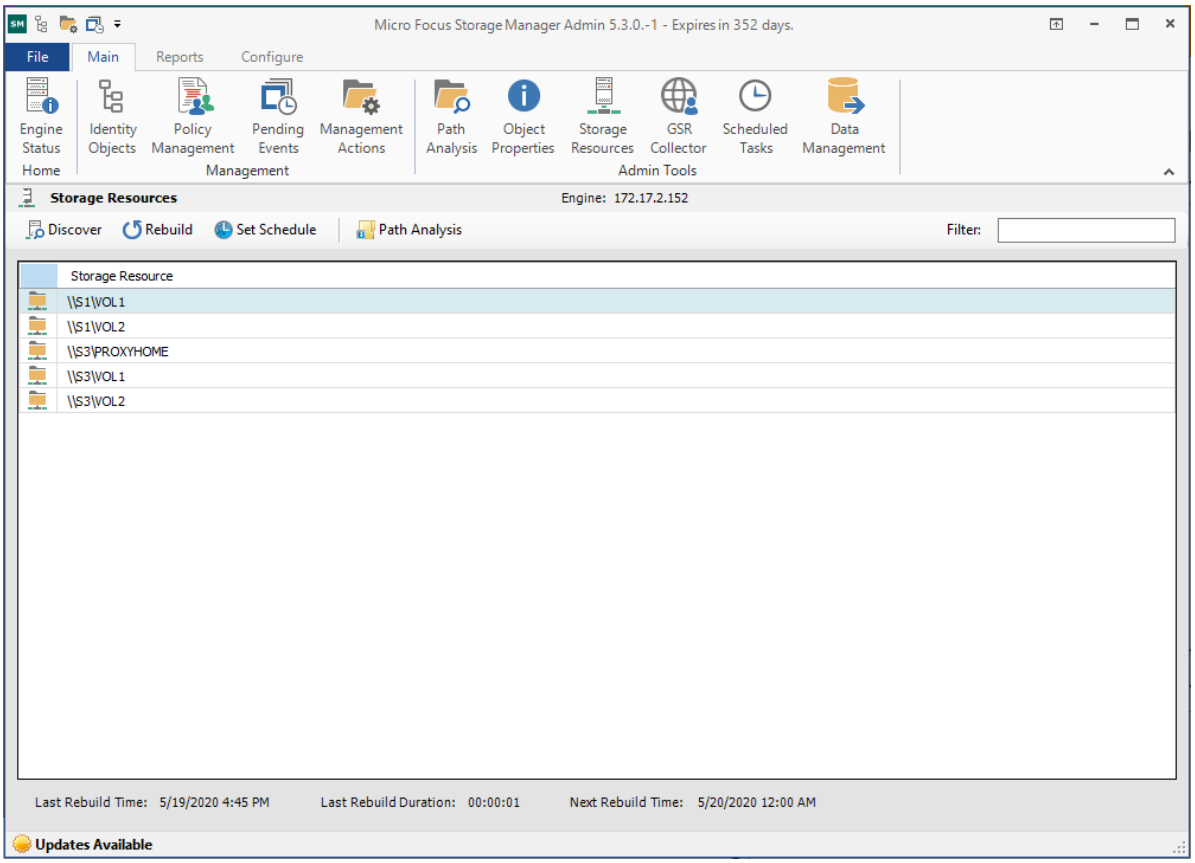
Transactions: Shows pending events for the selected object. If there are many pending events, but you only want to see those for a particular user, you can see the pending events for the User object.

History: Shows a history of managed storage that pertain to the selected User object. This information is only available after the GSR Collector has run.

9.1.9 Storage Resource List

This page lets you rebuild the storage resource cache used in Storage Manager for eDirectory. Because Storage Manager for eDirectory uses the storage resource cache to accelerate operations, there might be times when you need to use this page to populate the cache with new volumes.

Figure 9-8 *Storage Resource List Page*



Discover: Clicking this button initiates a search within the entire tree for any new volumes. Depending on the size, configuration, and topology of your network, this can take a significant amount of time.

Rebuild: Clicking this button initiates a search within the entire tree for all available volumes. When you create or edit a policy, you might need to rebuild the list if the volume you need does not appear in the storage resource list. Depending on the size, configuration, and topology of your network, this can take a significant amount of time.

Set Schedule: Allows you to set the schedule for rebuilding the storage resource cache.

Path Analysis Clicking this button opens the path analysis page for the selected storage resource, allowing you to browse it and do path analysis on any folder you select.

Last Rebuild Time Displays the last date and time that the storage resource list was rebuilt.

Last Rebuild Duration: Displays the length of time it took to generate the new storage resource list.

Next Rebuild Time: Displays the date and time when Storage Manager for eDirectory next rebuilds the storage resource list. Unless rebuilt through the **Rebuild Storage List** button, the storage resource list is rebuilt automatically at midnight each day.

9.1.10 GSR Collector

The Global Statistics Reporting (GSR) Collector gathers and presents an extensive amount of statistical summaries pertaining to file system data. The GSR Collector provides data for the various reports that you can generate in Storage Manager.

The GSR Collector can be run manually or based on a schedule.

Additionally, the GSR Collector maintains a history in the Storage Manager for eDirectory catalog of the movement of user managed paths.

The GSR Collector can be especially useful when Storage Manager for eDirectory has archived data. When data is archived, network administrators tend to move data from one storage area to another. Each time the GSR Collector is run, Storage Manager for eDirectory records the old and new locations for the data, so that the data can be easily located; for example, if an audit is necessary.

To view the history from the Identity Objects page, display a User object in the right pane and then double-click it. In the Object Properties dialog box, click the **History** tab to view historical information of data movement pertaining to the User object.

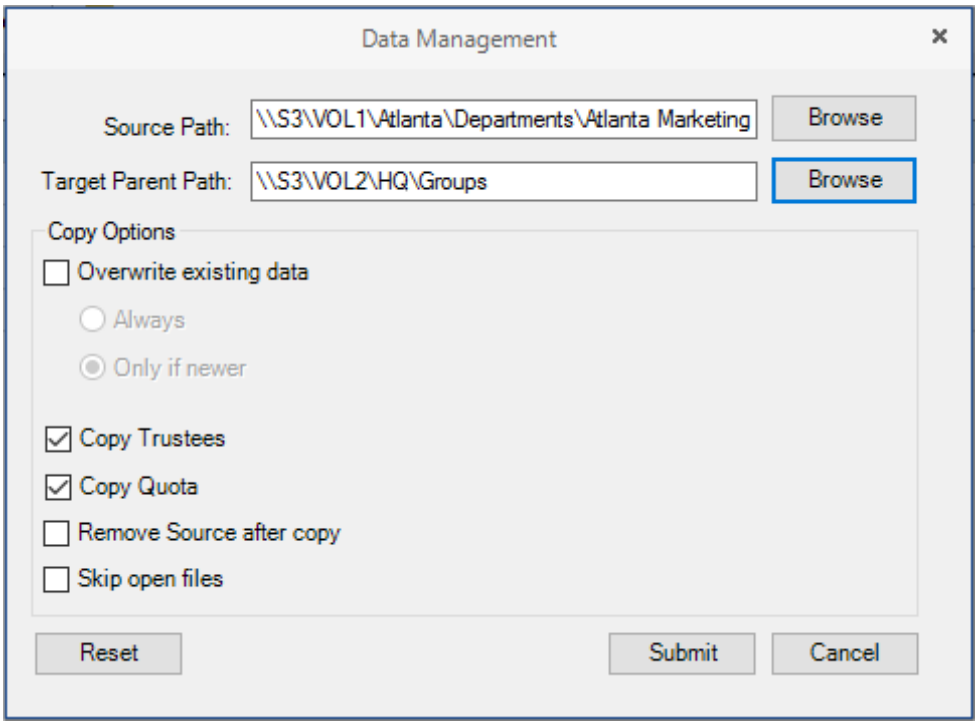
The GSR Collector can be resource intensive. You should be careful when running the GSR Collector during peak traffic load on the Engine.

9.1.11 Scheduled Tasks

You can use Scheduled Tasks to view, edit, and run tasks that are currently scheduled. Scheduled tasks include storage resource discovery, file grooming, data copying, and running the GSR Collector. To edit a scheduled task, select the task listing, click **Edit Scheduled Task**, and then select **Edit Schedule** to access the schedule dialog box. You can also access the same dialog box through the GSR Collector page, the Storage Resource List page, and on the Add Scheduled Tasks page to schedule grooming.

9.1.12 Data Management

Data Management (data copying) lets you copy a specific set of data and its associated rights, ownership, and other metadata from one location to another without requiring a policy. If you choose, you can preserve all of the permissions and quota settings in the process.



Additional options let you overwrite existing duplicate files or folders, remove files from the source location once they are copied to the target location, and skip open files. If you want Storage Manager for eDirectory to attempt to copy open files after they are closed, leave this option deselected.

9.2 Reports Tab

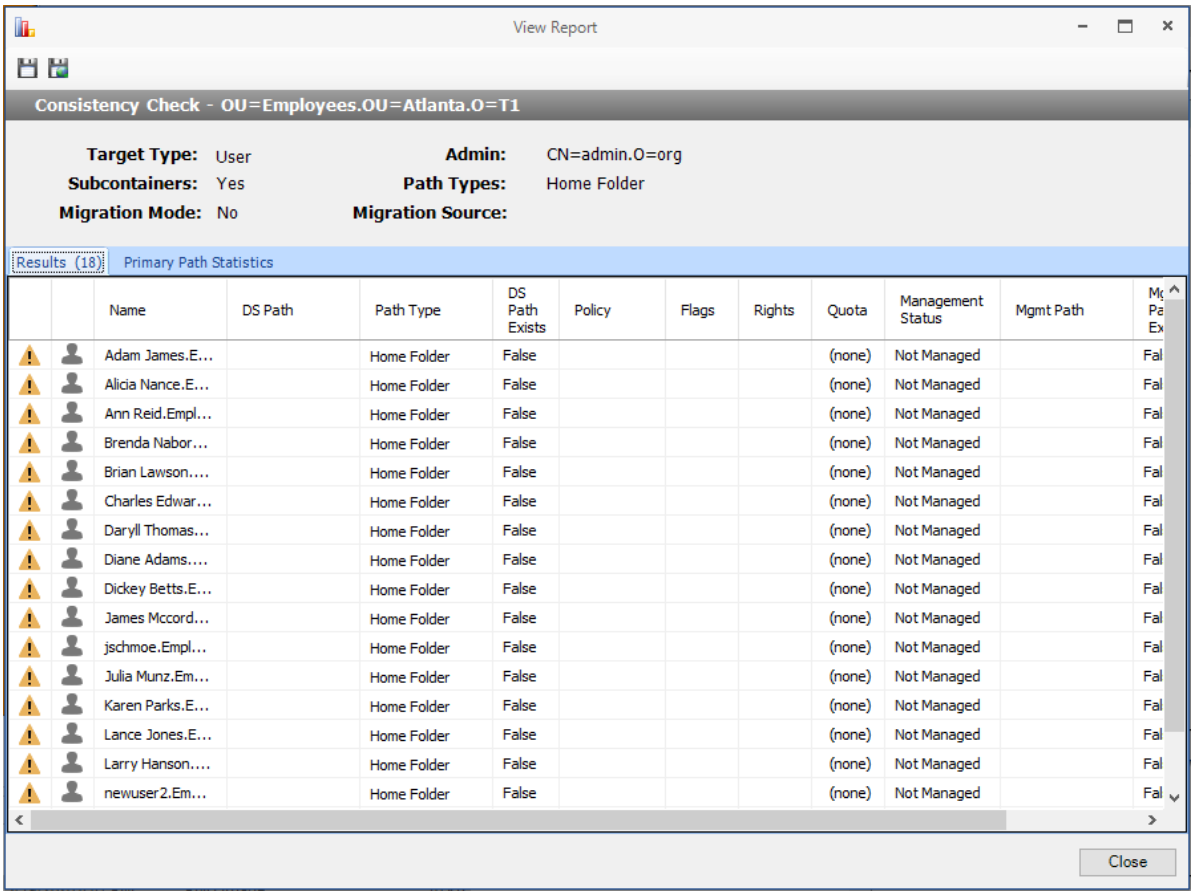
The **Reports** tab provides access to existing Consistency and Management Action reports for events and network storage. It also provides access to a Runtime Config report that reports on your Storage Manager for eDirectory configuration, environment, and pending events.

9.2.1 Consistency Check Reports

This page is used to access and export stored Consistency Check reports.

To access a report, double-click a report listing to access the View Report dialog box.

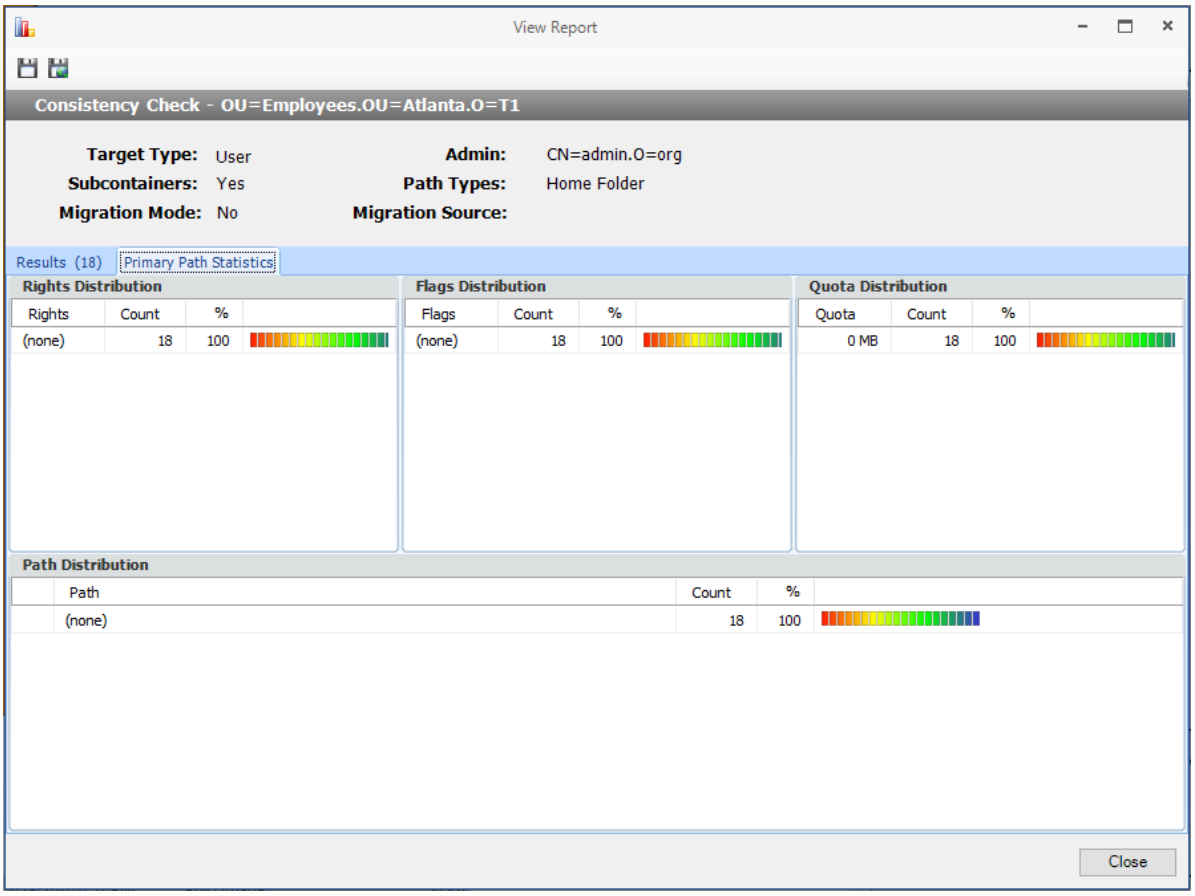
Figure 9-9 *Consistency Check Report*



The dialog box displays the contents of the Consistency Check report.

The **Primary Path Statistics** tab shows the rights, flag, and path distribution data in text and graphical format.

Figure 9-10 *Primary Statistics in a Consistency Check Report*



To export a Consistency Check report, double-click a report listing to access the View Report dialog box, and then in the upper-left corner of the dialog box, click either the **Save CSV Report** or **Save HTML Report** icons.

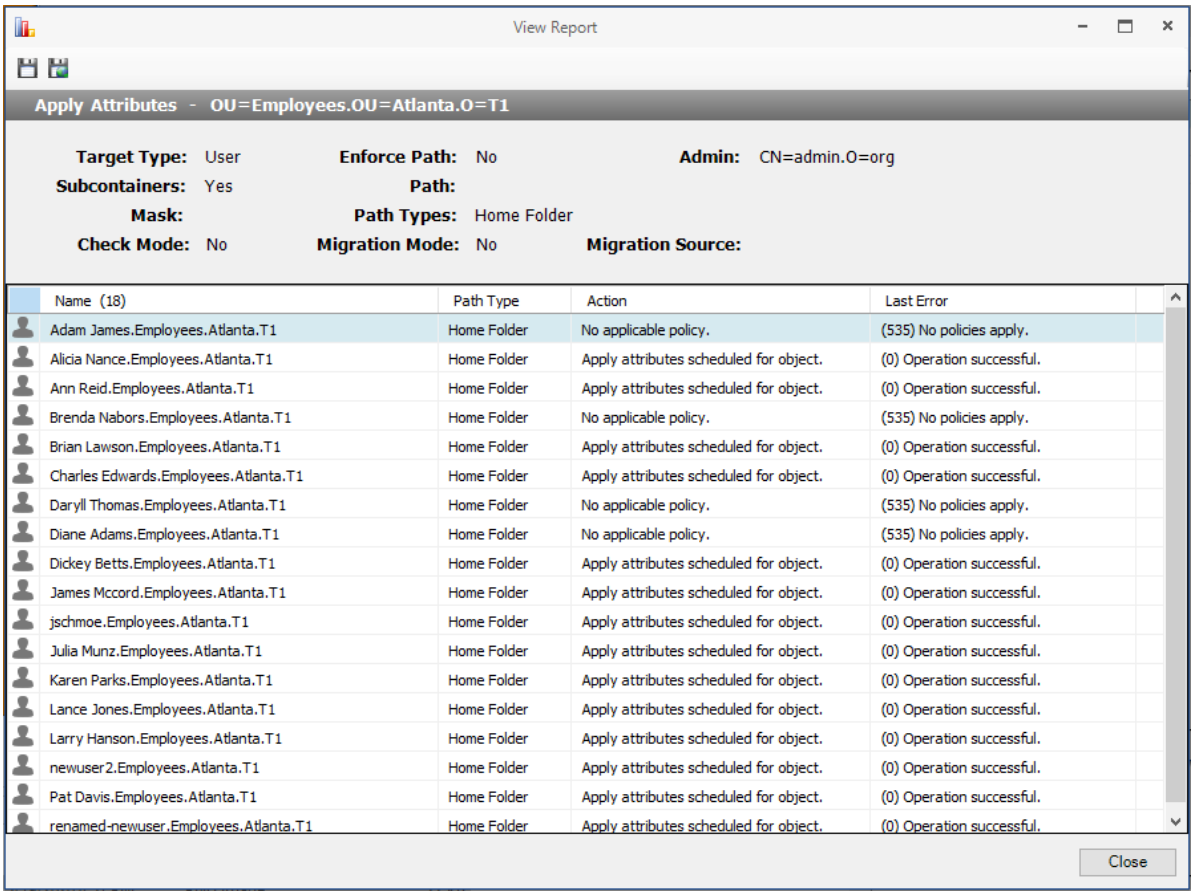
For more information on Consistency Check Reports, see Section 4.3, “Running Consistency Check Reports on Existing Storage,” on page 19 and Section 4.10, “Performing a Consistency Check,” on page 28.

9.2.2 Action Reports

Action reports are stored each time a Management Action is performed. Use this page to view or export to a report, the results of any Management Action performed. A list of available Management Action reports is presented, identifying the report by the eDirectory object it was run on, and the time the report was generated.

Double-clicking any item in the list brings up the individual Management Action report.

Figure 9-11 *Action Report*



To export an Action report, double-click a report listing to access the View Report dialog box, and then in the upper-left corner of the dialog box, click either the **Save CSV Report** or **Save HTML Report** icons.

9.2.3 Anomaly Reports

Anomaly reports indicate anomalies that can occur over time as a result of manual storage management practices. See Chapter 4, “Managing Existing User Storage,” on page 17, for information on Management Actions that are based on the anomalies in the Anomaly reports.

Anomaly reports are generated after the first time you run the GSR Collector. Any anomalies the GSR Collector finds are listed in one of the following category reports:

Table 9-1 *Categories for Anomaly Reports*

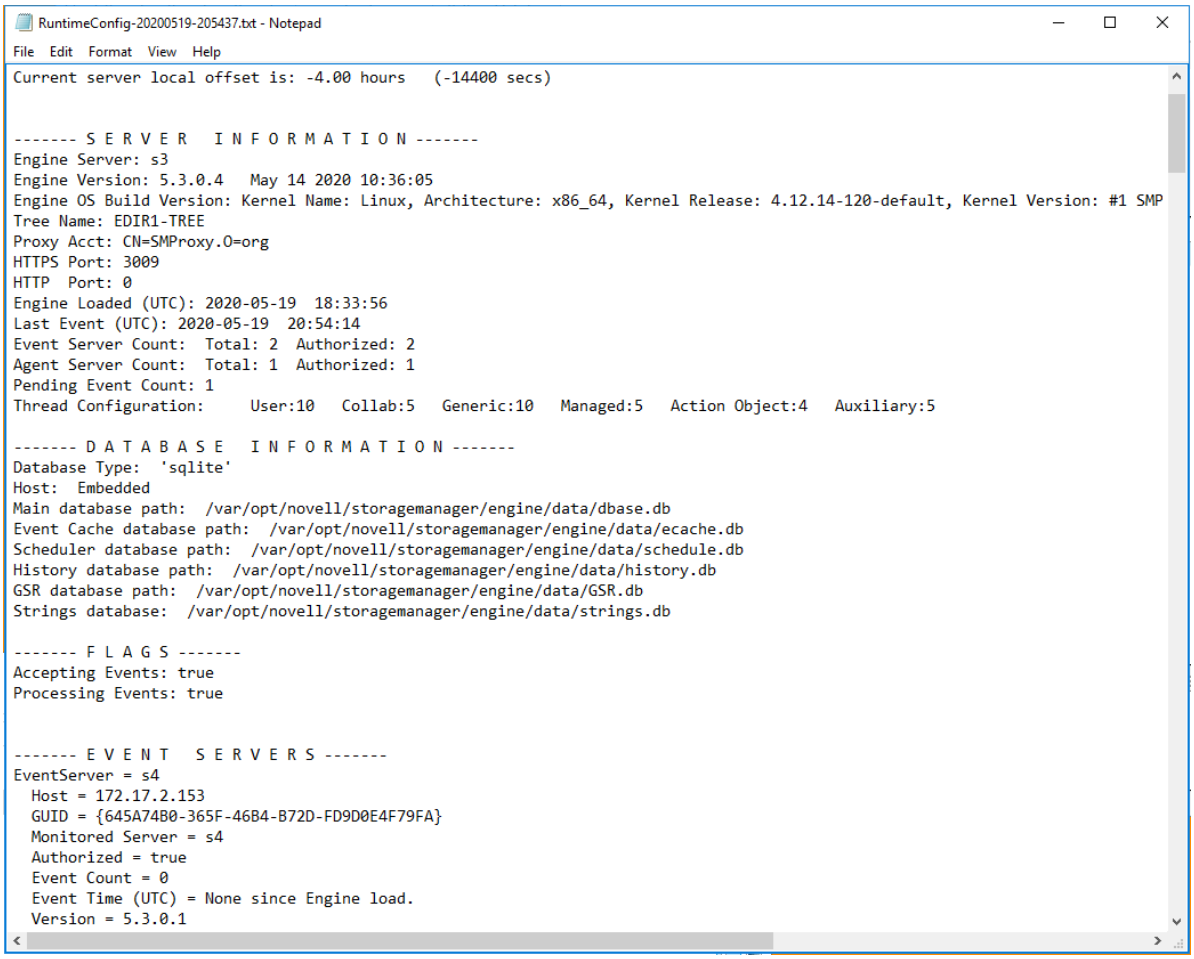
Tab Name	Explanation
Orphan Candidates	Lists home directories that are not currently assigned to a User object in eDirectory.
Name Mismatch	Lists cases where a username and the associated home directory name do not match. This is frequently the case when a User object is renamed, but the corresponding home directory is not.

Tab Name	Explanation
Path Overlap	List home directories that are parent paths of other user home directories. For example, a user's home directory attribute in eDirectory is set to VOL1:\HOME\USERS instead of VOL1:\HOME\USERS\JBANKS. This is a potential conflict because if you move an object that resides in the first path, it moves all users below the user.
Duplicate Storage Pointer	Lists users that have identical home directory paths.
Missing Primary Folders	Lists users who do not have assigned home directories.
Other Missing Folders	Lists users that have auxiliary storage assigned, but the storage is not yet created.
Objects Not Managed	Lists objects in eDirectory whose managed path is populated with a value but are not managed through Storage Manager for eDirectory.

9.2.4 Runtime Config

Runtime Config reports are used to build reports on the current configuration and pending events from the Engine. You can indicate which configuration data you want included in the report by selecting the desired check boxes.

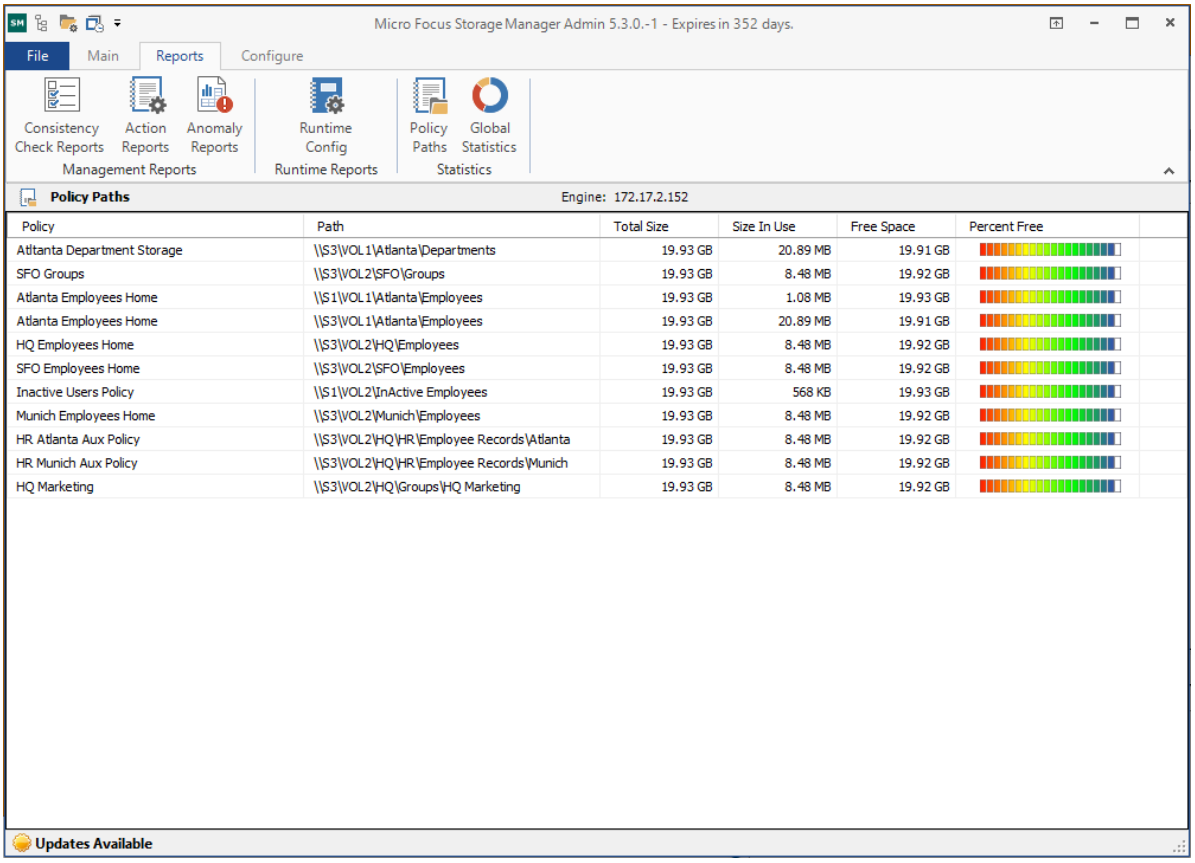
Figure 9-12 *Sample Runtime Config Report*



9.2.5 Storage Resource Statistics

This page shows high-level statistical information pertaining to your policies, their corresponding target paths, and size and free space information.

Figure 9-13 *Storage Resource Statistics Report*

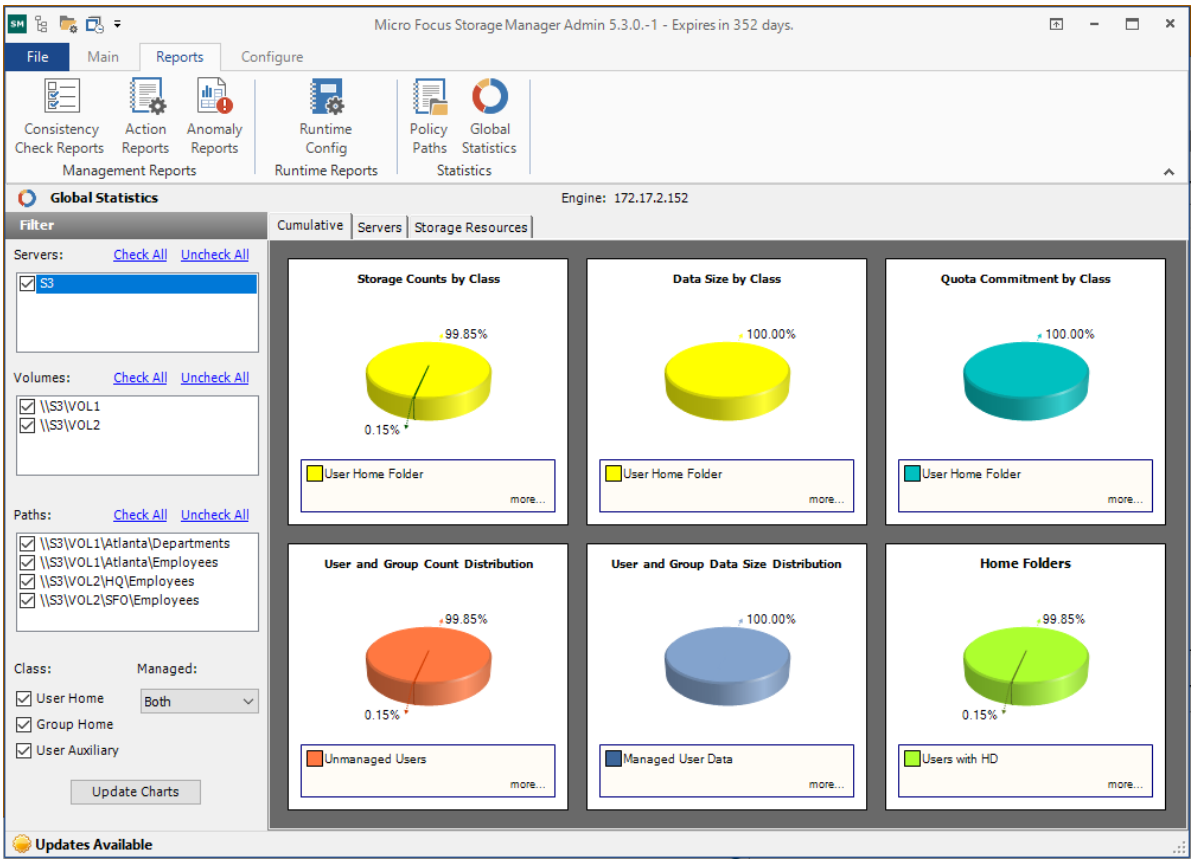


9.2.6 Global Statistics

Global Statistics provides a graphic view of the current state of your storage. The reports can be configured to show different the servers, volumes and paths. The class (user, collaborative, or auxiliary storage) can also be selected.

The reports can be configured to show different servers, volumes, and paths. The class (user, collaborative, or auxiliary storage) can also be selected. Expanding or stretching the Admin Client increases the size of the charts and the legend under each chart.

Figure 9-14 *Global Statistics Report*



Expanding or stretching the Admin Client increases the size of the charts and the legend under each chart.

9.3 Configure Tab

The **Configure** tab includes all of the operations to configure Storage Manager for eDirectory.

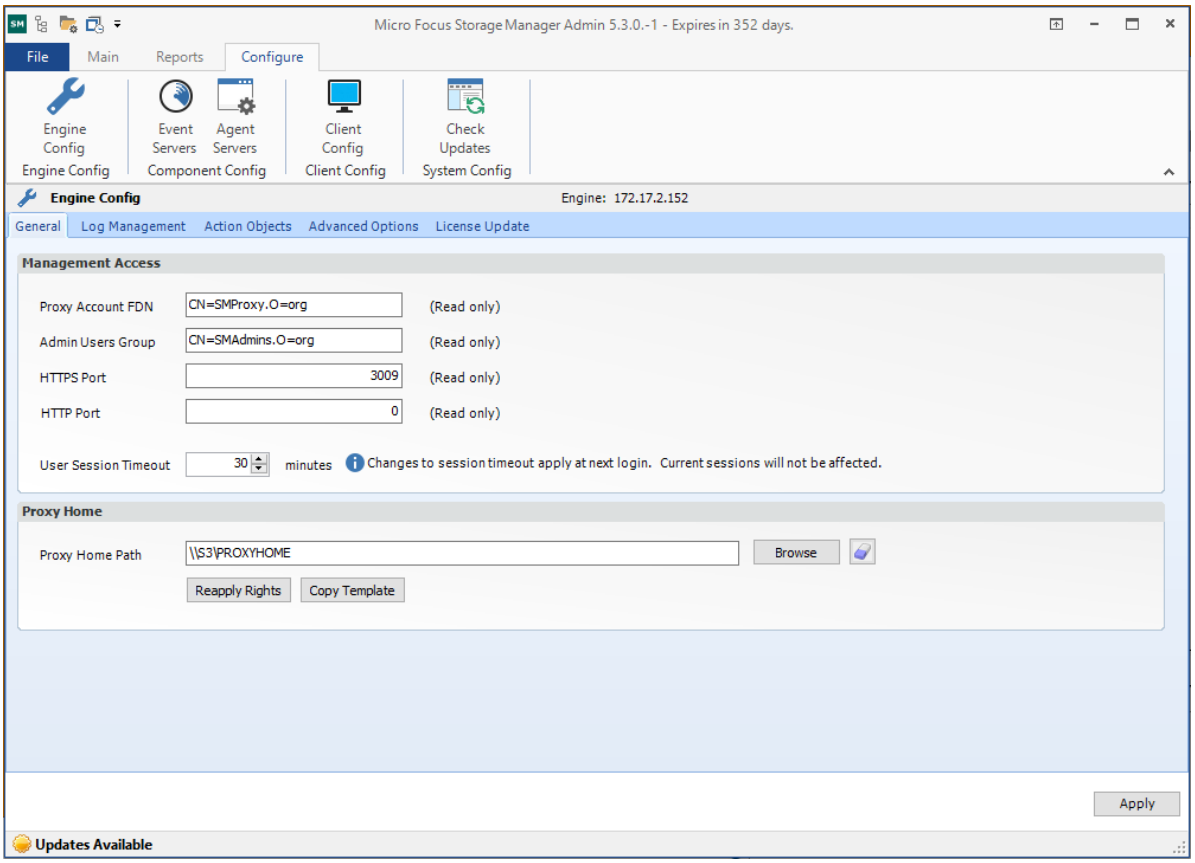
- Section 9.3.1, “Engine Config,” on page 109
- Section 9.3.2, “Event Servers,” on page 114
- Section 9.3.3, “Agent Servers,” on page 115
- Section 9.3.4, “Client Config,” on page 117
- Section 9.3.5, “Check Updates,” on page 119

9.3.1 Engine Config

This page lets you view and set Engine configuration settings.

The **General** tab includes proxy and management access settings. Each of the fields is described below.

Figure 9-15 *Engine Config General Tab Settings*



Proxy Account FDN: Displays the fully distinguished name that you established when you installed Storage Manager for eDirectory.

Admin Users Group: Displays the Admin Users Group that you established during the installation of Storage Manager for eDirectory.

User Session Timeout: Indicates the number of minutes the Admin Client can be left dormant before you need to reauthenticate.

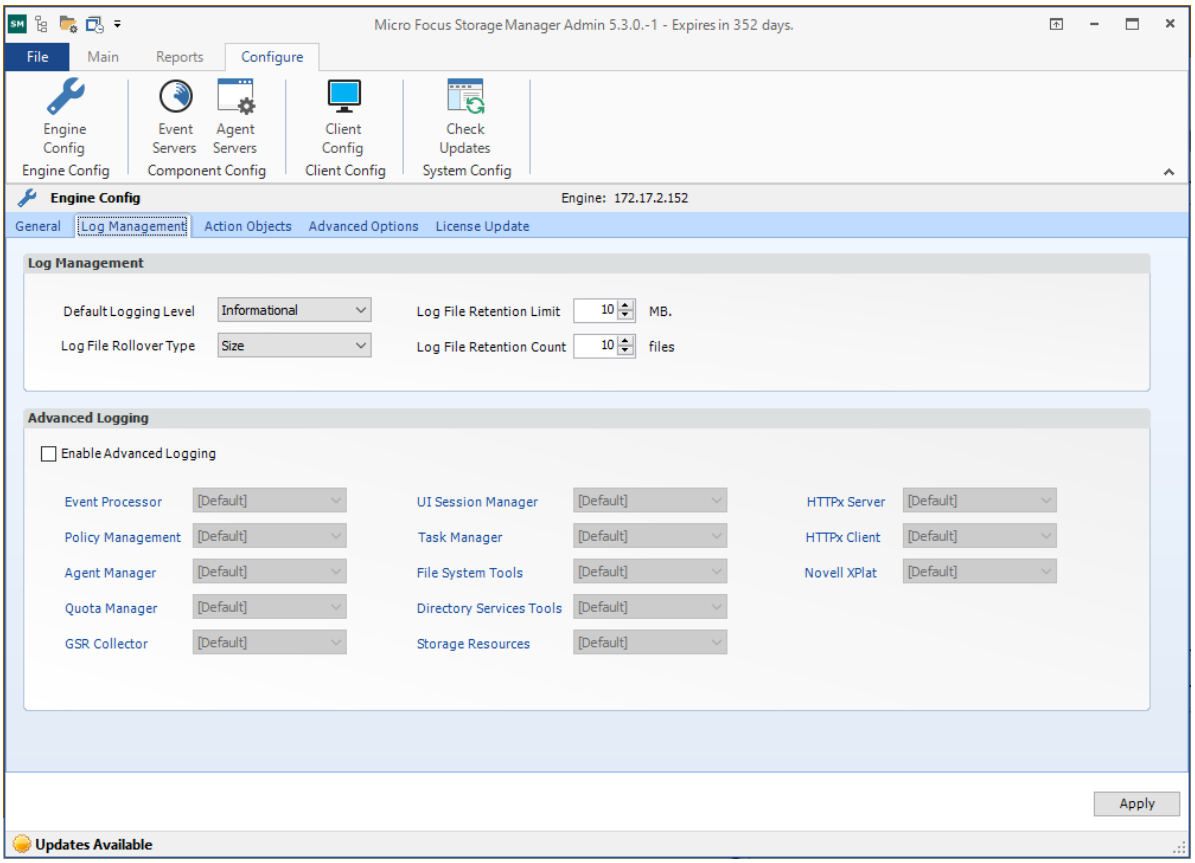
HTTPS Port: Displays the HTTPS port that you chose for Storage Manager for eDirectory when you installed it.

HTTP Port: If you chose to use an HTTP port during the installation of Storage Manager for eDirectory, the HTTP port is displayed here.

Proxy Home Path: This path was established during the installation of the Admin Client. If you need to, you can change the path by using the **Browse** button.

The **Log Management** tab includes settings specific to log files, which are accessible only from the server hosting the Engine. Each of the fields is described below.

Figure 9-16 *Engine Config Log Tab Settings*



Default Logging Level: By default, the log records informational level details. You can change the log to record the level you want. Be aware that some settings, such as debug or verbose, record much more information and can potentially make the log file much larger.

Log File Retention Count: By default, Storage Manager for eDirectory retains the 10 most recent log files, according to the Log File Rollover Type setting. For example, if the **Log File Rollover Type** setting is set to **Daily**, the retained log files are from the last 10 days.

Log File Rollover Type: You can choose whether to have log files roll over daily, hourly, when the log has reached a set size limit, or have no rollover setting. If you select **None**, the same log file is opened each time you start the Engine, and log entries are appended to it.

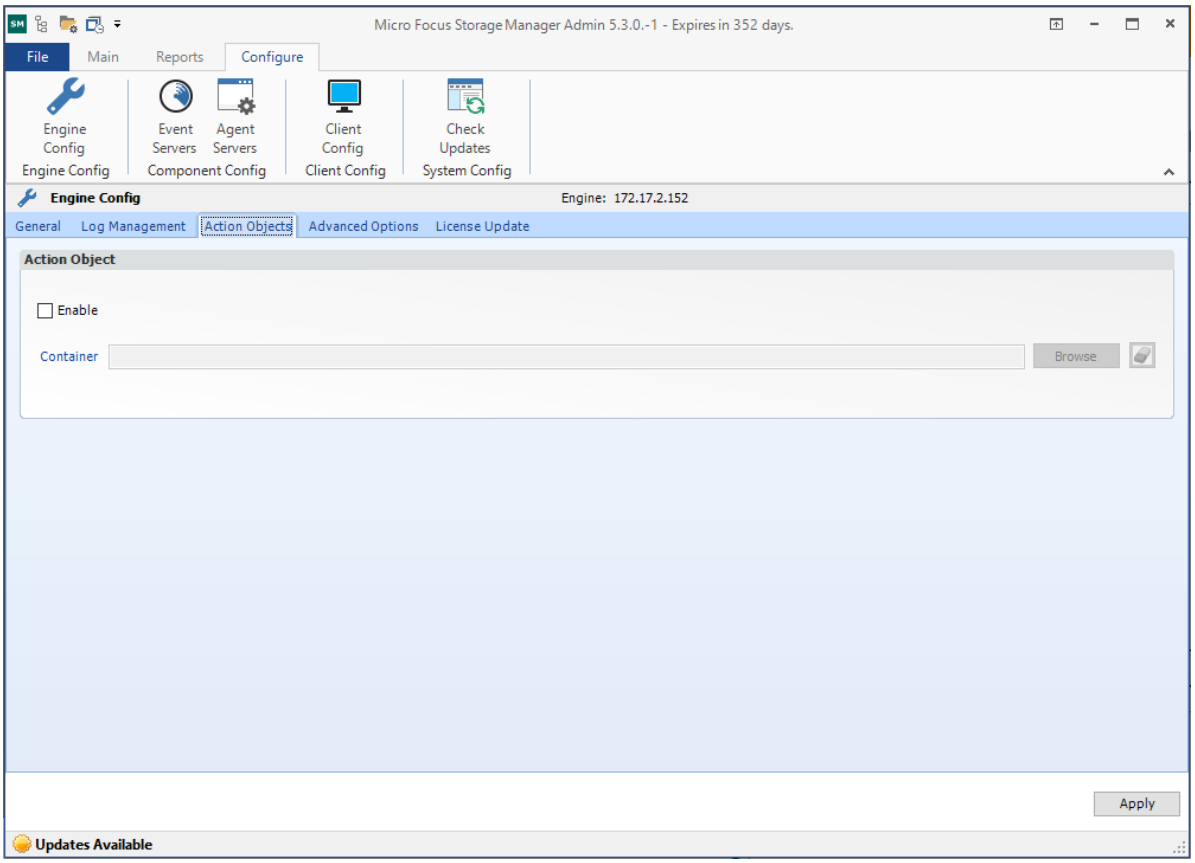
NOTE: If you delete the log file while the Engine is not running, a new log file is created the next time you start the Engine.

Log File Retention Limit: This field appears only when you select **Size** from the **Log File Rollover Type** field. You need to enter the size limit in MB for the log file before it creates a new file.

Enable Advanced Logging: Selecting this check box activates the Advanced Logging region of the page. This region allows you to specify the output of the log file according to the setting you indicate in each of 12 categories.

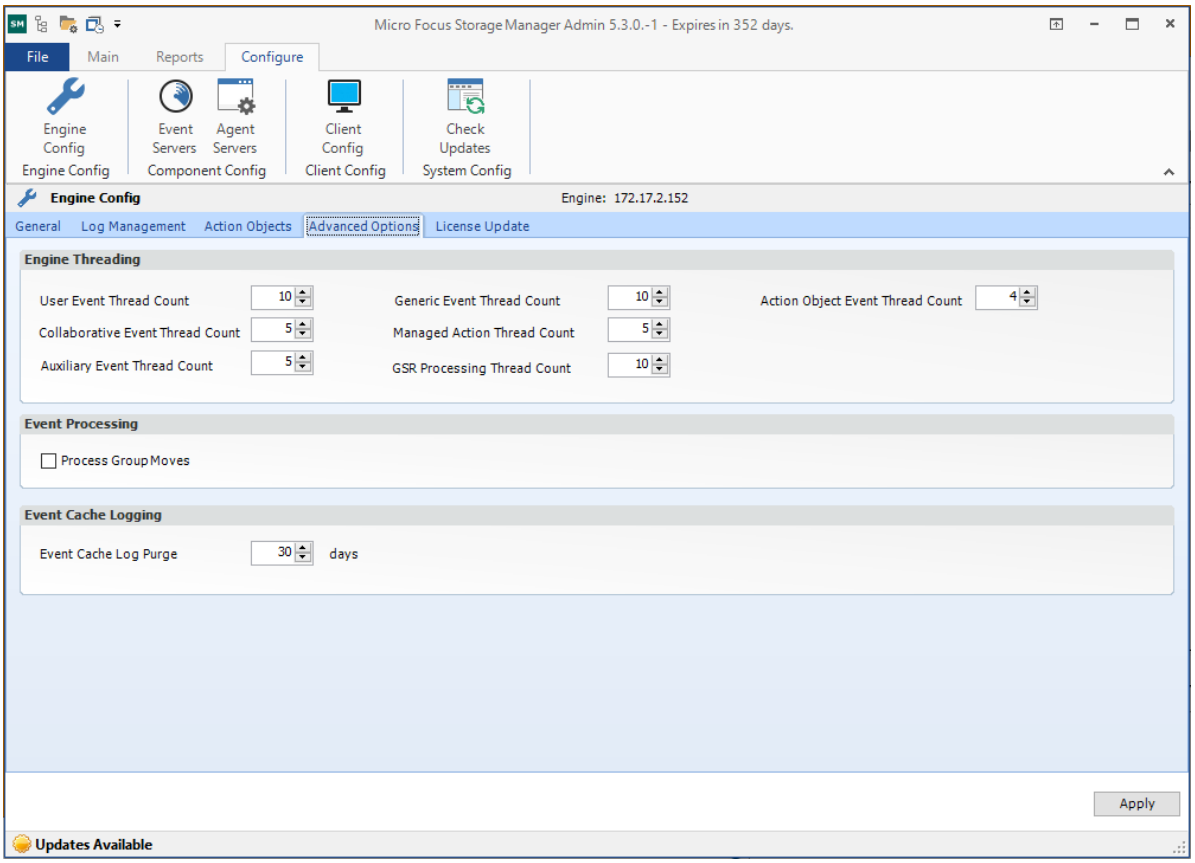
The **Action Objects** tab lets you lets you enable Storage Manager for eDirectory Action Objects by specifying the container where these Action Objects are located.

Figure 9-17 *Engine Config Action Options Tab Settings*



The **Advanced Options** tab lets you view or reconfigure the thread count settings allocated for the actions that Storage Manager for eDirectory performs.

Figure 9-18 *Engine Config Advanced Options Tab Settings*



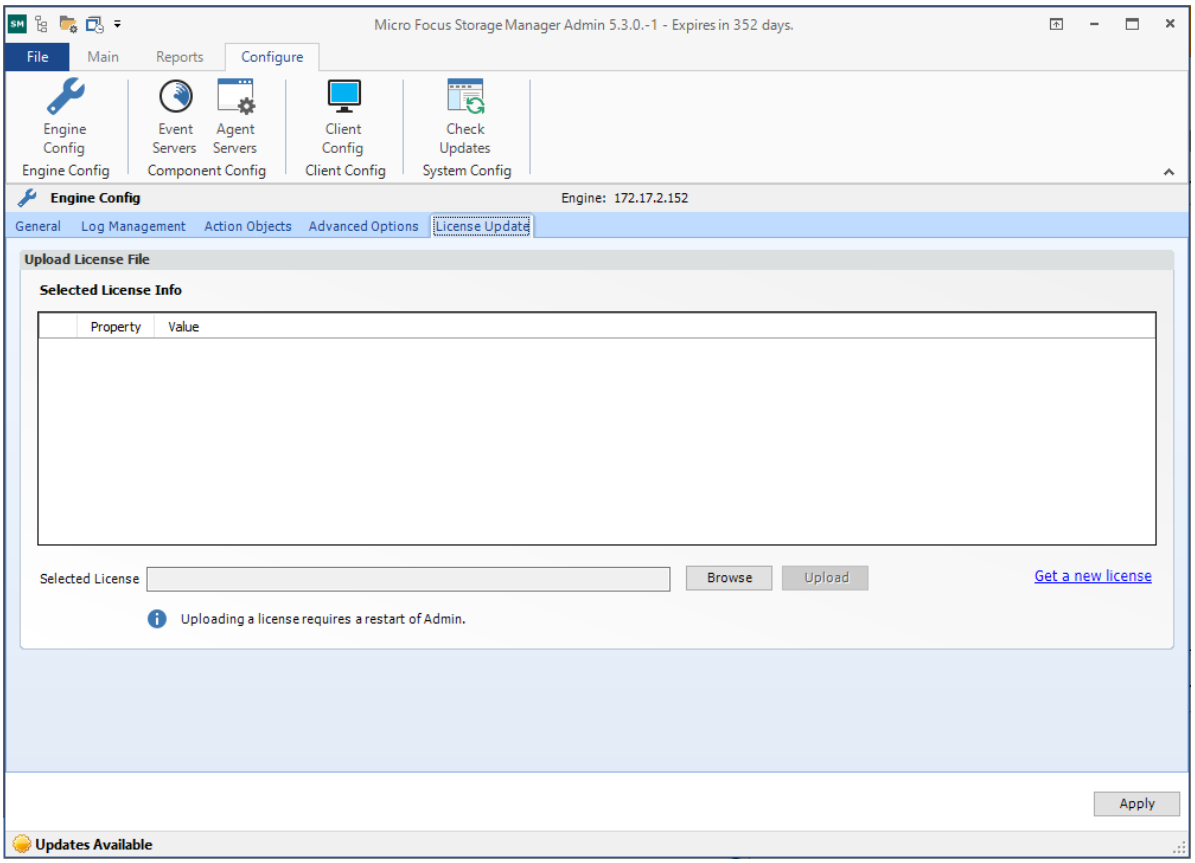
These settings are optimized for a normal Storage Manager for eDirectory workload.

Event Cache Log Purge: By default, Storage Manager for eDirectory keeps the most recent 30 days of event entries in cache. You can adjust the setting in the **Days** field.

The event cache can be helpful in providing you a recent history of all of the events that were sent from the Event Monitor.

The **License Update** tab lets you replace an unexpired license file.

Figure 9-19 *License Update Tab*



Replacing an Unexpired License File

1 Click **Browse** to locate and select the new license file.

2 Click **Upload**.

Replacing an Expired License File

You cannot replace an expired license using the Admin Client. To replace an expired license file:

1 At the server that is hosting the Engine, go to `/etc/opt/novell/storagemanager/engine/config/`.

2 Replace the old `nsm.lic` file with the new one.

9.3.2 Event Servers

The Event Monitor monitors changes to eDirectory based on create, move, rename, and delete events. The host for the Event Monitor is referred to as the Event Server.

The Event Server page lets you:

- Authorize an Event Monitor
- Verify that an Event Monitor is authorized
- View the Event Monitor software version installed

- View Event Monitor statistics
- Remove an Event Monitor

The **Event Count** number indicates the total number of events sent from the Event Monitor to the Engine.

Procedures for authorizing the Event Monitor are located in "Authorizing the Event Monitor"in the *Micro Focus Storage Manager 5.3 for eDirectory Installation Guide*.

Deleting an Event Monitor

Within the Admin Client, you can delete a deauthorized Event Monitor. Only deauthorized Event Monitors can be deleted. If you want to remove an Event Monitor, you must deauthorize it first.

9.3.3 Agent Servers

Agents perform copying, moving, grooming, and vaulting through directives from the Engine. Storage Manager for eDirectory determines which Agent to use based on the target destination of the data or via proxy configuration.

For optimum performance, Agents should be installed on all servers with storage managed by Storage Manager for eDirectory.

NOTE: Storage Manager for eDirectory does not provide NetWare based Agents, NetWare servers or Open Enterprise Server clusters need to be managed by Proxy Agents (see"Proxy Agents" on page 116)

The Agent Server page lets you:

- Authorize an Agent
- Verify that Agents are authorized
- View Agents software versions installed
- View Agent statistics
- Remove an Agent
- Configure a Proxy Agent

Procedures for authorizing an Agent are located in "Authorizing the Agents" of the *Micro Focus Storage Manager 5.3 for eDirectory Installation Guide*.

Deleting an Agent

Within the Admin Client, you can delete a deauthorized Agent. Only deauthorized Agents can be deleted. If you want to remove an Agent, you must deauthorize it first.

NOTE: If an Agent is deauthorized and it hasn't successfully sent a heartbeat within 7 days, it will automatically be removed.

Proxy Agents

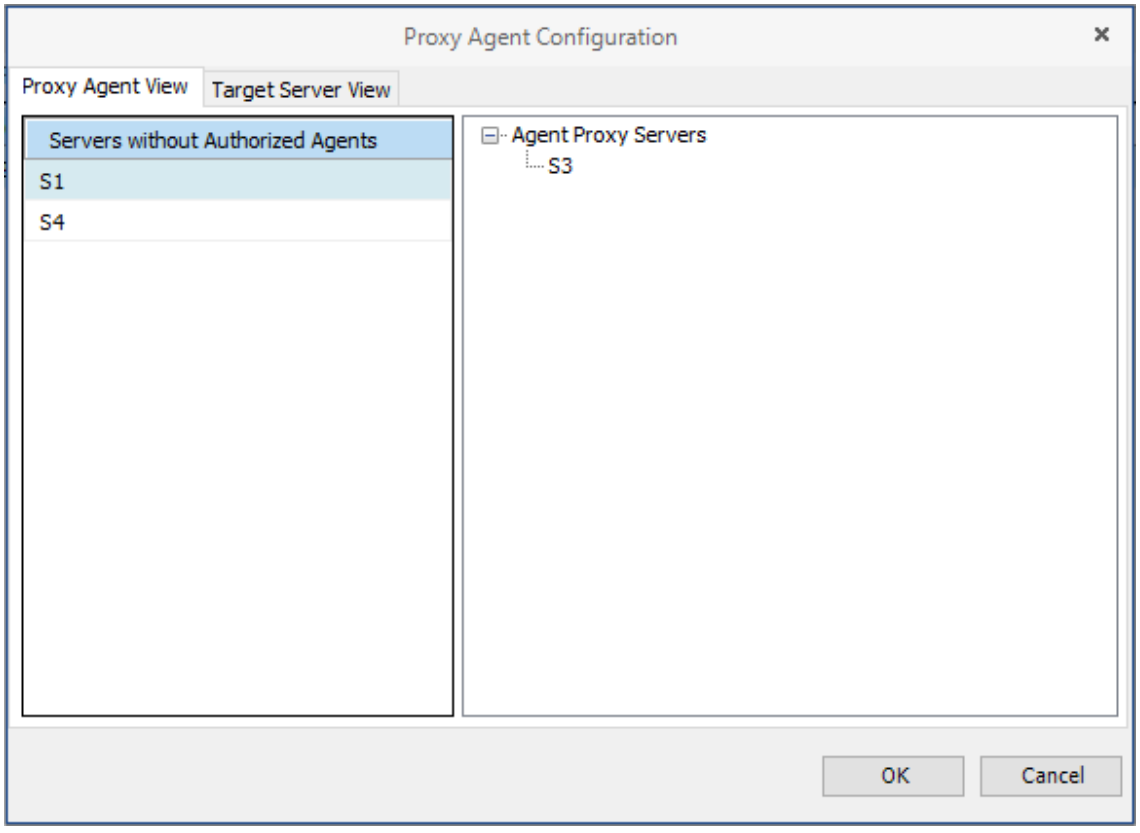
For storage resources that do not or cannot host an Agent, for example a NetWare server, Storage Manager for eDirectory can utilize an Agent running on another server to perform the copying, moving, grooming, and vaulting on the server. In this type of scenario, the Agent is serving as a “Proxy Agent.”

A Proxy Agent can also be set up to reduce the workload on the Engine. For example, a Proxy Agent can be configured for a server on one side of a WAN environment to move data from one server to another on the same side of the WAN link. This keeps the data from crossing the WAN link only to cross back again.

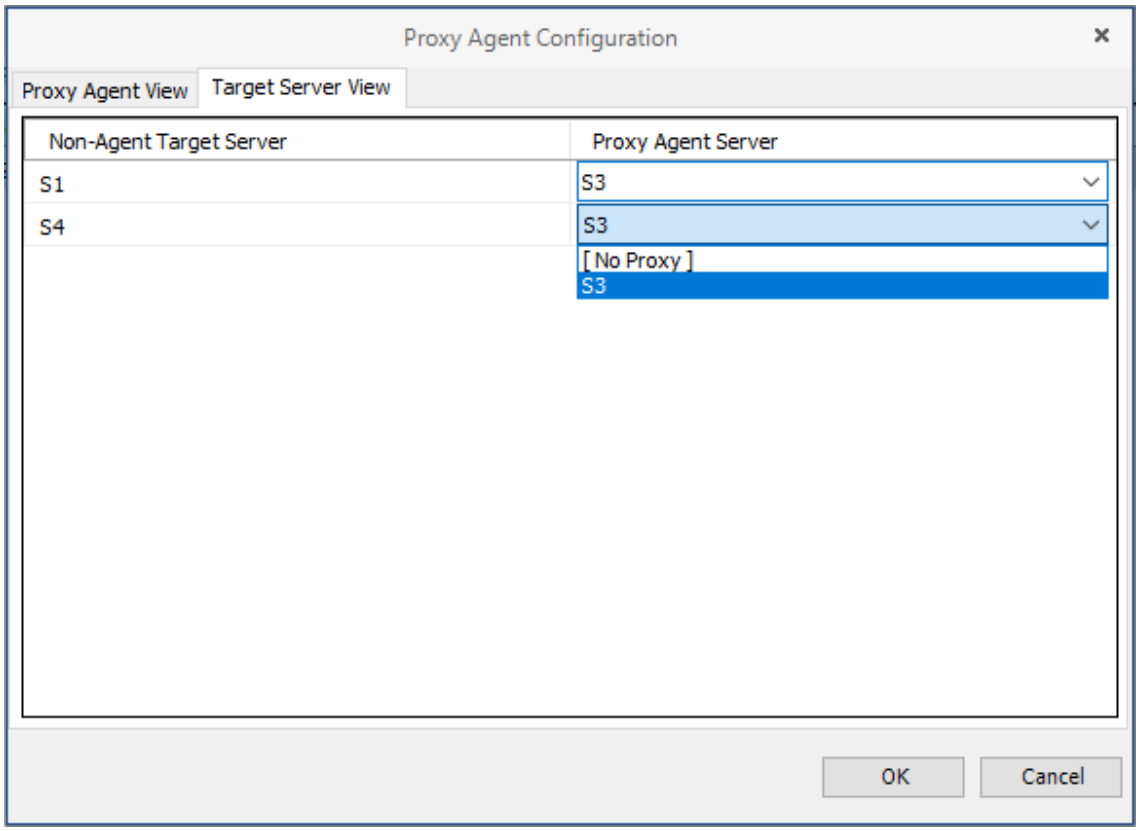
Configuring an Agent to be a Proxy Agent

1. Launch the Admin Client.
2. Click the **Configure** tab.
3. Right-click the Agent you want to authorize to be a Proxy Agent and select **Configure Proxy**.

   The left side of the Proxy Agent Configuration dialog box shows the list of servers without Agents installed. The right side shows the servers with Agents installed. In the example below, the Agent on OES11GM could be set up to be the Proxy Agent for the NW-OES11 and OES11SP2 servers.



4. Click the **Target Server View** tab.
5. From the drop-down list, select the Agent server you want to serve as the Proxy Agent for the server on the left.



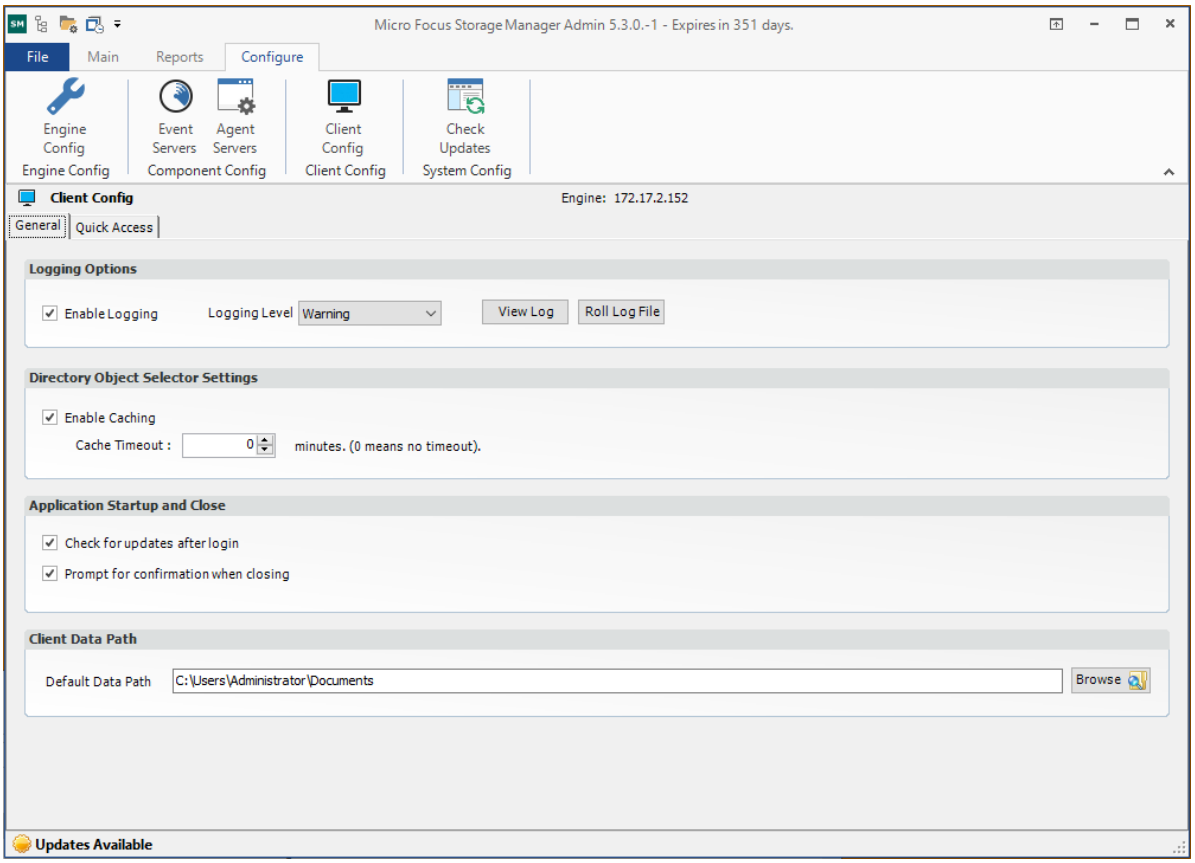
6 Click **OK** to save and close the proxy setting association.

9.3.4 Client Config

This page lets you configure various settings within the Admin Client.

An overview of settings specific to the **General** tab follows the graphic.

Figure 9-20 *Client Config General Tab*



Enable Logging: Selecting this check box enables logging the operations of the Admin Client and lets you specify the logging level and whether to roll the log or close the old log and start a new log.

Logging Level: This drop-down menu lets you select the classification of entry you want logged.

View Log: Clicking this button opens the log file.

Roll Log File: Clicking this button discontinues entries in the current log file and begins a new log file.

Enable Caching: When you are working in the Identity Objects page, selecting this check box enables the Admin Client to maintain the area of the directory tree that is visible in the right pane, if you move from the page to another. For example, if you locate a Group object in a container and then need to move to another page, when you return to the Identity Objects page, you do not need to navigate the directory tree to locate the Group object again.

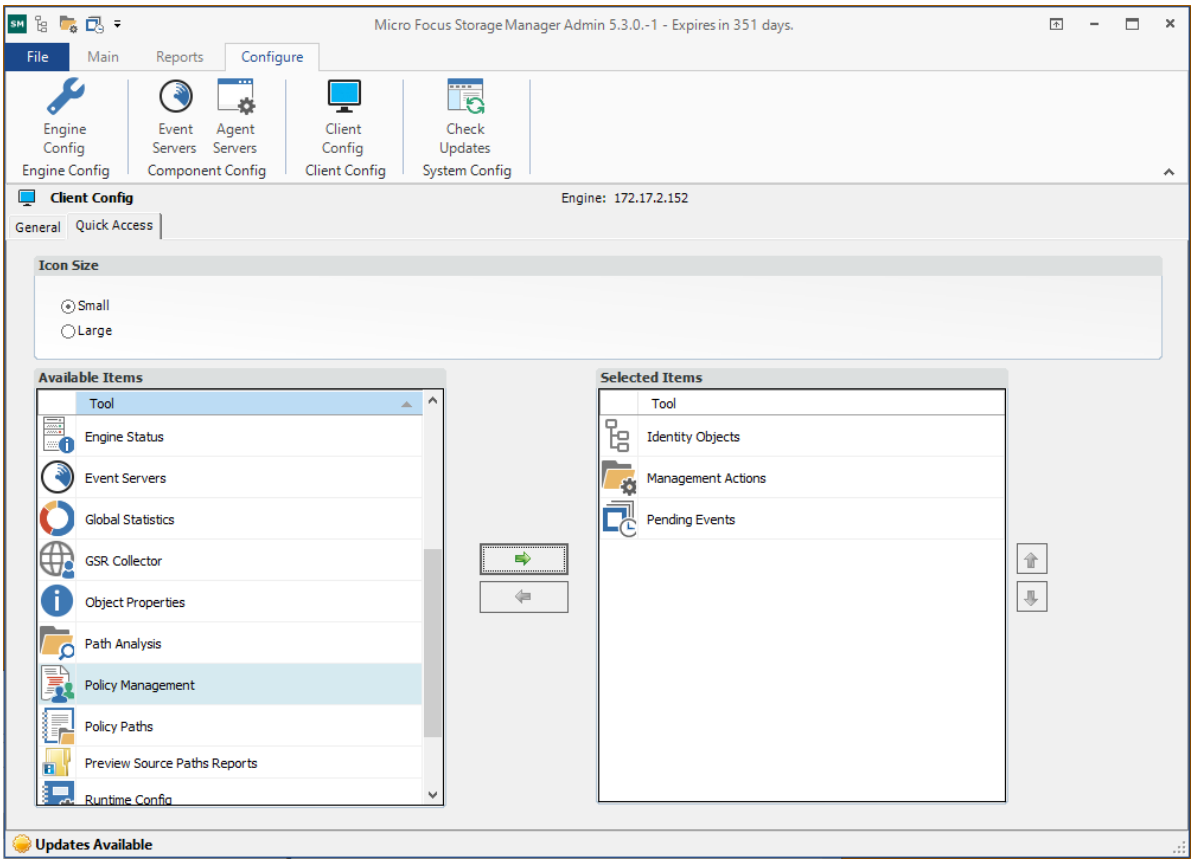
Check for Updates after Login: Selecting this check box allows the Admin Client to notify you of the availability of newer Storage Manager for eDirectory components.

Check for Confirmation When Closing: Selecting this check box prompts you with a confirmation of your choice when you close the Admin Client.

An overview of settings specific to the **Quick Access** tab follows:

This page lets you access the items you use most in the Admin Client from the Quick Access Toolbar. Items can be added or removed from the Quick Access Toolbar by right-clicking the item from its location in the interface, or through the Quick Access page shown below.

Figure 9-21 *Client Config Quick Access Tab*



By default, the Quick Access Toolbar is located in the title bar of the Admin Client, but the location can be changed by using the menu at the end of the Quick Access Toolbar.

A discussion of the settings in the **Advanced** tab follows.

Settings on this page should be changed only under the supervision of Micro Focus Support.

NOTE: Current values on this page are only active during the current session of the Admin Client and are reset when the Admin Client is closed or times out.

Bucket Load Parameters

These parameters are for adjusting the settings for the Engine and the Admin Client during enumeration operations.

9.3.5 Check Updates

This page compares the version numbers of Storage Manager for eDirectory components that you have installed with the latest versions available. It also provides links for downloading the latest versions of each of the components.

A eDirectory Schema Extensions

Storage Manager for eDirectory extends the eDirectory schema by adding thirteen new attributes and three new classes.

A.1 Attributes

A.1.1 cccFSFAction Cleanup

String indicating type of cleanup.

Table A-1 *cccFSFAction Cleanup Specifications*

eDirectory Attribute Property	Value
Name	ccxFSFActionCleanup
ASN.1 ID	2.16.840.1.113719.2.278.4.54.1
Syntax	SYN_CI_STRING
Sized – Lower Limit	-
Sized – Upper Limit	-
Single Valued	True
Sync Immediate	True

eDirectory Attribute Property	Value
Schedule Sync Never	False
Per Replica	False
Public Read	False
Hidden	False
Server Read	False
Write Managed	False

A.1.2 cccFSFactoryActionExecuteTime

Integer representing time_t value for execution.

Table A-2 *cccFSFactoryActionExectuteTime Specifications*

eDirectory Attribute Property	Value
Name	cccFSFactoryActionExecuteTime
ASN.1 ID	2.16.840.1.113719.2.278.4.49.1
Syntax	SYN_INTEGER
Sized – Lower Limit	-
Sized – Upper Limit	-
Single Valued	True
Sync Immediate	True
Schedule Sync Never	False
Per Replica	False
Public Read	False
Hidden	False
Server Read	False
Write Managed	False

A.1.3 cccFSFactoryActionLinkNext

FDN of next action.

Table A-3 *cccFSFactoryActionLinkNext Specifications*

eDirectory Attribute Property	Value
Name	cccFSFactoryActionLinkNext
ASN.1 ID	2.16.840.1.113719.2.278.4.60.1

eDirectory Attribute Property	Value
Syntax	SYN_CI_STRING
Sized – Lower Limit	-
Sized – Upper Limit	-
Single Valued	False
Sync Immediate	True
Schedule Sync Never	False
Per Replica	False
Public Read	False
Hidden	False
Server Read	False
Write Managed	False

A.1.4 cccFSFactoryActionOperation

Name of action operation.

Table A-4 *cccFSFactoryActionOperation Specifications*

eDirectory Attribute Property	Value
Name	cccFSFactoryActionOperation
ASN.1 ID	2.16.840.1.113719.2.278.4.47.1
Syntax	SYN_CI_STRING
Sized – Lower Limit	-
Sized – Upper Limit	-
Single Valued	True
Sync Immediate	True
Schedule Sync Never	False
Per Replica	False
Public Read	False
Hidden	False
Server Read	False
Write Managed	False

A.1.5 cccFSFactoryActionOption

Action options.

Table A-5 cccFSFactoryActionOption Specifications

eDirectory Attribute Property	Value
Name	cccFSFactoryActionOption
ASN.1 ID	2.16.840.1.113719.2.278.4.48.1
Syntax	SYN_CI_STRING
Sized – Lower Limit	-
Sized – Upper Limit	-
Single Valued	True
Sync Immediate	True
Schedule Sync Never	False
Per Replica	False
Public Read	False
Hidden	False
Server Read	False
Write Managed	False

A.1.6 cccFSFactoryActionPath1

Primary path for action.

Table A-6 cccFSFactoryActionPath1 Specifications

eDirectory Attribute Property	Value
Name	cccFSFactoryActionPath1
ASN.1 ID	2.16.840.1.113719.2.278.4.51.1
Syntax	SYN_PATH
Sized – Lower Limit	-
Sized – Upper Limit	-
Single Valued	True
Sync Immediate	True
Schedule Sync Never	False
Per Replica	False
Public Read	False
Hidden	False
Server Read	False
Write Managed	False

A.1.7 cccFSFactoryActionPath2

Secondary path for action.

Table A-7 *cccFSFactoryActionPath2 Specifications*

eDirectory Attribute Property	Value
Name	cccFSFactoryActionPath2
ASN.1 ID	2.16.840.1.113719.2.278.4.52.1
Syntax	SYN_PATH
Sized – Lower Limit	-
Sized – Upper Limit	-
Single Valued	True
Sync Immediate	True
Schedule Sync Never	False
Per Replica	False
Public Read	False
Hidden	False
Server Read	False
Write Managed	False

A.1.8 cccFSFactoryActionResult

Result string.

Table A-8 *cccFSFactoryActionResult Specifications*

eDirectory Attribute Property	Value
Name	cccFSFactoryActionResult
ASN.1 ID	2.16.840.1.113719.2.278.4.56.1
Syntax	SYN_CI_STRING
Sized – Lower Limit	-
Sized – Upper Limit	-
Single Valued	True
Sync Immediate	True
Schedule Sync Never	False
Per Replica	False
Public Read	False

eDirectory Attribute Property	Value
Hidden	False
Server Read	False
Write Managed	False

A.1.9 cccFSFactoryActionStatus

Intermediate status.

Table A-9 *cccFSFactoryActionStatus Specifications*

eDirectory Attribute Property	Value
Name	cccFSFactoryActionStatus
ASN.1 ID	2.16.840.1.113719.2.278.4.55.1
Syntax	SYN_CI_STRING
Sized – Lower Limit	-
Sized – Upper Limit	-
Single Valued	True
Sync Immediate	True
Schedule Sync Never	False
Per Replica	False
Public Read	False
Hidden	False
Server Read	False
Write Managed	False

A.1.10 cccFSFactoryActionTarget

FDN of object related to the action.

Table A-10 *cccFSFactoryActionTarget Specifications*

eDirectory Attribute Property	Value
Name	cccFSFactoryActionTarget
ASN.1 ID	2.16.840.1.113719.2.278.4.58.1
Syntax	SYN_CI_STRING
Sized – Lower Limit	-
Sized – Upper Limit	-

eDirectory Attribute Property	Value
Single Valued	True
Sync Immediate	True
Schedule Sync Never	False
Per Replica	False
Public Read	False
Hidden	False
Server Read	False
Write Managed	False

A.1.11 cccFSFactoryActionTrigger

Specifies triggering of action.

Table A-11 *cccFSFactoryActionTrigger Specifications*

eDirectory Attribute Property	Value
Name	cccFSFactoryActionTrigger
ASN.1 ID	2.16.840.1.113719.2.278.4.73.1
Syntax	SYN_CI_STRING
Sized – Lower Limit	-
Sized – Upper Limit	-
Single Valued	True
Sync Immediate	True
Schedule Sync Never	False
Per Replica	False
Public Read	False
Hidden	False
Server Read	False
Write Managed	False

A.1.12 ccx-FSFAuxiliaryStorage

List of one or more paths pointing to managed auxiliary storage associated with this object.

Table A-12 ccx-FSFAuxiliaryStorage Specifications

eDirectory Attribute Property	Value
Name	ccx-FSFAuxiliaryStorage
ASN.1 ID	1.3.6.1.4.1.35052.1.1.100.1.1
Syntax	SYN_CI_STRING
Sized – Lower Limit	-
Sized – Upper Limit	-
Single Valued	False
Sync Immediate	True
Schedule Sync Never	False
Per Replica	False
Public Read	False
Hidden	False
Server Read	False
Write Managed	False

A.1.13 ccx-FSFManagedPath

Managed home directory attribute for objects (such as groups and containers) that do not inherently have a home directory attribute.

Table A-13 ccx-FSFManagedPath Specifications

eDirectory Attribute Property	Value
Name	ccx-FSFManagedPath
ASN.1 ID	1.3.6.1.4.1.35052.1.1.100.2.1
Syntax	SYN_CI_STRING
Sized – Lower Limit	-
Sized – Upper Limit	-
Single Valued	True
Sync Immediate	True
Schedule Sync Never	False
Per Replica	False
Public Read	False
Hidden	False
Server Read	False

eDirectory Attribute Property	Value
Write Managed	False

A.2 Classes

A.2.1 cccFSFactoryAction

Action object for use with non-policy-based operations.

Table A-14 *cccFSFactoryAction Specifications*

eDirectory Class Property	Value
Name	cccFSFactoryAction
ASN.1 ID	2.16.840.1.113719.2.278.4.101.1
Class Type	Structural
Parent Class	top
Naming Attribute	cn
Mandatory Attributes	cn
Optional Attributes	cccFSFactoryActionCleanup
	cccFSFactoryActionExecuteTime
	cccFSFactoryActionLinkNext
	cccFSFactoryActionOperation
	cccFSFactoryActionOption
	cccFSFactoryActionPath1
	cccFSFactoryActionPath2
	cccFSFactoryActionResult
	cccFSFactoryActionStatus
	cccFSFactoryActionTarget
	cccFSFactoryActionTrigger
Is Container	False
Containment	Organization
	organizationalUnit

A.2.2 ccx-FSFManagedAttributes

Auxiliary class holding common attributes.

Table A-15 *ccx-FSFManagedAttributes Specifications*

eDirectory Class Property	Value
Name	ccx-FSFManagedAttributes
ASN.1 ID	1.3.6.1.4.1.35052.1.1.2.1.1
Class Type	Auxiliary
Parent Class	-
Naming Attribute	-
Mandatory Attributes	-
Optional Attributes	ccx-FSFAuxiliaryStorage
	ccx-FSFManagedPath
Is Container	False
Containment	-

A.2.3 ccx-ProxyAccount

Proxy account for service authentication.

Table A-16 *ccx-ProxyAccount Specifications*

eDirectory Class Property	Value
Name	ccx-ProxyAccount
ASN.1 ID	1.3.6.1.4.1.35052.1.1.1.2.1
Class Type	Structural
Parent Class	top
Naming Attribute	cn
Mandatory Attributes	cn
Optional Attributes	publicKey
	privateKey
	Description
Is Container	False

eDirectory Class Property	Value
Containment	domain
	Locality
	Organization
	organizationalUnit

B Glossary

Associated policy: A policy specifically assigned to a container, group, or user through the Associations settings in the Policy Editor.

Auxiliary policy: A policy associated with a User Home Folder policy that creates auxiliary storage for a user (along with the user home folder that is created from a User Home Folder policy) when a new user is created in eDirectory.

Backfill operation: Previous terminology for what is now known as a “Management Action.”

Blocking policy: A policy designed to block other Storage Manager policies from affecting members of organizational units, members of groups, or even individual users.

Consistency check: This Management Action notifies you of inconsistencies or potential problems pertaining to user and group storage being managed through Storage Manager. These potential problems might be missing storage quotas, inconsistent directory attributes, missing home directories, inconsistent file paths, and more.

Container: An eDirectory object that can contain another object. The term “container” can refer to either an Organization (O) object, or an Organizational Unit (OU) object.

Collaborative storage: A shared storage area where a group of people in an organization can collaborate by accessing files. Storage Manager lets you easily create collaborative storage areas through collaborative storage policies that you can assign to Group objects or to an organizational unit.

Deferred delete event: The scheduled deletion of a managed path, but has not yet taken place because the number of days in the Cleanup Storage parameter of the policy has not been met.

Dynamic Template Processing: Within Storage Manager, the process that creates personal folders in a collaborative storage folder.

Effective policy: A policy that is applied by default to a group, user, or subcontainer when no associated policy is specifically assigned.

Enumeration operation: The process of locating and displaying all objects.

Managed Path: A location that Storage Manager manages in an automated fashion for any of the following: Home folder, Collaborative storage (group and container), and Auxiliary storage.

Management Action: A manual action that allows you to enact a setting from a policy on existing users.

Personal folder: A user-specific folder in a collaborative storage area.

Policy: Rules and settings within Storage Manager that indicate what storage-specific actions to enact when an event in eDirectory takes place. These actions include creating user storage when a new user is added to eDirectory, moving storage when a user is moved from one container to another, and archiving or deleting storage when a user is removed.

Policy weight: When a user is a member of multiple groups and each group has a separate policy, Storage Manager uses this setting to determine which policies to apply. Storage Manager applies the policy with the largest numerical weight.

Primary policy: Previous terminology specific to user-based storage. Because there are so many different types of user-based policies in Storage Manager, this term is now rarely used.

Quota Manager: A Web browser-based management interface for designated users such as help desk administrators or support personnel that enables them to adjust quota on user home folder or collaborative storage areas without needing rights to the file system. Quota Manager can also provide select storage information such as total number of files and file types in a home folder.

Target Path: The path to the network volume where user home folders are hosted.

Template: If you want to have subfolders and documents provisioned in a home folder, auxiliary storage folder, or collaborative storage folder when they are created, you can use an existing path in the file system as a template.

C Documentation Updates

This section contains information about documentation content changes that were made in this *Micro Focus Storage Manager 5.3 for eDirectory Administration Guide* after the release of Storage Manager 5.0 for eDirectory. The changes are listed according to the date they were published.

The documentation for this product is provided on the Web in two formats: HTML and PDF. The HTML and PDF documentation are both kept up-to-date with the changes listed in this section.

If you need to know whether a copy of the PDF documentation that you are using is the most recent, the PDF document includes a publication date on the title page.

The documentation was updated on the following dates:

C.1 June 1, 2020

Based on changes within the interface of the Admin Client, many screen shots were updated.

C.2 July 19, 2016

Based on the re-branding of the product, updates were made to some filenames and paths throughout the manual.