opentext™ | File Dynamics

Administration Guide

Version 24.2

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.

Copyright © 2024 Condrey Corporation. All Rights Reserved.

No part of this publication may be reproduced, photocopied, or transmitted in any fashion with out the express written consent of the publisher.

Condrey Corporation
122 North Laurens St.
Greenville, SC 29601
U.S.A.

http://condrey.co

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

Administration Guide ... ***1***

Version 24.2 ... *1*

Legal Notices ... ***3***

Third Party Systems ... ***5***

Contents ... ***7***

About This Guide ... ***1***

Audience ... *1*

1 - Overview ... ***1***

1.1 - The Directory Service ... *1*

1.2 - Directory Service Events ... *1*

1.3 - Identity-Driven Policies ... *1*

1.4 - Target-Driven Policies ... *2*

1.5 - Engine ... *3*

1.6 - Event Monitor ... *3*

1.7 - File System Agents ... *3*

1.8 - Phoenix Agents ... *3*

2 - Using the Admin Client ... ***5***

2.1 - Launching the Admin Client ... *5*

2.2 - Using the Admin Client Interface ... *5*

3 - Event Monitor Scoping ... ***7***

3.1 - Include and Exclude Scopes ... *7*

3.1.1 - Include ... *7*

3.1.2 - Exclude ... *7*

3.2 - Container Restrictions ... *8*

3.2.1 - Allowed Container Types ... *8*

3.2.2 - Operational Containers ... *8*

3.3 - Configuring the Event Monitor Scope ... *9*

3.4 - Example Scenarios ... *10*

3.4.1 - Include Scope ... 10
3.4.2 - Exclude Scope ... 11
3.4.3 - Include and Exclude Scope ... 12
4 - Managing Existing User Storage ... ***15***
4.1 - Running Consistency Check Reports on Existing Storage ... 15
4.2 - Assigning Missing Home Folder Attributes ... 16
4.3 - Standardizing User Home Folder Attributes ... 18
4.4 - Creating a Blocking Policy ... 18
4.5 - Creating a User Home Folder Policy ... 20
4.6 - Removing a Preexisting Process for Creating User Home Folders ... 26
4.7 - Testing the User Home Folder Policy ... 26
4.8 - Performing a Consistency Check ... 27
4.9 - Running Management Actions ... 28
4.10 - Testing a Rename Event ... 28
4.11 - Testing a Cleanup Rule ... 28
4.12 - What's Next ... 29
5 - Managing User Home Folders ... ***31***
5.1 - Home Folder Management Overview ... 31
5.2 - User Policies ... 31
5.3 - Setting Up a Vault Location ... 32
5.4 - Enabling Your Network for Quota Management ... 32
5.5 - Creating a User Home Folder Policy ... 32
5.5.1 - Setting Policy Options ... 33
5.5.2 - Setting Associations ... 33
5.5.3 - Setting Provisioning Options ... 34
5.5.4 - Setting Target Paths ... 36
5.5.5 - Setting Quota Options ... 38
5.5.6 - Setting the Move Schedule ... 40
5.5.7 - Setting Cleanup Options ... 40
5.5.8 - Setting Vault Rules ... 41

5.5.9 - Setting Groom Rules ... 43
5.5.10 - Notes ... 43
5.5.11 - Summary ... 44
5.6 - Creating a User Profile Path Policy ... 44
5.6.1 - Create the Policy ... 44
5.7 - Creating a User Remote Desktop Services Home Folder Policy ... 45
5.7.1 - Create the Policy ... 46
5.8 - Creating a User Remote Desktop Services Profile Path Policy ... 47
5.8.1 - Create the Policy ... 47
5.9 - Using a Policy to Manage Inactive Users ... 49
5.9.1 - Creating an Inactive Users Organizational Unit ... 49
5.9.2 - Creating an Inactive Users Folder ... 49
5.9.3 - Creating an Inactive Users Policy ... 49
5.9.4 - Setting Inactive Users Policy Associations ... 50
5.9.5 - Setting Inactive Users Policy Provisioning Options ... 50
5.9.6 - Setting Inactive Users Policy Target Paths ... 50
5.9.7 - Setting Inactive Users Policy Cleanup Options ... 51
5.10 - Copying Policy Data ... 51
5.11 - Using a Policy to Manage Auxiliary Storage ... 52
5.11.1 - Creating an Auxiliary Storage Policy ... 53
5.11.2 - Linking a User Home Folder Policy to an Auxiliary Storage Policy ... 55
5.11.3 - Provisioning Auxiliary Storage for Existing Users ... 55
5.11.4 - Establishing Auxiliary Purpose Mappings ... 56
5.12 - Exporting Policies ... 57
5.13 - Importing Policies ... 58
6 - Managing Existing Collaborative Storage ... ***61***
6.1 - Assigning a Managed Path to Existing Group-based or Container-based Storage 61
6.2 - Creating a Collaborative Storage Policy ... 64
6.3 - Performing Management Actions ... 67
6.4 - Editing Collaborative Storage Policies ... 68

7 - Managing Collaborative Storage ... ***69***
7.1 - Creating Collaborative Storage Objects in Active Directory ... *69*
7.2 - Understanding Collaborative Storage Templates ... *70*
7.3 - Determining How You Want to Structure Your Collaborative Storage ... *70*
7.4 - Creating a Collaborative Storage Template ... *72*
7.5 - Setting Up Security for a Collaborative Storage Template ... *72*
7.5.1 - Establishing Permissions ... *76*
7.5.2 - Configuring Permissions for the Group Manager ... *76*
7.5.3 - Configuring Permissions for the Group Members' Personal Folders ... *77*
7.5.4 - Configuring Group Member Permissions to Other Folders ... *77*
7.6 - Understanding Collaborative Storage Policies ... *78*
7.7 - Creating a Group Collaborative Storage Policy ... *78*
7.7.1 - Setting Group Collaborative Storage Policy Options ... *79*
7.7.2 - Setting Group Collaborative Storage Policy Associations ... *79*
7.7.3 - Setting Group Collaborative Storage Policy Provisioning Options ... *80*
7.7.4 - Setting Group Collaborative Storage Policy Target Paths ... *81*
7.7.5 - Setting Group Collaborative Storage Policy Quota Options ... *83*
7.7.6 - Setting the Group Collaborative Storage Policy Move Schedule ... *85*
7.7.7 - Setting Group Collaborative Storage Policy Dynamic Template Processing ... *85*
7.7.8 - Setting Group Collaborative Storage Policy Cleanup Options ... *87*
7.7.9 - Setting Group Collaborative Storage Policy Vault Rules ... *87*
7.7.10 - Setting Group Collaborative Storage Policy Groom Rules ... *89*
7.8 - Creating a Container Collaborative Storage Policy ... *90*
7.8.1 - Setting Container Collaborative Storage Policy Options ... *90*
7.9 - Creating a Multi-Principal Collaborative Storage Policy ... *92*
7.9.1 - Multi-Principal Collaborative Storage Policy Overview ... *92*
7.9.2 - Group Naming Parameters ... *92*
7.9.3 - Multi-Principal Collaborative Policies ... *93*
7.9.4 - Multi-Principal Collaborative Events ... *93*
7.9.5 - Create a Multi-Principal Collaborative Storage Policy ... *93*

8 - Using Quota Manager ... ***105***
8.1 - Quota Management Prerequisites ... *105*
8.2 - Managing Quotas Through Quota Manager ... *106*
8.3 - Understanding Quota Manager Status Indicators ... *108*
9 - Creating Target-Driven Policies ... ***109***
9.1 - Target-Driven Policy Types ... *109*
9.1.1 - Content Control Policies ... *109*
9.1.2 - Data Location Policies ... *109*
9.1.3 - Workload Policies ... *109*
9.1.4 - Target-Driven Security Policies ... *110*
9.1.5 - Target-Driven Security Policy Types ... *110*
9.2 - Create a Groom Policy ... *111*
9.2.1 - Creating an Action Block for the Groom Policy ... *111*
9.2.2 - Creating a Groom Policy ... *112*
9.3 - Create a Copy Policy ... *115*
9.4 - Create a Move Policy ... *119*
9.5 - Create a Workload Policy ... *121*
9.5.1 - Workload Policy Example Scenario ... *122*
9.5.2 - Creating a Workload Policy ... *122*
9.5.3 - Remediating Using the Data Owner Client ... *124*
9.6 - Create a Security Notification Policy ... *125*
9.6.1 - How Security Notification Policy Reporting Works ... *125*
9.6.2 - Creating a Security Notification Policy ... *126*
9.6.3 - Editing a Security Notification Policy and Resetting the Baseline ... *128*
9.7 - Create a Security Lockdown Policy ... *130*
9.7.1 - Creating a Security Lockdown Policy ... *130*
9.7.2 - Editing a Security Lockdown Policy and Resetting the Baseline ... *133*
9.8 - Create a Security Fencing Policy ... *134*
9.8.1 - Creating a Security Fencing Policy ... *134*
9.8.2 - Editing a Security Fencing Policy and Resetting the Baseline ... *138*

9.9 - Executing a Security Scan ... 140
9.10 - Viewing Security Notifications ... 140
10 - Work Log Reports ... ***143***
10.1 - Work Log Reports Overview ... 143
10.1.1 - Restrictions ... 143
10.1.2 - Database ... 143
10.1.3 - Configuration ... 143
10.2 - Establishing the Work Log Database Settings in the Admin Client ... 144
10.3 - Building Work Log Reports ... 145
10.3.1 - Loading Work Log Entries ... 146
10.3.2 - Setting the Work Log Scope ... 148
10.3.3 - Data View Options ... 149
10.3.4 - Build a Work Log Report ... 153
10.3.5 - Saving a View ... 153
10.3.6 - Exporting a Work Log Report ... 154
11 - Reference ... ***155***
11.1 - Home Tab ... 155
11.1.1 - Status ... 155
11.1.2 - Runtime Config Report ... 155
11.1.3 - Path Analysis ... 156
11.1.4 - Scheduled Tasks ... 156
11.1.5 - Storage Resources ... 160
11.1.6 - Forest Trusts ... 162
11.1.7 - Agents ... 163
11.1.8 - Event Monitors ... 166
11.1.9 - Event Scope ... 167
11.1.10 - Check Updates ... 167
11.2 - Identity-Driven Tab ... 167
11.2.1 - Statistics ... 167
11.2.2 - Identity Objects ... 168

11.2.3 - Policies ... 176
11.2.4 - Action Blocks ... 178
11.2.5 - Management Actions ... 189
11.2.6 - Pending Events ... 195
11.2.7 - Consistency Check ... 197
11.2.8 - Management Action Reports ... 198
11.2.9 - Policy Paths ... 199
11.2.10 - Work Log ... 200
11.2.11 - Global Statistics Collector ... 200
11.2.12 - Global Statistics ... 202
11.2.13 - Anomaly Reports ... 203
11.3 - Target-Driven Tab ... 211
11.3.1 - Policies ... 211
11.3.2 - Policy Schedules ... 229
11.3.3 - Action Blocks ... 230
11.3.4 - Jobs ... 230
11.3.5 - Security Notifications ... 231
11.4 - Configuration Tab ... 233
11.4.1 - General Preferences ... 234
11.4.2 - Global Statistics Configuration ... 236
11.4.3 - Work Log Configuration ... 240
11.4.4 - Target-Driven Configuration ... 242
11.4.5 - Client Preferences ... 243
Appendix A - Security Specifications ... ***245***
A.1 - Firewall Requirements ... 245
A.1.1 - Windows Firewall ... 245
A.1.2 - Other Services ... 246
A.2 - LSA Rights and Privileges ... 246
A.2.1 - Engine Server ... 247
A.2.2 - Event Monitor Server ... 248

A.2.3 - Agent Server ... 248
A.2.4 - File Share Server ... 249
A.3 - Proxy Rights Group Permissions ... 249
A.3.1 - Windows Servers ... 249
A.3.2 - NAS File Servers ... 249
A.3.3 - Active Directory ... 250
A.4 - Windows Clustering ... 251
Appendix A - NAS Device Considerations ... ***252***
A.5 - NetApp Filer ... 252
A.6 - PowerScale OneFS ... 252
A.7 - Other NAS Devices ... 252
Appendix B - Distributed File System (DFS) ... ***253***
B.1 - Configuring DFS Folders ... 253
B.2 - Providing Only One Target Per DFS Link ... 253
B.3 - Disabling All But One Target Per DFS Link ... 254
B.4 - Enabling Multiple Target Paths ... 254
Appendix C - File Server Resource Manager ... ***257***
C.1 - Installing File Server Resource Manager ... 257
Appendix D - Active Directory Schema Extensions ... ***261***
D.1 - Attributes ... 261
D.1.1 - ccx-FSFAuxiliaryStorage ... 261
D.1.2 - ccx-FSFManagedPath ... 262
D.2 - Classes ... 262
D.2.1 - ccx-FSFManagedAttributes ... 262
Appendix E - Managed Path Naming Attribute Specifications ... ***265***
E.1 - Rules ... 265
E.1.1 - General ... 265
E.1.2 - Groom and Vault Paths ... 266
E.2 - Event Processing ... 266
E.3 - Management Actions ... 267

Appendix F - Glossary ***269***

About This Guide

This administration guide is written to provide the conceptual and procedural information for managing network-stored unstructured data using File Dynamics 24.2.

Audience

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

1 - Overview

File Dynamics is a product designed to address the ever-changing definition and requirements of network data management. With File Dynamics, you have the means to not only provision, manage, and dispose of network storage, but also to rectify the location of sensitive files, monitor and enforce file system permissions located on high-value targets within the network file system, and much more.

File Dynamics performs network file system management tasks standard Microsoft network components such as the Active Directory, along with added components. All of these are summarized in the links below.

1.1 - The Directory Service

Microsoft Active Directory stores the identity information about the users and groups that File Dynamics manages. When File Dynamics is installed it adds or modifies user and group attributes so that they can be managed through File Dynamics.

1.2 - Directory Service Events

When a user in Active Directory is added, moved, renamed, or deleted, it is known as a directory “event.”

1.3 - Identity-Driven Policies

Identity-Driven policies within File Dynamics indicate what user or group actions to enact when an event in Active Directory takes place or a Management Action is invoked by an administrator.

Automated actions include creating user or collaborative storage when a new user is added to Active Directory, 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.

Examples of invoked Management Actions include retroactively applying policies, permissions, attributes, and quotas to existing user storage, or performing some administrative corrective action or operation on a large set of users, groups, or containers.

File Dynamics lets you create the following types of Identity-Driven policies:

- **User Home Folder:** Manages the life cycle of the users’ home folder from the create, rename (name change), move (change in departments), and delete (deprovisioning with vaulting).
- **User Profile Path:** Manages the users’ Windows profile path.
- **User Remote Desktop Services Home Folder:** Manages the users’ remote desktop home folder.

- **User Remote Desktop Services Profile Path:** Manages the users' remote desktop profile path.
- **Container:** Manages storage for all of the users in an Active Directory container.
- **Group:** Manages storage for an Active Directory group.
- **Auxiliary:** Manages one or more additional storage locations in association with one of the four user policy types.
- **Multi-Principal Group Storage:** Allows for multiple groups to access a shared group folder, with each group having different sets of permissions to the group folder.

1.4 - Target-Driven Policies

Through Target-Driven policies, File Dynamics performs management tasks through policies associated directly with a network share or folder. Target-Driven policies include Data Location policies, Content Control policies, and Workload policies.

- **Data Location Policies:** These policies are the means of copying folders and their contents to a target parent folder. There is an option to remove the files from the source location after they have been copied. For example, if you were doing a server consolidation or moving data from a server to a NAS device (or vice versa), you could easily do so using Data Location policies.
- **Content Control Policies:** Similar to Identity-Driven file grooming, Target-Driven Content Control policies remove files according to file type, age, size, last accessed date, and more. From any file path, you can either vault files to a new location or delete the files altogether. For example, you could use this feature to easily delete temporary files and, in the process, make much more disk space available on your storage devices.
- **Workload Policies:** These policies provide the ability to import externally-generated files, such as security reports from OpenText File Reporter, and then rectify the location of sensitive files for regulatory compliance or optimization.
- **Security Notification Policies:** These policies enable administrators to be notified of any changes in access permissions to high-value targets paths. These changes in permissions include a user being given a new or updated permission to a specific folder, or a user being granted access permissions to a folder by being added to a group. Access permission updates are determined by the Phoenix Agent through a scheduled scan. Notifications are sent to administrators via email or viewed through the Data Owner client interface.
- **Lockdown Policies:** Once you have established the proper access permissions for a high-value target, you can establish the baseline of access permissions for the target path that will be strictly enforced through a Lockdown policy. When unauthorized access permission changes are made to the target path or any of its subfolders, the new permissions are removed and the original permissions are restored.
- **Fencing Policies:** These policies let you set limits on how access permissions may change over time. Using a set of criteria to define a "fence," the policy specifies Active Directory containers, users, or groups that might conceivably be given permissions to

a high-value target path in the future without an issue or should never be given permissions in the future.

1.5 - Engine

The Engine performs actions based on events in Active Directory and the defined File Dynamics policies. These actions include provisioning, moving, grooming, deleting, renaming, and archiving and recovering files and permissions. There is only a single Engine per forest and it can be installed on a domain controller or a member server. The Engine runs as a service on Windows.

1.6 - Event Monitor

The Event Monitor monitors changes to Active Directory based on create, move, rename, delete, add member to group, and delete user from group events. You install one Event Monitor per domain, and it can run on a domain controller or a member server. If you install the Event Monitor on a domain controller, the Event Monitor always monitors the local server for changes in the domain. If the Event Monitor is installed on a member server, it identifies the closest available domain controller and monitors it for changes in the domain. The Event Monitor runs as a service on Windows.

1.7 - File System Agents

File System 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 File Dynamics. The File System Agent runs as a service on Windows.

1.8 - Phoenix Agents

The Phoenix Agent is responsible for all security scanning and remediation required by the Security Lockdown and Security Fencing policies. The Phoenix Agent runs as service on Windows.

2 - Using the Admin Client

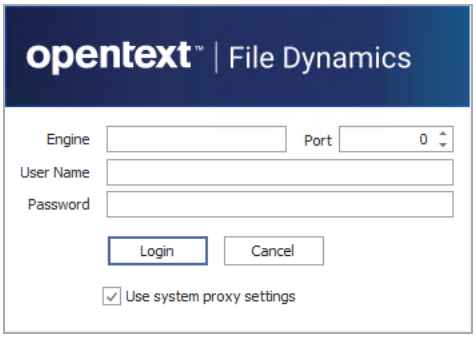
The Admin Client is the administrative interface for File Dynamics. Most management tasks run from this easy-to use Windows application. The Admin Client requires .NET 8.0 which is installed automatically on the Windows workstation or server during the Admin Client installation.

If you have not yet installed the Admin Client, install it before proceeding with this section. See Installing the Admin Client in the *File Dynamics 24.2 Installation Guide* for instructions.

For detailed information on the interaction between the Admin Client and the database, review .

2.1 - Launching the Admin Client

1. Double-click the *File Dynamics 6 Admin* icon from the Windows desktop.
2. An authentication dialog box appears.

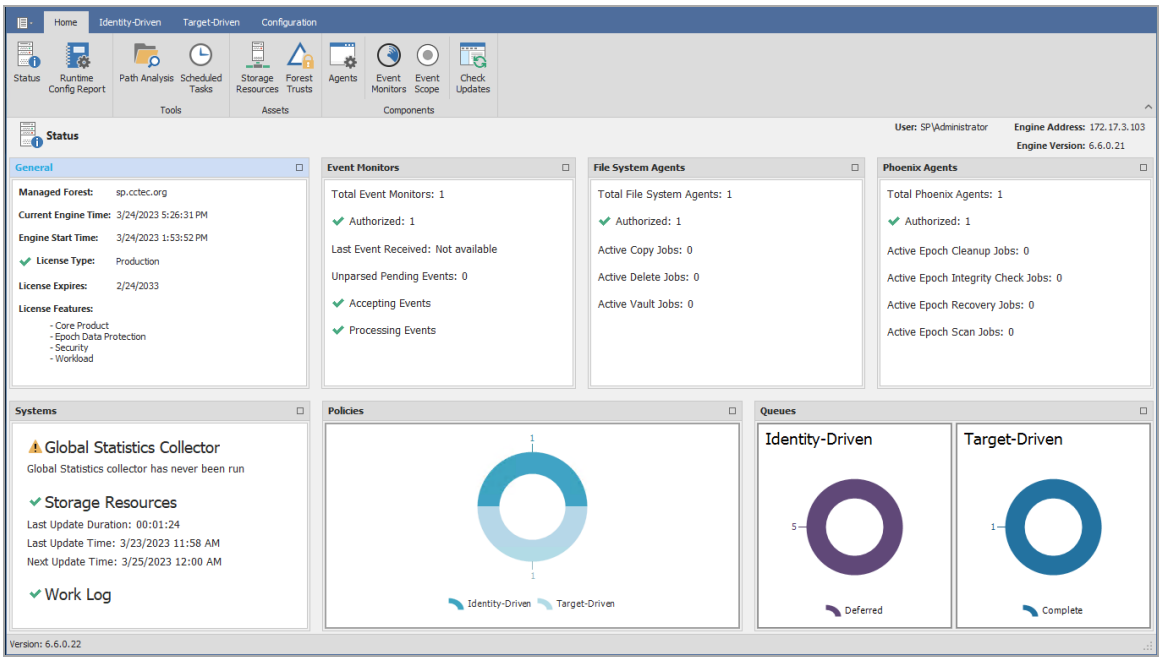


3. In the *Engine* field, specify the DNS name or IP address where the Engine service is installed.
4. In the *Port* field, specify the secure port number.
5. The default setting is 3009.
6. Specify the username and password.
7. The user must be a member of the File Dynamics Admins group to be able to log in.
8. Click *Login*.

2.2 - Using the Admin Client Interface

The Admin Client interface has multiple tabs. 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 Status page from the *Home* tab, which is discussed in detail in the *Reference (page 155)* chapter of this guide.



All other File Dynamics tools are covered in the other sections of this guide.

3 - Event Monitor Scoping

The Event Monitor scope identifies the portions of an Active Directory environment that are relevant for event monitoring purposes. You can define a scope using Include and Exclude lists to limit events only to appropriate containers and groups.

3.1 - Include and Exclude Scopes

You can define an Event Monitor scope by adding container and group objects to the Include and Exclude lists. By default there are no entries in either list so each domain and all of its objects are implicitly included where you have installed and configured an Event Monitor.

The following rules govern the behavior of items in the lists:

- Adding a container to a list affects all descendents of that container's subtree, not just immediate child objects.
- If the scope is defined only by container Includes, the remainder of the AD domain is implicitly excluded.
- If the scope is defined only by container Excludes, the remainder of the AD domain is implicitly included.
- You can only add groups to the Exclude list.
- Rules only apply within the context of a single domain. You may need to add additional rules for other domains to achieve the desired scope.

NOTE: You can override entries in the Include list by specifying subordinate items in the Exclude list, but the Event Scope does not support the opposite. You cannot override entries in the Exclude list.

3.1.1 - Include

The Include list provides a means for creating a whitelist for the specified objects. Anything not contained within the Include list is implicitly excluded.

Containers

Add containers to the Include list to limit the scope to those containers and their subordinate objects.

3.1.2 - Exclude

The Exclude list provides a means for creating a blacklist for specified objects. Anything not contained within the Exclude list is implicitly included.

Containers

Add containers to the Exclude list to prevent event reporting for those containers and their subordinate objects.

Groups

Add groups to the Exclude list to prevent event reporting for those groups.

NOTE: Setting the Event Scope to exclude either a group or its members will prevent monitoring of that groups membership. The same applies to group managers.

3.2 - Container Restrictions

3.2.1 - Allowed Container Types

Only the following container class types are permitted for Include and Exclude scopes:

- container
- country
- locality
- organization
- organizationalUnit

3.2.2 - Operational Containers

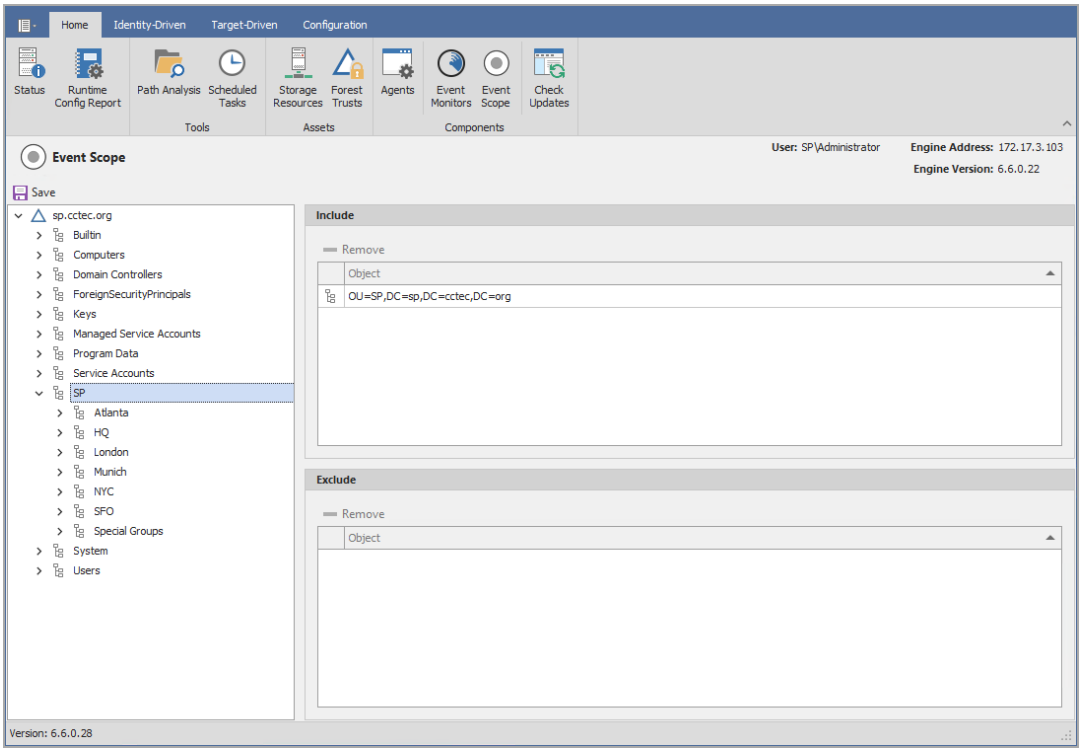
Certain operational portions of an AD domain are considered to be off-limits for event monitoring activities. These portions of an AD domain will always be excluded from consideration for event monitoring purposes regardless of the scope.

The Event Monitor never monitors activity in the following Active Directory containers:

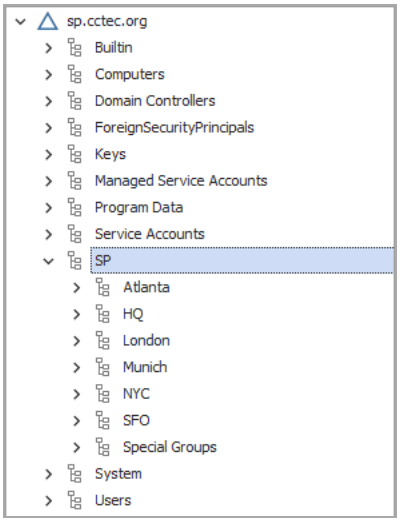
- Builtin
- Foreign Security Principals
- Lost and Found
- Managed Service Accounts
- NTDS Quotas
- Program Data
- System

3.3 - Configuring the Event Monitor Scope

1. In the Admin Client, click the *Home* tab.
2. Click Scope.



3. In the *Scope* pane, click the arrow to view the Active Directory containers.



4. Drag to containers, subcontainers, and groups you want to include or exclude into the

Include and *Exclude* panels respecitively.

Action	Result
Drag one or more containers to the *Include* pane.	The Event Monitor will only report on the selected containers and their subordinate objects and ignore all other objects in the domain.
Drag one or more containers or groups to the *Exclude* pane.	The Event Monitor will ignore the selected containers, their subordinate objects and selected groups, but continue to process events for other objects in the domain.

5. Click *Apply*.

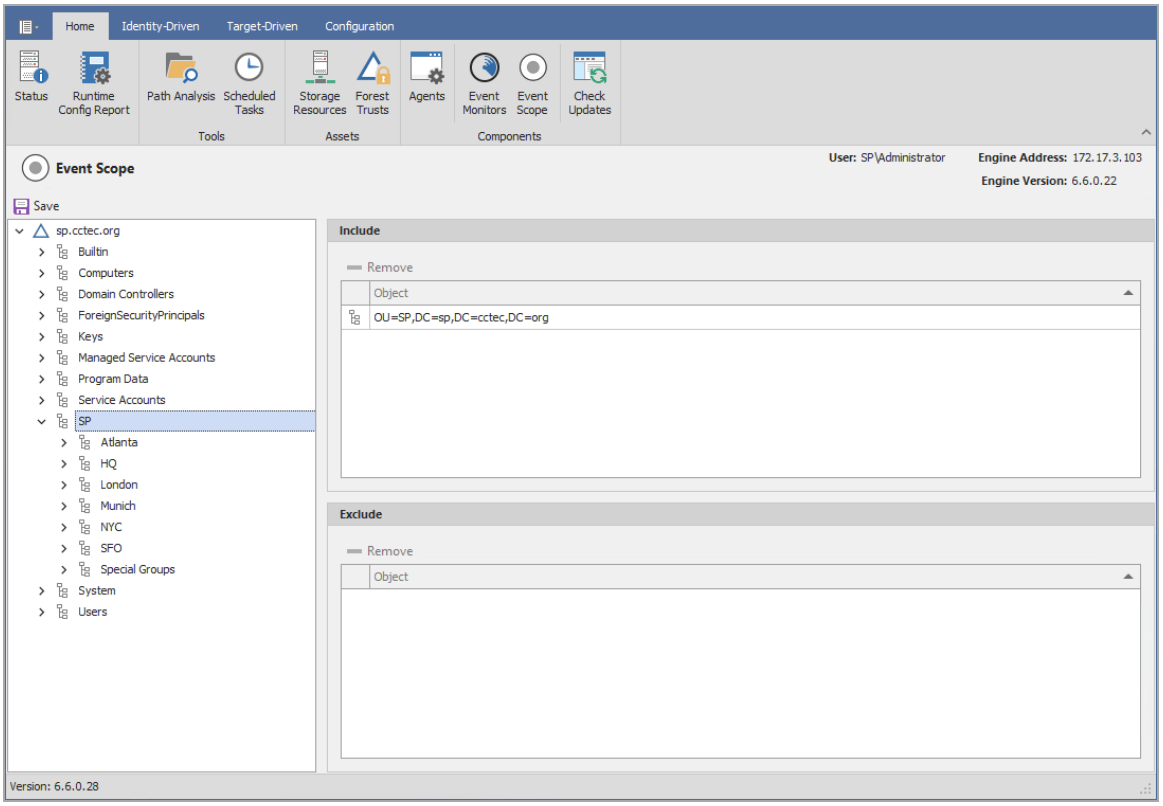
3.4 - Example Scenarios

The following are example scenarios of Event Monitor scoping that might help you configure your Event Monitor scope.

3.4.1 - Include Scope

In the following example the Event Monitor will monitor only the events that belong to the *OU=SP* container or any of its descendants.

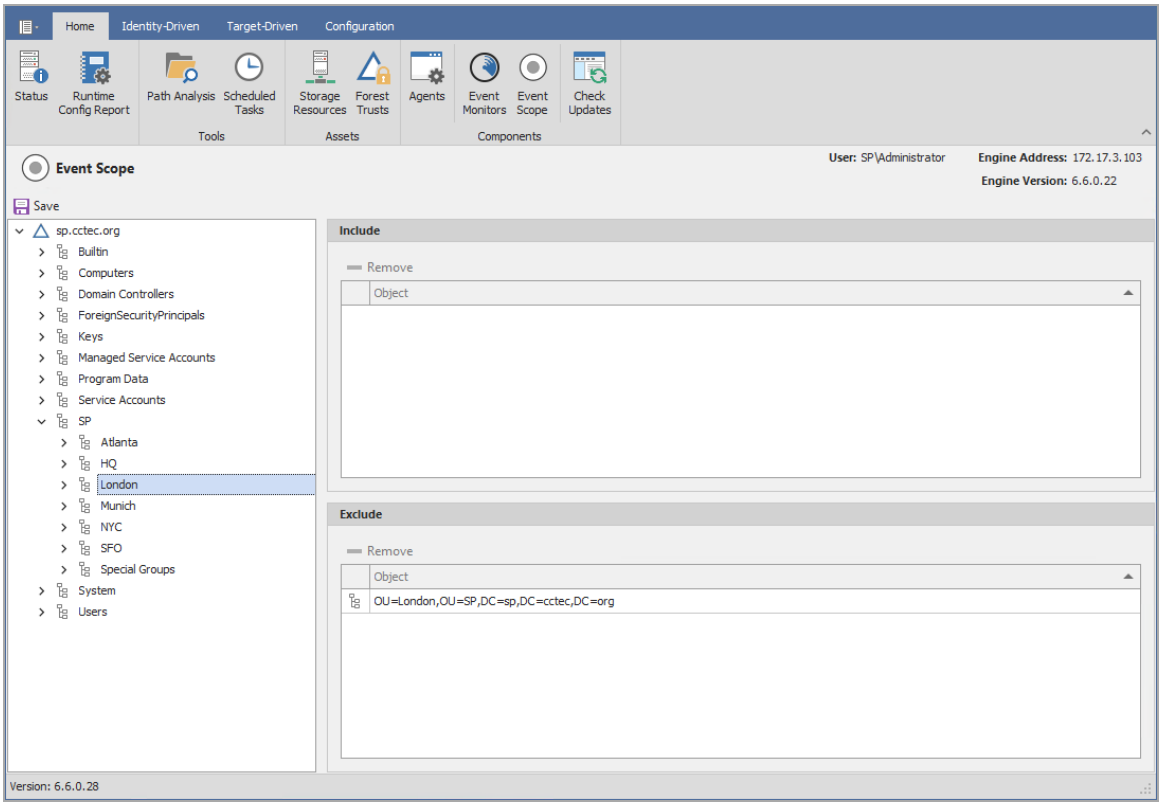
Container Specified for Include



3.4.2 - Exclude Scope

In the following example the Event Monitor will monitor all containers except for the *OU=London,OU=SP* subcontainer and its descendants.

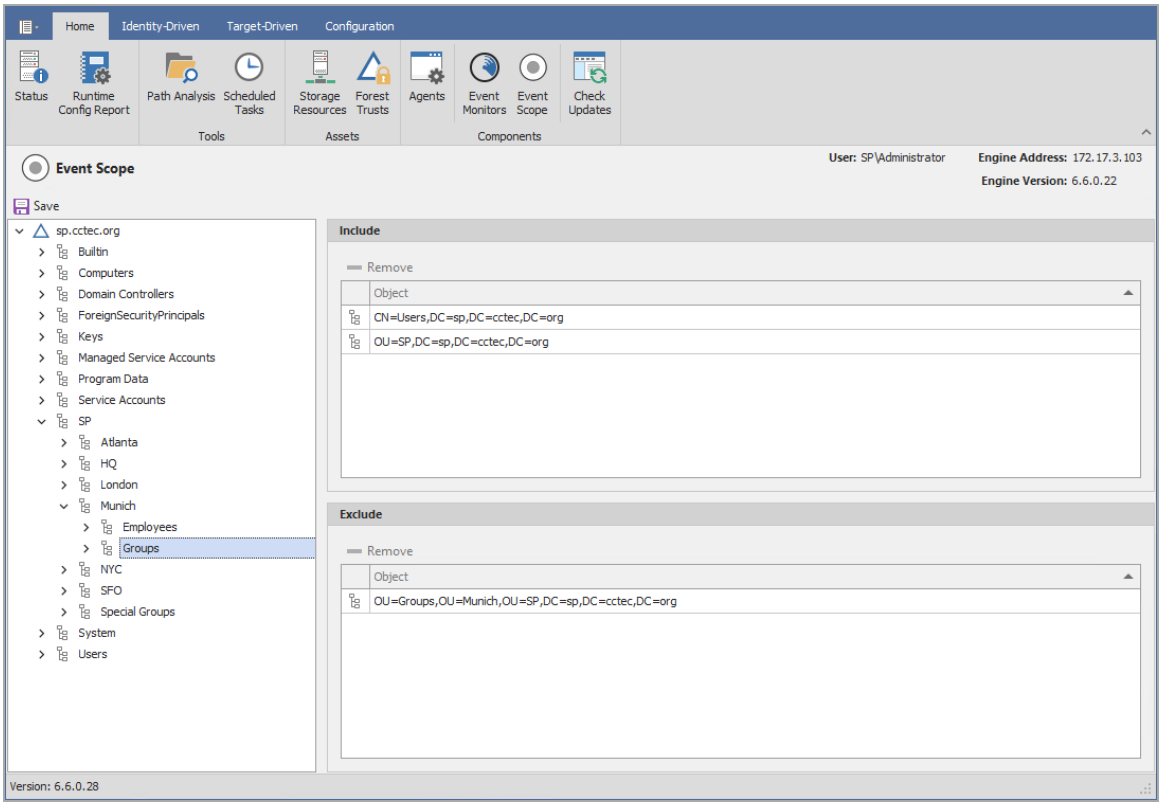
Container Specified for Exclude



3.4.3 - Include and Exclude Scope

In the following example the Event Monitor will only monitor the *CN=Users* and *OU=SP* containers and their descendants except for descendants of the *OU=Groups,OU=Munich,OU=SP* subcontainer.

Containers Specified for Include and Exclude



4 - Managing Existing User Storage

Because File Dynamics is deployed into an existing Microsoft network with users, groups, containers, and domains already established in Active Directory, 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
- Testing these policies to verify that they are working as desired
- Running Management Actions to invoke the policies settings on the existing users

By completing this section, you not only put your existing users' storage into a managed state and set it up for ongoing management through File Dynamics, but you also learn the basic procedures for reporting and for setting user policies. After completing the procedures in this chapter, refer to the remainder of the *File Dynamics 24.2 Administration Guide* for more detailed content on these tasks as well as many others.

4.1 - Running Consistency Check Reports on Existing Storage

When File Dynamics 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 permissions, 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 *Identity Driven* tab.
2. Click *Identity Objects*.
3. In the left pane, browse through the domain so that an organizational unit with the users you want to generate the consistency check report is displayed in the right pane.
4. In the left pane, right-click the container and select *User > Consistency Check*.
5. Click *Execute* and view the results in the bottom panel.
6. Click the ^ to expand the view.
7. Because none of the users are currently managed through File Dynamics, each user has a Management status of Not Managed. Additionally, there are no established storage quotas and there might be inconsistent directory attributes, permissions, flags, and file paths, along with various warnings or errors that you can mouse over to view the specifics.
8. To export a consistency check report for printing, see *Consistency Check (page 197)*.

4.2 - Assigning Missing Home Folder Attributes

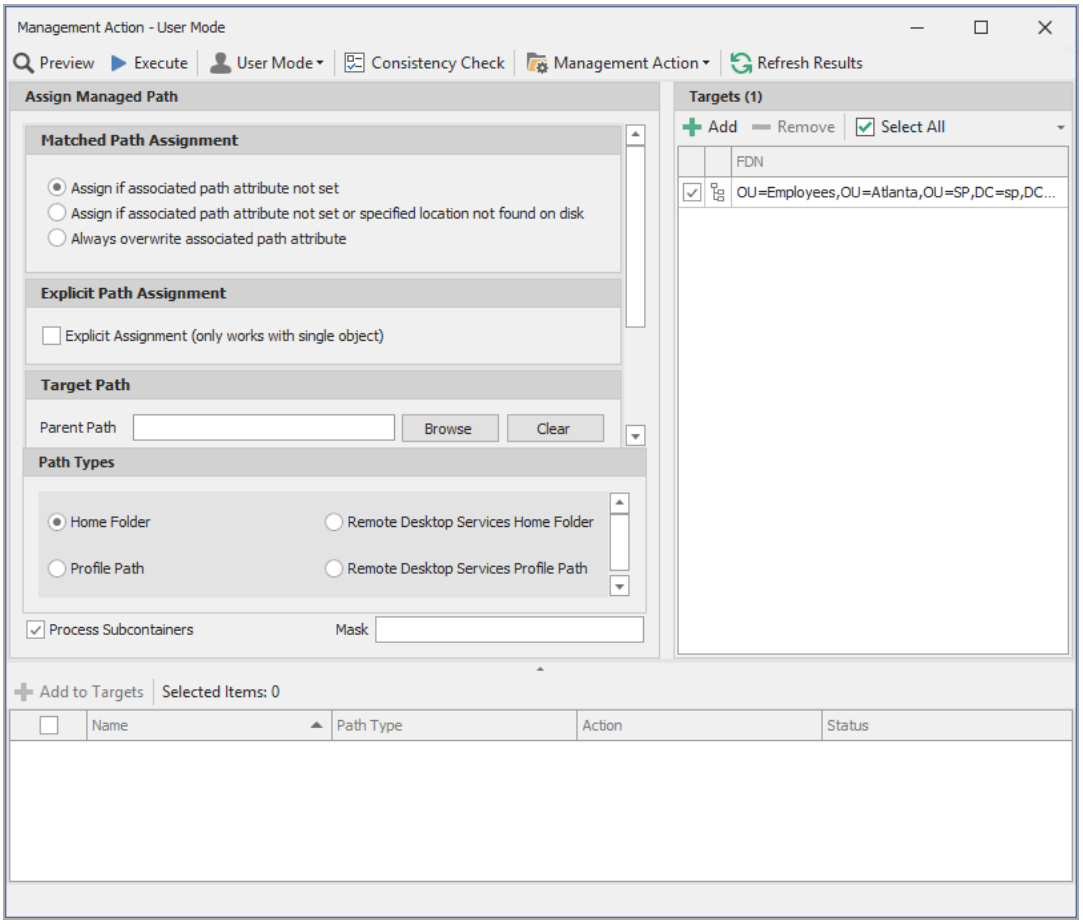
The consistency check report's DS Path column indicates the path (also referred to as "attributes") of the user's assigned home folder. If no path is indicated, it is because the home folder attribute is not set in Active Directory.

File Dynamics 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, File Dynamics can create one automatically once the target path for the home folder is indicated in the policy. For more information, see *Standardizing User Home Folder Attributes (page 18)*.

1. In the Admin Client, click the *Identity Driven* tab.
2. Click *Identity Objects*.
3. In the left pane, browse through the domain 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 > Assign Managed Path*.



6. In the *Matched Path Assignment* region of the window, make sure the *Assign if associated path attribute not set* option is selected.
7. Click *Browse*, use the Path Browser dialog box to browse to the path where you want all home folders in the selected organizational unit to reside, then click *OK*.
8. The selected path appears in the *Parent Path* field.
9. In the *Targets* region, click *Add*.
10. Use the Directory Services Browser to locate and specify the container where the users who will be assigned a managed path are located.
11. Click *Preview*.
12. *Preview* allows you to view the results of the action, without actually making changes.
13. Click ^ to expand the view.
14. File Dynamics summarizes any problems it can resolve in the *Action* column.
15. Click ˅ to collapse the view.
16. If you approve of the actions File Dynamics took in Preview mode, click *Execute*.

17. Run a new consistency check report by selecting the organizational unit you selected in Step 4, clicking *Consistency Check*, then clicking *Execute*.
18. Observe that all users now have home folder attributes listed in the *DS Path* column.

4.3 - 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 `\\SERVER-DNS-NAME\SHARE-NAME\HOME\USERS`, it should be set to `\\SERVER-DNS-NAME\SHARE-NAME\HOME\USERS\EBROWN`.

File Dynamics lets you easily standardize home folder attributes by overwriting attributes linked to the parent path.

1. In the Admin Client, click the *Identity Driven* tab.
2. Click *Identity Objects*.
3. In the left pane, browse through the domain 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 > Assign Managed Path*.
5. Select the *Always overwrite associated 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. Click *Preview*.
8. Click ^ to expand the view.
9. File Dynamics summarizes any problems it can resolve in the *Action* column. Resulting home folder attributes that are created will be displayed as "Match found. Managed Path would be set."
10. Click ˅ to collapse the view.
11. If you approve of the actions File Dynamics took in Preview mode, click *Execute*.
12. Run a new consistency check by selecting the organizational unit you selected in Step 4, clicking *Consistency Check*, then clicking *Execute*.
13. Observe that all users who did not previously have proper home folder attributes, now do.

4.4 - Creating a Blocking Policy

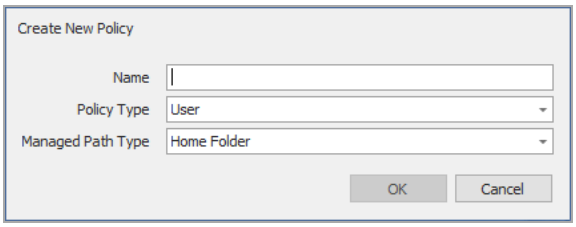
File Dynamics provides the ability to create "Blocking policies" that block other File Dynamics policies from affecting members of organizational units, members of groups, or even individual users. For example, you might have proxy users such as a BACKUP PROXY or VIRUS SCAN PROXY who do not need a home folder. Or, you might have an organizational

unit within an organizational unit whose members you do not want to be assigned home folders.

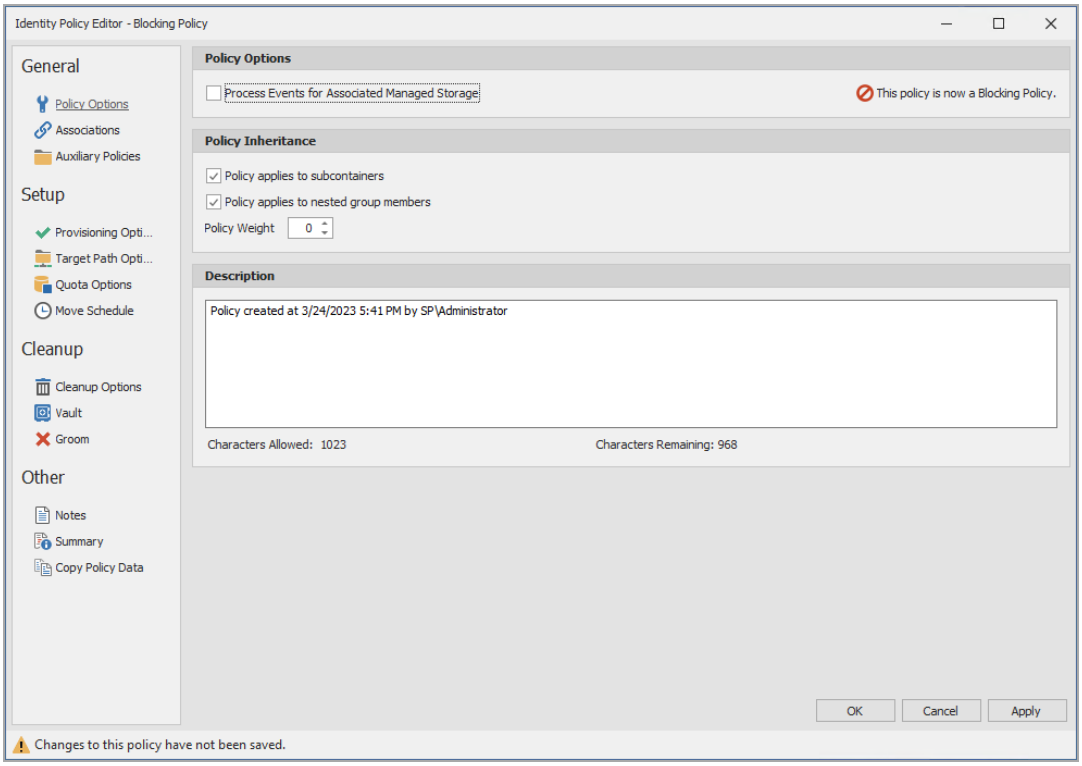
Creating a Blocking policy is as easy as creating a group, adding the users you want to block from a policy to the group, and then using the Admin Client to create the Blocking policy and associate it to the group.

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

1. In the Admin Client, click the *Identity Driven* tab.
2. Click *Policies*.
3. In the *Manage* menu, select *New* > *User Home Folder*.
4. The following dialog box appears:



5. Specify a descriptive name in the *Name* field, such as “Block Policy,” leave the *User* and *Home Folder* options selected, then click *OK*.
6. The Policy Options page appears.



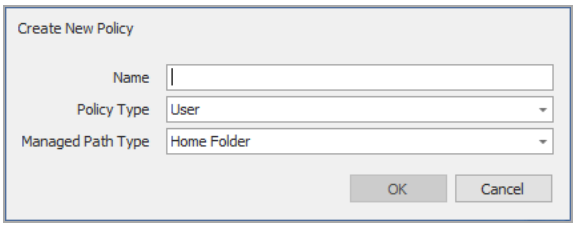
7. Deselect the *Process Events for Associated Managed Storage* check box.
8. A description at the right of the check box indicates that the policy is now a Blocking policy.
9. In the left pane, click *Associations*.
10. Click *Add*.
11. Browse down and locate the user, group, or container that you want to block from the effects of File Dynamics Identity-Driven policies, then drag it to the *Selected Items* pane.
12. Click *OK* to select the objects.
13. Click *OK* to save the Blocking policy.

4.5 - Creating a User Home Folder Policy

A policy in File Dynamics is the means by which the product provisions, manages, deletes, and archives storage. The parameters within an Identity-Driven policy dictate where user storage is created, what permissions are granted, what quota to assign, what to do when a user is deleted, and much more.

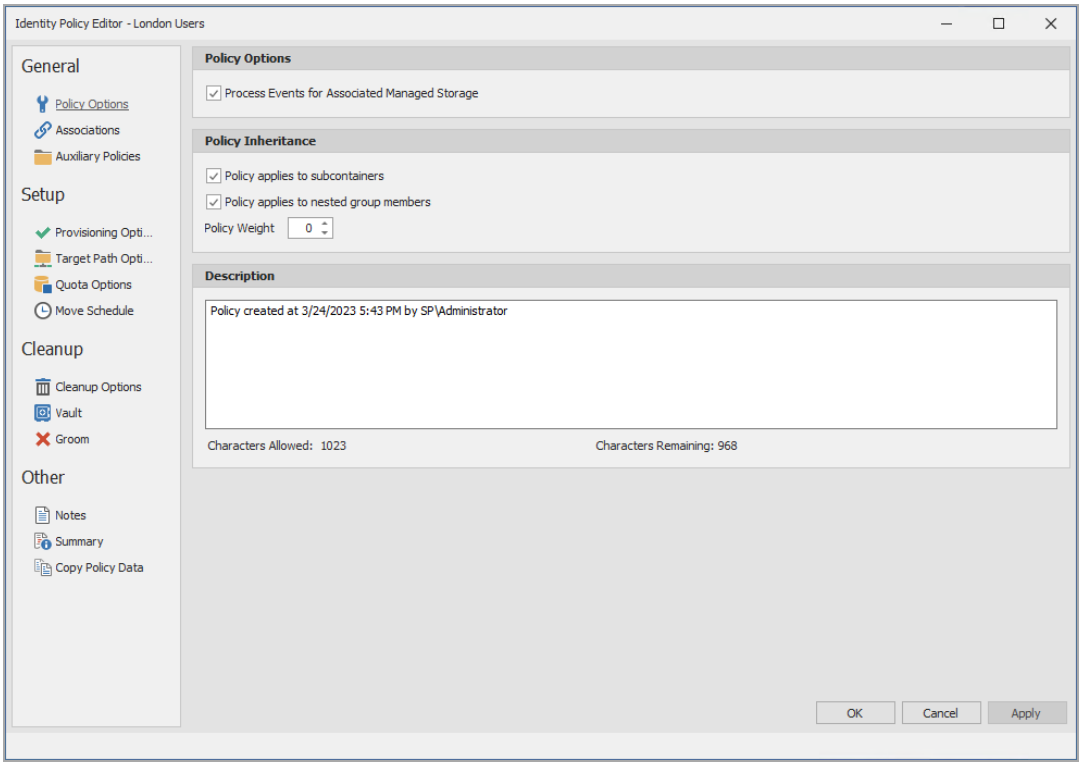
Only one Identity-Driven policy of the same type can be associated with an organizational unit, group, or user.

1. In the Admin Client, click the *Identity Driven* tab.
2. Click *Policies*.
3. In the *Manage* menu, select *New* > *User Home Folder*.
4. The following dialog box appears:



5. Specify a descriptive name for the policy, such as “London Users,” then click *OK*.

6. The Policy Options page appears.

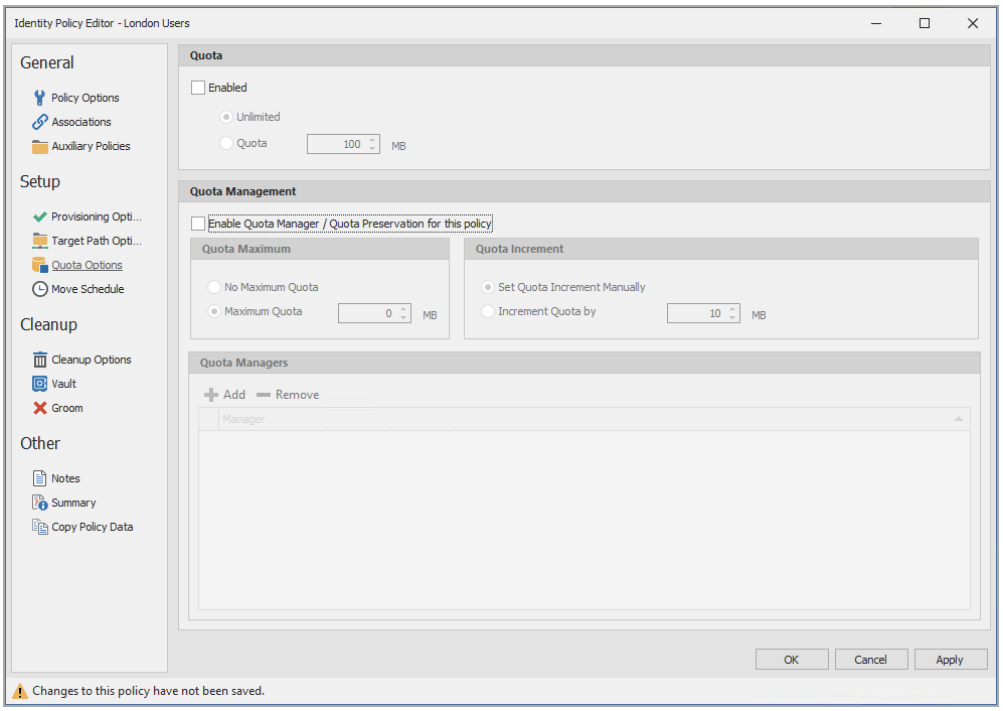


7. Set the Policy Options specifications for the policy:
    a. If you want the container's subcontainers to inherit the policy settings, leave the Policy applies to subcontainers check box selected. Otherwise, deselect it.
    b. If you will have users that are members of multiple groups, which means they could be affected by multiple policies, use the Policy Weight field to indicate a weight for this policy.
    c. When multiple policies pertain to a user, File Dynamics uses the highest weight number to determine which policy to apply.
    d. Click *Apply* to save your settings.
8. Set the associations:
    a. In the left pane, click *Associations*.
    b. Click *Add*.
    c. Browse to and locate the organizational unit, group object, or user object you want the policy applied to, then drag it to the *Selected Object* pane.
    d. Click *Apply* to save the settings.

9. Set the provisioning specifications:
    a. Click *Provisioning Options*.
    b. In the *Folder Properties* region, specify the settings to be for the permissions you want applied to network home folders that are created through this policy.
    c. 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.
    d. For more information on templates, see *Setting Provisioning Options (page 34)*.
    e. In the *Home Folder Options* region, indicate the network drive letter to assign to your users.
    f. Click *Apply* to save the settings.
10. Set the target paths:
    a. In the left pane, click *Target Path Options*.
    b. Click *Add*, browse to the share where you want your home folders to reside, right-click and choose *Select* to add the target path to the Selected Paths pane.
    -OR-
    Drag and drop the target path to the Selected paths pane.
    c. If you want to set the location of home folders among different paths, repeat Step 8b to include all the paths you want.
    d. If you have multiple paths listed, select a distribution method from the *Distribution* drop-down list.
    e. For an explanation of storage distribution, see *Setting Target Paths (page 36)*.
    f. Leave the other fields as they are currently set.
    g. Click *Apply* to save your settings.

11. Set the quota options:

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



    b. In the *Quota* region, click *Enabled* and specify the amount of initial storage space to be allocated to all users associated with this policy.

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

    d. 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 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.

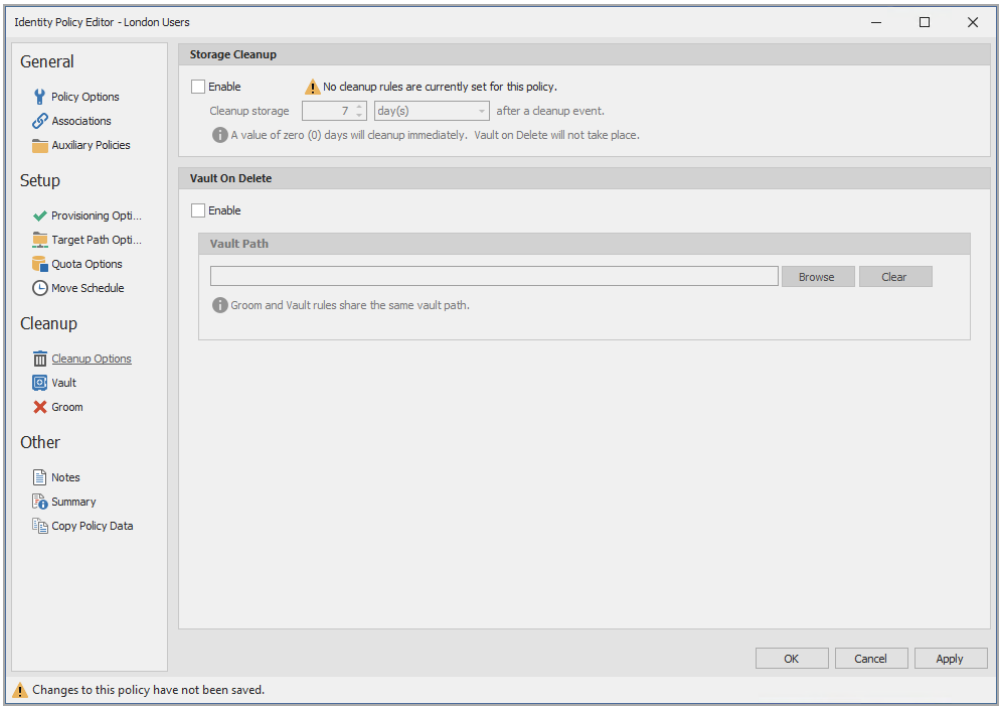
    a. Select one of the following Quota Increment options:

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

    a. In the *Quota Managers* region, click Add and specify users who will serve as quota managers.

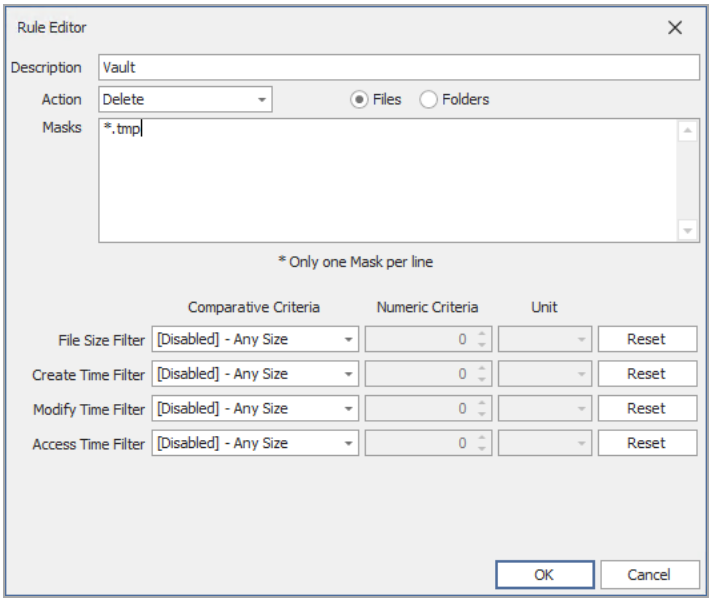
    b. Click *Apply* to save your settings.

12. Set the move schedule:
    a. In the left pane, click *Move Schedule*.
    b. Specify the hours when File Dynamics can perform data migrations.
    c. For more information on movement of data between multiple policy paths, see *Setting the Move Schedule (page 40)*.
    d. Click *Apply* to save the settings.
13. Set the cleanup options:
    a. In the left pane, click *Cleanup Options*.



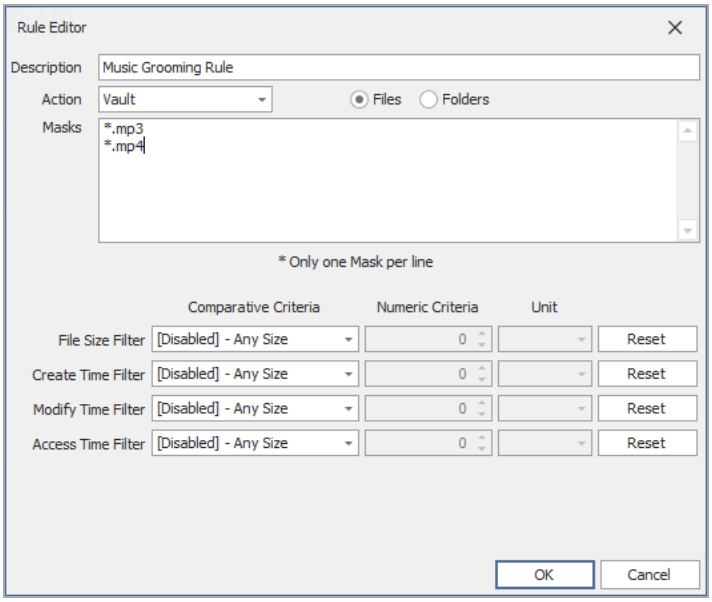
    b. In the *Storage Cleanup* region, select the *Enable* check box to indicate if you want user storage associated with this policy deleted when a user is removed from Active Directory.
    c. If you select the check box, you can specify the number of days a user home folder and its contents will remain before it is deleted.
    d. If you want user storage associated with this policy vaulted, in the *Vault on Delete* region, select the *Enable* check box and use the *Browse* button to indicate a path to the vault location.
    e. Click *Apply* to save your settings.
    f. If you have both *Storage Cleanup* and *Vault on Delete* enabled, File Dynamics vaults the data and then deletes it after the specified period of time. If you have *Vault on Delete* but not *Storage Cleanup* enabled, File Dynamics vaults the data immediately and never cleans it up.

14. Set the vault rules:
    a. In the left pane, click *Vault*.
    b. Click *Add* to create vault rules.



    c. 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.
    d. Click *Apply* to save your settings.
15. Set the groom rules:
    a. In the left pane, click *Groom*.
    b. Click *Add*.
    c. This brings up the Rule Editor dialog box.
    d. Select either *Vault*, *Delete*, or *Ignore* from the *Action* drop-down menu to specify whether to vault, delete, or ignore files or folders.
    e. In the *File Name Mask* field, indicate the type of file or the name of a folder for which this groom rule will take action. For example, `*.mp3` and `*.mp4`.

f. If you choose to vault files, you must have a specified vault path in the *Vault Path* field of the Vault Rules page.



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

h. 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 groom rule in this example vaults all MP3 and MP4 files greater than 2 MB. Setting additional filters narrows the scope of the grooming action even more.

i. Click *OK* to save the groom rule.

j. Repeat Step 13a through Step 13e to create additional groom rules.

k. Click *Apply* to apply the groom rules.

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

4.6 - Removing a Preexisting Process for Creating User Home Folders

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

If you have a network tool such as Microsoft Active Directory Users and Computers creating home folders, when a new user is added to the organizational unit or group associated with a policy, you need to remove the setting that creates the home folder.

4.7 - Testing the User Home Folder Policy

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

1. Use Active Directory Users and Computers to create a new user such as `TESTUSER` in the organizational unit associated with the policy you configured in *Creating a User Home Folder Policy (page 20)*.
2. In the Admin Client, click the *Engine* 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 *Permissions*.
6. This displays the View Permissions page.
7. Verify that the permissions that you set in Step 7a under *Creating a User Home Folder Policy (page 20)* are those that you set in the policy.
8. Close the View Permissions page.
9. Right-click and select *Quota*.
10. This displays the View Quota dialog box.
11. Verify that the quota specifications that you set in Step 9 under *Creating a User Home Folder Policy (page 20)* are those that you set in the policy.
12. Click *OK* to close the View Quota dialog box.

4.8 - 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 *Identity Driven* tab.
2. Click *Objects*.
3. In the left pane, browse to select the organizational unit associated with the policy that you created earlier.
4. Select the *Users* check box.
5. In the right pane, locate and right-click `TESTUSER`, then select *User > Consistency Check*.
6. The Take Action – User Mode page appears.
7. Click *Execute*.
8. Verify that the settings for the home folder 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).

4.9 - Running Management Actions

This procedure does the cataloging that enables the existing storage to be managed by File Dynamics.

1. In the Admin Client, click the *Identity Driven* tab.
2. Click *Objects*.
3. In the left pane, browse to select the organizational unit associated with the policy that you created earlier.
4. Right-click the organizational unit and select *User > Manage*.
5. Verify that the selected organizational unit is listed in the *Targets* region of the Take Action page.
6. From the *Management Action* menu, select *Manage*.
7. Click *Preview* to view what actions will be taken.
8. Click *Execute* to initiate the Management Actions.
9. (Conditional) If you have other policy settings to apply, including quota, permissions, and a template, do so using the *Apply Quota*, *Apply Permissions*, and *Apply Template* menu options respectively.
10. For more information on these, and other Management Actions, see *Management Actions (page 189)*.

4.10 - Testing a Rename Event

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

1. Use Active Directory Users and Computers to rename the user from the suggested TESTUSER name to a name such as TESTUSER2.
2. When renaming a user object, you must rename the sAMAccountName attribute, whose value is used to create managed storage.
3. In the Admin Client, while you are still displaying the users through the *Objects* form, click *Refresh* to refresh the screen and see the renamed user.
4. Right-click the renamed user and select *User > Consistency Check*.
5. Click *Execute*.
6. Verify that the home folder and the directory attribute have been updated in the *DS Path* and *Mgmt Path* columns.

4.11 - Testing a Cleanup Rule

This procedure lets you verify that File Dynamics cleans up a user's storage according to the user home folder policy that you created earlier.

1. Use Active Directory Users and Computers to delete TESTUSER2.
2. If you chose to delay the cleanup of user storage for a set amount of days in Step 11b under *Creating a User Home Folder Policy (page 20)*, open the Admin Client, click the *Identity Driven* tab and then click *Events* to view any information indicating the deferred number of days for the storage cleanup.
3. Click the *Engine* tab.
4. Click *Path Analysis*.
5. In the left pane, browse to the location where the TESTUSER2 resided and verify that the folder has been deleted.
6. (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 under *Creating a User Home Folder Policy (page 20)* and verify that TESTUSER2 was vaulted:
    a. If you set your policy to delay the cleanup of user storage for a set amount of days in Step 11b under *Creating a User Home Folder Policy (page 20)*, click *Events* and then from the *View Events* drop-down menu, select *Deferred Only* to view details on deferred action.
    b. Right-click the listed deferred action, and select *Properties*. In the Properties dialog box, then verify that the *Next Process Time* displays a date that corresponds to the number of days you set in your policy for the deleted storage to be cleaned up.
    c. Close the dialog box.
7. Because this is a test user, perform the storage cleanup immediately by once again right-clicking the listed deferred action and selecting *Make Eligible*.
8. Click the *Engine* tab.
9. 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.

4.12 - 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 organizational units or groups. You can do so based on the overview and procedures you were given in this chapter, or you can review *Managing User Home Folders (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 File Dynamics, you can proceed to have File Dynamics manage your collaborative-based storage. Refer to *Managing Collaborative Storage (page 69)* for a comprehensive discussion and procedures for performing collaborative storage tasks. Finally, you can refer to *Creating Target-Driven Policies (page 109)* to create Target Driven policies.

5 - Managing User Home Folders

This chapter provides you the information you need to understand and create policies for managing:

- User Home Folders
- User Profile Paths
- User Remote Desktop Services Home Folders
- User Remote Desktop Services Profile Paths
- Inactive Users

Additionally, this chapter provides information for setting up a vault location, enabling your network for quota management, importing and exporting policy information, and more.

5.1 - Home Folder Management Overview

In *Managing Existing User Storage (page 15)*, 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
- Profile path policies
- Remote Desktop Services policies that include
    - Remote desktop home folder
    - Remote desktop policy path

5.2 - User Policies

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

- Organizational Unit
- Container
- Security Group
- User

If you associate a user policy to a 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.

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, as well as all other policy types, are stored in the SQL Server database.

5.3 - Setting Up a Vault 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 Active Directory. If your user storage policies are to include vaulting rules, you must first set up a storage location (share) where the policy will vault the storage.

Ensure that the vault location has Full Control permission and Full Control security rights for the Proxy Rights group.

5.4 - Enabling Your Network for Quota Management

File Dynamics leverages the disk quota capabilities of Windows Server 2008 and later that are exposed via File Server Resource Manager (FSRM).

File Dynamics cannot manage quotas on home folders, collaborative storage folders, or auxiliary storage hosted on Windows Server 2003 machines. Furthermore, File Dynamics cannot manage quotas on NAS devices.

For all Windows Server 2008 and later servers hosting home, collaborative, or auxiliary storage managed by File Dynamics with quota management enabled, you must have the File Server Resource Manager (FSRM) role installed. Additionally, if the Windows Firewall is enabled, then you must set an exception rule on each server that permits remote FSRM management. FSRM management is needed because the Engine is managing the quota remotely. FSRM must also be installed on the server hosting the Engine.

For more information, see *Firewall Requirements (page 245)*.

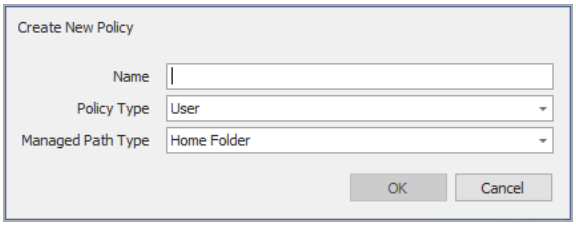
The process for setting an exception rule differs among the various offerings of Windows Server.

5.5 - Creating a User Home Folder Policy

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

1. Launch the Admin Client.
2. Click the *Identity Driven* tab.
3. Click *Policies*.

4. In the *Manage* menu, select *New* > *User Home Folder*.
   The following dialog box appears:



5. Specify a descriptive name in the *Name* field and click *OK*.
   The Policy Options page appears.

5.5.1 - Setting Policy Options

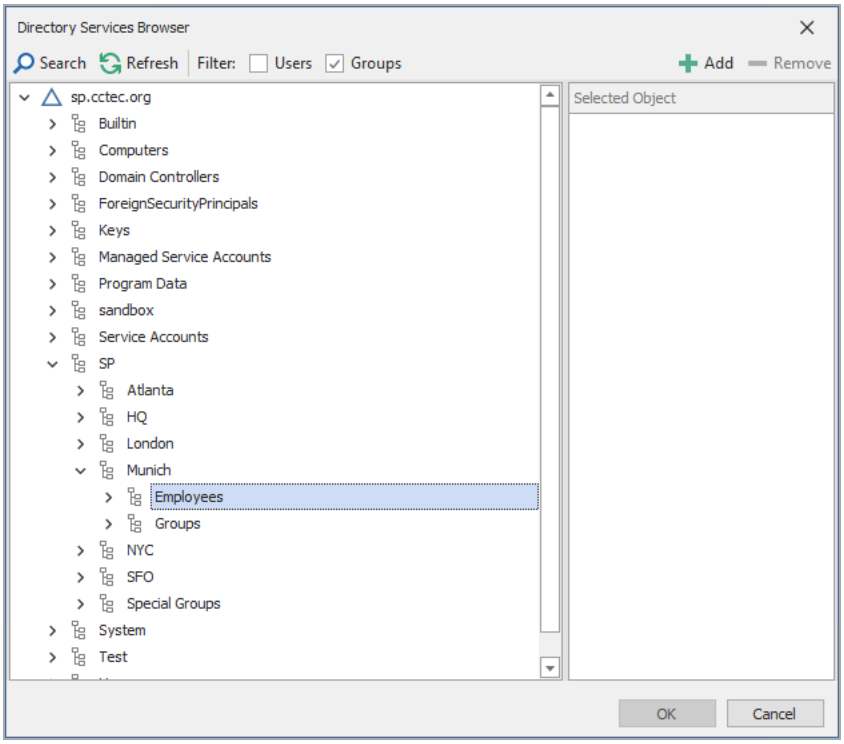
Settings within Policy Options let you indicate how to apply the policy, set policy inheritance and policy weight, and write an expanded policy description.

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 organizational unit 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 *Creating a Blocking Policy (page 18)*
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 organizational units that reside within the organizational unit where this policy is assigned.
   Policy applies to nested group members: When the policy applies to or is effective for groups, this option determines if nested group members will also be affected.
   Policy Weight: When a user is a member of multiple groups and each group has a separate effective policy, File Dynamics uses this setting to determine which policy to apply. File Dynamics 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. Click *Apply* to save your settings.
5. Proceed with *Setting Associations (page 33)*.

5.5.2 - Setting Associations

Associations is where you assign the policy you are creating to an organizational unit, group, or user object.

1. In the left pane, click *Associations*.
2. Click *Add* to bring up the Directory Services Browser.
3. If you plan to assign the policy to a User object, select the *Users* check box as a *Filter* option in the Directory Services Browser.
4. Browse through the directory structure and select the organizational unit, group object, or user object you want to associate the policy to.

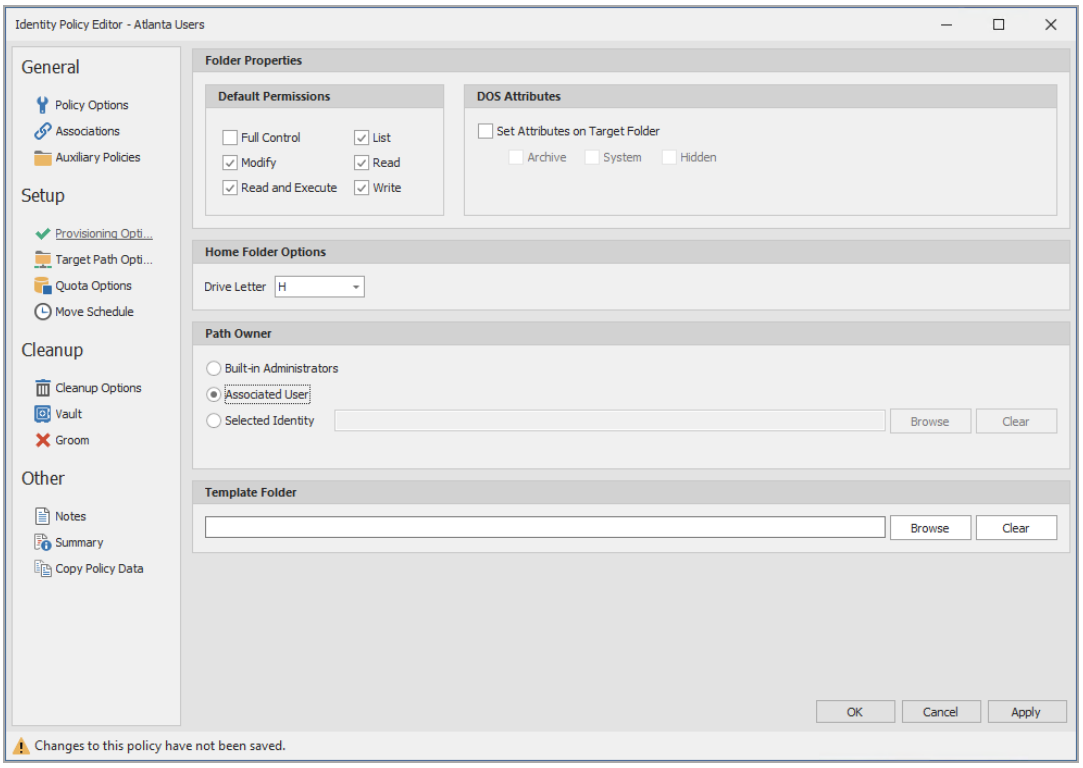


5. Drag the object to the *Selected Object* pane, then click *OK*.
   The Directory Services Browser is closed and the object is displayed in fully qualified name format in the right pane of the window. For example, `OU=Employees,DC=Munich,DC=SP,DC=cctec,DC=org`.
6. Click *OK* to close the Directory Services Browser.
7. Click *Apply* to save your settings.
8. Proceed with *Setting Provisioning Options (page 34)*.

5.5.3 - Setting Provisioning Options

The Provisioning Options page is where you indicate home folder permissions, the network drive letter for the home folder, 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 Permissions: By default, File Dynamics grants the user all file permissions to the home folder except for Full Control. Granting Full Control is not recommended because it provides administrator rights to the home folder and enables the user to rename and delete the folder.
   Set Attributes on Target Folder: Select this check box to enable the *Archive*, *System*, and *Hidden* check boxes. If you wanted home folders to be hidden from view, you could enable the Hidden attribute by selecting the *Hidden* check box.
   By default, File Dynamics assigns the user for whom a home folder is created as the home folder owner. Because this essentially provides the owner administrative rights to the home folder, you might want to provide ownership to a network administrator instead. To override the ownership and indicate a new owner, click the *Override Path Owner* check box, then browse to and select the User object you want to establish as the owner.
   The home folder user still has all permissions—with the exception of administrative permissions—to the home folder.
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, indicate the network drive letter that users associated with this policy will use to access their home folders.
   You can select an empty drive letter. In this scenario, the user's home drive property

will not be set. This results in Windows clients not mounting the network home folder when a user logs in.

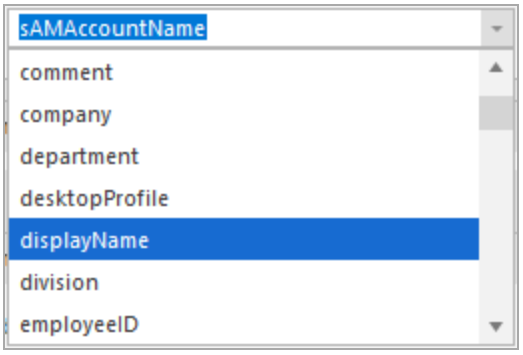
5. In the *Path Owner* region, select one of the following options:
   - **Built-in Administrator:** If you want the owner of the storage to be the Built-in Administrator, select this option.
   - **Associated User:** The associated user is the user whose home folder you are creating. If you want the associated user to own their own home folder, select this option.
   - **Selected Identity:** If you want another owner to be the owner of the home folder, browse and select the user or group object.
6. Click *Apply* to save your settings.
7. Proceed with *Setting Target Paths (page 36)*.

5.5.4 - Setting Target Paths

The Target Path Options page is where you select the naming attribute for the managed path, as well as set the paths to the shares where user home folders will be hosted.

1. In the left pane, click *Target Path Options*.
2. In the *Managed Path Naming Attribute* region, do one of the following:
   - From the drop-down menu, select the single-value Active Directory attribute you want as the means of naming your home folders.
   - Click *Link Action Block* and select a previously saved Action Block for the naming attribute.

   For some organizations, having the default `sAMAccountName` attribute as the means of naming home folders is not desirable. A school that generates student accounts using an account provisioning system for example, might generate a student account and `sAMAccountName` such as SA74556, rather than a more descriptive name such as William Sanders. To allow File Dynamics to create a home folder with a name like WSanders, rather than SA74556, you can select a different attribute from the drop-down list.



   Once you have saved the policy, you can use an account provisioning system such as

NetIQ Identity Manager to automatically populate the selected attribute with the desired folder name and then File Dynamics will automatically provision the home folder based on this attribute setting. Using the example above, the home folder name would be WSanders rather than SA74556.

For existing users whose home folders you would like to change to a new attribute value, you would follow the same procedures, followed by performing an Enforce Policy Path Management Action.

For specifications pertaining to Managed Path Naming Attribute, see *Managed Path Naming Attribute Specifications (page 265)*.

3. 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:

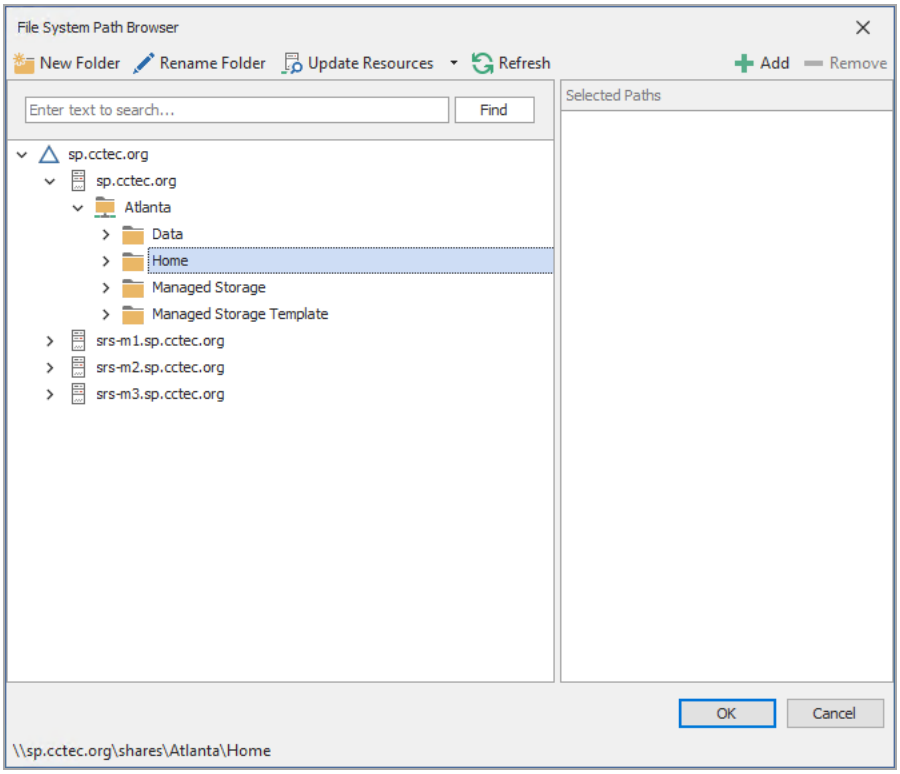
   - **Random:** Distributes storage randomly among the number of target paths.
   - **Actual Free Space:** Distributes the creation of user home folders according to shares with the largest amount of absolute free space. For example, if you have two target paths listed, target path 1 has 15 GB of free 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 folders to shares with the largest percentage of free space. For example, if you have two target paths listed, target path 1 is to a 10 TB share that has 30 percent free space and target path 2 is to a 500 GB share with 40 percent free space, the home 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 shares 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 `\\SERVER1-DNS-NAME\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 `\\SERVER1-DNS-NAME\HOME\H\BSMITH`.
   The *Last Letter* means the last character of the attribute File Dynamics uses to create storage. Once again, File Dynamics uses the SAM, not the character of the last name.
   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 BMITH2014 has a home folder located in a path such as `\\SERVER-DNS-NAME\HOME\2014\BSMITH2014`.

   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 File Dynamics 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*. File Dynamics 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.

4. For each target path that you want to establish, click *Add* to access the Path Browser.
5. Browse to the location of the target path you want and click *Add* to add the target path to the *Selected Paths* pane.



6. Click *Apply* to save your settings.
7. Proceed to *Setting Quota Options (page 38)*.

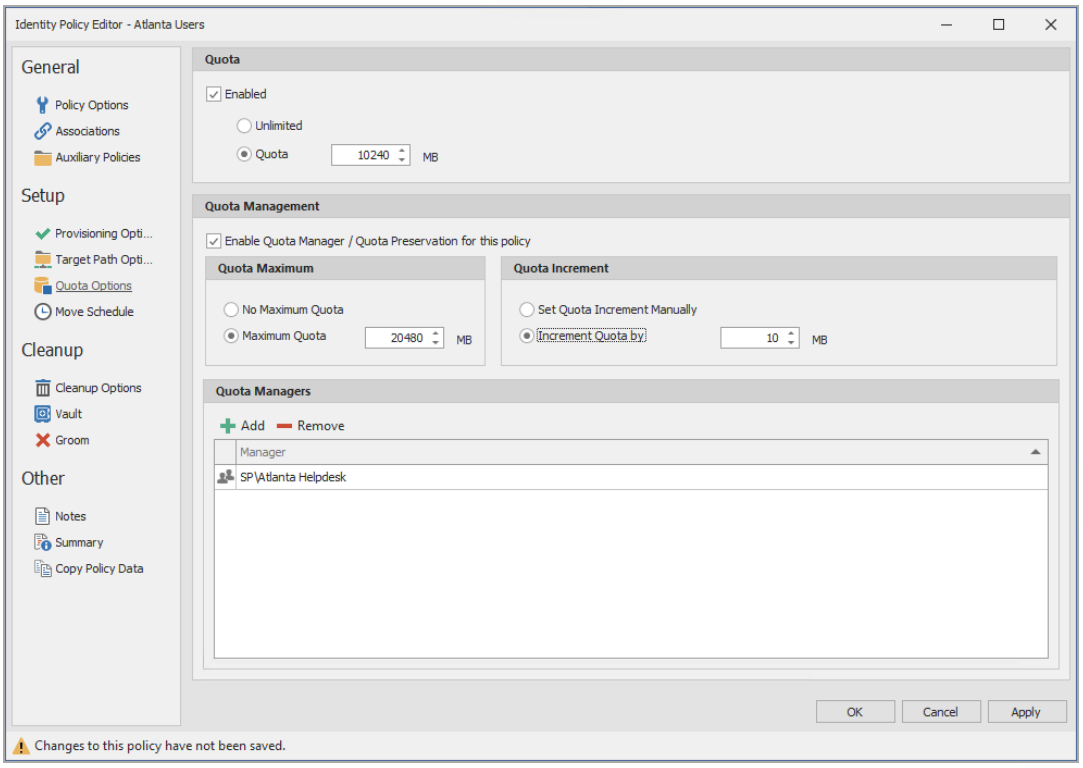
5.5.5 - Setting Quota Options

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

Quota management on NAS devices needs to be managed by the NAS vendor software.

This page is also where you establish quota management settings for quota managers. A quota manager is a specified user or group 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 *Using Quota Manager (page 105)*.

1. In the left pane, click *Quota Options*.
   The following page appears:



2. Select the *Enabled* check box to enable an initial storage quota for users to whom this policy will apply.
   Leaving this check box deselected gives users unlimited user home folder storage.
3. In the *MB* field, specify the initial storage quota for the user home folders.
4. Set up quota managers and enable the Quota Manager web interface 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 allow the Quota Manager web interface to apply to this policy.

   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 user home folders 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 Directory Services Browser to browse to and select a user or group you want to serve as a quota manager by dragging the User or Group object over to the right pane. Repeat this for each user or group you want to establish as a quota manager.

If you do not specify a user or group as a quota manager, only members of the File Dynamics Admins group will be able to use the Quota Manager web interface.

5. Click *Apply* to save your settings.
6. Proceed with *Setting the Move Schedule (page 40)*.

5.5.6 - 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 *Setting Cleanup Options (page 40)*.

5.5.7 - Setting Cleanup Options

This page lets you enable and specify cleanup rules for the user home folder policy. Options for cleanup include deleting a home folder after a set number of days following the removal of a User object from Active Directory, 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 Active Directory.
3. Enable Vault on Delete by filling in the following fields:
   Enable: Select this check box to enable Vault on Delete. If this is checked and storage cleanup is not enabled, the managed path will be immediately vaulted to the vault location based on the specified vault rules. If there are no vault rules, the managed path will be immediately vaulted to the vault location and removed from the source.
   Vault Path: Click *Browse* to browse and select the path where you want the managed storage vaulted after cleanup.

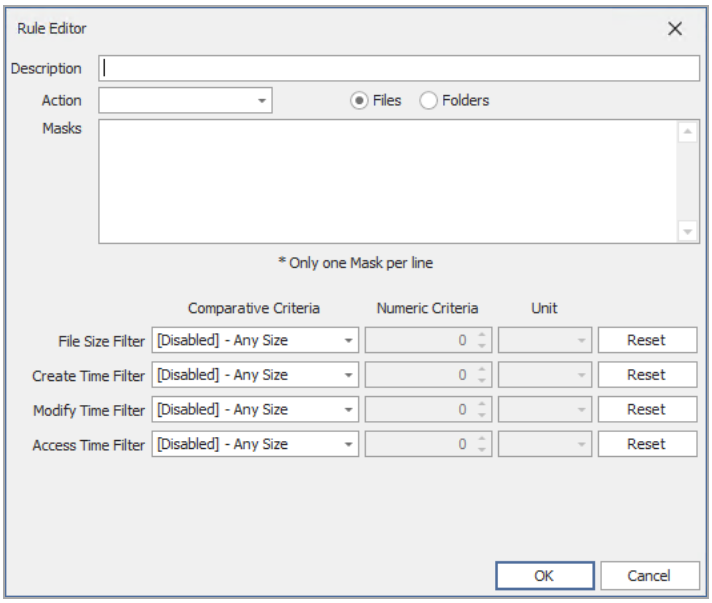
When you indicate this path, it also appears in the *Vault Path* field of the Groom page because groom and vault rules share the same path.

4. Click *Apply* to save the settings.
5. Proceed with *Setting Vault Rules (page 41)*.

5.5.8 - Setting Vault Rules

When a User object is removed from Active Directory, you can have File Dynamics vault the contents of the user's home folder from primary storage to less expensive secondary storage. File Dynamics 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 Rule Editor.

1. In the left pane, click *Vault*.
   The *Vault Path* field displays the vault path that you established when you set up cleanup rules.
2. Click *Add* to open the Rule 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. From the *Action* menu, select an action.
   Select whether the rule will vault files or folders, delete files or folders, or ignore a vault rule.

   There is only one action for each vault rule. For example, if you wanted to delete some files and vault others, you would need to establish two different vault rules.
   Vault: Moves all of the files or folders that meet the criteria specified in the vault rule to a location specified in the policy.
   Delete: Deletes all of the files or folders that meet the criteria specified in the vault

rule.
Ignore: Ignores the conditions that would normally vault or delete a file or folder, based on specifications you provide in the *Mask* field.
For example, if you wanted to vault all `.MOV` files, with the exception of approved training videos located in a folder named `Training Videos`, you could set an individual rule to vault `.MOV` files, and another rule to ignore vaulting the `Training Videos` folder.
Selecting *Folders* disables the filter settings in the lower portion of the Rule Editor.
File or folder names can contain an asterisk.

5. Specify whether the rule will apply to files or folders.
Files: If the vault rule you are creating will vault, delete, or ignore content at the file level, leave the *File* option selected.
Folders: If the vault rule you are creating will vault, delete, or ignore content at the folder level, select the *Folders* option.

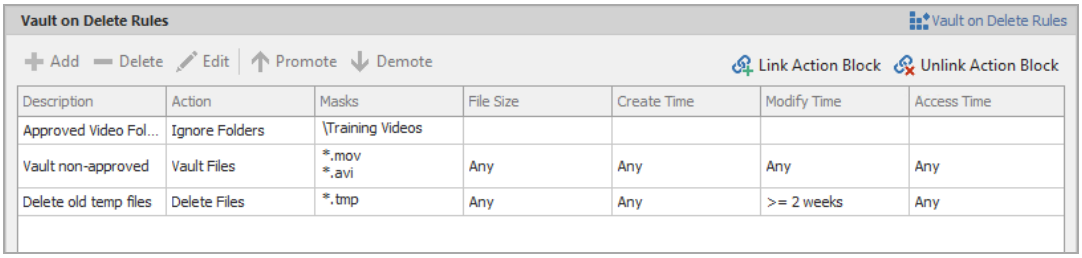
6. Specify the masks for the rule.
Masks: List the files or folders you want to be vaulted or deleted, according to what is indicated in the *Action* drop-down menu. For example, if you wanted to delete all temporary files, you could list `*.TMP` in the *Masks* field.
Be aware that if you select *Vault*, only the files or folders that you list in the *Masks* text box are vaulted and the remainder of the managed path 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.

7. (Conditional) If the 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 *Masks* 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.
ghghgh

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

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

10. (Conditional) If you have set any rules designed to ignore a vault or delete action, in the *Vault on Delete* region of the Vault page, use the *Promote* arrow to move the rule to the top. This protects files or folders specified in the *Masks* field from being vaulted or deleted.



11. Proceed with *Setting Groom Rules (page 43)*.

5.5.9 - Setting Groom Rules

Groom rules in File Dynamics specify the file types that you want to be removed from managed primary storage. Examples of these might be MP3 and MP4 files, MOV files, and many others. You specify in a groom rule whether to delete or vault a file based on the rule's criteria.

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 *Management Actions (page 189)*.

1. In the left pane, click *Groom*.
   The *Vault Path* field displays the vault path that you established when you set up cleanup rules.
2. Click *Add* to bring up the Rule Editor.
3. In the *Description* field, enter a description of the groom rule.
   For example, "Files to groom in Henderson OU."
4. Fill in the following fields:
   Action: Select whether this groom rule will delete or vault groomed files.
   Files: If the groom rule you are creating will vault or delete content at the file level, leave the *File* option selected.
   Folders: If the groom 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 Rule 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 groom 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 *Masks* 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 groom rule.
7. Proceed with *Notes (page 43)*.

5.5.10 - 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.

5.5.11 - Summary

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

5.6 - Creating a User Profile Path Policy

For users in Active Directory who access the network through Remote Desktop Services, File Dynamics can provision and manage a user's profile path, quota, grooming, and vaulting by setting and managing the profile path attribute.

Microsoft stores a user's profile path as follows: `\\server-name\share-name\users\user\profile`.

In managing the user's roaming profile path, File Dynamics creates two separate profile paths in the UNC network path. For Windows workstations running Windows Vista, Windows 7, or Windows 8, the path is similar to the following: `\\server-dns-name\share-name\users\user\profile.V2`.

For Windows workstations running Windows XP and earlier, the path is similar to the following: `\\server-dns-name\share-name\users\user\profile`.

Support for Windows XP and earlier has been kept for backwards compatibility and will be deprecated in a future release.

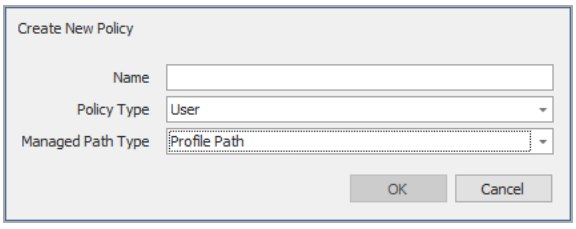
When a profile is specified for the policy, the profile is created in both of these locations. Additionally, when quota and vault paths are specified, the specifications also apply to both of the paths.

When File Dynamics has provisioned a profile path for the Remote Desktop Services user, it enters settings in the *Profile path* field of the User object's Profile property.

The Windows Full Control NTFS permission is established and cannot be modified.

5.6.1 - Create the Policy

1. In the Admin Client, click the *Identity Driven* tab.
2. Click *Policies*.
3. In the *Manage* menu, select *New > User Profile Path*.
   The following dialog box appears:



4. Specify a name in the *Name* field and click *OK*.

The Policy Options page appears.

5. Select the options and settings that you want the policy to use.

Policy Options: The fields presented on the Policy 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 policy options, see *Setting Policy Options (page 33)*.

Associations: The Associations page is identical to the Associations page presented when you create a User Home Folder policy. For an explanation of the page, along with procedures for setting associations, see *Setting Associations (page 33)*.

Auxiliary Policies: Lets you link an Auxiliary policy to the profile path. For more information on Auxiliary policies, see *Using a Policy to Manage Auxiliary Storage (page 52)*.

Provisioning Options: The Provisioning Options page provides only the Path Owner and Template Folder settings that are described in detail in *Setting Provisioning Options (page 34)*.

When you create a User Profile Path policy, the *Folder Properties* and *Home Folder Options* settings are included in the Provisioning Options page for User Home Folder policies are not included because you are only setting the profile path and not the user home folder storage.

Target Path Options: The fields presented on the Target Path 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 target paths, see *Setting Target Paths (page 36)*.

Quota Options: 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 *Setting Quota Options (page 38)*.

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 *Setting the Move Schedule (page 40)*.

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 *Setting Cleanup Options (page 40)*.

Vault: 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 *Setting Vault Rules (page 41)*.

Groom: The fields presented in the Groom 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 *Setting Groom Rules (page 43)*.

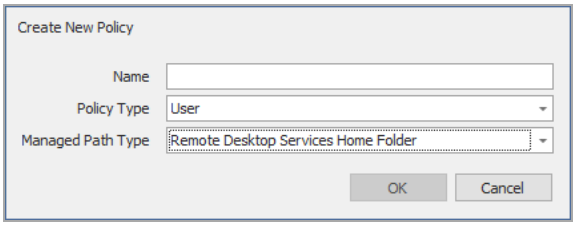
5.7 - Creating a User Remote Desktop Services Home Folder Policy

Remote Desktop Services provides users network access from remote client machines. File Dynamics provisions and manages these users' home folders through User Remote Desktop

Services Home Folder policies.

5.7.1 - Create the Policy

1. In the Admin Client, click the *Identity Driven* tab.
2. Click *Policies*.
3. In the *Manage* menu, select *New > User Remote Desktop Services Home Folder*.
   The following dialog box appears:



4. Specify a name in the *Name* field and click *OK*.
   The Policy Options page appears.
5. Select the options and setting that you want the policy to use:

Policy Options: The fields presented on the Policy 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 policy options, see *Setting Policy Options (page 33)*.

Associations: The Associations page is identical to the Associations page presented when you create a User Home Folder policy. For an explanation of the page, along with procedures for setting associations, see *Setting Associations (page 33)*

Provisioning Options: The fields presented on the Provisioning 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 provisioning options, see *Setting Provisioning Options (page 34)*.

Target Path Options: The fields presented on the Target Path 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 target paths, see *Setting Target Paths (page 36)*

Quota Options: 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 *Setting Quota Options (page 38)*

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 *Setting the Move Schedule (page 40)*.

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 *Setting Cleanup Options (page 40)*.

Vault: 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 *Setting Vault Rules (page 41)*.

Groom: The fields presented on the Groom 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 *Setting Groom Rules (page 43)*.

5.8 - Creating a User Remote Desktop Services Profile Path Policy

File Dynamics provisions and manages Remote Desktop Services profile policy paths through Remote Desktop Services profile path policies.

For users in Active Directory who access the network through Remote Desktop Services, File Dynamics can provision and manage a user's profile path, quota, grooming, and vaulting by setting and managing the profile path attribute.

Microsoft stores a user's profile path as follows: `\\server-dns-name\share-name\users\user\profile`.

In managing the user's roaming profile path, File Dynamics creates two separate profile paths in the UNC network path. For Windows workstations running Windows Vista, Windows 7, or Windows 8, the path is similar to: `\\server-dns-name\share-name\users\user\profile.V2`.

For Windows workstations running Windows XP and earlier, the path is similar to: `\\server-dns-name\share-name\users\user\profile`.

Support for Windows XP and earlier has been kept for backwards compatibility and will be deprecated in a future release.

When a profile is specified for the policy, the profile is created in both of the locations above. Additionally, when quota and vault paths are specified, the specifications apply to both of the paths as well.

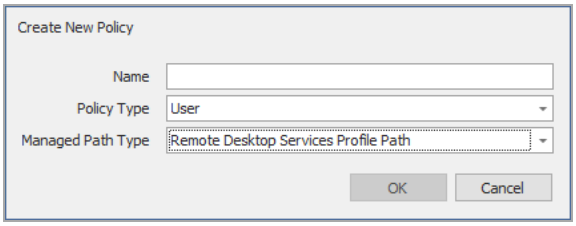
When File Dynamics has provisioned a profile path for the Remote Desktop Services user, it enters settings in the *Profile path* field of the User object's Remote Desktop Services Profile property.

The Windows Full Control NTFS permission is established and cannot be modified.

5.8.1 - Create the Policy

1. In the Admin Client, click the *Identity Driven* tab.
2. Click *Policies*.

3. In the *Manage* menu, select *New > User Remote Desktop Services Profile Path*.
   The following dialog box appears:



4. Specify a name in the *Name* field and Click *OK*.
   The Policy Options page appears.
5. Select the options and settings that you want the policy to use:

Policy Options: The fields presented on the Policy 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 policy options, see *Setting Policy Options (page 33)*.

Associations: The Associations page is identical to the Associations page presented when you create a User Home Folder policy. For an explanation of the page, along with procedures for setting associations, see *Setting Associations (page 33)*

Provisioning Options: The Provisioning Options page provides only the Path Owner and Template Folder settings that are described in detail in *Setting Provisioning Options (page 34)*.

When you create a User Remote Desktop Services Profile Path policy, the Folder Properties and Home Folder Options settings that are included in the Provisioning Options page for User Home Folder policies are not included because you are only setting the profile path and not the user home folder storage.

Target Path Options: The fields presented on the Target Path 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 target paths, see *Setting Target Paths (page 36)*.

Quota Options: 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 *Setting Quota Options (page 38)*.

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 *Setting the Move Schedule (page 40)*.

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 *Setting Cleanup Options (page 40)*

Vault: 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 *Setting Vault Rules (page 41)*.

Groom: The fields presented on the Groom 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 *Setting Groom Rules (page 43)*

5.9 - 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.

With File Dynamics, 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 inactive users organizational unit, the access rights for that user are immediately removed.

5.9.1 - Creating an Inactive Users Organizational Unit

1. In the Admin Client, click the *Identity Driven* tab.
2. Click *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.
7. Continue with *Creating an Inactive Users Folder (page 49)*

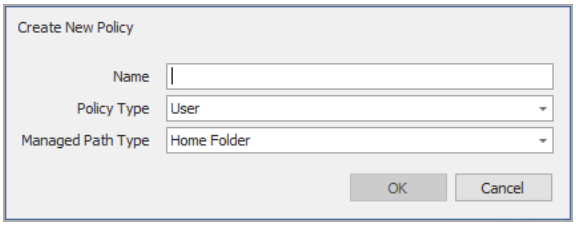
5.9.2 - Creating an Inactive Users Folder

1. Launch Windows Explorer.
2. On a network share, create a folder to store inactive user home folders.
3. Give the folder a descriptive name, such as "Inactive Users."
4. Continue with *Creating an Inactive Users Policy (page 49)*

5.9.3 - Creating an Inactive Users Policy

1. In the Admin Client, click the *Identity Driven* tab.
2. Click *Policies*.

3. In the *Manage* menu, select *New > User Home Folder*.
   The following dialog box appears:



4. Specify a descriptive name in the *Name* field and click *OK*.
   The Policy Options page appears.
5. Continue with *Setting Inactive Users Policy Associations (page 50)*.

5.9.4 - Setting 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 3 under *Creating an Inactive Users Organizational Unit (page 49)*.
3. Click *Add* to add the inactive users organizational unit to the *Selected Object* panel.
4. Click *OK* to save the setting.
5. Proceed with *Setting Inactive Users Policy Provisioning Options (page 50)*

5.9.5 - 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 permissions check boxes.
   This assures that User objects placed in the inactive users organizational unit do not have permissions to home folders.
3. Click *Apply* to save the setting.
4. Proceed with *Setting Inactive Users Policy Target Paths (page 50)*

5.9.6 - Setting Inactive Users Policy Target Paths

1. In the left pane, click *Target Path Options*.
2. Click *Add*, then browse to and select the inactive users folder that your created in Step 2 under *Creating an Inactive Users Folder (page 49)*
3. Click *Add* to add the inactive users folder to the *Selected Items* panel.
4. Click *Apply* to save the setting.
5. Proceed with *Setting Inactive Users Policy Cleanup Options (page 51)*

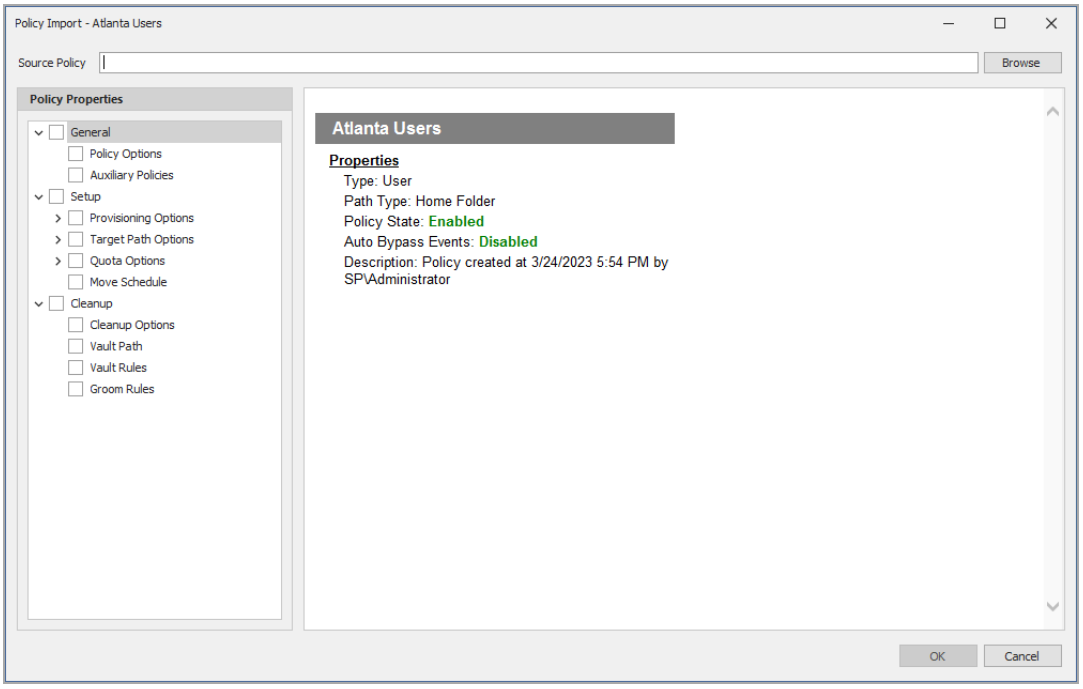
5.9.7 - Setting Inactive Users Policy Cleanup Options

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.

5.10 - Copying Policy Data

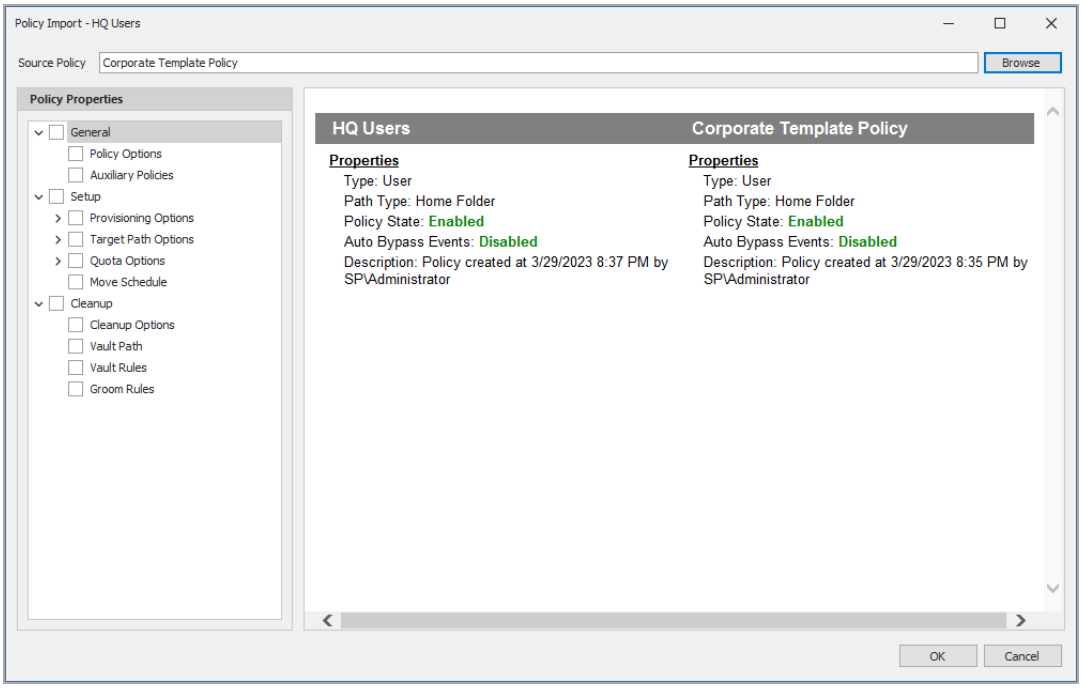
Policy Import allows you to copy all or a portion of the policy settings of one policy into another policy.

1. In the Admin Client, click the *Identity Driven* tab.
2. Click *Policies*.
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 with the name of the policy from which you are copying settings.

5. In the Policy Properties tree, click the settings from the policy you want to import.



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

5.11 - Using a Policy to Manage Auxiliary Storage

Auxiliary storage allows administrators to create 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 File Dynamics creates and provisions his or her home folder. The user never sees the auxiliary storage, because the policy gives Read and Write permissions only to the HR department.

Additionally, the auxiliary storage can be as large as the policy specifies. This means that even though the user's home folder might have 500 MB, the auxiliary storage could be as small as the HR department needs 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.

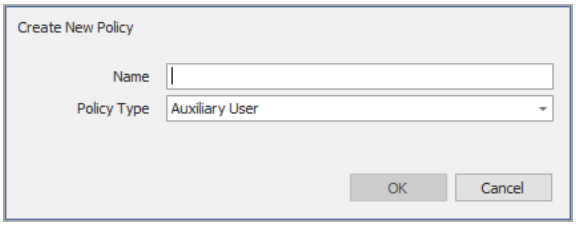
Of course, you can configure auxiliary user storage so that a user can access it. For example, you might want to have a separate storage folder for application-specific files. It is important to remember that auxiliary storage is simply another home folder for a user. To provide access to this storage, 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 shares that differ from the location of the user's home folder.

The life cycle management capabilities in File Dynamics 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 *Establishing Auxiliary Purpose Mappings (page 56)*.

5.11.1 - Creating an Auxiliary Storage Policy

1. In the Admin Client, click the *Identity Driven* tab.
2. Click *Policies*.
3. In the *Manage* menu, select *New* > *Auxiliary*.
   The following dialog box appears:



4. Specify a descriptive name in the *Name* field, such as “HR-AUX,” and click *OK*.
   The Policy Options page appears.
5. Proceed with *Setting Auxiliary Storage Policy Options (page 53)*

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 (page 53)*

Enabling Auxiliary Storage Extended Options

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.

   We recommend that once you have made an entry in the *Tag* field, 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 (page 54)*

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 Permissions* check boxes.
   - If you want the associated user to have access to the auxiliary storage folder, select the appropriate permissions from the *Default Permissions* 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.
5. Proceed with *Setting Additional Auxiliary Storage Options (page 54)*

Setting Additional Auxiliary Storage Options

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

Target Path Options: 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 share specific to the HR Department.

The fields presented on the Target Path 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 target paths, see *Setting Target Paths (page 36)*.

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 *Setting Quota Options (page 38)*

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 *Setting the Move Schedule (page 40)*.

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 *Setting Cleanup Options (page 40)*

Vault: The fields presented on the Vault 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 *Setting Vault Rules (page 41)*.

Groom: The fields presented on the Groom 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 *Setting Groom Rules (page 43)*.

2. Proceed with *Linking a User Home Folder Policy to an Auxiliary Storage Policy (page 55)*

5.11.2 - 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 *Provisioning Auxiliary Storage for Existing Users (page 55)*

1. In the Admin Client, click the I*dentity Driven* tab.
2. Click *Policies*.
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.

5.11.3 - Provisioning Auxiliary Storage for Existing Users

This procedure lets File Dynamics 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, File Dynamics corrects any potential problems.

1. In the Admin Client, click the *Identity Driven* tab.
2. Click *Policies*.
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 if 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 SAM 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.

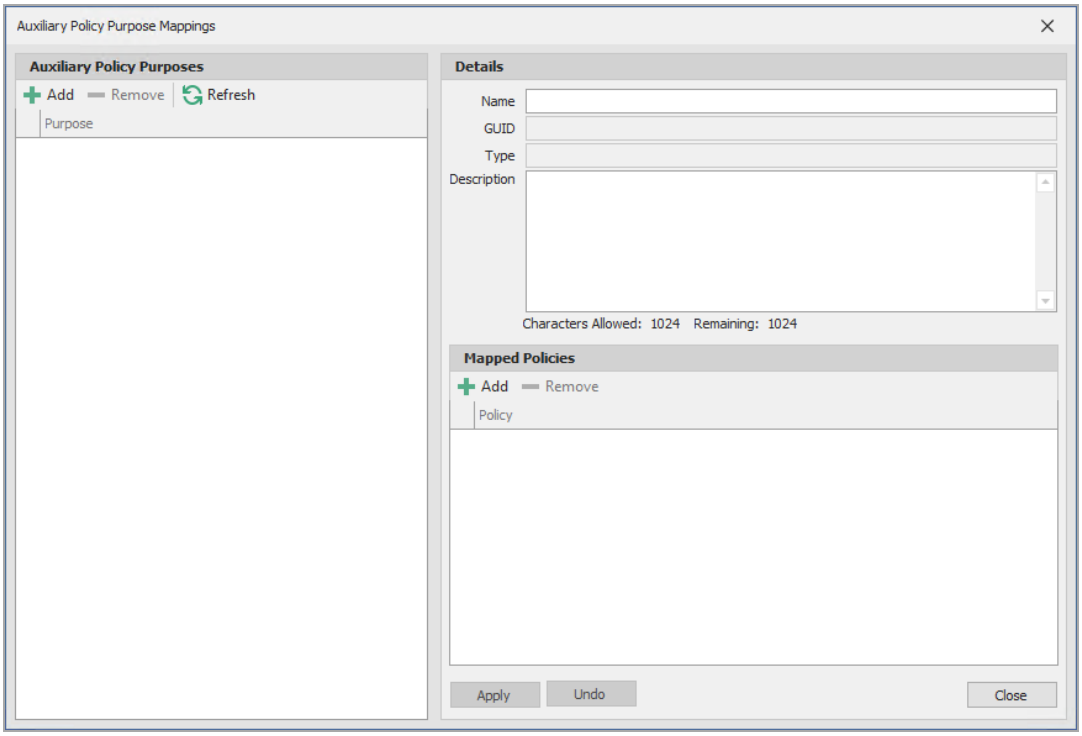
6. Click *Preview*.
   Preview mode allows you to view the results of an action without actually making changes.
7. Click *Execute* to set the Auxiliary Attribute.
8. From the *Auxiliary Policy Action* drop-down menu, select *Apply Quota*.
9. Select *Set quota for all directories*. Overwrite any existing quota assignments except where the existing quota is larger than the quota defined in the policy.
10. Click *Preview*.
11. Click *Execute* to set the quota for the auxiliary storage.

5.11.4 - Establishing Auxiliary Purpose Mappings

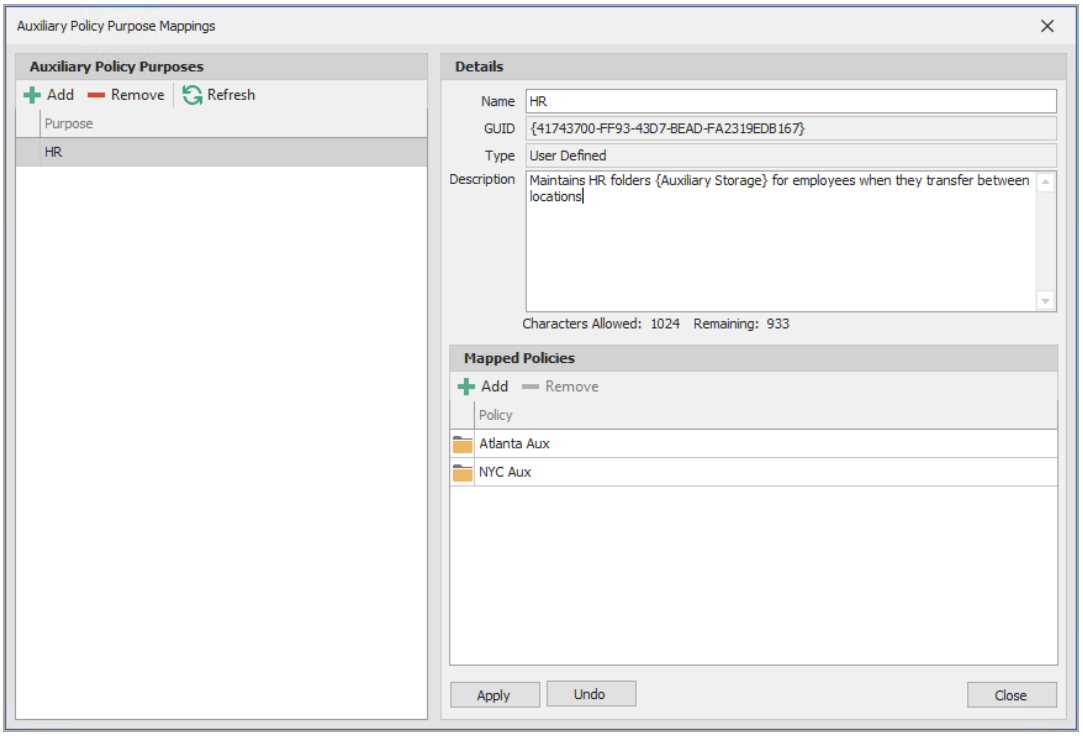
Auxiliary Purpose Mappings are the means of moving a user's auxiliary storage when a user is moved in Active Directory. For example, if a user were moved from the Atlanta container to the Detroit container, and the two container's Auxiliary Storage policies were part of the same Auxiliary Purpose Mapping, the user's Auxiliary storage would move to the Detroit Auxiliary storage location.

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 *Identity Driven* tab.
2. Click *Policies*.
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.
   You can hold down the Control key to select multiple Auxiliary Policy purposes.
   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 Purpose Mapping.

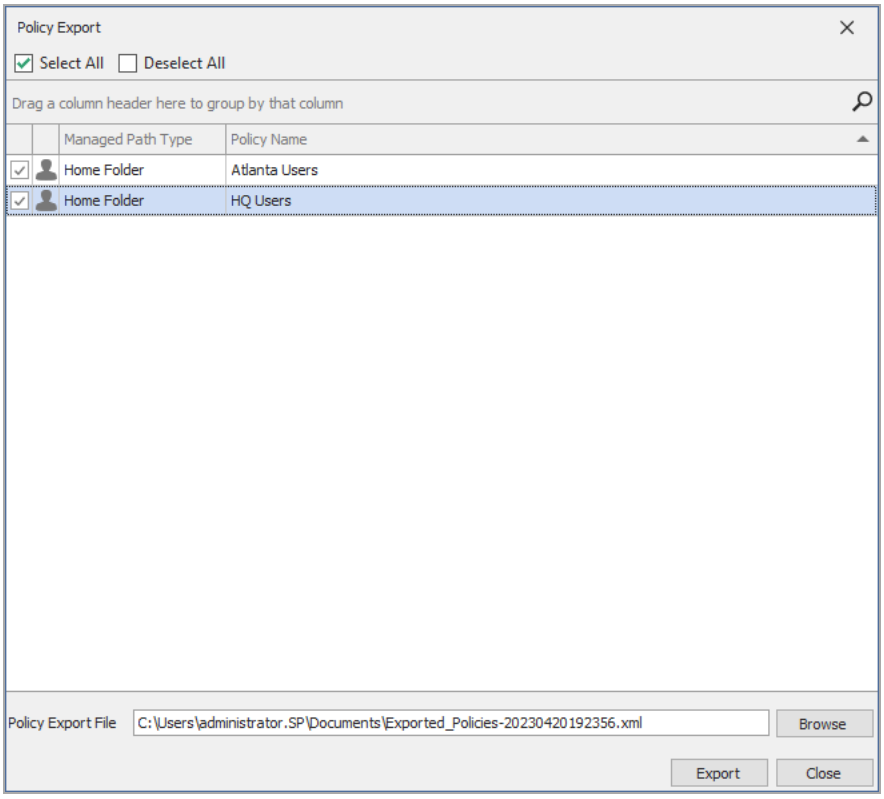


11. Click *Apply*.
12. Click *Close*.

5.12 - Exporting Policies

File Dynamics provides the ability to export policies so that they can be imported later. For example, many customers first evaluate File Dynamics 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 *Identity Driven* tab.
2. Click *Policies*.
3. From the *Manage* drop-down menu, select *Export Policies*.



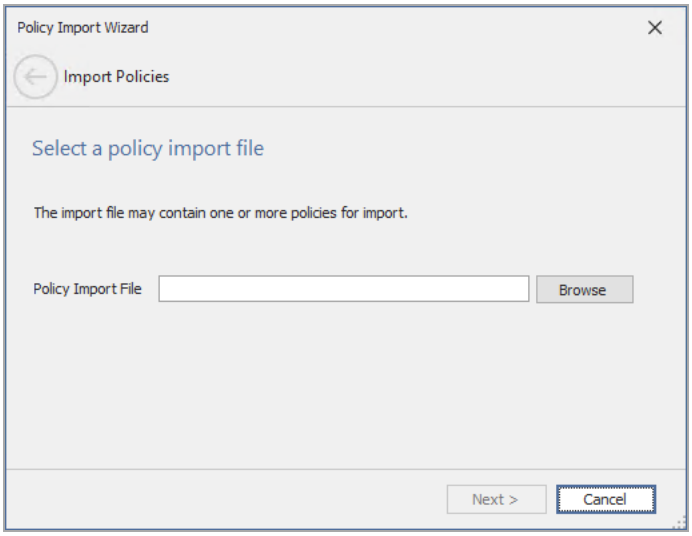
4. Select the check boxes of those policies you want to export.
5. Accept the default export filename or indicate a new one in the *Policy Export File* field.
6. Accept the default path of the file or browse to select a new path.
7. Click *Export*.
8. After you are notified that the policies have been exported, click *Close*.

5.13 - Importing Policies

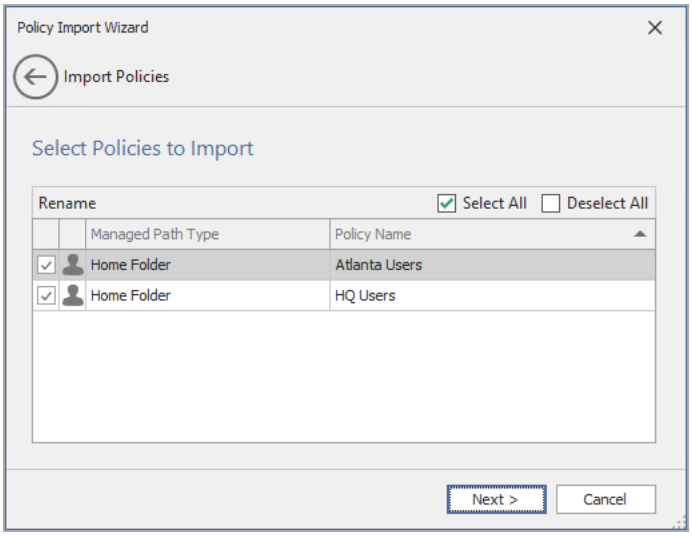
Previously exported policies are imported by using the Import Policies feature.

1. In the Admin Client, click the *Identity Driven* tab.
2. Click *Policies*.

3. From the *Manage* drop-down menu, select *Import Policies*.
   The following wizard is launched.



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 File Dynamics to manage the managed paths that are assigned to Group objects or containers in Active Directory.

In a File Dynamics environment, group-based or container-based storage is referred to as “collaborative storage,” because File Dynamics, 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 *Managing Existing User Storage (page 15)*, 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 groom 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 *Managing Collaborative Storage (page 69)*.

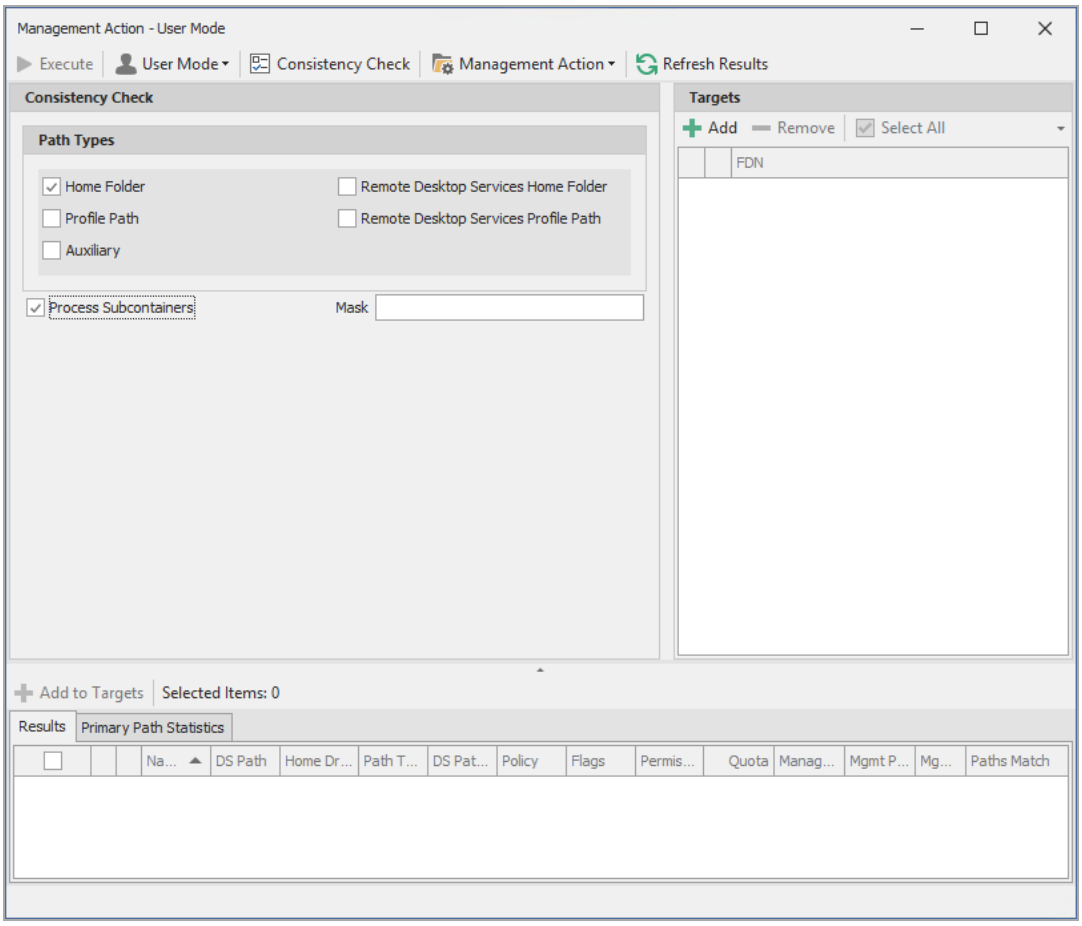
The process for managing existing storage and creating personal subfolders involves the tasks linked below.

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

A collaborative managed path attribute is created by File Dynamics when the Active Directory schema is extended. The attribute is used to associate a Group or container object with a managed path.

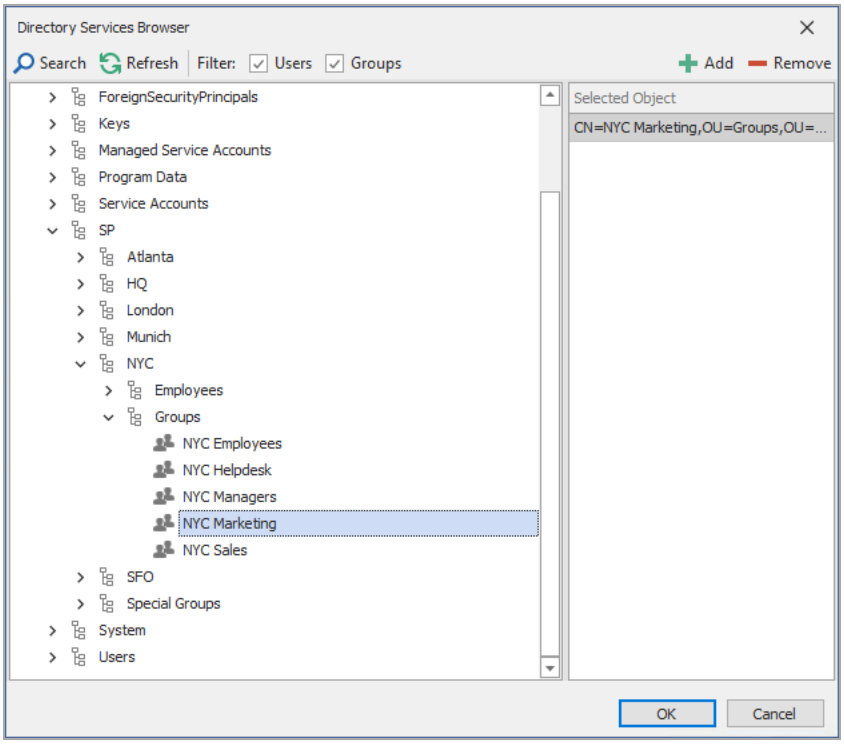
In this procedure, you assign a managed path to a Group or container object that has existing collaborative storage and then assign the storage path.

1. In the Admin Client, click the *Identity Driven* tab.
2. Click *Actions*.



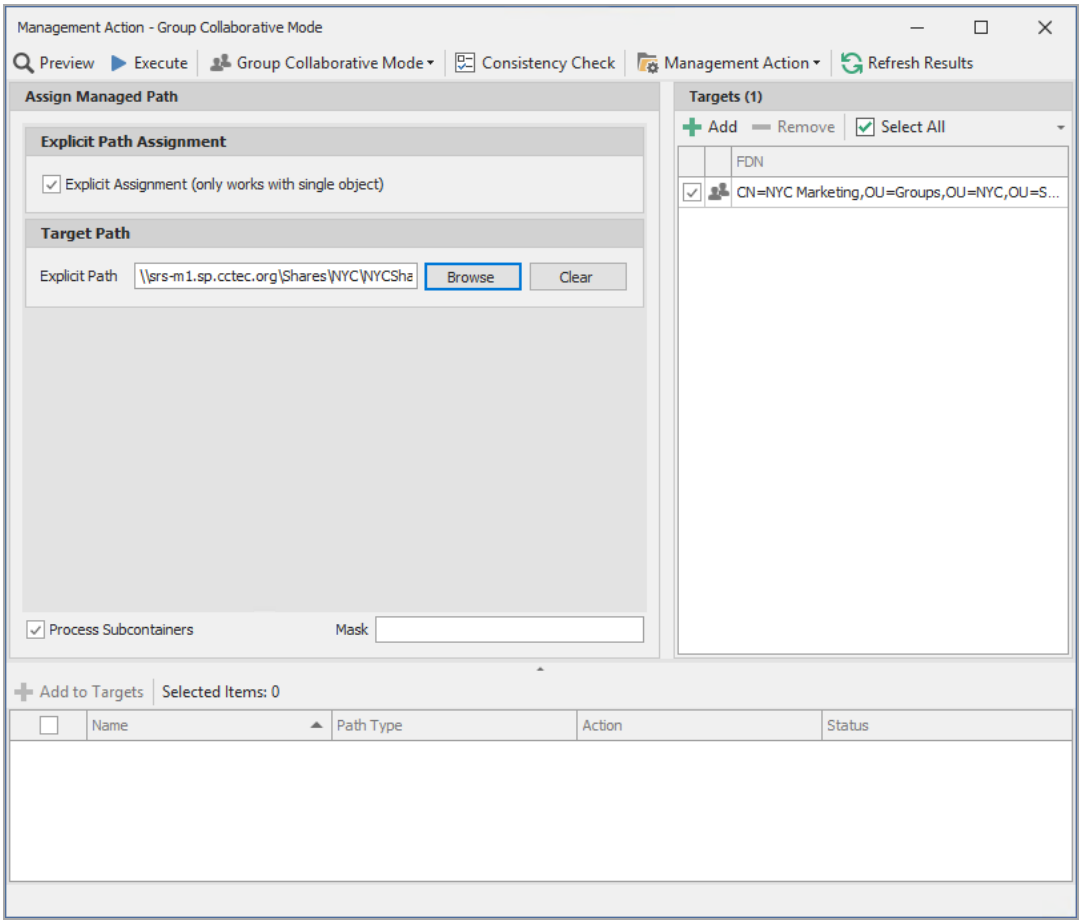
3. Use the menu to replace *User Mode* with *Group Collaborative* or *Container Collaborative* mode.
4. In the *Targets* region, click *Add*.

5. Browse to locate and select the container or group you want to associate to a collaborative 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 File Dynamics.

10. Click *Preview*.



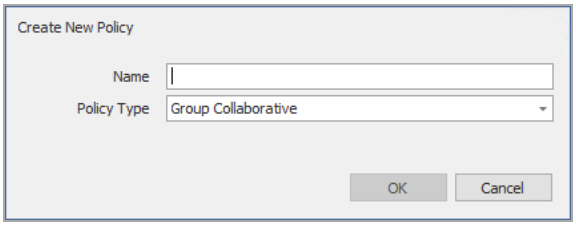
11. Click *Execute*.
12. Observe in the bottom portion of the page that the managed path has been set.
13. Continue with *Creating a Collaborative Storage Policy (page 64)*.

6.2 - Creating a Collaborative Storage Policy

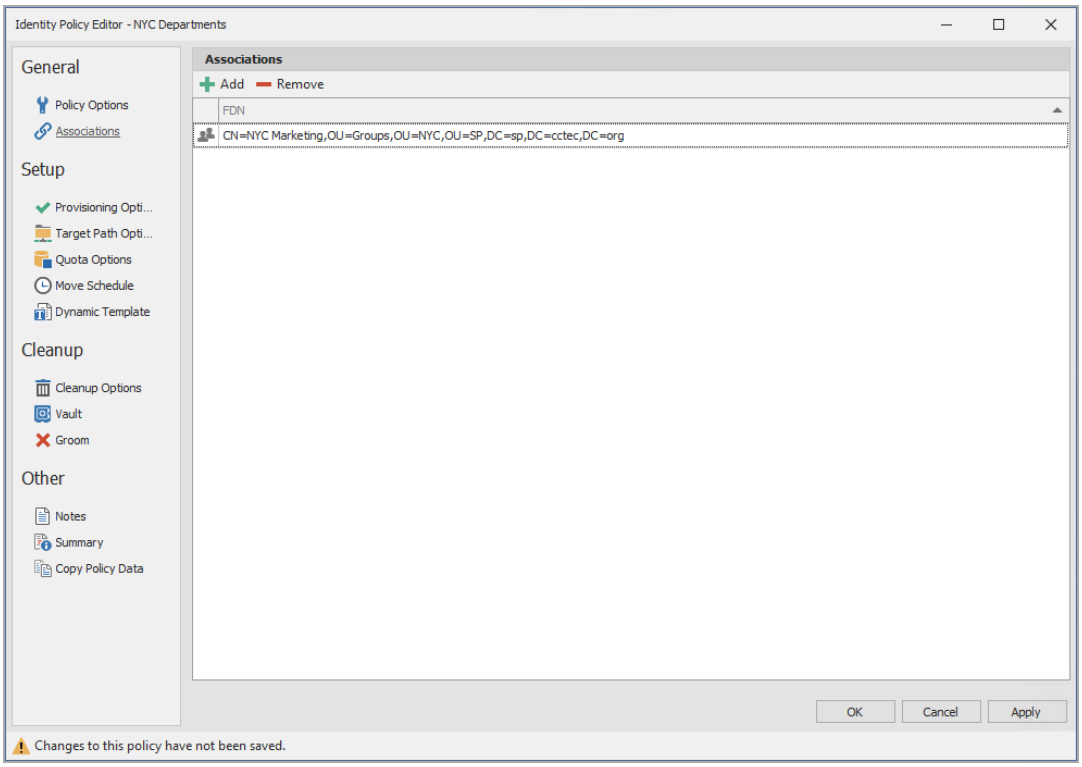
After you assign a managed path, the next step is to create a Collaborative Storage policy for the group or container you selected in Step 5 under *Assigning a Managed Path to Existing Group-based or Container-based Storage (page 61)*. In this procedure, the Collaborative Storage policy will apply to 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 *Identity Driven* tab.
2. Click *Policies*.

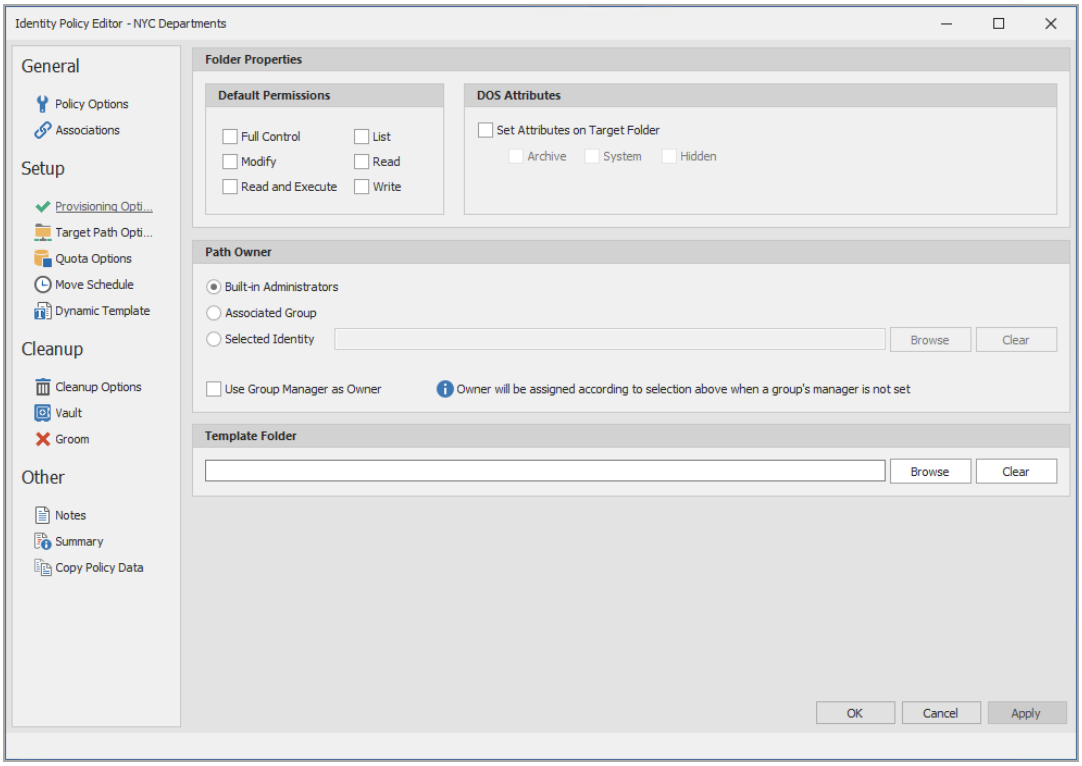
3. Select *Manage > New > Group Collaborative*.
   The following dialog box appears:



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 under *Assigning a Managed Path to Existing Group-based or Container-based Storage (page 61)*.
7. Click *Add*, then click *Apply* to save your changes.

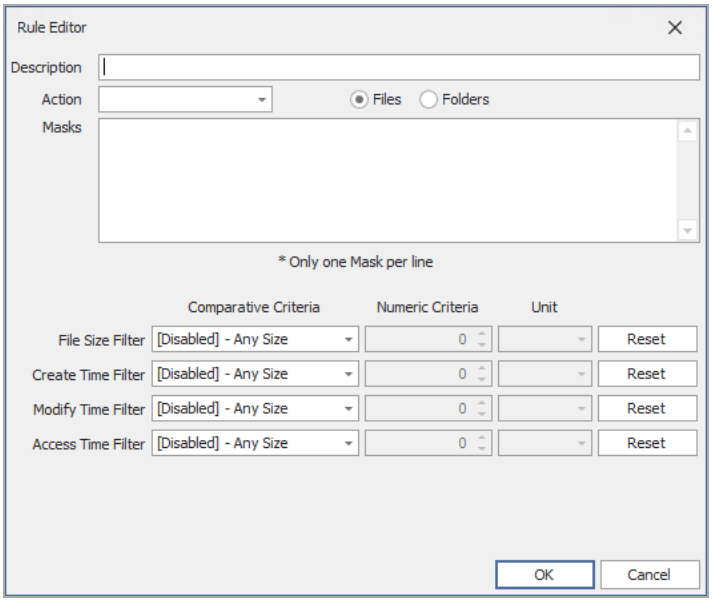


8. In the left panel, click *Provisioning Options*.



9. In the *Default Permissions* region, specify the permissions that you want the managed object to have to the collaborative managed path.
10. (Conditional) Select any DOS Attributes you want to apply to the target folder.
11. In the *Path Owner* region, select one of the following options:
    - **Built-in Administrator:** If you want the owner of the storage to be the Built-in Administrator, select this option.
    - **Associated Group:** The associated group is the group whose folder you are creating. If you want the associated group to own their own folder, select this option.
    - **Selected Identity:** If you want another object to be the owner of the folder, browse and select the object.
    - **Use Group Manager as Owner:** To use the Active Directory Group Object Manager as the owner, select this check box. If the manager is not found, File Dynamics will use the option selected above.
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 under *Assigning a Managed Path to Existing Group-based or Container-based Storage (page 61)*.
14. Click *Add*, then click *OK*.
15. In the left panel, select *Quota Options*.

16. In the *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 Groom.
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 Rule Editor dialog box, indicate the files that File Dynamics will groom from the collaborative storage pertaining to this policy.
    For information on each of the fields in this dialog box, refer to *Setting Groom Rules (page 43)*
22. Click *OK* to save the groom rule.
23. Continue with *Performing Management Actions (page 67)*

6.3 - Performing Management Actions

This procedure enforces all of the policy specifications to the collaborative storage managed by File Dynamics.

1. In the Admin Client, click the *Identity Management* tab.
2. Click *Objects*.
3. Browse to and select the group or container that you specified in Step 5 under *Assigning a Managed Path to Existing Group-based or Container-based Storage (page 61)*.

4. Right-click the group or container and select *Group Collaborative > Manage*.
5. Click *Preview*.
6. Verify that the following message appears in the lower panel of the window:
   `Existing managed path location would be catalogued.`
7. Click *Execute*.
8. From the *Management Action* menu, select *Apply Attributes*.
9. Select the *Use policy defined DOS attributes* check box.
10. Click *Preview*.
11. Verify that the following message appears in the lower panel of the window:
    `Apply attributes will be scheduled for object.`
12. Click *Execute*.
13. From the *Management Action* menu, select *Apply Quota*.
14. Verify that the *Set quota for directories that do not currently have a quota defined* option is selected.
15. Click *Preview*.
16. Verify that the following message appears in the lower panel of the window:
    `Apply quota will be scheduled for object.`
17. Click *Execute*.
18. From the *Management Action* menu, select *Apply Permissions*.
19. Click *Preview*.
20. Verify that the following message appears in the lower panel of the window:
    `Apply rights will be scheduled for object.`
21. Click *Execute*.
22. From the *Management Action* menu, select *Groom*.
23. Click *Preview*.
24. Verify that the following message appears in the lower panel of the window:
    `Groom will be scheduled for object.`
25. Click *Execute*.

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 *Managing Collaborative Storage (page 69)*.

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.

File Dynamics 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 three ways:

- Creating a single project folder where all project members have access and have the same permissions.
- 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 Collaborative Storage Policy Dynamic Template Processing (page 85)*.
- Creating a multi-group owned project folder with each group having distinct access rights. This capability is available through Multi-Principal Group Collaborative Storage policies. For more information, see *Create a New Multi-Principal Collaborative Storage Policy (page 96)*.

File Dynamics works with Active Directory 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 `#REMOVED#username`, 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
- Group Multi-Principal collaborative policies

7.1 - Creating Collaborative Storage Objects in Active Directory

For File Dynamics to manage collaborative storage, it must have the following Group or User objects located in an organizational unit in Active Directory:

- -MEMBER-
- -MANAGER-

- -GROUP-

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

You only need to create these objects in one organizational unit.

1. At a Windows workstation, launch Active Directory Users and Computers.
2. Right-click an organizational unit and select *New > Group*.
3. Give the Group object the name `-MEMBER-` and leave the Group Scope setting as *Global* and the Group Type setting as *Security*.
4. Repeat Step 2 to create a `-MANAGER-` group and a `-GROUP-` group.
   These three objects are used to automatically set permissions 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 Templates

When you created User Home Folder policies in *Managing User Home Folders (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 File Dynamics creates a collaborative managed path for a group, File Dynamics examines the policy to determine if a template has been defined and, if so, it copies the contents of the template directory along with all attributes, permissions, and quotas.

If you want to enable quota management for collaborative storage folders, the folders must have the following characteristics:

- Be located on servers running either Windows Server 2008 or above
- Have a firewall exception for the Remote File Server Resource Manager

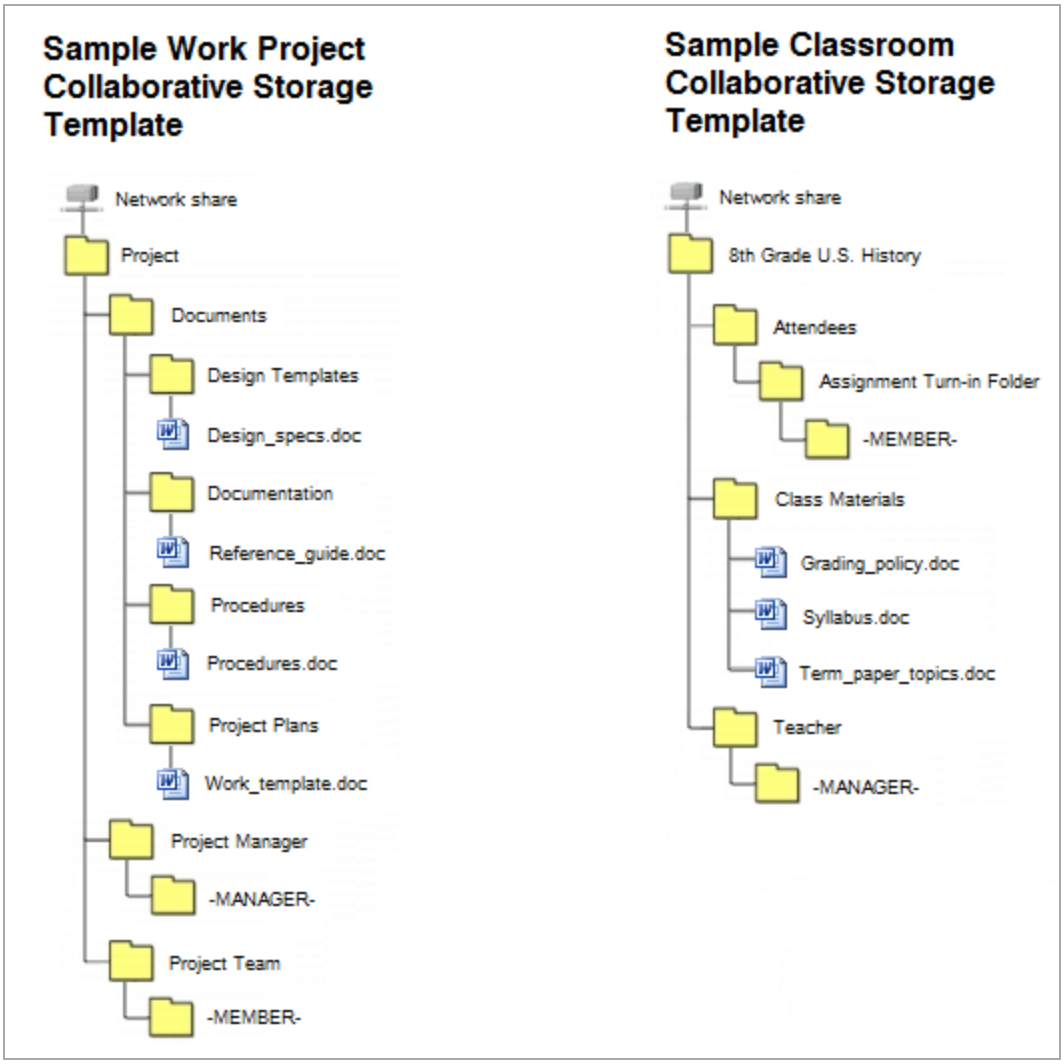
Unlike user home folders, collaborative storage managed by File Dynamics is dynamic in that the member attributes of Group objects are monitored so that the addition and deletion of members can have a direct impact on the structure of the individual file system of a group as well as the permissions given 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.

Sample Collaborative Storage Templates



In the template structures above, both have –MANAGER– 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 –MANAGER– 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

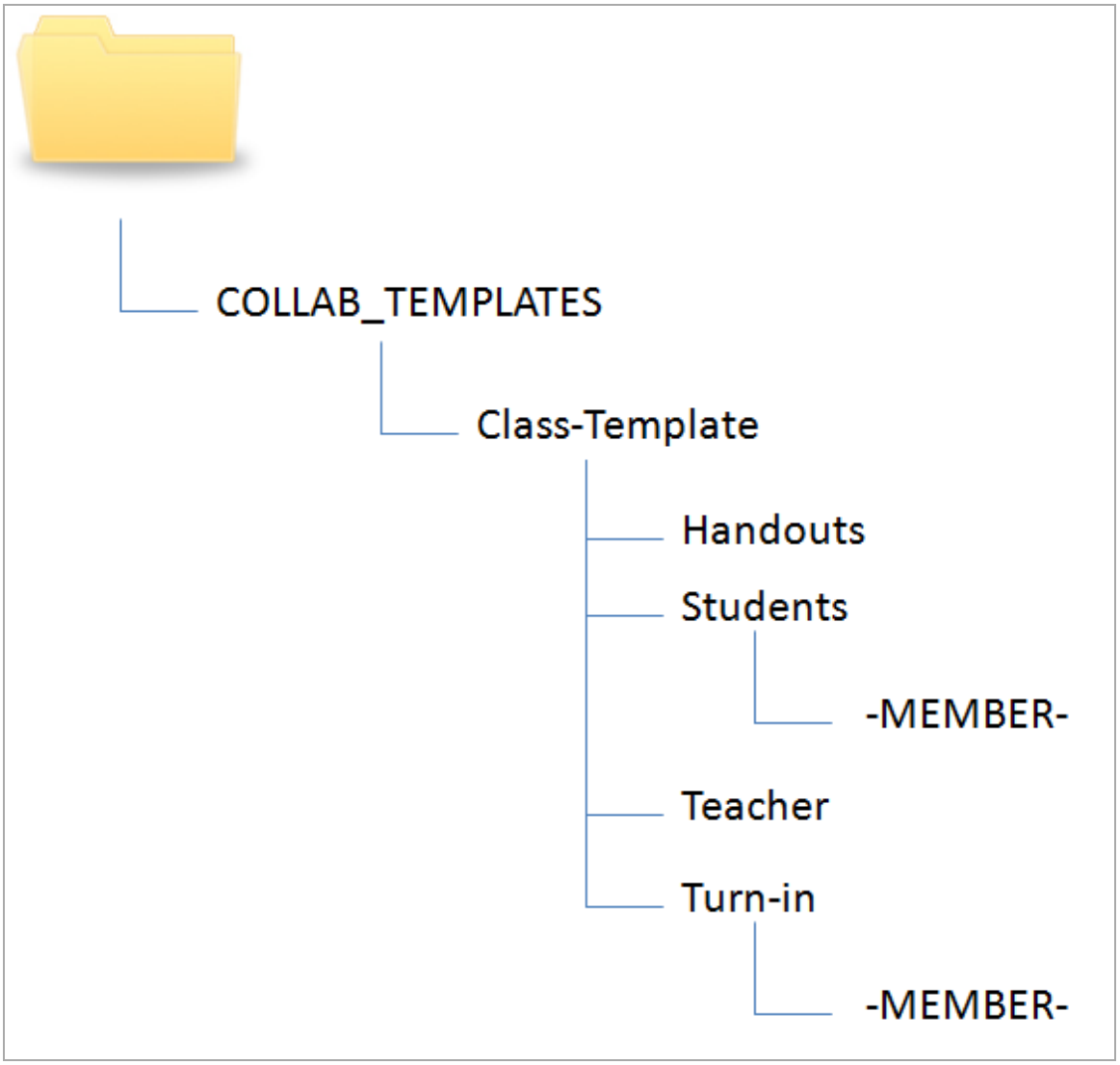
1. Launch Windows Explorer.
2. On a network share, create a file structure for a group that you will provide collaborative storage.
3. Place any documents you want available to the group in the appropriate folders.

7.5 - Setting Up Security for a Collaborative Storage Template

Properly setting security and permissions for collaborative storage in Active Directory 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.

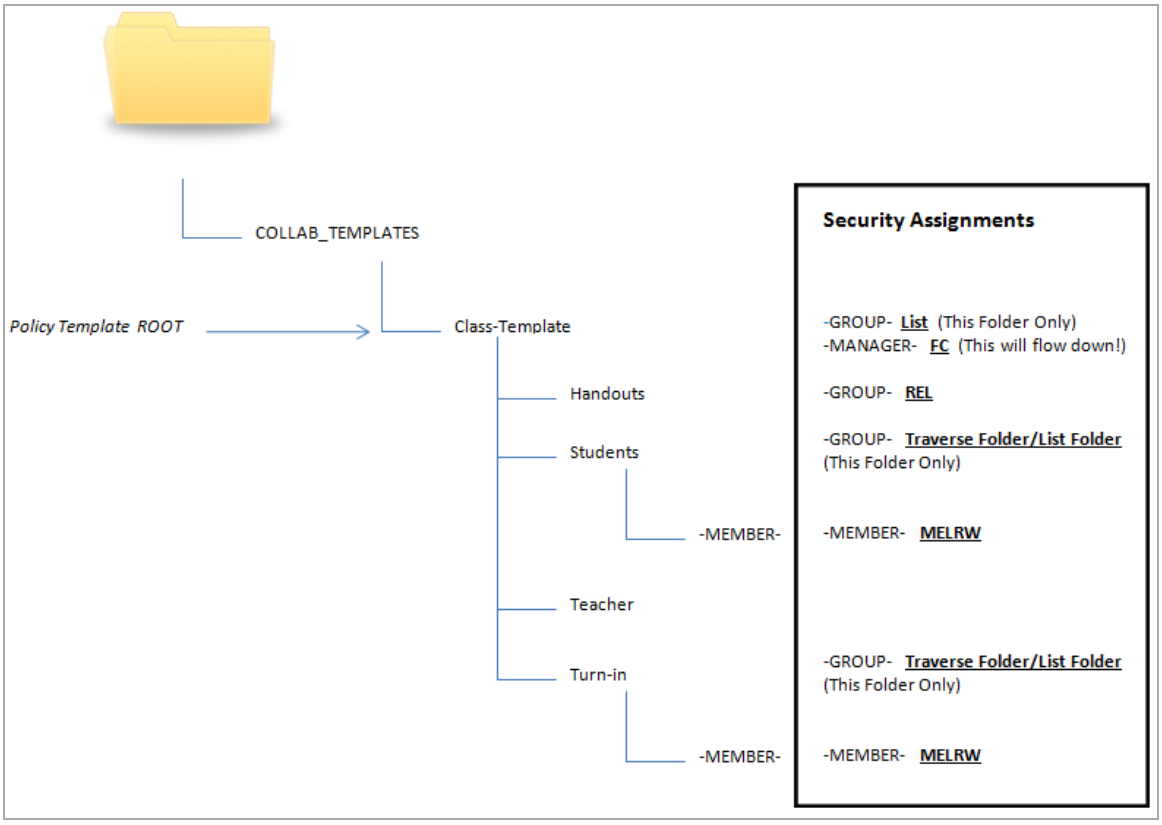
Common Academic Setting Collaborative Storage Template Structure



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.

Security Permissions for Each Folder in the Sample Template

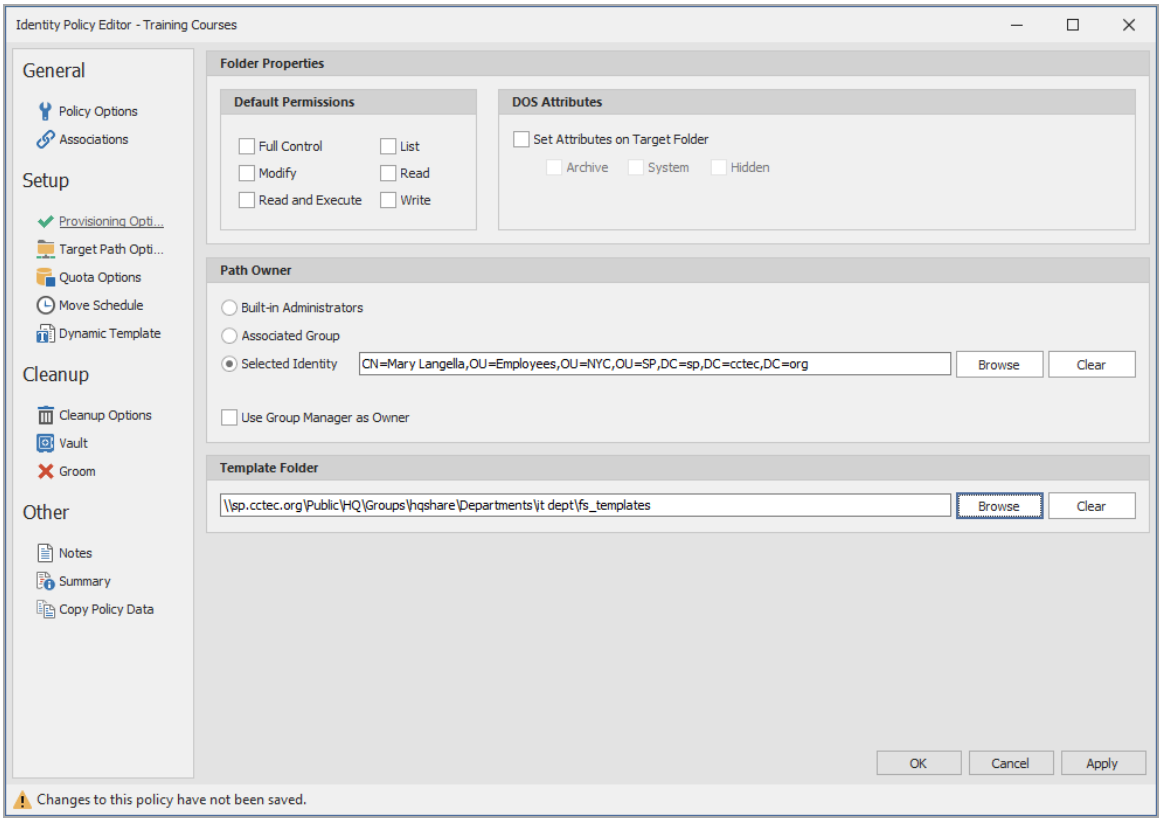


The diagram above shows the security permissions that must be established for each of the folders in the template structure. For example, the `-GROUP-` object must be given the List permission to the `Class-Template` folder and the `-MANAGER-` object must be given Full Control. List, Traverse Folder, and List Folder are all advanced permissions.

When you set the provisioning options for the Collaborative Storage policy, you must override the path owner and indicate an owner, unless you want all users in the group to have all rights to the collaborative storage area.

In the example in the figure above, Teacher1 is specified as the owner.

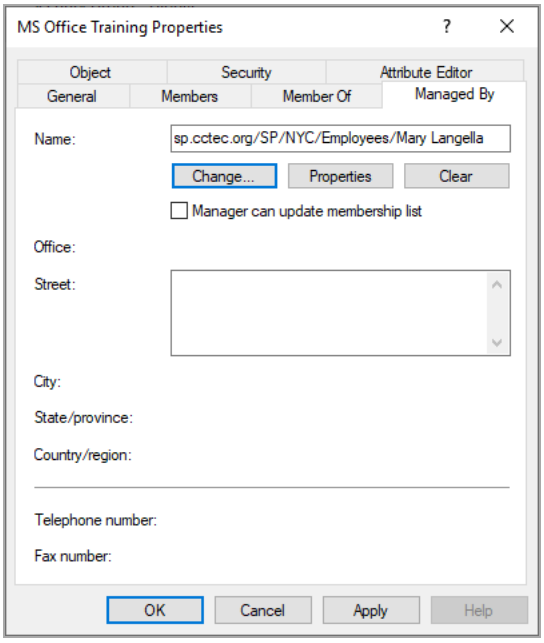
Owner of a Collaborative Storage Folder



The *Selected Identity* option is selected and the owner of the folder is set to Mary Langella. The template is indicated in the Template Folder region.

You use the Group properties of Active Directory Users and Computers to indicate the group owner in the Managed By screen. In this example, the owner is Mary Langella.

Group Owner Specified in Managed By Page



Establishing an owner in the *Name* field enables the `-MANAGER-` object to function properly.

7.5.1 - Establishing Permissions

You establish the permissions specified for each of the folders in the second diagram under *Setting Up Security for a Collaborative Storage Template (page 72)* through the Windows Explorer *Security* tab. Permissions such as Traverse Folder, are special permissions.

To set special permissions:

1. In Windows Explorer, right-click the desired folder and select *Properties*.
2. Click the *Security* tab.
3. Click *Advanced*.
4. Click *Change Permissions*.
5. Click *Add*.
6. In the *Enter the object name to select* field, specify the name of the desired user or group and click *OK*.
7. In the new dialog box, use the *Apply to* drop-down menu to select the desired application level, select the check boxes for all special permissions for the user or group, and click *OK*.

7.5.2 - Configuring Permissions for the Group Manager

This procedure grants Manager permissions to the group's designated manager, meaning that he or she is given all permissions needed to view and modify any document within the structure of the collaborative storage area.

1. Launch Windows Explorer.
2. In the file structure that you created earlier, browse to and right-click the topmost folder, then select *Properties*.
   For example, in the sample work project collaborative storage template example in the first diagram under *Setting Up Security for a Collaborative Storage Template (page 72)*, the topmost folder would be the `Project` folder.
3. Click the *Security* tab.
4. Click *Edit*.
5. Click *Add*.
6. In the *Enter the object names to select* field, specify `-MANAGER-`.
7. Click *Check Names*.
8. Click *OK*.
9. In the Permissions dialog box, select the *Modify* check box and click *OK* to save the settings.
10. Click *OK* to close the Properties dialog box.

7.5.3 - Configuring Permissions for the Group Members' Personal Folders

This procedure grants the permissions needed for group members to work in their personal folders within the collaborative storage area.

1. Launch Windows Explorer.
2. In the structure that you created under *Creating a Collaborative Storage Template (page 72)*, browse to and right-click the `-MEMBER-` folder, then select *Properties*.
3. Click the *Security* tab.
4. Click *Edit*.
5. Click *Add*.
6. In the *Enter the object names to select* field, specify `-MEMBER-`.
7. Click *Check Names*.
8. Click *OK*.
9. In the Permissions dialog box, select the *Modify* check box and click *OK* to save the settings.
10. Click *OK* to close the Properties dialog box.

7.5.4 - Configuring Group Member Permissions to Other Folders

This procedure grants List and Read permissions to other areas of the collaborative storage area.

1. Launch Windows Explorer.
2. In the structure that you created under *Creating a Collaborative Storage Template (page 72)*, browse to and right-click one of the subfolders, then click *Properties*.
   For example, in the sample work project collaborative storage template example in the first diagram under *Setting Up Security for a Collaborative Storage Template (page 72)*, a subfolder would be the `Documents` folder.
3. Click the *Security* tab.
4. Click *Edit*.
5. Click *Add*.
6. In the *Enter the object names to select* field, specify `-MEMBER-`.
7. Click *Check Names*.
8. Click *OK*.
9. Click *OK* to close the Properties dialog box.
10. Repeat Step 1 through Step 9 for each additional folder where you want to grant users List and Read permissions.

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.

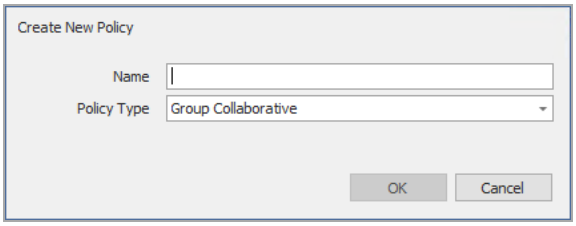
A Group Collaborative Storage policy creates storage for a group when a Group object is created in an organizational unit where the policy is associated. For example, if a cross-functional team named HEALTHFAIR2018 is created in an organizational unit associated with the Group Collaborative Storage policy, 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. In the Admin Client, click the *Identity Driven* tab.
2. Click *Policies*.

3. In the *Manage* menu, select *New* > *Group Collaborative*.
   The following dialog box appears:



4. Specify a descriptive name in the *Name* field.
   The Policy Options page appears.
5. Continue with the following.

7.7.1 - Setting Group Collaborative Storage Policy Options

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

Group Policies in File Dynamics 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 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 *Creating a Blocking Policy (page 18)*.
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 *Apply* to save your settings.
5. Proceed with *Setting Group Collaborative Storage Policy Associations (page 79)*.

7.7.2 - Setting Group Collaborative Storage Policy Associations

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

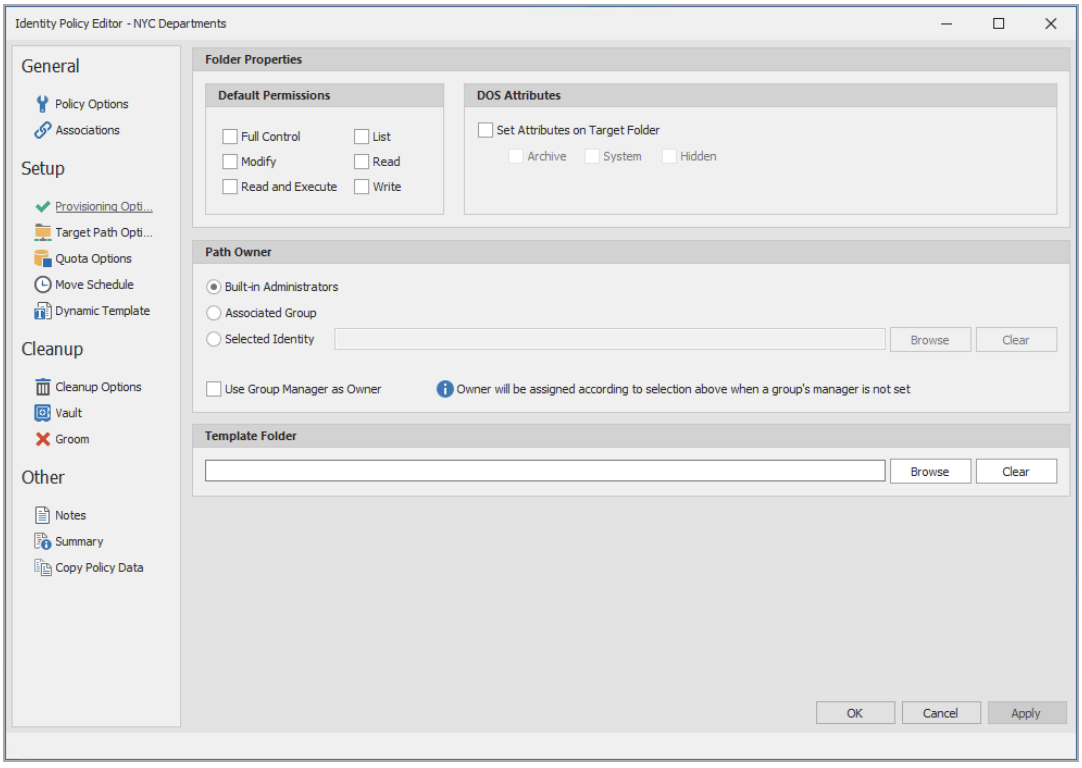
1. In the left pane, click *Associations*.
2. Click *Add* to bring up the Directory Services Browser.

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 Directory Services Browser is closed and the object is displayed in fully qualified name format in the right pane of the window. For example, `OU=Groups,OU=Munich,DC=SP,DC=cctec,DC=org`.
5. Click *OK* to close the Directory Services Browser.
6. Click *Apply* to save your settings.
7. Proceed with *Setting Group Collaborative Storage Policy Provisioning Options (page 80)*.

7.7.3 - Setting Group Collaborative Storage Policy Provisioning Options

The Provisioning Options page is where you indicate collaborative storage permissions, 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, select the desired permissions to be applied to the target folder.
   If you chose to create a Collaborative Storage template, the permissions will be

applied from the template that you created earlier under *Configuring Permissions for the Group Members' Personal Folders (page 77)* and *Configuring Group Member Permissions to Other Folders (page 77)*.

3. In the *Path Owner* region, select one of the following options:
    - **Built-in Administrator:** If you want the owner of the storage to be the Built-in Administrator, select this option.
    - **Associated Group:** The associated group is the group whose folder you are creating. If you want the associated group to own their own folder, select this option.
    - **Selected Identity:** If you want another object to be the owner of the folder, browse and select the object.
    - **Use Group Manager as Owner:** To use the Active Directory Group Object Manager as the owner, select this check box. If the manager is not found, File Dynamics will use the option selected above.
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 under *Creating a Collaborative Storage Template (page 72)*.
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 the first diagram under *Setting Up Security for a Collaborative Storage Template (page 72)*, you would select "8th Grade U.S. History."
7. Click *Apply* to save your settings.
8. Proceed with *Setting Group Collaborative Storage Policy Target Paths (page 81)*.

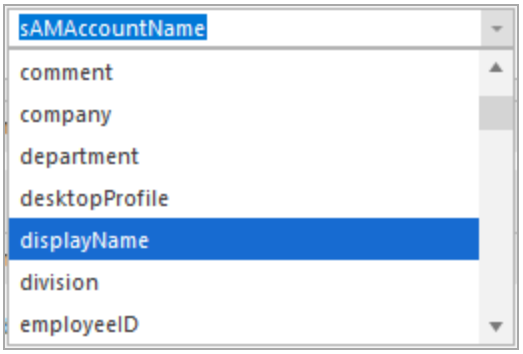
7.7.4 - Setting Group Collaborative Storage Policy Target Paths

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 Path Options*.
2. In the *Managed Path Naming Attribute* region, do one of the following:
    - From the drop-down menu, select the single-value Active Directory attribute you want as the means of naming your collaborative storage folders.
    - Click *Link Action Block* and select a previously saved Action Block for the naming attribute.

   For some organizations, having the default `sAMAccountName` attribute as the means of naming group home folders is not desirable. To allow File Dynamics to create a collaborative storage folder with a name you can define, you can select a different

attribute from the drop-down list.



Once you have saved the policy, you can use an account provisioning system such as NetIQ Identity Manager to automatically populate the selected attribute with the desired folder name and then File Dynamics will automatically provision the group home folder based on this attribute setting.

For existing groups whose collaborative storage folders you would like to change to a new attribute value, you would follow the same procedures, followed by performing an Enforce Policy Path Management Action.

For specifications pertaining to Managed Path Naming Attribute, see *Managed Path Naming Attribute Specifications (page 265)*.

3. In the *Target Placement* region, select a option from the *Distribution* drop-down menu.

   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 collaborative storage folders according to shares 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 shares 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 shares of different sizes.

4. From the *Leveling* drop-down menu, choose an option.

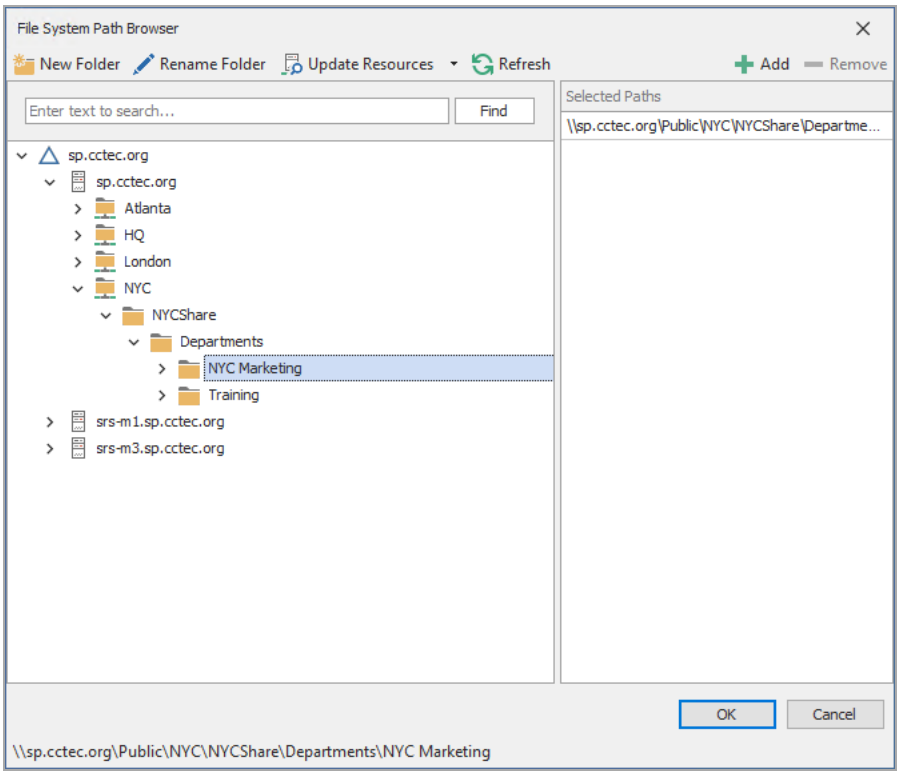
   This setting is used to structure the group home folders so that they are categorized by the first or last letter of a group name through a subordinate folder. For example, if you choose *First Letter*, and the *Leveling Length* field is set to *1*, a group named

Engineering has a home folder located in a path such as `\\SERVER1-DNS-NAME\GROUPS\E\Engineering`.

The *Last Letter* means the last character of the attribute File Dynamics uses to create storage.

The *Leveling Length* field allows you to enter up to 4 characters. This makes it so that you can organize folders by year. For example, if your Leveling Algorithm setting is *Lirst Letter*, and the *Leveling Length* setting is *4*, a group named Engineering has a home folder located in a path such as `\\SERVER-DNS-NAME\GROUPS\Engi\Engineering`.

5. For each target path that you want to establish, click *Add* to access the Path Browser.
6. Browse to the location of the target path you want and click *Add* to add the target path to the *Selected Paths* pane.



7. Click *Apply* to save your settings.
8. Proceed to *Setting Group Collaborative Storage Policy Quota Options (page 83)*.

7.7.5 - Setting Group Collaborative Storage Policy Quota Options

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

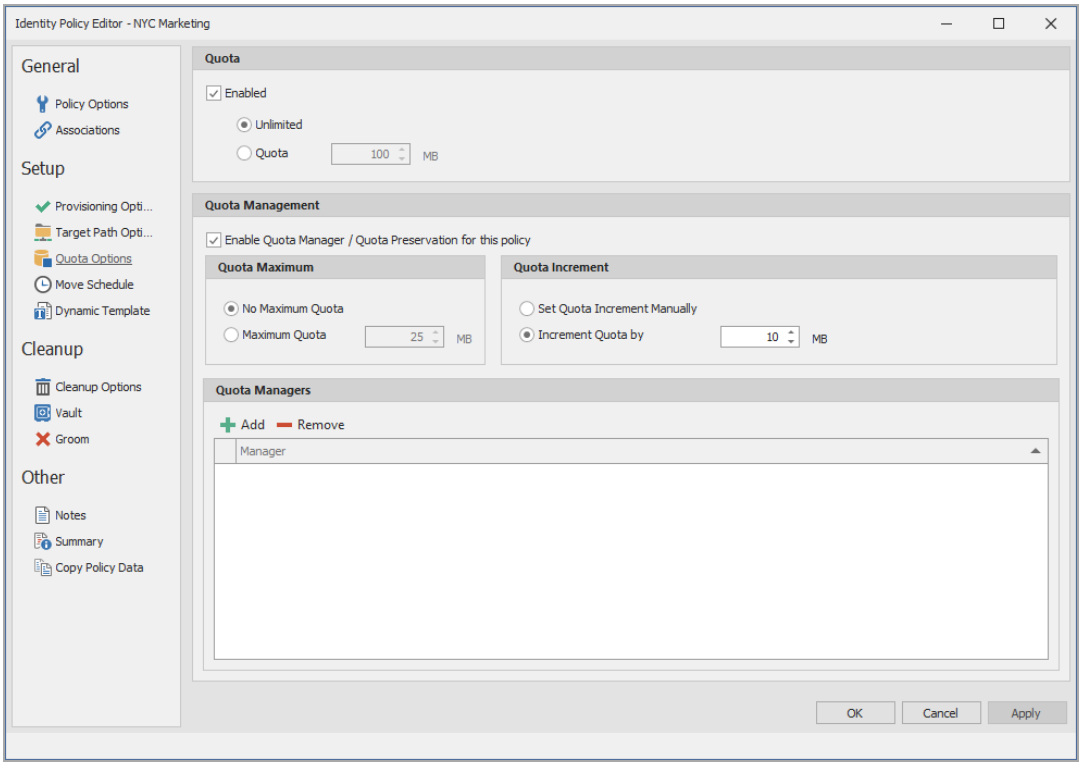
- The quota for the entire storage folder
- Quotas for personal folders in the collaborative storage folder

In order for the quota to be managed on a personal folder, you must also manage the quota on the –MANAGER– or –MEMBER– folder. You can set this in the template through the Windows Server Manager in the same way you set the folder options.

Quota management on NAS devices needs to be managed by the NAS vendor software.

This page is also where you establish quota management settings for quota managers. A quota manager is a specified user or group 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 *Using Quota Manager (page 105)*.

1. In the left pane, click *Quota Options*.
   The following page appears:



2. Select the *Enabled* check box to enable an initial storage quota for collaborative storage paths managed by this policy.
3. In the *MB* field, specify the initial storage quota for the collaborative storage folders.
4. Set up quota managers 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 collaborative storage folders associated with 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 Directory Services Browser to browse to and select a user or group you want to be a quota manager, then drag the User or Group object to the right pane. Repeat this for each user or group you want to be a quota manager.

If you do not specify a user or group as a quota manager, only members of the File Dynamics Admins group will be able to use the Quota Manager web insterface.

5. Click *Apply* to save your settings.
6. Proceed with *Setting the Group Collaborative Storage Policy Move Schedule (page 85)*.

7.7.6 - Setting the Group Collaborative Storage Policy Move Schedule

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

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.

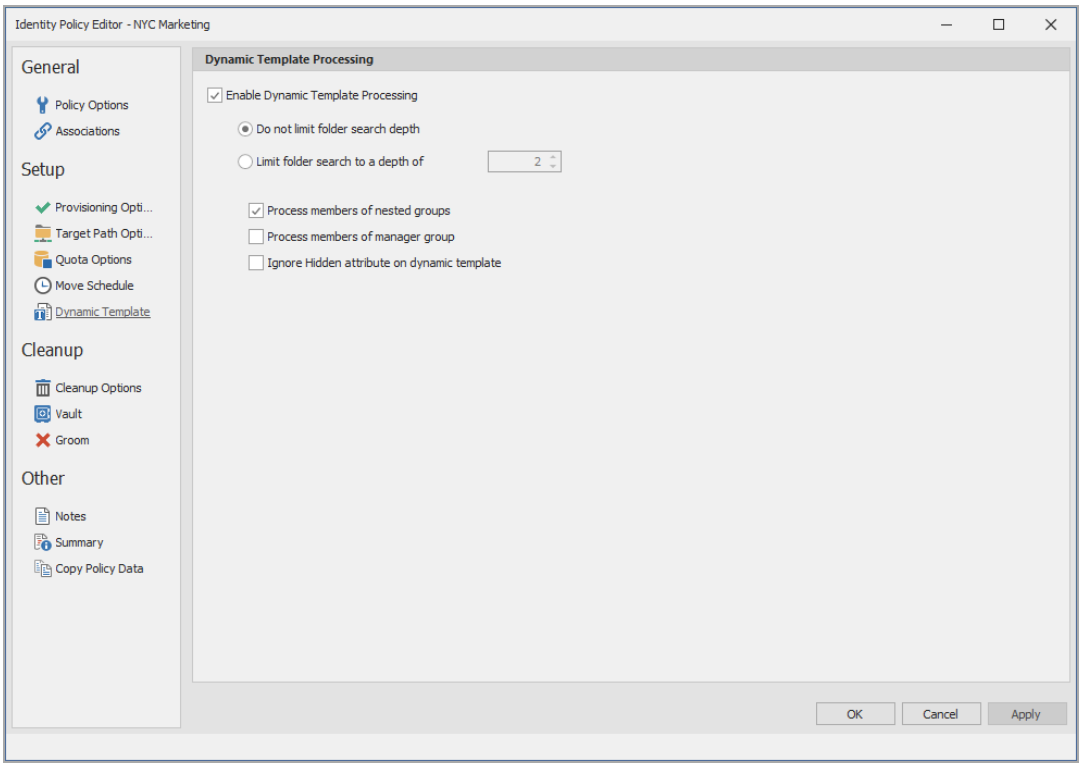
The collaborative storage folder will not move if there are any open files. Until the folder can be moved, the Move event will be listed as a pending event.

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 *Setting Group Collaborative Storage Policy Dynamic Template Processing (page 85)*.

7.7.7 - Setting Group Collaborative Storage Policy Dynamic Template Processing

Dynamic Template Processing is the term used in File Dynamics for creating personal folders in a collaborative storage folder. If Dynamic Template Processing is enabled, creating a `-MEMBER-` or `-MANAGER-` folder in the collaborative storage file structure automates the management of personal storage within the collaborative storage when a user is added, deleted, or renamed in Active Directory.

1. In the left pane, click *Dynamic Template*.
   The following page appears:



2. Do one of the following:
    - If the folder structure in your collaborative storage template includes a –MEMBER– folder, File Dynamics 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, File Dynamics will not create personal folders within the collaborative storage folder. Deselect the *Enable Dynamic Template Processing* check box and proceed with *Setting Group Collaborative Storage Policy Cleanup Options (page 87)*.
3. Choose one of the following options:
    - **Do not limit folder search depth:** The Engine searches through the collaborative storage folder looking for –GROUP–, –MANAGER–, 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 –GROUP–, –MEMBER–, and –MANAGER– folders are located in your collaborative storage template, you can select this option and indicate the level. For example, in the Sample Classroom Collaborative Storage Template under *Setting Up Security for a Collaborative Storage Template (page 72)*, the –MEMBER– folder is located four levels down.
4. Select the applicable check boxes:

Process members of nested groups: If you have nested groups in your Active Directory deployment, selecting this check box creates personal storage for group members that are part of a group via group nesting.

Ignore hidden attribute on dynamic template: Selecting this check box ignores the Hidden DOS attribute on the `-MEMBER-`, `-MANAGER-`, and `-GROUP-` folders in the collaborative managed path when provisioning the corresponding folder for the user or group. Thus, the D`ynamic Template Processing` folder will not have the Hidden DOS attribute set when it is created.

5. Click *Apply* to save your settings.
6. Proceed with *Setting Group Collaborative Storage Policy Cleanup Options (page 87)*

7.7.8 - Setting Group Collaborative Storage Policy Cleanup Options

This page lets you enable and specify cleanup rules for the Group Collaborative Storage 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 Active Directory, 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, weeks, or years a collaborative storage folder remains after the associated Group object is removed from Active Directory.

3. Enable Vault on Delete by filling in the following fields:

   Enable: Select this check box to enable Vault on Delete.

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

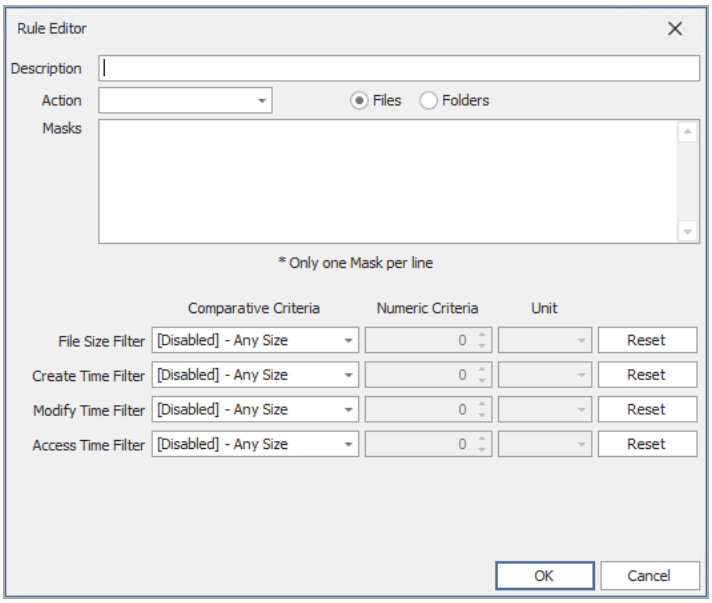
   When you indicate this path, it also appears in the *Vault Path* field of the Groom page, because groom rules and vault rules share the same vault path.

4. Click *Apply* to save the settings.
5. Proceed with *Setting Group Collaborative Storage Policy Vault Rules (page 87)*.

7.7.9 - Setting Group Collaborative Storage Policy Vault Rules

When a Group object is removed from Active Directory, you can have File Dynamics vault the contents of the associated collaborative storage folder from primary storage to less expensive secondary storage. File Dynamics 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 Rule Editor.

1. In the left pane, click *Vault*.
   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 Rule 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. From the *Action* menu, select an action.

   Select whether the rule will vault files or folders, delete files or folders, or ignore a vault rule.

   There is only one action for each vault rule. For example, if you wanted to delete some files and vault others, you would need to establish two different vault rules.

   Vault: Moves all of the files or folders that meet the criteria specified in the vault rule to a location specified in the policy.

   Delete: Deletes all of the files or folders that meet the criteria specified in the vault rule.

   Ignore: Ignores the conditions that would normally vault or delete a file or folder, based on specifications you provide in the *Mask* field.

   For example, if you wanted to vault all `.MOV` files, with the exception or approved training videos located in a folder named `Training Videos`, you could set an individual rule to vault `.MOV` files, and another rule to ignore vaulting the `Training Videos` folder.

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

   File or folder names can contain an asterisk.

5. Specify whether the rule will apply to files or folders.

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

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

6. Specify the masks for the rule.

   Masks: List the files or folders you want to be vaulted or deleted, according to what is indicated in the *Action* drop-down menu. For example, if you wanted to delete all temporary files, you could list `*.TMP` in the *Masks* field.

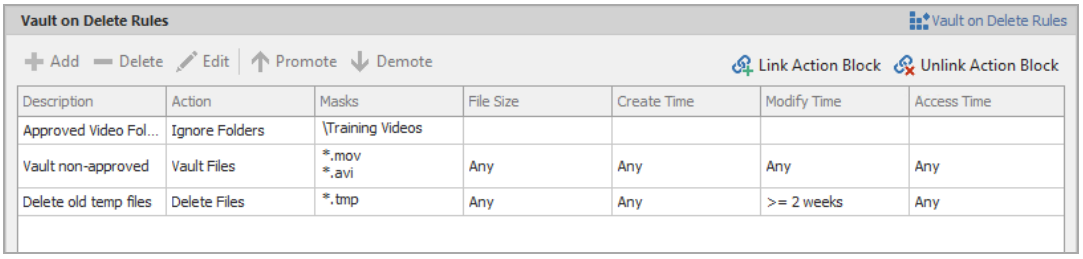
   Be aware that if you select *Vault*, only the files or folders that you list in the *Masks* text box are vaulted and the remainder of the managed path content is deleted. Conversely, if you select *Delete*, only the files or folders that you list in the *Masks* text box are deleted, and everything else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

7. (Conditional) If the 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 *Masks* 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.

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

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

10. (Conditional) If you have set any rules designed to ignore a vault or delete action, in the *Vault on Delete* region of the Vault page, use the *Promote* arrow to move the rule to the top. This protects files or folders specified in the *Masks* field from being vaulted or deleted.|



11. Proceed with *Setting Group Collaborative Storage Policy Groom Rules (page 89)*

7.7.10 - Setting Group Collaborative Storage Policy Groom Rules

Groom rules in File Dynamics specify the file types that you want to be removed from primary managed storage. Examples of these might be `mp3` and `mp4` files, `mov` files, and many

others. You specify in a groom rule whether to delete or vault a file based on the rule's criteria.

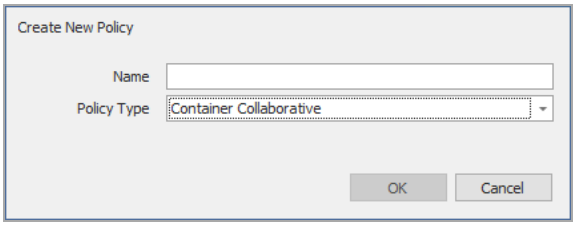
Grooming takes place as a Management Action that is run by the administrator. A Management Action is a manual action that is enacted through the Admin Client. For more information, see *Management Actions (page 189)*.

You might notice the nearly identical look of the Vault and Groom pages, including the Rule Editors. You might naturally wonder what the differences are between a Vault rule and Groom rule. A Vault rule is enacted automatically when a User or Group object with managed storage is deleted from Active Directory. A Groom rule is enacted by a Management Action performed by the administrator.

For an explanation of the fields and procedures for setting up a Groom rule, refer to *Setting Group Collaborative Storage Policy Vault Rules (page 87)*.

7.8 - Creating a Container Collaborative Storage Policy

1. In the Admin Client, click the *Identity Driven* tab.
2. Click *Policies*.
3. In the *Manage* menu, select *New > Container Collaborative*.
   The following dialog box appears:



4. Specify a name in the *Name* field.
   The Policy Options page appears.
5. Continue with *Setting Container Collaborative Storage Policy Options.*

7.8.1 - Setting Container Collaborative Storage 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 *Creating a Blocking Policy (page 18)*.

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:

   Associations: The Associations page is identical to the Associations page presented when you create a Group Collaborative Storage policy. For an explanation of the page, along with procedures for setting associations, see *Setting Group Collaborative Storage Policy Associations (page 79)*.

   Provisioning Options: The fields presented on the Provisioning Options page are identical to those presented when you create a Group Collaborative Storage policy. For an explanation of the page, along with procedures for setting provisioning options, see *Setting Group Collaborative Storage Policy Provisioning Options (page 80)*.

   Target Path Options: The fields presented on the Target Path Options page are identical to those presented when you create a Group Collaborative Storage policy. For an explanation of the page, along with procedures for setting target paths, see *Setting Group Collaborative Storage Policy Target Paths (page 81)*.

   Quota Options: The fields presented on the Quota Options page are identical to those presented when you create a Group Collaborative Storage policy. For an explanation of the page, along with procedures for setting quota options, see *Setting Group Collaborative Storage Policy Quota Options (page 83)*.

   Move Schedule: The fields presented in the Move Schedule page are identical to those presented when you create a Group Collaborative Storage policy. For an explanation of the page, along with procedures for setting the move schedule, see *Setting the Group Collaborative Storage Policy Move Schedule (page 85)*.

   Dynamic Template: The fields presented on the Dynamic Template page are identical to those presented when you create a Group Collaborative Storage policy. For an explanation of the page, along with procedures for setting the move schedule, see *Setting Group Collaborative Storage Policy Dynamic Template Processing (page 85)*.

   Cleanup Options: The fields presented on the Cleanup Options page are identical to those presented when you create a Group Collaborative Storage policy. For an explanation of the page, along with procedures for setting cleanup options, see *Setting Group Collaborative Storage Policy Cleanup Options (page 87)*.

   Vault: The fields presented on the Vault page are identical to those presented when you create a Group Collaborative Storage policy. For an explanation of the page, along with procedures for setting vault rules, see *Setting Group Collaborative Storage Policy Vault Rules (page 87)*.

   Groom: The fields presented on the Groom page are identical to those presented when you create a Group Collaborative Storage policy. For an explanation of the page, along with procedures for setting grooming rules, see *Setting Group Collaborative Storage Policy Groom Rules (page 89)*.

5. Click *Apply* to save your settings.

7.9 - Creating a Multi-Principal Collaborative Storage Policy

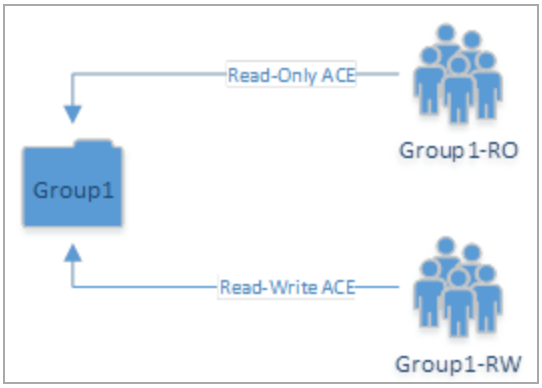
This section provides details for understanding and creating Multi-Principal Collaborative storage policies.

7.9.1 - Multi-Principal Collaborative Storage Policy Overview

File Dynamics provides the ability to provision and manage folders that can be owned by multiple Active Directory security groups. Each group's access to these folders is dependent on the security group object's security principal. For example, one group's access could be Read-Only, another's could Read/Write, and another's could be Full Control. Based on their support for multiple security principals, these folders are known as "Multi-Principal Managed Paths," and they are issued through "Multi-Principal Collaborative Storage" policies.

Multi-Principal Managed Paths are owned and accessed by security groups with the same group prefix name separated by a suffix separator, and then distinguished by a unique security separator. In the figure below for example, the managed path Group1 is owned by both Group1-RO and Group1-RW, with the members of each group having Read Only and Read Write permissions respectively.

Example of a Multi-Principal Managed Path



7.9.2 - Group Naming Parameters

Security groups that own and access a Multi-Principal Path must be in the `Group_Prefix_Name-Security_Suffix format`. In the table below, the naming components of the security group names in the figure under *Multi-Principal Collaborative Storage Policy Overview (page 92)* are identified.

Group Prefix Name	Suffix Separator	Security Suffix
Group1	-	RO
Group1	-	RW

The group prefix names cannot be different. For example, you cannot have Accounting-RW and Sales-RO groups managed by a Multi-Principal Collaborative policy against the same managed path. Multiple groups are considered to be participating in the security of the managed path if they have the same group prefix name up to the well-defined suffix separator string. The suffix separator can be a character or a string of characters and is configured in a Multi-Principal Suffix Mapping Action Block.

7.9.3 - Multi-Principal Collaborative Policies

The change in paradigm to support Multi-Principal Managed Paths requires the introduction of a new Multi-Principal Collaborative policy type. The policy follows the standard association rules to support effective policy calculation. This means that the policy can be associated to a container or directly to security groups.

The new policy type provides the ability to link to a Multi-Principal Suffix Mapping Action Block where the separator character or string sequence that differentiates the group's name from its security suffix.

7.9.4 - Multi-Principal Collaborative Events

To handle the constraints on the managed path imposed from multiple security principals managing a folder, new provisioning and de-provisioning events have been introduced. The primary reason for this is that provisioned managed paths for the Multi-Principal Collaborative policy can be thought of as referenced-counted based on the number of participating security groups. For instance, if Group1-RW, Group1-RO, and Group1-A all have active ACEs on the managed path, then the reference-count for the managed path is 3 and deletion of only one of these groups does not imply deletion of the folder as a whole. Rather, when any given security principal is deleted or moved out of policy scope, the corresponding event needs to scan the corresponding Active Directory container to look for the presence of any other groups by the group name prefix. If none exist, then the folder can potentially be scheduled for cleanup, otherwise no action is taken, except for when the ACE is removed.

Similarly, for provisioning, the first group for which an event is received would be responsible for creating the folder based on the group name prefix and assigning its respective rights. Any other events for complimentary groups must perform the equivalent of an apply permissions (ACE) in order to populate their respective transform entries. This allows for a flexible implementation that does not require a base security principal to be created first.

7.9.5 - Create a Multi-Principal Collaborative Storage Policy

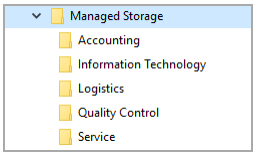
Follow the prerequisites and procedures in the following sections to create a Multi-Principal Collaborative Storage policy.

Prerequisites for a Multi-Principal Collaborative Storage Policy

- Structure Active Directory in a logical manner for the new groups that you will be creating.

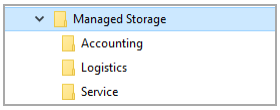
  For example, a division of a company has many departments with complex permissions. For instance, the Accounting Department might have a group of

individuals that need Read/Write permissions, while another group needs Read Only.



- Structure your network file system so that there is a storage area that will host the collaborative storage for the new groups.

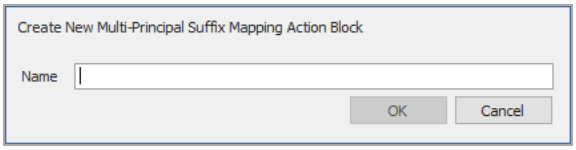
  As an example, the file system might look like this:



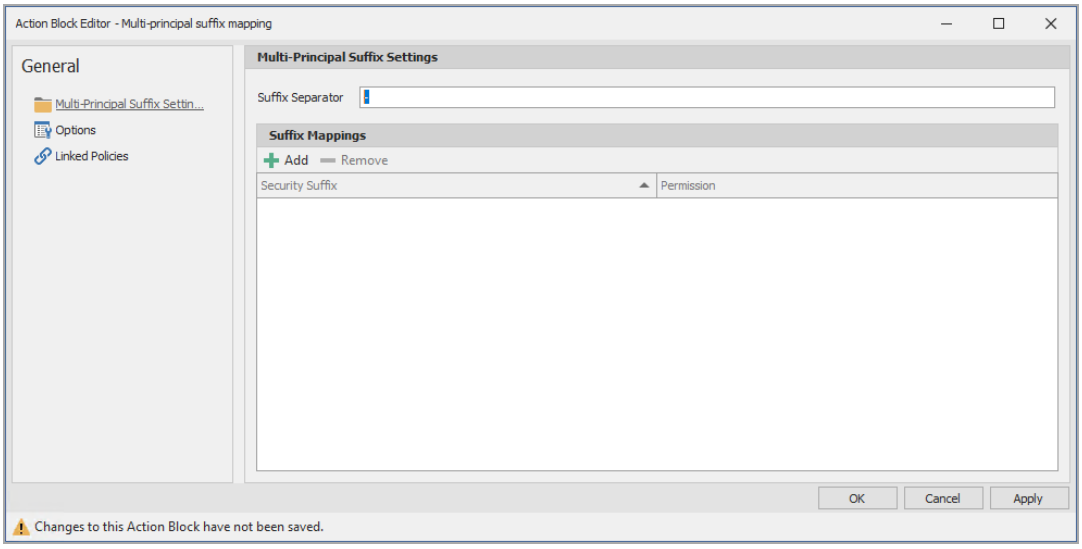
Create a Multi-Principal Suffix Mapping Action Block

This procedure lets you standardize the groups and their associated permissions for the collaborative storage folders that will be provisioned by File Dynamics.

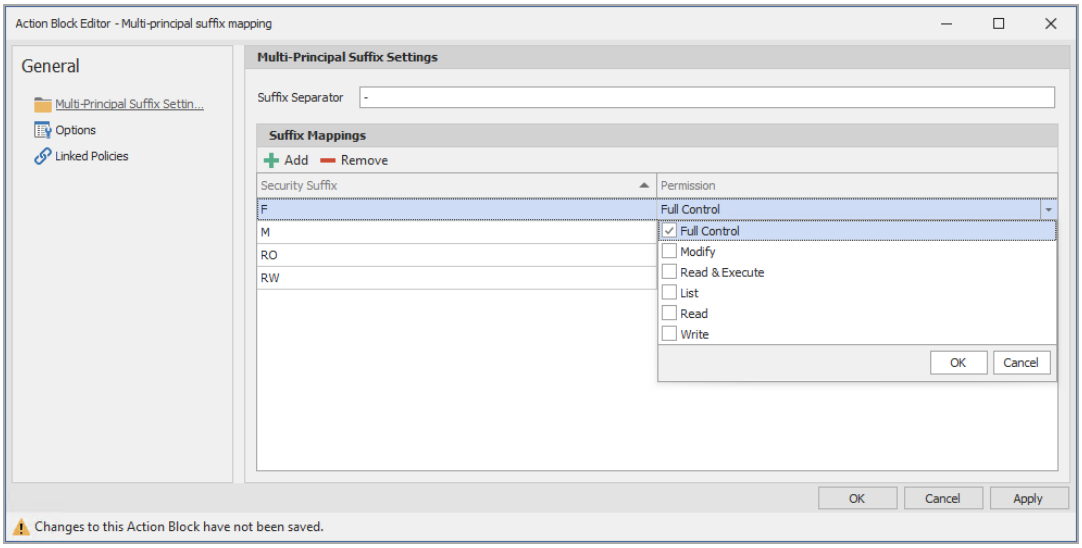
1. In the Admin Client, click the *Identity Driven* tab.
2. Click *Action Blocks*.
3. From the *Manage* menu, select *New* > *Multi-Principal Suffix Mapping*.



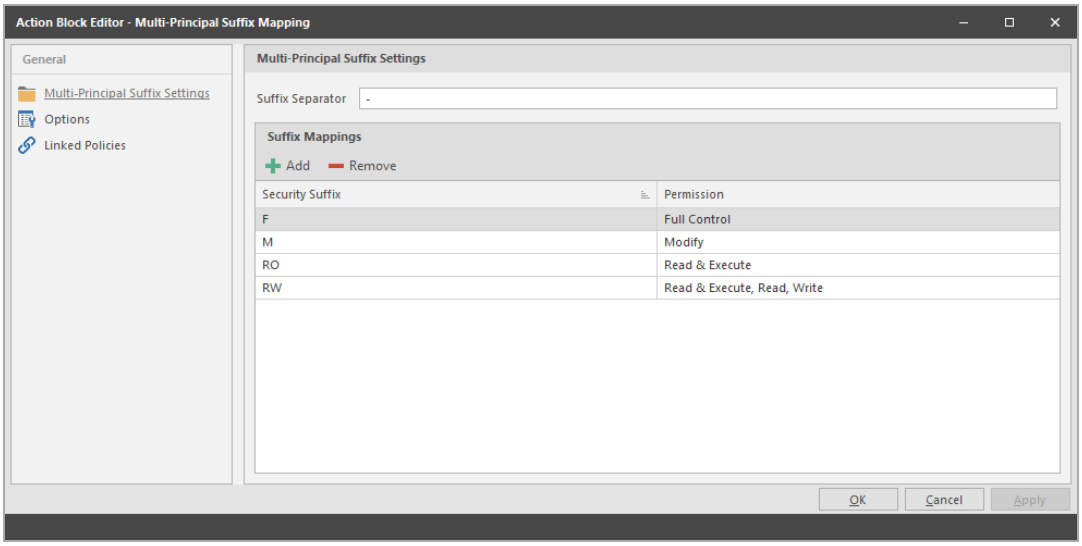
4. Enter a descriptive name for the new Action Block and click *OK*.
   The following page appears:



5. Click *Add*.
6. In the *Security Suffix* column, highlight *SampleSecuritySuffix* and edit it to a more descriptive name of a group that will access the collaborative storage folder. For example: Shipping.
7. Click the *Full Control* setting to access a drop-down menu of access permissions.
8. Specify the permissions for the particular group and click *OK*.



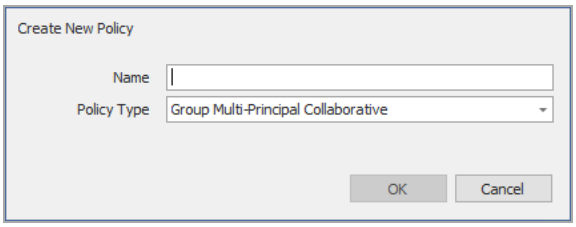
9. Repeat Step 5 through Step 8 to create all groups and permissions to the collaborative storage folder.



10. Click *Apply*.
11. Click *OK*.

Create a New Multi-Principal Collaborative Storage Policy

1. In the Admin Client, click the *Identity Driven* tab.
2. Click *Policies*.
3. In the *Manage* menu, select *New > Group Multi-Principal Collaborative*.
   The following dialog box appears:



4. Specify a descriptive name in the *Name* field and click *OK*.
5. Proceed with *Setting Policy Options (page 96)*.

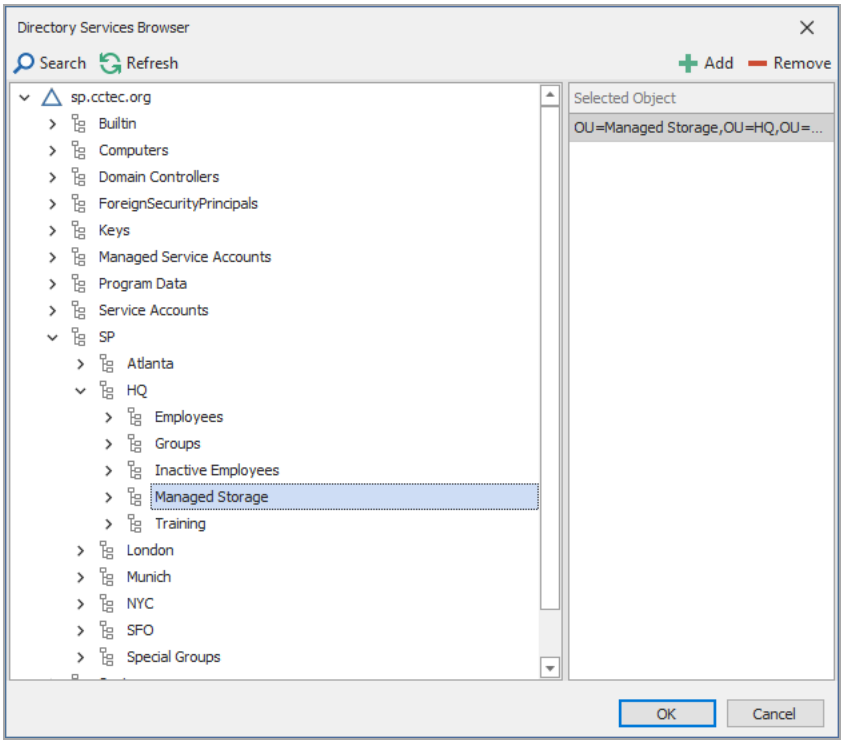
Setting Policy Options

1. Verify that the *Process Events for Associated Managed Storage* check box is selected.
2. Verify that the *Policy applies to subcontainers* check box is selected.
3. (Optional) Enter an expanded description of the policy in the *Description* field.
4. Proceed with *Setting Associations (page 96)*

Setting Associations

1. Click *Associations*.
2. Click *Add*.

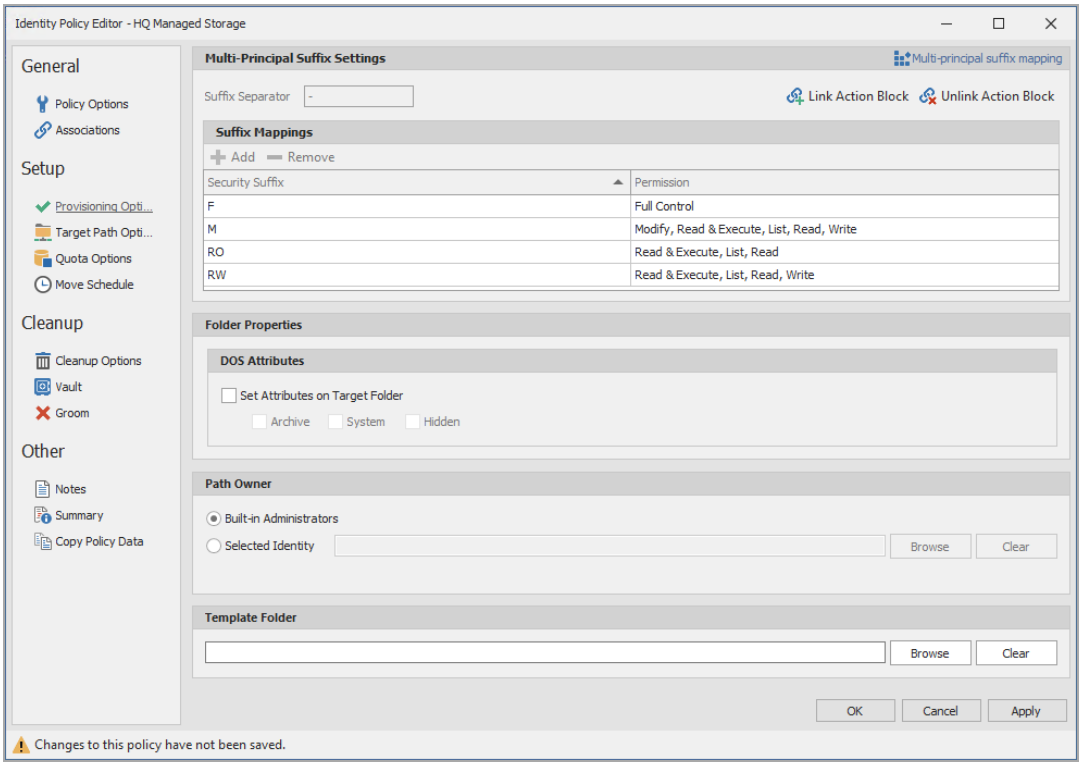
3. In the browser, locate the organizational unit where the group objects will reside and drag it to the right pane.



4. Click *OK* to close the browser.
5. Proceed with *Setting Provisioning Options (page 98)*.

Setting Provisioning Options

1. Click *Provisioning Options*.
2. Click *Link Action Block*, select the Action Block you created earlier, and click *OK*.

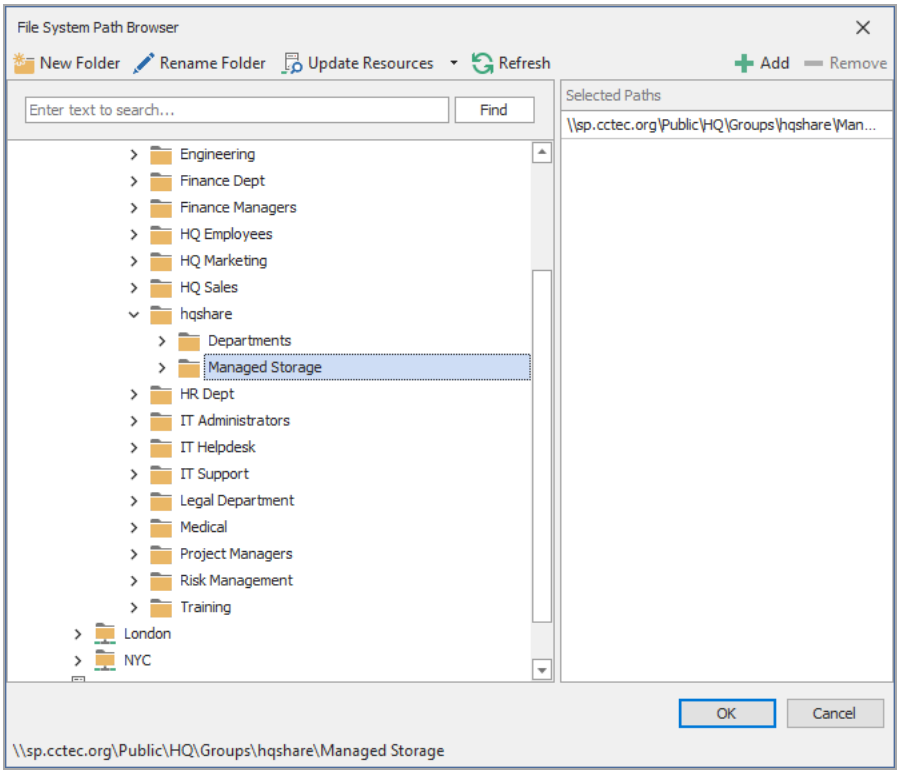


3. In the *Path Owner* region of the page, click *Browse* and browse to specify an owner of all of the collaborative storage folders that will be created with this policy.
4. (Optional) In the *Template Folder* region, click *Browse* to specify a template for the collaborative storage folders that will be created by this policy.
5. Proceed with *Setting the Target Path (page 98)*.

Setting the Target Path

1. Click *Target Path Options*.
2. In the *Target Paths* region of the page, click *Add*.

3. In the browser, locate the share or folder where the collaborative storage folders will reside and drag it to the right pane.



4. Click *OK* to close the browser.
5. Click *Apply*.
6. Proceed with *Setting Cleanup Options (page 99)*

Setting Cleanup Options

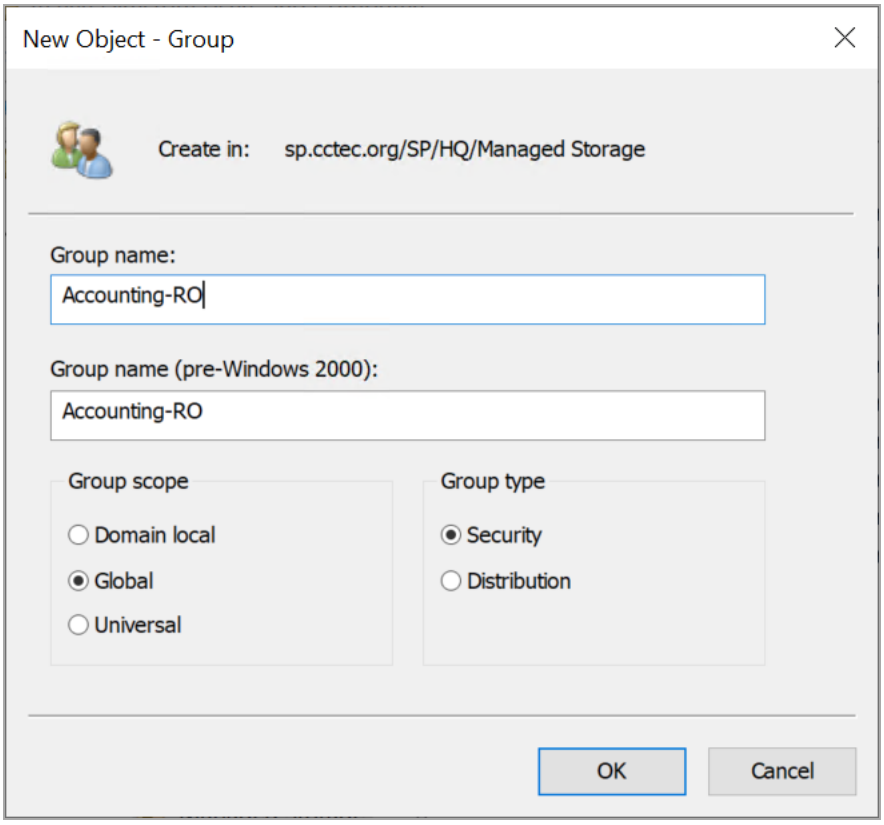
1. In the *Vault on Delete* region, select the *Enable* check box.
2. Click *Browse*.
3. In the browser, locate the share or folder where deleted folders will be archived once all of the groups that own a collaborative storage folder have been deleted and click OK.
4. Click *Apply*.
5. Click *OK* to close the Policy Editor.
6. Proceed with *Testing the Policy (page 99)*.

Testing the Policy

These procedures let you verify that the policy is functioning as you designed it.

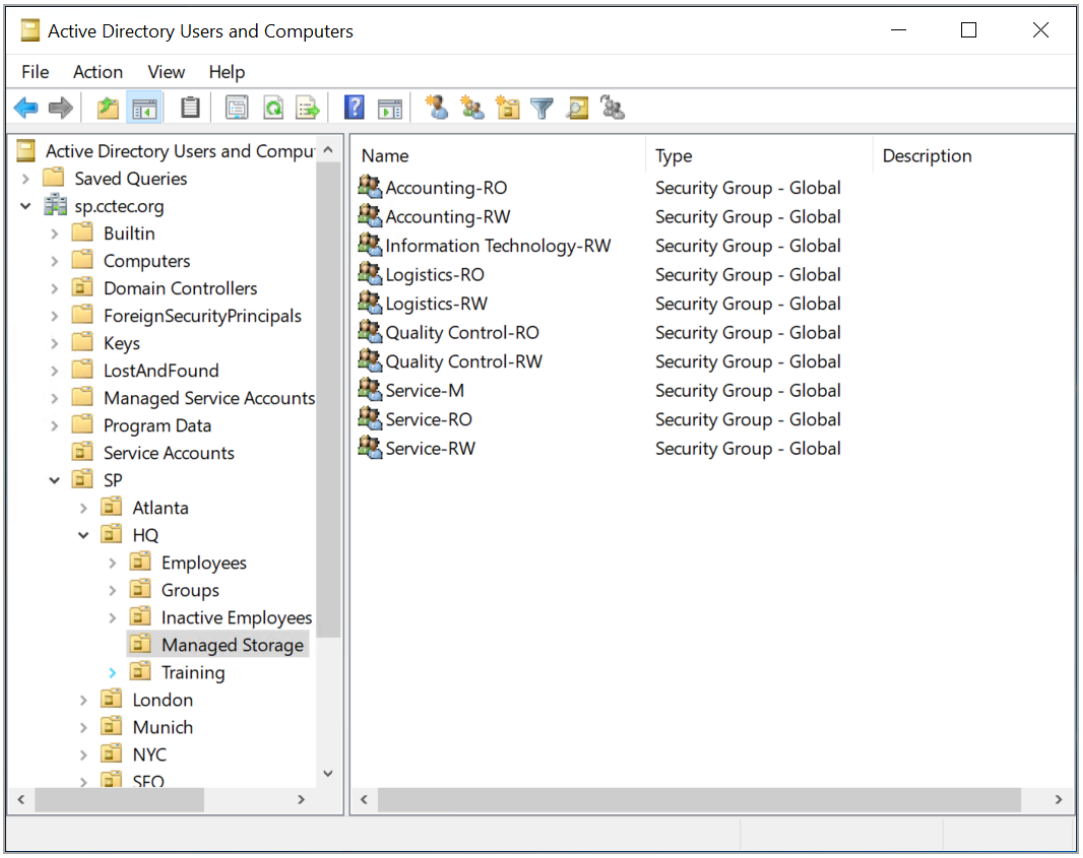
1. In one of the organizational units associated with the new Multi-Principal Collaborative Storage policy, create a new group that includes a - and one of the security suffixes

you established earlier.

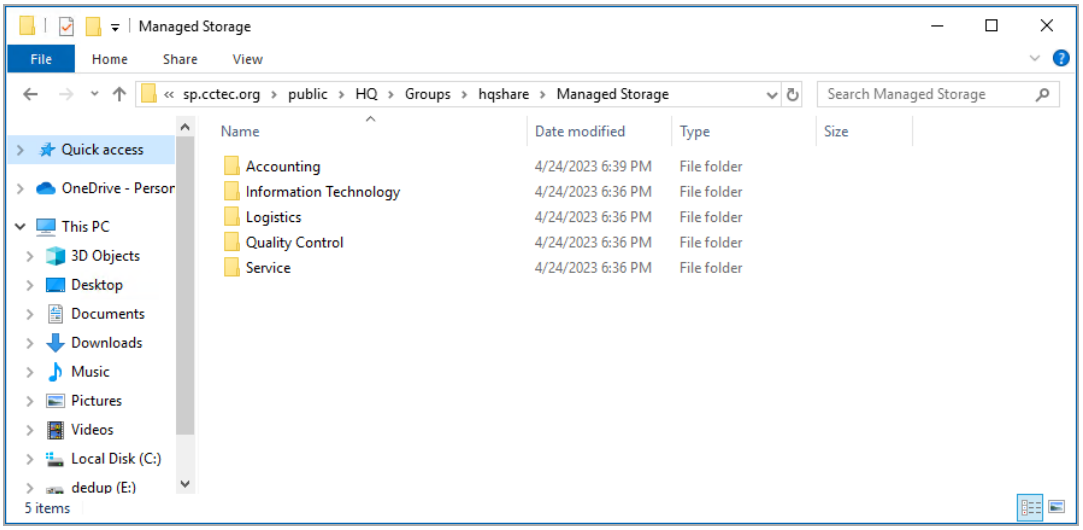


2. In the same organizational unit, and using the same group prefix name and suffix separator, create additional groups for each of the security suffixes you created

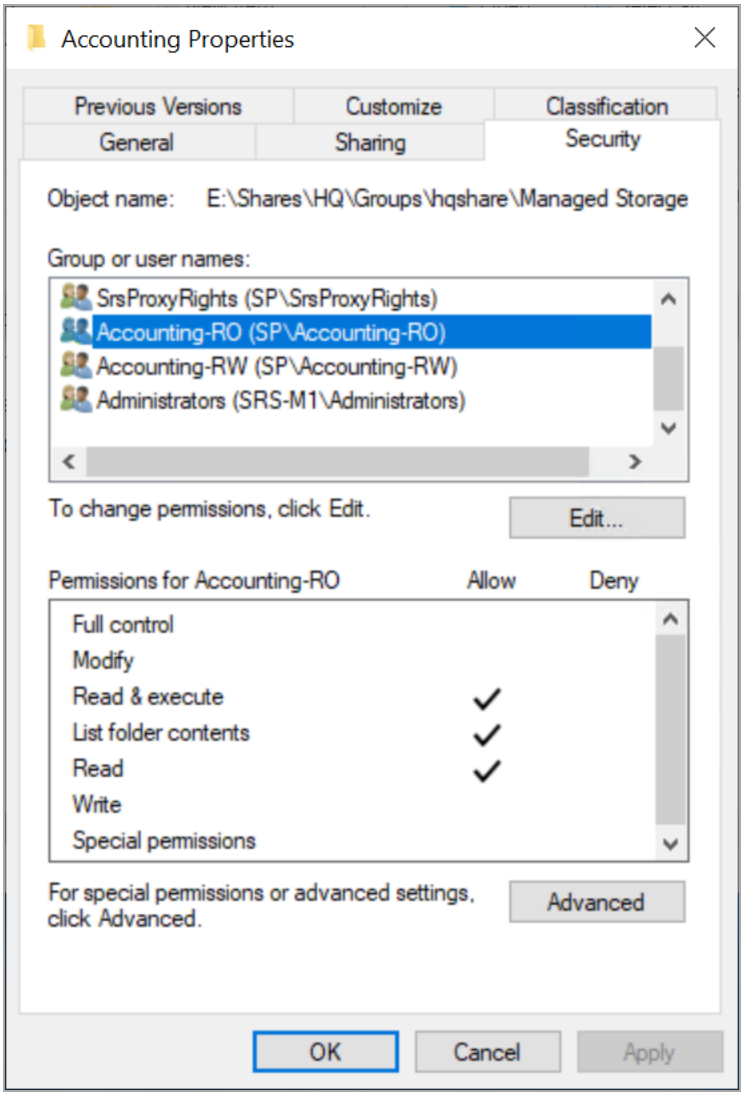
earlier.

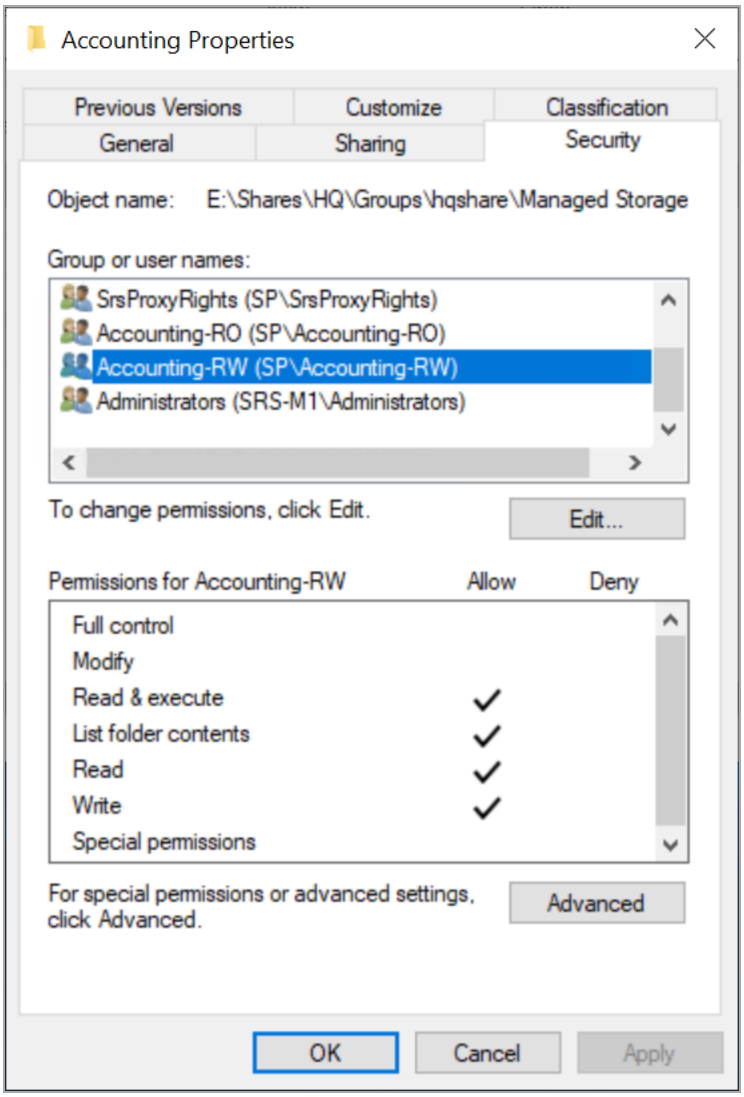


3. Using File Explorer, verify that each of the collaborative storage folders were created.



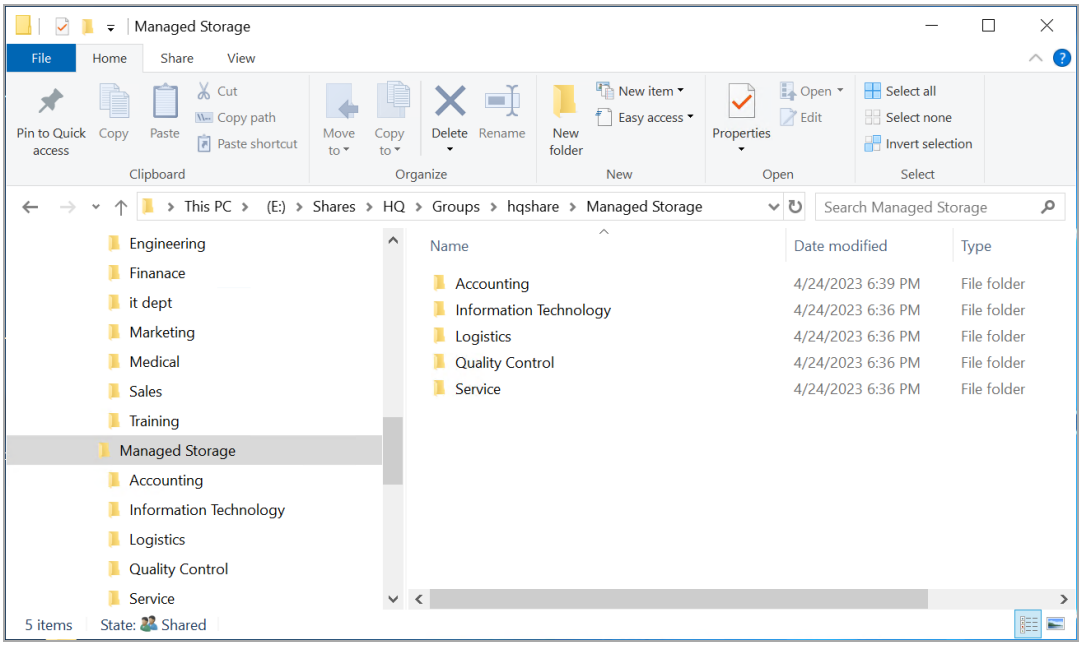
4. While still in File Explorer, verify that the permissions for each of the groups are correct.





5. Once you have verified that the Multi-Principal Collaborative Storage policy is creating collaborative storage with the correct access permissions for the various groups, create the remaining groups in all of the organizational units associated with the new

Multi-Principal Collaborative Storage policy.



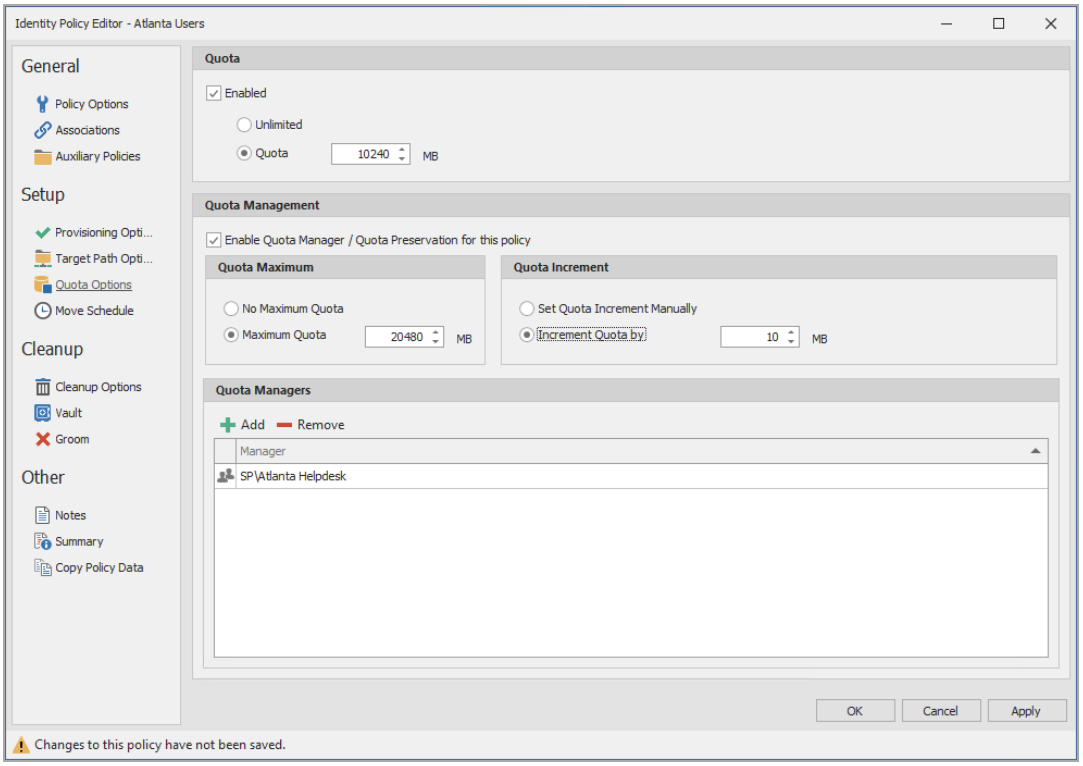
8 - Using Quota Manager

Quota Manager is a separate management interface for designated users, such as help desk or support personnel, to adjust user home folder or collaborative storage quota without needing permissions 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 representative can make suggestions for freeing up space in the managed path rather than simply granting additional storage quota.

8.1 - Quota Management Prerequisites

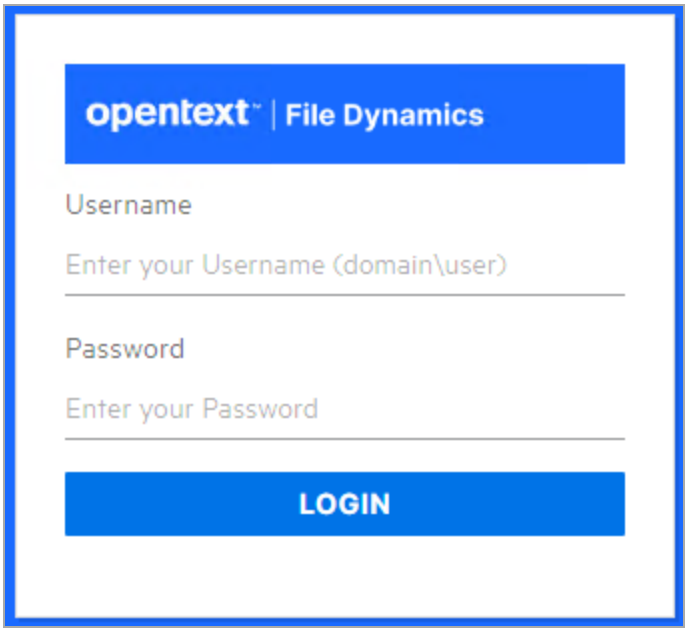
1. Using the Admin Client, verify that all of the policies managing the users for whom you want to manage quotas through Quota Manager have the *Enable Quota Manager* check box selected, with a *Quota Maximum* and/or *Quota Increment* setting.



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

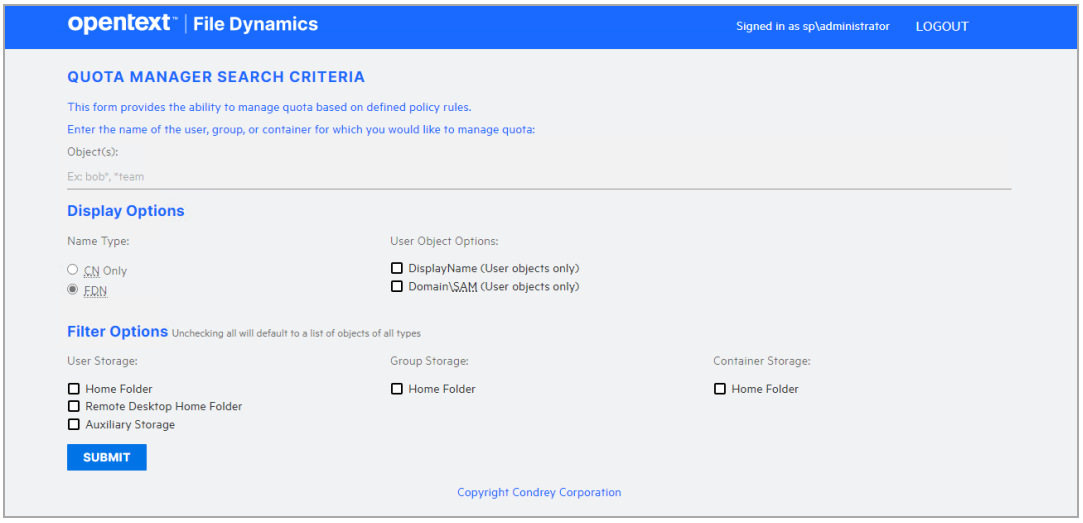
1. Launch a web browser.
2. Enter the following address: `https://ip-address-or-dns-name-of-engine-server:3009/qm`
3. (Conditional) If a message appears informing you that the connection is not trusted, proceed by adding the security exception and downloading the certificate.
   The following screen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



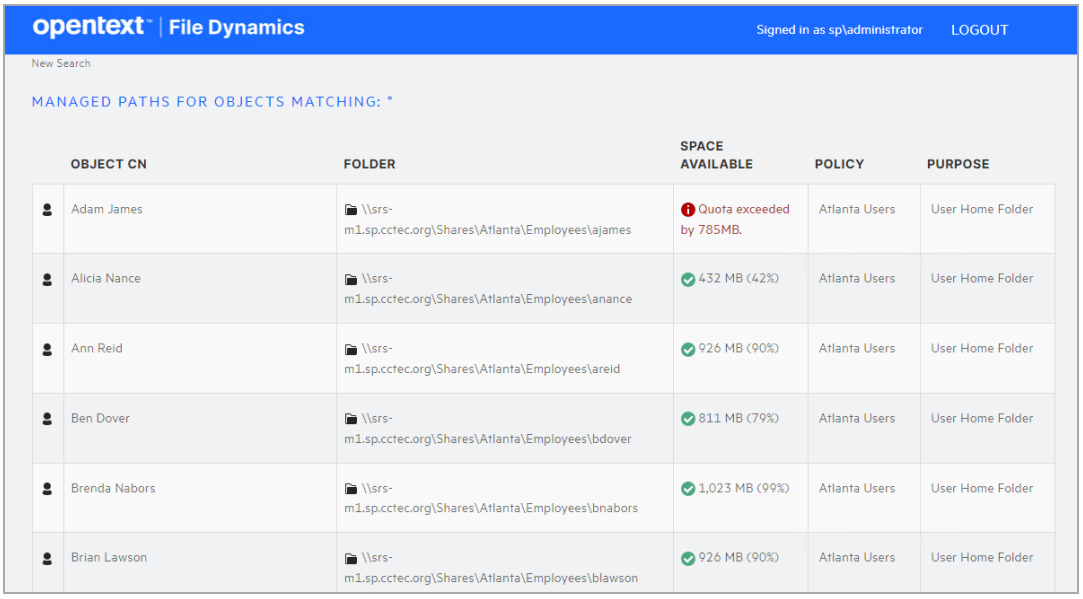
4. Enter a username and password and click *Login*.

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

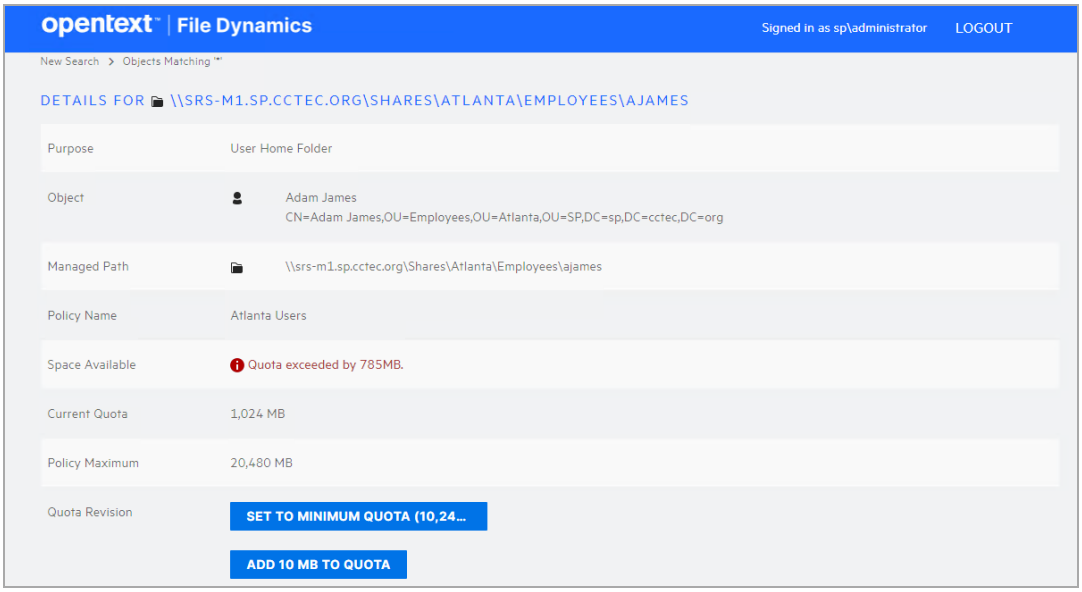
The username must be in Domain\Account or User Principal Name format such as *domain\user* or *user@full.domain.com*.



5. In the *Object(s)* field, specify a user, group, or container 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. Select the user, group, or container you want to manage and click the *Manage Object* button.



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 folder or collaborative storage folder.

Red: Denotes one of the following conditions:

- Quota usage has exceeded 90 percent.
- The Engine is unable to contact the server containing the share.
- The share does not support quota management.
- The home folder does not exist.
- The server containing the share gave an Access Denied error, indicating that either remote storage management is not configured or enabled for the 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 - Creating Target-Driven Policies

In previous chapters, you worked with Identity-Driven policies that manage data associated with users and groups. File Dynamics also lets you manage data through Target-Driven policies that are associated directly with a network folder or share. Target-Driven polices provide unique management capabilities that are detailed in this chapter.

9.1 - Target-Driven Policy Types

There are presently seven types of Target-Driven policies in File Dynamics:

- Content Control policies
- Data Location policies
- Workload policies
- Target-Driven Security policies
    - Security Notification policies
    - Security Lockdown policies
    - Security Fencing policies

9.1.1 - Content Control Policies

File Dynamics provides a Groom policy option for its Content Control policies. Groom policies remove files according to file type, age, size, last accessed date, and more. From any file path, you can either vault files to a new location or delete the files altogether. For example, you could use this feature to easily delete temporary files and, in the process, make much more disk space available on your storage devices.

9.1.2 - Data Location Policies

These policies are the means of copying or moving folders and their contents to another location on the network. Copy policies duplicate a folder's contents and file structure to a location of your choosing. Move policies move the folder's contents and file structure to a target parent folder.

9.1.3 - Workload Policies

Workload policies in File Dynamics provide the ability to handle work processes initiated from other applications. For example, reports generated in OpenText File Reporter that specify the location of sensitive files can be imported into the Data Owner Client where a designated Data Owner can remediate the location of these sensitive files. This approach empowers organizations to provide automated network file system security remediation approved by a gatekeeper familiar with the files.

Workload policies specify source paths, along with the Data Owners who can access these paths.

9.1.4 - Target-Driven Security Policies

With the objective of providing data access governance to high-value target paths located on your enterprise network, File Dynamics provides a variety of Target-Driven Security policies designed to inform you of changes in access permissions, lock down access to an baseline that is strictly enforced, and provide and deny access based on group memberships.

How Target-Driven Security Policies Work

File Dynamics scans the security of the network file system and records the results. The first scan is considered the baseline and is the means of comparing changes produced by each scheduled follow-up Security Scan. The Security Scan records the following:

- Access Control Entries for the file share
- Security Descriptor (including Access Control Entries, Owner, etc.) of the target path and all subordinate folders
- Group memberships (Optional)

How Target-Driven Security Policies Address Changes in Security

Any changes detected result in a security alert to the associated email recipients and notification records written to the database. Each policy type handles these security changes in different ways.

The Notification policy simply records what changed to the database, updates it baseline, and alerts the associated email recipients that there was a change.

The Lockdown policy records what changed along with what action was taken to remediate the changes back to the baseline and then alerts the associated email recipients that changes were made. This baseline scan acts as the baseline, and must be rebuilt when security changes are needed to this associated target path.

The Fencing policy records the security changes identified but applies the rules from the policy to determine if the security changes should be allowed or reverted. If the rules allow for the change, the baseline is update automatically. If the rules do not allow for the change, the change is reverted and a notification record is created. An alert is sent the associated email recipients that a change occurred.

9.1.5 - Target-Driven Security Policy Types

At the present time, File Dynamics includes three Target-Driven Security policy types: Security Notification policies, Security Lockdown policies, and Security Fencing policies.

Security Notification Policies

Security Notification policies enable administrators to be notified of any changes in access permissions to network folders. These changes in permissions include a user being given a new or updated permission to a specific folder, or a user has been granted access permissions to a folder by being added to a group.

Notification emails are sent to the specified recipients. Only the recipients that are also Data Owners can log in to the Data Owner Client to view the changes.

Security Lockdown Policies

Security Lockdown policies let you establish the baseline permissions for a high-value target. When unauthorized access permissions are made, the new permissions are removed and the appropriate permissions are restored.

Updates to security permissions are logged and notifications are sent via email to specified recipients.

Security Fencing Policies

Security Fencing policies set limits on how access permissions may change over time by specifying groups that can be given permissions and others that should never be given access permissions.

Updates to security permissions are logged and notifications are sent via email to specified recipients.

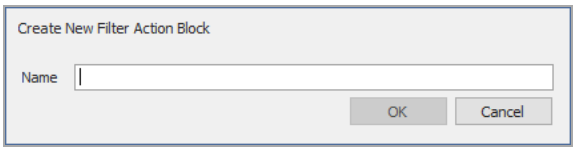
9.2 - Create a Groom Policy

Groom policies remove files from any arbitrary path to a vault location. The files that are removed and the frequency that the removals are performed are in accordance to the specifications that you establish.

9.2.1 - Creating an Action Block for the Groom Policy

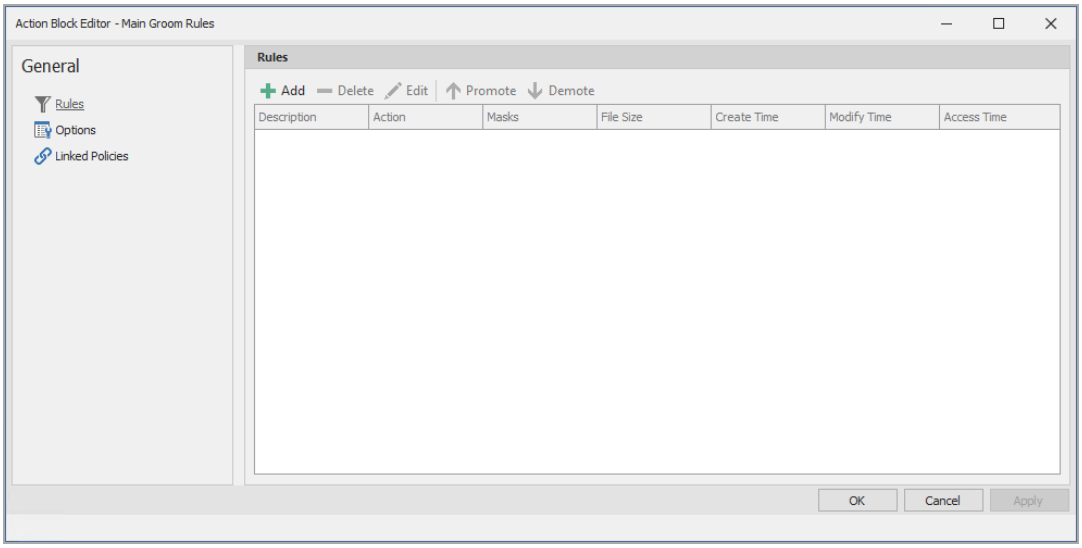
A Groom policy utilizes groom specifications that have been established and saved in an Action Block.

1. In the Admin Client, click the *Target Driven* tab.
2. Click *Action Blocks*.
3. In the Manage menu, select *New* > *Filter*.



4. In the Create New Filter Action Block dialog box, give the new Action block a descriptive name.
   For example, Main Groom Rules.

5. Click *OK*.
   The Rule Editor dialog box appears.



6. Establish your groom rules by specifying in separate rules, the file or folder types to be vaulted or deleted, and under which conditions they are to be ignored.

   For detailed procedures on how to set up groom rules, see *Setting Groom Rules (page 43)*.

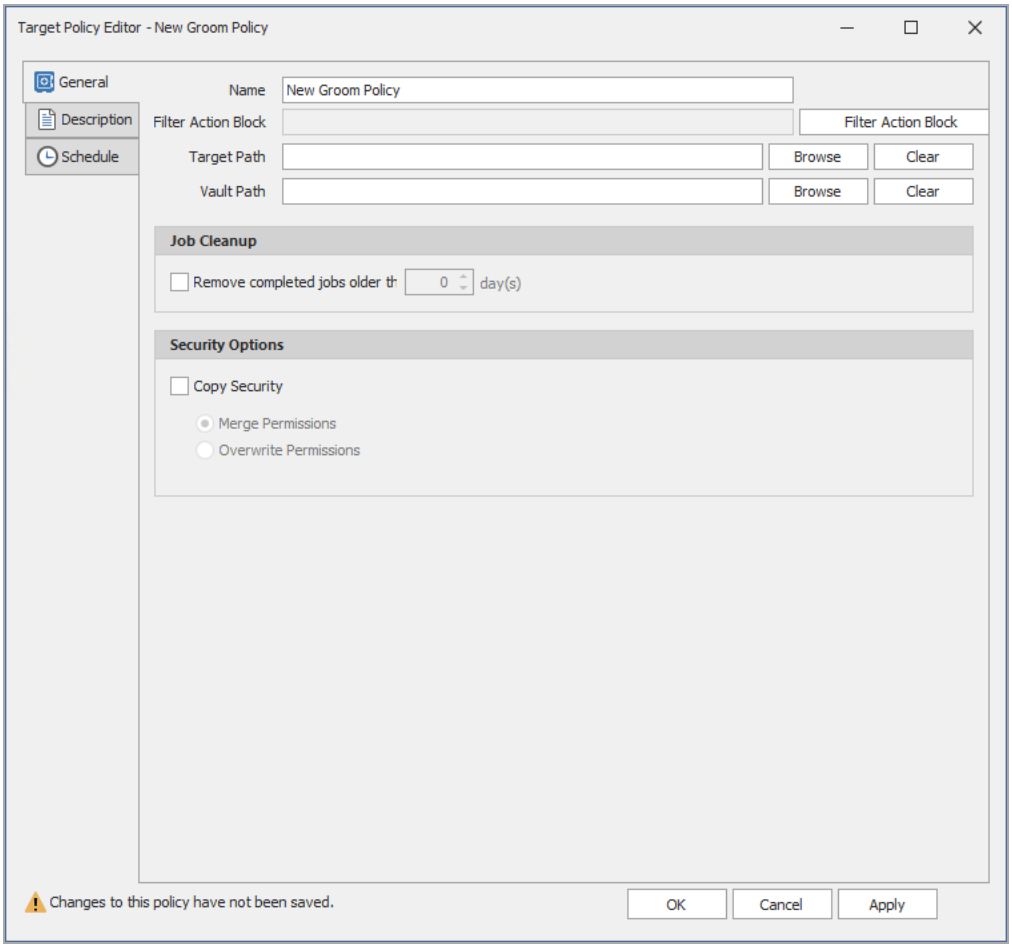
7. When you have finished creating your groom rules, close the Action Block Editor.

9.2.2 - Creating a Groom Policy

With the groom rules now saved to an Action Block, you can now create the Groom policy.

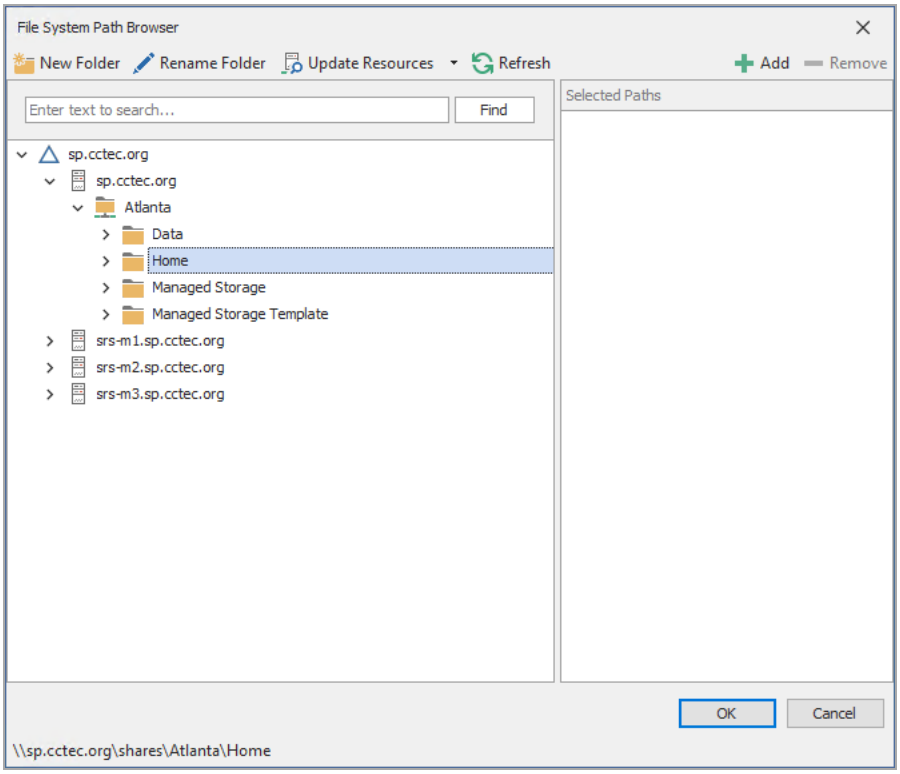
1. In the Admin Client, click the *Target Driven* tab.
2. Click *Policies*.

3. Select *New > Groom Policy*.



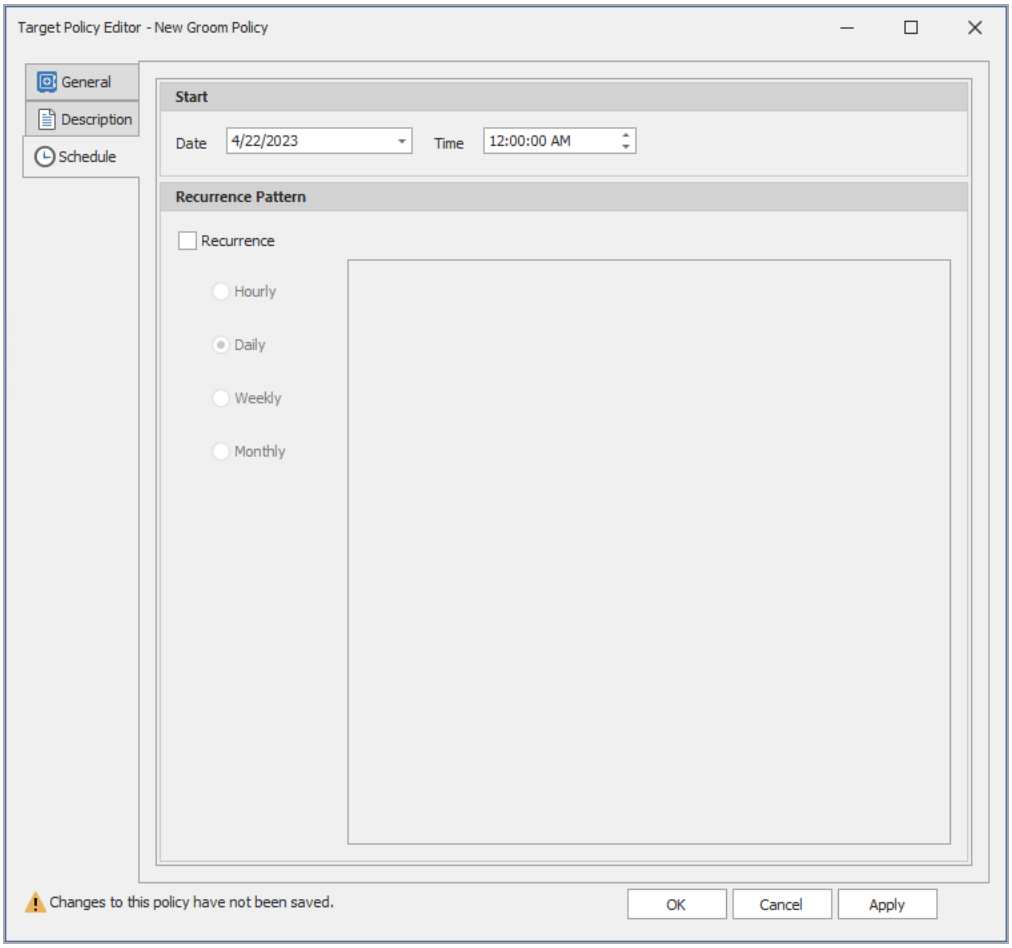
4. In the *Name* field, give the Groom policy a descriptive name.
   For example, Main Groom for General Atlanta Storage.
5. Click *Filter Action Block*.
6. In the Action Block Selector dialog box, locate and select the Action Block you created under *Creating an Action Block for the Groom Policy (page 111)*.
7. Click the *Browse* button that pertains to the *Target* field.

8. In the File System Path Browser, specify the location in the file system from where you will be grooming files for this policy.



9. Click the *Browse* button that pertains to the *Vault Path* field.
   A vault path is not required if the filter block does not contain a vault action. If the filter is later updated to add a vault action, then a vault path is required.
10. In the File System Path Browser, specify the location in the file system where you want groomed files stored for this policy.
11. Select the *Remove completed jobs older than* check box and specify the number of days that a Groom task from this policy is listed on the Jobs list before it is purged.
12. (Conditional) If you want your users to be able to continue to access groomed files from the new vault location, select the Copy Security check box and choose one of the following options:
    - **Merge Permissions:** Merges permissions from the source to the target if the target contains permissions that are not present in the source. This applies to all folders and files in the source folder structure.
    - **Overwrite Permissions:** Overwrites permissions in the target with those found in the source. This applies to all folders and files in the target folder structure.
13. Click *Apply* to save your settings.
14. Click the *Description* tab and enter any information you want about the policy.
15. Click *Apply*.

16. Click the *Schedule* tab.

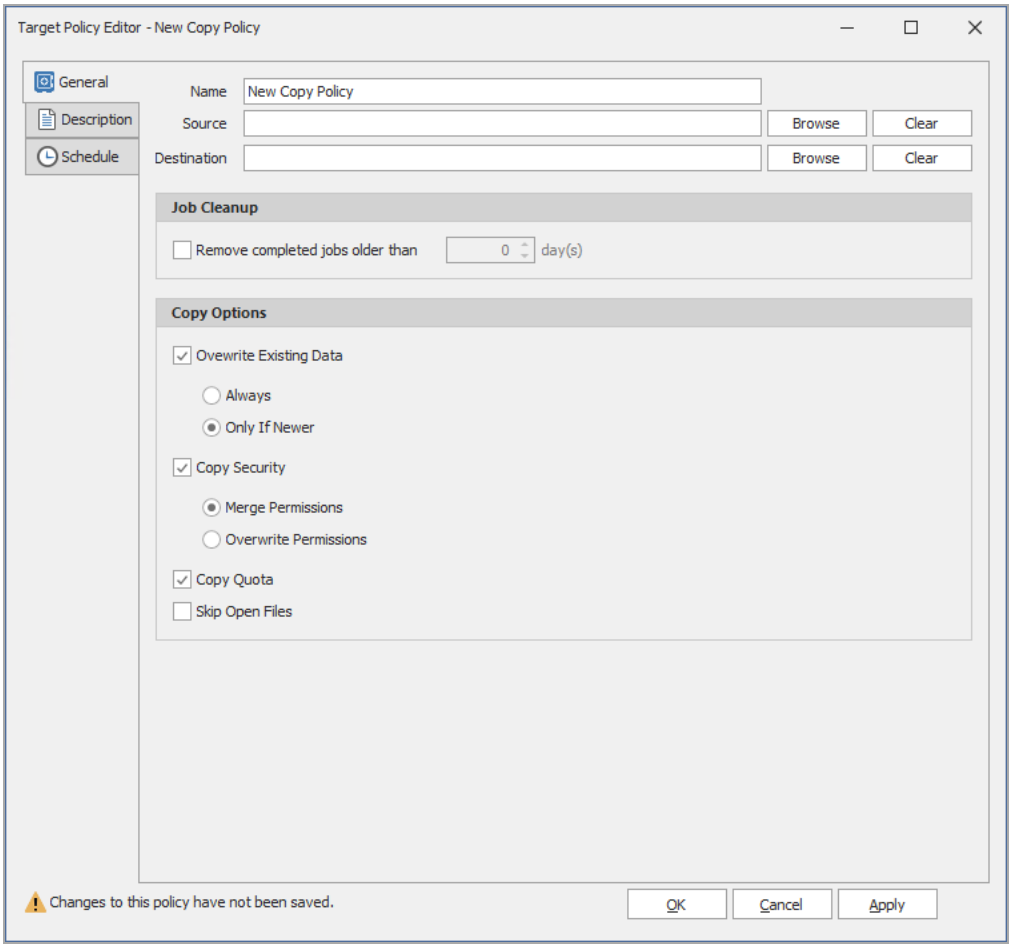


17. In the *Date* field, specify the date you want the policy to be initially invoked.
18. In the *Time* field, specify the time you want the policy to be initially invoked.
19. (Conditional) If you want the Groom policy to run on a recurrent basis, select the *Recurrence* check box and then select one of the options.
20. Click *Apply* to save the schedule.
21. Click *OK*.

9.3 - Create a Copy Policy

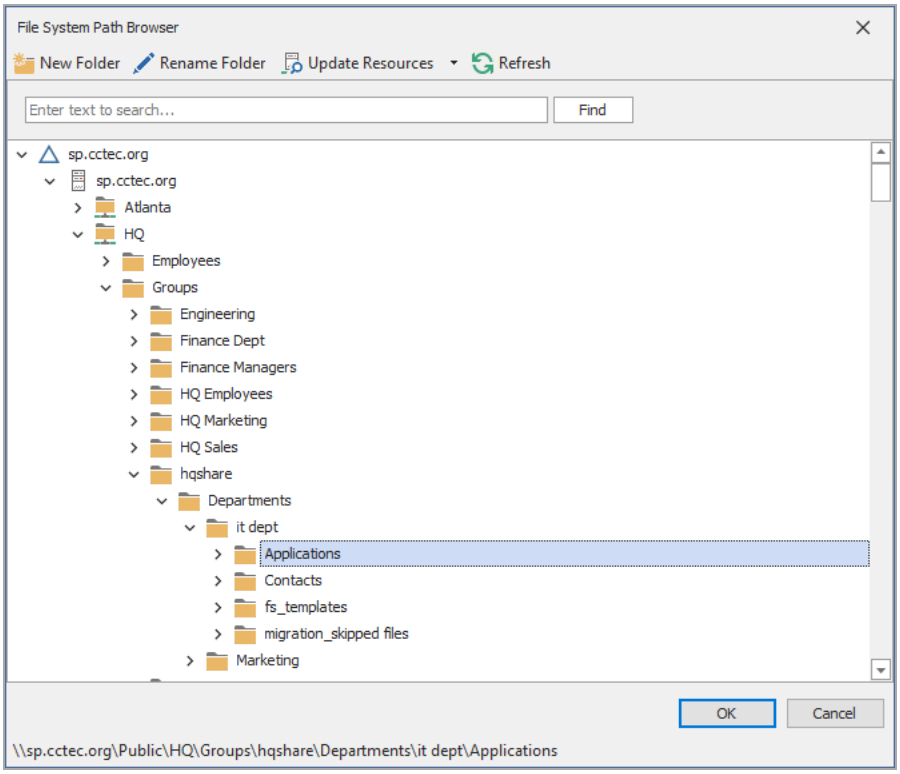
1. In the Admin Client, click the *Target Driven* tab.
2. Click *Policies*.

3. Select *New > Copy Policy*.



4. In the *Name* field, give the Copy policy a descriptive name.
   For example: Copy User Available Apps from Helpdesk Share to London Server.
5. Click the *Browse* button that pertains to the *Source* field.

6. In the File System Path Browser, specify the location in the file system from where you will be copying files for this policy.



7. Click the *Browse* button that pertains to the *Destination* field.
8. In the File System Path Browser, specify the location in the file system where you want the selected files copied for this policy.
9. Select the *Remove completed jobs older than* check box and specify the number of days that a Copy task from this policy is listed on the Jobs list before it is purged.
10. In the *Copy Options* region, specify your copy settings.

    Overwrite Existing Data: With the default setting, File Dynamics will overwrite an existing file on the target destination only if the same file from the source location is newer. You can adjust this setting to your preferences. If the *Overwrite Existing Data* check box is deselected, all duplicate named files will not be copied.

    Copy Security: When selected, this setting maintains the file permissions from the source location to the destination location.

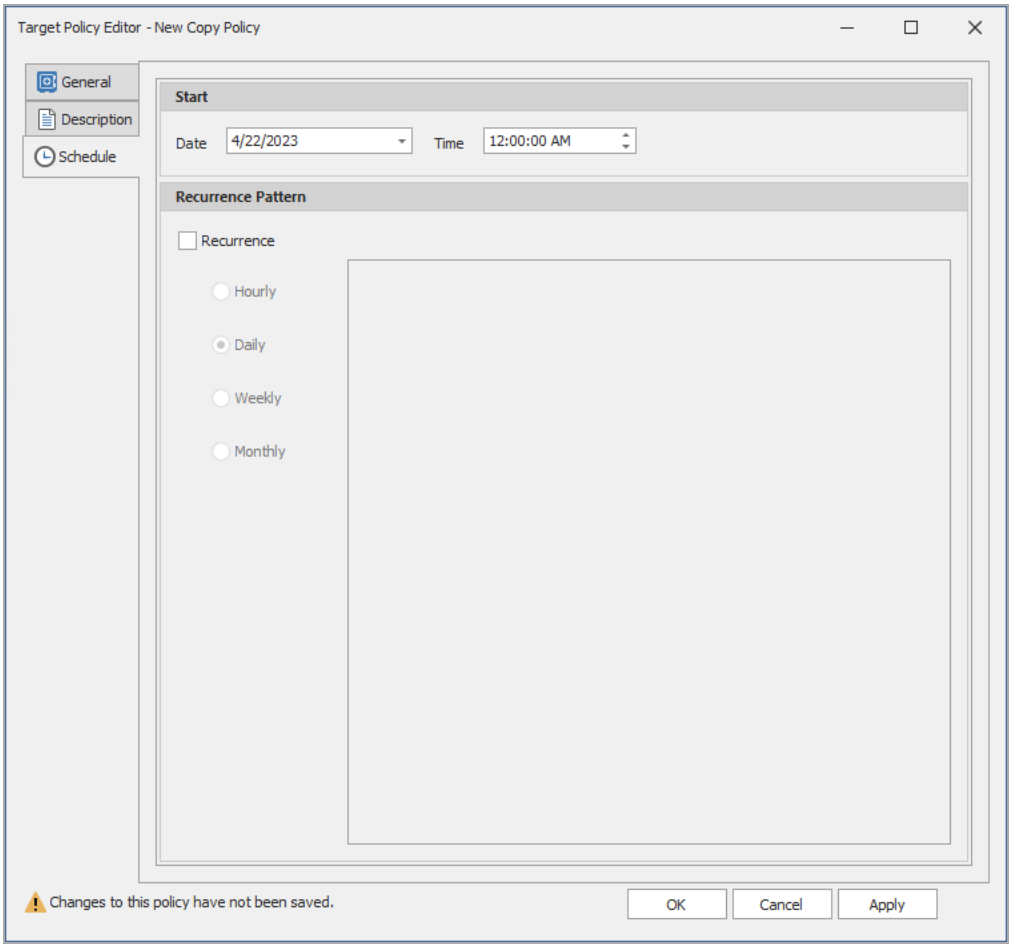
    - **Merge Permissions:** Merges permissions from the source to the target if the target contains permissions that are not present in the source. This applies to all folders and files in the source folder structure.
    - **Overwrite Permissions:** Overwrites permissions in the target with those found in the source. This applies to all folders and files in the target folder structure.

Copy Quota: If the target supports quota management, this setting maintains the disk quota settings from the source location to the destination location.

Skip Open Files: Skips all of the files that are opened from the source folder.

With Copy policies, File Dynamics does not attempt to copy skipped files later. You might want to therefore schedule a Copy policy to run during a time when users are logged out.

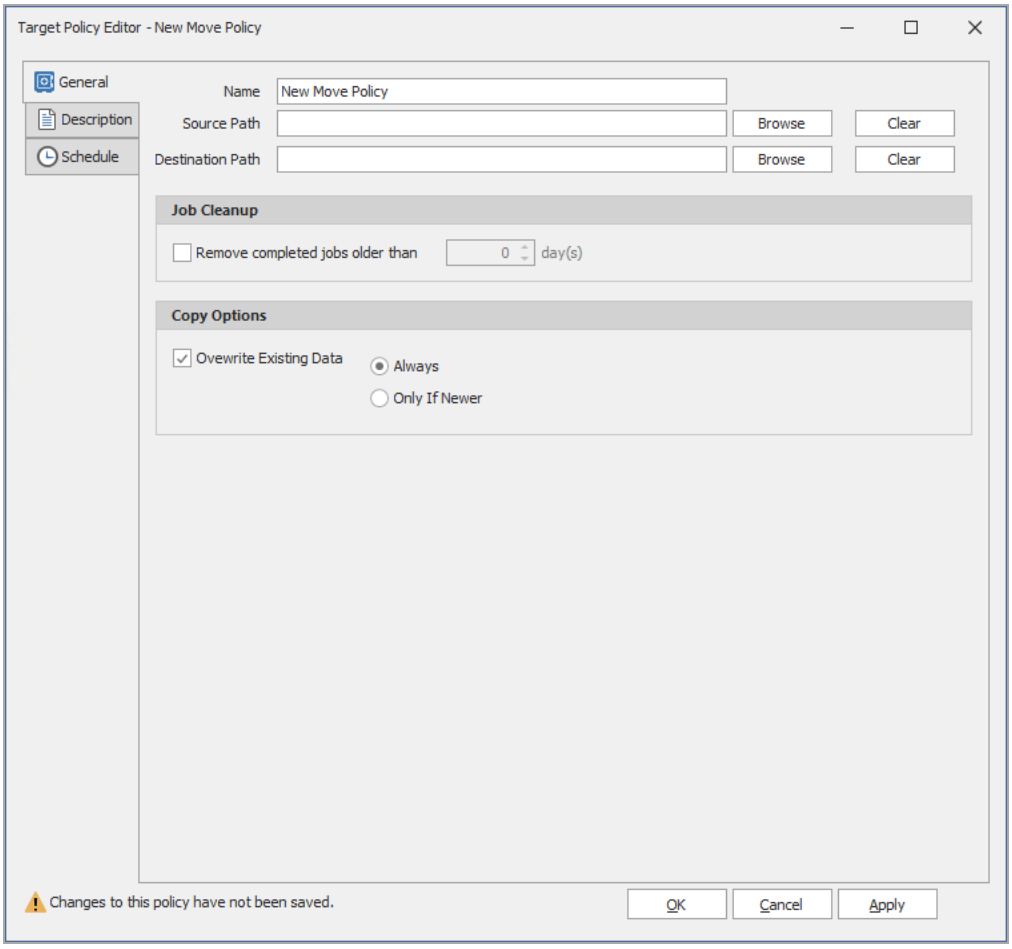
11. Click the *Description* tab and enter any information you want about the policy.
12. Click the *Schedule* tab.



13. In the *Date* field, specify the date you want the policy to be initially invoked.
14. In the *Time* field, specify the time you want the policy to be initially invoked.
15. (Conditional) If you want the Copy policy to run on a recurrent basis, select the *Recurrence* check box and then select one of the options.
16. Click *Apply* to save the schedule.
17. Click *OK*.

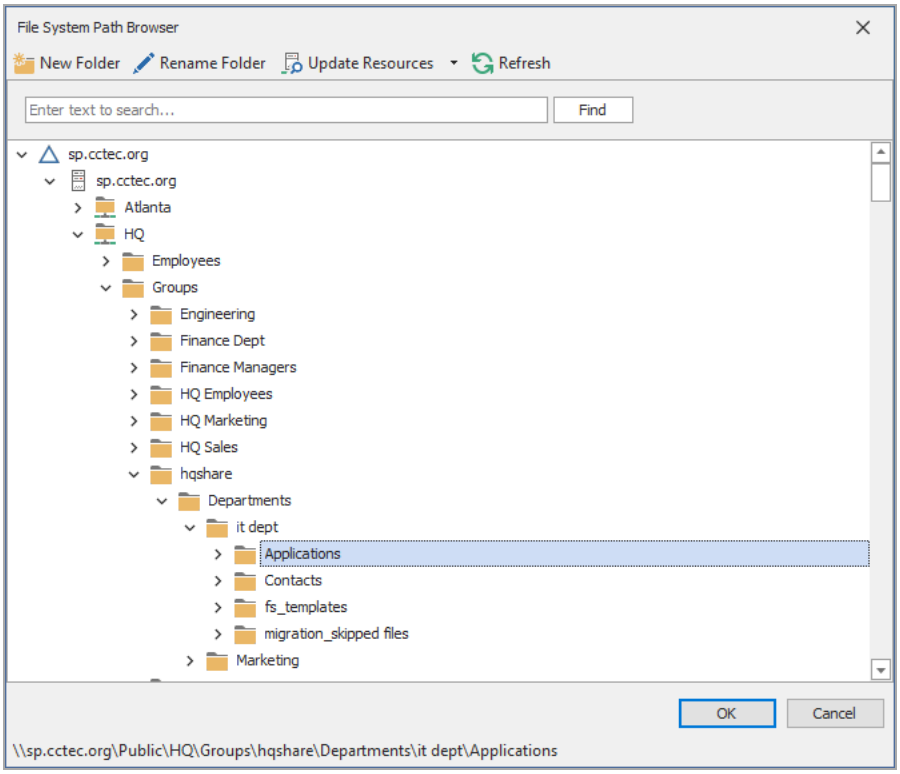
9.4 - Create a Move Policy

1. In the Admin Client, click the *Target Driven* tab.
2. Click *Policies*.
3. Select *New > Move Policy*.



4. In the *Name* field, give the Move policy a descriptive name.
   For example, Move NY Departments to Atlanta.
5. Click the *Browse* button that pertains to the *Source Path* field.

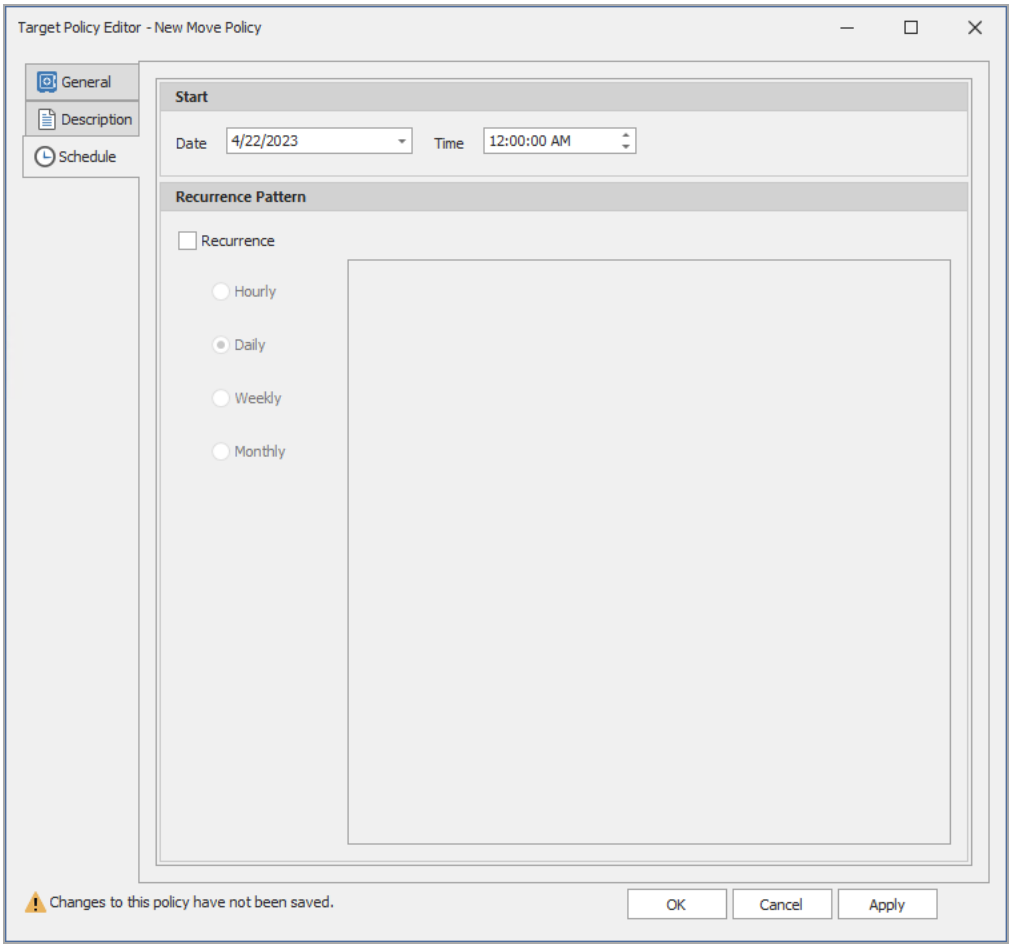
6. In the File System Path Browser, specify the location in the file system from where you will be moving files for this policy.



7. Click the *Browse* button that pertains to the *Destination Path* field.
8. In the File System Path Browser, specify the location in the file system where you want the selected files moved for this policy.
9. Select the *Remove completed jobs older than* check box and specify the number of days that a Move task from this policy is listed on the Jobs list before it is purged.
10. In the *Copy Options* region, specify your copy settings.

    Overwrite Existing Data: With the default setting, File Dynamics will overwrite an existing file on the target destination only if the same file from the source location is newer. You can adjust this setting to your preferences. If the *Overwrite Existing Data* check box is deselected, all duplicate named files will not be copied.
11. Click the *Description* tab and enter any information you want about the policy.

12. Click the *Schedule* tab.



13. In the *Date* field, specify the date you want the policy to be initially invoked.
14. In the *Time* field, specify the time you want the policy to be initially invoked.
15. (Conditional) If you want the Move policy to run on a recurrent basis, select the *Recurrence* check box and then select one of the options.
16. Click *Apply* to save the schedule.
17. Click *OK*.

9.5 - Create a Workload Policy

Workload policies in File Dynamics provide the ability to handle work processes initiated from other applications. For example, reports generated in OpenText File Reporter that specify the location of sensitive files can be imported into the Data Owner Client where a designated Data Owner can remediate the location of these sensitive files. This approach empowers organizations to provide automated network file system security remediation approved by a gatekeeper familiar with the files.

Workload policies specify source paths, along with the Data Owners who can access these paths.

Before Data Owners can move file to a destination target path, you should verify that the Data Owners have permissions to the destination target path.

9.5.1 - Workload Policy Example Scenario

A network administrator uses OpenText File Reporter to generate a report of potentially sensitive files and their locations on the network. Through the report, it is discovered that there are a number of files with Social Security numbers buried deep in a subfolder accessible by a group of users who shouldn't have access to that sensitive information.

The network administrator decides that these sensitive files need to be moved to the `HR` folder, where only members of the HR group have access. He creates a Workload policy and within the policy, specifies which users in the `HR` container are to be Data Owners for this policy as well as each of the file system paths where the sensitive files currently reside on the network.

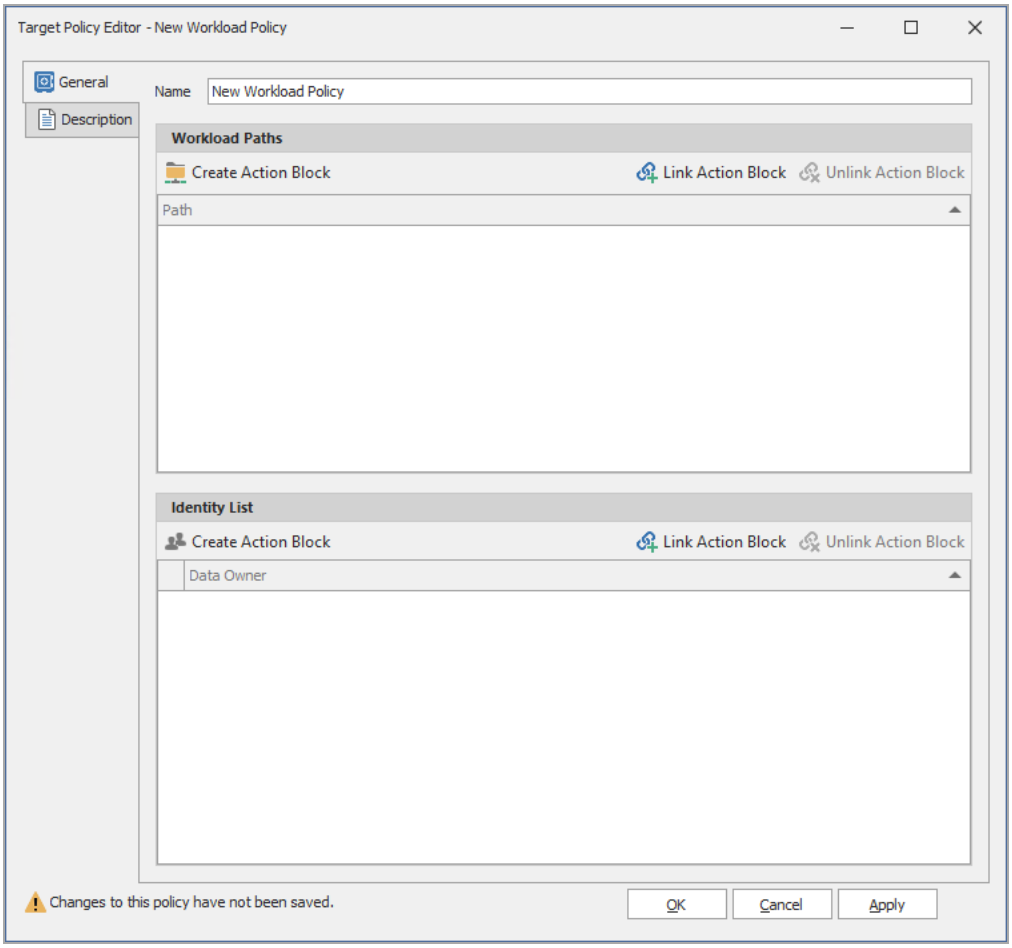
With the Workload policy saved, a Data Owner designated in the policy can now launch the Data Owner Client, import the `CSV` file listing all of the sensitive files and their locations, and then specify where to move those files – in this example, to the network path of the `HR` folder.

Upon clicking *OK*, each file to be moved is consolidated into a single move job in the job queue. Once the files have been moved, the specific details are recorded, where they can be reviewed.

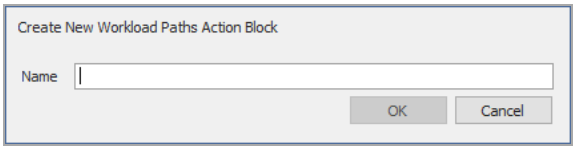
9.5.2 - Creating a Workload Policy

1. In the Admin Client, click the *Target Driven* tab.
2. Click *Policies*.

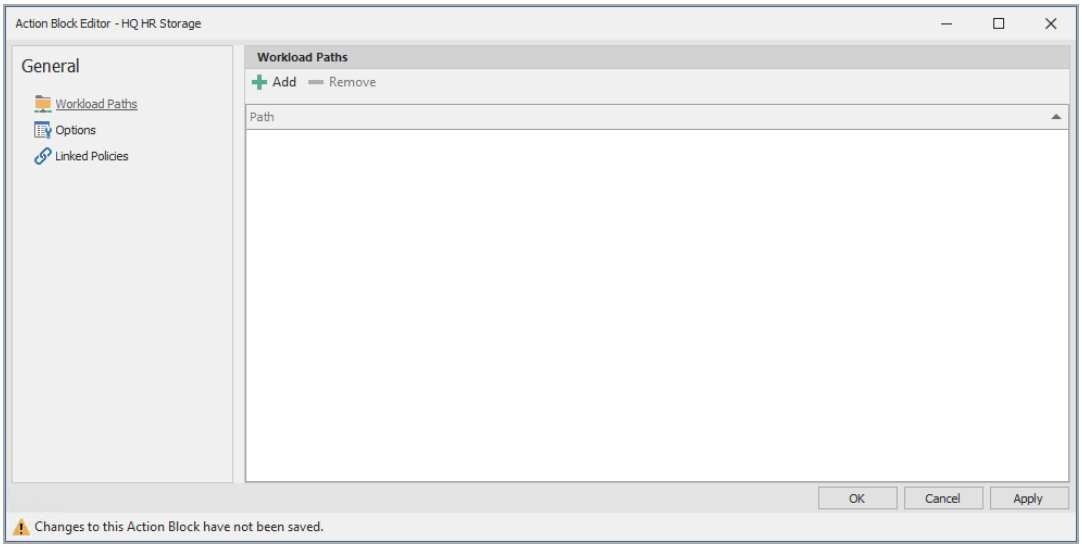
3. Select *New > Workload Policy*.



4. In the *Name* field, give the Workload policy a descriptive name. For example, HR Data Owners.
5. In the *Workload Paths* region, click *Create Action Block*.



6. In the *Name* field, enter a descriptive name and click *OK*.
   For example HQ HR Storage.



7. Click *Add* and from the File System Path Browser, select a path from which the Data Owners will be able to perform Workload policy management tasks.

   For example, moving sensitive files from the specified path to a new location.

   Add all applicable paths.

8. Click *Apply*.
9. Click *OK*.
10. In the *Identity List* region, click *Link Action Block*.
11. In the *Name* field, enter a descriptive name and click *OK*.
    For example HQ HR Data Owners.
12. In the Action Block Editor, click *Add* and from the Directory Services Browser, select the users who you want to be Data Owners for this policy.
13. Click *Apply*.
14. Click *OK* to close the Action Block Editor.
15. Click the *Description* tab and in the *Description* field, specify any information you want to include pertaining to this policy.
16. Click *Apply* to save the Workload policy.
17. Click *OK* to close the Workload policy editor.

9.5.3 - Remediating Using the Data Owner Client

Once Workload policies have been established, the specified Data Owners have the ability through the Data Owner Client to perform remediation tasks. Procedures for doing so are detailed in the *File Dynamics 24.2 Data Owner Client Guide*.

9.6 - Create a Security Notification Policy

Many organizations must comply with security regulations that require vigilance in user access to areas of the network containing personal data or other restricted or sensitive information. An HR folder containing employee Social Security numbers or a Legal Department share would both contain files whose access permissions would need to be regularly analyzed for access and security compliance.

Security Notification policies let you specify the shares or folders to be analyzed, the frequency of this analysis through scheduled scans, and the administrators who are to be notified when changes in access permissions take place.

Analysis is performed through scans conducted by the Phoenix Agents and stored in the SQL Server database. The baseline scan is stored in the SQL Database while the security notifications are stored in the CouchDB database.

9.6.1 - How Security Notification Policy Reporting Works

Reporting on security access changes is accomplished via a Security Scan, which is performed using the following information for comparison against the previous Security Scan for notification purposes:

- Discretionary access control list (DACL) of the security descriptor (SD) for the share through which the target path is being accessed
- Owner field of the SD
- Access Allowed & Access Denied (Access Control Entry) ACEs in the DACL

  Inherited ACEs in the DACL are only evaluated on the target path.

  Directly assigned ACEs are evaluated on the target path and all subordinate folders.
- Group memberships in AD for security-enabled Domain Global Groups and Universal Groups
- Local groups on the member server that may have members that reside in an AD domain

If there are any changes to these items, a notification is sent identifying the scope of the change.

Security Notification Policy Scan

A Security Scan will retrieve the DACL and Owner sections of the SD of folders for storage and evaluation purposes.

A Security Scan can be scheduled or executed manually. A Phoenix Agent is responsible for performing the scan.

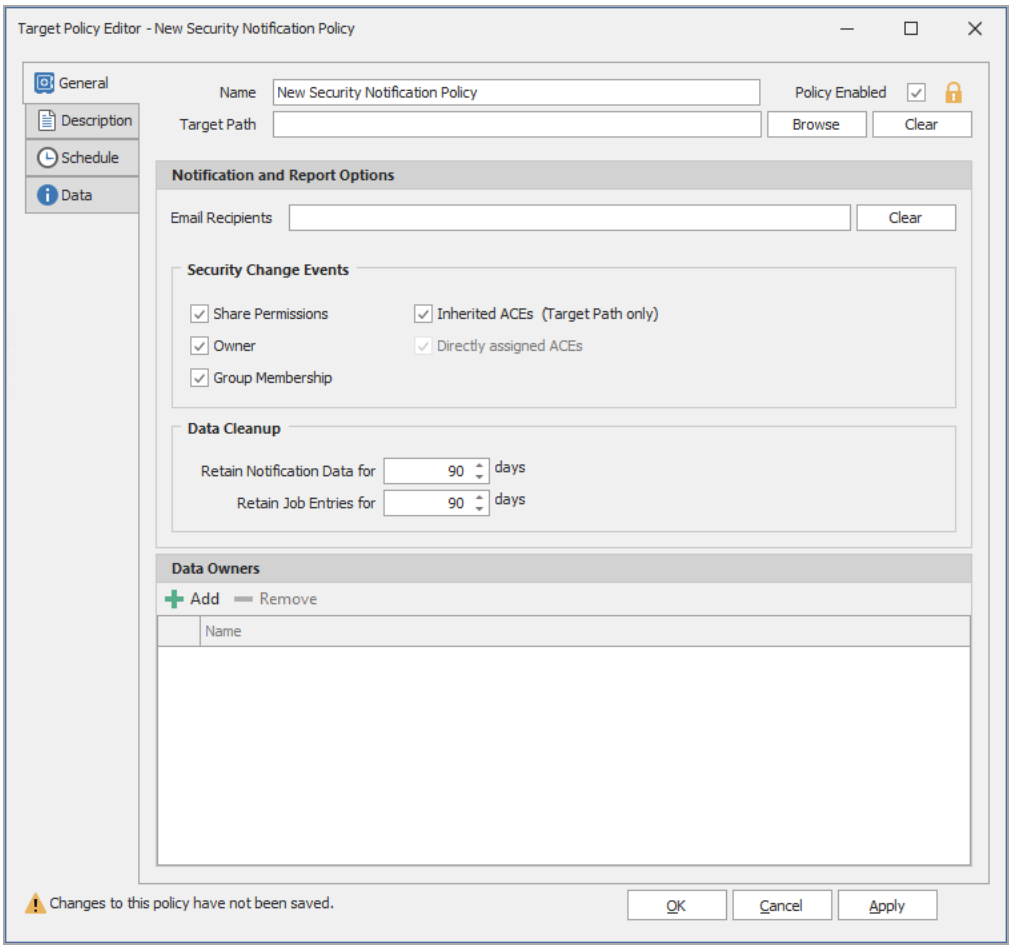
Email Reporting

The email report is text based and includes the following:

- The policy responsible for triggering the notification
- The target path of the policy

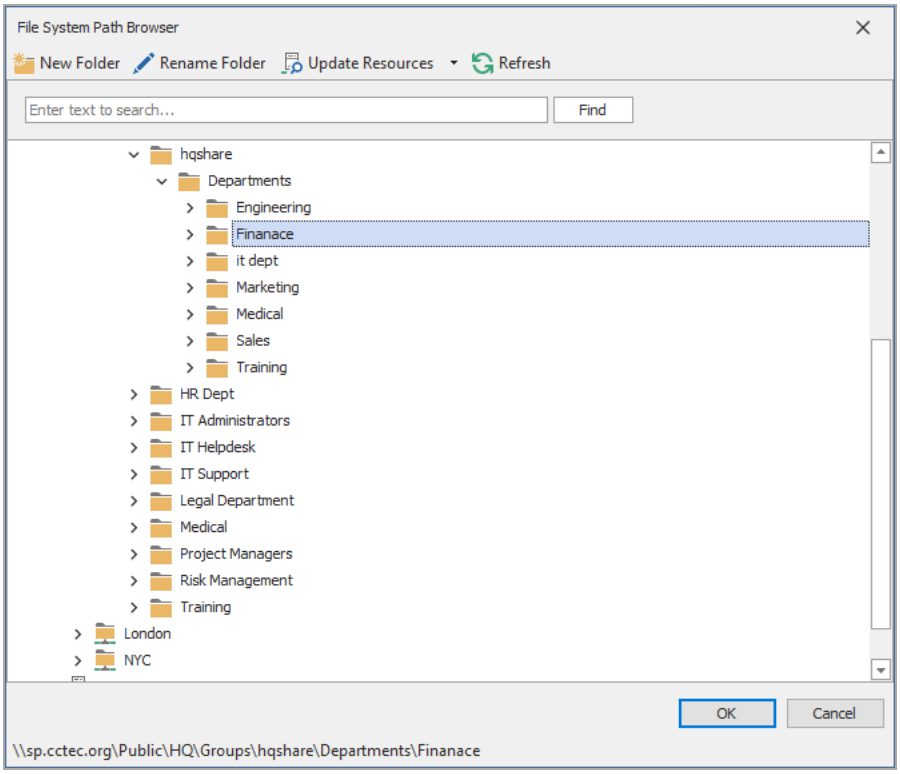
9.6.2 - Creating a Security Notification Policy

1. In the Admin Client, click the *Target Driven* tab.
2. Click *Policies*.
3. Select *New > Security Notification Policy*.



4. In the *Name* field, give the Security Notification policy a descriptive name.
   For example, HQ Finance Notification Policy
5. Leave the *Policy Enabled* check box selected.
   This check box is provided for administrators when they are editing a policy. Deselecting this check box lets you suspend all notifications scanning and notifications for this policy until the administrator has finished updating the policy or file system permissions.

6. Click the *Browse* button pertaining to the *Target Path* field and specify the share or folder for this policy.



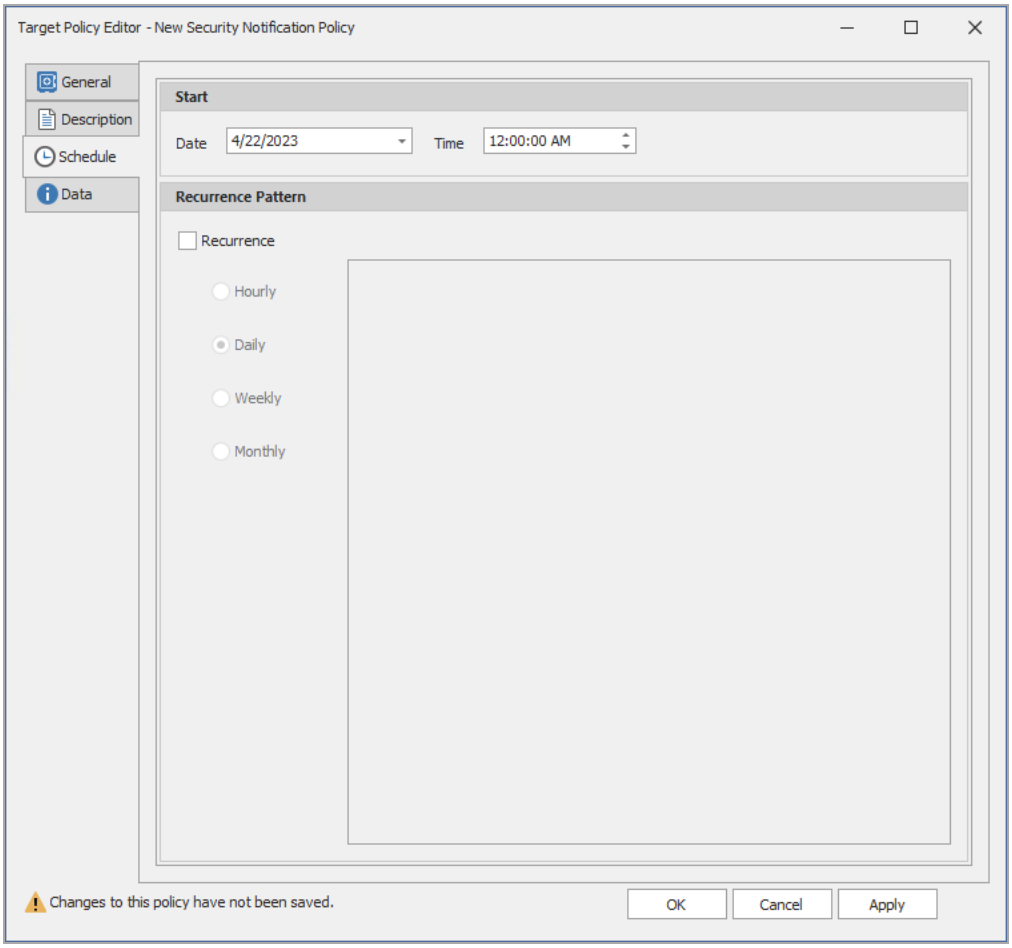
7. In the *Email Recipients* field, specify the email addresses of each user you want notified when access permissions to the selected folder or share are changed.

   Email addresses can be separated by a comma, semicolon, or a space.

   File Dynamics only reports on the changes in permissions between one scan and the next. Therefore, if there are no changes in access permissions between scans, no notifications will be emailed.

8. In the *Security Change Events* region, specify the event types for which this policy will email notifications.
9. In the *Data Cleanup* region, specify how long you want scan job information to remain in the database.
   For more information, see *Security Lockdown Policy (page 219)*.
10. In the *Data Owners* region, click *Add* to specify the users or groups that will serve as Data Owners for this policy.
    Data Owners assigned for a Security Notification policy will be enabled to view changes in the security reports via the Data Owner Client.
11. Click the *Description* tab and in the *Description* field, specify any information you want to include pertaining to this policy.

12. Click *Schedule*.



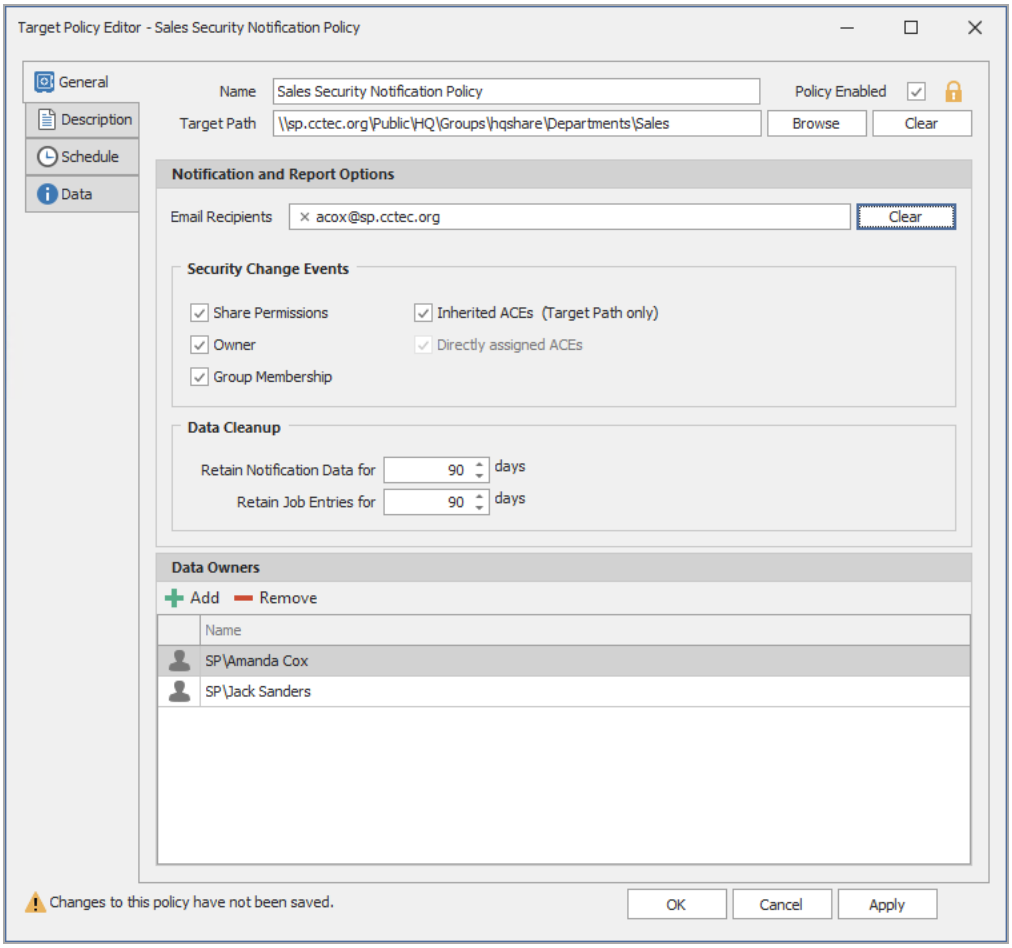
13. In the *Date* field, specify the date you want the policy to be initially invoked.
14. In the *Time* field, specify the time you want the policy to be initially invoked.
15. (Conditional) If you want the policy to run on a recurrent basis, select the *Recurrence* check box and then select one of the options.
16. Click *Apply* to save the schedule.
17. Click *OK*.

9.6.3 - Editing a Security Notification Policy and Resetting the Baseline

There might be times when you need to adjust the permissions assignments for a target path that is being monitored through a Security Notification policy.

1. In the Admin Client, click the *Target-Driven* tab.
2. Click Policies.

3. From the list of policies, double-click the Security Notification policy you want to edit.



4. Deselect the *Policy Enabled* check box.
5. Click *OK*.
   In the policy list, note the new warning icon indicating that the policy you are editing is now disabled.
6. In the network file system, make any needed security changes.
7. From the list of policies, double-click the Security Notification policy you disabled previously.
8. Select the *Policy Enabled* check box.
9. Click *OK*.
10. From the *Execute* drop-down menu, select *Reset Baseline*.
11. From the *Execute* drop-down menu, select *Security Scan*.
    This creates the new baseline.

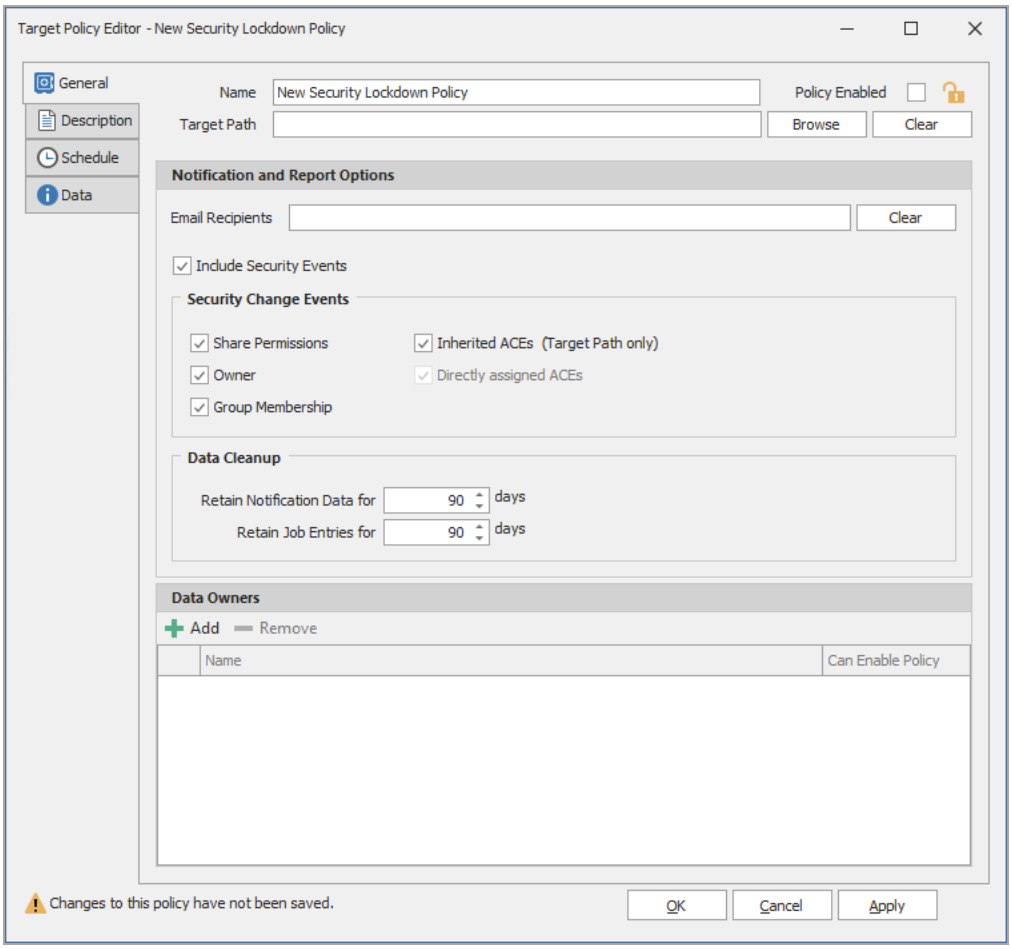
9.7 - Create a Security Lockdown Policy

Sensitive data should be accessible on a “need to know” basis, meaning that only a limited set of individuals, based on their roles, should have access to this sensitive data. Furthermore, Data Owners, those most familiar with the sensitivity of the data and who should have access to it, should be empowered to be the ultimate decision makers.

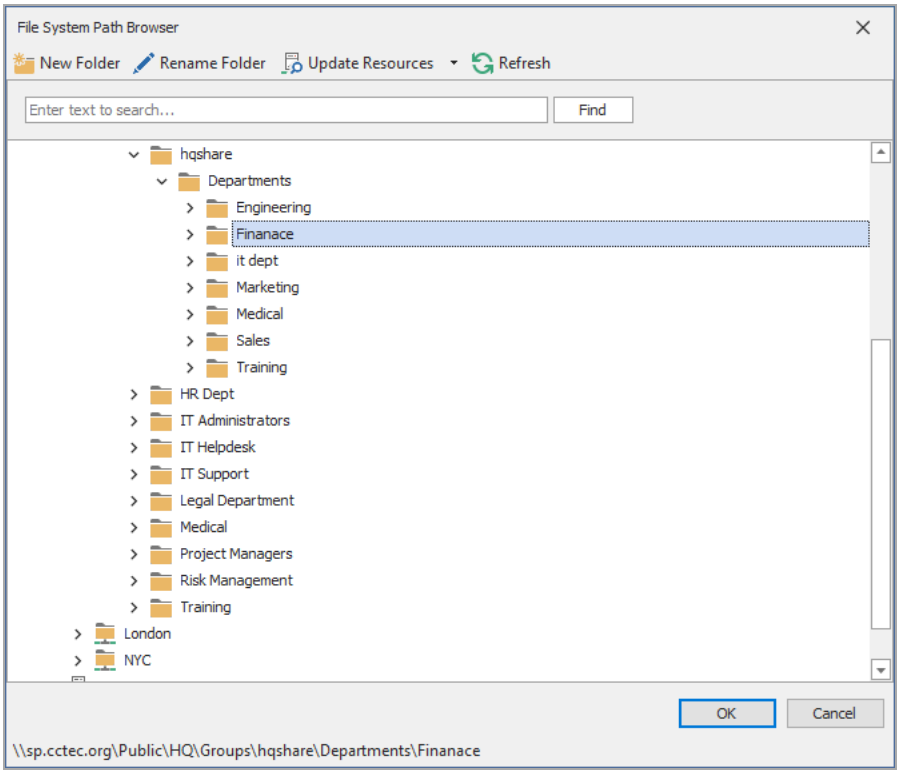
Once you have established the proper access permissions for a high-value target, you can establish the baseline of access permissions for the target path that will be strictly enforced through a Lockdown policy. When unauthorized access permission changes are made to the target path or its subfolders, the new permissions are removed and the permissions specified in the Lockdown policy are restored.

9.7.1 - Creating a Security Lockdown Policy

1. In the Admin Client, click the *Target Driven* tab.
2. Click *Policies*.
3. Select *New* > *Security Lockdown Policy*.



4. In the *Name* field, give the Security Lockdown policy a descriptive name. For example, HQ Finance Lockdown Policy.
5. Click the *Browse* button pertaining to the *Target Path* field and specify the share or folder for this policy.



6. (Conditional) If the currently established access permissions to the specified target path are the permissions you want enforced, select the *Policy Enabled* check box.

   Otherwise, come back and select the check box after you have updated the access permissions to the target path.

   Once this option is selected, this becomes the baseline for comparison for all Security Scans.

7. In the *Email Recipients* field, specify the email addresses of each user you want notified when access permissions to the selected folder or share take place.

   Email addresses can be separated by a comma, semicolon, or a space.

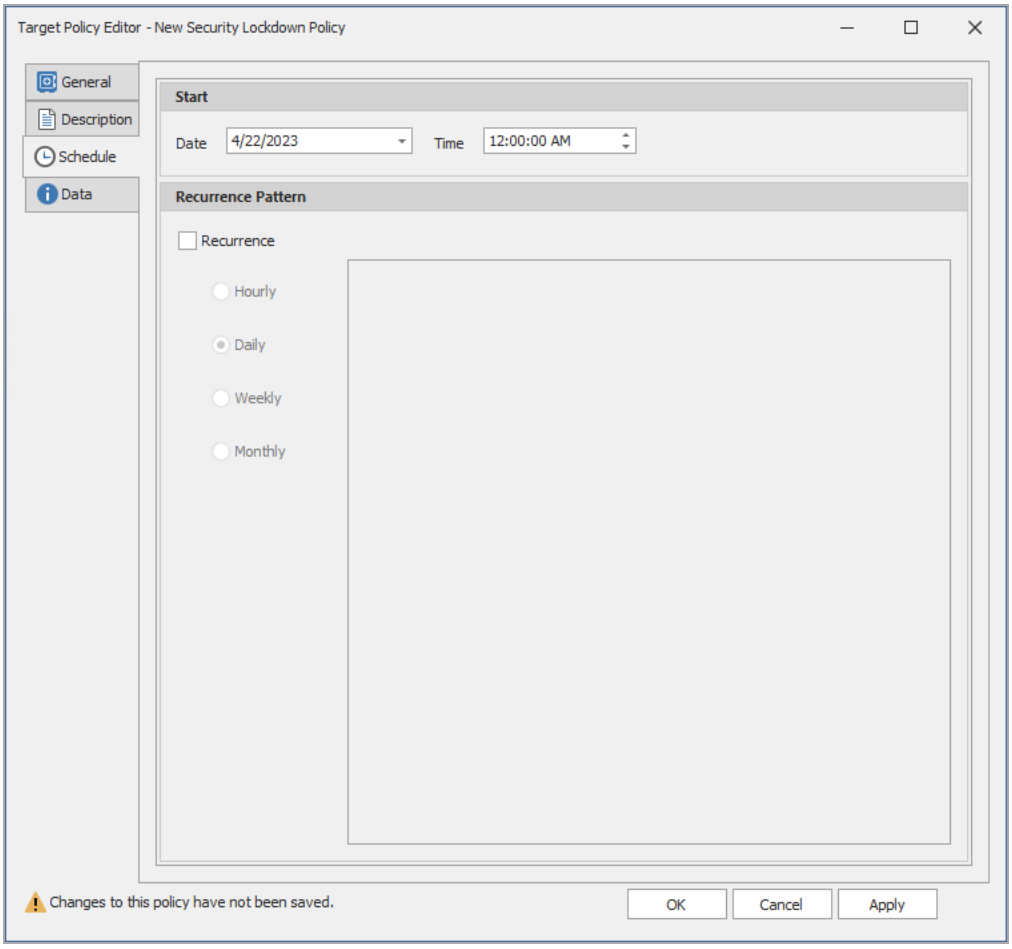
   File Dynamics only reports on the changes in permissions between one scan and the next. Therefore, if there are no changes in access permissions between scans, no notifications will be emailed.

8. In the *Security Change Events* region, specify the event types for which this policy will email notifications.

9. In the *Data Cleanup* region, specify how long you want scan job information to remain in the database.
   For more information, see *Security Lockdown Policy (page 219)*.
10. In the *Data Owners* region, click *Add* to specify the users or groups that will serve as Data Owners for this policy.
    Data Owners assigned for a Security Lockdown policy will be enabled to view changes in access permissions in the security reports via the Data Owner Client.
11. (Conditional) If you want the specified Data Owners to be able to enable the policy, select the *Can Enable Policy* check box.

    When a Data Owner can enable a policy, he or she can enable or disable the policy. An example of when this might be helpful is when the access permissions for the target path need to be updated.

    If a Data Owner disables and then enables a policy, the Data Owner is given the option to rebuild the baseline.
12. Click the *Description* tab and in the *Description* field, specify any information you want to include pertaining to this policy.
13. Click *Schedule*.

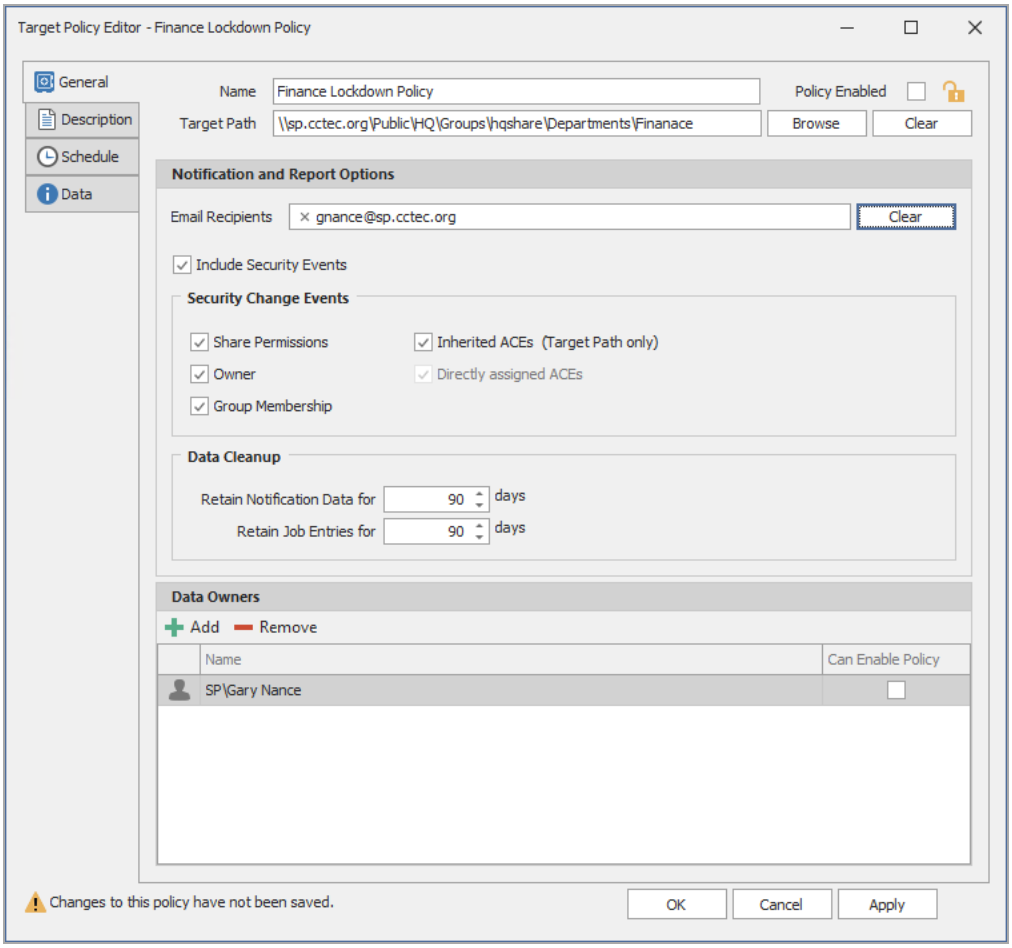


14. In the *Date* field, specify the date you want the policy to be initially invoked.
15. In the *Time* field, specify the time you want the policy to be initially invoked.
16. (Conditional) If you want the policy to run on a recurrent basis, select the *Recurrence* check box and then select one of the options.
17. Click *Apply* to save the schedule.
18. Click *OK*.

9.7.2 - Editing a Security Lockdown Policy and Resetting the Baseline

There might be times when you need to adjust the permissions assignments for a target path that is locked down through a Security Lockdown policy.

1. In the Admin Client, click the *Target-Driven* tab.
2. Click *Policies*.
3. From the list of policies, double-click the Security Lockdown policy you want to edit.



4. Deselect the *Policy Enabled* check box.

5. Click *OK*.
   In the policy list, note the new warning icon indicating that the policy you are editing is now disabled.
6. In the network file system, make any needed security changes.
7. From the list of policies, double-click the Security Lockdown policy you disabled previously.
8. Select the *Policy Enabled* check box.
9. Click *OK*.
10. From the *Execute* drop-down menu, select *Reset Baseline*.
11. From the *Execute* drop-down menu, select *Security Scan*.
    This creates the new baseline.

9.8 - Create a Security Fencing Policy

There might be some high-value targets on which you might not want to place the same level of restrictions as a Security Lockdown policy, but might nevertheless want to secure the access to only authorized users or roles.

Security Fencing policies let you set limits on how access permissions might change over time. Using a set of rules by creating inclusion and exclusion lists to define a “fence,” the policy specifies Active Directory containers, groups, users, and Security Identifiers (SIDs) that might be given permissions to a high-value target in the future without an issue or should never be given rights in the future.

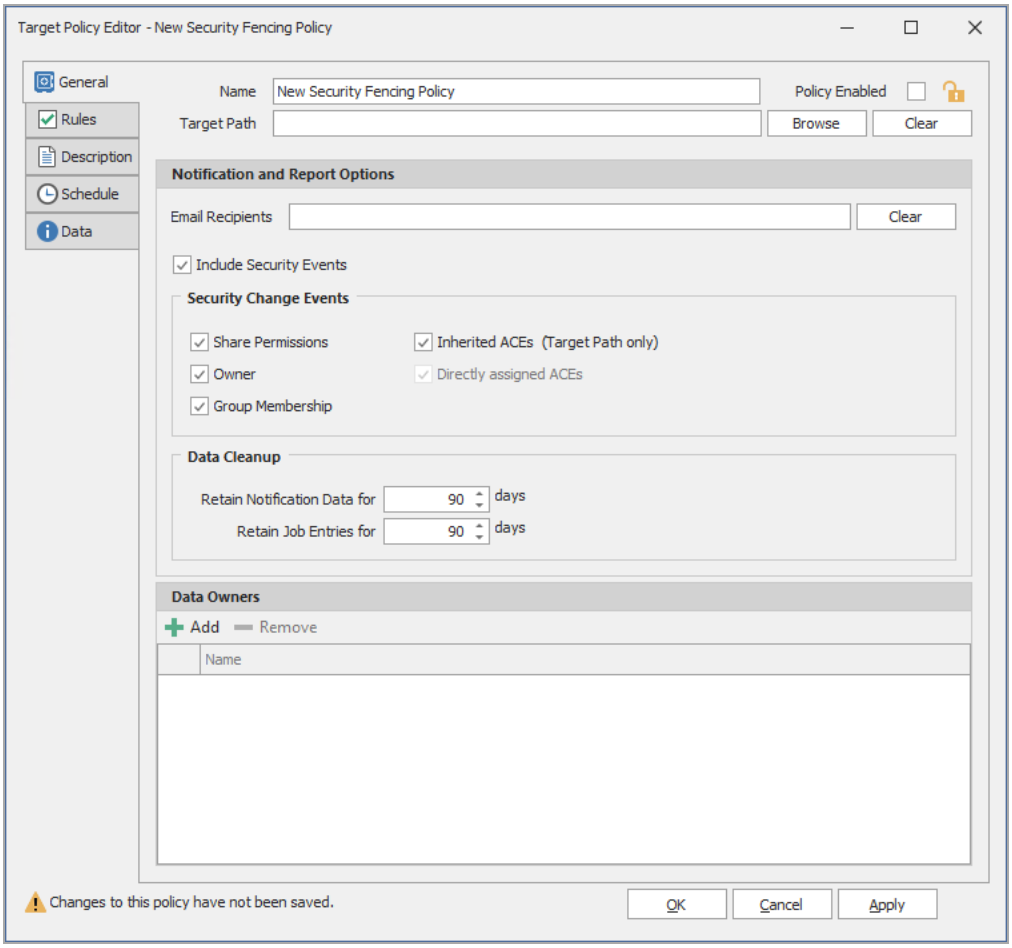
Security Fencing policies work by creating a set of rules that create a boundary around your storage against which any security will be evaluated. The security changes are then preserved or reverted based on the rules created. You should therefore create your rules carefully, potentially using tools like OpenText File Reporter to verify the permissions granted to subfolders of your target path.

There is currently no path overlap protection between policies. While this is ideal for flexibility, it is not so when you have conflicting policies.

9.8.1 - Creating a Security Fencing Policy

1. In the Admin Client, click the *Target Driven* tab.
2. Click *Policies*.

3. Select *New > Security Fencing Policy*.



4. In the *Name* field, give the Security Fencing policy a descriptive name.
   For example, Engineering Department Fencing Policy.
5. Click the *Browse* button pertaining to the *Target Path* field and specify the share or folder for this policy.
6. (Conditional) If the currently established access permissions to the specified target path are the permissions you want enforced, select the *Policy Enabled* check box.

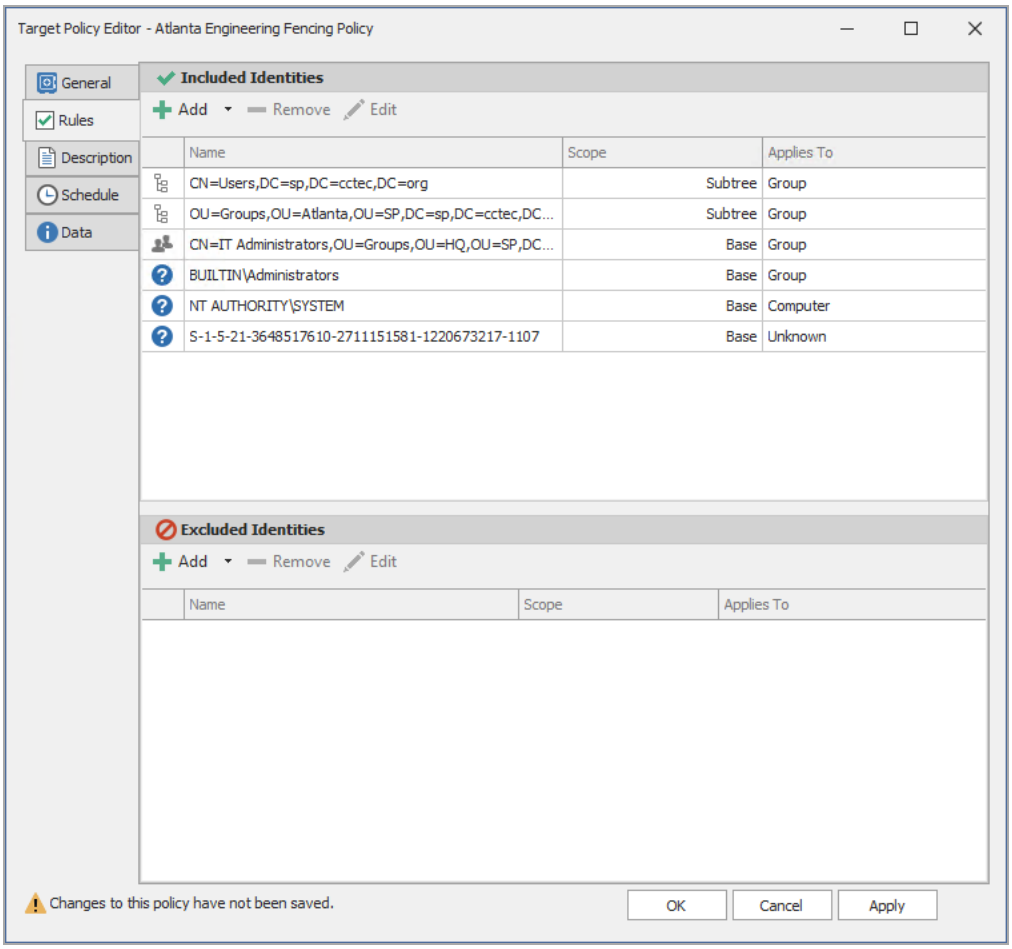
   Otherwise, come back and select the check box after you have updated the access permissions to the target path.

   Once this option is selected, this becomes the baseline for comparison for all Security Scans.
7. In the *Email Recipients* field, specify the email addresses of each user you want notified when access permissions to the selected folder or share take place.

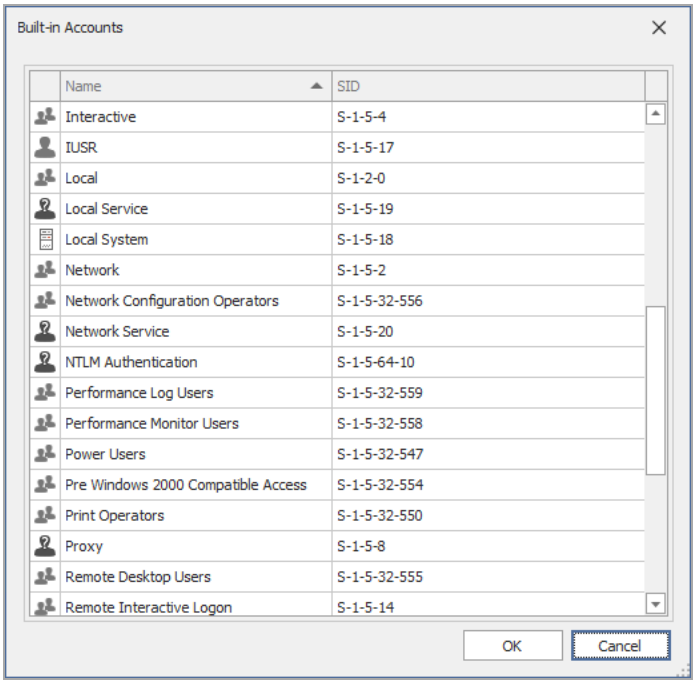
   Email addresses can be separated by a comma, semicolon, or a space.

File Dynamics only reports on the changes in permissions between one scan and the next. Therefore, if there are no changes in access permissions between scans, no notifications will be emailed.

8. In the *Security Change Events* region, specify the event types for which this policy will email notifications.
9. In the *Data Cleanup* region, specify how long you want scan job information to remain in the database.
   For more information, see *Security Fencing Policy (page 221)*.
10. In the *Data Owners* region, click *Add* to specify the users or groups that will serve as Data Owners for this policy.
    Data Owners assigned for a Security Fencing Policy will be enabled to view permitted changes in security, ownership, and group membership of folders in the target path via the Data Owner Client.
11. Click *Apply* to save your settings.
12. Click *Rules*.



13. In the *Included Identities* and *Excluded Identities* regions, use the *Add* drop-down buttons to include and exclude groups, users, and SIDs for this Fencing policy.

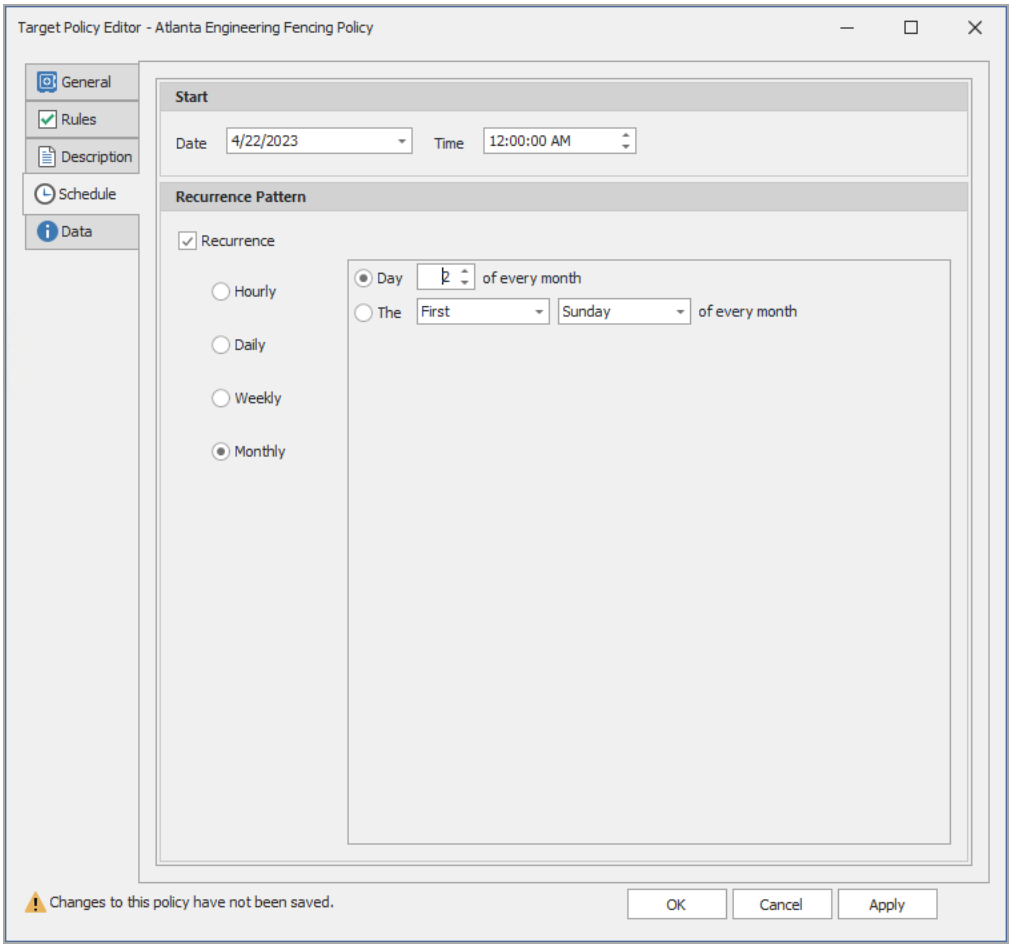


Be sure to include any desired well known security objects such as `BUILTIN\Administrators` and `NT Authority\SYSTEM` appropriate to your environment, before you perform a Security Scan. If you do not include these objects, their access will be disabled following the initial Security Scan.

For more information on creating rules for a Fencing policy, including adding Built-in accounts and Security Identifiers, see the Rules Tab under *Security Fencing Policy (page 221)*.

14. Click the *Description* tab and in the *Description* field, specify any information you want to include pertaining to this policy.

15. Click *Schedule*.

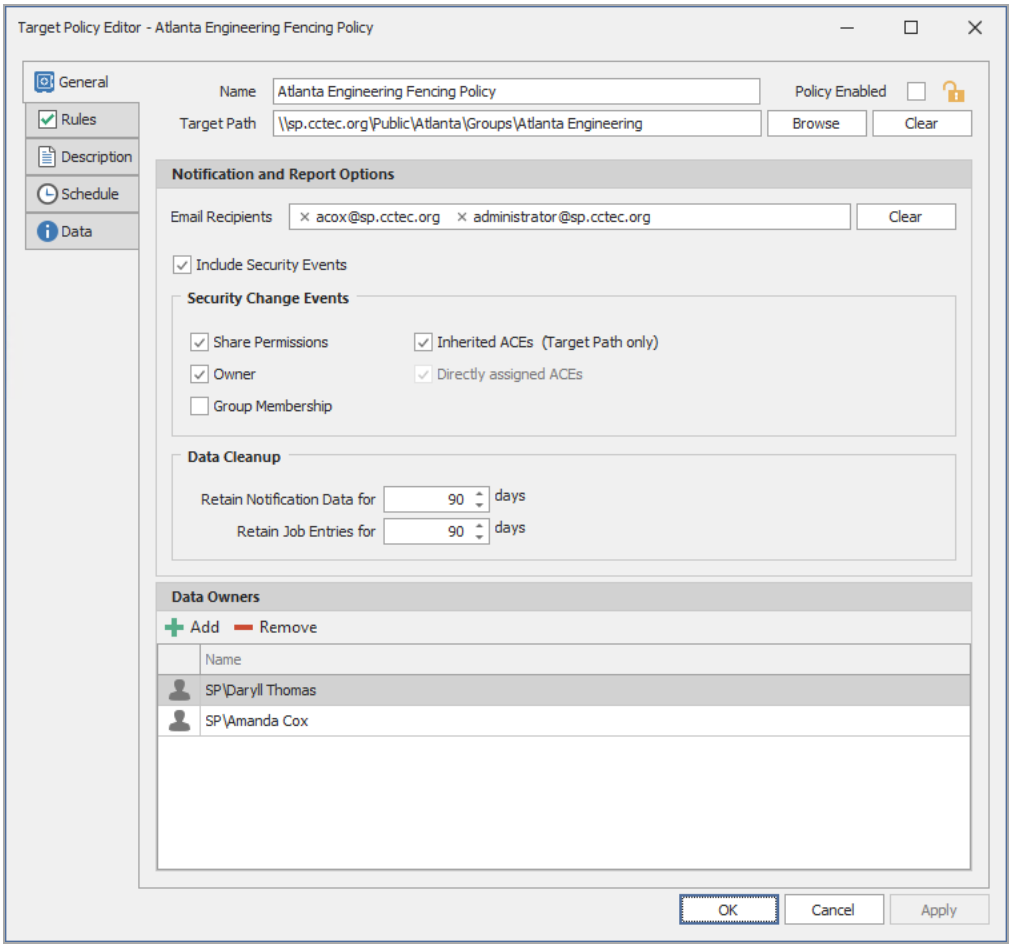


16. In the *Date* field, specify the date you want the policy to be initially invoked.
17. In the *Time* field, specify the time you want the policy to be initially invoked.
18. (Conditional) If you want the policy to run on a recurrent basis, select the *Recurrence* check box and then select one of the options.
19. Click *Apply* to save the schedule.
20. Click *OK*.
21. From the Target Policies page, highlight the Security Fencing policy and from the *Execute* drop-down menu, select *Security Scan*.
22. In the confirmation dialog box, click *Yes*.

9.8.2 - Editing a Security Fencing Policy and Resetting the Baseline

There might be times when you need to adjust the permissions assignments for a target path whose access permissions are managed through a Security Fencing policy.

1. In the Admin Client, click the *Target-Driven* tab.
2. Click *Policies*.
3. From the list of policies, double-click the Security Fencing policy you want to edit.



4. Deselect the *Policy Enabled* check box.
5. Click *OK*.
   In the policy list, note the new warning icon indicating that the policy you are editing is now disabled.
6. In the network file system, make any needed security changes.
7. From the list of policies, double-click the Security Fencing policy you disabled previously.
8. Click the *Rules* tab.
9. Preserve the security changes made in the network file system by making any needed updates in the *Included Identities* and *Excluded Identities* lists.
10. Click the *General* tab.
11. Select the *Policy Enabled* check box.

12. Click *OK*.
13. From the *Execute* drop-down menu, select *Reset Baseline*.
14. From the *Execute* drop-down menu, select *Security Scan*.
    This creates the new baseline.

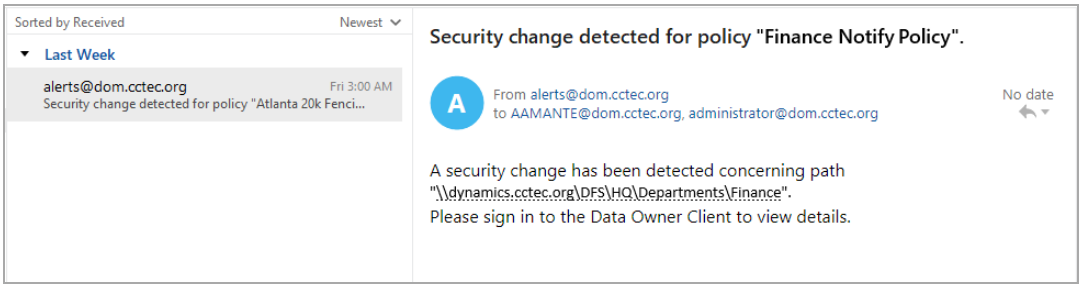
9.9 - Executing a Security Scan

In addition to executing scans through a schedule, you can do so at any time through the Admin Client.

1. In the Admin Client, click the *Target Driven* tab.
2. Click *Policies*.
3. Right-click the name of the Security policy and click *Execute* > *Security Scan*.
4. When the confirmation screen appears, click *Yes*.

   The target path for the selected Security policy is scanned for security changes. If changes are determined, an email is sent to the users specified in the *Email Recipients* field of the policy.

   A sample email is shown below:



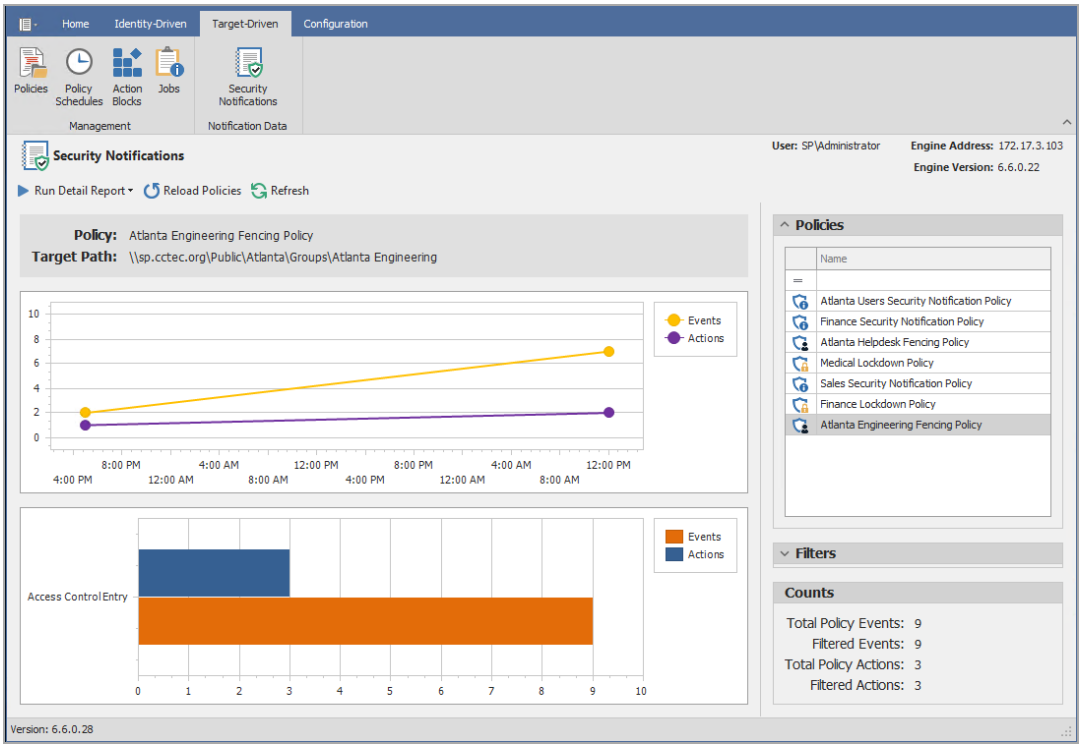
   Depending on the policy type, the email specifies that access permissions to a high-value target have been changed.

9.10 - Viewing Security Notifications

Viewing security notifications through the Security Notifications page is the means of determining changes in access permissions and group memberships for target paths managed through security policies and obtaining additional details through Detail Reports.

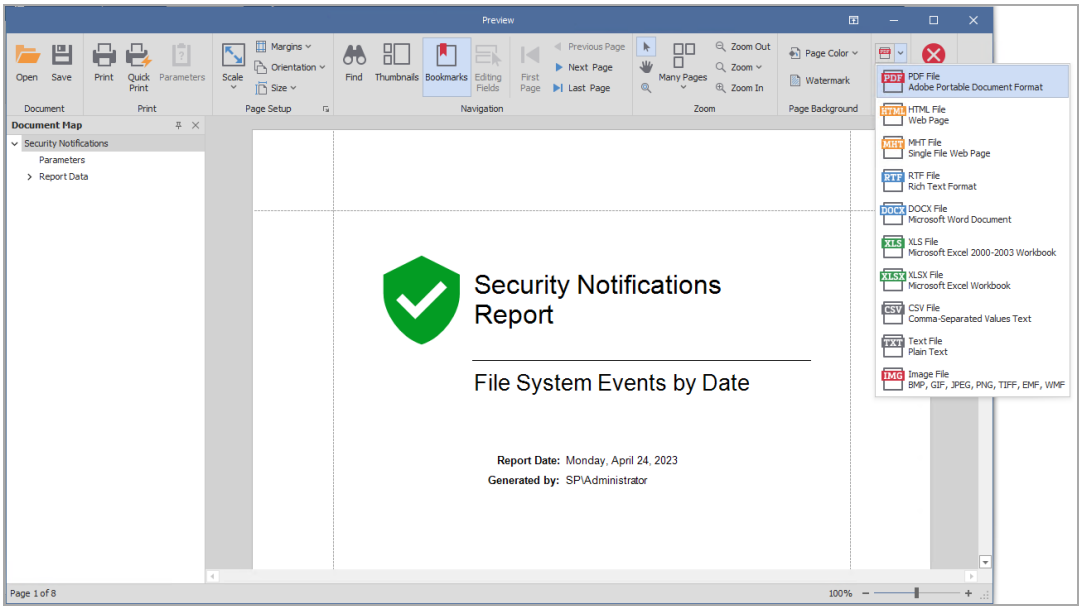
1. In the Admin Client, click the *Target Driven* tab.

2. Click *Security Notifications*.



3. From the *Policies* list, select the policy for which you want to see graphical information and reported in the Detail Report.
   If the policies are not displayed, you can click *Reload Policies* and select the security policy types to display.
4. From the *Filters* region, specify the options you want displayed in the graphs and reported in the Detail Report.
5. In the same region, specify the date range you want displayed in the graphs and reported in the Detail Report.
6. From the *Run Detail Report* drop-down menu, choose one of the following options:
   - **File System Events:** Generates a preview report of file system events that have taken place within the parameters you have specified in the right-hand portion of the Security Notifications page.
   - **Group Membership Events:** Generates a preview report of group membership events that have taken place within the parameters you have specified in the right-hand portion of the Security Notifications page.

7. From the report dialog box, export or email the report in the format you want.



10 - Work Log Reports

This chapter provides a detailed explanation of Work Log reports along with procedures for setting up and generating Work Log reports.

10.1 - Work Log Reports Overview

The Work Log is a mechanism that maintains a history of File Dynamics events. The Work Log contains summary records for events that have reached the processed state; in other words, those that have run to completion or have been aborted by administrative action.

Data from the Work Log is presented in a pivot grid based on the parameters you choose. You can use this data for historical event tracking.

The Work Log is an optional component of File Dynamics and requires you to install Apache CouchDB.

10.1.1 - Restrictions

The current Work Log implementation has the following restrictions:

- Work Log entries include only those pertaining to Identity-Driven policies. No Target-Driven policy entries are logged.
- Not all incoming events from the Event Monitor are logged. Only Event Monitor generated events that have calculated an effective policy are logged.
- A Work Log entry is written only after the event has run to completion or has been aborted.
- Events are written to the database once every minute.
- After an upgrade of a previous version of Storage Manager or File Dynamics that does not support the Work Log, or Work Log was not configured, any existing events that are active or pending will not be logged. Only new events, new events generated via Management Actions, and new Operations will be logged.

10.1.2 - Database

The Work Log leverages Apache CouchDB, an open source NoSQL database.

For recommended disk space and RAM allocations, see Installing CouchDB

10.1.3 - Configuration

You are required to install and configure CouchDB prior to enabling and configuring the Work Log.

Similar to the File Dynamics SQL Server configuration, the following will be created and managed for you via the Admin Client

- User for managing the CouchDB instance from the Engine
- User for reading from CouchDB instance from the Admin Client
- CouchDB database for the Work Log
- Any necessary views for querying the CouchDB database

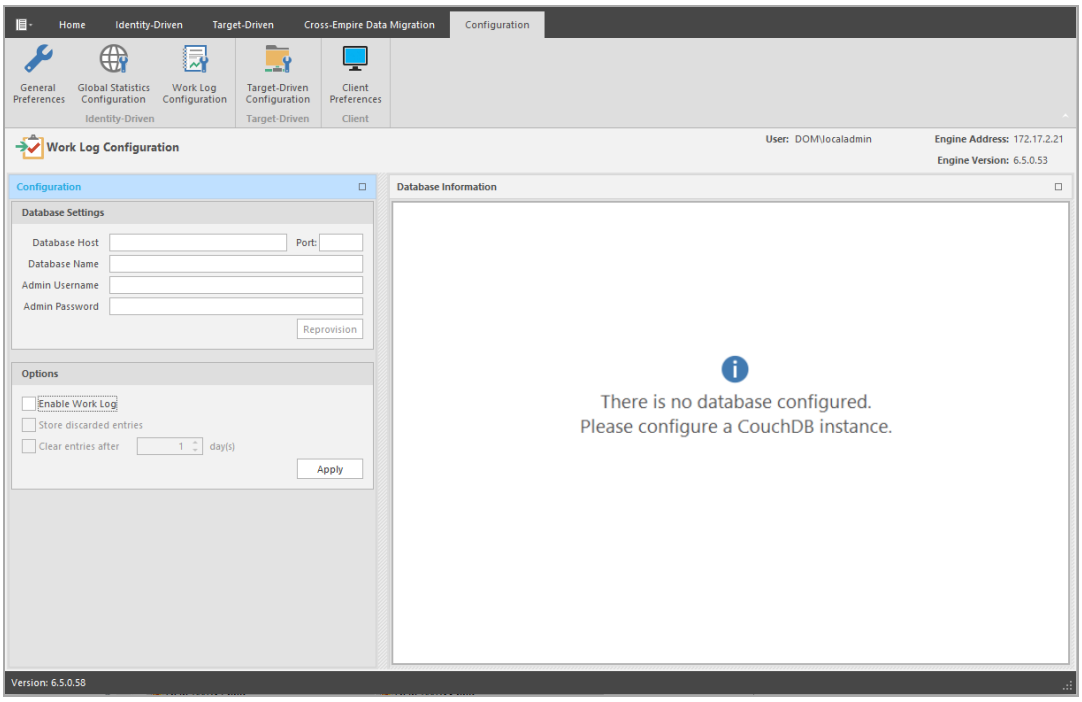
The following options are provided:

- The number of days to retain Work Log Entries
- The ability to turn the Work Log on or off

10.2 - Establishing the Work Log Database Settings in the Admin Client

Follow these procedures to establish the CouchDB settings in the Admin Client.

1. In the Admin Client, click the *Configuration* tab.
2. Click *Work Log Configuration*.



3. In the *Database Host* field, enter the IP address or DNS hostname of the server hosting the CouchDB database.
4. In the *Port* field, enter `5984`.
5. In the *Database Name* field, establish a name for the CouchDB database instance for the Work Log.
   Letters used for the database name must be lowercase.

6. In the *Admin Username* and *Admin Password* fields, enter the username and passwords you established in when you installed CouchDB.
7. Click *Provision*.
   If you go back to the Apache CouchDB administrative interface and click Databases in the menu bar, you should now see the database name you entered in Step 5.
8. Return to the Admin Client and in the *Work Log Configuration* region, specify the settings you want for Work Log entries.
9. Click *Apply*.

10.3 - Building Work Log Reports

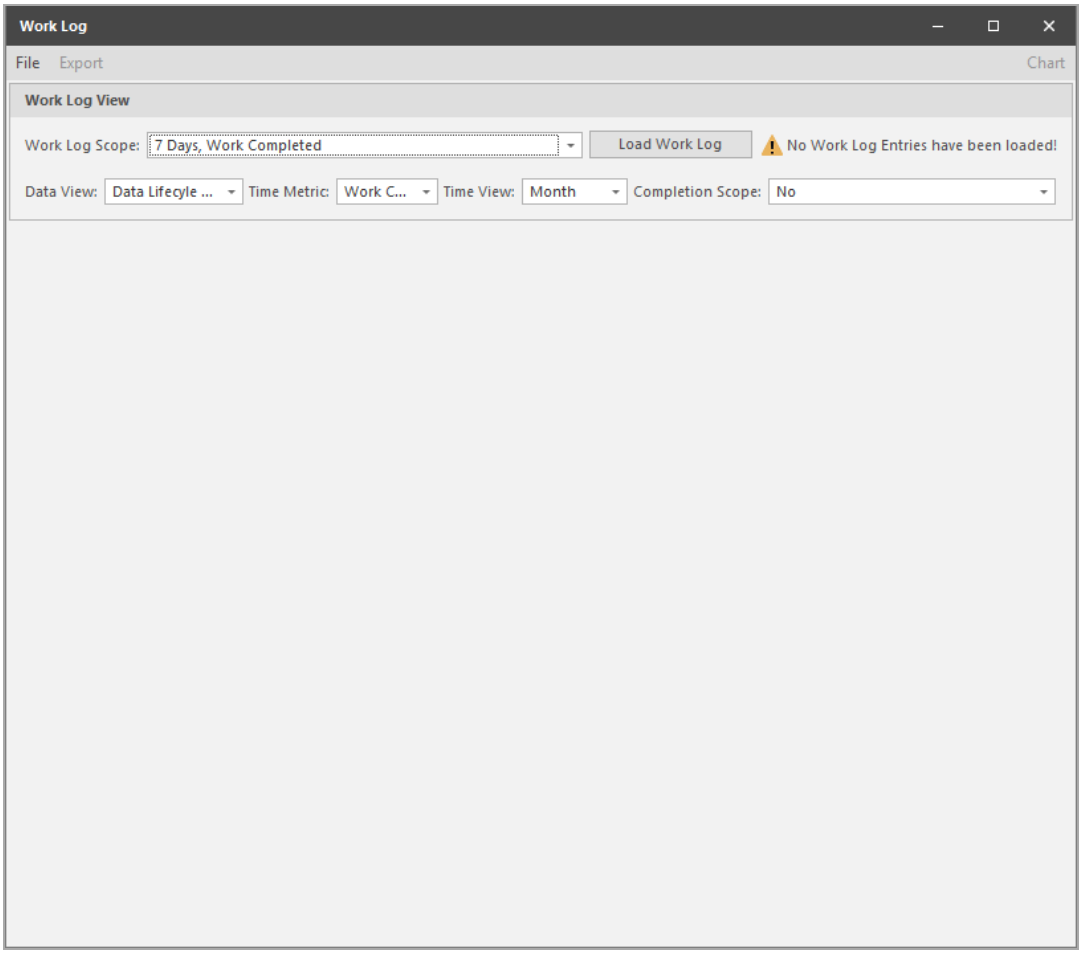
With the CouchDB database installed and the Work Log database settings established in the Admin Client, you are ready to build Work Log reports.

Work Log reports are built in the Admin Client using a pivot grid interface. There are four preset options for viewing data, along with a playground option that lets you choose the parameters and presentation of the report.

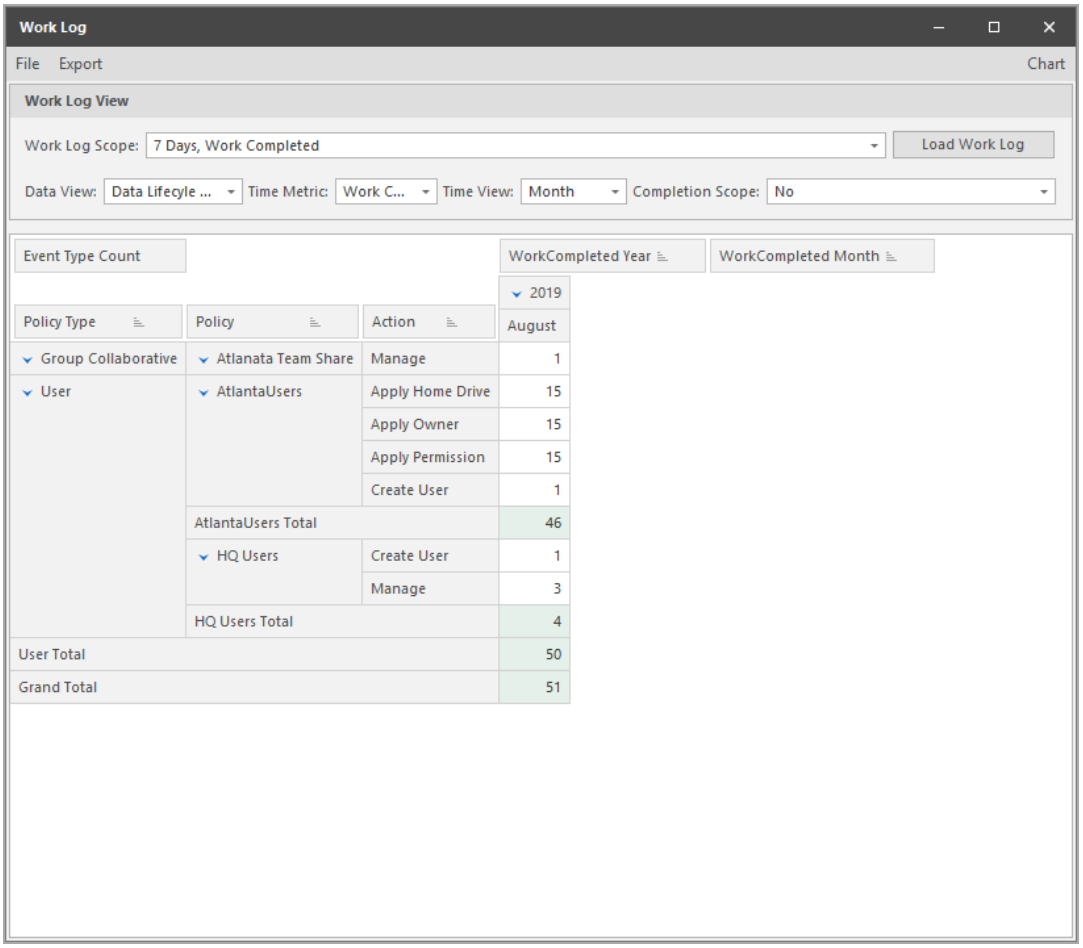
The remainder of this chapter briefly introduces you to the features and capabilities of Work Log reports through some basic procedures.

10.3.1 - Loading Work Log Entries

1. In the Admin Client, click the *Work Log* tab.
2. Click *Reports*.



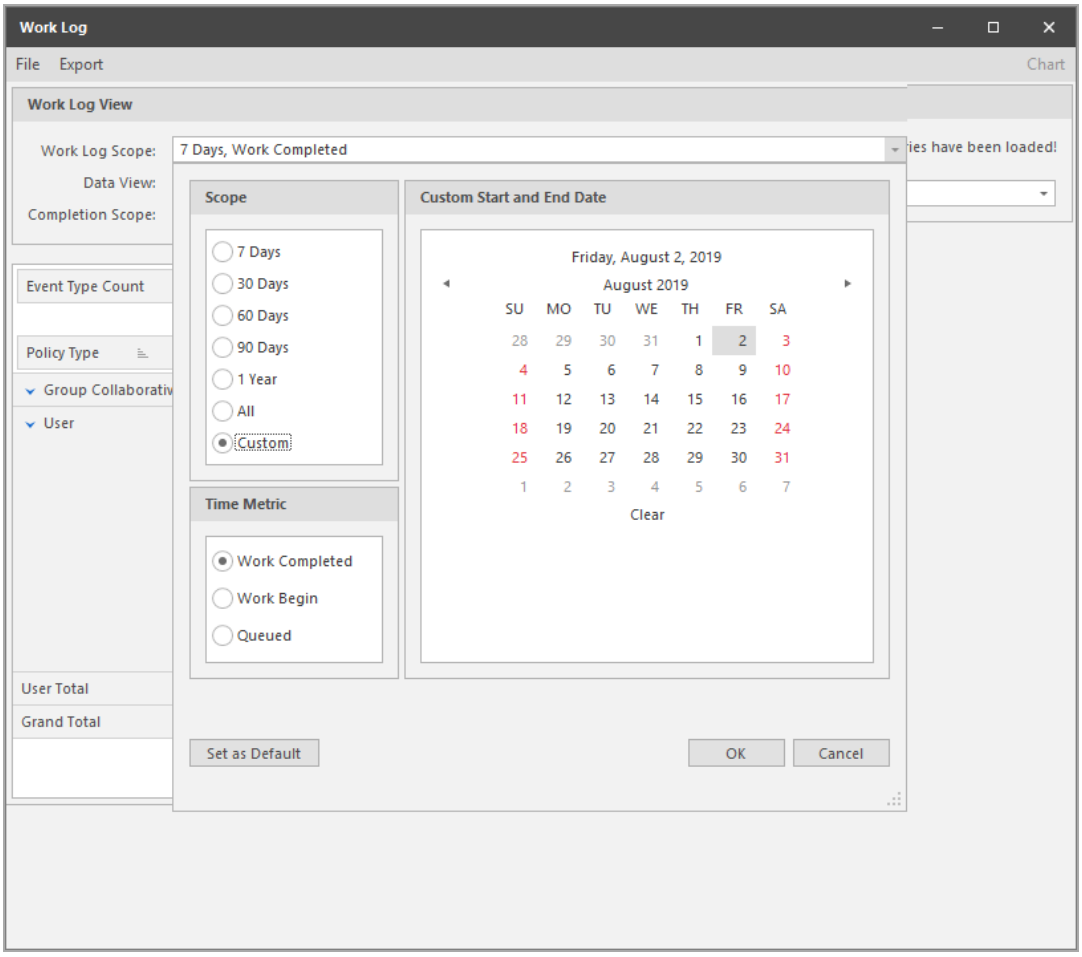
3. Click *Load Work Log Entries*.



All Work Log entries in the CouchDB database are loaded and displayed with default parameters that you can modify.

10.3.2 - Setting the Work Log Scope

1. Click the down arrow that pertains to the *Work Log Scope* field.



2. In the dialog box, specify the parameters you want by selecting applicable options.

   Scope: Lets you specify the timespan for the report. All of the *Days* options will include events, according to the selected *Time Metric* option from today's date. The *All* option will include all events, according to the selected *Time Metric* option. The *Custom* option lets you select a start and stop date from the calendar using the Shift key.

   Time Metric: Lets you specify what types of events to include in the Work Log report.

   Custom Start and End Date: This calendar is activated when you select the *Custom* option from the *Scope* region. Select a start and end date using the Shift key.

   Set as Default: Lets you establish your selected options and specifications as the default setting for all Work Log reports.

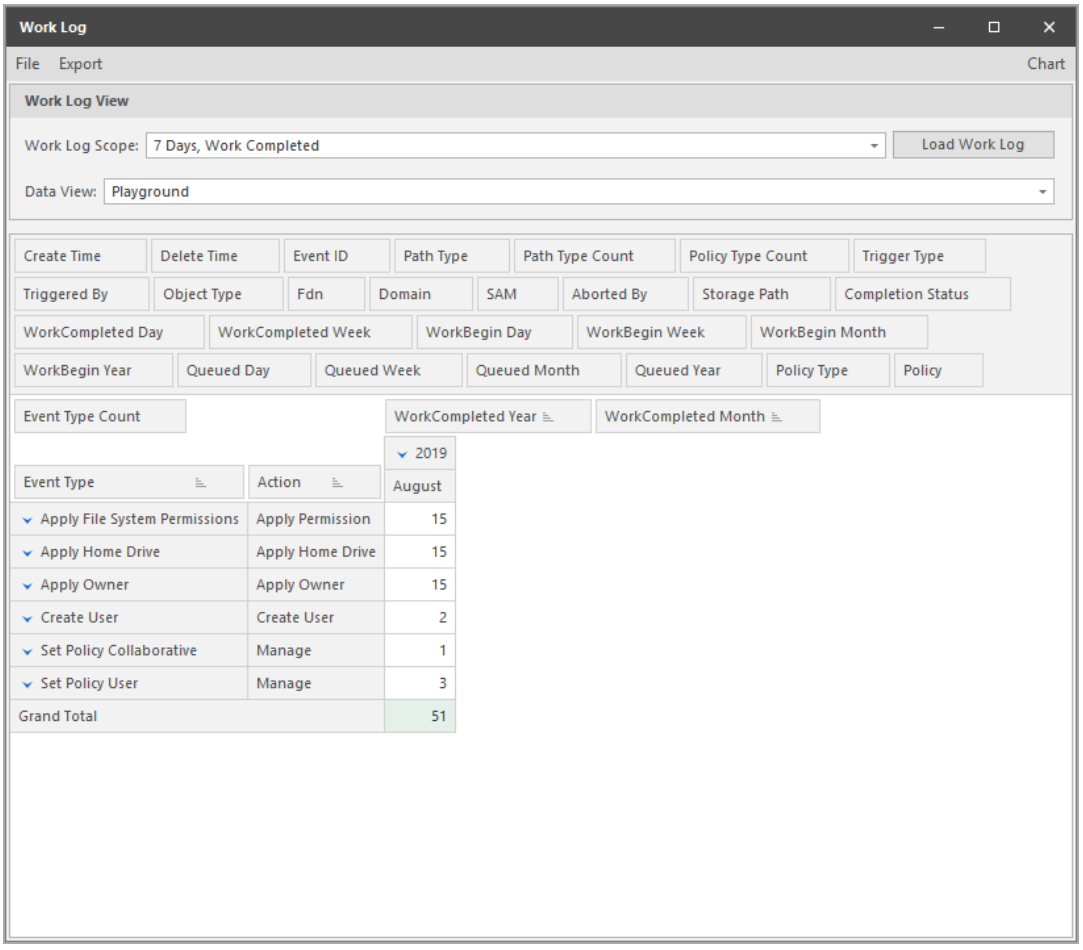
3. Click *OK*.

   The new parameters are specified in the *Work Log Scope* field.

10.3.3 - Data View Options

The Data View drop-down menu has five options:

- **Playground:** This Work Log report option enables you to specify what fields to include in the report. All of the reporting parameters are available for selection in the top portion of the pivot grid. You build the Work Log report by dragging the desired fields where you want them placed in the report. These fields can be displayed as either rows or columns.

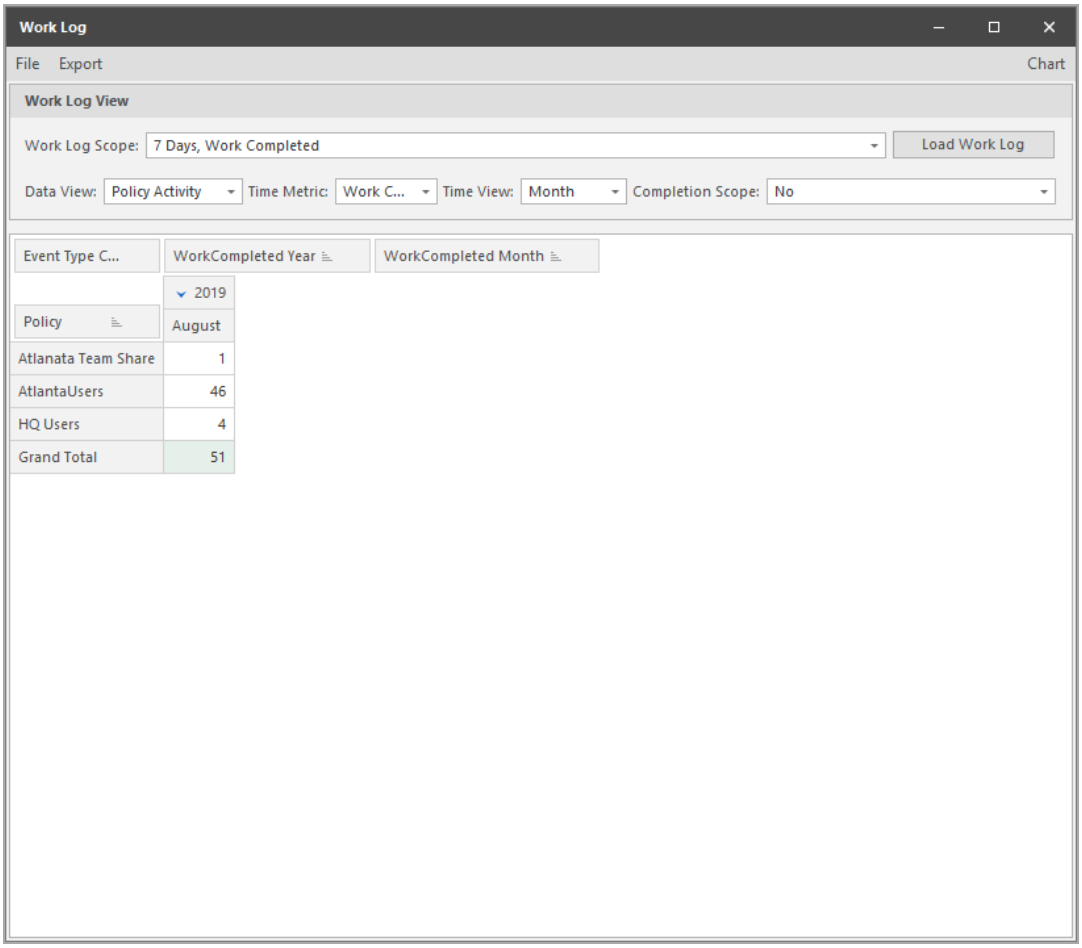


  In any cell with a numeral, you can double-click to access an expanded, detailed report of events.

  You can also click *Chart* to view the data in a graphical format of your choosing.

- **Policy Activity:** This Work Log report option specifies events for all policies regardless of how they were triggered. according to the selected *Time Metric*, *Time View*, and *Completion Scope* options.

In the example below, the Work Log report lists completed File Dynamics events for the Month of May 2018.

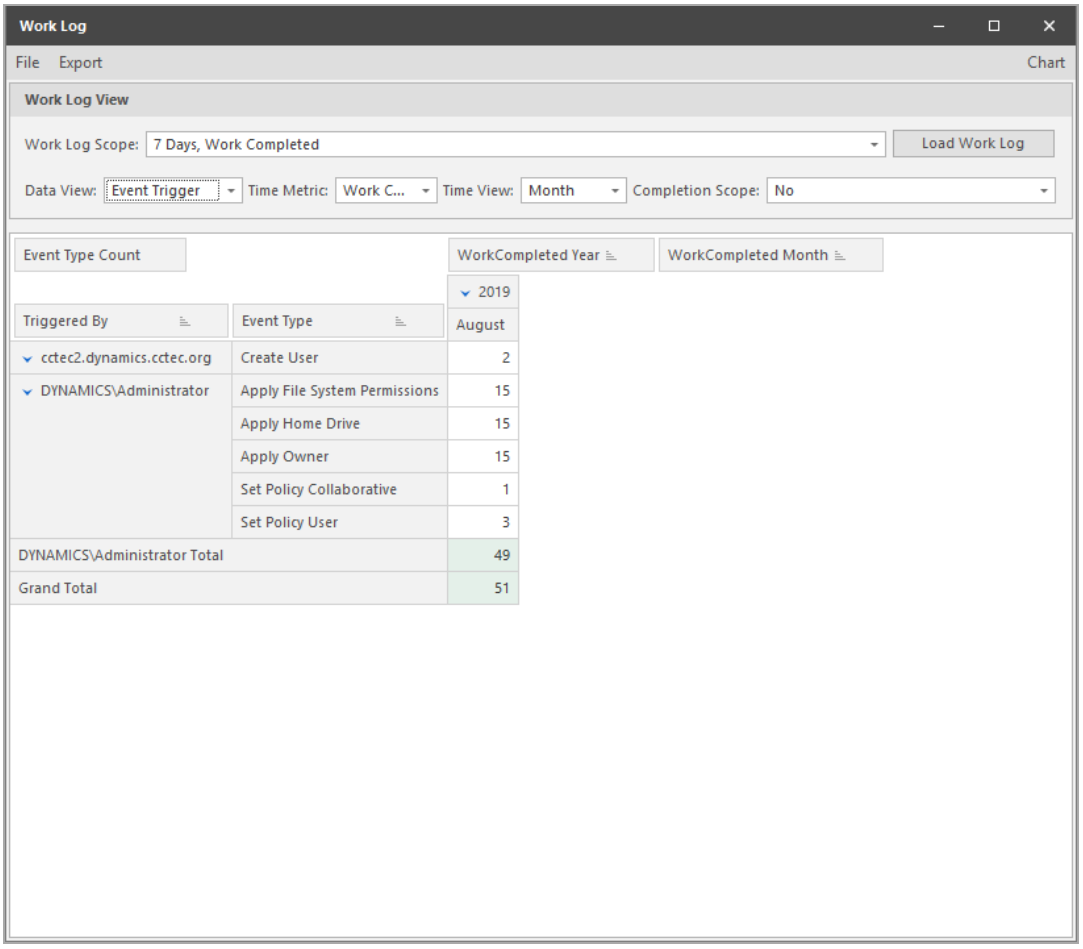


In any cell with a numeral, you can double-click to access an expanded, detailed report of events.

You can also click *Chart* to view the data in a graphical format of your choosing.

- **Event Trigger:** This Work Log report option specifies events generated by an Event Monitor or a File Dynamics administrator performing Management Actions, according to the selected *Time Metric*, *Time View*, and *Completion Scope* options.

In the example below, the Work Log report lists completed Active Directory enacted events for the Month of May 2018.

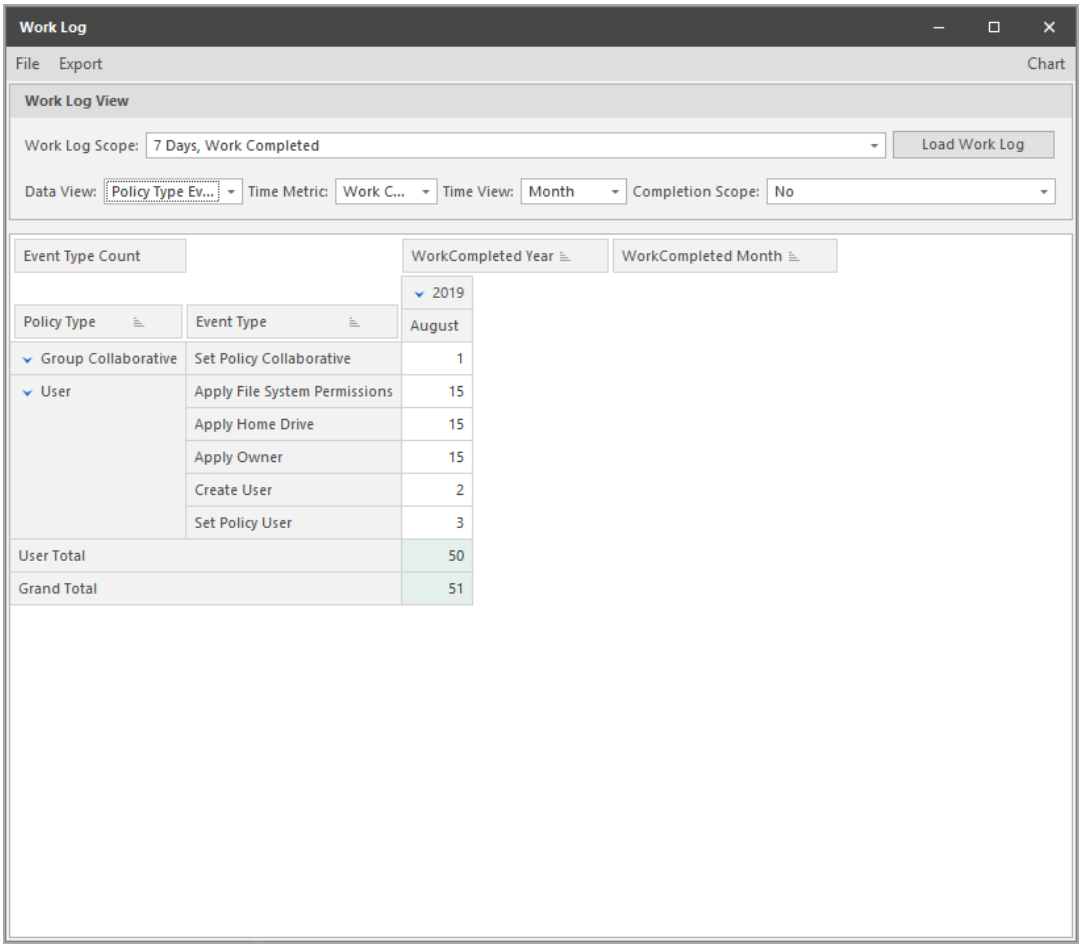


In any cell with a numeral, you can double-click to access an expanded, detailed report of events.

You can also click *Chart* to view the data in a graphical format of your choosing.

- **Policy Type Event Distribution:** This Work Log report option distinguishes events by File Dynamics policy types according to the selected *Time Metric*, *Time View*, and *Completion Scope* options.

In the example below, the Work Log report lists completed events for the Month of May 2018.

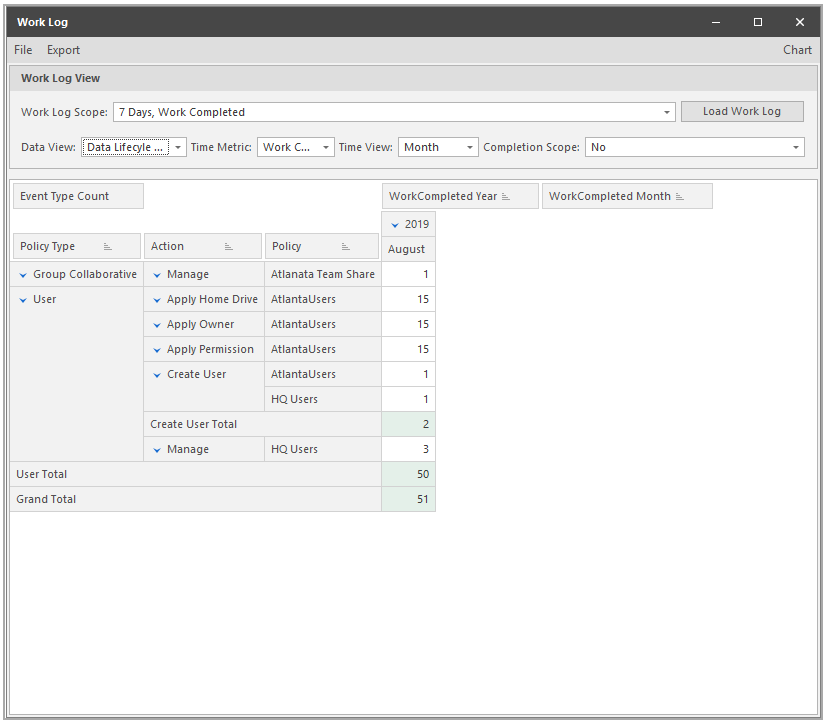


In any cell with a numeral, you can double-click to access an expanded, detailed report of events.

You can also click *Chart* to view the data in a graphical format of your choosing.

- **Data Lifecycle Monthly:** This Work Log report option specifies events by policy type, policy name, action, and month according to the selected *Time Metric*, *Time View*, and *Completion Scope* options.

In the example below, the Work Log report lists completed events for the Month of May 2018.



In any cell with a numeral, you can double-click to access an expanded, detailed report of events.

You can also click *Chart* to view the data in a graphical format of your choosing.

10.3.4 - Build a Work Log Report

1. In the Admin Client, click the *Work Log* tab.
2. Click *Reports*.
3. Click *Load Work Log Entries*.
4. From the *Data View* drop-down menu, select the data view option you want.
5. (Conditional) If you select *Playground*, select and position the fields you want in the report.
6. Select your *Time Metric*, *Time View*, and *Completion Scope* options.

10.3.5 - Saving a View

After you have designed a Work Log report using the *Playground* data view option, you can save it and then use it to again to report on updated event data.

1. In the Admin Client, click the *Work Log* tab.
2. Click *Reports*.

3. Click *Load Work Log Entries*.
4. From the *Data View* drop-down menu, select *Playground*.
5. Select your *Time Metric*, *Time View*, and *Completion Scope* options.
6. Select and position the fields you want in the report.
7. From the *File* menu, select *Save View*.
8. Name and save the view.
   With the view saved, you can retrieve through the *Load View* or *Views* menu options of the *File* menu.

10.3.6 - Exporting a Work Log Report

File Dynamics enables you to export Work Log reports to the following formats:

- CSV
- HTML
- MHT
- PDF
- RTF
- TXT
- XLS
- XLSX

1. In the Admin Client, click the *Work Log* tab.
2. Click *Reports*.
3. Click *Load Work Log Entries*.
4. From the *Data View* drop-down menu, select the data view option you want.
5. (Conditional) If you select *Playground*, select and position the fields you want in the report.
6. Select your *Time Metric*, *Time View*, and *Completion Scope* options.
7. From the *Export* menu, select the format you want.
8. Name and save the exported Work Log report.

11 - Reference

This chapter 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 *Home* tab.

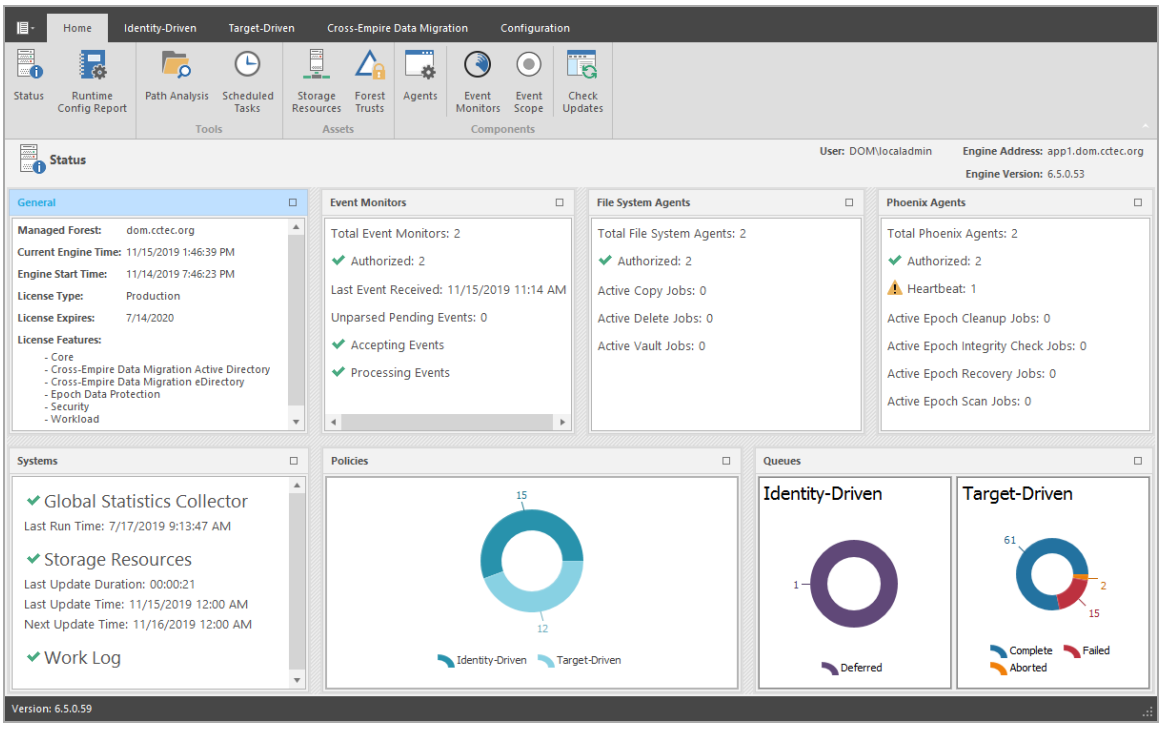
11.1 - Home Tab

The *Home* tab provides a dashboard of File Dynamics component summaries, statistics, access to Engine services settings, and more.

11.1.1 - Status

This displays a dashboard summarizing the status of the product license, the Event Monitor and Agents, if the Work Log is configured, the last time the GSR Collector was run, and graphic summaries of policy and jobs in the queue. You can resize and rearrange the presentation to your preferences.

The Status Page



11.1.2 - Runtime Config Report

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.

Runtime Config Report

11.1.3 - 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 share 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 permissions assigned to individual files.

Whether managed by File Dynamics 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 shares and folders. Use the right pane to view the files within a selected folder.

Clicking a share or folder in the left pane activates the toolbar. The toolbar has the following options:

Information: Lets you view a variety of information pertaining to a selected share or folder.

- **Quota:** Specifies if 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.
- **Permissions:** Opens the View Permissions dialog box, which lists all users and objects that have any type of rights to the selected share, folder, or file. The View Permissions dialog box also indicates the permissions that each of these users and objects have as well as how these rights are obtained.

Tools: Lets you create, rename, and delete folders within the network file system.

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.

File Permissions: This opens a dialog box displaying all the objects that have permissions to a selected folder, the specific permissions, and how those permissions were obtained.

Filter: This lets you filter the view of the subfolders for a specified folder.

11.1.4 - Scheduled Tasks

Use the Scheduled Tasks page to schedule storage resources discoveries and database cleanup tasks as well as schedule Groom policies.

Schedule a Storage Resources Discovery

This task initiates a search within the entire forest domain for any new shares or DFS namespaces. Depending on the size, configuration, and topology of your network, this can take a significant amount of time.

1. In the Admin Client, click the *Engine* tab.
2. Click *Scheduled Tasks*.
3. From the list of scheduled tasks, double-click *Storage Resources Discovery*.
4. In the *Schedule Start* region, set the time and data parameters when you want the storage resources discovery to take place.
5. In the *Schedule Recurrence* region, specify the frequency of the storage resources discovery.
6. Click *OK*.

Run a Storage Resources Discovery

In addition to scheduling a storage resources discovery, you can run the storage resources discovery immediately.

1. In the Admin Client, click the *Engine* tab.
2. Click *Scheduled Tasks*.
3. From the list of scheduled tasks, right-click *Storage Resources Discovery* and select *Run*.
4. Click *Yes* in the confirmation dialog box.

Schedule a Database Cleanup

A database cleanup reduces database bloat that can affect File Dynamics performance. A database cleanup does the following:

- Removes old scan entries
- Removes deleted path history entries
- Removes deleted object entries
- Removes events that are marked as completed
- Cleans up DS objects based on their delete time
- Removes orphaned action blocks

While the database cleanup is in process, event processing is turned off. Once the cleanup finishes, event processing is turned on.

1. In the Admin Client, click the *Engine* tab.
2. Click *Scheduled Tasks*.
3. From the list of scheduled tasks, double-click *Database Cleanup*.
4. In the *Schedule Start* region, set the time and data parameters when you want the database cleanup to take place.
5. In the *Schedule Recurrence* region, specify the frequency of the database cleanup.
6. Click *OK*.

Run a Database Cleanup

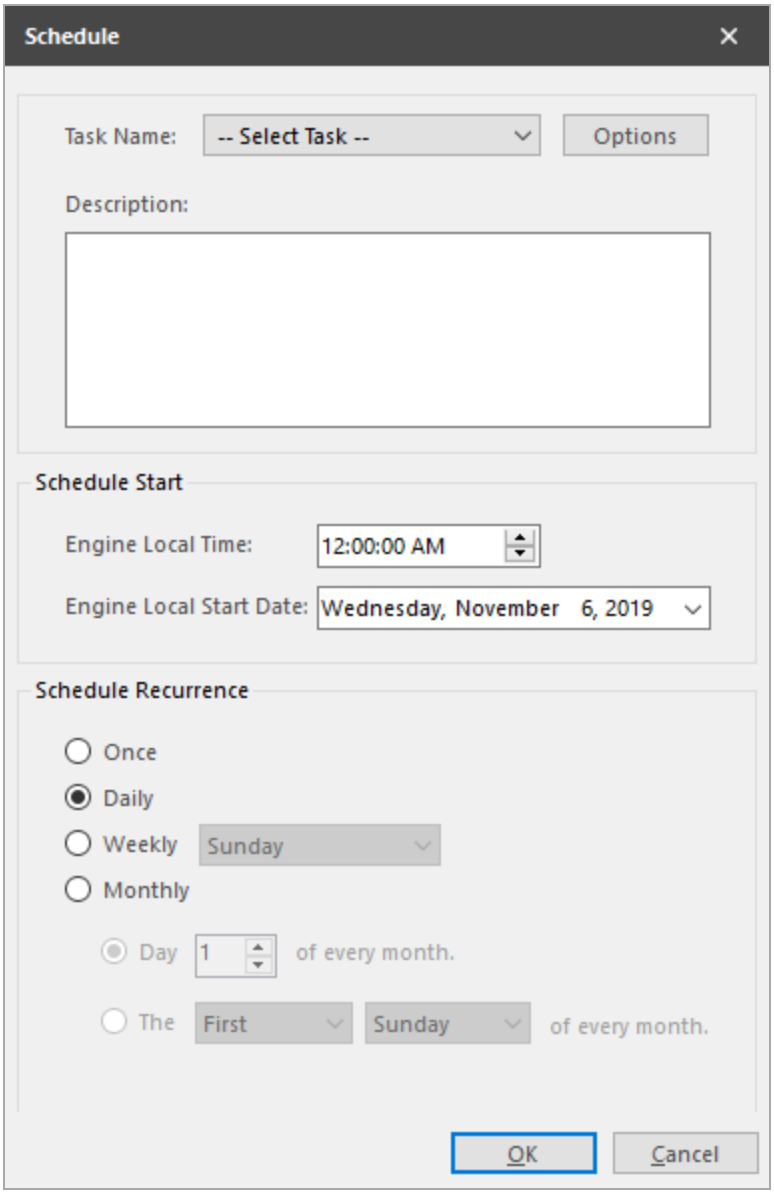
In addition to scheduling a database cleanup, you can run a database cleanup immediately.

1. In the Admin Client, click the *Engine* tab.
2. Click *Scheduled Tasks*.
3. From the list of scheduled tasks, right-click *Database Cleanup* and select *Run*.
4. Click *Yes* in the confirmation dialog box.

Schedule a Groom Policy

1. In the Admin Client, click the *Engine* tab.
2. Click *Scheduled Tasks*.

3. Click *Add*.



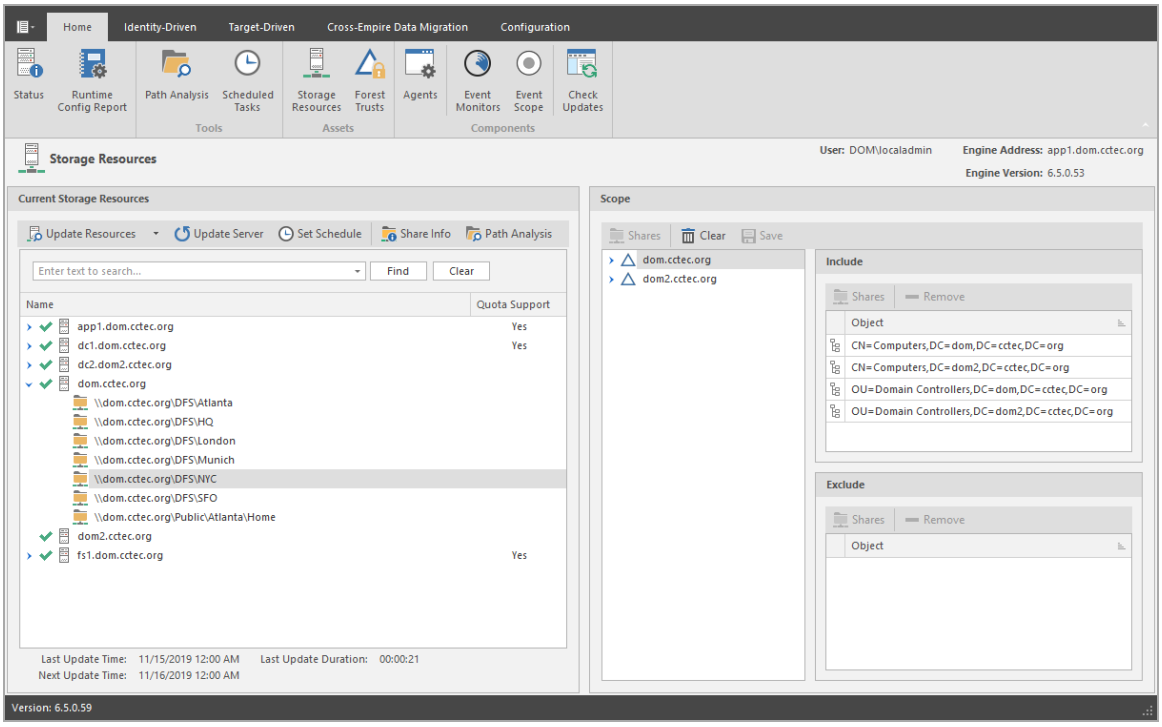
4. From the *Task Name* drop-down menu, select *Policy-based Groom*.
5. Click *Options* to access the Take Action dialog box.
6. Enter the settings in the dialog box and click *OK*.
7. In the *Description* field, enter a description of the scheduled groom.
8. In the *Schedule Start* region, set the time and data parameters when you want the scheduled groom to take place.
9. In the *Schedule Recurrence* region, specify the frequency of the scheduled groom.
10. Click *OK*.

11.1.5 - Storage Resources

This page lets you rebuild the storage resource cache used in File Dynamics. Because File Dynamics 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 shares.

To prevent burdening the File Dynamics Engine in listing or rebuilding all storage devices and shares in the Active Directory forest or domain, you can "scope" the containers of the forest or domain for storage devices and shares to be included or excluded as managed storage resources.

Storage Resources Page



Current Storage Resources: This region displays storage resources while providing tools for performing actions pertaining to these storage resources.

Update Resources: Clicking this button initiates a search within the specified scope for all available shares or DFS namespaces. When you create or edit a policy, you might need to rebuild the list if the share or DFS namespace 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.

Clear Resources: Available from the *Update Resources* drop-down menu, this option clears the current storage resource list so that it can be completely rebuilt when issues arise.

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

Share Info: Selecting a share and then clicking this button opens the Server Share Properties dialog box which displays the permissions and Local Security Authority (LSA) settings for the share.

Share Info requires elevated privileges.

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

Scope: This region lets you specify the scope within Active Directory and the network file system of the containers and servers to include and exclude. Based on the specified scope, the available shares will be displayed in the *Storage Resource* list.

Shares: When you expand a container object and select a server, you can click *Shares* to view details about the shares located on that server. Clicking *Shares* opens the Server Shares Properties dialog box where you can view the permissions and Local Security Authority (LSA) settings for each share.

Clear: Clicking this removes any object located in the *Include* and *Exclude* lists.

Save: Saves the scope settings.

Remove: Removes objects located in the corresponding Include or *Exclude* lists.

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

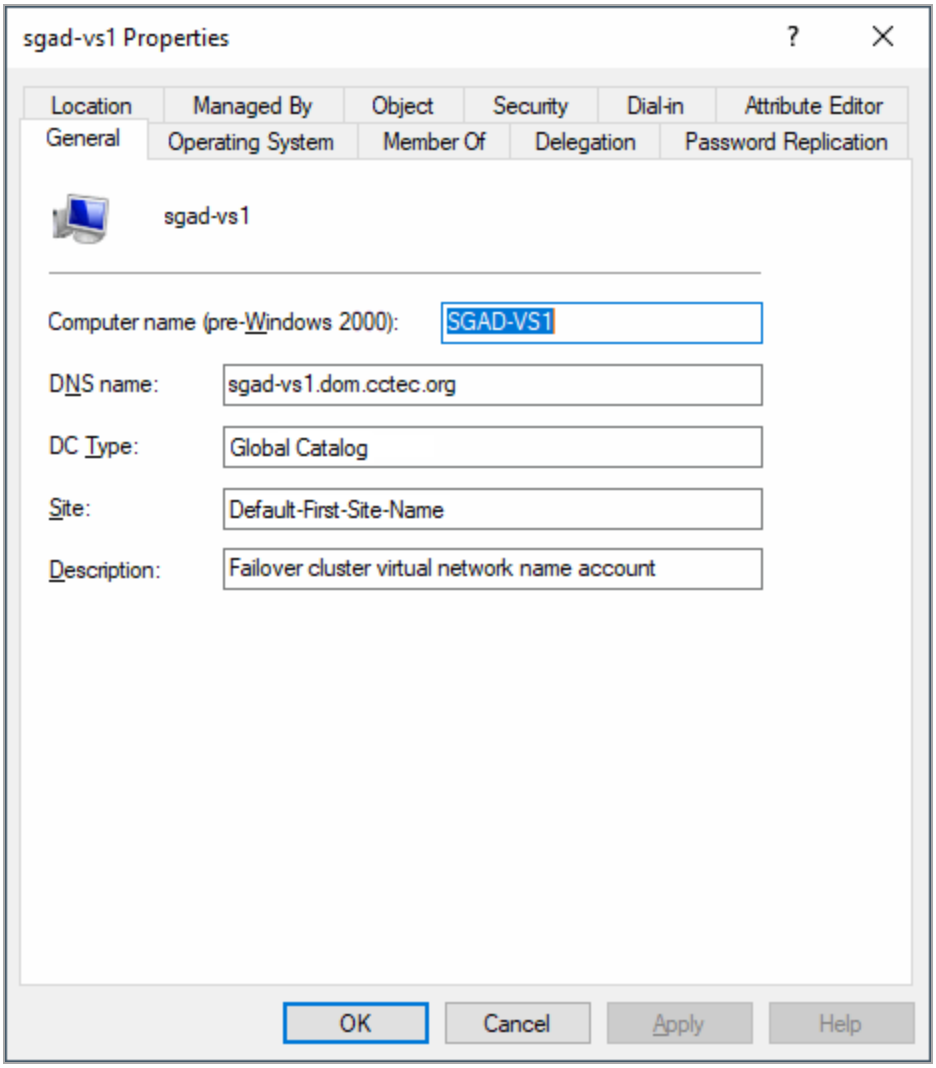
Last Rebuild Duration: Displays the length of time it took to generate the new storage resource list.

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

Displaying Windows Server Clusters

If a Windows Cluster File Server Resource is not displayed in the Storage Resource List, verify that the *Description* field of the cluster file server resource includes the words `cluster` and `virtual`. If these two words are not included in the description, File Dynamics cannot see it

as a storage resource.



Once you modify the description in the *Description* field, you can perform a storage resources discovery from the Scheduled Tasks page to add the resource to the Storage Resource List. For more information, see *Run a Storage Resources Discovery (page 157)*.

11.1.6 - Forest Trusts

Forest trust relationships provide security across multiple Active Directory forests. Before you can authenticate across trusts and migrate folders from one forest to another, Windows must first establish a trust path between the forests.

Forest Trusts Overview

File Dynamics has limited support for forest trusts for Target-Driven content control policies (Copy, Move, and Vault policies) and for managing storage resources in another forest. The trust cannot be leveraged to monitor for events in another forest.

After a forest trust is configured for use, you will need to grant the proxy account appropriates rights and permissions to shares on servers in the trusting forest. This is the same process used for granting access to servers where Agents have not been deployed in the primary forest. See Setting Rights and Privileges on Managed Storage in the *File Dynamics 24.2 Installation Guide* for details.

Supported Trust Models

Active Directory provides a number of configurations for forest trusts. File Dynamics currently supports only forest-wide *one-way incoming* and *two-way* forest trust models.

Trust Type	Direction	Scope of Authentication	Supported
External	One-way or two-way	Selective or Forest-wide	No
Forest	One-way or two-way	Selective	No
Forest	One-way incoming or two-way	Forest-wide	Yes
Shortcut	One-way or two-way	Selective	No

11.1.7 - Agents

File System Agents perform copying, moving, grooming, and vaulting. Phoenix Agents conduct scans and enforcement forTarget-Driven Security Policies and Workload Policies. All Agents tasks are done through directives from the Engine. File Dynamics determines which Agent to use based on the task, as well as the target destination of the data or via proxy configuration.

For optimum performance, File System Agents should be installed on all servers with storage managed by File Dynamics. Agents run as a service on Windows.

The Agent 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

The Agent page also indicates:

- Whether the Agent is capable of being utilized in an eDirectory-to-Active Directory Cross-Empire Data Migration
- Whether the Agent is functioning as a Proxy Agent and for which server and share

Procedures for authorizing an Agent are located in Authorizing the Agents in the *File Dynamics 24.2 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.

If an Agent is deauthorized and it hasn't successfully sent a heartbeat within 7 days, it will automatically be removed

Configuring Proxy Agents

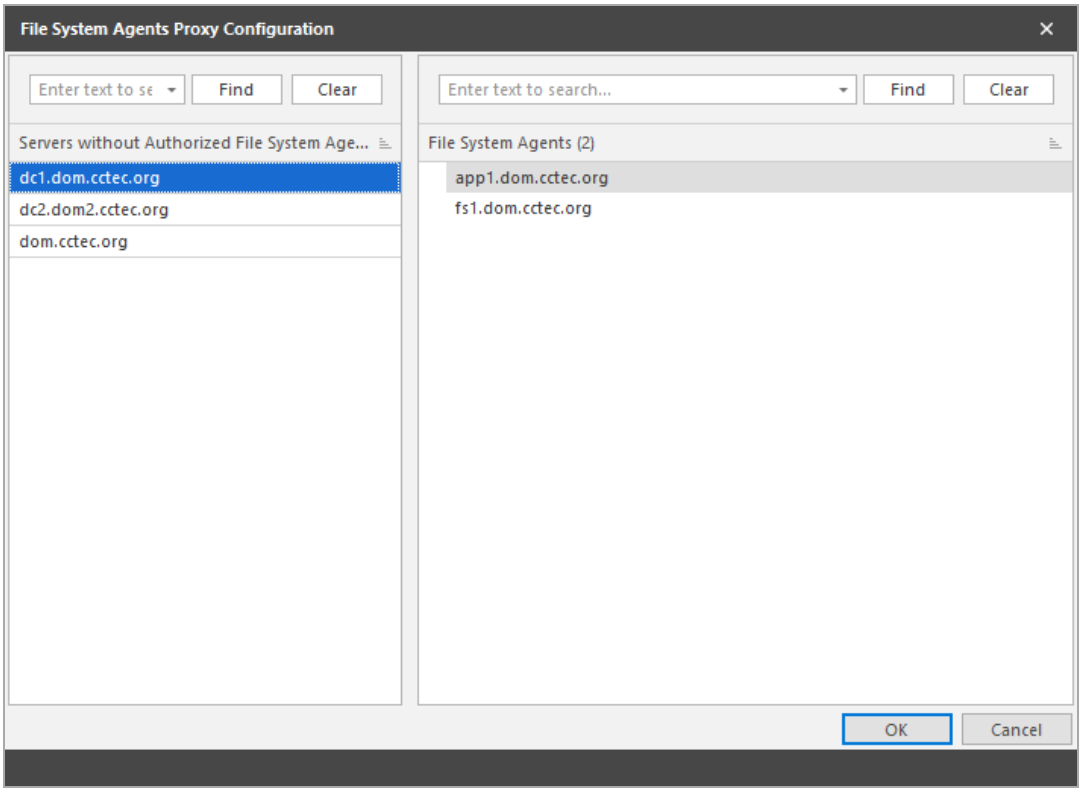
For storage resources that do not or cannot host an Agent, for example a NAS (Network Attached Storage) device, File Dynamics can utilize an Agent running on another server to perform the copying, moving, grooming, and vaulting on the server or NAS device. In this type of scenario, the Agent is serving as a “Proxy Agent.” Both File System Agents and Phoenix Agents can serve as Proxy Agents.

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.

To configure a proxy agent:

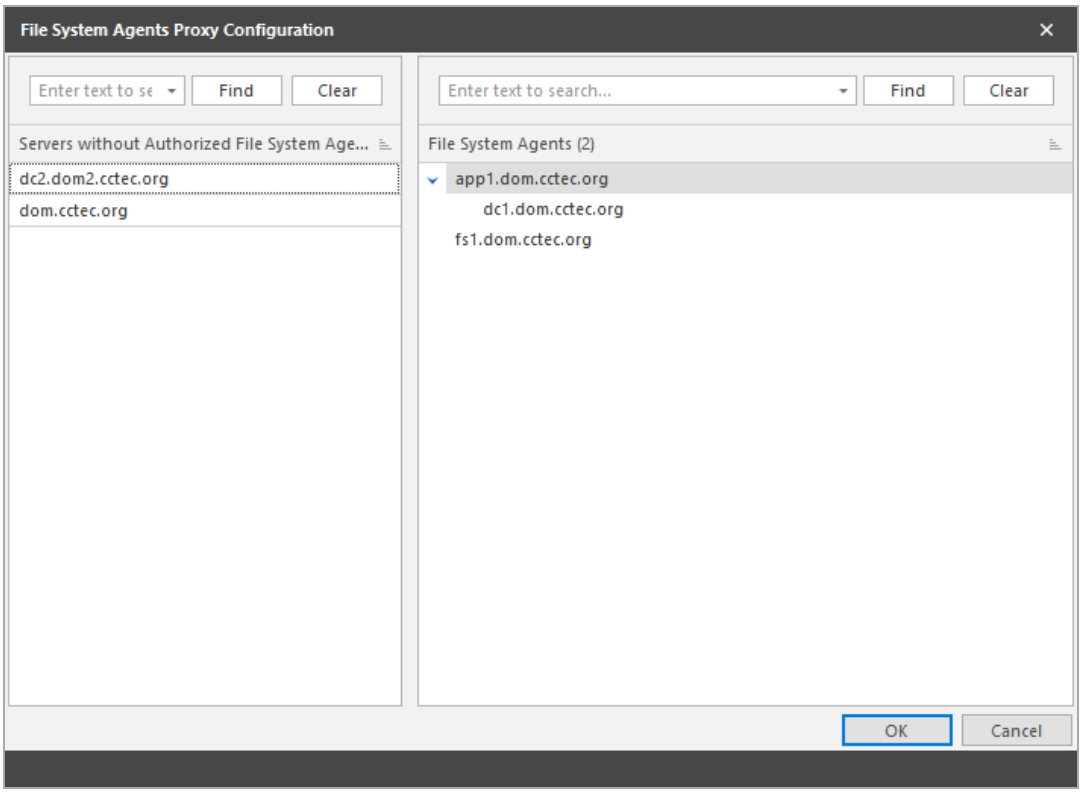
1. In the Admin Client, click the *Engine* tab.
2. Click *Agents*.

3. From the *Configure Proxies* drop-down menu, select the Agent type you will be configuring.



The left pane displays all servers without an authorized Agent. The right displays servers hosting Agents, and consequently, can serve as Proxy Agents

4. From the left pane, select and drag a listed server to one on the right pane that you want to serve as a Proxy Agent.



5.
6. Click *OK* to save the Proxy Agent assignments.
7. Click *OK* to save and close the proxy setting association.

11.1.8 - Event Monitors

The Event Monitor monitors changes to Active Directory based on create, move, rename, and delete events.

You install one Event Monitor per domain, and it can run on a domain controller or a member server. If you install the Event Monitor on a domain controller, the Event Monitor always monitors the local server for changes in the domain. If you install the Event Monitor on a member server, the Event Monitor identifies the closest available domain controller and monitors it for changes in the domain. The Event Monitor runs as a service on Windows.

In the Event Monitors page, you can:

- 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 under Authorizing the Event Monitor in the *File Dynamics 24.2 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.

11.1.9 - Event Scope

Rather than burdening the Event Monitor in observing all events in the Active Directory forest or domain, this feature lets you "scope" the segments of the forest or domain that the Event Monitor will monitor. A scoped segment of the forest or domain might include specific containers or groups.

For procedures on how to use this feature, see *Event Monitor Scoping (page 7)*. For a complete discussion of the Scope feature, including Include and Exclude behaviors, see .

11.1.10 - Check Updates

This page compares the version numbers of File Dynamics components that you have installed with the latest versions available. It also provides links for downloading the latest versions of each of the components.

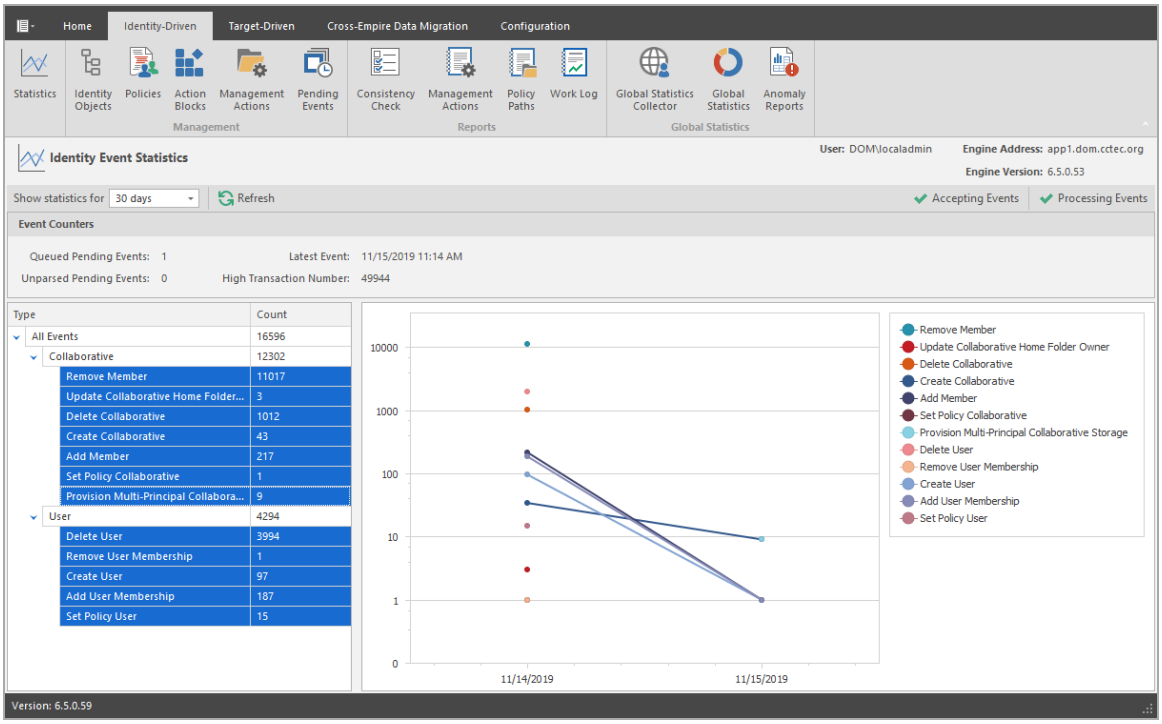
11.2 - Identity-Driven Tab

The Identity Driven tab provides access to tools for creating and managing Identity-Driven policies in File Dynamics.

11.2.1 - Statistics

This page charts graphical statistics for all Identity-Driven actions taken over a specific period of time.

Statistics Page

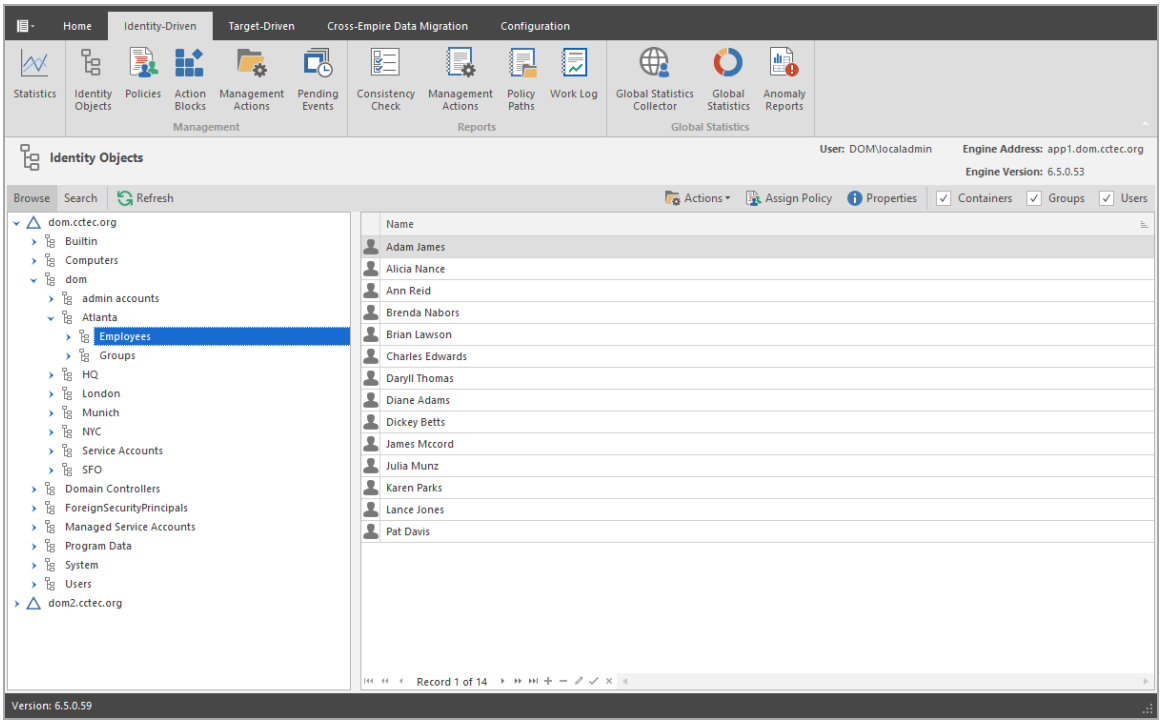


By default, all actions indicated in the legend will appear on the chart. To make the chart less busy, you can remove categories by holding the Control key and in the left pane, deselecting categories.

11.2.2 - Identity Objects

The Identity Objects page lets you manage the associations between File Dynamics Identity-Driven policies and Active Directory objects such as organizational units, groups and users. This management includes creating organizational units, setting context, viewing properties, performing Management Actions, and assigning policies.

Identity Objects



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

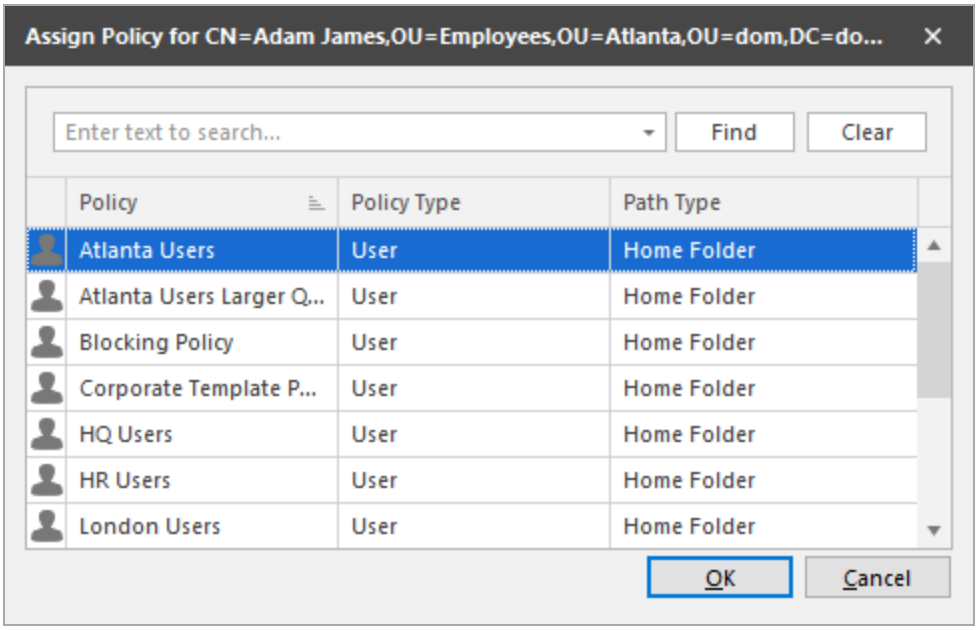
Use the right pane to view the objects within a selected organizational unit as well as view properties, perform Management Actions, and assign policies. The right pane displays containers (organizational units), groups, and users, according to what you have selected in the *Filter* check boxes.

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

Assign Policy

Right-clicking a User, Group, or Organizational Unit object and selecting *Assign Policy* lets you easily assign any of these objects a policy while you are in the 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.

Policy Selector Dialog Box



Properties

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

The five tabs display the following information:

Properties: Displays Active Directory values and Engine database values.

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 domain, 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 domain, 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: The GSR Collector maintains multiple histories for an object in Active Directory.

The FDN History records the FDN and SAM Account name of an object, when applicable (e.g. organization unit objects do not have a sAMAccount attribute). When an object gets renamed or moved, on the next run, it will catalog the new location or new name and the corresponding timestamp when the change was recorded.

The Path History records the location of paths that are commonly associated to users. When the Active Directory schema is extended to support user auxiliary storage and collaborative storage, the managed path attributes for user auxiliary, groups, and containers can be

cataloged as well. The Path History consists of path types that are managed by File Dynamics. The possible recorded path types are:

- User Home folder
- User Profile path
- User Remote Desktop Services Home Folder
- User Remote Desktop Services Profile Path
- User Auxiliary (ccx-FSFAuxiliaryStorage)
- Collaborative – Groups (ccx-FSFManagedPath)
- Collaborative – Container (ccx-FSFManagedPath)

The granularity of the historical data is only as fine as the frequency at which you schedule the GSR Collector to run. For more information, see *Global Statistics Collector (page 200)*.

If you schedule it to run once a week and you have objects that move several times over the course of a week between the runs, you'll lose the interim historical move data.

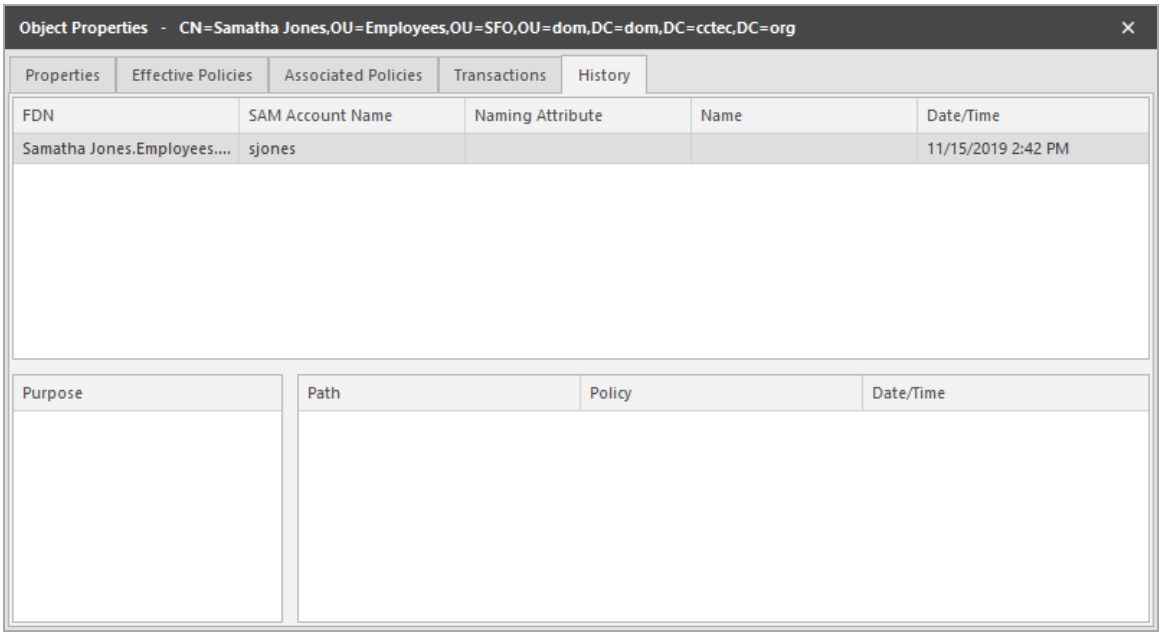
The GSR Collector's historical data can be especially useful when managed paths are moved based on policy.

To view the history of an object, from the 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.

The example below shows an unmanaged user without a cataloged path.

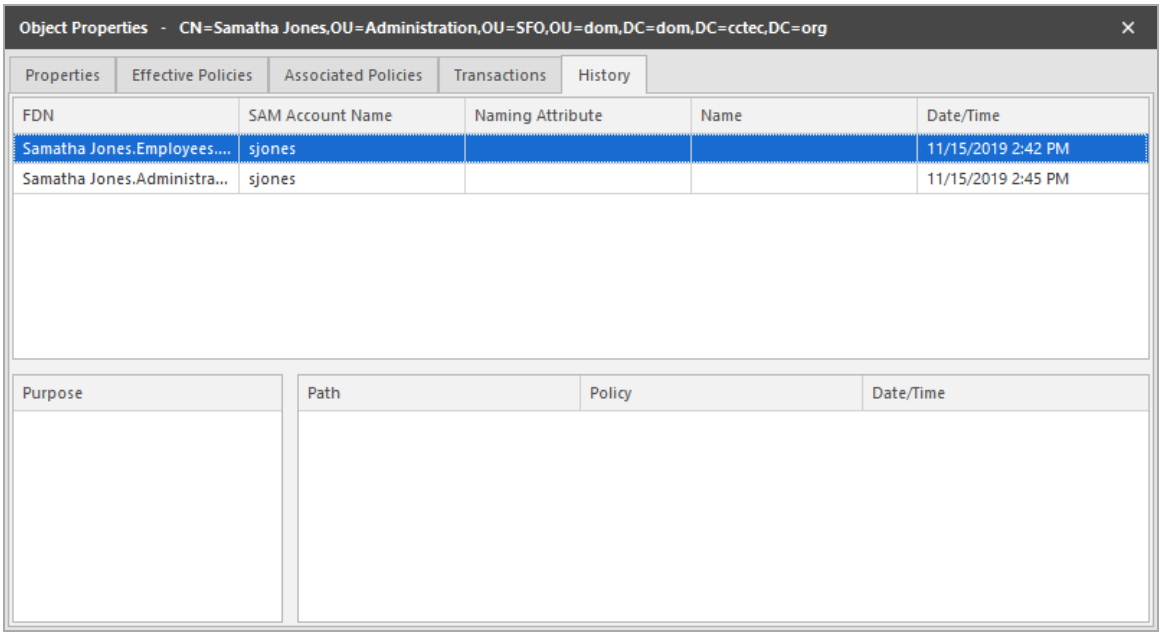
Example of an Unmanaged User without a Cataloged Path



The *FDN* column is the LDAP formatted location of the object. The *SAM Account Name* column is the sAMAccount attribute value. The *Date/Time* column is based on the local time of the Engine when the history record was cataloged.

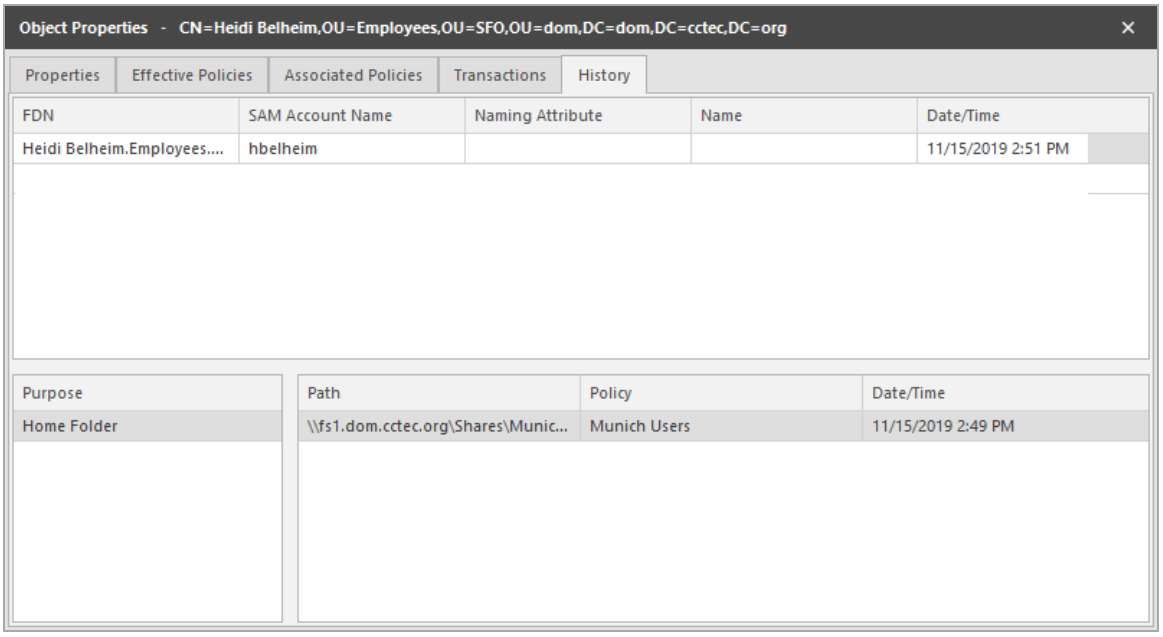
The example below shows the same unmanaged user that was moved from one organizational unit to another. This example demonstrates a change in the FDN and the date when the new value was cataloged by the GSR Collector when it was run.

Example of a Moved Unmanaged User



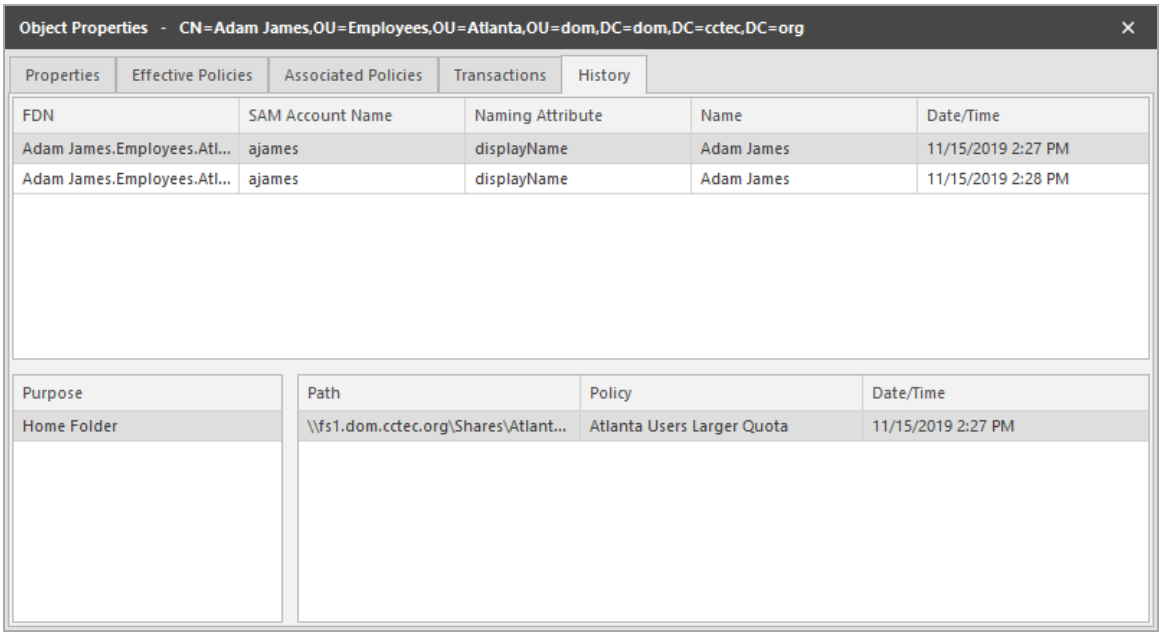
The example below shows an unmanaged user that has a home folder. The *Policy* column is empty because this user has not been managed. The *Date/Time* column for the path indicates the time at which the GSR Collector recorded the path.

Example of an Unmanaged User with a Home Folder



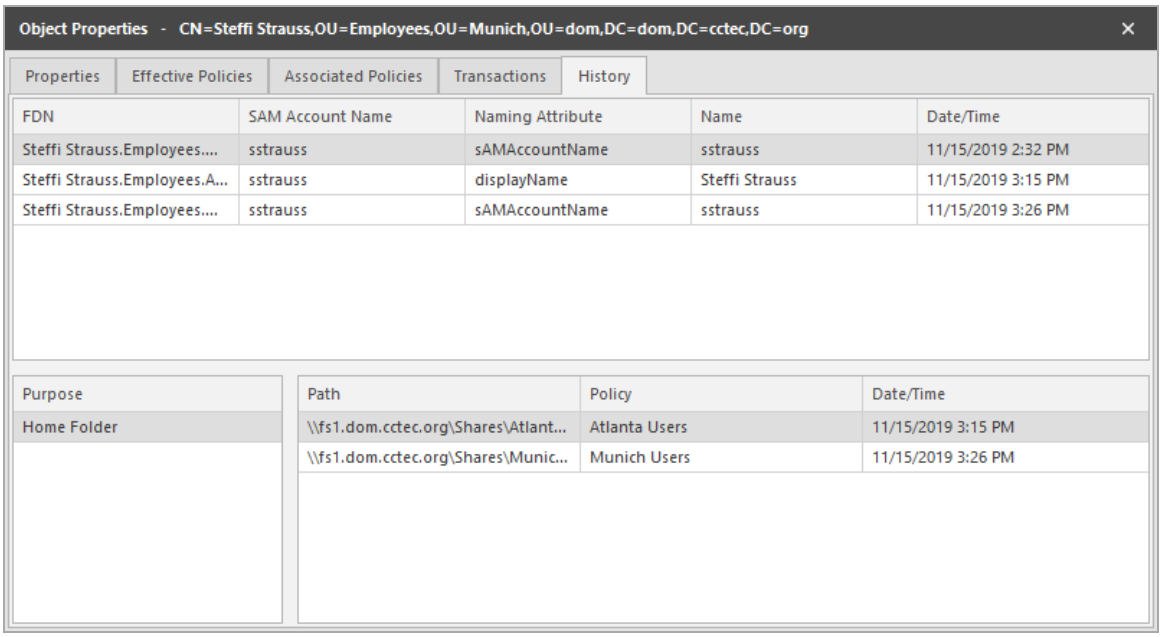
The example below shows the same user that has now been managed. The path now contains two entries. The first path reflects when the user was originally cataloged. The second path reflects that the user is now managed and the policy that is managing it. This is useful because the *Date/Time* for *Policy* "History" indicates when the object became managed.

Example of a Managed User



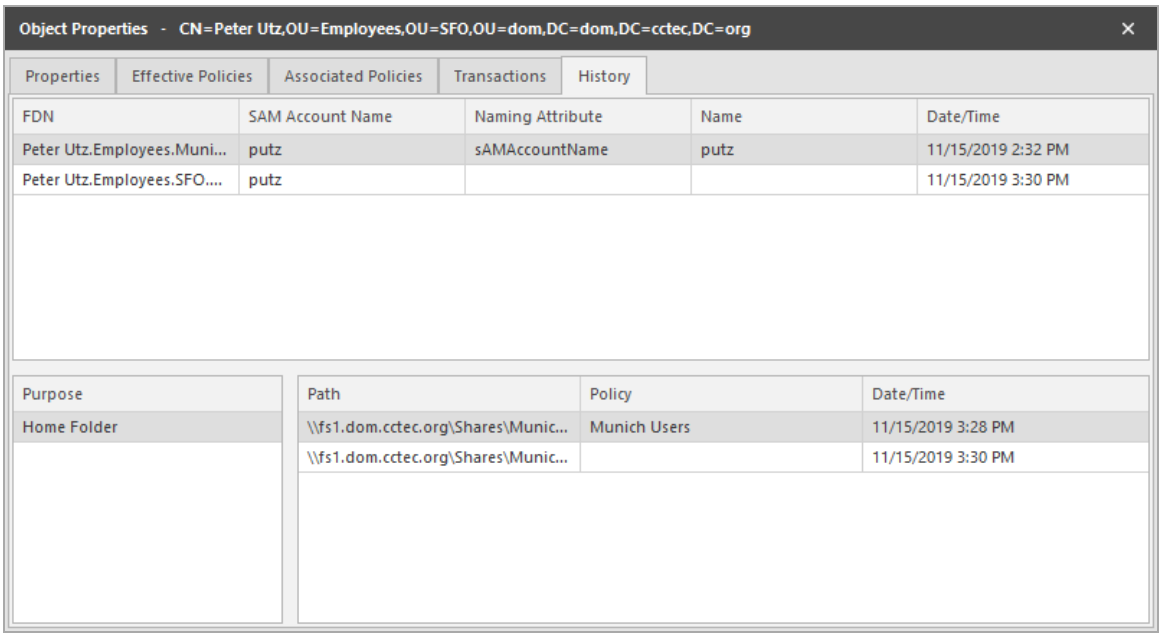
The example below shows the same user has now been moved from one container to another that is managed by a different policy. The user's new FDN has been recorded as well as the new location of the path.

Example of a Moved Managed User



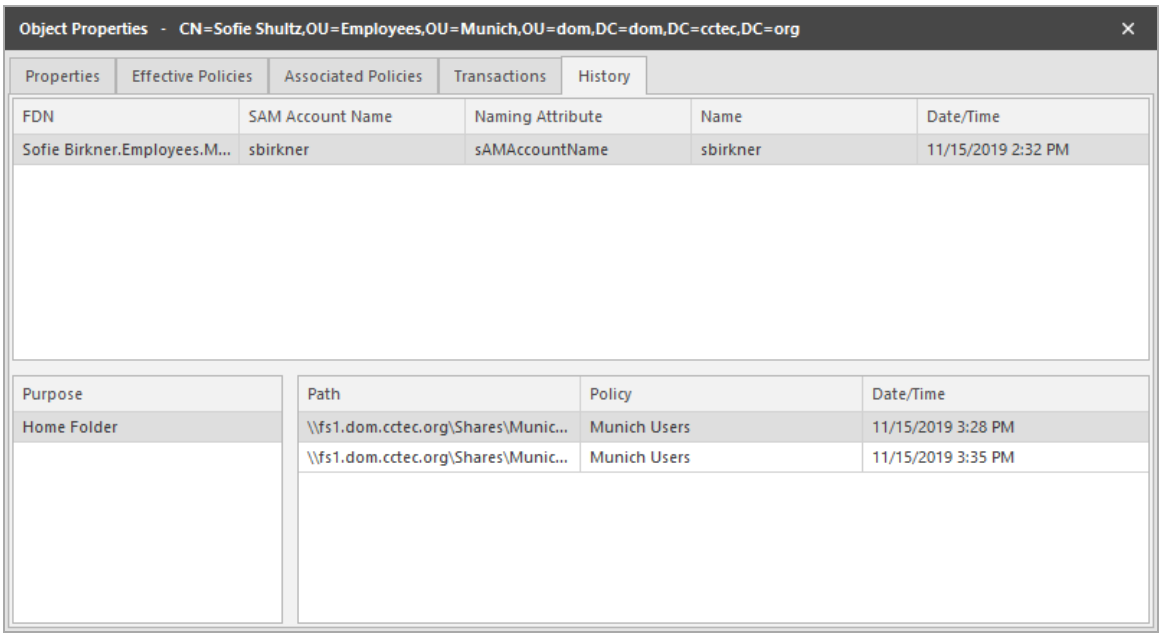
The example below shows the same user has now been moved to a container that is not managed by policy. The *Policy* column now shows that the path is no longer managed by an effective policy.

Example of a Moved User to a Container Not Managed by a Policy



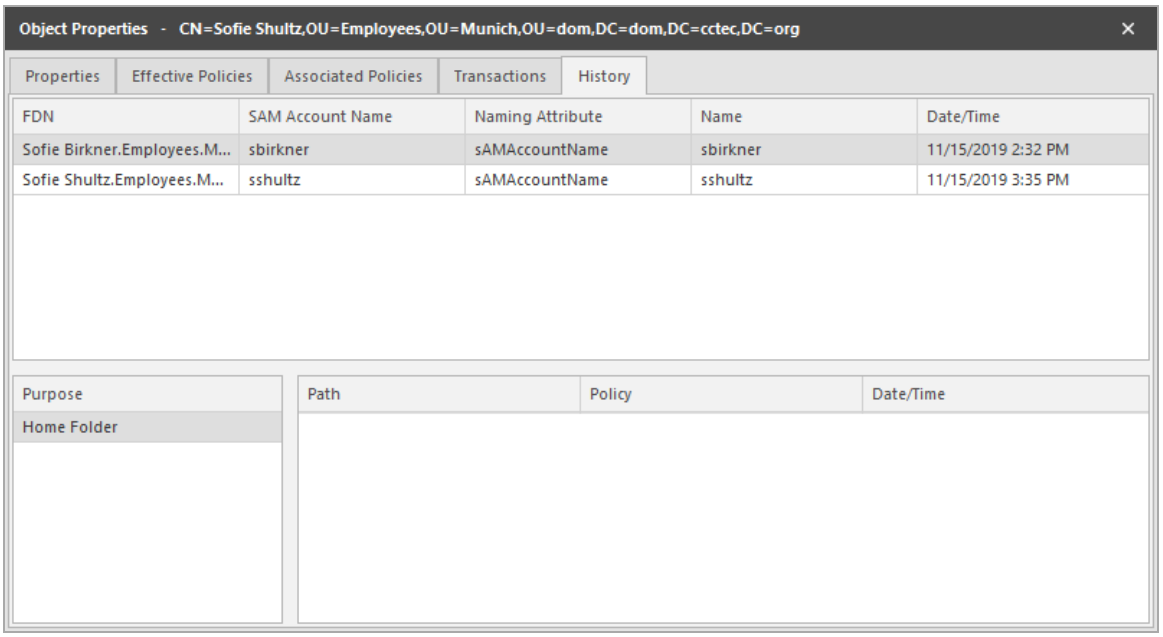
The History data also tracks the rename of objects and the relevant paths. The example below shows a managed user before it has been renamed.

Example of a Managed User Before Being Renamed



The example below shows the new *FDN*, *SAM Account Name*, and *Path* after having been renamed.

Example of a Managed User After Being Renamed



11.2.3 - Policies

The Policies 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.

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
- User Profile Path
- User Remote Desktop Services Home Folder
- User Remote Desktop Services Profile Path
- Group Multi-Principal Collaborative
- Group Collaborative
- Container Collaborative
- Auxiliary

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

Rename: Lets you rename the selected policy.

Delete: Lets you delete the selected policy.

Auxiliary Purpose Mappings: Selecting this brings up the Auxiliary Purpose Mappings page, where you can establish or edit 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 folder assigned the same purpose, it makes it possible for File Dynamics 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. For procedures on establishing Auxiliary Purpose Mappings, see *Establishing Auxiliary Purpose Mappings (page 56)*.

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

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

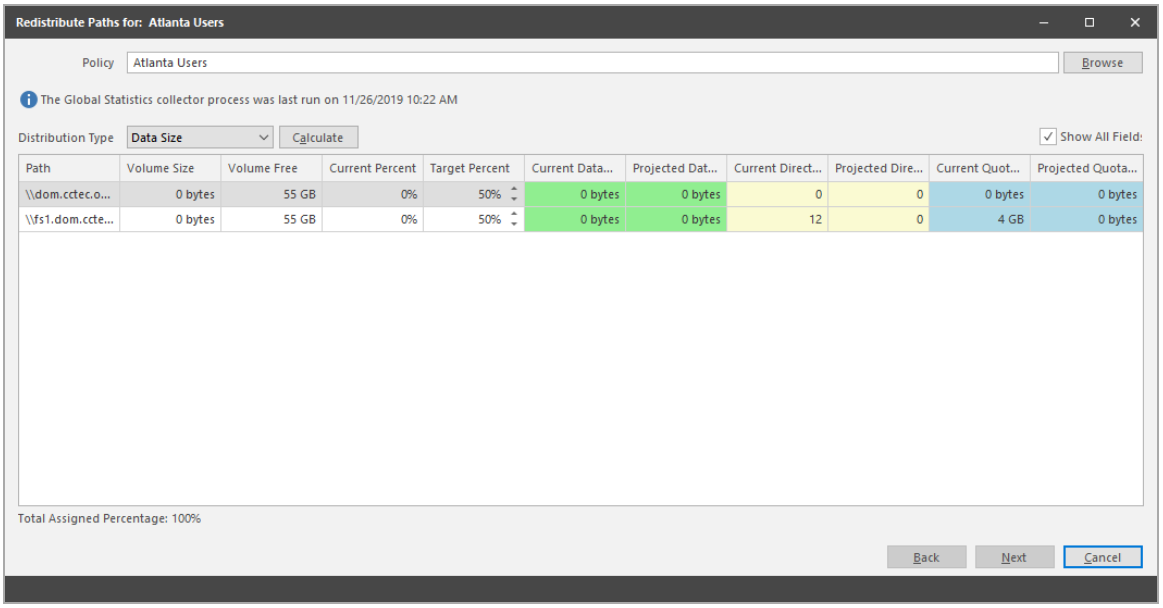
For more information on importing policies, see *Importing Policies (page 58)*.

Export: Provides the ability to export policies so that they can be imported later. For example, many customers first evaluate File Dynamics 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. For more information, see *Exporting Policies (page 57)*.

Actions: 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*.

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

Redistribute Policy Paths Dialog Box



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

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 File Dynamics 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.

Search: Provides a search field for locating policies.

Refresh: Refreshes the list of policies.

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

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

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

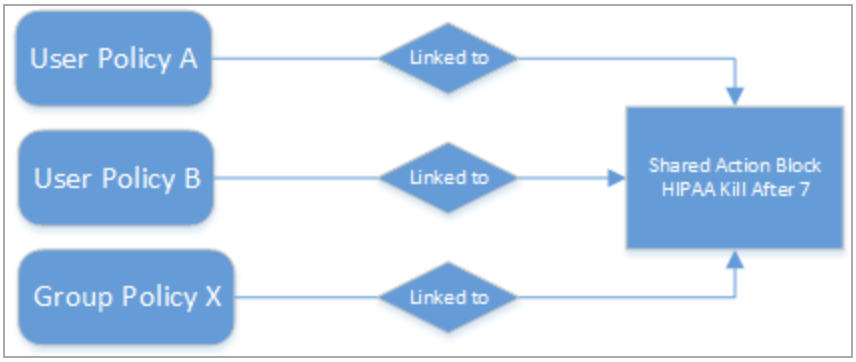
11.2.4 - Action Blocks

This page lets you create Action Blocks that can be linked to a policy.

Action Block Overview

Action Blocks allow the sharing of specific policy options between multiple policies. The design goal behind Action Blocks is to provide a framework where the sharing of options between policies can be achieved in a straightforward and easy to understand manner.

Action Block Overview



Action Blocks do not introduce a new policy type. Rather, they are extensions of policies in that the set of options they represent are not contained within the policy itself. This eliminates the need for policies to inherit from each other and promotes the sharing of general and often-repeated policy options such as groom and vault rules. Existing User, Group, and Collaborative policy types remain as they previously did with the exception that they have been extended to support a relationship value providing the necessary link for a given Action Block.

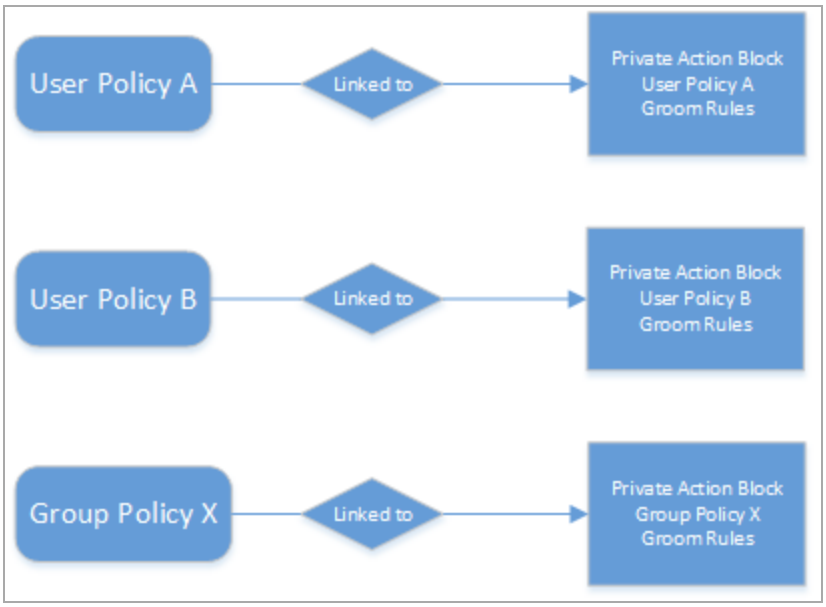
An Action Block can have a many-to-one relationship. This means that any number of policies can share any particular Action Block for a given policy option. Action Block inheritance cannot be chained. That is to say, “Policy A” cannot inherit the Filter rules from “Groom Block A” and “Groom Block B”. “Policy A” can only be to linked to one of the two Action Blocks and they do not inherit from each other. When changes are made to an Action Block, those changes are implicitly taken up by every linked policy. Thus, before making changes to an Action Block, it is important to understand the impact of those changes. As with normal event processing and policy editing, if a change is made to an Action Block while an event is in-flight for its given options, those changes may not be reflected in the outcome of the event.

Private Versus Shared

Regardless of an Action Block's type, it is either Private or Shared.

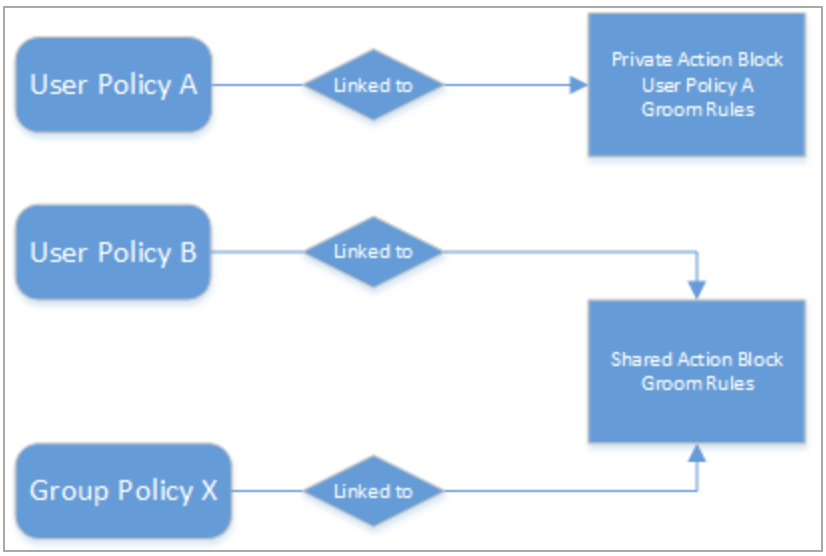
A Private Action Block represents a set of policy options that aren't shared, yet have been migrated to the Action Block architecture. Private Action Blocks are also created and associated to a policy when the policy is upgraded as new Action Block types are supported. Below is an example of the relationships between policies and their Private Action Blocks for Filters. Any of these might be the result of creating a new policy with Groom Rules or an upgrade from the legacy policy architecture.

Relationships Between Policies and their Private Action Blocks for Filters



When you create an Action Block, it is automatically marked as Shared and is available for being shared with other policies. However, if you edit a policy that does not derive a particular policy option from an Action Block, a Private Action Block is created and associated to the policy when the policy is saved. If you change a policy that has a Private Action Block to use a Shared Action Block, the policy's Action Block reference is updated to that of the Shared Action Block and the Private Action Block is deleted.

Shared and Private Action Block Associations

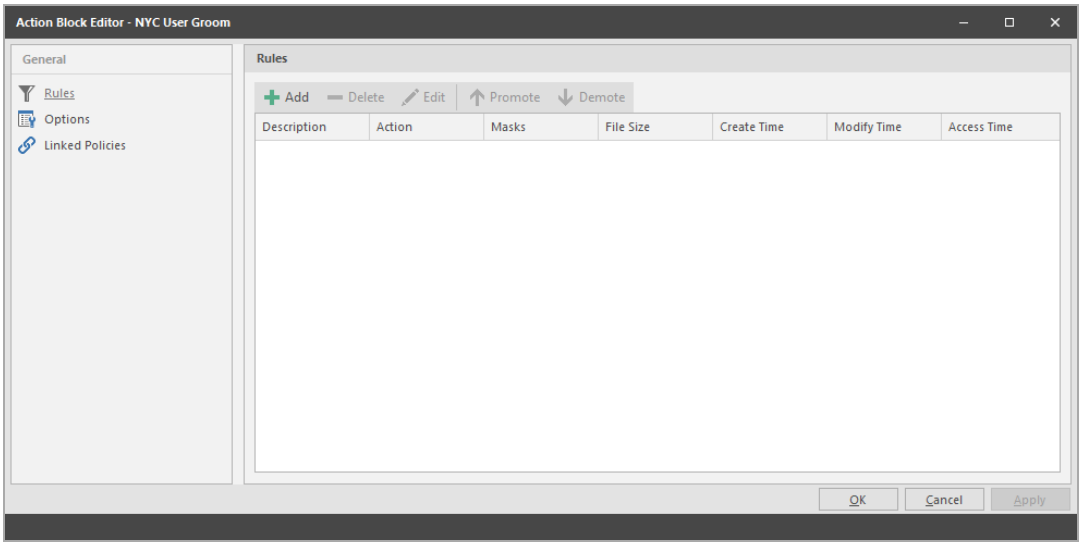


By default, a Private Action Block is not viewable in the list of Shared Action Blocks.

Creating a Filter Action Block

1. In the Admin Client, click the *Identity Driven* tab.
2. Click *Action Blocks*.
3. Select *Manage > New> Filter*.
4. In the *Name* field, give the new Action Block a name and click *OK*.

   The following dialog box appears:



Rules: Rules are composed of the standard File Dynamics rule options. Rules cans be added, deleted, edited, promoted, and demoted. Once a Filter Action Block is saved, those settings will be effective immediately.

Options: The *Description* option can be used to provide detailed context for the usage and implementation of the Filter Action Block.

Linked Policies: Linked Policies is a read-only view of which policies are linked to the Filter Action Block.

5. Click *Add*.
6. In the Rule Editor, specify the parameters for the Action Block Filter and click *OK*.

   For procedures on entering settings in the Rule Editor, see *Setting Vault Rules (page 41)*.
7. Click *OK* to close the Action Block Editor dialog box.

Linking Filter Action Blocks

Filter Action Blocks can be linked to the following:

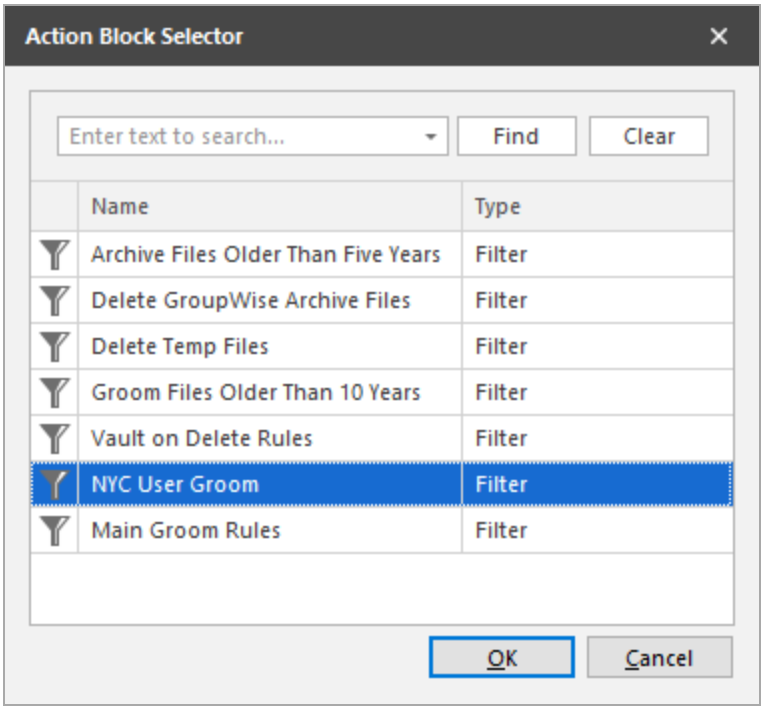
- Policy-based Vault
- Policy-based Groom

Linking a Filter Action Block to a Policy

These procedures specify how to link a Filter Action Block to an existing policy. You can also link a Filter Action Block to a new policy as you create one.

1. In the Admin Client, click the *Identity Driven* tab.
2. Click *Policies*.
3. Right-click a selected policy and select *Edit*.
4. Click either *Vault* or *Groom*.
5. Click *Link Action Block*.

6. From the Action Block Selector dialog box, select the Filter Action Block you want to link.



7. Click *OK*.

   The link is specified in the *Groom Rules* or *Vault on Delete Rules* header.

   When a policy's Vault or Groom Rules are linked to a Filter Action Block, the rules displayed in the policy editor are read-only. To edit the Filter Action Block, click the name as it appears in the header.

8. Click *OK* to save the link.

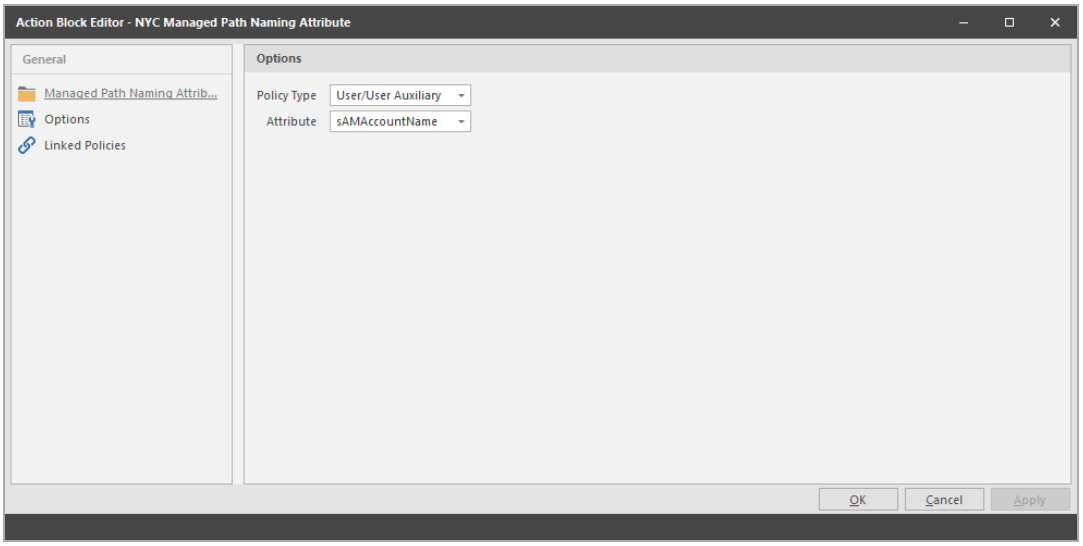
Creating a Managed Path Naming Attribute Action Block

You can use a Managed Path Naming Attribute Action Block to specify the naming attribute and its corresponding definition, to an existing policy.

For specifications pertaining to Managed Path Naming Attribute, see *Managed Path Naming Attribute Specifications (page 265)*.

1. In the Admin Client, click the *Identity Driven* tab.
2. Click *Action Blocks*.
3. Select *Manage > New> Managed Path Naming Attribute*.
4. In the *Name* field, give the new Action Block a name and click *OK*.

The following dialog box appears:



Managed Path Naming Attribute: Displays the *Policy Type* and *Attribute* drop-down menus.

Options: The *Description* option can be used to provide detailed context for the usage and implementation of the Managed Path Naming Attribute Action Block.

Linked Policies: Linked Policies is a read-only view of which policies are linked to the Managed Path Naming Attribute Action Block.

5. From the *Policy Type* drop-down menu, specify whether the Managed Path Naming Attribute Action Block will be linked to a *User/User Auxiliary* policy or a *Group Collaborative* storage policy.

   The attributes types that you can select vary based on the selected policy type.

6. From the *Attribute* drop-down list, select one of the single-valued Active Directory attributes for the User or Group object.

   You have the ability to specify an attribute other than `sAMAccountName`. This ability was added to provide network administrators the ability to give provisioned folders a more descriptive name.

   Once you select a different attribute, you can then use an account provisioning system such as NetIQ Identity Manager to automatically populate the selected attribute with a desired folder name and then File Dynamics will automatically provision the home folder based on this attribute setting.

   For more information, see *Setting Target Paths (page 36)*

7. Click *Apply*.

Linking a Managed Path Naming Attribute Action Block to a Policy

These procedures specify how to link a Managed Path Naming Attribute Action Block to an existing policy. You can also link a Managed Path Naming Attribute Action Block to a new policy as you create one.

1. In the Admin Client, click the *Identity Driven* tab.
2. Click *Policies*.
3. Right-click a selected policy and select *Edit*.
4. In the Policy Editor, click *Target Paths*.
5. Click *Link Action Block*.
6. Select the Action Block you want to link.
7. Click *OK*.

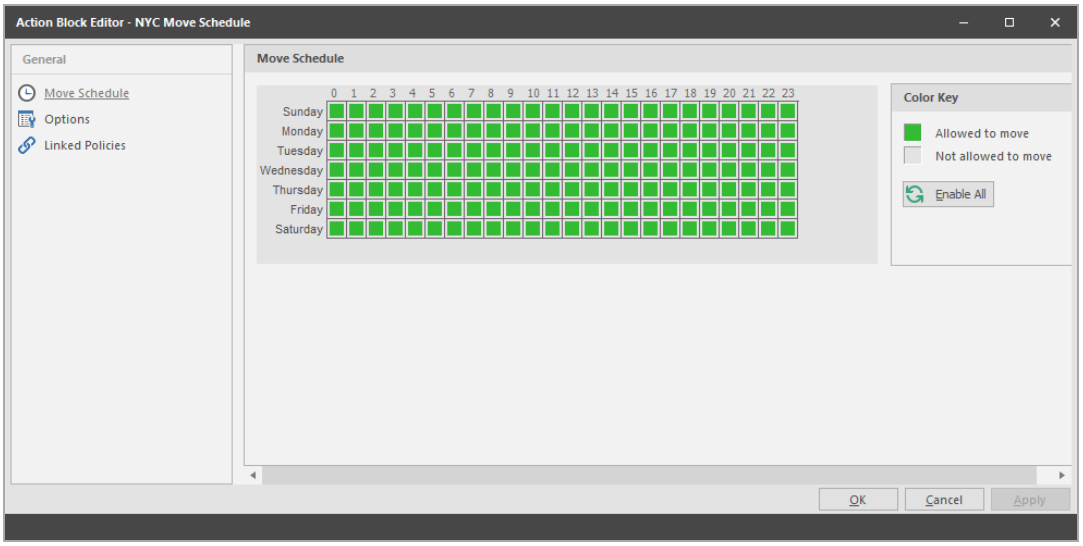
Creating a Move Schedule Action Block

Use Move Schedule Action Blocks to standardize when data can be moved during data movement operations.

1. In the Admin Client, click the *Identity Driven* tab.
2. Click *Action Blocks*.
3. From the *Manage* menu, select *New* > *Move Schedule*.

4. Enter a descriptive name for the new Action Block and click *OK*.

The following page appears:



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.

5. In the *Move Schedule* grid, click the squares for the day and hour you want to disable for data movement.
6. Click *Apply* to save your settings.
7. Click *OK* to close the page.

Linking a Move Schedule Action Block to a Policy

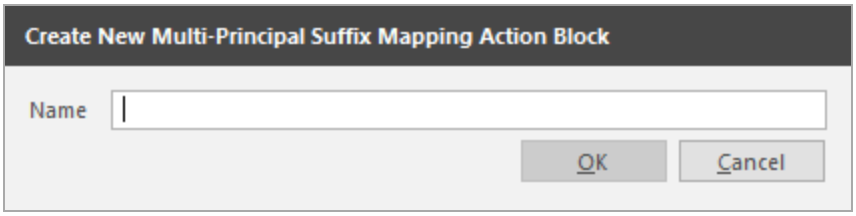
These procedures specify how to link a Move Schedule Action Block to an existing policy. You can also link a Move Schedule Action Block to a new policy as you create one.

1. In the Admin Client, click the *Identity Driven* tab.
2. Click *Policies*.
3. Right-click a selected policy and select *Edit*.
4. In the Policy Editor, click *Move Schedule*.
5. Click *Link Action Block*.
6. Select the Action Block you want to link.
7. Click *Apply* to save your settings.
8. Click *OK* to close the page.

Creating a Multi-Principal Suffix Mapping Action Block

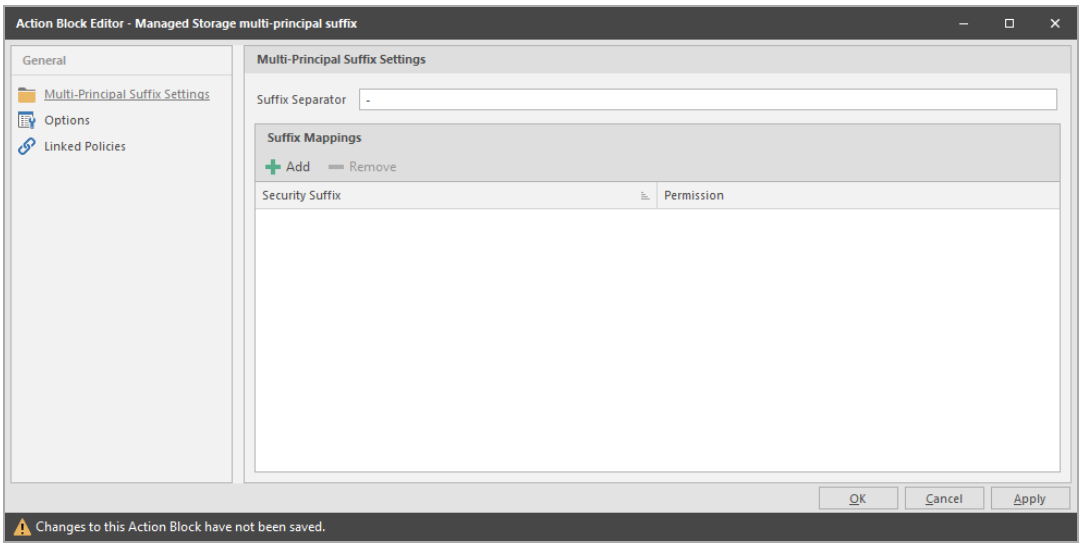
Use Multi-Principal Suffix Mapping Action Blocks to standardize the groups and their associated permissions for the collaborative storage folders that are provisioned by File Dynamics.

1. In the Admin Client, click the *Identity Driven* tab.
2. Click *Action Blocks*.
3. From the *Manage* menu, select *New > Multi-Principal Suffix Mapping*.



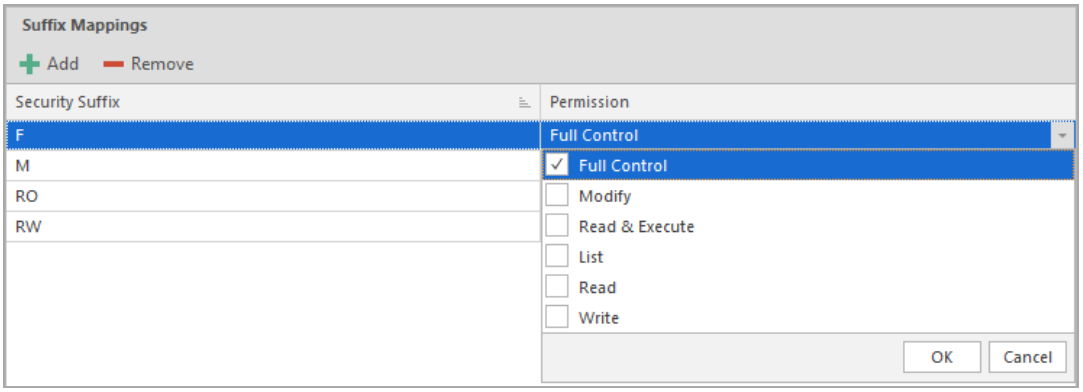
4. Enter a descriptive name for the new Action Block and click *OK*.

   The following page appears:

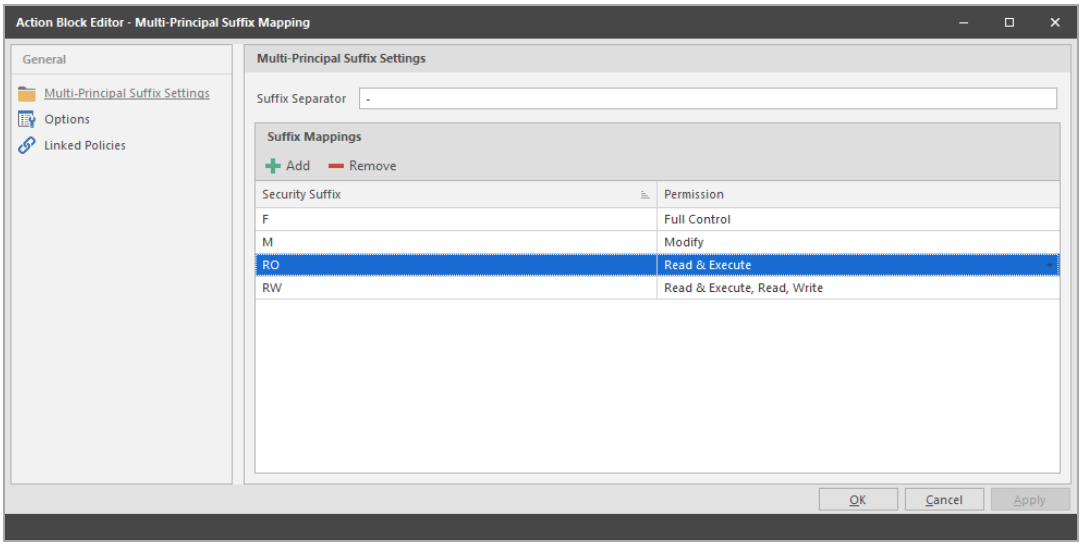


5. Click *Add*.
6. In the *Security Suffix* column, highlight *SampleSecuritySuffix* and edit it to a more descriptive name of a group that will access the collaborative storage folder.
7. Click the *Full Control* setting to access a drop-down menu of access permissions.

8. Specify the permissions for the particular group and click *OK*.



9. Repeat Step 5 through Step 8 to create all groups and permissions to the collaborative storage folder.



10. Click *Apply*.
11. Click *OK*.

Linking a Multi-Principal Suffix Mapping Action Block to a Policy

These procedures specify how to link a Multi-Principal Suffix Mapping Action Block to an existing policy. You can also link a Multi-Principal Suffix Mapping Action Block to a new policy as you create one.

1. In the Admin Client, click the *Identity Driven* tab.
2. Click *Policies*.
3. Right-click a selected Group Multi-Principal Collaborative policy and select *Edit*.
4. In the Policy Editor, click *Provisioning Options*.
5. Click *Link Action Block*.

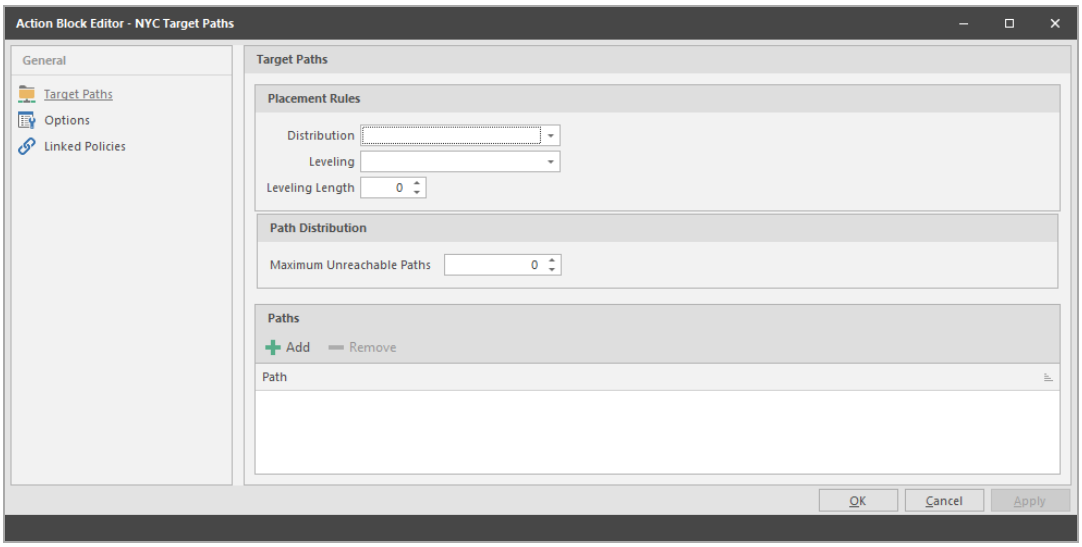
6. Select the Action Block you want to link.
7. Click *Apply* to save your settings.
8. Click *OK* to close the page.

Creating a Target Paths Action Block

Use Target Paths Action Blocks to standardize the placement rules for the managed path, as well as the paths to the shares where managed paths will be hosted.

1. In the Admin Client, click the *Identity Driven* tab.
2. Click *Action Blocks*.
3. From the *Manage* menu, select *New* > *Target Paths*.
4. Enter a descriptive name for the new Action Block and click *OK*.

   The following page appears:



5. Click *Add* to access the Path Browser.
6. Browse to the location of the target path you want and click *Add* to add the target path to the *Selected Paths* pane.
7. Click *OK* to close the Path Browser.
8. In the *Placement Rules* region, specify a *Distribution* field setting and if you choose, *Leveling* parameters.

   For more information on target path distribution and leveling, see *Setting Target Paths (page 36)*.
9. Click *Apply*.
10. Click *OK*.

Linking a Target Paths Action Block to a Policy

These procedures specify how to link a Target Paths Action Block to an existing policy. You can also link a Target Paths Action Block to a new policy as you create one.

1. In the Admin Client, click the *Identity Driven* tab.
2. Click *Policies*.
3. Right-click a selected policy and select *Edit*.
4. In the Policy Editor, click *Target Path Options*.
5. Click *Link Action Block*.
6. Select the Action Block you want to link.
7. Click *Apply* to save your settings.
8. Click *OK* to close the page.

11.2.5 - Management Actions

In managing user and collaborative storage with File Dynamics, 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 File Dynamics, performing these types of operations is collectively referred to as performing a Management Action and is done through the Take Action page.

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.

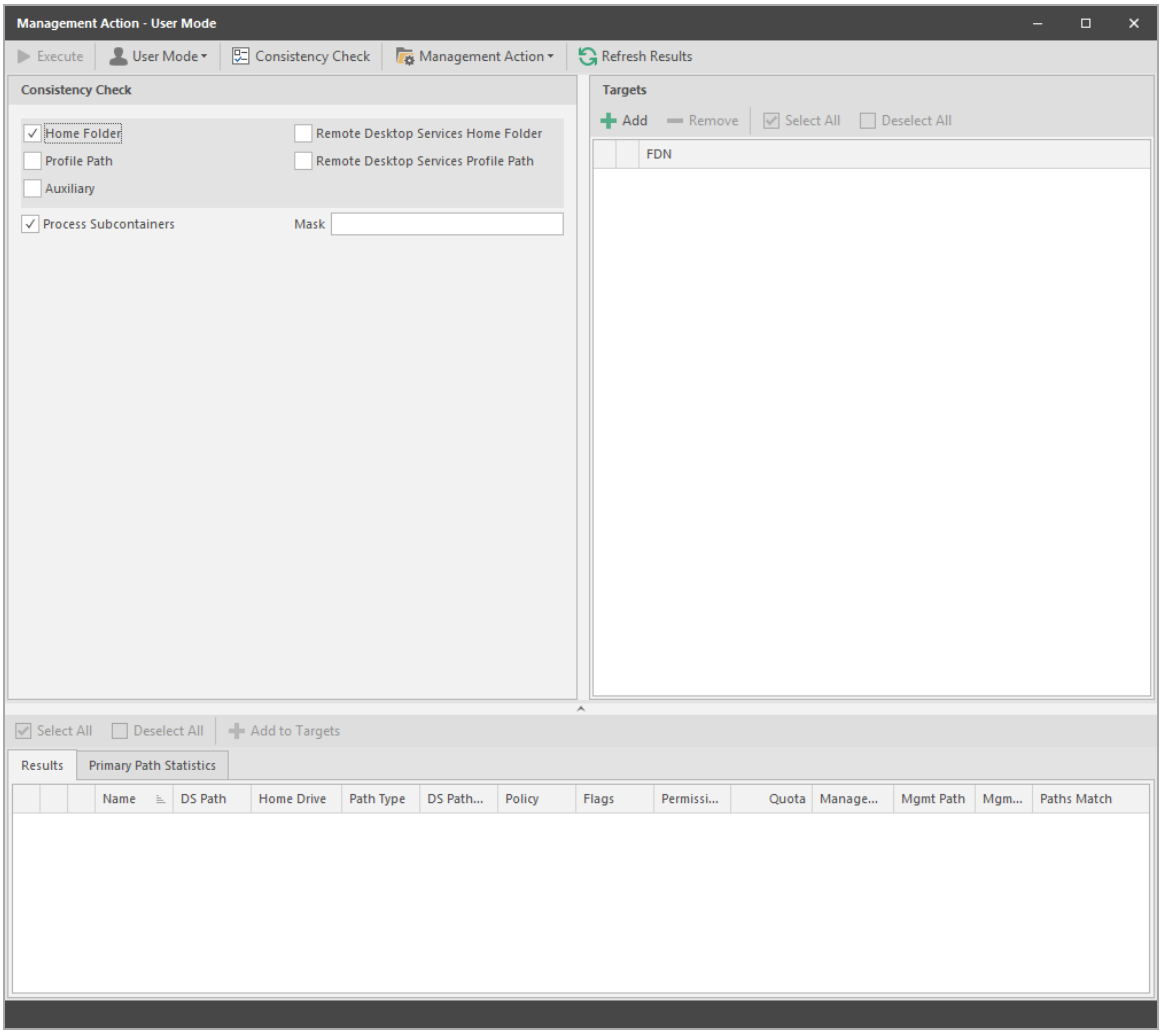
The Management Actions vary based on whether the selected mode is *User*, *Group*, or *Container*. For example, if *Group* mode is selected, the Management Action will be performed for collaborative storage processing using Dynamic Template processing. If *Collaborative* mode is selected, the Management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

File Dynamics 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

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.

Management Action Dialog Box



Execute: Clicking this button executes the management action. Once you have specified a target and selected a Management Action, a *Preview* option appears, allowing you to preview the effects of the Management Action before executing the action.

Mode: This drop-down menu lets you indicate if the Management Action is to apply to a 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.

A consistency check notifies you of inconsistencies or potential problems pertaining to user and group storage being managed through File Dynamics. 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 *Running Consistency Check Reports on Existing Storage (page 15)*, you ran a consistency check before creating your first primary user policy to help you determine how to configure the policy.

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
- Mask

When you perform a Management Action on an organizational unit, File Dynamics applies the action to all subcontainers. If you do not want the action applied to subcontainers, you can deselect the *Process Subcontainers* check box.

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 File Dynamics analyzes. You can enter standard wildcard 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 the ^.

Available Management Actions

File Dynamics lets you perform an extensive set of Management Actions. For details on each, click a link below.

Manage

This Management Action catalogs objects in File Dynamics, putting them in a managed state.

If the existing objects already have established managed paths, attributes, and rights, File Dynamics 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 Path

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 select *Enforce Policy Path* 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.

Enforce Policy Path for Vault

This Management Action will set or reset the user's vault path to one that matches their managing policy's vault path. This can be useful in cases where a previous vault is no longer valid. For example, when an administrator decommissions the previous server or share used for vaulting and has established a new vault location.

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 (page 191)*). 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 Active Directory, to the drive letter that is specified in the File Dynamics policy.

If you have a File Dynamics Remote Desktop Services home folder policy and you want to apply the drive letter that is established in that policy, you can select the *Remote Desktop Services Home Folder* check box.

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

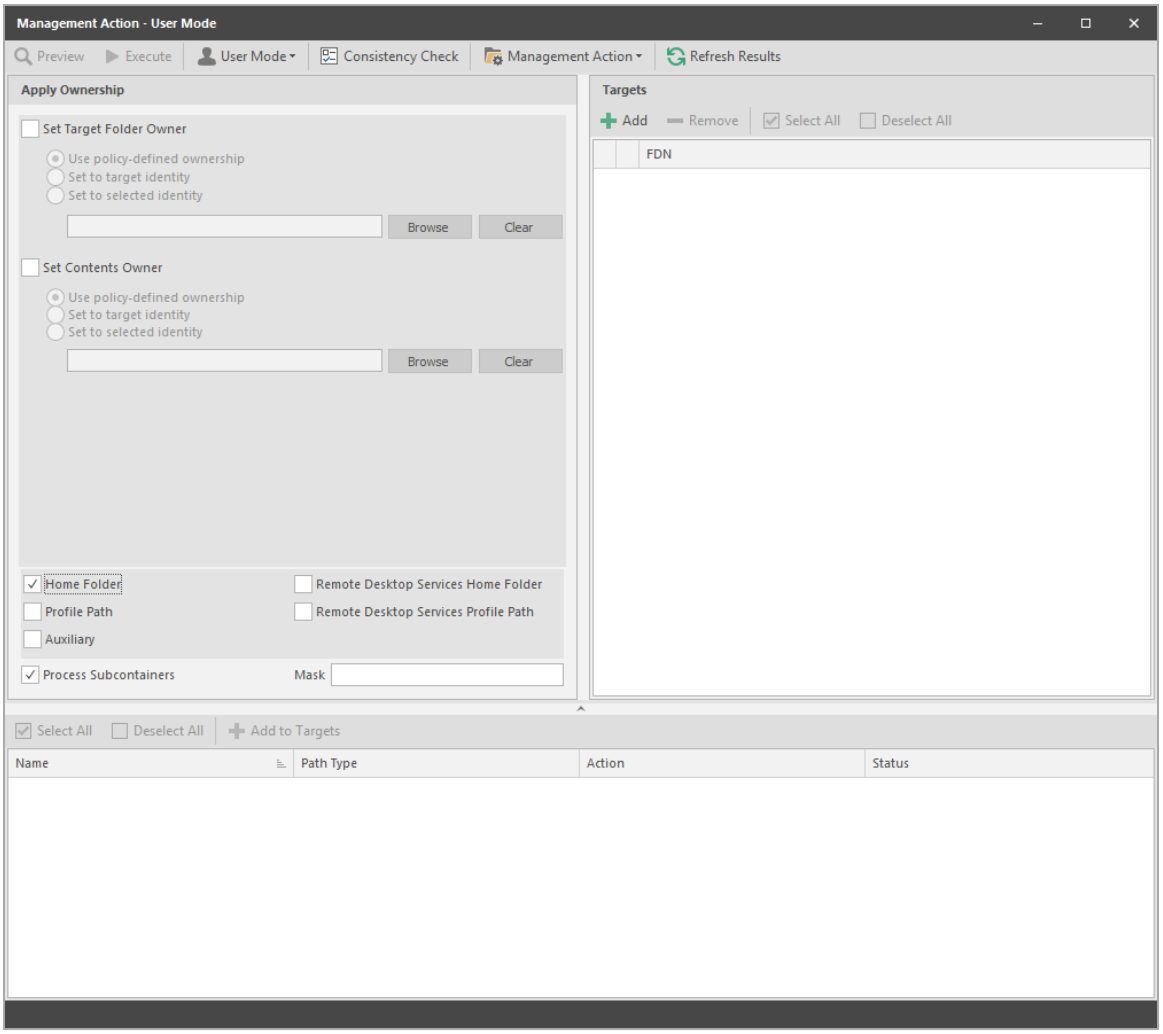
modify the collaborative storage template in the policy to include –OWNER– and –MEMBER–. For more information, see *Managing Collaborative Storage (page 69)*.

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 Owner

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

Apply Owner Management Action Page



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.

Specify the policy types you want this Management Action to apply to by selecting from the policy type check boxes.

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.

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 File Dynamics analyzes. You can enter standard wildcard 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 Permissions

This Management Action lets you apply NTFS file system permissions. If you decide to modify the file system permissions in a policy, you can select *Apply Permissions* to immediately apply the new permissions 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 (page 191)*). 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 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, profile path, Remote Desktop Services home folder, or Remote Desktop Services profile path ever becomes corrupted, this Management Action can be used to recover an uncorrupted version of the attribute from the File Dynamics database.

Assign Managed Path

You can use this Management Action to assign an attribute to a user folder, profile path, Remote Desktop Services home folder, or Remote Desktop Services profile path.

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 Engine Database

This Management Action removes objects from the File Dynamics database and makes the object unmanaged.

11.2.6 - 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.

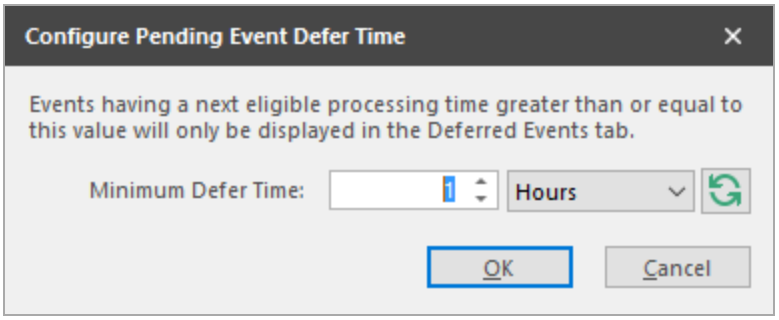
Make Eligible: If an event is deferred, you can click this option to make the event eligible immediately.

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.

Configure: Lets you adjust the time parameter for making pending events eligible for display as deferred events.

The default setting is one hour, meaning that any pending events scheduled to be addressed within one hour will be displayed when the *Active Only* menu option is selected. Those events scheduled to be addressed later than one hour will be displayed when the *Deferred Only* menu option is selected.

Configure Pending Event Defer Time Dialog Box



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

Abort: Lets you terminate the selected event or events.

Refresh: Refreshes the event list.

View Events: Lets you filter the displayed events by displaying *All*, *Active*, or *Deferred* pending events.

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.

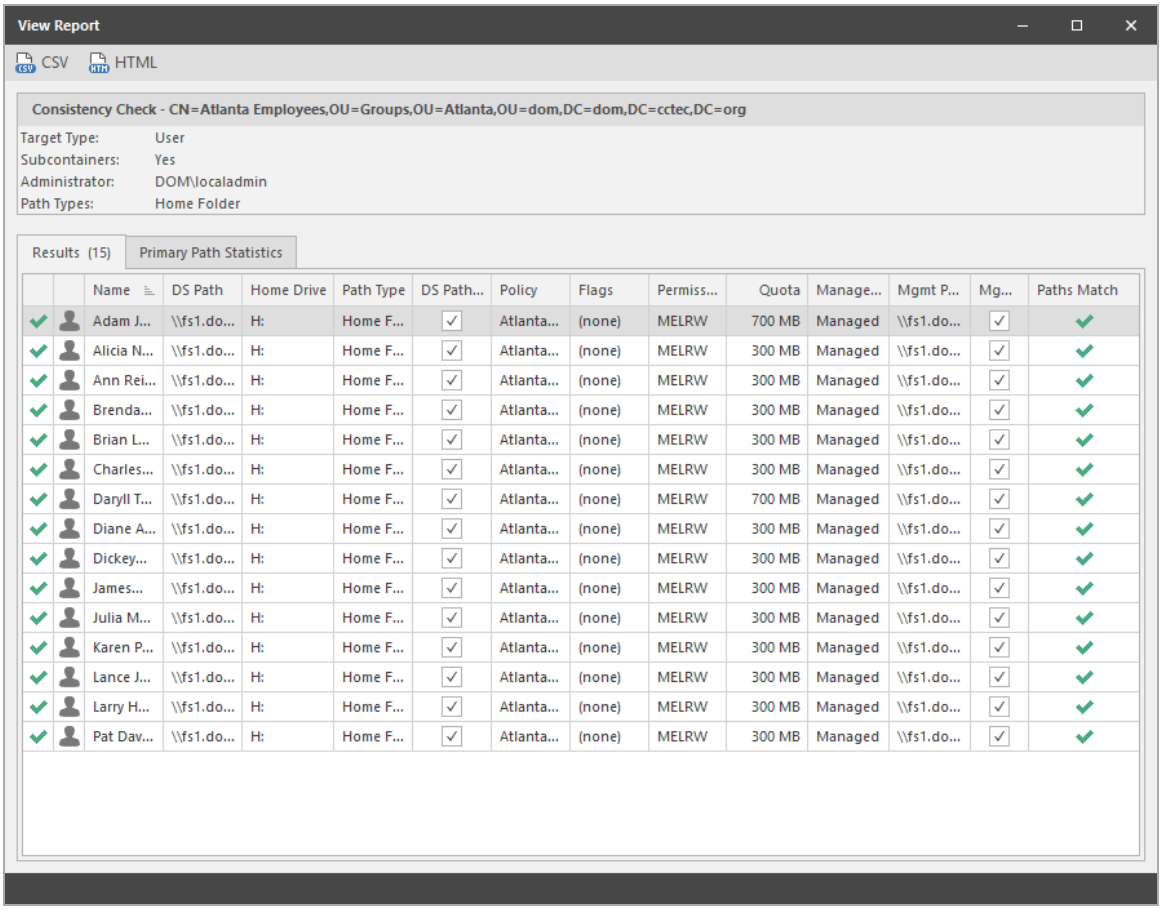
- **Accepting:** A green check mark indicates that File Dynamics is accepting events to process. You can stop accepting events to process by clicking this button. You are prompted to enter text in a field indicating your reason for stopping the acceptance of events. The text you enter is recorded on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

11.2.7 - Consistency Check

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.

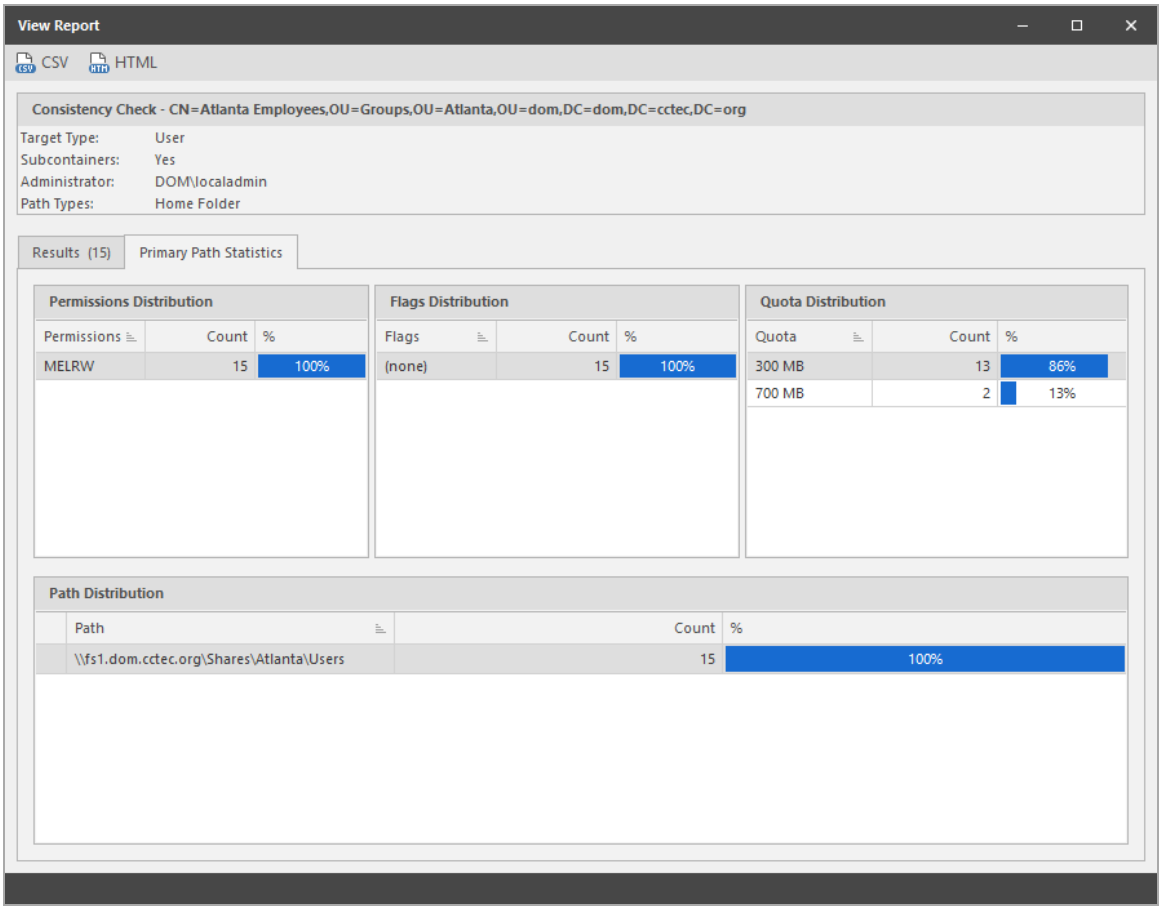
Consistency Check Report



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.

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 *CSV* or *HTML* icons.

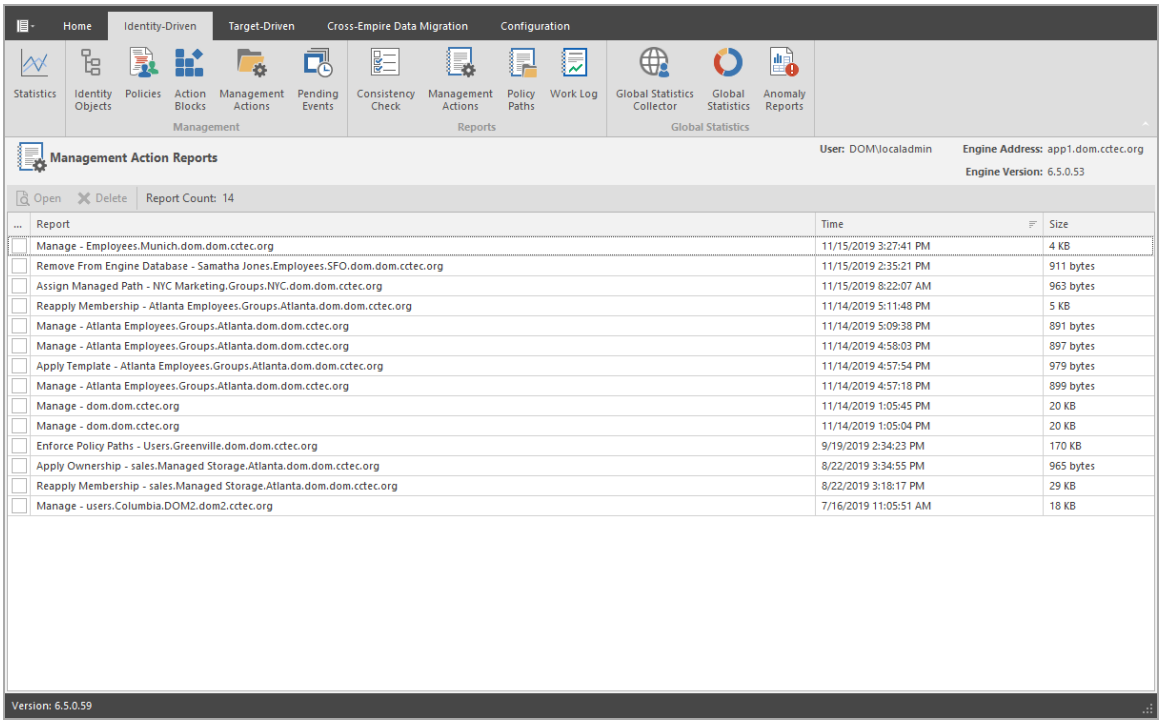
For more information on Consistency Check Reports, see *Running Consistency Check Reports on Existing Storage (page 15)* and *Performing a Consistency Check (page 27)*.

11.2.8 - Management Action Reports

Management 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 Active Directory 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.

Management Action Report

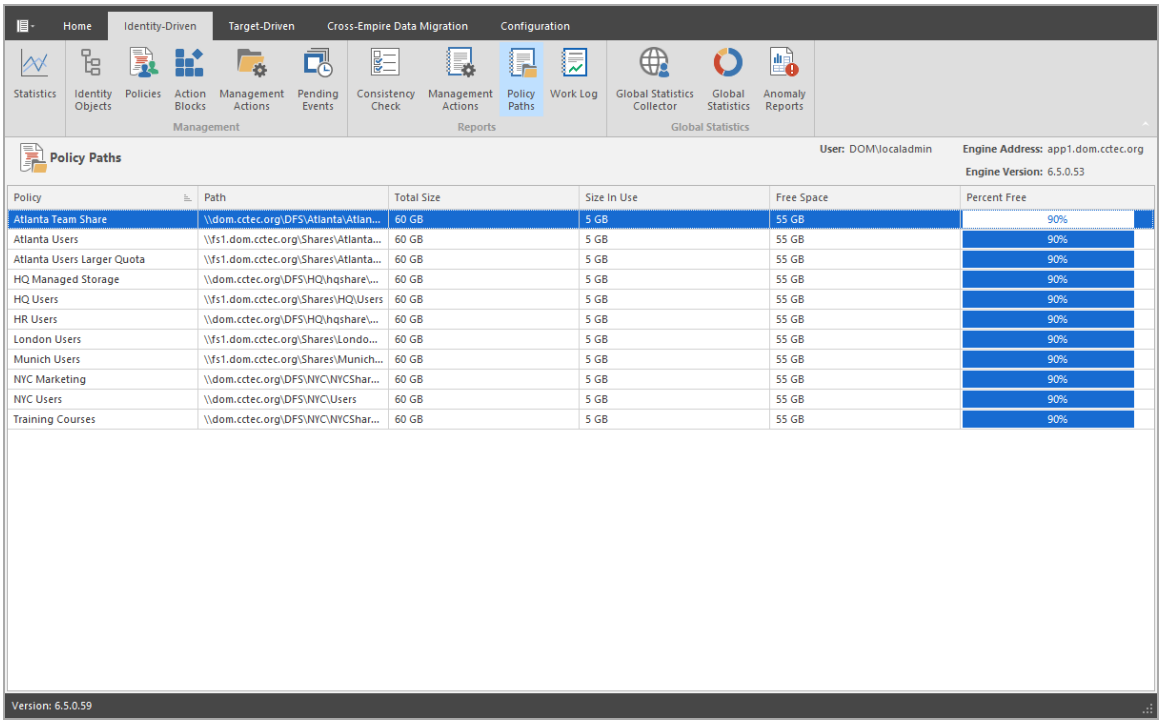


To export an Action report, double-click a report listing to access the View Report dialog box, and then in the upper-left corner of the dialog box, click either the *CSV* or *HTML* icons.

11.2.9 - Policy Paths

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

Policy Paths Report



11.2.10 - Work Log

Click *Work Log* to build Work Log reports. For details and procedures for doing so, see *Building Work Log Reports (page 145)*.

11.2.11 - Global Statistics Collector

The Global Statistics Report (GSR) Collector is a multi-purpose mechanism that collects data for storage usage statistics and policy-based storage redistribution, generates reports on anomalies such as a user with a non-existent home folder, and catalogs objects and their paths for historical purposes.

The data collected by the GSR Collector has four primary uses:

- GSR Collector Anomaly Analysis
- Global Statistics
- History
- Policy-based Path Redistribution

Your usage of the GSR Collector data may be specific to all of these or some subset. You should analyze your needs of the feature set it provides and weigh them with the frequency and scope that best suits your needs.

For example, Anomaly Analysis may be an important tool for helping you determine the state of your unmanaged data when you have no configured policies or when you're initially

implementing File Dynamics. Thereafter, you may not need to examine the reports on a daily basis. In this case, after your policies are configured and users are managed, you might opt to change the schedule of the GSR Collector to run weekly.

GSR Anomaly Analysis is discussed in *Anomaly Reports (page 203)*.

The Global Statistics provided by the GSR Collector offer insight into how your storage is being consumed by the supported categories of objects (e.g. user and collaborative) but it comes at a price. It can be expensive to run if you do not have quotas enabled via File Storage Resource Manager (FSRM) or your managed storage resources primarily consist of NAS devices.

Alternatively, you might find that the Global Statistics are less important in lieu of your need for a finer granularity of historical data. The same size data used for the Global Statistics is also used for Policy-based Path Redistribution. Depending on the policies for which you plan to redistribute data, you might configure the GSR Collector to perform a Complete Inspection on the paths for a specific policy. Thus eliminating the need to wait for Complete Inspection to be performed needlessly against all storage resources.

The GSR Collector is designed to be run on a scheduled interval so that you can collect the appropriate data to provide the necessary granularity for your needs. By default, the GSR Collector will not run unless you run it manually or configure it to run based on a schedule.

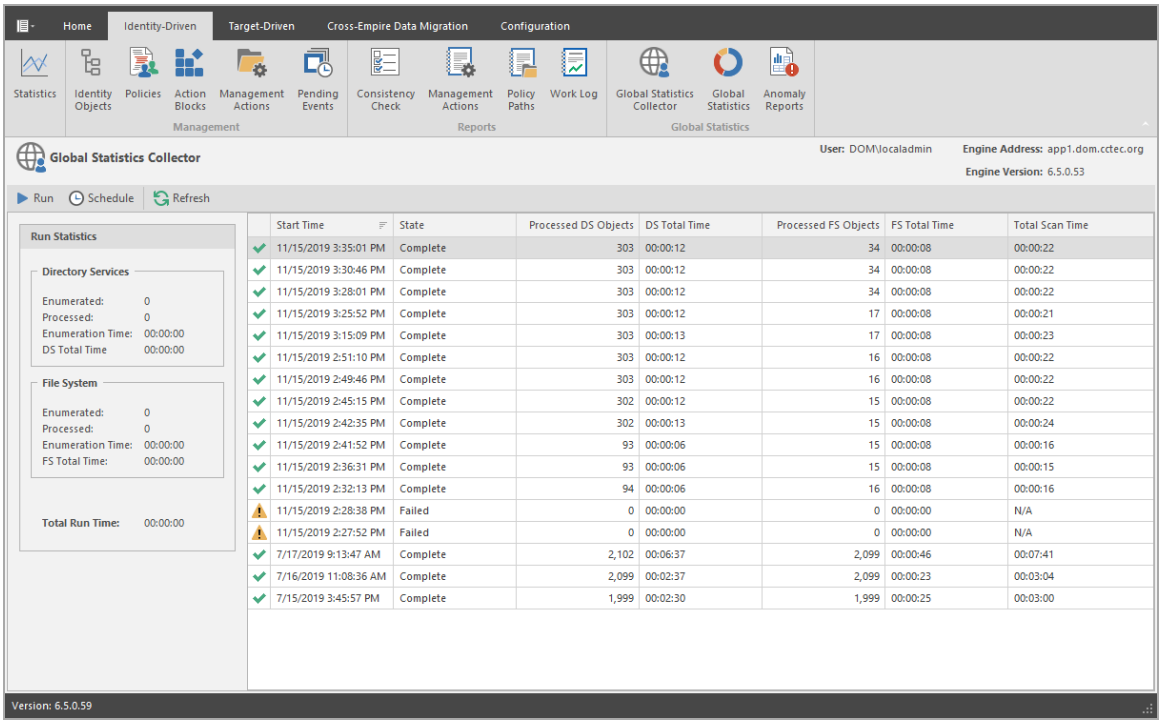
Performance Caveats

Due to the number of objects, amount of data to scan, and your configuration, the GSR Collector can be resource intensive and long running. By default, it will collect data on all objects and accessible shares in Active Directory. This default configuration is not ideal for most File Dynamics deployments. However, the configuration of the GSR Collector allows you to scope it according to your needs. You are encouraged to scope it according to the objects and shares that will be managed by File Dynamics. You should be careful when running the GSR Collector during peak traffic load on the Engine.

Global Statistics Collector Interface

The GSR Collector interface is the means of running and scheduling the GSR Collector, as well as viewing the results of when it was run previously.

Global Statistics Collector



Run: Runs the GSR Collector according to the current GSR Collector configuration. For information on the GSR Collector configuration, see *Global Statistics Configuration (page 236)*.

Schedule: Lets you schedule when the GSR Collector is run.

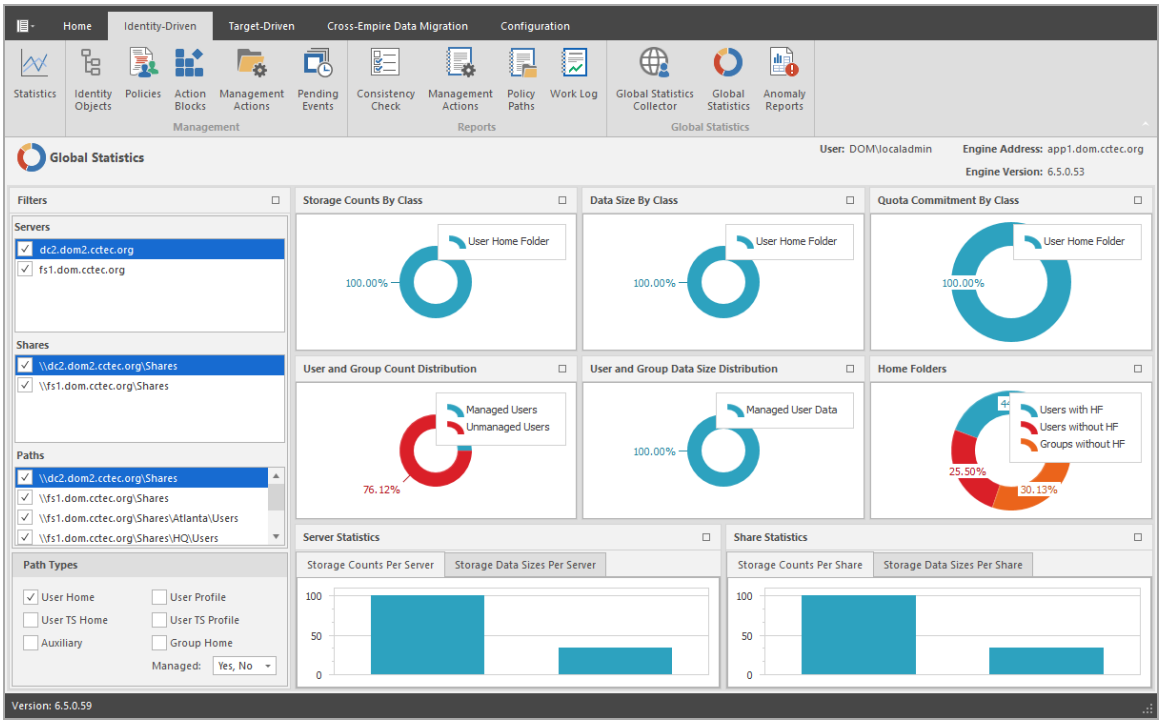
Refresh: Refreshes the list of GSR Collector runs listed in the right pane of the page.

Run Statistics: Displays statistics as the GSR Collector is being run. Once the GSR Collector has completed its run, the statistics are appended to the top of the list in the pane on the right side of the page.

11.2.12 - Global Statistics

This page displays a variety of statistics according to the findings of the GSR Collector.

Global Statistics

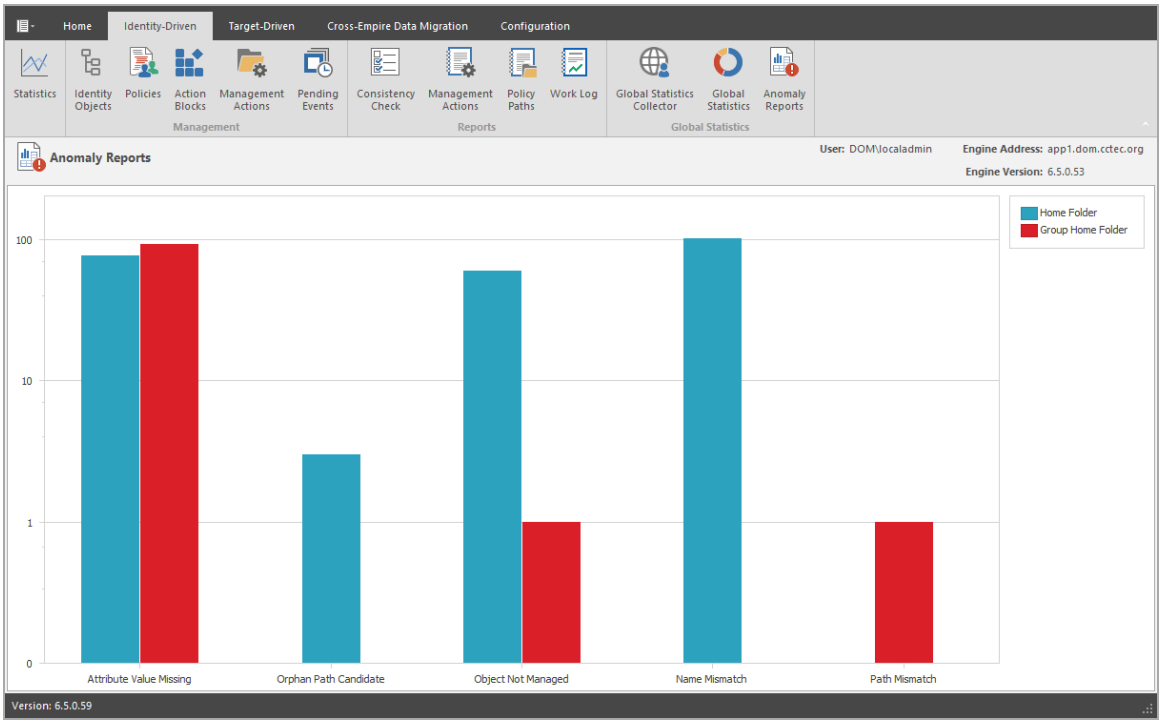


The Global Statistics page is laid out in a way that you can set the parameters for display on the left-hand portion of the page and then see the results on the right.

11.2.13 - Anomaly Reports

The GSR Collector performs Anomaly Analysis that generates data for Anomaly Reports. These reports are designed to help you evaluate the state of your storage infrastructure. Additionally, they can be used in preparation for using File Dynamics to bring storage under management by policy. Anomaly data will be produced for each object and path type specified in the GSR Collector configuration.

GSR Anomaly Report



To see further detail about a specific anomaly report, single-click on the column.

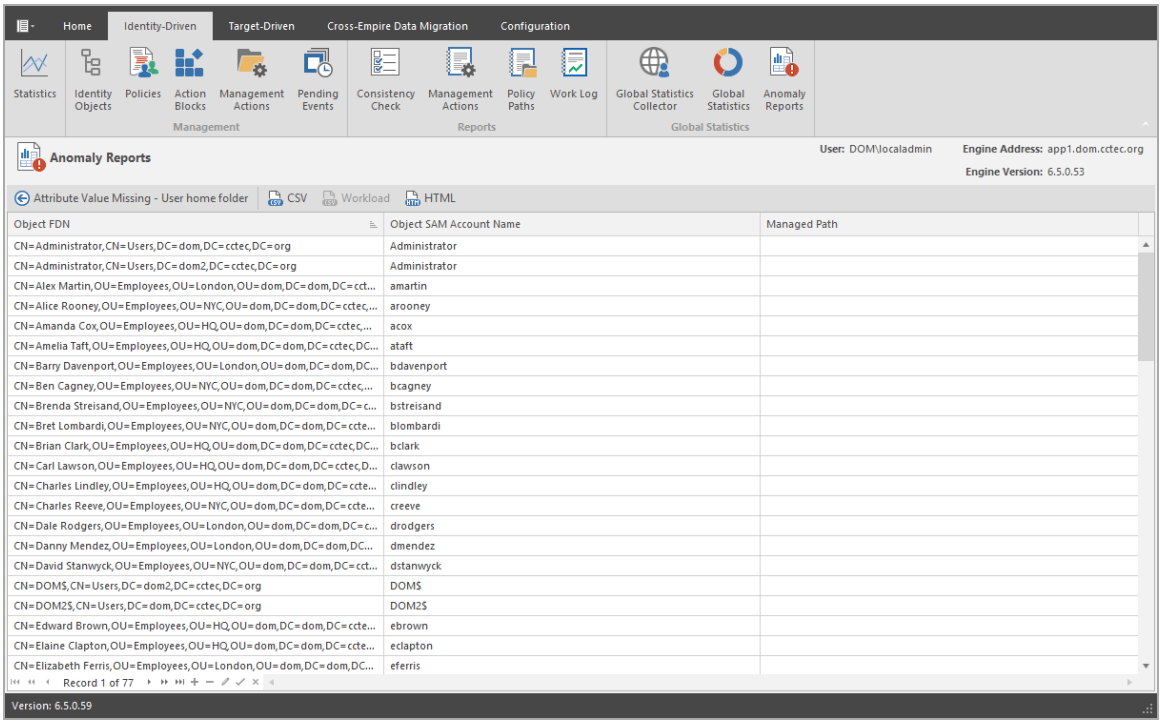
A detailed summary of each of the GSR Anomaly reports follows in the sections below.

Attribute Value Missing

This Anomaly report indicates that the respective path attribute (e.g. home folder) does not have a value for a given object in Active Directory.

The graphic below is an example of an Attribute Value Missing Anomaly report. The *Object FDN* and *Object SAM Account Name* columns display the respective attributes. The *Managed Path* column does not have a value because this object is not yet managed by File Dynamics. These objects are reported because they do not have homeDirectory attribute values. This report can be used to identify objects that should be managed. It can also identify objects that have had their respective path attribute cleared accidentally or erroneously by an identity management system.

Attribute Value Missing

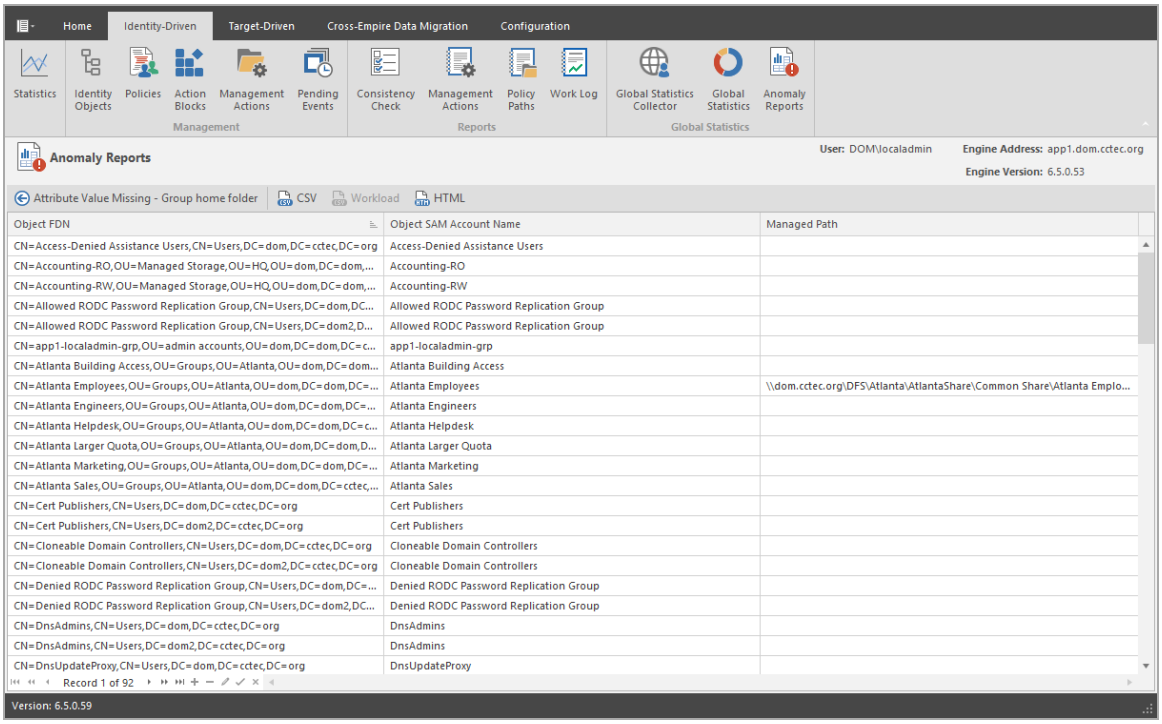


Path Missing on Disk

This Anomaly report indicates that the respective path attribute value (e.g. home folder) for a given object cannot be found on disk.

The graphic below is an example of a Path Missing on Disk Anomaly report. The *Object FDN* and *Object SAM Account Name* columns display the respective attributes. The *Path* column is the value of the homeDirectory attribute. The *Managed Path* column does not have a value because this object is not yet managed by File Dynamics. This object is reported because the path specified by its homeDirectory attribute does not exist on disk or could not be found. This report can be used to identify objects whose respective path attribute value no longer exists at that location because of accidental deletion or being moved manually.

Path Missing on Disk

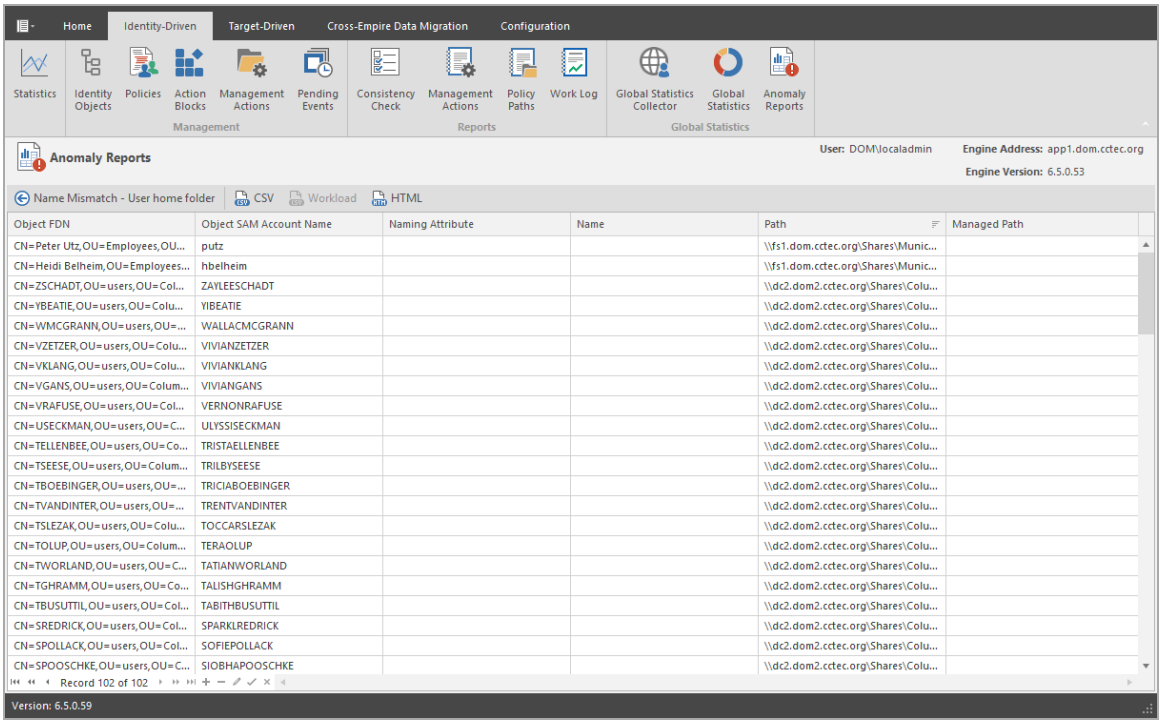


Name Mismatch

This Anomaly report indicates that the leaf path name of the respective attribute value (e.g. home folder) does not match that of the respective object's name.

The graphic below is an example of the Name Mismatch report. The *Object FDN* and *Object SAM Account Name* columns display the respective attributes. The *Path* column is the value of the homeDirectory attribute. The *Path* column contains the current respective path attribute value obtained from Active Directory. The *Managed Path* column contains the path value when the object was last managed. This object is reported because the leaf path name specified by its homeDirectory attribute does not match the sAMAccount name attribute. This report can be used to identify objects whose respective path might have been changed manually.

Name Mismatch

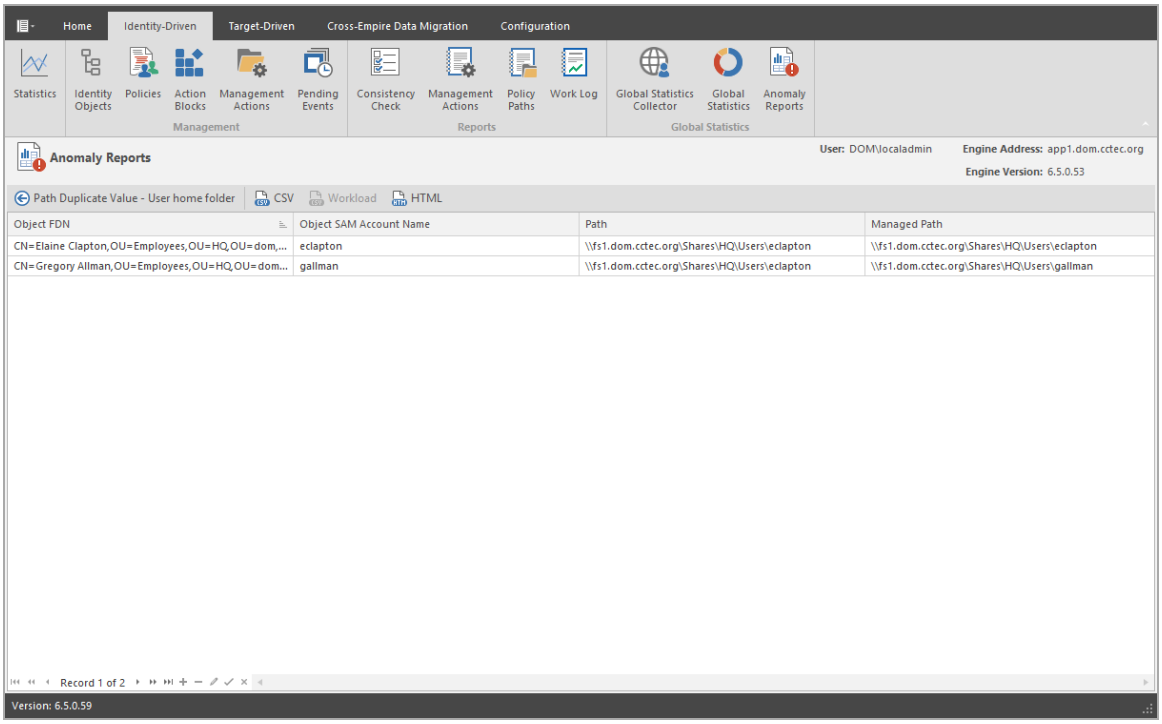


Path Duplicate Value

This Anomaly report indicates that two or more objects have been detected that contain the same value for the respective path attribute (e.g. home folder).

The graphic below is an example of the Path Duplicate Value report. The *Object FDN* and *Object SAM Account Name* columns display the respective attributes. The *Path* column is the value of the homeDirectory attribute. The *Path* column contains the current respective path attribute value obtained from Active Directory. The *Managed Path* column does not have a value because these objects are not yet managed by File Dynamics. These objects are reported because they have the same value for their homeDirectory attribute. This report can be used to identify objects who erroneously share the same path for the respective path attribute.

Path Duplicate Value

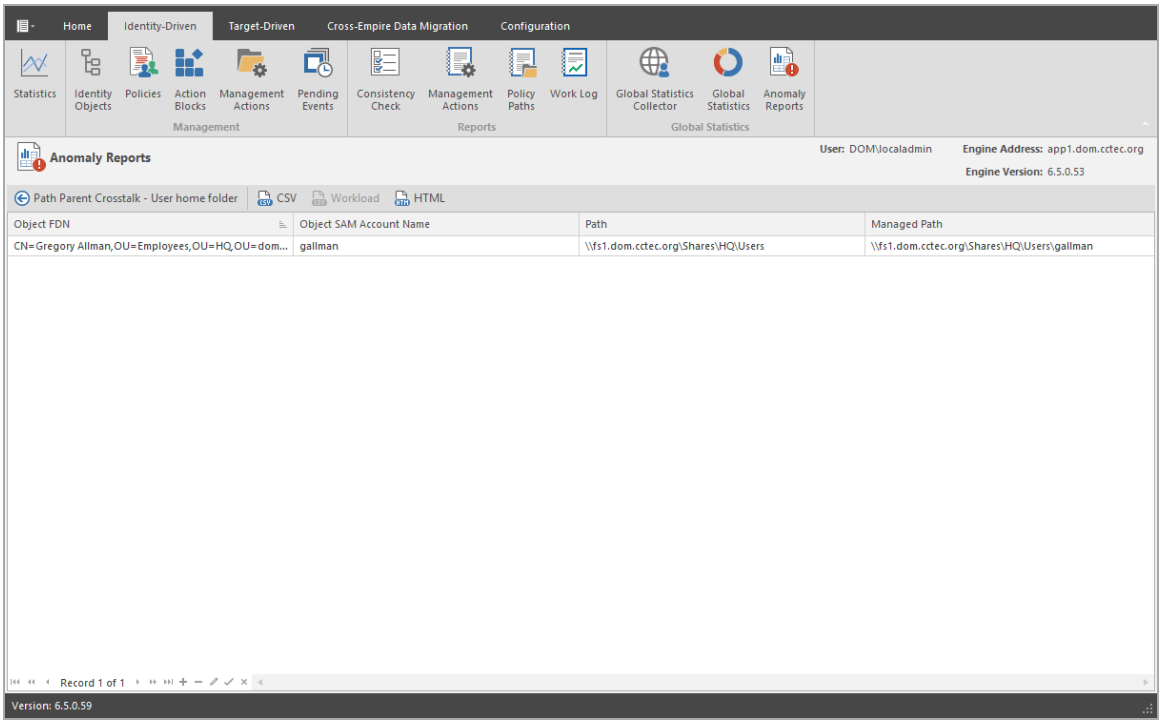


Path Parent Crosstalk

This Anomaly report indicates that the object's respective path attribute value (e.g. home folder) has been detected as being the parent of another object's path attribute value (e.g. home folder).

The graphic below is an example of the Path Parent Crosstalk report. The *Object FDN* and *Object SAM Account Name* columns display the respective attributes. The *Path* column is the value of the homeDirectory attribute. The *Path* column contains the current respective path attribute value obtained from Active Directory. The *Managed Path* column does not have a value because these objects are not yet managed by File Dynamics. This object is reported because the value for its homeDirectory attribute has been detected as being the parent of another object's homeDirectory attribute. This report can be used to identify objects whose respective path attribute is set to the wrong location and might impact another object's storage.

Path Parent Crosstalk

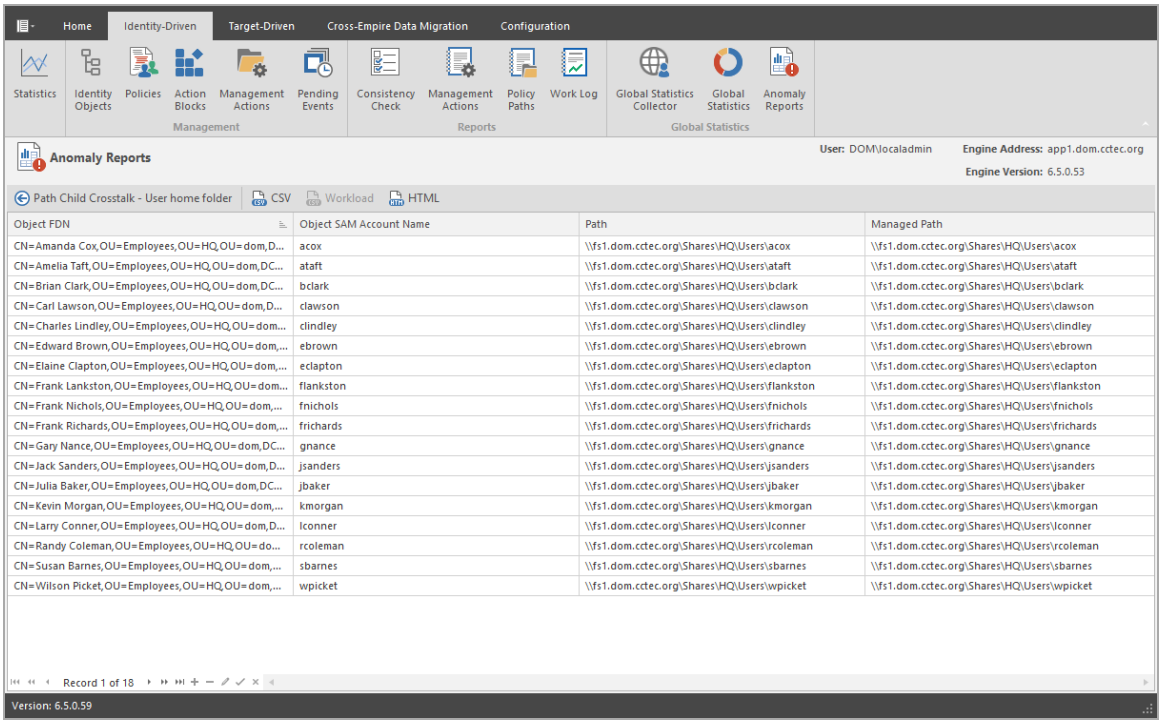


Path Child Crosstalk

This Anomaly report indicates that the object's respective path attribute value (e.g. home folder) has been detected as being the subordinate of another object's path attribute value (e.g. home folder).

The graphic below is an example of the Path Child Crosstalk report. The *Object FDN* and *Object SAM Account Name* columns display the respective attributes. The *Path* column is the value of the homeDirectory attribute. The *Path* column contains the current respective path attribute value obtained from Active Directory. The *Managed Path* column does not have a value because these objects are not yet managed by File Dynamics. This object is reported because the value for its homeDirectory attribute has been detected as being the child of another object's homeDirectory attribute. This report can be used to identify objects whose respective path attribute might be impacted by another object's storage.

Path Child Crosstalk



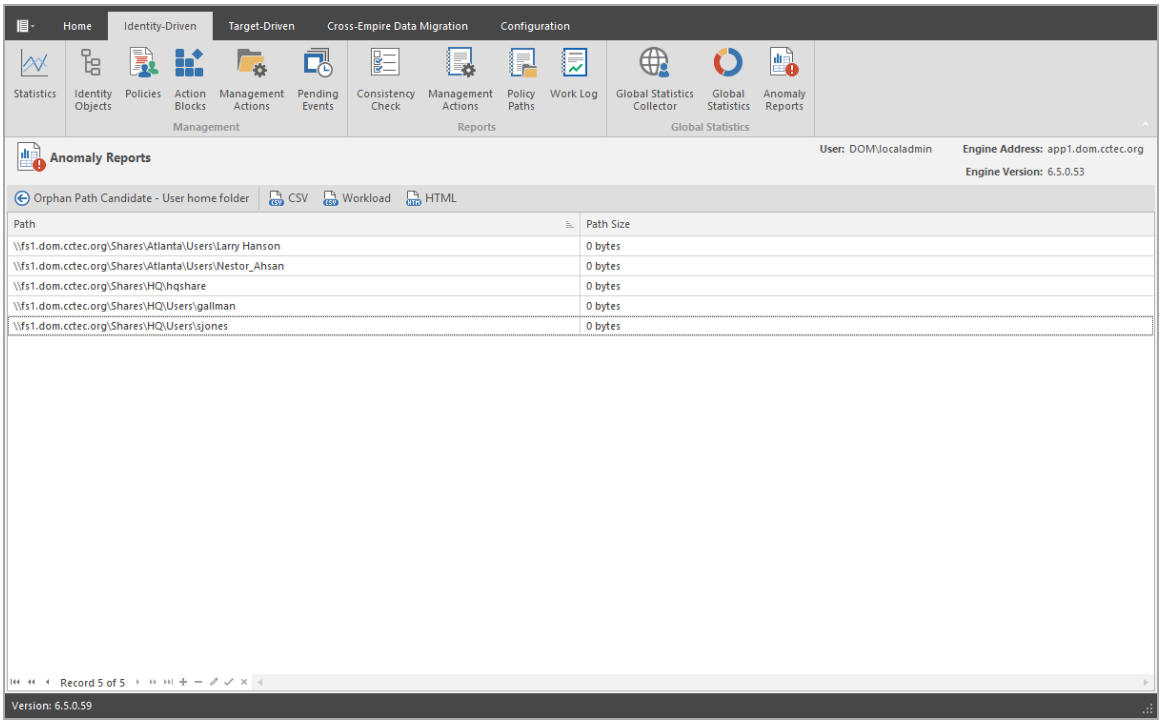
To see which object is a parent of this object's homeDirectory attribute value, see *Path Parent Crosstalk (page 208)*.

Orphan Path Candidate

This anomaly report indicates that the path is directly subordinate to a path at which other DS-associated paths have been found, but has not been detected as being associated with any DS object via a path attribute (e.g. home folder).

The graphic below is an example of the Orphan Path Candidate report. The *Path* column is any path that is directly subordinate to a path at which other DS-associated paths have been found. However, the path is not associated with any object via a path attribute. This report can be used to identify folders that don't belong to objects or are considered unmanaged.

Orphan Path Candidate



11.3 - Target-Driven Tab

The Target Driven tab is the means of enabling and establishing Target-Driven policies.

Policies (page 211)

Policy Schedules (page 229)

Action Blocks (page 230)

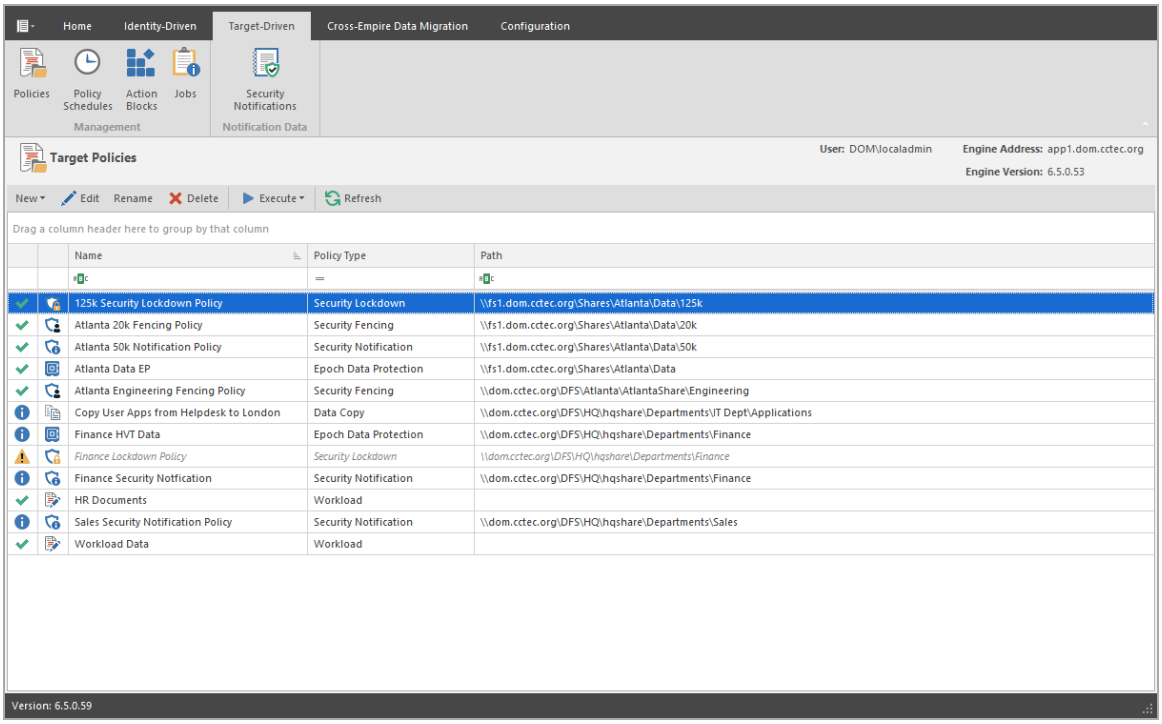
Jobs (page 230)

Security Notifications (page 231)

11.3.1 - Policies

All Target-Driven policies in File Dynamics are managed through this page.

Target-Driven Policies Page



For procedures on creating and managing Target-Driven policies, refer to *Creating Target-Driven Policies (page 109)*.

Left Pane: This region displays all Target-Driven policies according to classification. If you click a classification such as *Copy*, only Copy policies will be listed in the Right Pane. If you click a named Target-Driven policy such as *Main Groom Policy for Atlanta Users*, the policy settings appear in the Right Pane.

You can right-click listed policies and policy classifications in the Left Pane to create new policies, delete policies, and execute policies.

Right Pane: Depending on what is selected in the Left Pane, this region either lists specific Target-Driven policies, or displays the policy settings for a selected Target-Driven policy.

Manage: Use this menu to create, delete, or execute Target-Driven policies.

Refresh: Updates the list of Target-Driven policies.

Copy Policy (page 213)

Move Policy (page 214)

Groom Policy (page 216)

Security Notification Policy (page 217)

Security Lockdown Policy (page 219)

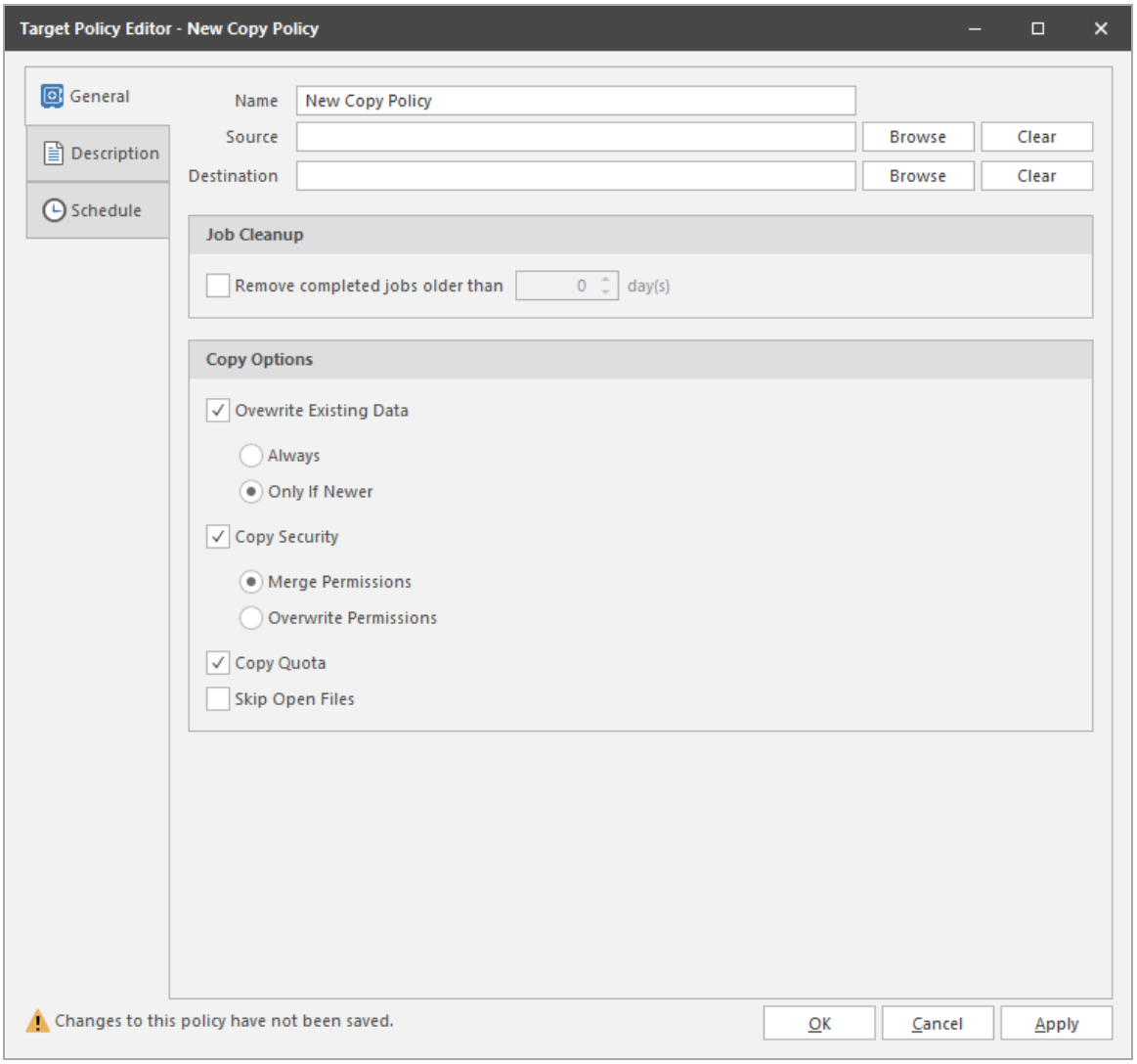
Security Fencing Policy (page 221)

Workload Policy (page 227)

Copy Policy

A discussion of fields and settings specific to a Copy policy follows.

Copy Policy Page



General Tab

Name: Use this field to specify a name for the Copy policy.

Source: Displays the location in the file system from where the files will be copied.

Destination: Displays the location in the file system where all copied files for this policy will be relocated.

Remove completed jobs older than: Lets you specify the number of days that a Copy task from this policy is listed on the Jobs list before it is purged.

Overwrite Existing Data: With the default setting, File Dynamics will overwrite an existing file on the target destination only if the same file from the source location is newer. You can adjust this setting to your preferences.

Copy Security: When selected, this maintains the file permissions from the source location to the destination location.

Copy Quota: If the destination supports quota management, it will maintain the disk quota settings from the source location to the destination location.

Skip Open Files: Skips all of the files that are opened from the source folder.

With Copy policies, File Dynamics does not attempt to copy skipped files later. You might want to therefore schedule the policy to run during a time when users are logged out. For procedures on scheduling a Copy policy to run, see *Create a Copy Policy (page 115)*.

Description Tab

The *Description* box indicates when the policy was created. It also lets you write notes pertaining to the policy. The *Description* box allows up to 255 characters.

Schedule Tab

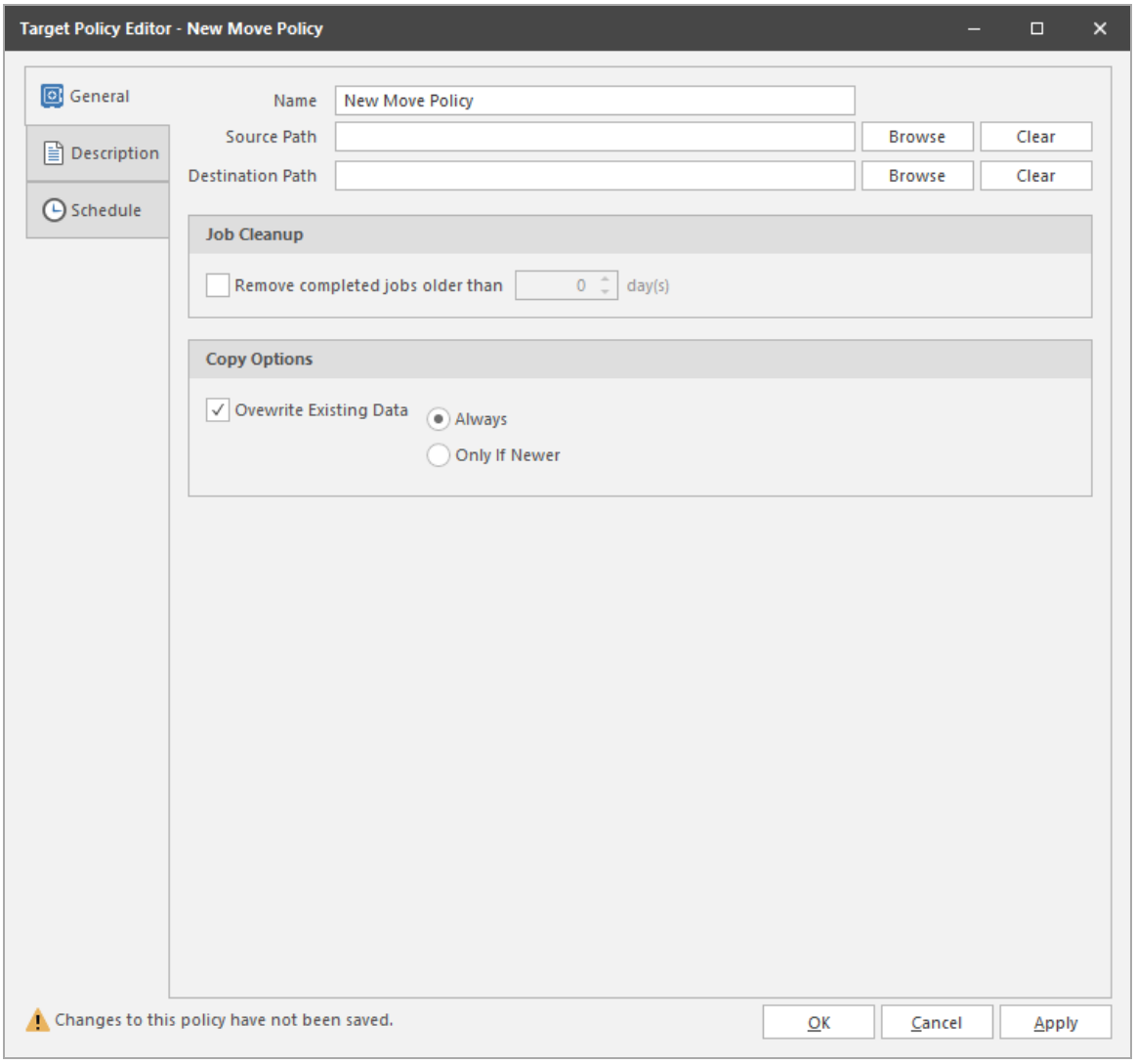
Displays the schedule for the Copy policy.

For procedures on scheduling a Copy policy, see *Create a Copy Policy (page 115)*.

Move Policy

A discussion of fields and settings specific to a Move policy follows.

Move Policy Page



General Tab

Name: Use this field to specify a name for the Move policy.

Source Path: Displays the location in the file system from where the files will be moved.

Destination Path: Displays the location in the file system where all moved files for this policy will be relocated.

Remove completed jobs older than: Lets you specify the number of days that a Move task from this policy is listed on the Jobs list before it is purged.

Overwrite Existing Data: With the default setting, File Dynamics will overwrite an existing file on the target destination only if the same file from the source location is newer. You can adjust this setting to your preferences.

Description Tab

The *Description* box indicates when the policy was created. It also lets you write notes pertaining to the policy. The *Description* box allows up to 255 characters.

Schedule Tab

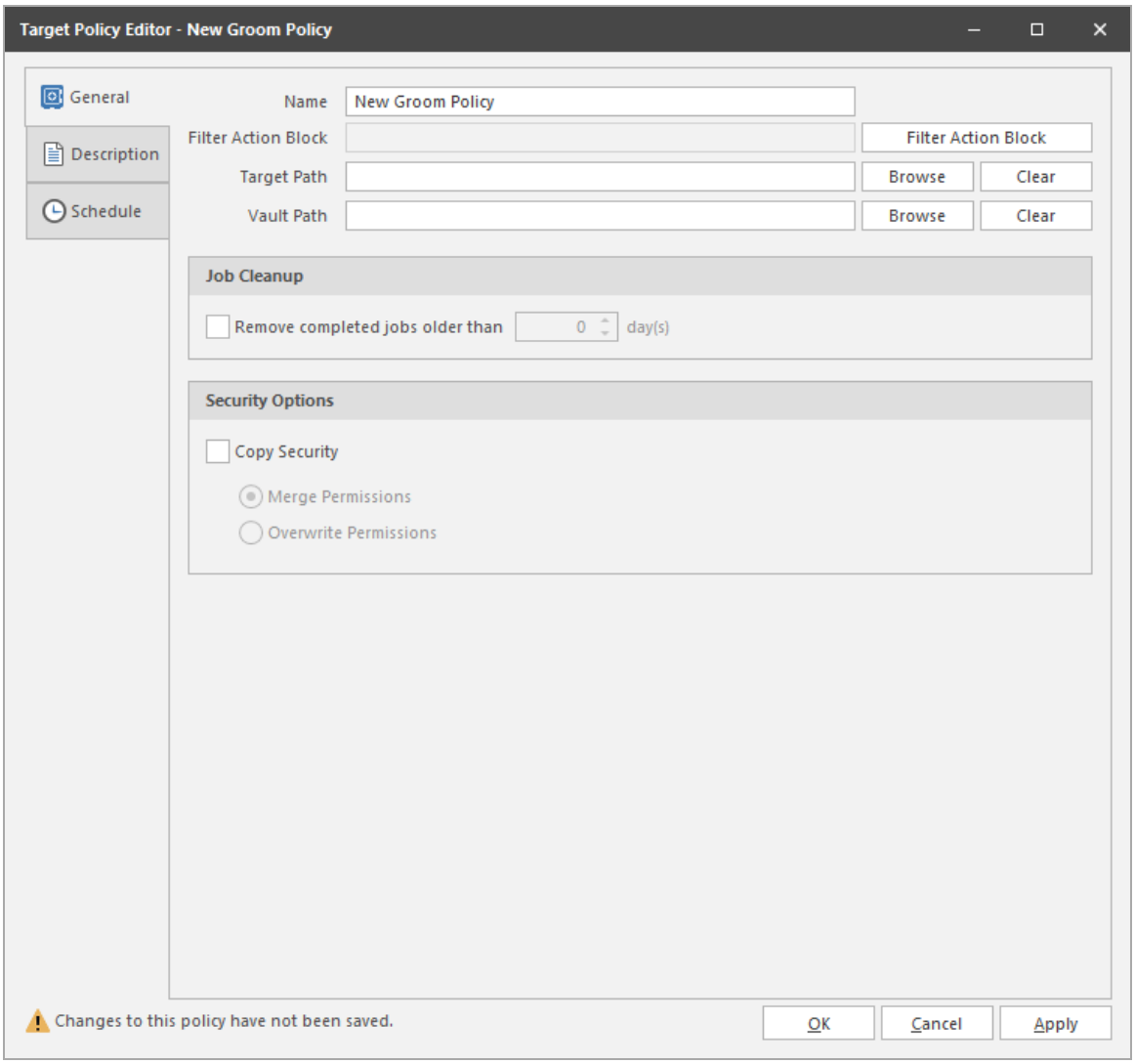
Displays the schedule for the Move policy.

For procedures on scheduling a Move policy, see *Create a Move Policy (page 119)*.

Groom Policy

A discussion of fields and settings specific to a Groom policy follows.

Groom Policy Page



General Tab

Name: Use this field to specify a name for the Groom policy.

Filter Action Block (field): Specifies the name of the Filter Action Block with the groom rule specifications for this policy.

Filter Action Block (button): Clicking this button brings up the Action Block Selector dialog box where you can select from all available Groom Rule Action Blocks.

Target Path: Displays the location in the file system where files will be groomed.

Vault Path: Displays the location in the file system where all groomed files for this policy will be relocated.

Remove completed jobs older than: Lets you specify the number of days that a Groom task from this policy is listed on the Jobs list before it is purged.

Copy Security: Selecting this check box will allow users to access groomed files from the new vault location.

- **Merge Permissions:** Merges permissions from the source to the target if the target contains permissions that are not present in the source. This applies to all folders and files in the source folder structure.
- **Overwrite Permissions:** Overwrites permissions in the target with those found in the source. This applies to all folders and files in the target folder structure.

Description Tab

The *Description* box indicates when the policy was created. It also lets you write notes pertaining to the policy. The *Description* box allows up to 255 characters.

Schedule Tab

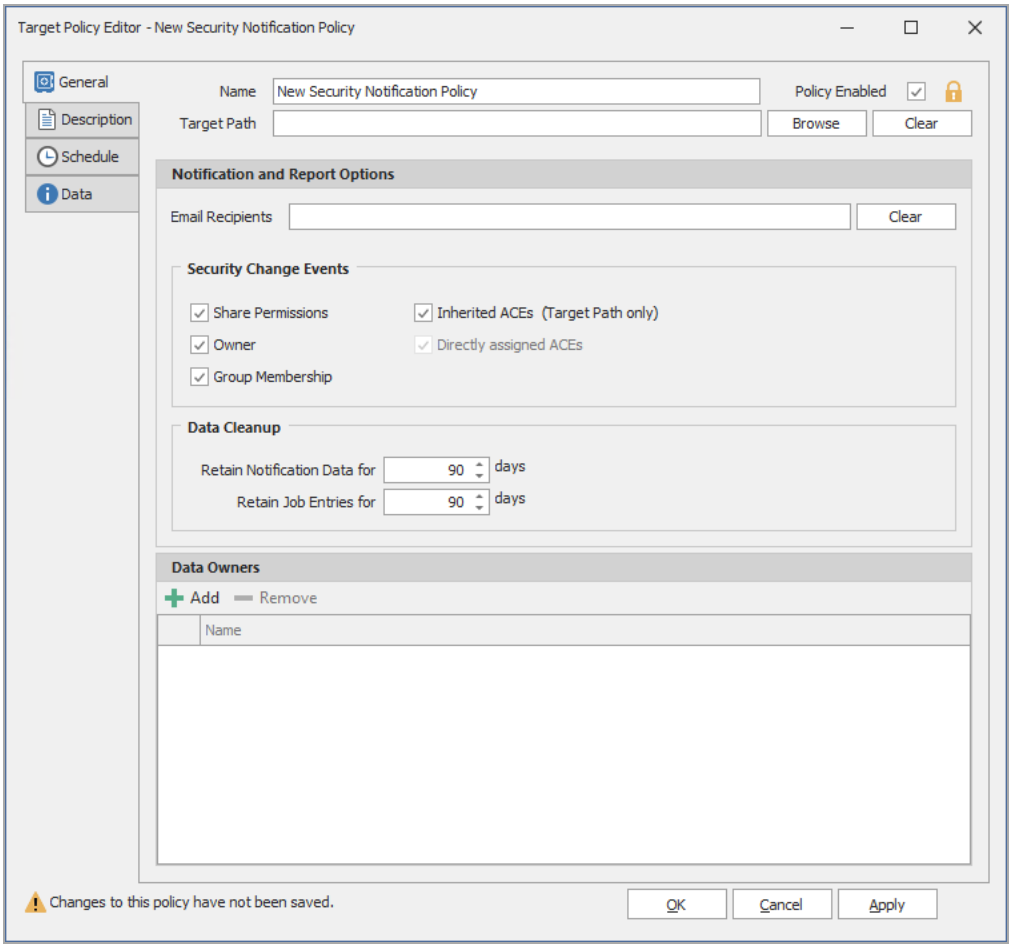
Displays the schedule for the Groom policy.

For procedures on scheduling a Groom policy, see *Create a Groom Policy (page 111)*.

Security Notification Policy

A discussion of fields and settings specific to a Security Notification policy follows.

Security Notification Policy Page



General Tab

Name: Use this field to specify a name for the Security Notification policy.

Target Path: Indicates the folder or share that will be analyzed for access permission changes.

Browse: Click to access the File System Browser where you can select the folder or share for the Security Notification policy.

Clear: Click to clear the path specified in the *Target* field.

Email Recipients: Specify the email addresses of each user you want notified when access permissions to the selected folder or share are changed. Email addresses can be separated by a comma, semicolon, or a space.

Clear: Click to clear the email addresses specified in the *Email Recipients* field.

Security Change Events: This region displays options for notifications. For example, if the *Group Membership* check box were selected, data owners would be notified whenever there was a change to a group that has access to the target path.

Data Cleanup: Options for specifying how long you want scan job information to remain in the database.

Retain Notification Data for: Lets you specify how long the Security Notification data will remain in the database.

Retain Job Entries for: Lets you specify how long you want scan job information to remain in the database. If you do not select the check box, the scan job stays in the database indefinitely.

Data Owners: This region lets you specify the data owners for the target path. The data owners will receive security notifications based on changes to the selected options in the *Security Change Events* region.

Description Tab

The *Description* box indicates when the policy was created. It also lets you write notes pertaining to the policy.

Schedule Tab

Displays the schedule for the Security Notification policy.

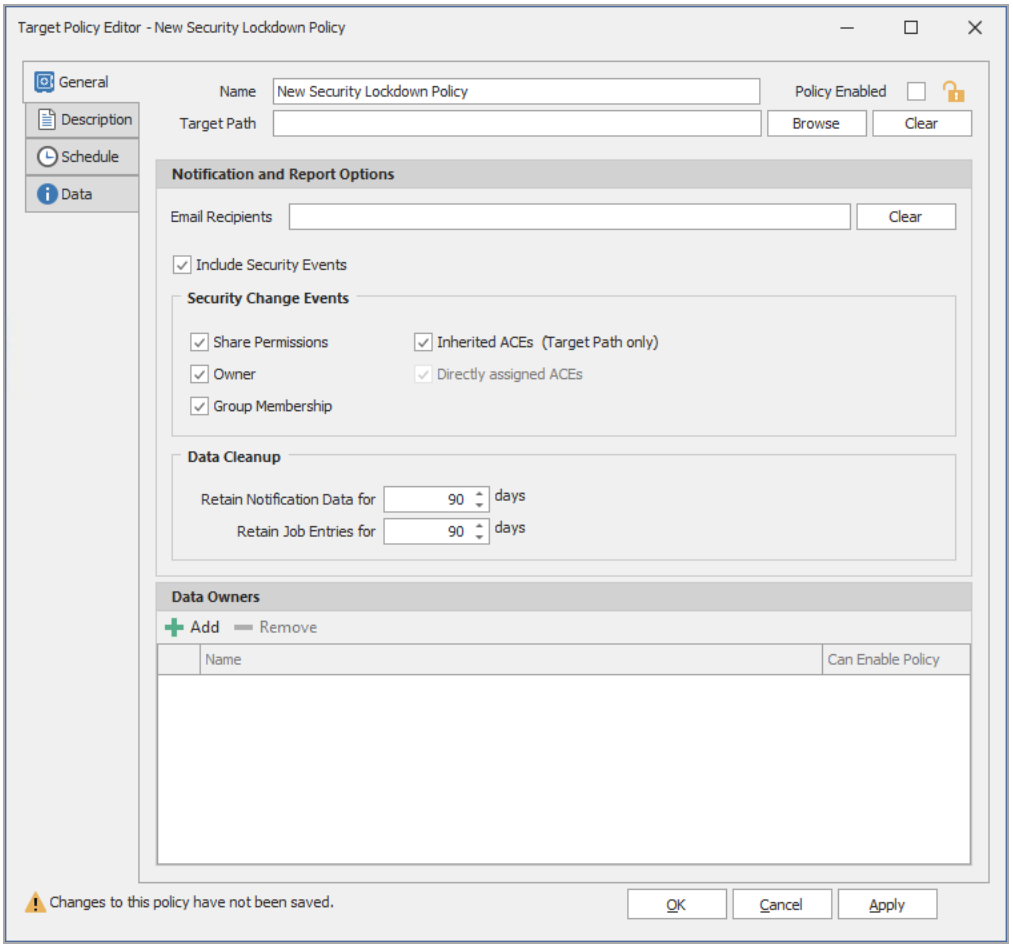
Data Tab

This page displays the properties of the CouchDB database.

Security Lockdown Policy

A discussion of fields and settings specific to a Security Lockdown policy follows.

Security Lockdown Policy Page



General Tab

Name: Use this field to specify a name for the Security Lockdown policy.

Policy Enabled: Once the access permissions to the specified target path are the permissions you want enforced, select this check box to enable the policy. Otherwise, come back and select the check box after you have updated the access permissions to the target path.

Target Path: Indicates the folder or share that will be analyzed for access permission changes.

Notification and Report Options: This region includes the settings specific to who is notified, what is reported, and how long the report information remains accessible.

Email Recipients: Specify the email addresses of each user you want notified when access permissions to the selected folder are changed (and subsequently reverted back through the Lockdown policy). Email addresses can be separated by a comma, semicolon, or a space.

Include Security Events: When this check box is selected, all specified recipients listed in the *Email Recipients* field will also receive security notifications according to the options

selected in the *Security Change Events* region. Deselecting this option limits the notifications to only changes in access permissions to the target path (and subsequently reverted via the Lockdown policy).

Security Change Events: This region displays options for notifications. For example, if the *Group Membership* check box were selected, data owners would be notified whenever there was a change to a group that has access to the target path.

Data Cleanup: Options for specifying how long you want scan job information to remain in the database.

Retain Notification Data for: Lets you specify how long the Security Lockdown data will remain in the database.

Retain Job Entries for: Lets you specify how long you want scan job information to remain in the database. If you do not select the check box, the scan job stays in the database indefinitely.

Data Owners: This region lets you specify the data owners for the target path.

Can Enable Policy: Select this option if you want the selected data owner to be able to enable the Lockdown policy

Description Tab

The *Description* box indicates when the policy was created. It also lets you write notes pertaining to the policy. The *Description* box allows up to 255 characters.

Schedule Tab

Displays the schedule for the Security Lockdown policy.

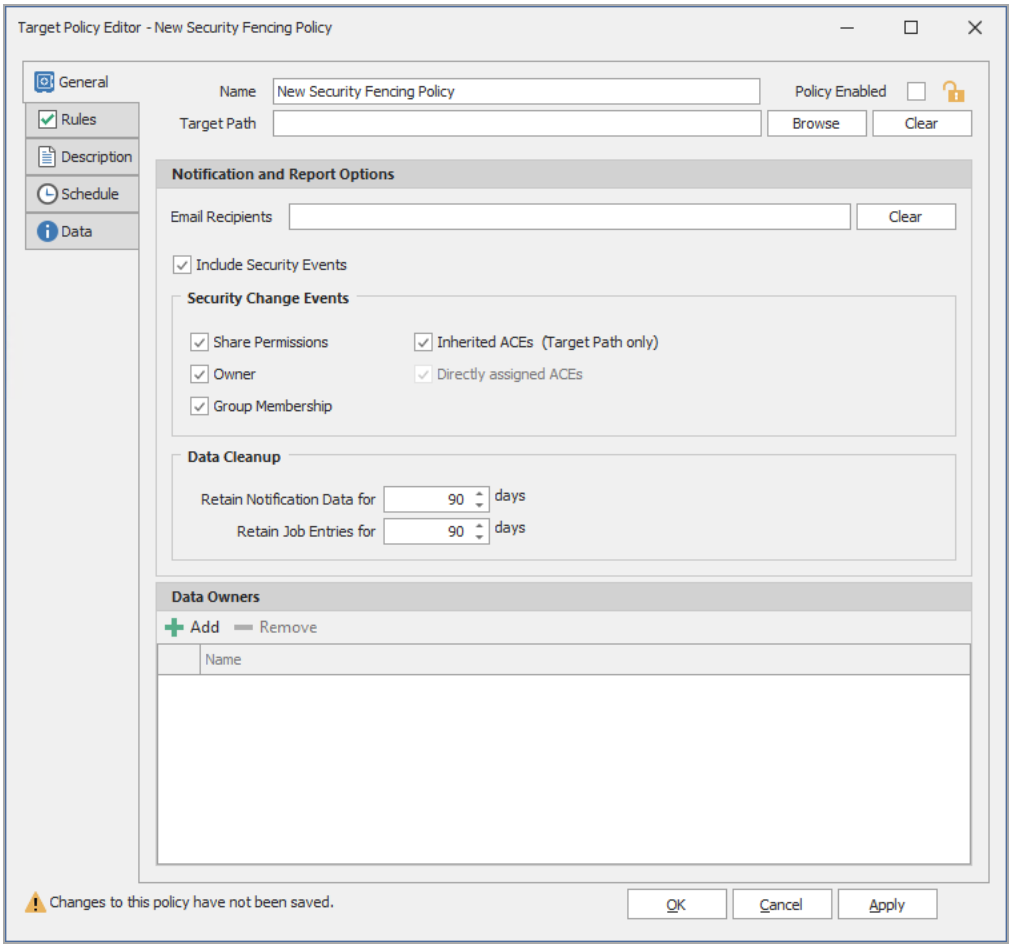
Data Tab

This page displays the properties of the CouchDB database.

Security Fencing Policy

A discussion of fields and settings specific to a Security Fencing policy follows.

Security Fencing Policy Page



General Tab

Name: Use this field to specify a name for the Security Fencing policy.

Policy Enabled: Once the access permissions to the specified target path are defined the way you want enforced, select this check box to enable the policy. Otherwise, come back and select the check box after you have updated the access permissions to the target path.

Target Path: Indicates the folder or share that will be analyzed for access permission changes.

Notification and Report Options: This region includes the settings specific to who is notified, what is reported, and how long the report information remains accessible.

Email Recipients: Specify the email addresses of each user you want notified when access permissions to the selected folder are changed. Email addresses can be separated by a comma, semicolon, or a space.

Include Security Events: When this check box is selected, all specified recipients listed in the *Email Recipients* field will also receive security notifications according to the options

selected in the *Security Change Events* region. Deselecting this option limits the notifications to only changes in access permissions to the target path.

Security Change Events: This region displays options for notifications. For example, if the *Group Membership* check box were selected, data owners would be notified whenever there was a change to a group that has access to the specified target path or one of its subfolders.

Data Cleanup: Options for specifying how long you want scan job information to remain in the database.

Retain Notification Data for: Lets you specify how long the Security Fencing data will remain in the database.

Retain Job Entries for: Lets you specify how long you want scan job information to remain in the database. If you do not select the check box, the scan job stays in the database indefinitely.

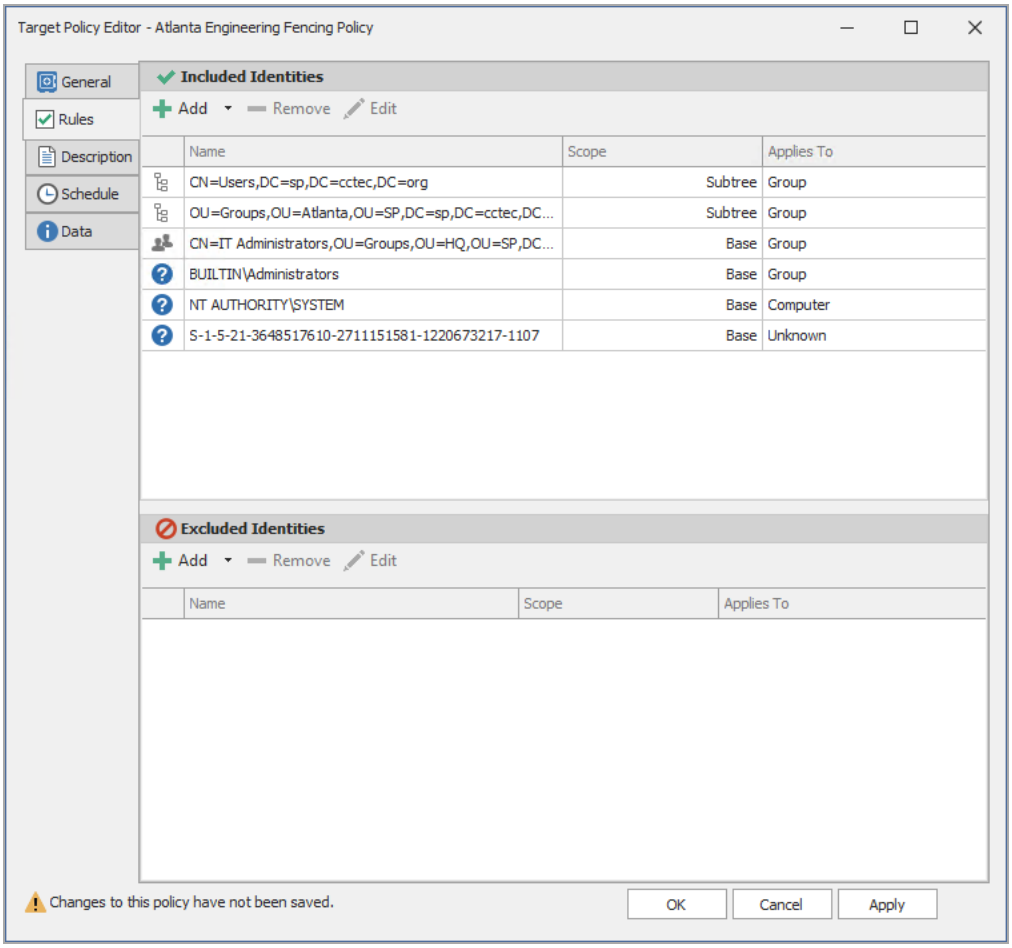
Data Owners: This region lets you specify the data owners for the target path.

Rules Tab

On this page, you specify the policy's "fence" for inclusion and exclusion. A Security Fencing policy can be very detailed in its inclusion and exclusions. For example, you can include an Active Directory container, but exclude a group within the container. Additionally, your list for inclusion or exclusion can specify unresolved or well-known Security Identifiers (SIDs). In many cases, you will need to include unresolved or well-known SIDs, or the policy will prevent access for those identities.

You can access a list of Windows well-known SIDs at: https://learn.microsoft.com/en-US/windows-server/identity/ad-ds/manage/understand-security-identifiers.

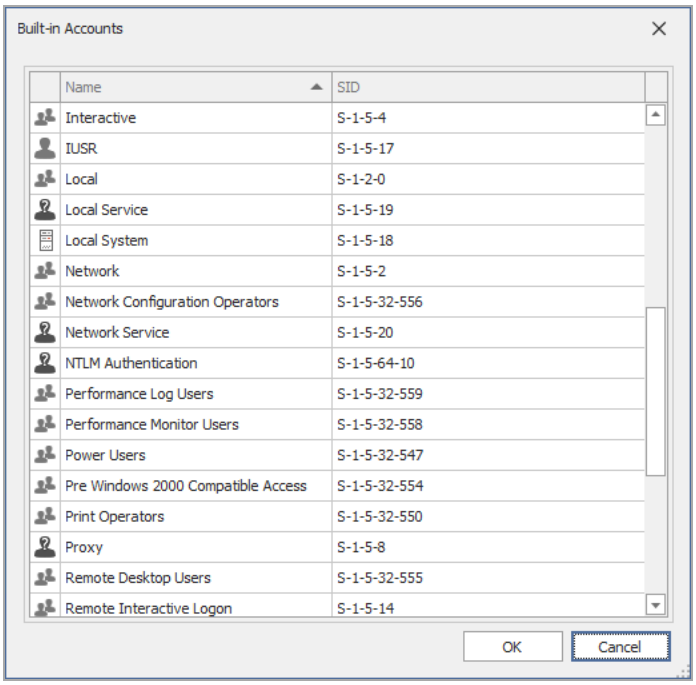
Security Fencing Policy Rules Page



In the graphic above, the *Included Identities* list displays containers, groups, well-known and unresolved SIDs.

To Add or Exclude a Well-Known SID as a Built-in Account

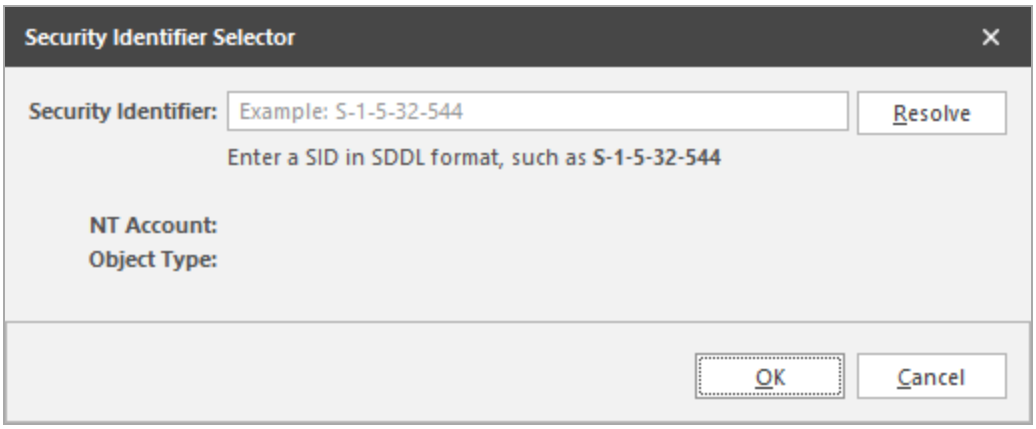
1. In the *Included Identities* or *Excluded Identities* region, from the *Add* drop-down menu, select *Built-in Accounts*.



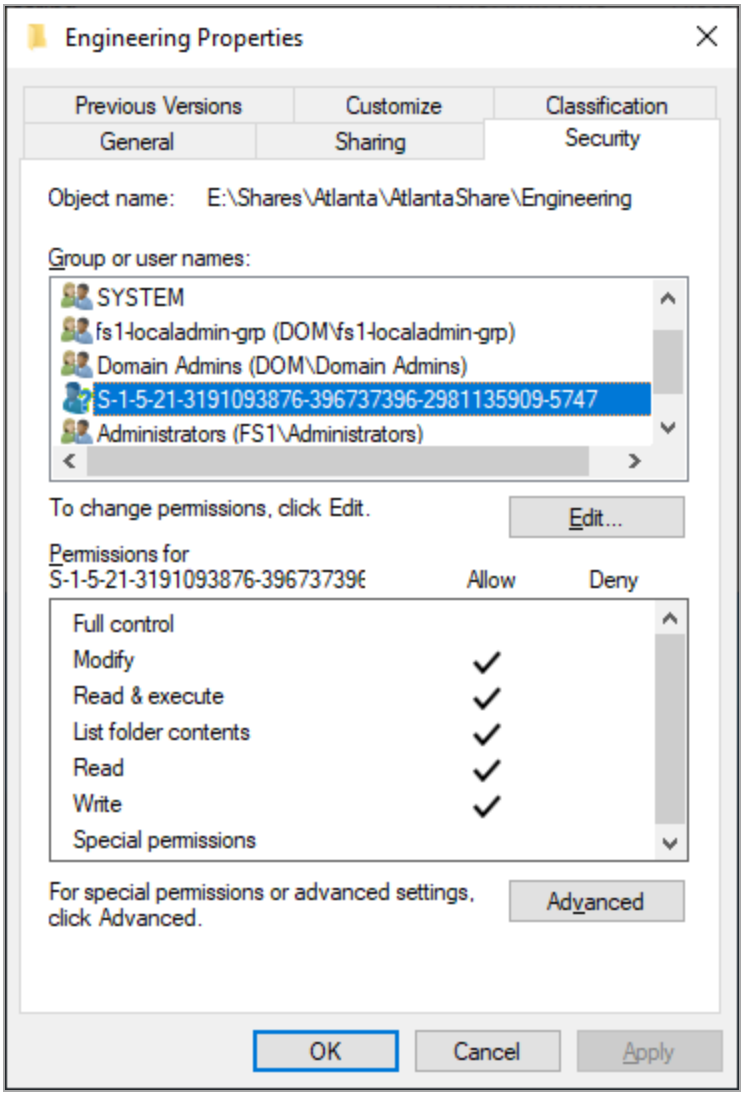
2. Hold down the Control key and select the Built-in SIDs.
3. Click *OK*.

To Add or Exclude an Unknown SID

1. In the *Included Identities* or *Excluded Identities* region, from the *Add* drop-down menu, select *Add Security Identifier*.

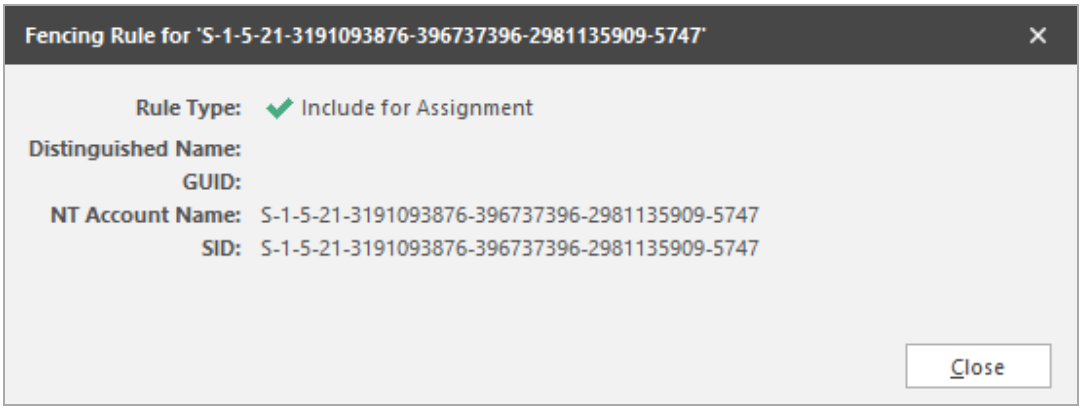


2. Refer to the unresolved SID listed on the *Security* tab of the Properties dialog box.



3. In the *Security Identifier* field of the Security Identifier Selector dialog box, enter the SID in SDDL format and click *Resolve*.

4. Click *OK*.



Included Identities: Use to display, add, and remove objects for inclusion in the Security Fencing policy.

Excluded Identities: Use to display, add, and remove for exclusion in the Security Fencing policy.

Description Tab

The *Description* box indicates when the policy was created. It also lets you write notes pertaining to the policy. The *Description* box allows up to 255 characters.

Schedule Tab

Displays the schedule for the Security Fencing policy.

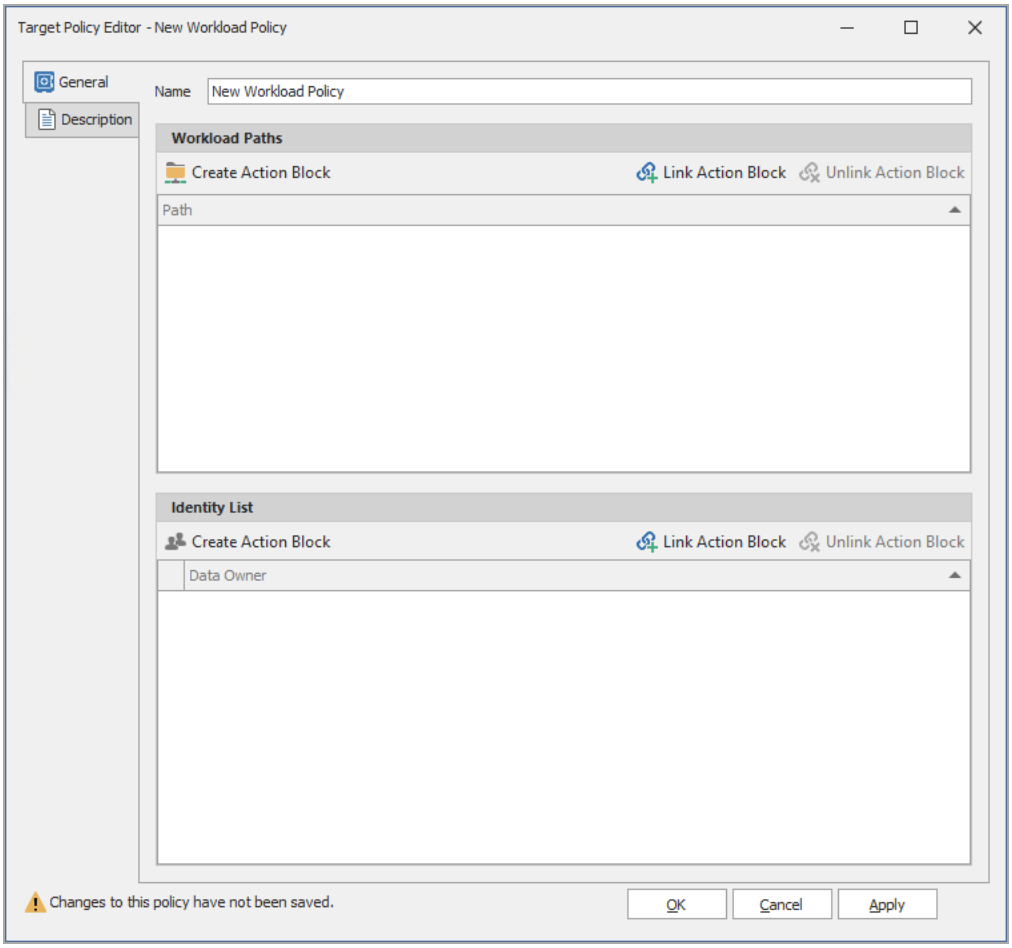
Data Tab

This page displays the properties of the CouchDB database.

Workload Policy

A discussion of fields and settings specific to a Workload policy follows.

Workload Policy Page



General Tab

Name: Use this field to specify a name for the Workload policy.

Workload Paths: This region displays the Workload path for this policy, as well as provides the means of linking, unlinking, and viewing Action Blocks pertaining to the path.

Paths: Displays the selected Action Block for this Workload policy.

Link Action Block: Lets you specify an Action Block for this policy.

Unlink Action Block: Removes a selected Action Block from the *Path* list.

Action Block Editor Link: Located in the upper right-hand corner of the *Workload Paths* region, clicking this opens the Action Block Editor dialog box and lets you add new Workload paths.

Identity List: This region displays the Data Owners for the policy, as well as provides the means of linking, unlinking, and viewing Data Owners pertaining to the Workload policy.

Data Owner: Displays the Data Owners for this policy.

Link Action Block: Lets you specify an Action Block for this policy. This will display the Data Owners specified in the Action Block.

Unlink Action Block: Removes the listed Data Owners.

Data Owners Link: Located in the upper right-hand corner of the *Identity List* region, clicking this opens the Action Block Editor dialog box where you can edit the list of Data Owners for this policy.

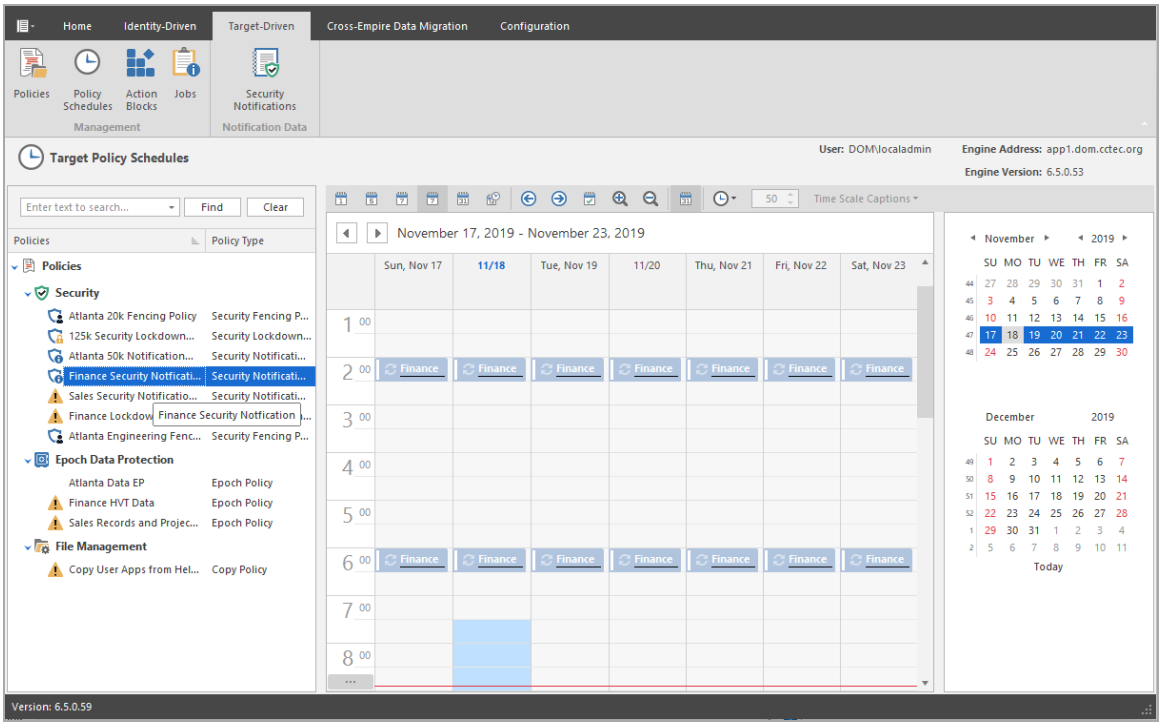
Description Tab

The *Description* box indicates when the policy was created. It also lets you write notes pertaining to the policy. The *Description* box allows up to 255 characters.

11.3.2 - Policy Schedules

Use this page to view and schedule all Target-Driven policy schedules.

Schedule Page



Left Pane: This region displays all Target-Driven policies according to classification. If you click a classification such as *Groom*, only scheduled Groom policies will be displayed on the calendar in the Middle Pane. If you click a named Target-Driven policy such as *Main Groom Policy for Atlanta Users*, the schedule for that policy appears in the calendar of the Middle Pane.

You can right-click a listed policy in the Left Pane to create new schedules, edit, schedules, and delete schedules.

A search field at the top of the Left Pane lets you search for policies by name.

Middle Pane: This calendar displays scheduled Target-Driven policy actions. You can display the calendar as a single day, 5-day week, 7-day week, or as a month using the calendar number icons above the Middle Pane.

The icons above the Middle Pane also allow you to edit the schedule, move through the calendar, zoom in or out, group scheduled tasks, and change the time scales and captions.

Right Pane: This region displays a monthly calendar for the current and next month, which you can change using the arrows. Clicking a date adjusts the calendar in the Middle Pane to the selected date.

For procedures on scheduling a Target-Driven policy, see *Creating Target-Driven Policies (page 109)*.

11.3.3 - Action Blocks

You can use this page to locate and create Filter Action Blocks that can be used in Target-Driven policies.

Double-clicking a selected Filter Action Block brings up the Action Block Editor where you can view specific details about the Filter Action Block, edit rules, and more.

Manage: This menu lets you create, edit, rename, or delete a Filter Action Block.

For procedures on creating a Filter Action Block, see *Creating a Filter Action Block (page 180)*.

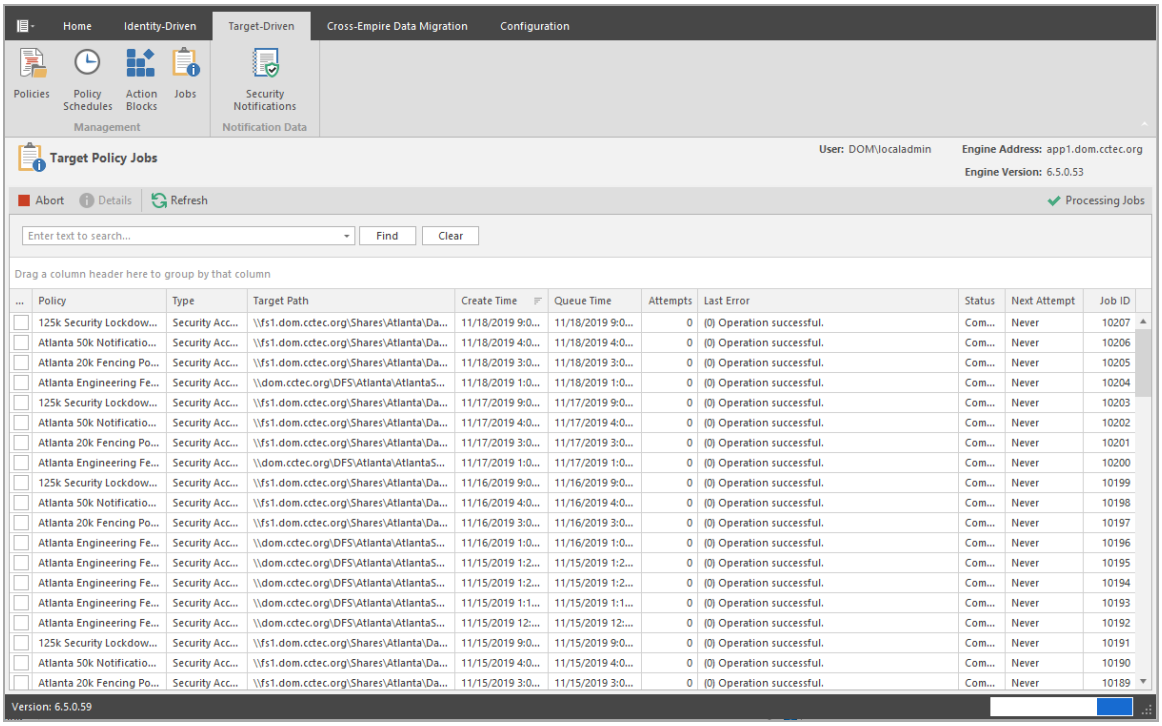
Search: Clicking this provides a new field for locating a Filter Action Block. Enter a search string in the field and click *Find*.

Refresh: Updates the list of Filter Action Blocks.

11.3.4 - Jobs

This page provides details on all Target-Driven jobs that have taken place or are pending.

Jobs Page

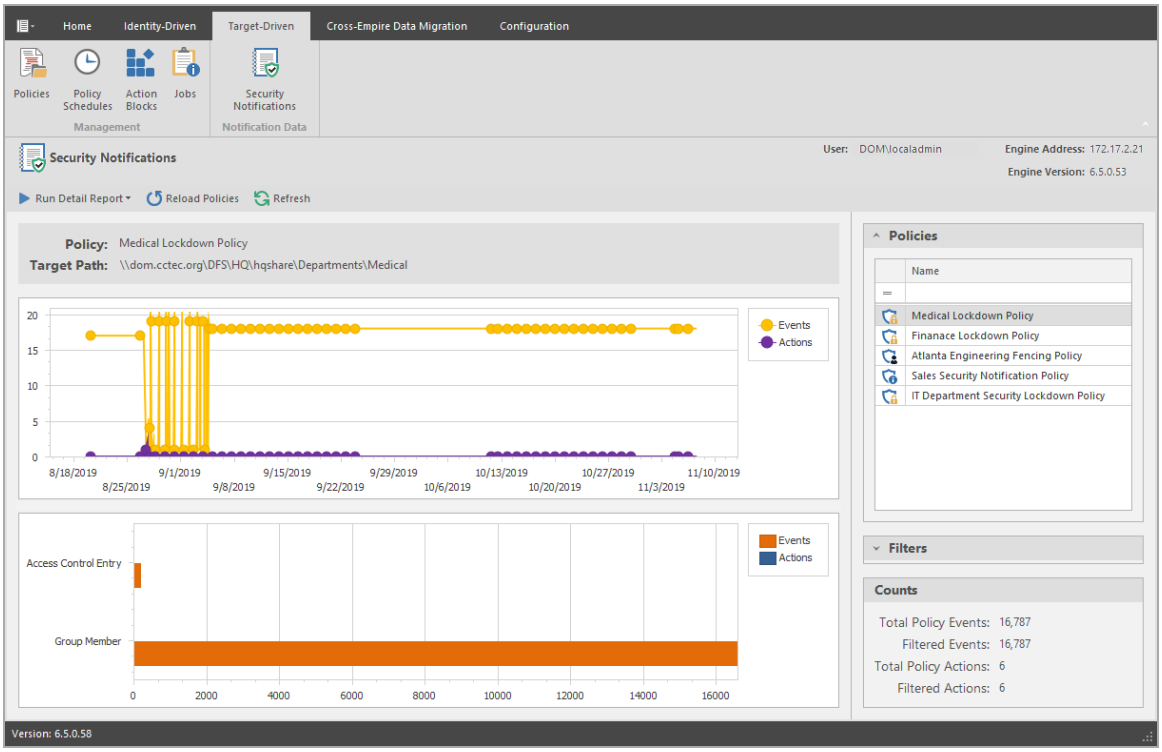


The page lists completed and pending jobs. You can maximize the list by clicking the *Maximize* icon in the upper right corner of the *Jobs* region.

11.3.5 - Security Notifications

This page provides a graphical summary of changes in security access permissions and group memberships for high-value targets managed through security policies. Using the information you ascertain from the graphs, you can in-turn run a Detail Report to view the details of the changes.

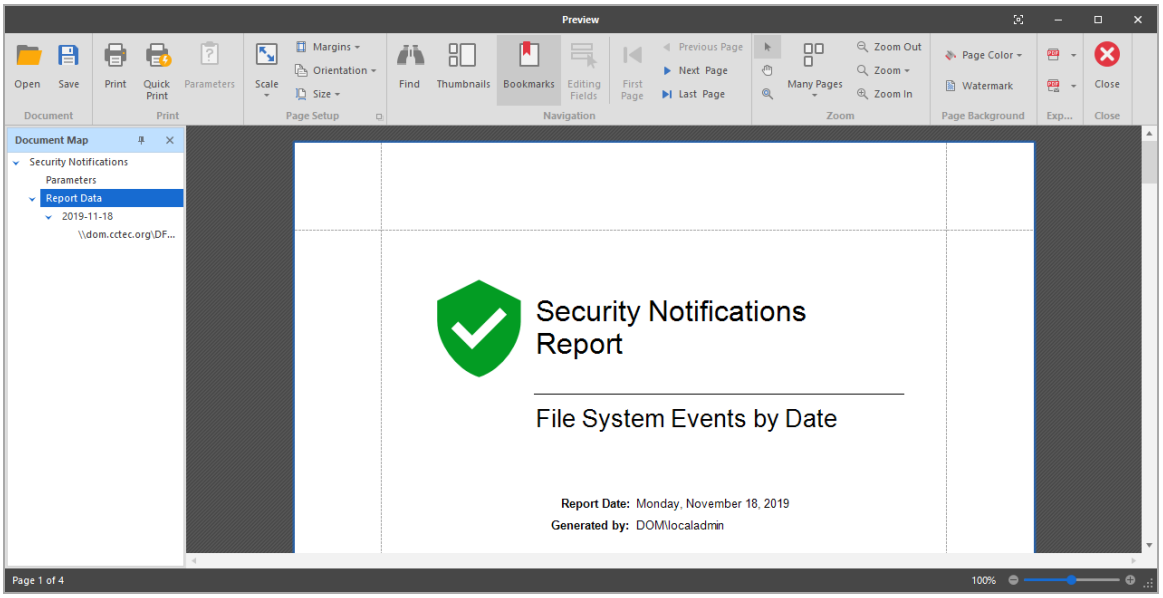
Security Notifications Page



Run Detail Report: This drop-down menu is the means of generating detail reports for either file system events or group membership events. Reports are generated according to the selected policy, filter settings, and date range settings located on the right-hand portion of the page.

Reports are first generated in preview mode, where they can then be saved in a number of different format types.

Sample File Systems Event Report



Reload Policies: Adds to the list of policies, any new security policies that have been created since the Security Notification page was opened.

Refresh: Refreshes the Security Notifications page.

Upper Graph: According to the specifications on the right-hand side of the page, displays a graph of the number of events and actions in a timeline from the first security scan, to the most recent. Placing the pointer on lines of the graph provides additional numerical information.

Lower Graph: According to the specifications on the right-hand side of the page, displays a graph of the totals for the specified data range.

Policies: Select from this list to display the policy-specific data in the graphs and in the Detail Report.

Filters: Lets you specify what criteria and date range to include in the graphs and in the Detail report.

Counts: Based on the selected policy, criteria, and date range, displays the total count of policy events, filtered events, policy actions, and filtered actions.

11.4 - Configuration Tab

Use this page to establish configurations and set preferences for an extensive set of File Dynamics tools.

General Preferences (page 234)

Global Statistics Configuration (page 236)

Work Log Configuration (page 240)

Target-Driven Configuration (page 242)

Client Preferences (page 243)

11.4.1 - General Preferences

This page lets you view and set Engine configuration settings.

General

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

The General Tab of the Configuration Page

Proxy Rights Group: Displays the Proxy Rights Group that you established when you installed File Dynamics.

Admin Users Group: Displays the Admin Users Group that you established during the installation of File Dynamics.

HTTPS Port: Displays the HTTPS port that you chose when you installed File Dynamics.

HTTP Port: If you chose to use an HTTP port during the installation of File Dynamics, the HTTP port is displayed here.

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

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.

Reapply Rights: Clicking this button reestablishes the ability of the Proxy Rights group to manage the Proxy home share. It also reestablishes the group Everyone with the Read right so that its members can read contents. The Read right is needed in case the Proxy home share is being used as the managed path attribute while storage is being moved.

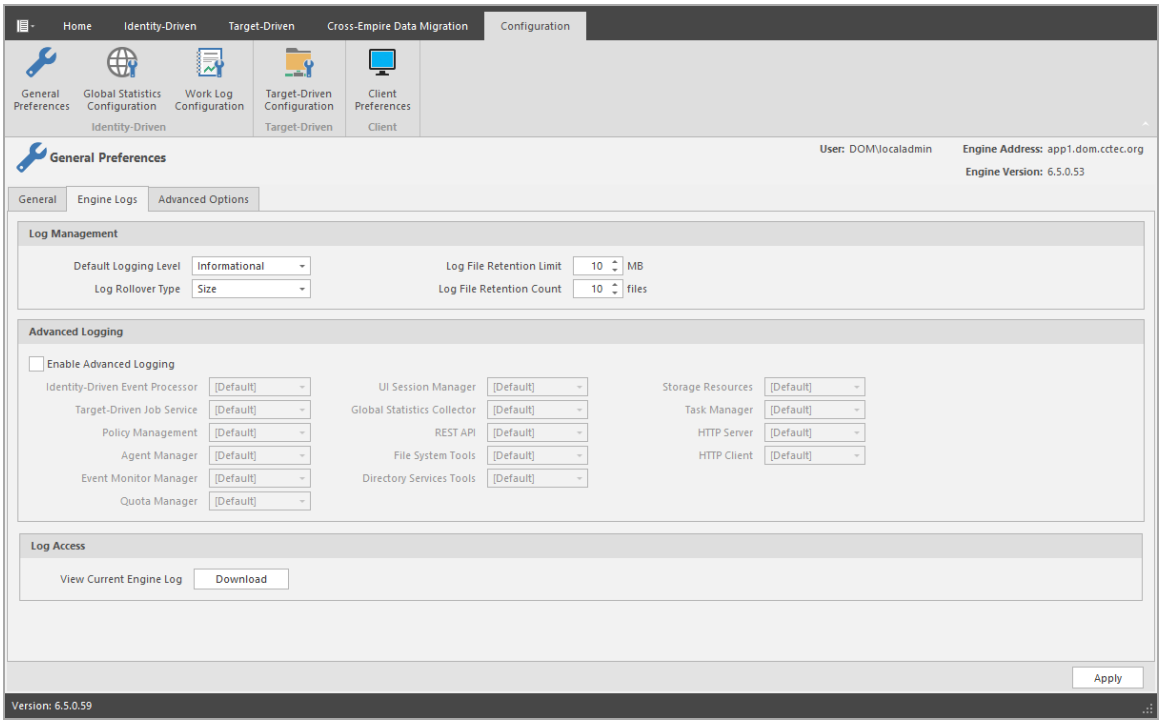
Copy Template: Clicking this button recopies default proxy home template files to the location specified by the share.

Engine Logs

The *Engine Logs* tab includes settings specific to log files.

Each of the fields is described below.

The Engine Logs Tab of the Configuration Page



Default Logging Level: By default, the log records warning 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 Limit: This field appears only when you select *Size* from the *Log Rollover Type* field. You need to enter the size limit in MB for the log file before it creates a new file.

Log 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.

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.

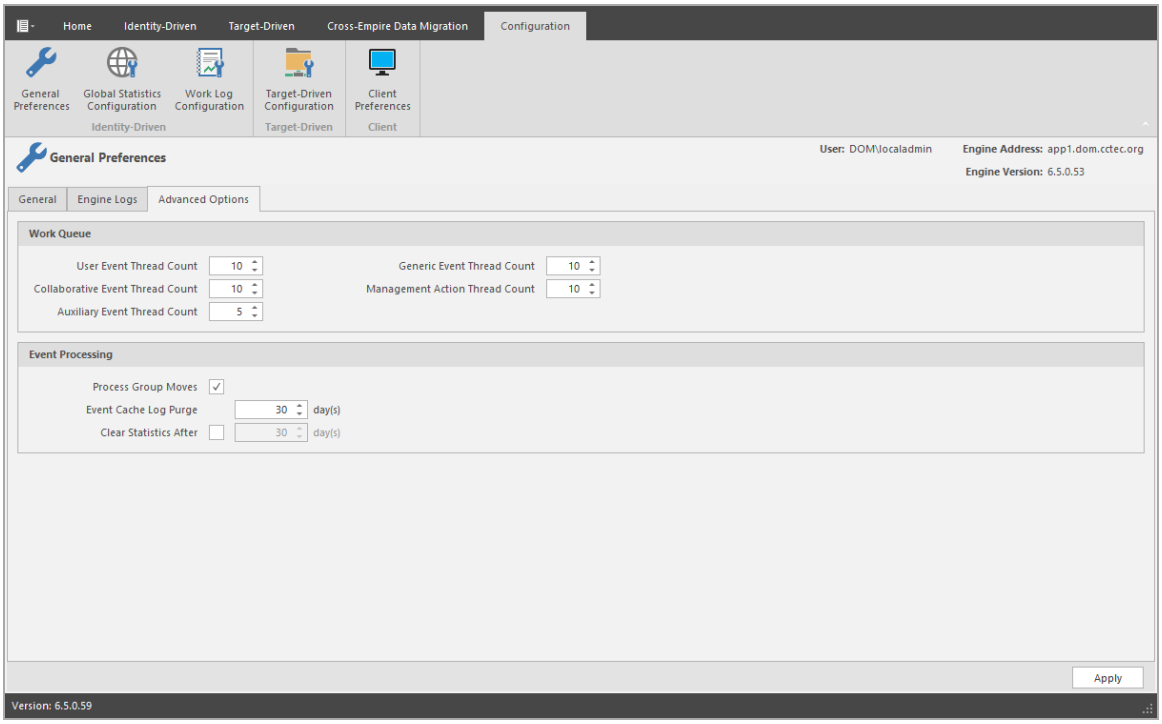
Log File Retention Count: By default, File Dynamics retains the 10 most recent log files, according to the *Log Rollover Type* setting. For example, if the *Log Rollover Type* setting is set to *Daily*, the retained log files are from the last 10 days.

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 13 categories.

Advanced Options

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

The Advanced Options Tab of the Configuration Page



Work Queue: These settings are optimized for a normal File Dynamics workload.

Process Group Moves: Click this box to enable File Dynamics to move collaborative storage.

'**Event Cache Log Purge:** By default, File Dynamics 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.

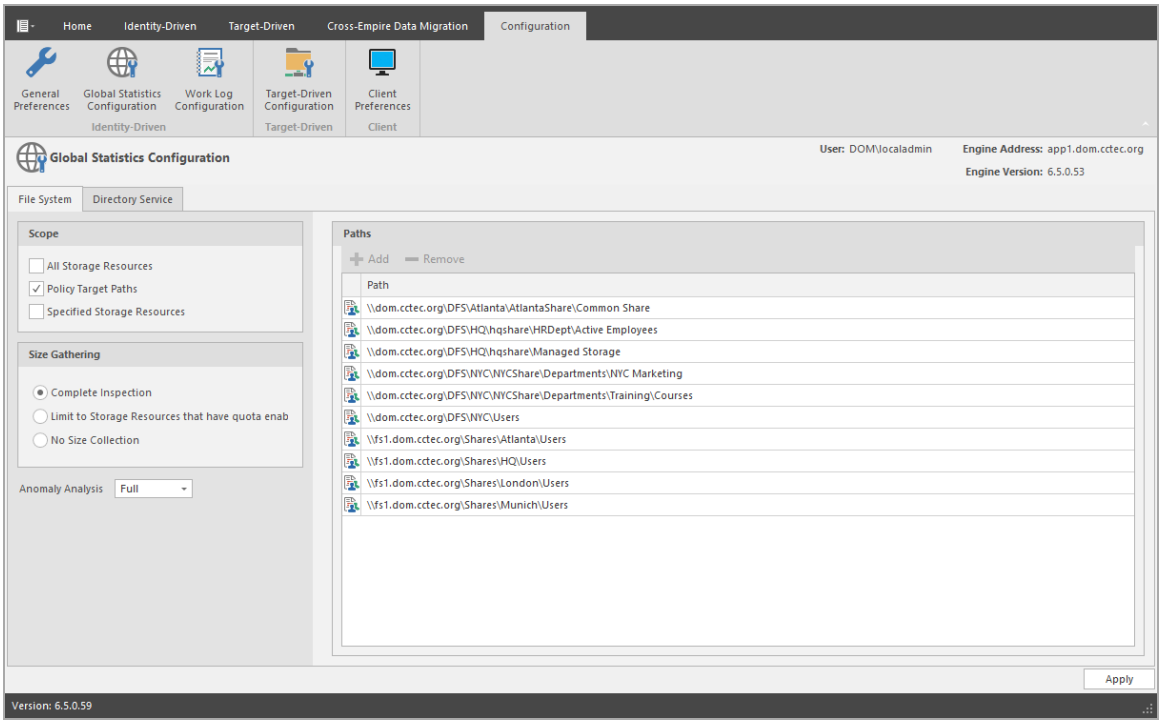
Clear statistics after: This option specifies how long statistics are kept for the graphs displayed on the Statistics page.

11.4.2 - Global Statistics Configuration

The default configuration of the GSR Collector forces it to behave in a manner consistent with legacy versions of the product. However, it is not optimal for most deployments.

The GSR Collector can be scoped by file system and directory service parameters.

File System Configuration Settings for the GSR Collector



File System Tab

Scope: The file system scope provides the means for you to determine which shares should be scanned by the GSR Collector. The file system scopes are:

- **All Storage Resources:** This is the default option and mutually exclusive of *Policy Target Paths* and *Specified Storage Resources*. This will cause the GSR Collector to scan the root of all shares that appear in Storage Resources for size and anomaly data. This can take a significant amount of time to complete depending on the share type, contents, and the chosen *Size Gathering* option. In large environments, this is not the recommended configuration.
- **Policy Target Paths:** This option can be checked separately or combined with *Specified Storage Resources* for greater flexibility. This will cause the GSR Collector to only scan paths defined as policy target paths for size and anomaly data. After you have your storage managed by policy, use this option to limit the scope and provide meaningful size and anomaly analysis data for the storage resources that matter most.
- **Specified Storage Resources:** This option can be checked separately or combined with *Policy Target Paths* for greater flexibility. This will cause the GSR Collector to only scan paths defined by you for size and anomaly data. When running the GSR Collector for the first time, this option serves as the best choice because it allows you to target specific paths and storage resources.

Size Gathering: The size gathering options allow you to control the method by which aggregate size data for global statistics and policy-based path redistribution is collected.

- **Complete Inspection:** This is the default option. To collect size data, folders are checked for quota. If quota is determined to be supported by the hosting server and the folder has a quota, FSRM is queried to obtain the relevant data. In the case where the folder does not have a quota managed by FSRM or it simply has no quota at all, the folder is traversed to collect size data of all files.
- **Limit to Storage Resources that have quota enabled:** If quota is determined to be supported by the hosting server and the folder has a quota, FSRM is queried to obtain the relevant data. The folder must have a quota set to eliminate brute force enumeration to collect size data.
- **No Size Collection:** No size data collection is attempted.

Anomaly Analysis: The file system anomaly analysis provides the means for you to determine the level of anomaly analysis. The options are:

- **None:** Anomaly analysis will not be performed.
- **Simple:** This is the default option and sufficient for most purposes. The following anomalies are reported:
    - **Attribute Value Missing:** The respective path attribute (e.g. home folder) does not have a value.
    - **Path Missing On Disk:** The respective path attribute value cannot be found on disk.
    - **Path Validation Issue:** Attempting to retrieve or verify the existence of the respective path attribute value failed.
    - **Name Mismatch:** The respective leaf path value does not match the object's name value.
    - **Path Mismatch:** The respective path attribute value does not match the last known managed path database entry.
    - **DS Path Duplicate Value:** Two or more objects have been detected that contain the same path for the respective path attribute.
    - **DS Path Crosstalk Parent:** The object's respective path attribute has been detected as being the parent of another object's path attribute.
    - **DS Path Crosstalk Child:** The object's respective path attribute has been detected as being the subordinate of another object's path attribute.
    - **Orphan Path Candidate:** The path is directly subordinate to a path at which other DS-associated paths have been found, but has not been detected as being associated with any DS object via a path attribute.
- **Full:** Reports additional policy related anomalies.
    - **Policy Not Found:** The respective auxiliary policy attribute entry references an auxiliary policy that was not found in the database.
    - **Policy Object Not Managed:** Effective policy calculations indicate that a policy is effective for the respective object and path type, but the object is not known to be managed.

- **Policy Mismatch:** The respective path is indicated as being managed in the database, but the policy under which it is currently managed does not match what effective policy calculation indicates it should be.
- **Policy Validation:** An error occurred while attempting to calculate effective policy for the object and respective path type.

Directory Service Tab

Container Scope: The directory service container scope provides the means for you to determine which containers should be enumerated by the GSR Collector for Anomaly Analysis, Global Statistics, and History. The container scopes are:

- **All Containers:** This is the default option and mutually exclusive of *Policy Associated Objects* and *Specified Containers*. This will cause the GSR Collector to enumerate all object types specified by the Object Scope for size and anomaly data.
- **Policy Associated Objects:** This option can be checked separately or combined with *Specified Containers* for greater flexibility. This will cause the GSR Collector to only enumerate and evaluate objects that are associated to policies. After you have your objects managed by policy, use this option to limit the scope and provide meaningful anomaly analysis data for the objects that matter most.
- **Specified Containers:** This option can be checked separately or combined with *Policy Associated Objects* for greater flexibility. This will cause the GSR Collector to only enumerate and evaluate objects defined by you for size and anomaly data. When running the GSR Collector for the first time, this option serves as the best choice because it allows you to target specific objects for analysis.

The containers specified in the container scope are searched recursively for object types configured in the Object Scope.

Object Scope: The directory service object scope provides the means for you to determine which object types and path types should be enumerated by the GSR Collector for Anomaly Analysis, Global Statistics, and History. The object scopes and path types are:

- Users
  - Home Folder
  - Profile Path
  - Remote Desktop Services Home Folder
  - Remote Desktop Services Profile Path
  - Auxiliary (ccx-FSFAuxiliaryStorage)
- Groups – Collaborative managed path (ccx-FSFManagedPath)
- Containers – Collaborative managed path (ccx-FSFManagedPath)

GSR Collector Configuration Scenarios

Configuration scenarios for the GSR Collector are detailed in the sections below.

All Storage Resources + Complete Inspection

This default configuration will cause the GSR Collector to enumerate all shares found in Storage Resources. During the enumeration, child folders at the root of shares are inspected for anomaly analysis and checked to determine if they have a quota applied to them via File Server Resource Manager (FSRM). If they have a quota, FSRM is queried to obtain it. In the case where a server hosting a share does not support quota (e.g. FSRM is not installed, the server is a NAS device) a brute force enumeration of the child directories is performed to collect size data for statistics and policy-based storage redistribution. Depending on the number of directories and their contents, this is a time consuming and resource intensive operation. While it ensures that all of the available shares are scanned, it is not the most efficient use of the GSR Collector.

All Storage Resources + Limited to Storage Resources that Have Quota Enabled

This configuration will cause the GSR Collector to enumerate all shares found in Storage Resources. During the enumeration, child folders at the root of shares are inspected for anomaly analysis and checked to determine if they have a quota applied to them via FSRM. If they have a quota, FSRM is queried to obtain it. This configuration is more efficient than Complete Inspection. However, if you have folders that do not have quota, there will be size data missing from Global Statistics and Policy-based Path Redistribution that would skew your results.

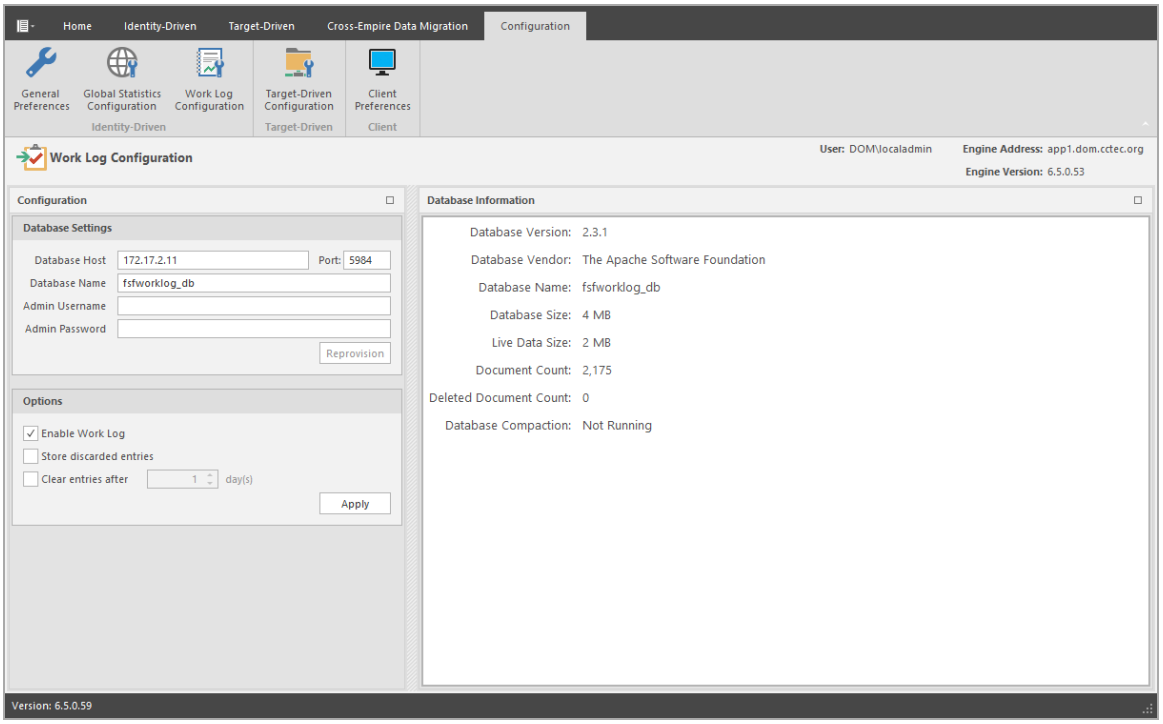
All Storage Resources + No Size Collection

This configuration will cause the GSR Collector to skip enumeration of all shares found in Storage Resources for size related data. If Global Statistics are not needed on a regular basis or you have a need for finer granularity in your historical data, this option may be best suited for your goals. However, if you choose this option, there will be no size data to drive Global Statistics and Policy-based Path Redistribution.

11.4.3 - Work Log Configuration

This page lets you establish the Work Log Database Settings in the Admin Client. For detailed procedures, see *Establishing the Work Log Database Settings in the Admin Client (page 144)*.

Work Log Configuration Page



Database Settings: Fields in this region are specific to the CouchDB database.

For information on setting up the CouchDB database, see Installing CouchDB.

Database Host: Specifies the IP address or DNS hostname of the server hosting the CouchDB database.

Port: Specifies the port number utilized by the CouchDB database.

The default number is 5984.

Database Name: The established name for the CouchDB database instance for the Work Log.

Admin Username: The administrator username you established when you installed the CouchDB database.

Admin Password: The password you established when you installed the CouchDB database.

Reprovision: Once you have entered the username and password, clicking this button re-provisions the user and database for the Work Log.

Options: Fields in this region are specific to the File Dynamics Work Log.

Enable Work Log: Once this option is selected, events will be recorded as entries in the Work Log.

Store Discarded Entries: Store Work Log entries for events where no action is ultimately taken, such as a user created outside the scope of any policy.

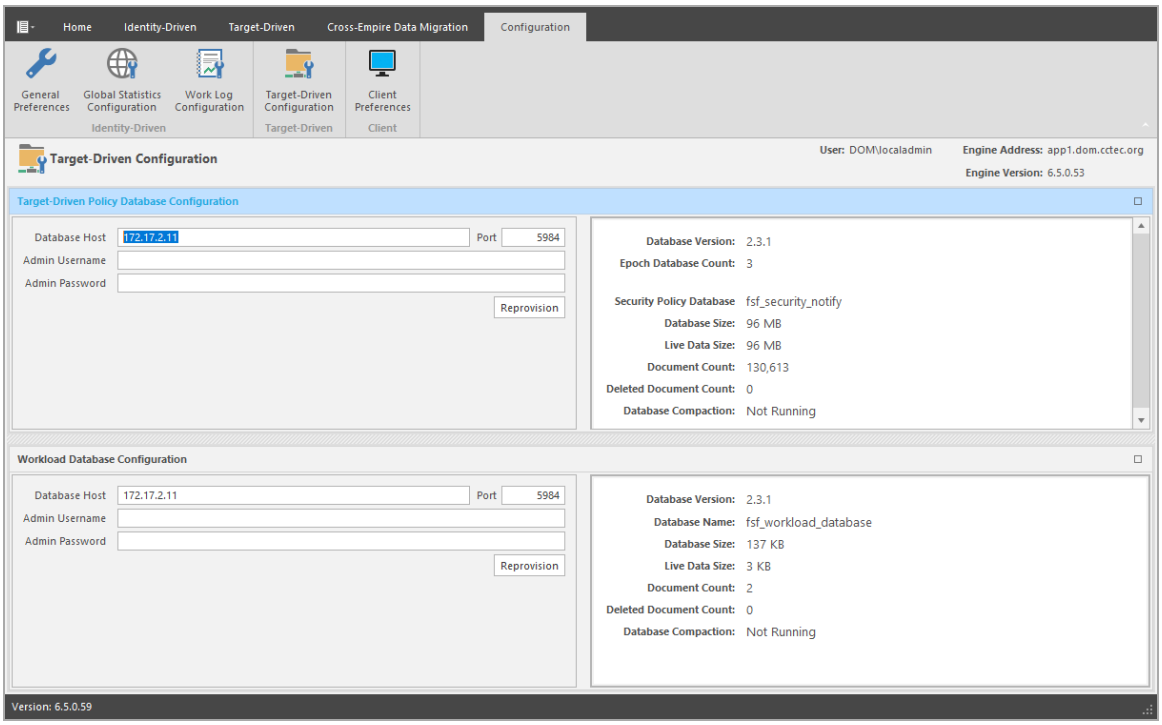
Clear Entries After: Select this option to specify the number of days before an entry is cleared. Once cleared the entry will not be listed in the Work Log.

Apply: Click to apply the settings in the *Options* region.

11.4.4 - Target-Driven Configuration

Use this page to establish the CouchDB database settings for all security-based Target-Driven policies, as well as for Workload policies.

Target-Driven Configuration Page



Target-Driven Policy Database Configuration: This region is specific to the CouchDB database instance for security-based Target-Driven policies.

Database Host: Enter the IP address or DNS host name or the server hosting CouchDB.

Port: Set the port address to `5984`.

Admin Username: Enter the username for the previously-installed CouchDB instance.

Admin Password: Enter the password for the previously-installed CouchDB instance.

Provision: Click to provision the database instance.

Workload Database Configuration: This region is specific to the Couch DB database instance for Workload policies.

The results of Workload actions are stored in a CouchDB instance and can be accessed via the Data Owner Client.

Database Host: Enter the IP address or DNS host name of the server hosting Couch DB.

Admin Username: Enter the username for the previously-installed CouchDB instance.

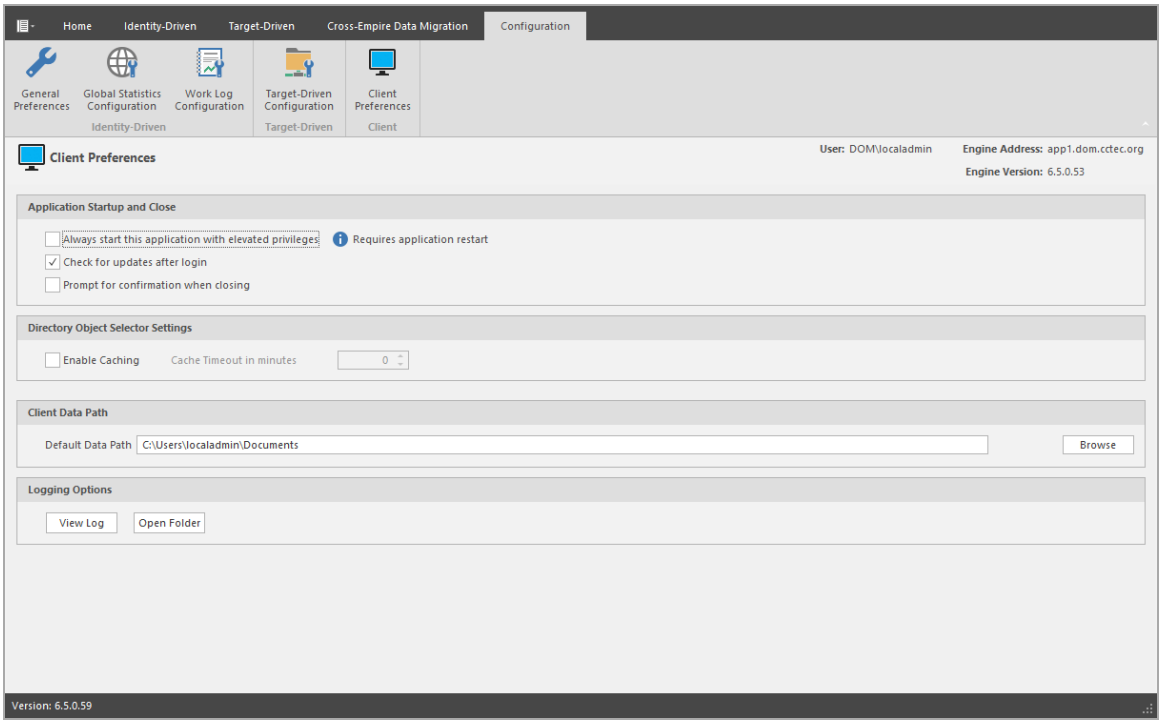
Admin Password: Enter the password for the previously-installed Couch DB instance.

Provision: Click to provision the database instance.

11.4.5 - Client Preferences

Use this page to set preferences specific to the File Dynamics Admin Client.

Client Preferences Page



Application Startup and Close: This region provides preference settings for when the Admin Client is launched and closed.

Always start this application with elevated privileges: When selected, this option allows you to run the Admin Client as the Administrator, enabling you to view settings that are not visible to non-administrators. For example, Server Share properties can only be seen when someone is logged in as an administrator.

Check for updates after login: Selecting this check box allows the Admin Client to notify you of the availability of newer File Dynamics components.

Prompt for confirmation when closing: When selected, this option specifies that you want a confirmation prompt before closing the Admin Client.

Directory object Selector Settings: This region lets you establish caching settings specific to the Admin Client.

Enable Caching: Selecting this check box enables the Admin Client to maintain the area of the directory tree that is visible in the right pane of the Objects page, if you move from the Objects 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 Objects page, you do not need to navigate the directory tree to locate the Group object again.

Cache Timeout in minutes: In large enterprises, it can take a long time to build up the directory services cache. In these type of environments, consider increasing this setting so that you can use the cache, instead of querying directory services again for information.

Default Data Path: This field specifies the location where all exported reports are stored. For example, if you were to export a Consistency Check report as a CSV or HTML file, it would be saved in this location.

Browse: Locate the destination where you want exported reports stored.

Logging Options: This region enables you to access the Admin Client's log files.

View Log: Clicking this button opens the log file.

Open Folder: Clicking this button opens the folder where the Admin Client's compressed log files are stored.

Appendix A - Security Specifications

This section provides details on the necessary security settings needed for the File Dynamics components .

A.1 - Firewall Requirements

A.1.1 - Windows Firewall

The Windows Firewall has different default configurations based on the version of Windows Server.

In most cases, the File Dynamics installation enables the following firewall settings. In the rare circumstances where it does not, you will have to establish these manually.

Engine

- The Engine must be permitted to make outbound connections.
- The Engine must be able to listen on port 3009. This is the default port choice presented during the installation and configuration.
- The default firewall rule for the Engine allows access to the application on any port it listens on.

File System Agent

- The Agent must be permitted to make outbound connections.
- The Agent must be able to listen on port 3011. This is the default port choice that is presented during the installation and configuration.
- The default firewall rule for the Agent allows access to the application on any port it listens on.

Phoenix Agent

- The Phoenix Agent must be permitted to make outbound connections.
- The Phoenix Agent must be able to listen on port 3013. This is the default port choice that is presented during the installation and configuration.
- The Phoenix Agent makes use of the Windows http.sys HTTP listener, so firewall rules must specify a port and not an application.
- If you use the Phoenix Agent Configuration utility, it will adjust the listening port and the associated firewall rule.

Event Monitor

- The Event Monitor component must be permitted to make outbound connections.

Data Owner Web Service

- The Data Owner web service must be permitted to make outbound connections.
- The Data Owner web service must be able to listen on port 3079. The is the default port choice that is presented during the installation and configuration.
- The default firewall rule for the Data Owner web service allows access to the application on any port it listens on.

Admin Client

- The Admin desktop client must be permitted to make outbound connections.

Resource Servers

- On each Windows server hosting user or collaborative storage with managed quota, you must enable the `Remote File Server Resource Manager Management - FSRM Service (RPC-In) firewall rule`.

A.1.2 - Other Services

The following services may run on Windows or Linux, so firewall rules management may vary depending on the service host.

SQL Server Database

- The associated SQL Server instance hosting the File Dynamics database must listen on TCP/IP.
- Currently only IPv4 addresses are supported.
- The listening TCP/IP port (default port 1433) must be enabled for access in the firewall where SQL Server is running.
- The Admin Client, Engine, and Phoenix Agents must all have access to the IP address and TCP port where SQL Server is listening.

CouchDB

- The host where CouchDB is installed must allow inbound access for TCP port 5984 which is the default port for CouchDB.
- The Engine, Data Owner Client web service, Phoenix Agent, and Admin Client must all have access to to the IP address and TCP port where CouchDB is listening.

A.2 - LSA Rights and Privileges

The following table identifies the security principals, sets of rights and privileges and the computers on which the rights and privileges must be granted for File Dynamics to function properly.

Each component's configuration utility will setup the required privileges and group membership for the host server on which it is installed.

IMPORTANT: Changes to a given User Rights Assignment in a server's Local Security Policy or in applicable Group Policy Objects (GPOs) can interfere with the expected assignments for the BUILTIN\Adminstrators group or the File Dynamics Admins and Data Owners groups.

In particular, if you use GPOs for managing User Rights Assignments you may need to add the group assignments listed below to applicable Group Policies.

A.2.1 - Engine Server

Security Principal	User Rights Assignment	Notes
Proxy Rights Group	Backup	Provided by membership in BUILTIN\Administrators local group.
	Batch Logon	
	Change Notify	
	Impersonate	
	Network Logon	
	Restore	
	Security	
	Take Ownership	
Admins Group	Batch Logon	Setup as part of Engine configuration.
Data Owners Group	Batch Logon	Setup as part of Engine configuration.

A.2.2 - Event Monitor Server

Security Principal	User Rights Assignment	Notes
Proxy Rights Group	Batch Logon	Provided by membership in BUILTIN\Administrators local group.
	Impersonate	
	Backup	
	Restore	
	Security	
	Take Ownership	

A.2.3 - Agent Server

These permissions apply to servers hosting either the File System Agent or Phoenix Agent.

Security Principal	User Rights Assignment	Notes
Proxy Rights Group	Backup	Provided by membership in BUILTIN\Administrators local group.
	Batch Logon	
	Change Notify	
	Impersonate	
	Network Logon	
	Restore	
	Security	
	Take Ownership	

A.2.4 - File Share Server

Security Principal	User Rights Assignment	Notes
Proxy Rights Group	Backup	Provided by membership in BUILTIN\ Administrators local group.
	Change Notify	
	Network Logon	
	Restore	
	Security	
	Take Ownership	

A.3 - Proxy Rights Group Permissions

The Proxy Rights Group is responsible for holding permissions and privileges necessary for the File Dynamics Proxy user account.

A.3.1 - Windows Servers

File Shares

Each file share managed by File Dynamics must have the Proxy Rights Group assigned with **Full Control** to the share itself.

Built-in Administrators Group

Some system calls used by File Dynamics require membership in each managed Windows server's **BUILTIN\ Administrators** local group. This group membership also provides a number of user rights and privileges required by the proxy account for proper operation with each managed Windows server.

When you install and configure the Engine or Agent components from File Dynamics on a domain member server, the configuration tools grant the Proxy Rights group membership in the built-in Administrators group on that member server.

For other servers in the domain that are hosting storage managed by File Dynamics, you must grant Proxy Rights group membership in the built-in Administrators group.

A.3.2 - NAS File Servers

See *NAS Device Considerations (page 252)* for details on the Proxy Rights Group permissions and group memberships requirements for NAS devices.

A.3.3 - Active Directory

Proxy Rights Group Permissions

The Proxy Rights Group requires the following access at the root of each domain in the forest:

Access	Applies To	Notes
Read (Read all properties, Read permissions, List contents)	This object and all descendants	Required for basic management and navigation
Replicating Directory Changes	This object only	Required for Event Monitor [1]
Read/Write ccx-FSFAuxiliaryStorage	Descendant ccx-FSFManagedPathAttributes	Required for management of File Dynamics Auxiliary policy schema extensions [2]
Read/Write ccx-FSFManagedPath	Descendant ccx-FSFManagedPathAttributes	Required for management of File Dynamics Collaborative policy schema extensions [2]
Read/Write objectClass	Descendant user, group objects	Required for managing auxiliary class custom schema extensions for user Auxiliary and group Collaborative storage management [2]
Read/Write homeDirectory	Descendant user objects	Required for management of home directory attributes
Read/Write homeDrive	Descendant user objects	Required for management of home directory attributes

1. This permission only applies to the domain root. Additionally, it is only needed if the File Dynamics Event Monitor for AD is installed.
2. These permissions only apply when using User Auxiliary or Collaborative storage policies and the custom schema extensions have been applied.

Delegated Administration

For environments requiring delegated administration in Active Directory, apply the previous list of rights to the specific containers where management by File Dynamics is allowed to operate.

You can then remove any assigned permissions from the domain root as necessary.

NOTE: The *Replicating Directory Changes* permission only works on the domain root and cannot be delegated to any subcontainers.

A.4 - Windows Clustering

File Dynamics supports clustering of Windows Server through Proxy Agents. Configuring a cluster to be managed through a Proxy Agent is similar to configuring an individual server to be managed by a Proxy Agent. In particular, the Proxy Rights group must be granted membership in the built-in Administrators group and it must also be granted all of the LSA rights and privileges that are granted at each cluster node. When this is done, the folder share permissions that are required must be granted to the Proxy Rights group for all shares that will be managed by File Dynamics.

Appendix A - NAS Device Considerations

A.5 - NetApp Filer

For a NetApp Filer device, the configuration is very simple because the device does not fully emulate

a Windows Server at the operating system level.

1. Use the NetApp Filer administration utility to join the NAS device to a domain where File Reporter can report.
2. Grant the proxy rights group membership in the NAS device's built-in Administrators group.
3. Grant the proxy rights group the folder share permissions that are required to access the storage.

There are no LSA privileges to grant on a NetApp Filer NAS device.

A.6 - PowerScale OneFS

Perform the following steps to integrate a PowerScale OneFS device (formerly EMC Isilon). You can use these same steps to see if other NAS devices integrate with File Reporter.

1. Rebuild the storage resources and verify that the NAS device is displayed on the list.
2. Perform any needed steps for giving the proxy rights group access to the desired shares and folders on the NAS device.

A.7 - Other NAS Devices

Perform the following steps to see if other NAS devices integrate with File Reporter.

1. In the associated Computer object in Active Directory, add the following text somewhere in the description attribute for that object:

   ```
   ***SRGenericNASDevice***
   ```

2. Rebuild the storage resources and verify that the NAS device is displayed on the list.
3. Perform any needed steps for giving the proxy rights group access to the desired shares and folders on the NAS device.

Appendix B - Distributed File System (DFS)

This section provides guidance for configuring DFS namespaces to work with File Dynamics.

IMPORTANT: File Dynamics only supports domain-based DFS namespaces. DFS in standalone mode is not supported.

B.1 - Configuring DFS Folders

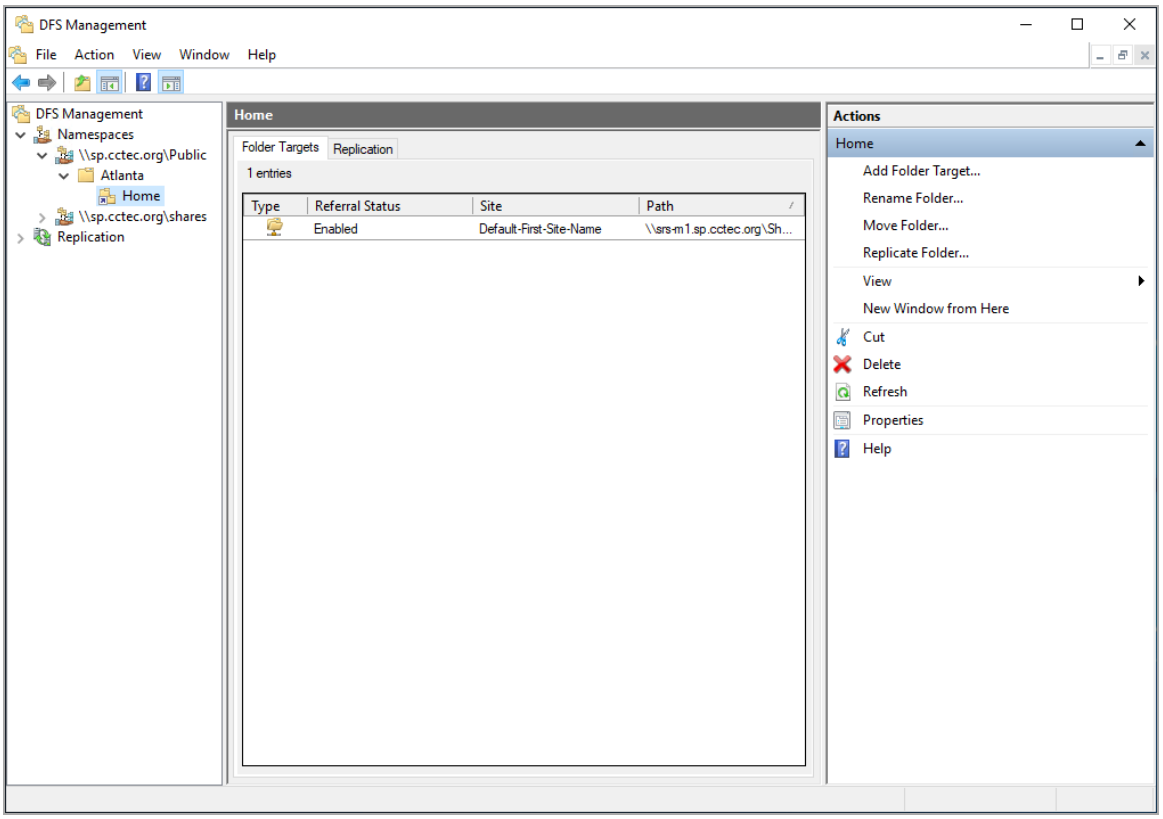
File Dynamics requires definite paths in its policies. Because namespaces can provide multiple targets for DFS links and thereby introduce ambiguity, a DFS namespace must be configured with one of the following three options linked below.

B.2 - Providing Only One Target Per DFS Link

The simplest way to guarantee that File Dynamics has unambiguous DFS paths is to give each DFS link a single target.

In the following graphic, there is just one target path and it is enabled.

One Target Path

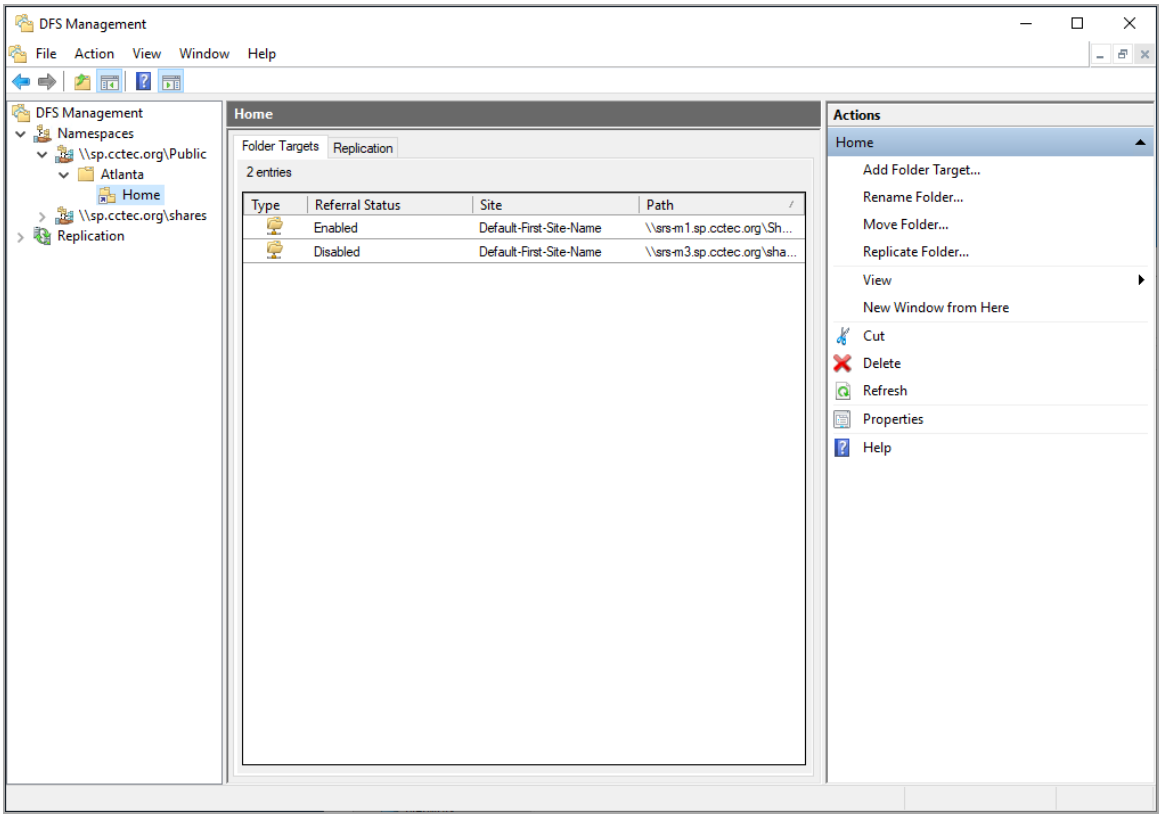


B.3 - Disabling All But One Target Per DFS Link

If a DFS namespace is used for high availability, such as ensuring that users can access a replicated copy of their data, it might be appropriate to create multiple targets in a DFS link and disable all but one. If the enabled link target becomes unavailable, an administrator can disable the downed target and enable a replication target. As long as only one target is enabled for a given DFS link, File Dynamics can successfully provision and manage storage through the DFS path.

In the following graphic, there are multiple target paths, but only one is enabled.

Multiple Target Paths with One Enabled



B.4 - Enabling Multiple Target Paths

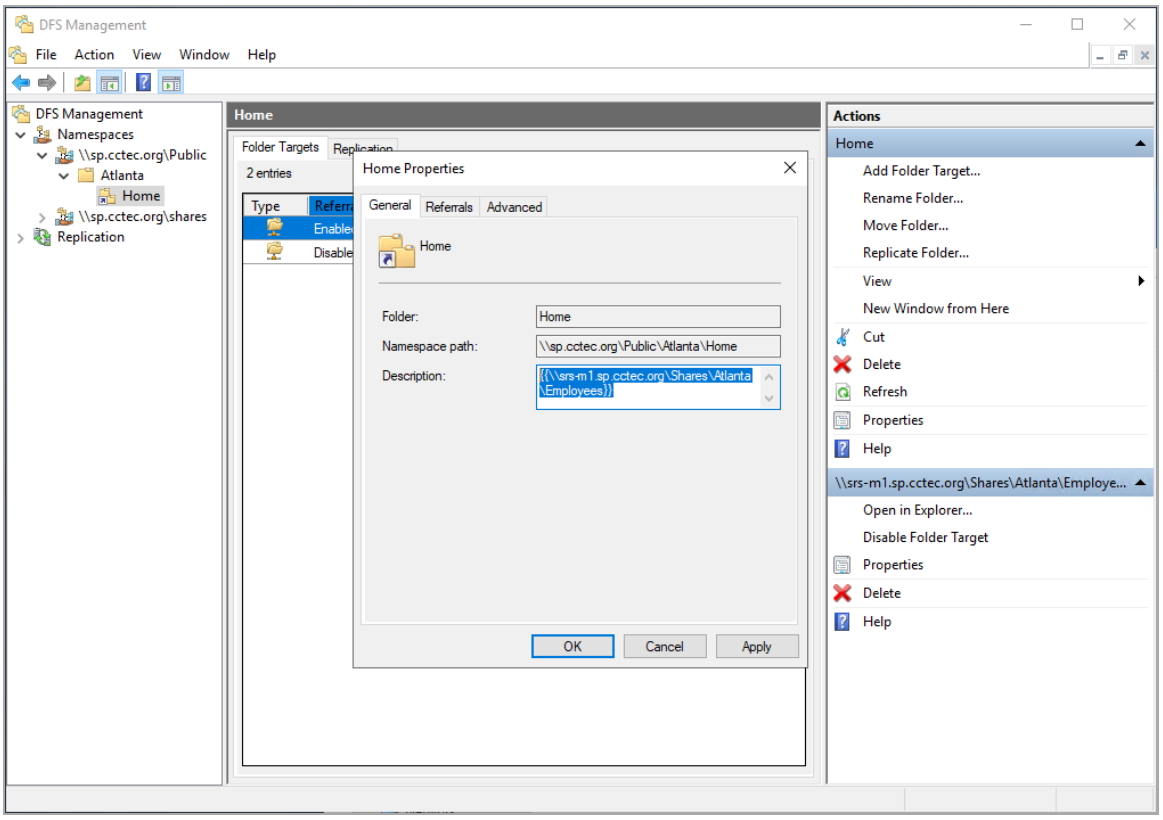
File Dynamics can parse the description field on a DFS folder to determine which of several enabled targets is the primary, unambiguous target. This allows File Dynamics to manage namespaces with multiple enabled targets in a DFS link.

To do this, the description for the DFS link must enclose the complete UNC path of the path File Dynamics should use in double curly braces. For example, {{*Server**Share**Path*}}. This must be identical to the UNC path in the target link; it cannot be a subdirectory.

In the graphic below, there are two target paths enabled.

The Home Properties dialog box is accessed by double-clicking the listing in the DFS Management console.

Two Target Paths Enabled



Appendix C - File Server Resource Manager

Microsoft File Server Resource Manager (FSRM) is a suite of tools from Microsoft that allows administrators to better understand, control, and manage the quantity and type of data stored on their servers. File Dynamics uses File Server Resource Manager to enable quota management.

You must install FSRM on all servers where File Dynamics will be managing quotas, including the server that will host the Engine. Even if the Engine host does not contain shares that will be managed, FSRM is still required because the FSRM COM interfaces must be present for the Engine to call them remotely on other servers.

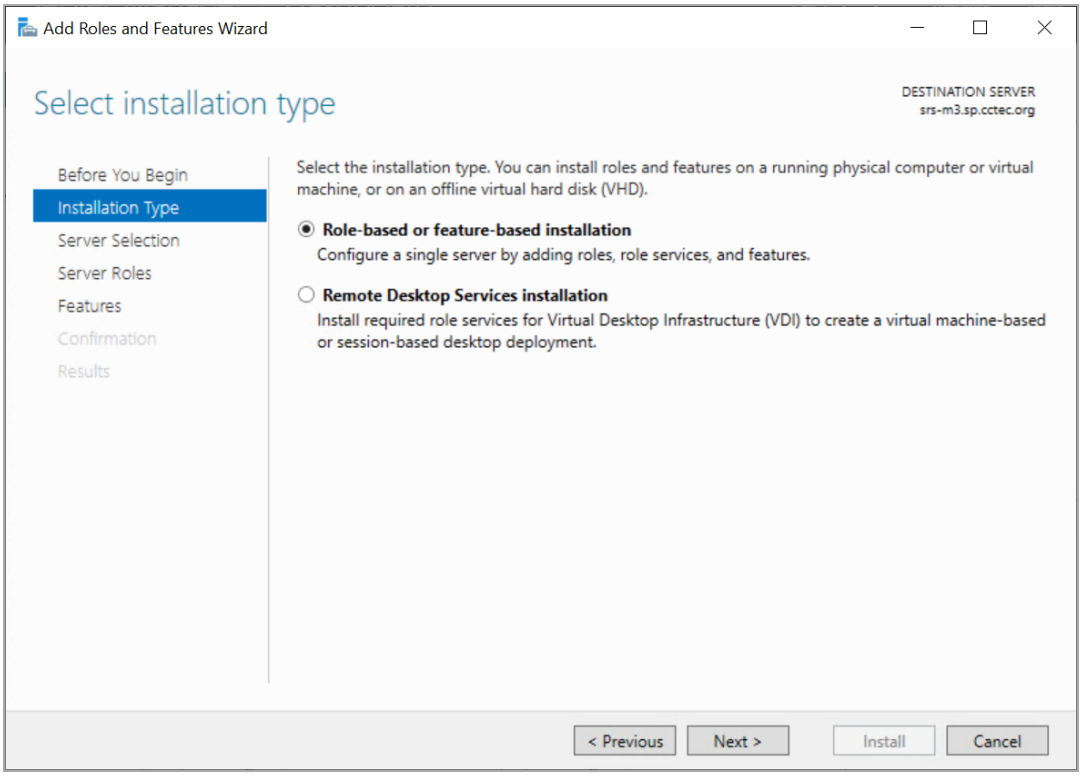
C.1 - Installing File Server Resource Manager

Quotas for user and collaborative storage can be managed through File Dynamics on all versions of Windows Server from 2008 and beyond. You need to install FSRM on every server or active node that will be hosting user or collaborative quota-managed storage.

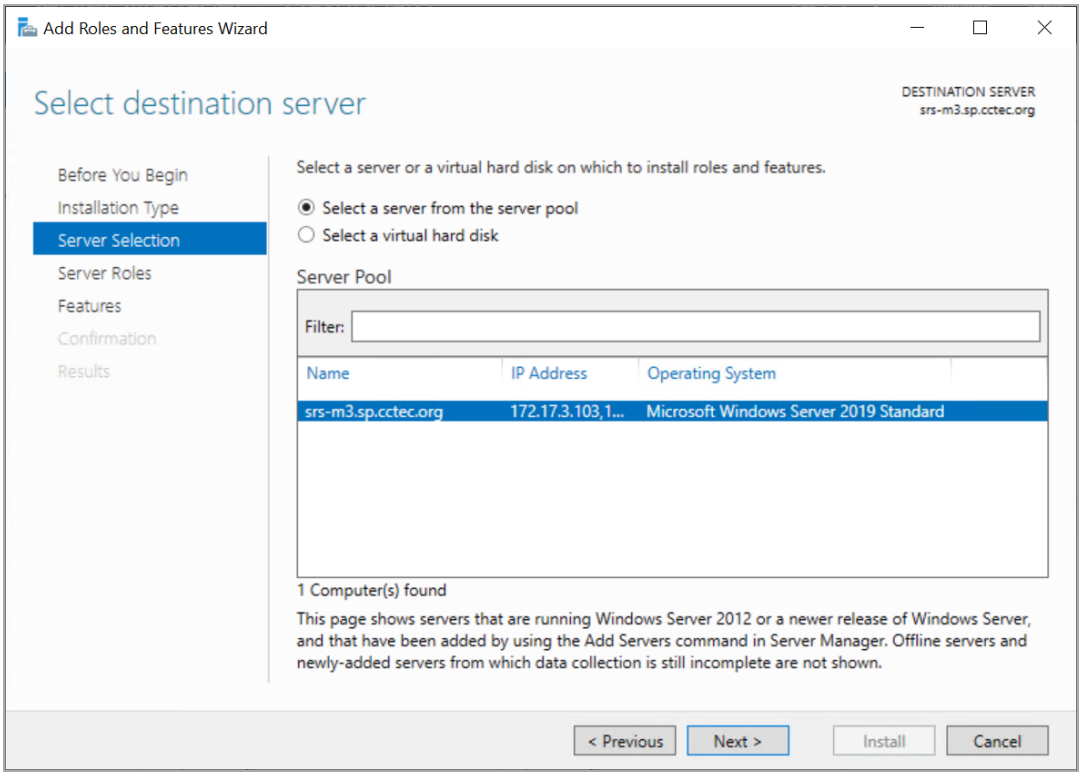
These procedures are specific to Windows Server 2022. Procedures vary for each version of Windows Server.

1. Launch Server Manager.
2. Click *Add roles and features*.
3. This launches the Add Roles and Features Wizard.

4. Click *Next*.

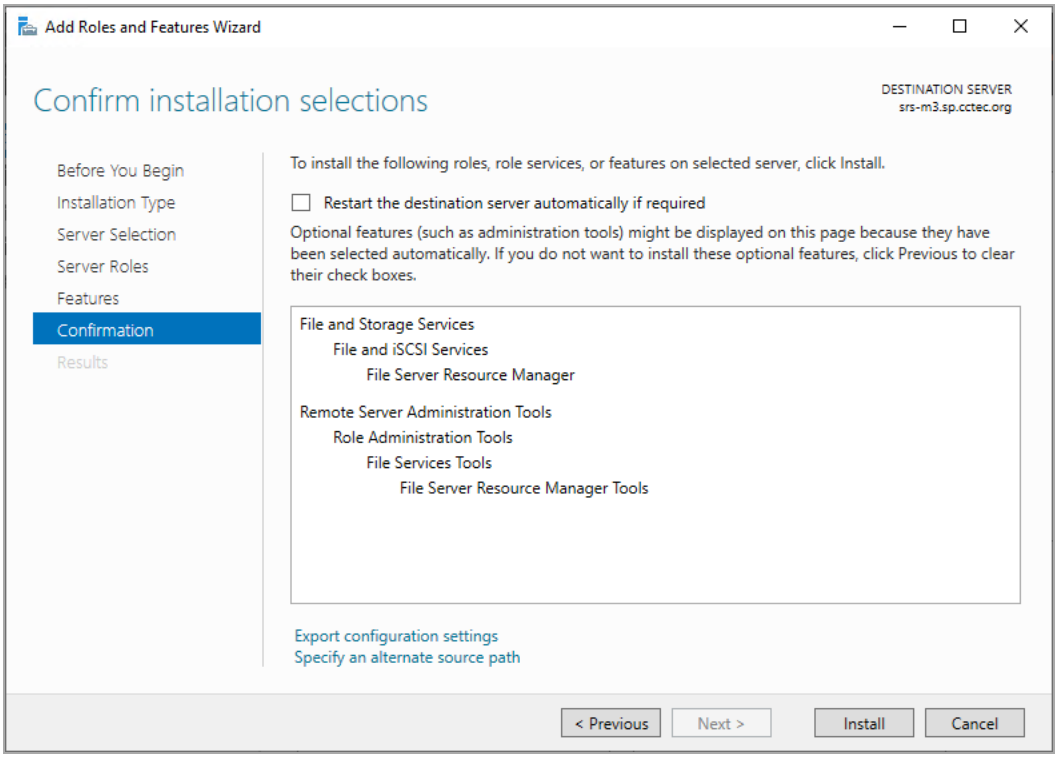

Add Roles and Features Wizard
Select installation type
DESTINATION SERVER
srs-m3.sp.cctec.org
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).
Role-based or feature-based installation
Configure a single server by adding roles, role services, and features.
Remote Desktop Services installation
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.
< Previous
Next >
Install
Cancel

5. Verify that *Role-based or feature-based installation* is selected and click *Next*.



6. Select the server where you are going to install the Engine and click *Next*.
7. From the list of roles, expand *File and Storage Services*.
8. Expand *File and iSCSI Services*.

9. Select the *File Server Resource Manager* check box.



10. Click *Add Features*.
11. Click *Next*.
12. Click *Next*.
13. Click *Install*.

Appendix D - Active Directory Schema Extensions

File Dynamics extends the Active Directory schema by adding new attributes and classes.

D.1 - Attributes

The following are new attributes added to the Active Directory schema.

D.1.1 - ccx-FSFAuxiliaryStorage

A list of one or more paths pointing to managed auxiliary storage associated with this object.

ccx-FSFAuxiliaryStorage Specification

Active Directory Attribute Property	Value
Name	ccx-FSFAuxiliaryStorage
LDAP Display Name	ccx-FSFAuxiliaryStorage
Admin Display Name	ccx-FSF-Auxiliary-Storage
Admin Description	List of one or more paths pointing to managed auxiliary storage associated with this object
ASN.1 ID	1.3.6.1.4.1.35052.1.1.100.1.1
Syntax	ADSTYPE_CASE_IGNORE_STRING
Sized – Lower Limit	-
Sized – Upper Limit	-
Single Valued	False
Schema ID GUID	c4bacb95-075e-11df-bcab-eee40b817f62
Search Flags	-
System Flags	-
Link ID	-
Attribute Security GUID	cd55682f-3987-446d-a18e-cfd8d53b95f2
Partial Attribute Set Member	False

D.1.2 - ccx-FSFManagedPath

The managed path attribute for objects (such as groups and containers) that do not inherently have a home folder attribute.

ccx-FSFManagedPath Specification

Active Directory Attribute	Property Value
Name	ccx-FSFManagedPath
LDAP Display Name	ccx-FSFManagedPath
Admin Display Name	ccx-FSFManagedPath
Admin Description	Managed path attribute for collaborative objects
ASN.1 ID	1.3.6.1.4.1.35052.1.1.100.2.1
Syntax	ADSTYPE_CASE_IGNORE_STRING
Sized – Lower Limit	-
Sized – Upper Limit	-
Single Valued	True
Schema ID GUID	c4bacb96-075e-11df-bcab-eee40b817f62
Search Flags	-
System Flags	-
Link ID	-
Attribute Security GUID	cd55682f-3987-446d-a18e-cfd8d53b95f2
Partial Attribute Set Member	False

D.2 - Classes

The following are new attributes added to the Active Directory schema.

D.2.1 - ccx-FSFManagedAttributes

An auxiliary class holding common attributes managed by File Dynamics.

ccx-FSFManagedAttributes Specifications

Active Directory Class Property Value	Active Directory Class Property Value
Name	ccx-FSF-Managed-Attributes
LDAP Display Name	ccx-FSF-Managed-Attributes
Admin Display Name	ccx-FSF-Managed-Attributes
Description	Auxiliary class for managed storage attributes
ASN.1 ID	1.3.6.1.4.1.35052.1.1.2.1.1
Schema ID GUID	c4bacb93-075e-11df-bcab-eee40b817f62
Class Type	Auxiliary
Parent Class	top
Default Object Category	ccx-FSFManagedAttributes
Naming Attribute	-
Mandatory Attributes	-
Optional Attributes	ccx-FSFAuxiliaryStorage ccx-FSFManagedPath
Possible Superiors	-
System Possible Superiors	-
System Flags	-
Default Security Descriptor	-

Appendix E - Managed Path Naming Attribute Specifications

File Dynamics traditionally uses the `sAMAccountName` attribute values for naming managed paths for user and group collaborative policies. The Managed Path Naming Attribute (MPNA) provides more granular control over how managed paths are named for user and group collaborative policies. Each MPNA Action Block applies to either a User/User Auxiliary policy type or a Group Collaborative policy type. You can link one or more policies to an appropriate MPNA Action Block to control which attribute applies for naming the managed path as well as the Groom and Vault paths.

The MPNA doesn't apply to Dynamic Template Folders that are created as part of the collaborative template processing. These folders are not managed per se and will continue to be named based on the `sAMAccountName` attribute.

As with the `sAMAccountName` attribute, values should be unique for the attribute you choose for an MPNA Action Block or policy in order to avoid naming collisions in the file system as you manage storage with File Dynamics. If you choose an attribute other than `sAMAccountName` for a MPNA Action Block or policy, ensure that the process used to populate the attribute's values can guarantee unique values for the storage objects being managed by that policy. If duplicate values occur for the policy, it is possible for related storage management events to go pending because the target path is not available.

E.1 - Rules

The following are rules specific to managed path naming attribute specifications.

E.1.1 - General

The MPNA is configured through an MPNA Action Block. For procedures on creating an MPNA Action Block, see *Creating a Managed Path Naming Attribute Action Block (page 182)*.

- If you do not configure an explicit MPNA Action Block, a private Action Block applies in which the `sAMAccountName` is used for user and group collaborative policies.
- An MPNA Action Block can be linked only to policies that match its type. An MPNA Action Block can be one of the following policy types:
    - User/User Auxiliary
    - Group Collaborative
- After you link an MPNA Action Block to one or more policies, you cannot change the block's policy type without first removing the policy links.

  The list of available attributes for an MPNA Action Block depend on its associated policy type. The User/User Auxiliary policy type displays only attributes for the User object class. The Group Collaborative policy type displays only attributes for the Group object class.

- Only single-valued domain-replicated, stored attributes are eligible to be chosen as the MPNA.
- Multi-valued domain-replicated, stored attributes are not eligible to be chosen as the MPNA. One example is the `Description` attribute:

  https://msdn.microsoft.com/en-us/library/ms675492(v=vs.85).aspx
- Constructed and non-replicated attributes are not eligible to be chosen as the MPNA. See Attributes:

  https://msdn.microsoft.com/en-us/library/ms675155(v=vs.85).aspx
  - A constructed attribute has values that are computed from normal attributes for read, or affects the values of normal attributes for writes. For example, `canonicalName` and `allowedAttributes` are non-stored, constructed attributes.
  - Non-replicated attributes are stored on each domain controller, but are not replicated. For example, `badPwdCount`, `Last-Logon`, and `Last-Logoff` are non-replicated attributes.
- MPNA does not support auxiliary classes and their attributes.

E.1.2 - Groom and Vault Paths

A Groom or Vault path follows the MPNA for the policy's managed path. For example, if Policy 1's MPNA is the `employeeNumber` attribute, the attribute's value is used in the managed path and in the path for a Groom or Vault action.

- Policy 1 Managed Path for user Keith whose `employeeNumber` attribute is "123456789": `\\Server1-dns-name\Share1\Users\123456789`
- Policy 1 Vault or Groom Path for user Keith whose `employeeNumber` attribute is "123456789": `\\Server9-dns-name\Vault\Users\123456789`

E.2 - Event Processing

The MPNA is retrieved from Active Directory during Create events and when it is time for an event to calculate the best target path based on the MPNA and other policy leveling and distribution criteria. If the MPNA has not yet been populated (such as if the MPNA value is blank or the attribute doesn't exist), the event will go pending until the MPNA has a value.

The Event Monitor watches for changes to the MPNA. When the attribute's value changes, a Rename event is generated.

If you unlink a policy from an MPNA Action Block, and link it to a different MPNA Action Block, you will need to issue the Enforce Paths Management Action to enforce policy compliance.

E.3 - Management Actions

If you modify the MPNA Action Block to use a new attribute, you must run an Enforce Paths management action to bring the affected objects' managed paths into compliance with the policy.

Appendix F - Glossary

Action Block: A feature of File Dynamics that allow the sharing of specific policy options between multiple policies.

Admin Client: The management interface for File Dynamics.

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 Active Directory.

Auxiliary storage: Home folders associated to a user in addition to the regular network home folder. Depending on the storage policy, auxiliary storage can be made accessible or unaccessible to the associated user.

Blocking policy: A policy designed to block other File Dynamics 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 File Dynamics. These potential problems might be missing storage quotas, inconsistent directory attributes, missing home directories, inconsistent file paths, and more.

Container: A synonym for organizational unit in the File Dynamics documentation.

Content Control policy: Similar to identity-driven file grooming, Target-Driven Content Control policies remove files according to file type, age, size, last accessed date, and more. From any file path, you can either vault files to a new location or delete the files altogether.

Collaborative storage: A shared storage area where a group of people in an organization can collaborate by accessing files. File Dynamics lets you easily create collaborative storage areas through collaborative storage policies that you can assign to Group objects or to an organizational unit.

Data Location policy: These policies are the means of copying folders and their contents to a target parent folder. There is an option to remove the files from the source location after they have been copied.

Data Owner: An individual assigned by a network administrators to be notified of access permission changes, perform data recovery, or perform remediation of data located on high-value targets. Data Owners are normally assigned based on a user's association with a folder or share that is classified as a high-value target.

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 File Dynamics, 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.

High-Value Target: A file system directory deemed to hold valuable information. Administrators or Data Owners in an organization can classify a folder as a high-value target based on appropriate evaluation.

Identity-Driven Policies: Automated storage management tasks that are enacted through an association with Active Directory users and groups.

Managed Path: A location that File Dynamics manages in an automated fashion for any of the following: Home folder, Profile path, Remote Desktop Services Home folder, Remote Desktop Services Profile path, 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.

Nearline: An intermediate storage location that provides fast access to the data, but is not a generally accessible storage location on the network. Nearline storage inherently provides some level of security and data integrity.

Personal folder: A user-specific folder in a collaborative storage area.

Phoenix Agent: An agent that assists with Target-Driven policy management actions.

Policy: Rules and settings within File Dynamics that indicate what storage-specific actions to enact when an event in Active Directory takes place. These actions include creating user storage when a new user is added to Active Directory, moving storage when a user is moved from one organizational unit 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, File Dynamics uses this setting to determine which policies to apply. File Dynamics applies the policy with the largest numerical weight.

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.

Security Fencing Policies: Target-Driven policies that let you set limits on how access permissions can change over time by specifying containers, groups, or users that can be given access permissions and others that should never be given access permissions.

Security Lockdown Policies: Target-Driven policies that let you establish the baseline permissions for a high-value target. When unauthorized access permissions are made, the new permissions are removed and the baseline permissions are restored.

Security Notification Policies: Policies that allow you to analyze and be notified of the changes in security permissions for a selected target path. Notifications are sent via email and specify the added, modified, or removed permissions for users and groups.

Target-Driven Policies: Policies that manage and perform tasks through direct association with a network share or folder. Target-Driven policies include Data Location policies, Content Control policies, Workload policies, Security Notification policies, Security Lockdown policies, and Security Fencing policies.

Target Path: The path to the network share where managed paths 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.

Work Log: An optional mechanism that maintains a history of File Dynamics events. The Work Log contains summary records for events that have reached the processed state; in other words, those for which an effective policy has been calculated and run to completion or have been aborted by administrative action.

Workload Policy: Policies that provide the ability to import externally-generated files and be enacted through a Data Owner via the Data Owner Client.