# Micro Focus Storage Manager 5.2 for Active Directory

## Administration Guide

**May 16, 2017**

## Legal Notices

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

# Contents

# About This Guide

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

## Audience

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

## Feedback

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

## Documentation Updates

For the most recent version of the *Micro Focus Storage Manager 5.2 for Active Directory Administration Guide*, visit the Micro Focus Storage Manager Web site (http://www.novell.com/documentation/storagemanager5/index.html).

## Additional Documentation

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

- *Micro Focus Storage Manager 5.2 for Active Directory Installation Guide*

# 1 What's New

Micro Focus Storage Manager 5.2 for Active Directory includes performance enhancements and new features that expand the management capabilities of the product. An overview of these performance enhancements and new features follows:

## 1.1 New in Version 5.2

### Work Log Reports

The Work Log is a mechanism that maintains a history of Storage Manager 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 Storage Manager and requires you to install Apache CouchDB. For more information see Chapter 12, "Work Log Reports," on page 229.

### New Action Blocks

There are new Action Blocks for Move Schedule and Target Path. For more information, see "Creating a Move Schedule Action Block" on page 263 and "Creating a Target Paths Action Block" on page 266.

### Nested DFS Namespace Support

This enhancement addresses DFS configurations where a DFS link is configured to point to the root of a DFS namespace.

### Updated Engine Status Page

Information on this page is now presented graphically. Additionally, the event logging is now on a persistent basis. For more information, see Section 13.1.1, "Status," on page 245.

### Ability to Specify Years for File Retention and Grooming

A new option for groom rules lets you now specify a set number of years that the contents of a user or group folder will be vaulted, based on a specified policy or groom operation. This is particularly useful for archiving files that have not been accessed or modified since a specific year.

## 1.2 New in Version 5.1

### Event Monitor Scope

Rather than burdening the Storage Manager Event Monitor in observing all events in the Active Directory forest or domain, this new 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 more information, see Chapter 4, “Configure the Event Monitor Scope,” on page 27 and Appendix G, “Event Monitor Scope,” on page 359.

### Managed Path Naming Attribute

No longer dependent on the name of the `sAMAccountName` attribute value, which might or might not be a descriptive name of the user or group, you can now choose from among multiple attributes for the user or group folder name. For more information, see Section 6.5.4, “Setting Target Paths,” on page 54.

### Multi-Principal Group Storage Policies

This new policy type allows for multiple groups to access a shared group folder, with each group having different sets of permissions to the group folder. For more information, see Section 8.9, “Creating a Multi-Principal Collaborative Storage Policy,” on page 107.

### Cross-Forest Data Management

Once you have established a trust relationship, you now have the ability to manage data in a secondary forest. For more information, see “Cross-Forest Data Management” on page 309.

### Faster Data Copying

Multi-threaded data copying now speeds up any management task involving data movement.

### New Action Blocks

There are new Action Blocks for Managed Path Naming Attributes and Multi-Principal Group Storage policies. For more information, see “Creating a Managed Path Naming Attribute Action Block” on page 261 and “Creating a Multi-Principal Suffix Mapping Action Block” on page 264.

## 1.3 New in Version 5.0

### Action Blocks

Action Blocks are a new feature in Storage Manager that allow the sharing of specific policy options among multiple policies. 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. For more information, see Section 13.1.5, “Action Blocks,” on page 257.

### Extended Capabilities for Non-Policy Managed Storage

In version 4.0, we introduced the ability to copy data across the network without the need for a policy. This ability to perform what we now term “operations” (an action performed in Storage Manager that is not tied to a policy) has now been extended to include File Grooming. For more information, see Section 13.1.9, “Operations,” on page 276.

### Active Directory to Active Directory Cross-Empire Data Migration

This new feature allows you to migrate data from Active Directory forest to another. Similar in approach to the previously-available eDirectory to Active Directory Cross-Empire Data Migration, this feature uses an easy-to-use wizard interface. For more information, see Chapter 11, “Performing an Active Directory to Active Directory Cross-Empire Data Migration,” on page 207.

### Updated Management Interface

The interface for what is now known as SMAdmin has been modernized.

### Other Changes

In addition to a number of bug fixes, the speed of data copying and migrations has been increased.

## 1.4 New in Version 4.0

### SQL Server Database

Novell Storage Manager for Active Directory now utilizes Microsoft SQL Server 2012 or 2014 as the product database. If you do not already have SQL Server, you can download the Express version of SQL Server for free. Novell Storage Manager 4.0 includes a utility for migrating the contents of the SQLite database to the SQL Server database. These contents include policies, schedules, pending events, and so forth. For more information, see “Migrating the Database”in the *Novell Storage Manager 4.0 for Active Directory Installation Guide*.

### Data Copying

This new feature allows you to copy specific data across the network without the need for a policy.

### Pre-copy during Enforce Policy Path

Lets you move files in two stages—closed files first, then the open ones once they have been closed. For more information, see “Enforce Policy Path” on page 271.

### Search Feature Enabled on New Pages in NSMAdmin

Allows you to browse and filter through a tree structure of the file system to locate data.

### Re-Drive Management Actions

Allows you to select a subset of the results of a management action and perform other actions to that subset.

### Clear Managed Path Attribute

This new Management Action allows for the desired policy type attribute to be cleared in Active Directory. For more information, see “Clear Managed Path Attribute” on page 273.

## 1.5 New in Version 3.1.1

### Leveling Algorithm

The Leveling Algorithm setting of a policy's Target Paths page now lets you structure the home folders so that they are categorized by the first or last letter of a username through a subordinate folder. A new **Leveling Length** field allows you to enter up to 4 characters, making it so that you can organize home folders by year. For more information, see Section 6.5.4, "Setting Target Paths," on page 54.

### Pending Events

You can now place comments on deferred pending events. This allows an administrator to specify to other administrators the reason why he or she deferred the event. For more information, see Section 13.1.7, "Events," on page 274.

### Bypassable Events

Allows Novell Storage Manager to automatically attempt to address any pending events that can bypass administrative action. For more information, see Section 6.5.1, "Setting Policy Options," on page 51.

### Displaying Administrative and Hidden Shares:

You have the option to display Active Directory administrative and hidden shares in NSMAdmin.

## 1.6 New in Version 3.1

### Cross-Empire Data Migration

For file to file migrations, Novell Storage Manager now lets you identify and move all files that are new or have been modified after a given date. Additionally, you can verify that all of the files you wanted to migrate from a source server have been migrated. You use four new utilities to perform these tasks:

- **novscan.nlm:** A NetWare NLM that scans the contents of the target server and determines which files have been modified or created since you performed a preliminary file to file migration.
- **NovScanConfig.exe:** This Windows executable configures what file system data you want identified from the NetWare or Novell Open Enterprise Server source.
- **WinScan.exe:** This Windows executable lists the contents of the file system on the target Microsoft server following a file to file migration.
- **ScanCompare.exe:** This Windows executable compares the files on the NetWare or Open Enterprise Server source server and the Microsoft Server target server.

All of these new utilities are used in Section 10.12, "Performing a Folder to Folder Migration," on page 180.

### Integration with Novell File Reporter 2.0

Novell File Reporter 2.0 can report on the files and folders of the target paths of Novell Storage Manager 3.1 policies.

## 1.7 New in Version 3.0.4

### Tivoli Support

Novell Storage Manager 3.0.4 for AD now supports IBM Tivoli Hierarchical Storage Management.

### Certificate Management

Enhanced SSL Certificate Management enables you to generate your own SSL certificates.

### Enhanced DFS Namespace Support

Enhanced Microsoft Distributed File System support now allows for multiple namespaces to be managed. For more information, see Appendix C, "Distributed File System (DFS)," on page 339.

## 1.8 New in Version 3.0.3

### Performance Enhancements

This update includes significant performance enhancements that speed up provisioning user storage, processing templates, enforcing policy paths, cross-empire data migrations, and vaulting.

## 1.9 New in Version 3.0.2

### Identity Mapping in Cross-Empire Data Migration

To retain security and ownership information for files and folders being migrated from a Novell network platform to a Microsoft network platform, an identity mapping technology has been added to Cross-Empire Data Migration. Within the identity map, you indicate object equivalence from the Novell network source to the Microsoft network target.

For more information, see Section 10.2.1, "Defining an Identity Map for Security and Ownership Migration," on page 129.

## 1.10 New in Version 3.0.1

### Cross-Empire Data Migration

Cross-Empire Data Migration is a subsystem within Novell Storage Manager that allows for the movement of file system data between storage infrastructures on different platforms governed by different identity and security frameworks. You can perform the following types of data copying:

- User to User
- Folder to User
- Group to Group
- Folder to Group
- Folder to Folder

For more information, see Chapter 10, "Performing an eDirectory to Active Directory Cross-Empire Data Migration," on page 125.

### Microsoft DFS Namespace Support

Distributed File System (DFS) namespace technology helps Microsoft network administrators group shared folders located on different servers and presents them to users as a virtual tree of folders known as a namespace. Novell Storage Manager now presents these namespaces as available storage resources in the Storage Resource List.

### Copy Policy Data

Copy Policy Data allows you to copy all or a portion of the policy settings of one policy into another policy. For more information, see Section 6.10, “Copying Policy Data,” on page 68.

### Export Policy

Provides the ability to export policies so that they can be imported later. For more information, see Section 6.12, “Exporting Policies,” on page 74.

### Import Policy

Provides the ability to import policies that were previously exported. For more information, see Section 6.13, “Importing Policies,” on page 75.

## 1.11 New in Version 3.0

### Collaborative Storage

Novell Storage Manager 3.0 for Active Directory provides administrators the ability to create and manage collaborative storage areas for groups and containers. These storage areas can be structured in multiple ways including:

- A single project folder where all project members have access
- A project folder with personal subfolders for each of the members of a group. This configuration is done through Dynamic Template Processing
- Classroom-based storage for education customers providing the ability to structure the storage to support assignment and class work turn-in folders for each student

For more information, see Chapter 8, “Managing Collaborative Storage,” on page 87.

### Quota Management

Quota management lets administrators set storage quota limits for users based on their roles in the organization. Additionally, administrators can designate individuals as quota managers, who can then grant storage quota increase requests when needed. For user storage quota management, see Section 6.4, “Enabling Your Network for Quota Management,” on page 50 and Section 6.5.5, “Setting Quota Options,” on page 56. For collaborative storage quota management, see Section 8.7.5, “Setting Group Collaborative Storage Policy Quota Options,” on page 99. For administering quota, see Chapter 9, “Using Quota Manager,” on page 119.

### Profile Path and Remote Desktop Services Support

In addition to creating User Home Folder policies, administrators can create a User Profile Path policy, a User Remote Desktop Services Home Folder policy, and a User Remote Desktop Services Profile Path policy, with each of these policies governing storage management independently. For more information, see Section 6.6, “Creating a User Profile Path Policy,” on page 61, Section 6.7, “Creating a User Remote Desktop Services Home Folder Policy,” on page 63, and Section 6.8, “Creating a User Remote Desktop Services Profile Path Policy,” on page 64.

### Auxiliary Storage Policies

Auxiliary storage allows administrators to create one or more policies for creating and managing auxiliary storage folders when a new user is created. This auxiliary storage can even be hidden from the user for whom it was created. For example, administrators can create an HR Folder for confidential information about the user. For more information, see Section 6.11, “Using a Policy to Manage Auxiliary Storage,” on page 69.

### GSR Collector

The Global Statistics Reporting (GSR) Collector collects data for general statistics, presents historical data, reports on anomalies such as potential orphaned home folders, and catalogs managed storage movement. For more information, see Section 13.1.13, “GSR Collector,” on page 283.

### Anomaly Reports

The GSR Collector generates anomaly reports that identify issues that might need to be addressed before you create storage policies.

### Policy Location

In previous versions of Novell Storage Manager for Active Directory, the policies were stored as text files in a `POLICY` folder where the NSM Engine was installed. Policies are now stored in an SQLite database.

# 2 Overview

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

## The Directory

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

## Events

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

## Policies

Policies within Storage Manager indicate what storage-specific actions to enact when an event in Active Directory takes place. These 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.

Storage Manager lets you create the following types of policies:

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

**User Profile Path:** Used for profile path management

**User Remote Desktop Services Home Folder:** Used for users who get network access from remote client machines. Prior to Windows Server 2008, these were referred to as Terminal Services Home Folders.

**User Remote Desktop Services Profile Path:** Used for profile path management for users who get network access from remote client machines. Prior to Windows Server 2008, these were referred to as Terminal Services Profile Paths.

**Container:** Manages the users located in an organizational unit.

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

## Management Actions

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

In Storage Manager, 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.

## Operations

Despite Storage Manager's ability to automate network file system management actions through policies or Management Actions, there are some cases where you will want to perform non-policy based management tasks. For example, suppose that in addition to Storage Manager, you also had Micro Focus File Reporter and through a Date-Age report, you determined that you had some department shares storing files that had not been accessed for five years or more.

Through a Groom operation, you could move these files to a less expensive secondary storage location, without having to first create a policy associated to the department shares.

## Engine

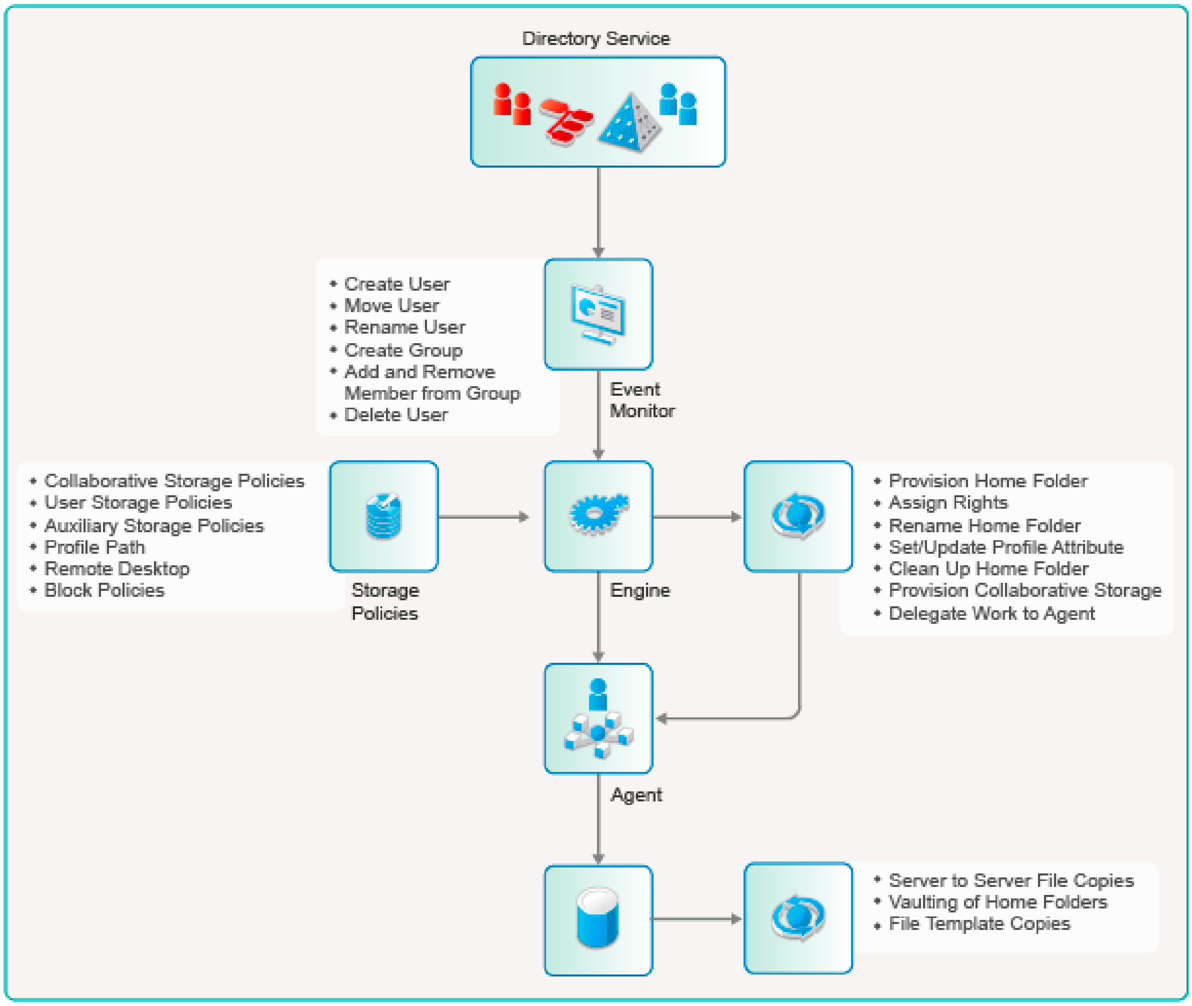
The Engine performs actions based on events in Active Directory and the defined Storage Manager policies. These actions include provisioning, moving, grooming, deleting, renaming, and vaulting in the file system. There is only a single Engine per forest and it can be installed on a domain controller or a member server. The Engine runs as a native NT service on Windows.

## 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 native NT service on Windows.

## Agents

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 Storage Manager. The Agent runs as a NT native service on Windows.


Directory Service
• Create User
• Move User
• Rename User
• Create Group
• Add and Remove Member from Group
• Delete User
Event Monitor
• Collaborative Storage Policies
• User Storage Policies
• Auxiliary Storage Policies
• Profile Path
• Remote Desktop
• Block Policies
Storage Policies
Engine
• Provision Home Folder
• Assign Rights
• Rename Home Folder
• Set/Update Profile Attribute
• Clean Up Home Folder
• Provision Collaborative Storage
• Delegate Work to Agent
Agent
• Server to Server File Copies
• Vaulting of Home Folders
• File Template Copies

# 3 Using SMAdmin

SMAdmin is the administrative interface for Micro Focus Storage Manager. All management tasks run from this easy-to use Windows application. SMAdmin requires the Microsoft .NET 4.5.2 Framework, which is installed automatically on the Windows workstation or server during the SMAdmin installation.

Procedures for installing SMAdmin are included in the "Micro Focus Storage Manager 5.2 for Active Directory Installation Guide." If you have not yet installed SMAdmin, go to that guide to install it before proceeding with this section.

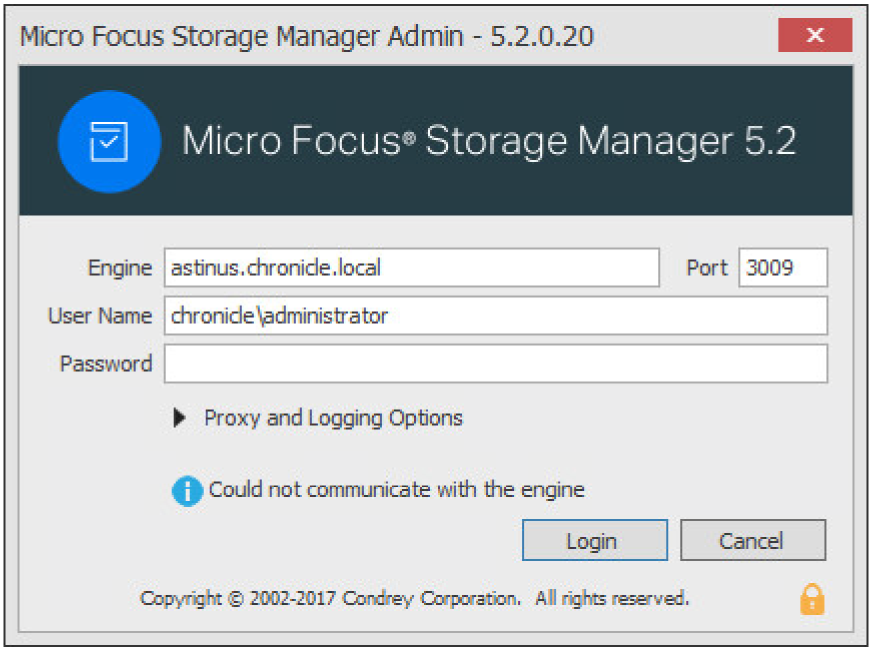
- Section 3.1, "Launching SMAdmin," on page 23
- Section 3.2, "Using the SMAdmin Interface," on page 25

**IMPORTANT:** For detailed information on the interaction between SMAdmin and the database, review Appendix A, "SMAdmin and Database Communication," on page 331.

## 3.1 Launching SMAdmin

1 Double-click the SMAdmin icon from the Windows desktop.

An authentication dialog box appears.



Micro Focus Storage Manager Admin - 5.2.0.20

Micro Focus® Storage Manager 5.2

Engine: astinus.chronicle.local

Port: 3009

User Name: chronicle\administrator

Password:

Could not communicate with the engine

Copyright © 2002-2017 Condrey Corporation. All rights reserved.

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

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

The default setting is 3009.

4 Specify the username.

You must specify the username in the form *Domain\username*.

5 Specify the password.

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

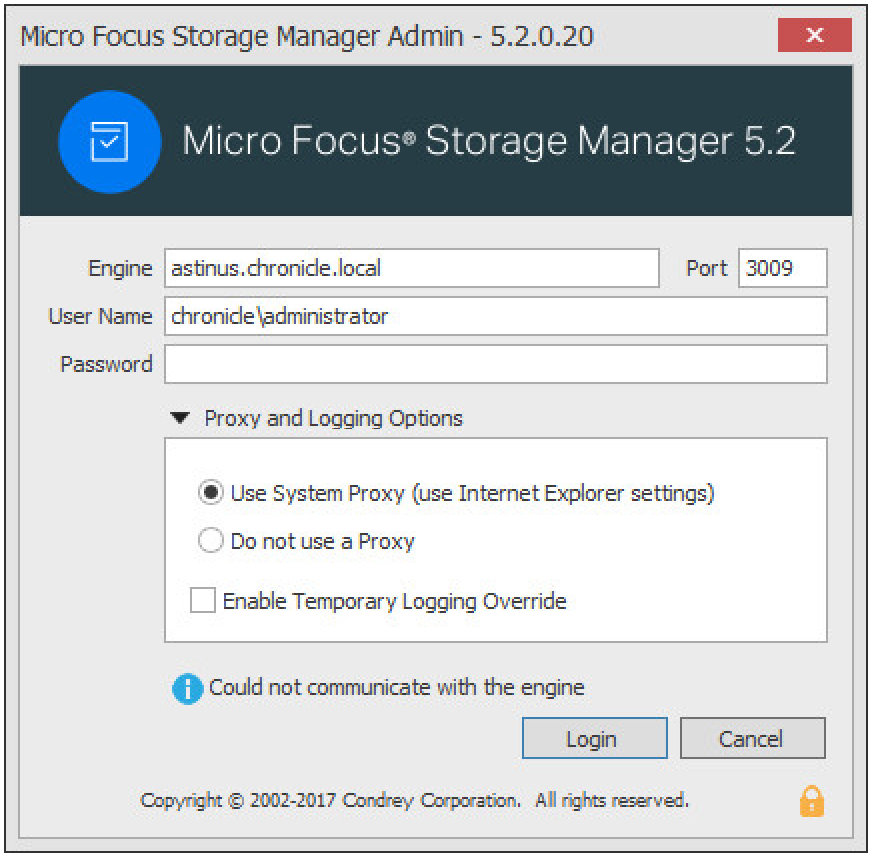
6 Click **Login**.

### 3.1.1 Overriding Proxy Settings at Login

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

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

1 Repeat Step 1 on page 23 through Step 5, then click the **Proxy and Logging Options** button to expand the authentication dialog box.


Micro Focus Storage Manager Admin - 5.2.0.20
Micro Focus® Storage Manager 5.2

Engine astinus.chronicle.local Port 3009

User Name chronicle\administrator

Password

Proxy and Logging Options

● Use System Proxy (use Internet Explorer settings)

○ Do not use a Proxy

□ Enable Temporary Logging Override

Could not communicate with the engine

Copyright © 2002-2017 Condrey Corporation. All rights reserved.

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

3 Click **Login**.

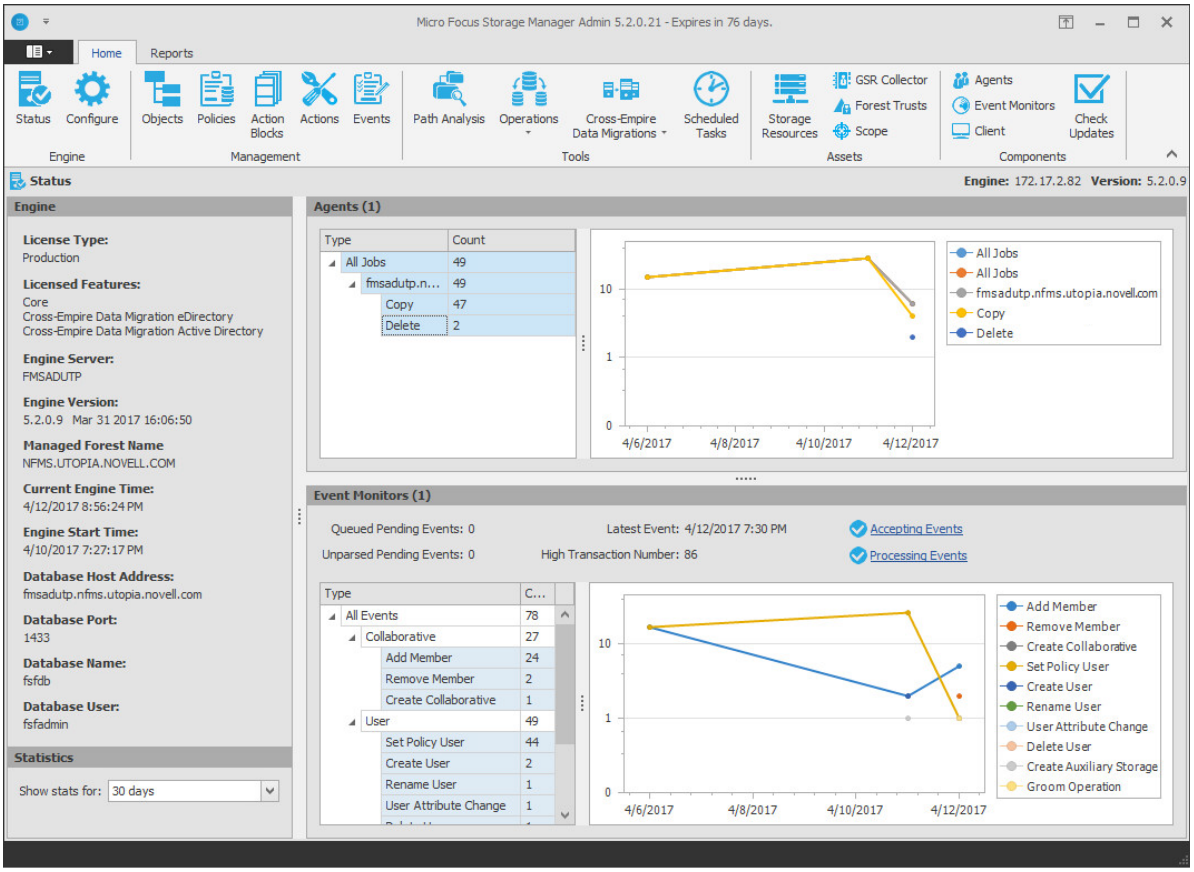
### 3.1.2 Enabling Temporary Logging Override

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

## 3.2 Using the SMAdmin Interface

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

The default display is the Engine Status page, which displays current running statistics of the Engine. The Engine Status page is discussed in detail in the Reference chapter of this guide (see Section 13.1.1, "Status," on page 245).



**Engine:** 172.17.2.82 **Version:** 5.2.0.9

**License Type:**
Production

**Licensed Features:**
Core
Cross-Empire Data Migration eDirectory
Cross-Empire Data Migration Active Directory

**Engine Server:**
FMSADUTP

**Engine Version:**
5.2.0.9 Mar 31 2017 16:06:50

**Managed Forest Name**
NFMS.UTOPIA.NOVELL.COM

**Current Engine Time:**
4/12/2017 8:56:24 PM

**Engine Start Time:**
4/10/2017 7:27:17 PM

**Database Host Address:**
fmsadutp.nfms.utopia.novell.com

**Database Port:**
1433

**Database Name:**
fsfdb

**Database User:**
fsfadmin

Show stats for: 30 days

| Type | Count |
|---|---|
| All Jobs | 49 |
| fmsadutp.n... | 49 |
| Copy | 47 |
| Delete | 2 |

Queued Pending Events: 0
Unparsed Pending Events: 0
Latest Event: 4/12/2017 7:30 PM
High Transaction Number: 86

| Type | C... |
|---|---|
| All Events | 78 |
| Collaborative | 27 |
| Add Member | 24 |
| Remove Member | 2 |
| Create Collaborative | 1 |
| User | 49 |
| Set Policy User | 44 |
| Create User | 2 |
| Rename User | 1 |
| User Attribute Change | 1 |

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

# 4 Configure the Event Monitor Scope

Products like Microsoft Exchange frequently create and remove objects such as groups that are not managed by Storage Manager. Prior to the release of Storage Manager for Active Directory 5.1, the Event Monitor would monitor all of these types of events, oftentimes burdening the Event Monitor and slowing down Storage Manager's ability to monitor and respond to relevant network storage events.

As a means of avoiding the monitoring of non-applicable network events, the Event Monitor no longer monitors the following Active Directory containers:

- Builtin
- Foreign Security Principals
- Managed Service Accounts
- Program Data
- System

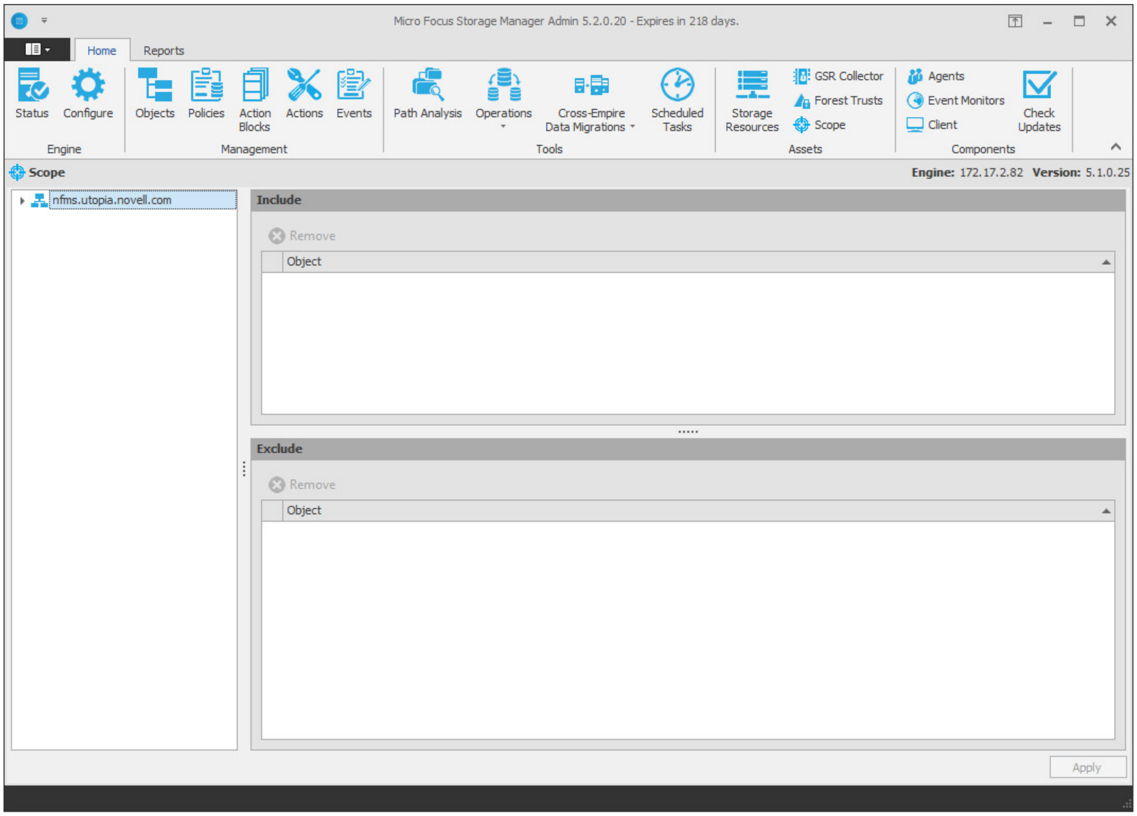
Additionally, Storage Manager for Active Directory lets you specify the Active Directory containers or subcontainers that will be included or excluded for monitoring. When you specify the containers and subcontainers to be monitored, you set the Event Monitor scope.

**NOTE:** For a complete discussion of the Scope feature, including Include and Exclude behaviors, see Appendix G, "Event Monitor Scope," on page 359.

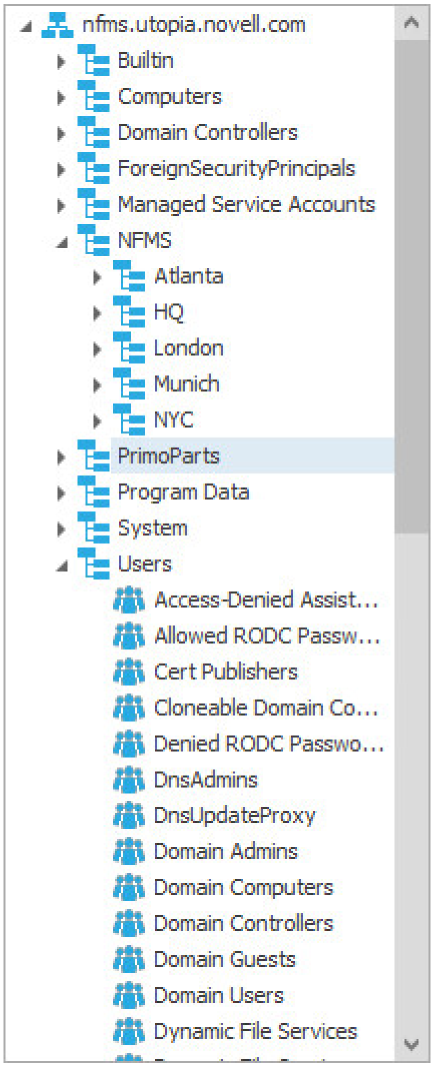
## 4.1 Configuring the Event Monitor Scope

1 In SMAdmin, click the **Home** tab.

2 Click **Scope**.



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



4 Drag to the **Include** and **Exclude** panes, the containers, subcontainers, and groups you want included and excluded respectively.

Remember that the Builtin, Foreign Security Principals, Managed Service Accounts, Program Data, and System containers are excluded automatically.

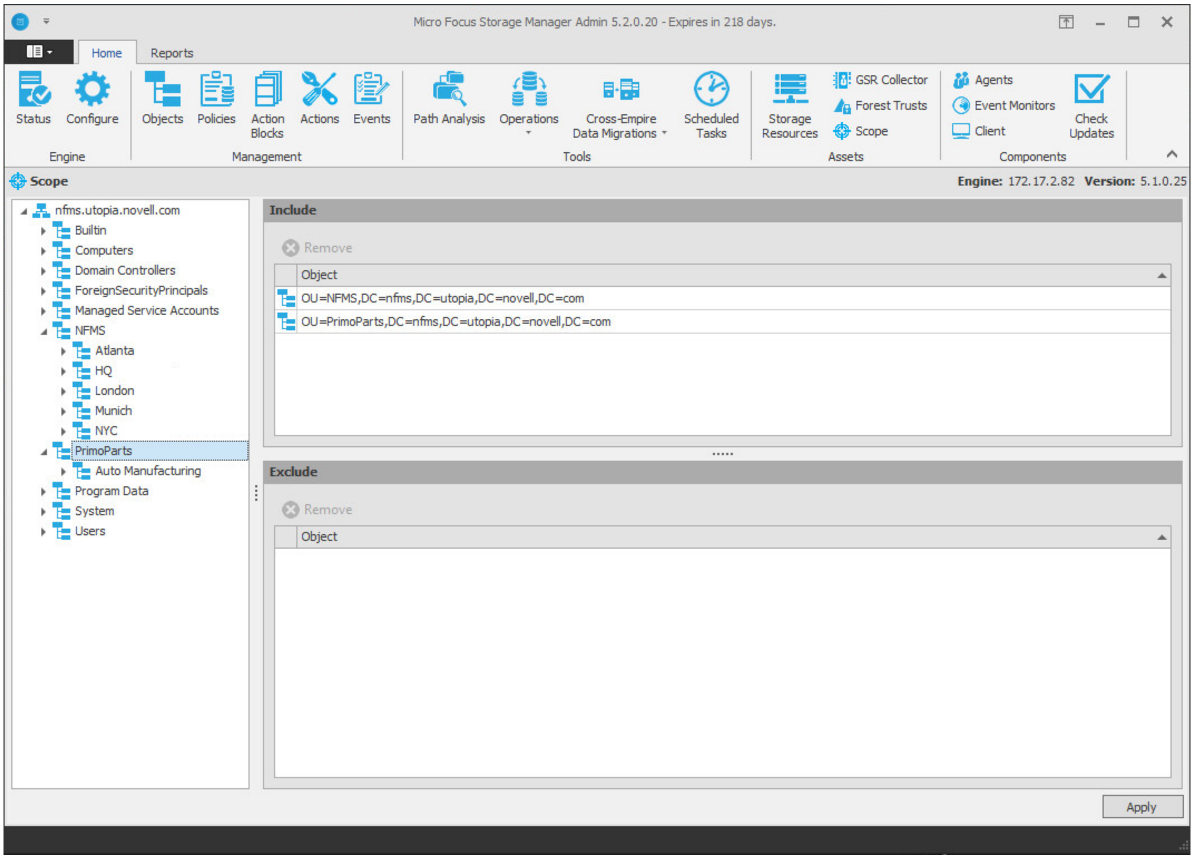
| Action | Result |
|---|---|
| Dragging one or more containers or groups to the **Include** pane | Specifies that those selected containers and their subcontainers, and groups and their nested groups will be monitored by the Event Monitor, while all other containers and groups will not be monitored. |
| Dragging one or more containers or groups to the **Exclude** pane | Specifies that those selected containers and their subcontainers, and groups and their nested groups will not be monitored by the Event Monitor, while other containers and groups residing at the same level of the excluded container and group in the AD forest or domain, will be monitored. |

5 Click **Apply**.

## 4.2 Example Scenarios

The following are example scenarios of Event Monitor scoping that might help you configure your Event Monitor scope. For expanded information, see Appendix G, “Event Monitor Scope,” on page 359.

*Figure 4-1 Containers Specified to Include*



Engine: 172.17.2.82 Version: 5.1.0.25

- nfms.utopia.novell.com
  - Builtin
  - Computers
  - Domain Controllers
  - ForeignSecurityPrincipals
  - Managed Service Accounts
  - NFMS
    - Atlanta
    - HQ
    - London
    - Munich
    - NYC
  - PrimoParts
    - Auto Manufacturing
  - Program Data
  - System
  - Users

Include

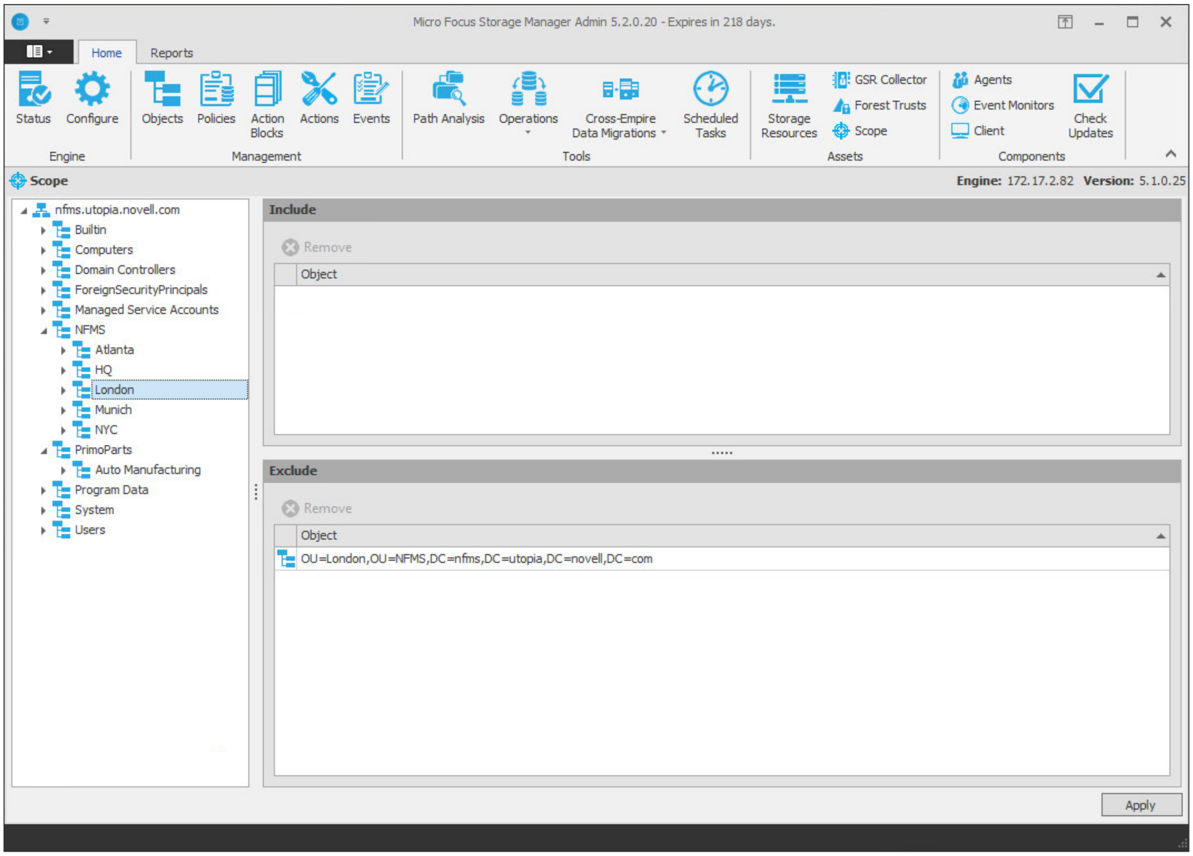
| Object |
|---|
| OU=NFMS,DC=nfms,DC=utopia,DC=novell,DC=com |
| OU=PrimoParts,DC=nfms,DC=utopia,DC=novell,DC=com |

Exclude

| Object |
|---|

In the example in Figure 4-1, the Event Monitor will monitor only the events that pertain to the NFMS and PrimoParts containers, including their subcontainers.

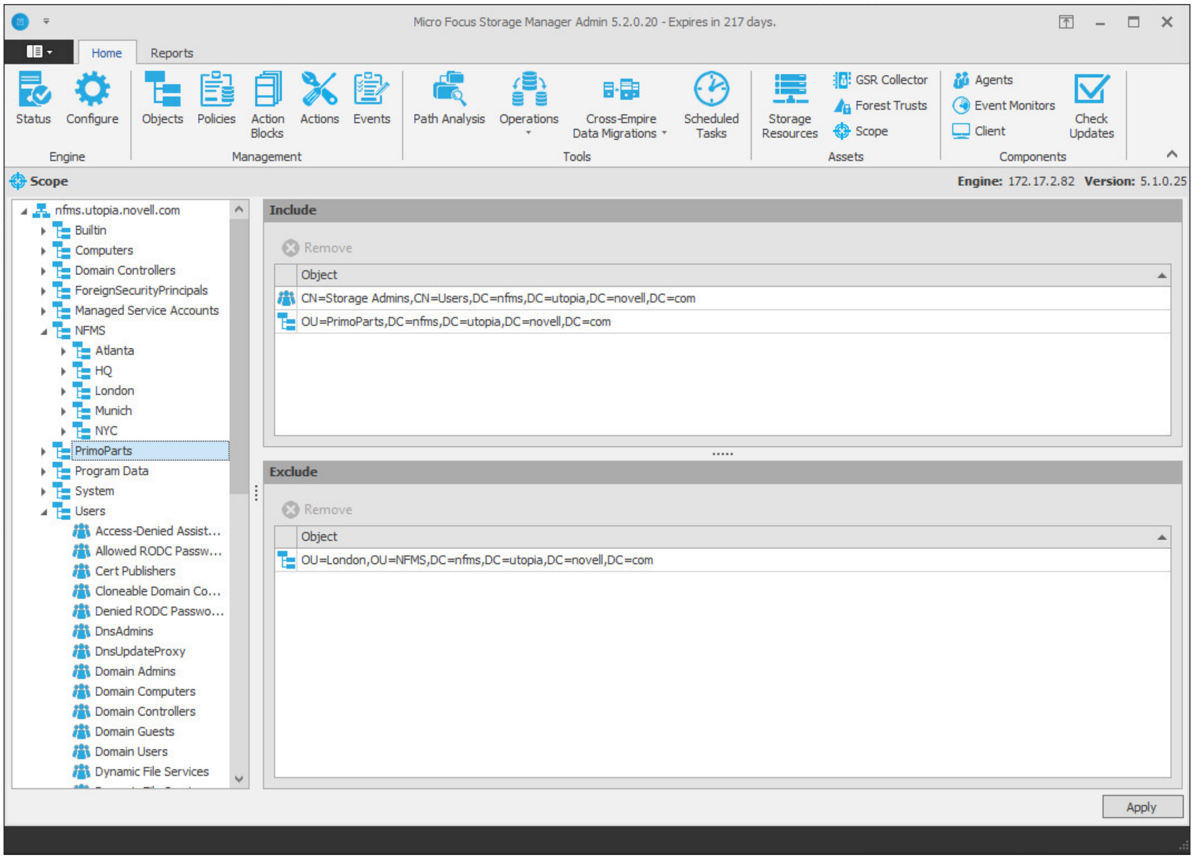
*Figure 4-2 Container Specified to Exclude*



OU=London,OU=NFMS,DC=nfms,DC=utopia,DC=novell,DC=com

In the example in Figure 4-2, the Event Monitor will monitor all containers except for the London subcontainer.

*Figure 4-3 Containers Specified to Include and Exclude*



**Include**

| Object |
|---|
| CN=Storage Admins,CN=Users,DC=nfms,DC=utopia,DC=novell,DC=com |
| OU=PrimoParts,DC=nfms,DC=utopia,DC=novell,DC=com |

**Exclude**

| Object |
|---|
| OU=London,OU=NFMS,DC=nfms,DC=utopia,DC=novell,DC=com |

In the example in Figure 4-3, the Event Monitor will monitor the PrimoParts container and Auto Manufacturing subcontainer, and all of the subcontainers in the NFMS container, with the exception of London. It will also exclusively monitor the Storage Admins group and exclude all other groups.

# 5 Managing Existing User Storage

Because Storage Manager 5.2 for Active Directory 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
- Running Management Actions to invoke the policies settings on the existing users
- Testing these policies to verify that they are working as desired

By completing this section, you not only put your existing users' storage into a managed state and set it up for ongoing management through Storage Manager, 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 *Micro Focus Storage Manager 5.2 for Active Directory Administration Guide* for more detailed content on these tasks as well as many others.

## 5.1 Running the GSR Collector

The Global Statistics Reporting (GSR) Collector collects data for general statistics, presents historical data, reports on anomalies such as potential orphaned home folders, and catalogs managed storage movement. For details about the GSR Collector and its usage scenarios, see Section 13.1.13, "GSR Collector," on page 283.

As the first step in managing your existing user storage through Storage Manager, you should run the GSR Collector. Depending on the size of your network, running the GSR Collector might be resource intensive and can take some time to complete. After you run the GSR Collector the first time, you should schedule it to run at a regularly scheduled time, preferably after regular business hours. For more information, see Section 13.1.11, "Scheduled Tasks," on page 279.

1. Launch SMAdmin.
2. In the **Home** tab options, click **GSR Collector**.
3. Click **Run**.

## 5.2 Viewing 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 Storage Manager to bring storage under management by policy. Anomaly data will be produced for each object and path type specified in the GSR Collector configuration.

By default, the following Anomaly Reports are available:

| Anomaly Report | Explanation |
|---|---|
| Attribute Value Missing | The respective path attribute (such as home folder) does not have a value. For more information, see "Attribute Value Missing" on page 319. |
| Path Missing On Disk | The respective path attribute (such as home folder) value cannot be found on disk. For more information, see "Path Missing on Disk" on page 320. |
| Path Validation Issue | Attempting to retrieve or verify the existence of the respective path attribute (such as home folder) value failed. For more information, see "Path Validation Issue" on page 321. |
| Name Mismatch | The leaf path name of the respective attribute (such as home folder) value does not match that of the respective object's name. For more information, see "Name Mismatch" on page 322. |
| Path Duplicate Value | Two or more objects have been detected that contain the same path for the respective path attribute (such as home folder). For more information, see "Path Duplicate Value" on page 322. |
| Path Parent CrossTalk | The object's respective path attribute (such as home folder) has been detected as being the parent of another object's path attribute (such as home folder). For more information, see "Path Parent Crosstalk" on page 323. |
| Path Child CrossTalk | The object's respective path attribute (such as home folder) has been detected as being the subordinate of another object's path attribute (such as home folder). For more information, see "Path Child Crosstalk" on page 323. |

| Anomaly Report | Explanation |
|---|---|
| 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 (such as home folder). For more information, see "Orphan Path Candidate" on page 324. |

### 5.2.1 View Anomaly Reports

1 In SMAdmin, click the **Reports** tab.

2 Click **GSR Anomaly**.

3 Within the graph, click the category you want to view.

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

## 5.3 Running Consistency Check Reports on Existing Storage

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

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

1 In SMAdmin, click the **Home** tab.

2 Click **Objects**.

3 In the left pane, browse through the domain so that an organizational unit with the users for whom you want to generate the consistency check report is displayed in the right pane.

4 In the right pane, right-click the container and select **User > Consistency Check**.

5 Click **Execute** and view the results in the bottom panel.

6 Click the expansion arrow in the split view slider to expand the view.

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

To export a consistency check report for printing, see Section 13.2.1, "Consistency Check," on page 315.

## 5.4 Assigning Missing Home Folder Attributes

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

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

If no home folder exists for the user, Storage Manager can create one automatically once the target path for the home folder is indicated in the policy. For more information, see Section 5.5, "Standardizing User Home Folder Attributes," on page 37.

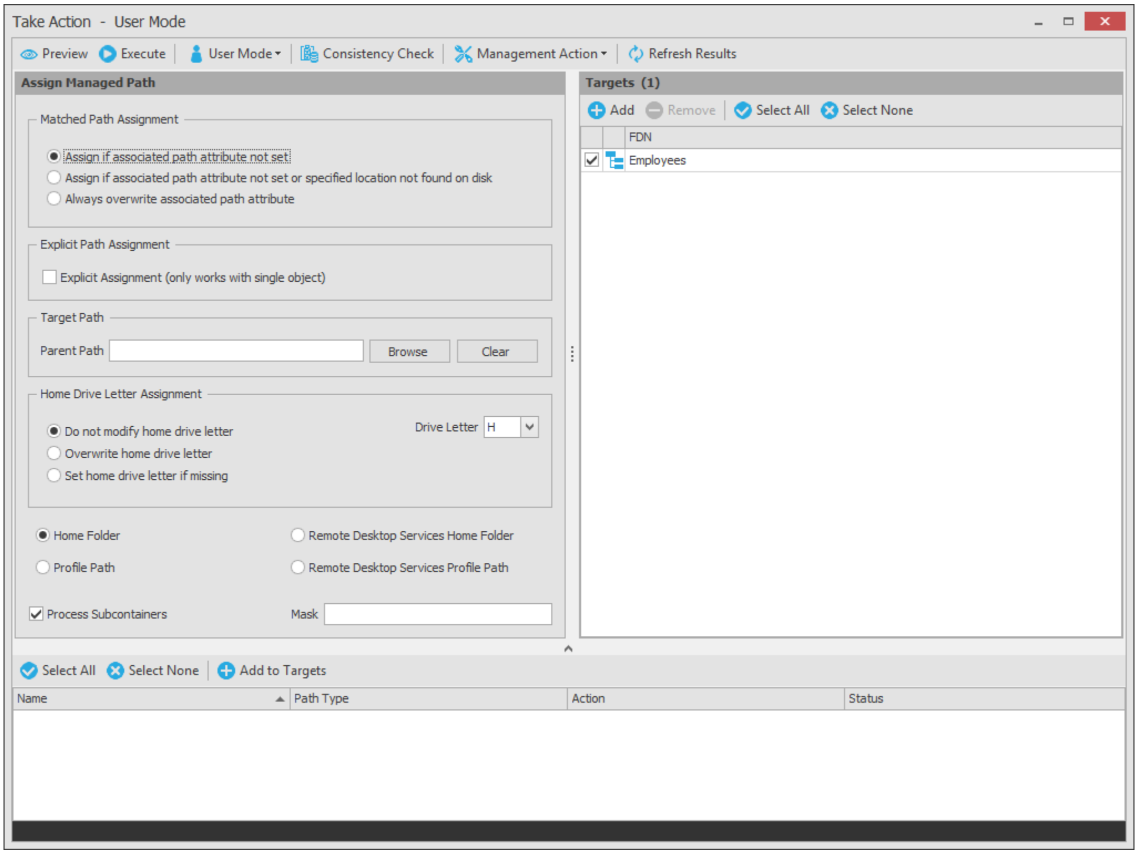
1 In SMAdmin, click the **Home** tab.

2 Click **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**.



Matched Path Assignment

● Assign if associated path attribute not set
○ Assign if associated path attribute not set or specified location not found on disk
○ Always overwrite associated path attribute

Explicit Path Assignment

☐ Explicit Assignment (only works with single object)

Target Path

Parent Path

Home Drive Letter Assignment

● Do not modify home drive letter
○ Overwrite home drive letter
○ Set home drive letter if missing

Drive Letter H

● Home Folder
○ Profile Path
○ Remote Desktop Services Home Folder
○ Remote Desktop Services Profile Path

☑ Process Subcontainers

Mask

☑ Employees

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**.

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

8. Click **Preview**.
9. If you approve of the actions Storage Manager took in Preview mode, click **Execute**.
10. Run a new consistency check by selecting the organizational unit you selected in Step 4, clicking **Consistency Check**, then clicking **Execute**.
11. Observe that all users now have home folder attributes listed in the **DS Path** column.

## 5.5 Standardizing User Home Folder Attributes

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

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

1. In SMAdmin, click the **Home** tab.
2. Click **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**.

   Storage Manager 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."
8. If you approve of the actions Storage Manager took in preview mode, click **Execute**.
9. Run a new consistency check by selecting the organizational unit you selected in Step 4, clicking **Consistency Check**, then clicking **Execute**.
10. Observe that all users who did not previously have proper home folder attributes, now do.

## 5.6 Creating a Blocking Policy

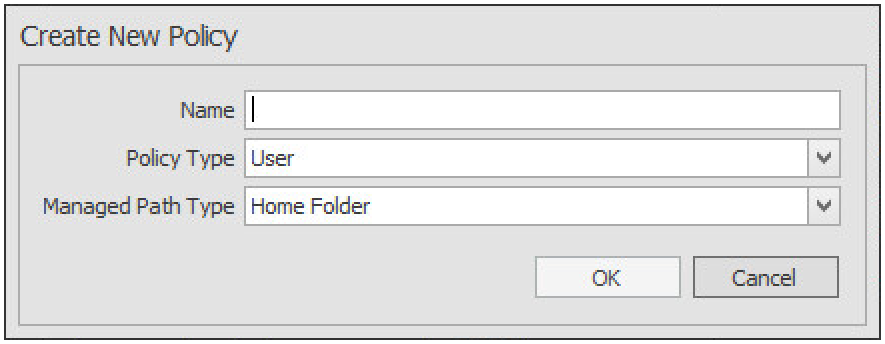
Storage Manager provides the ability to create "Blocking policies" that block other Storage Manager policies from affecting members of organizational units, members of groups, or even individual users. For example, you might have proxy users such as a BACKUP PROXY or VIRUS SCAN PROXY who do not need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

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 SMAdmin to create the Blocking policy and associate it to the group.

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

1. In SMAdmin, click the **Home** tab.
2. Click **Policies**.
3. In the **Manage** menu, select **New > User Home Folder**.

   The following dialog box appears:



Create New Policy

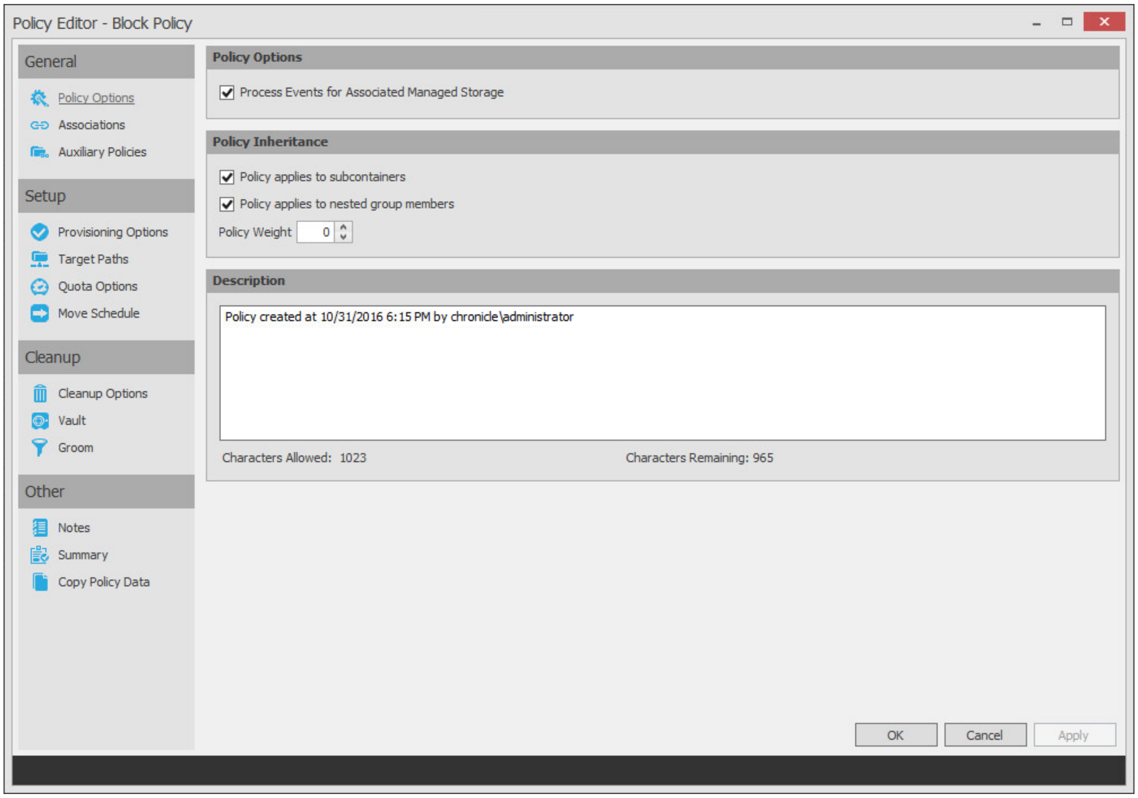
Name:

Policy Type: User

Managed Path Type: Home Folder

4. Specify a descriptive name in the **Name** field, such as “Block Policy,” leave the **User** and **Home Folder** options selected, then click **OK**.

   The Policy Options page appears.



Policy Editor - Block Policy

**Policy Options**

☑ Process Events for Associated Managed Storage

**Policy Inheritance**

☑ Policy applies to subcontainers

☑ Policy applies to nested group members

Policy Weight: 0

**Description**

Policy created at 10/31/2016 6:15 PM by chronicle\administrator

Characters Allowed: 1023 Characters Remaining: 965

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

   A description at the right of the check box indicates that the policy is now a Blocking policy.
6. In the left pane, click **Associations**.

7 Click **Add**.

8 Browse down and locate the user, group, or container that you want to block from the effects of Storage Manager policies, then drag it to the **Selected Items** pane.

9 Click **OK** to select the objects.

10 Click **OK** to save the Blocking policy.

## 5.7 Creating a User Home Folder Policy

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

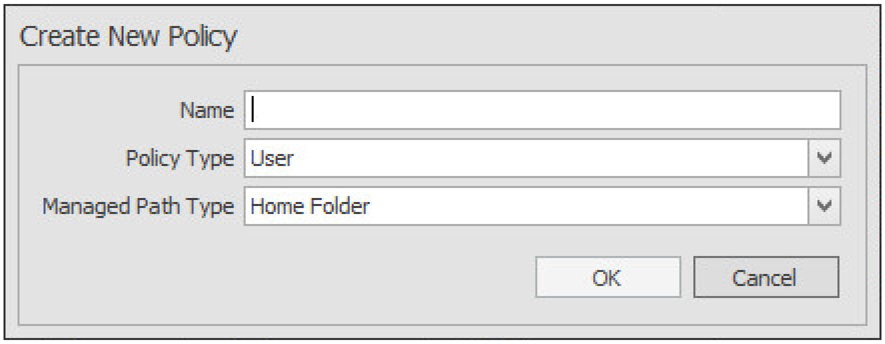
**IMPORTANT:** Only one policy of the same type can be associated with a domain, organizational unit, group, or user.

1 In SMAdmin, click the **Home** tab.

2 Click **Policies**.

3 In the **Manage** menu, select **New > User Home Folder**.

The following dialog box appears:



Create New Policy

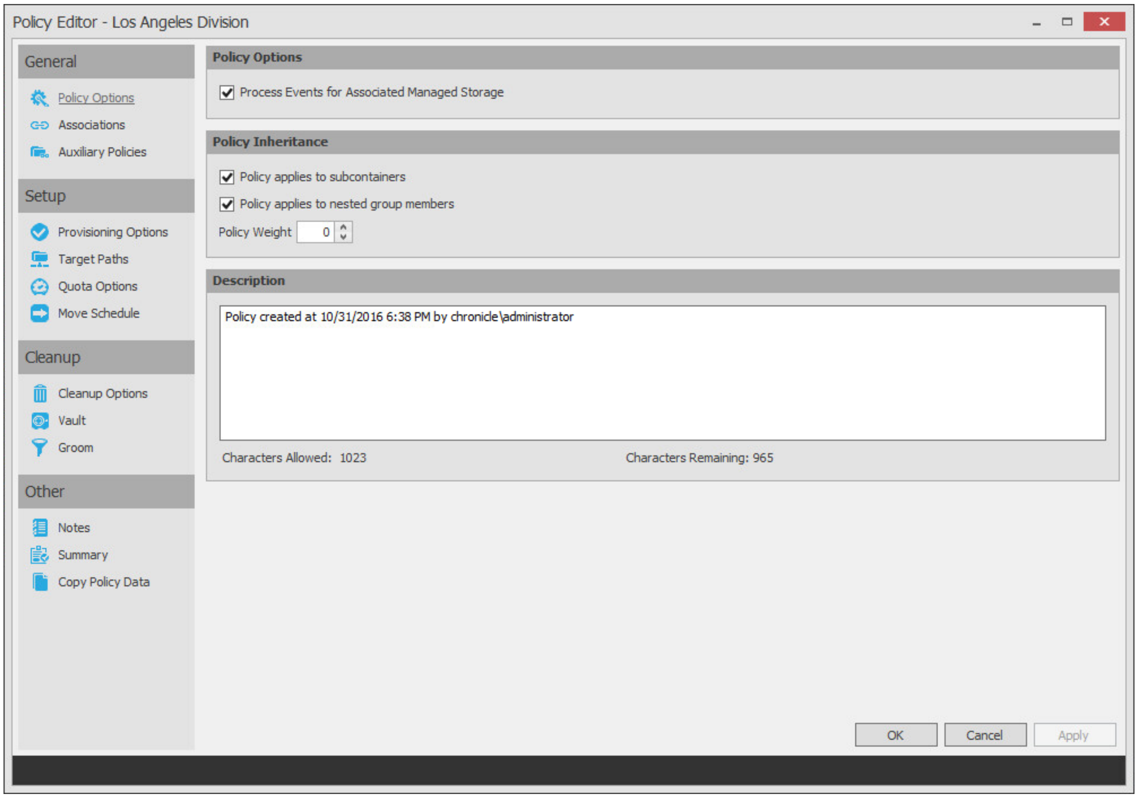
Name

Policy Type: User

Managed Path Type: Home Folder

4 Specify a descriptive name for the policy, such as “Los Angeles Division,” then click **OK**.

The Policy Options page appears.



Policy Editor - Los Angeles Division

**Policy Options**

☑ Process Events for Associated Managed Storage

**Policy Inheritance**

☑ Policy applies to subcontainers

☑ Policy applies to nested group members

Policy Weight 0

**Description**

Policy created at 10/31/2016 6:38 PM by chronicle\administrator

Characters Allowed: 1023 Characters Remaining: 965

**5** Set the **Policy Options** specifications for the policy:

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

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

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

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

**6** Set the associations:

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

**6b** Click **Add**.

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

**6d** Click **Apply** to save the settings.

**7** Set the provisioning specifications:

**7a** In the **Folder Properties** region, specify the default permissions you want applied to network home folders that are created through this policy. Check the **Set Attributes on Target Folder** check box to activate additional check boxes to specify the desired DOS attributes.

**7b** In the **Home Folder Options** region, indicate the network drive letter to assign to your users.

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

For more information on templates, see Step 3 on page 53.

**7d** Click **Apply** to save the settings.

**8** Set the target paths:

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

**8b** 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.

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

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

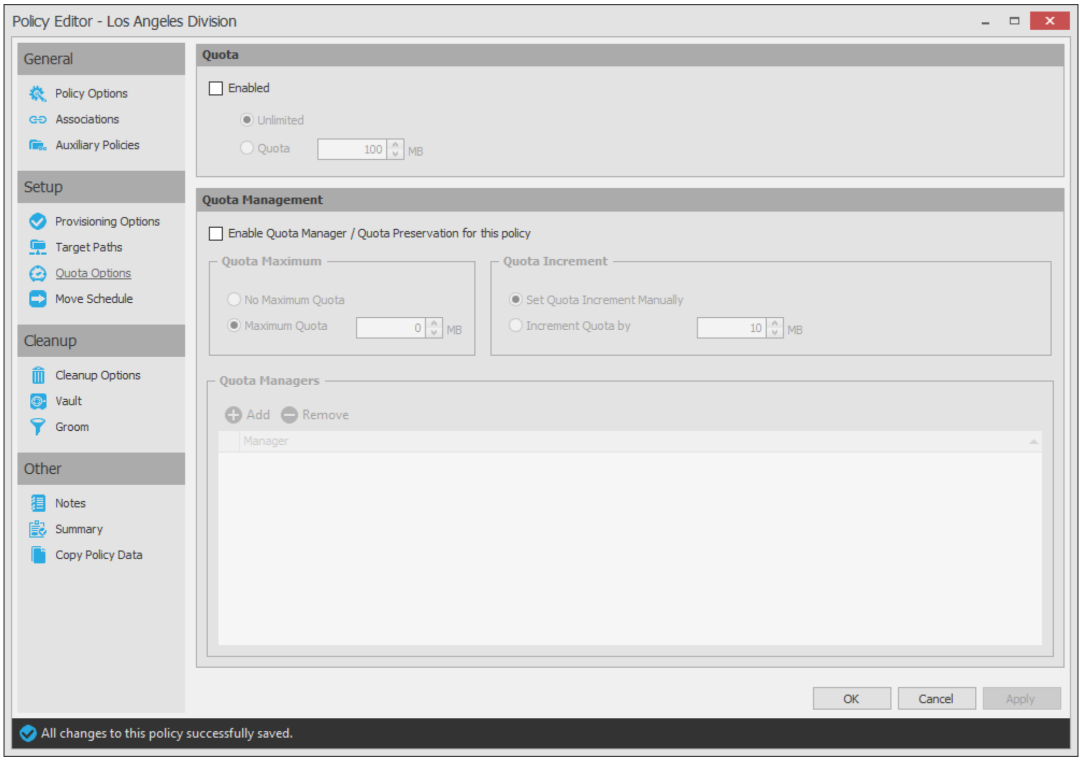
For an explanation of storage distribution, see Section 6.5.4, “Setting Target Paths,” on page 54.

**8e** Leave the other fields as they are currently set.

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

**9** Set the quota options:

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



Quota

□ Enabled

● Unlimited

○ Quota 100 MB

Quota Management

□ Enable Quota Manager / Quota Preservation for this policy

Quota Maximum

○ No Maximum Quota

● Maximum Quota 0 MB

Quota Increment

● Set Quota Increment Manually

○ Increment Quota by 10 MB

Quota Managers

All changes to this policy successfully saved.

**9b** In the **Quota** region, click **Enabled** and specify the initial quota limit assigned to all users associated with this policy.

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

**9d** Select one of the following Quota Maximum options:

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

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

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

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

**10** Set the move schedule:

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

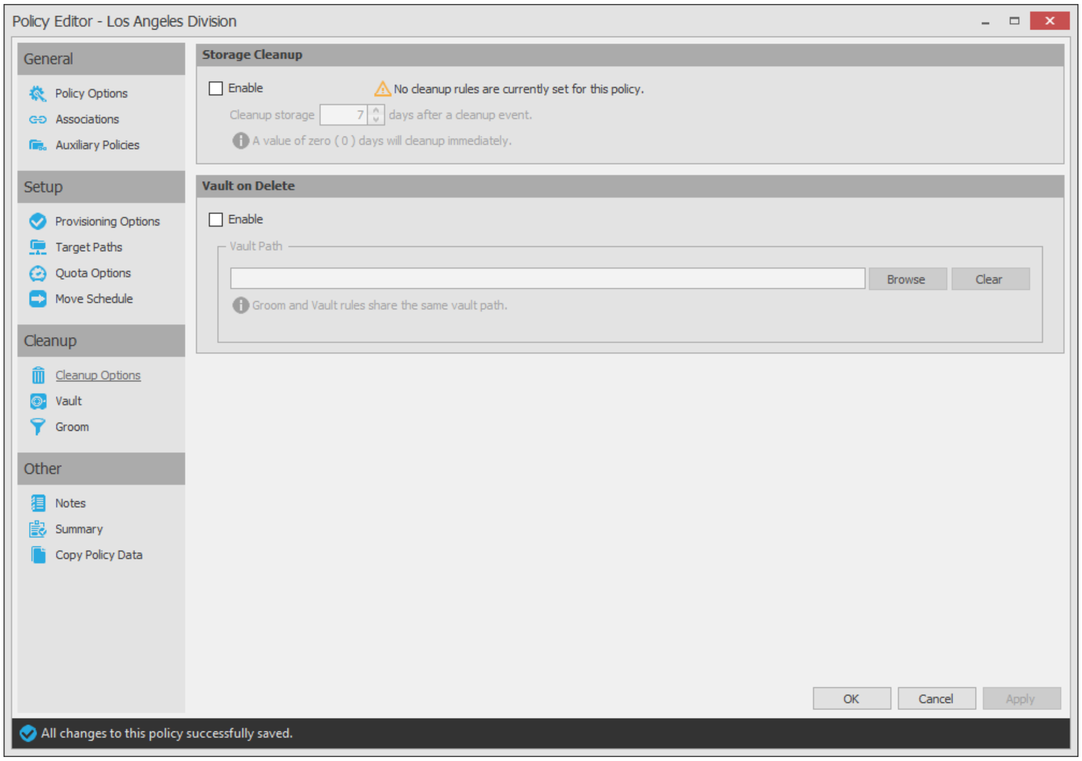
**10b** Specify the hours when Storage Manager can perform movement of data between multiple policy paths.

For more information on movement of data between multiple policy paths, see Section 6.5.6, “Setting the Move Schedule,” on page 58.

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

**11** Set the cleanup options:

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



Storage Cleanup

☐ Enable

No cleanup rules are currently set for this policy.

Cleanup storage 7 days after a cleanup event.

A value of zero ( 0 ) days will cleanup immediately.

Vault on Delete

☐ Enable

Vault Path

Groom and Vault rules share the same vault path.

All changes to this policy successfully saved.

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

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

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

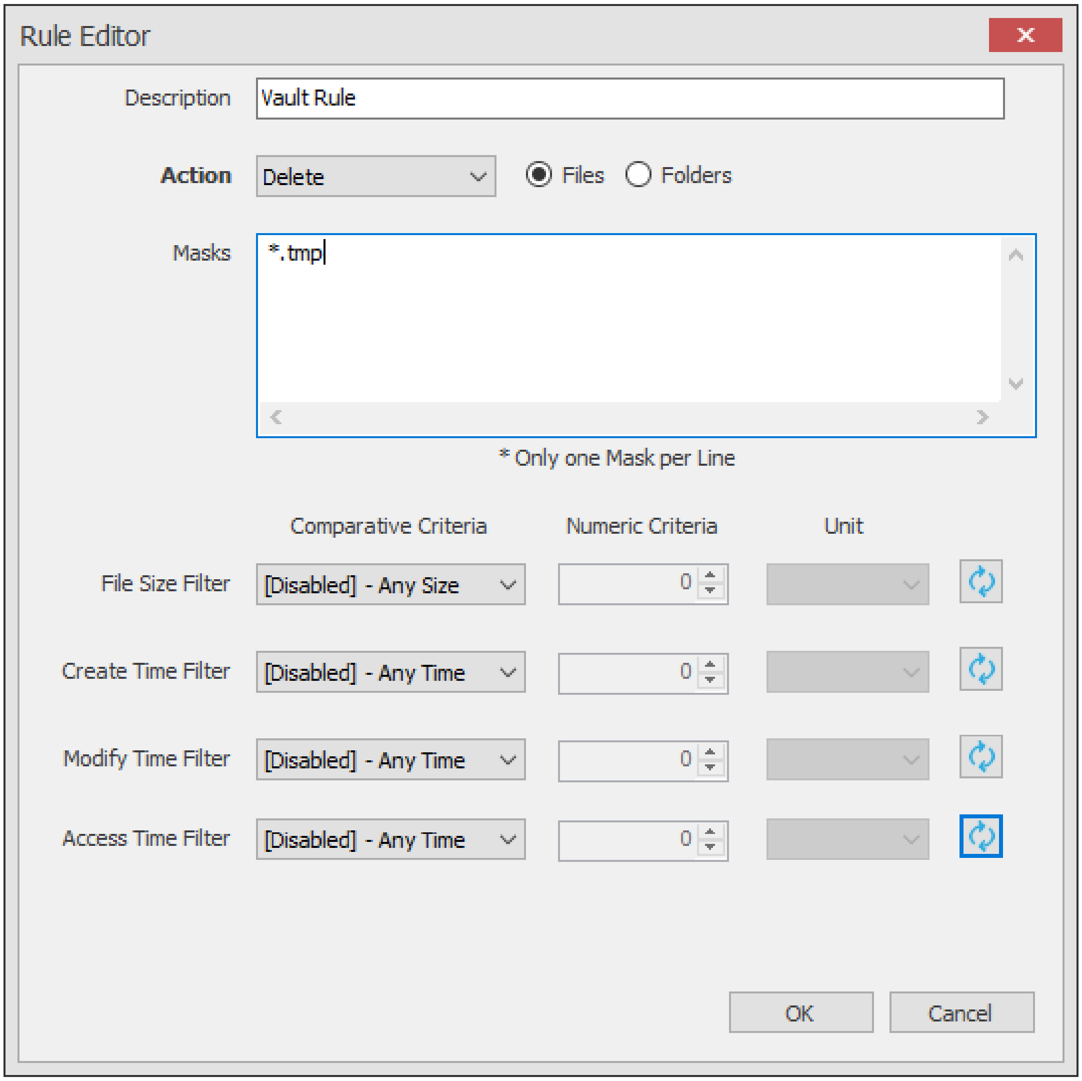
**11d** Click **Apply** to save your settings.

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

**12** Set the vault rules:

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

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



Rule Editor

Description: Vault Rule

**Action**: Delete ● Files ○ Folders

Masks: *.tmp

* Only one Mask per Line

| | Comparative Criteria | Numeric Criteria | Unit |
|---|---|---|---|
| File Size Filter | [Disabled] - Any Size | 0 | |
| Create Time Filter | [Disabled] - Any Time | 0 | |
| Modify Time Filter | [Disabled] - Any Time | 0 | |
| Access Time Filter | [Disabled] - Any Time | 0 | |

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

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

**13** Set the groom rules:

**13a** In the left pane, click **Groom**.

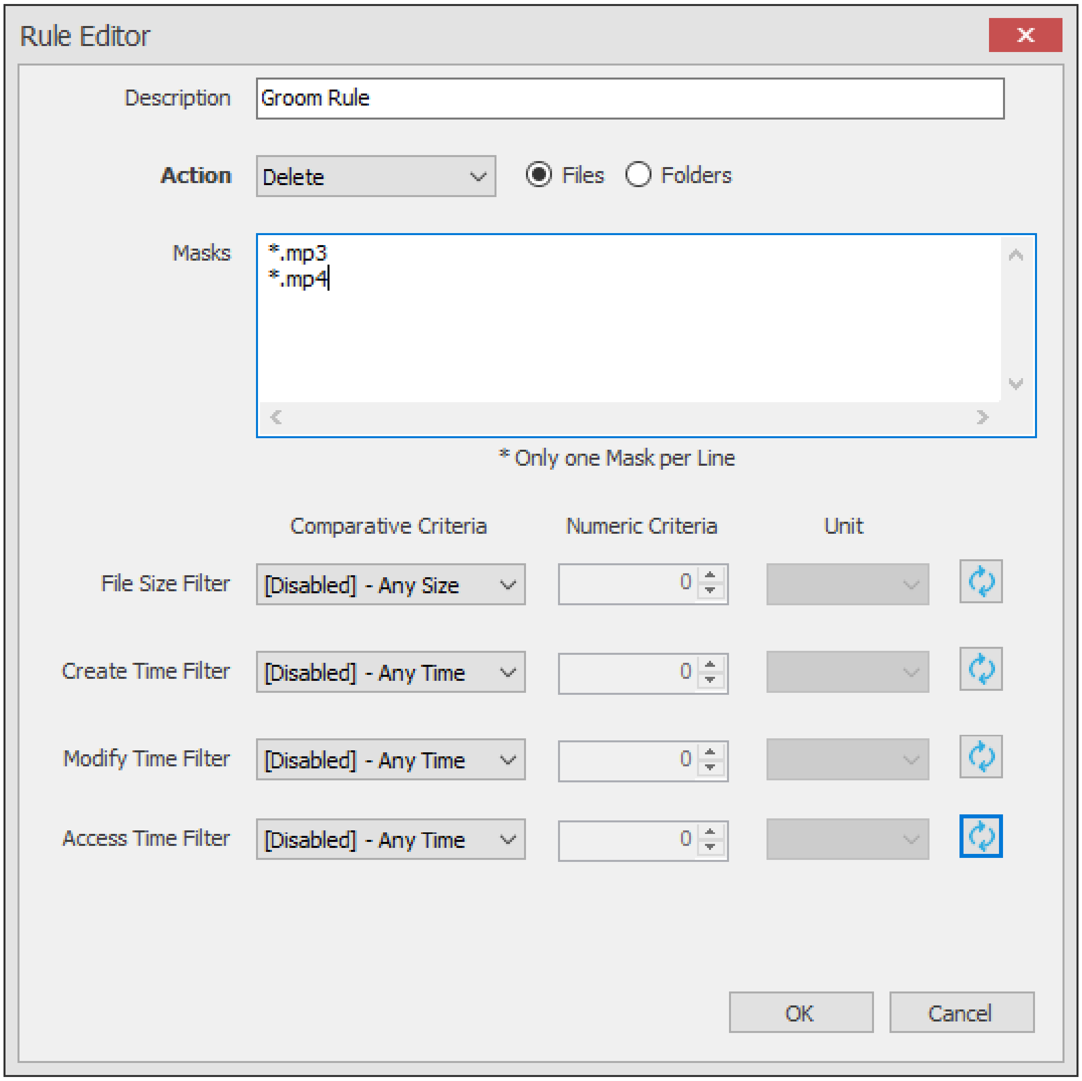
**13b** Click **Add**.

This brings up the Rule Editor dialog box.

**13c** Select either **Vault**, **Delete**, or **Ignore** from the **Action** drop-down menu to specify whether to vault, delete, or ignore files or folders.

**13d** In the **Masks** 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.

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



Rule Editor

Description: Groom Rule

Action: Delete ● Files ○ Folders

Masks:
*.mp3
*.mp4

* Only one Mask per Line

| | Comparative Criteria | Numeric Criteria | Unit |
|---|---|---|---|
| File Size Filter | [Disabled] - Any Size | 0 | |
| Create Time Filter | [Disabled] - Any Time | 0 | |
| Modify Time Filter | [Disabled] - Any Time | 0 | |
| Access Time Filter | [Disabled] - Any Time | 0 | |

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

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

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

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

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

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

## 5.8 Removing a Preexisting Process for Creating User Home Folders

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

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

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

## 5.9 Testing the User Home Folder Policy

You should now create a test user to confirm that Storage Manager 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 Section 5.7, "Creating a User Home Folder Policy," on page 39.
2. In SMAdmin, click the **Home** 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**.

   This displays the View Permissions page.
6. Verify that the rights that you set in Step 7a on page 40 are those that you set in the policy.
7. Click **OK** to close the View Permissions page.
8. Right-click and select **Quota**.

   This displays the View Quota dialog box.
9. Verify that the quota specifications that you set in Step 9 on page 41 are those that you set in the policy.
10. Click **OK** to close the View Quota dialog box.

## 5.10 Performing a Consistency Check

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

1. In SMAdmin, click the **Home** 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.**

The Take Action – User Mode page appears.

6 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).

## 5.11 Running Management Actions

This procedure does the cataloging that enables the existing storage to be managed by Storage Manager.

1 In SMAdmin, click the **Home** 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.

For more information on these, and other Management Actions, see Section 13.1.6, “Actions,” on page 268.

## 5.12 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.

When renaming a user object, you must rename the SAM (Service Account Manager), whose value is used to create managed storage.

2 In SMAdmin, while you are still displaying the users through the **Objects** form, click **Refresh** to refresh the screen and see the renamed user.

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

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

## 5.13 Testing a Cleanup Rule

This procedure lets you verify that Storage Manager 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 on page 42, open SMAdmin, click the **Home** tab and then click **Events** to view any information indicating the deferred number of days for the storage cleanup.

3 Click **Path Analysis**.

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

5 (Conditional) If you set your policy to vault deleted storage, browse to the location in the left pane where you chose to vault deleted storage in Step 11c on page 42 and verify that TESTUSER2 was vaulted:

    5a If you set your policy to delay the cleanup of user storage for a set amount of days in Step 11b on page 42, click **Events** to view details on deferred action.

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

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

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

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

## 5.14 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 Chapter 6, "Managing User Home Folders," on page 49, which provides a more comprehensive discussion of performing user-based storage tasks in SMAdmin.

When you have a better understanding of the user-based storage capabilities in Storage Manager, you can proceed to have Storage Manager manage your collaborative-based storage. Refer to Chapter 8, "Managing Collaborative Storage," on page 87 for a comprehensive discussion and procedures for performing collaborative storage tasks.

# 6 Managing User Home Folders

## 6.1 Overview

In Chapter 5, “Managing Existing User Storage,” on page 33, 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

## 6.2 User Policies

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

- Domain
- Organizational Unit
- Security Group
- User

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

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

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

## 6.3 Setting Up a Vault Location

Vaulting is the process of saving the contents of the object's managed storage after the object has been removed from Active Directory. If your user policies are to include vault rules, you must first set up a storage location (share) where the policy will vault the storage.

Ensure that the SMProxyRights group has Full Control permissions to the share hosting the vault path.

## 6.4 Enabling Your Network for Quota Management

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

**IMPORTANT:** Storage Manager cannot manage quotas on home folders, collaborative storage folders, or auxiliary storage hosted on Windows Server 2003 machines. Furthermore, Storage Manager cannot manage quotas on NAS devices.

For all Windows Server 2008 and later servers hosting home, collaborative, or auxiliary storage managed by Storage Manager 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 Section B.1, "Windows Firewall Requirements," on page 335.

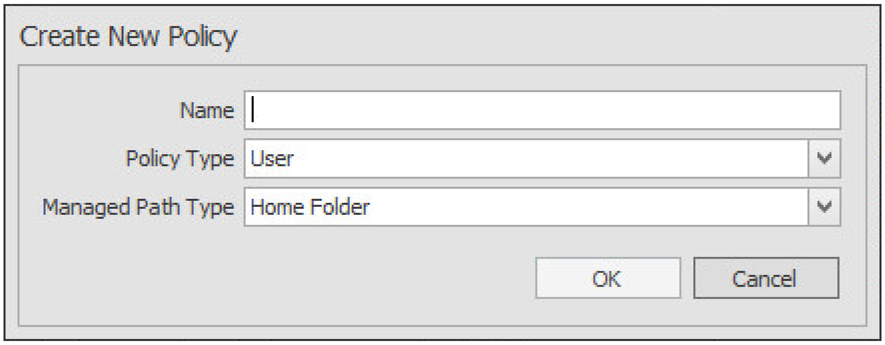
The process for setting an exception rule differs among the various offerings of Windows Server.

## 6.5 Creating a User Home Folder Policy

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

1. In SMAdmin, click the **Home** tab.
2. Click **Policies**.
3. In the **Manage** menu, select **New > User Home Folder.**

   The following dialog box appears:



Create New Policy

Name

Policy Type: User

Managed Path Type: Home Folder

4 Specify a descriptive name in the **Name** field and leave the **User** and **Home Folder** options selected.

The Policy Options page appears.

5 Continue with Section 6.5.1, “Setting Policy Options,” on page 51.

## 6.5.1 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 domain or 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 Section 5.6, “Creating a Blocking Policy,” on page 37.

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 domain or 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, Storage Manager uses this setting to determine which policy to apply. Storage Manager 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 Section 6.5.2, “Setting Associations,” on page 52.

### 6.5.2 Setting Associations

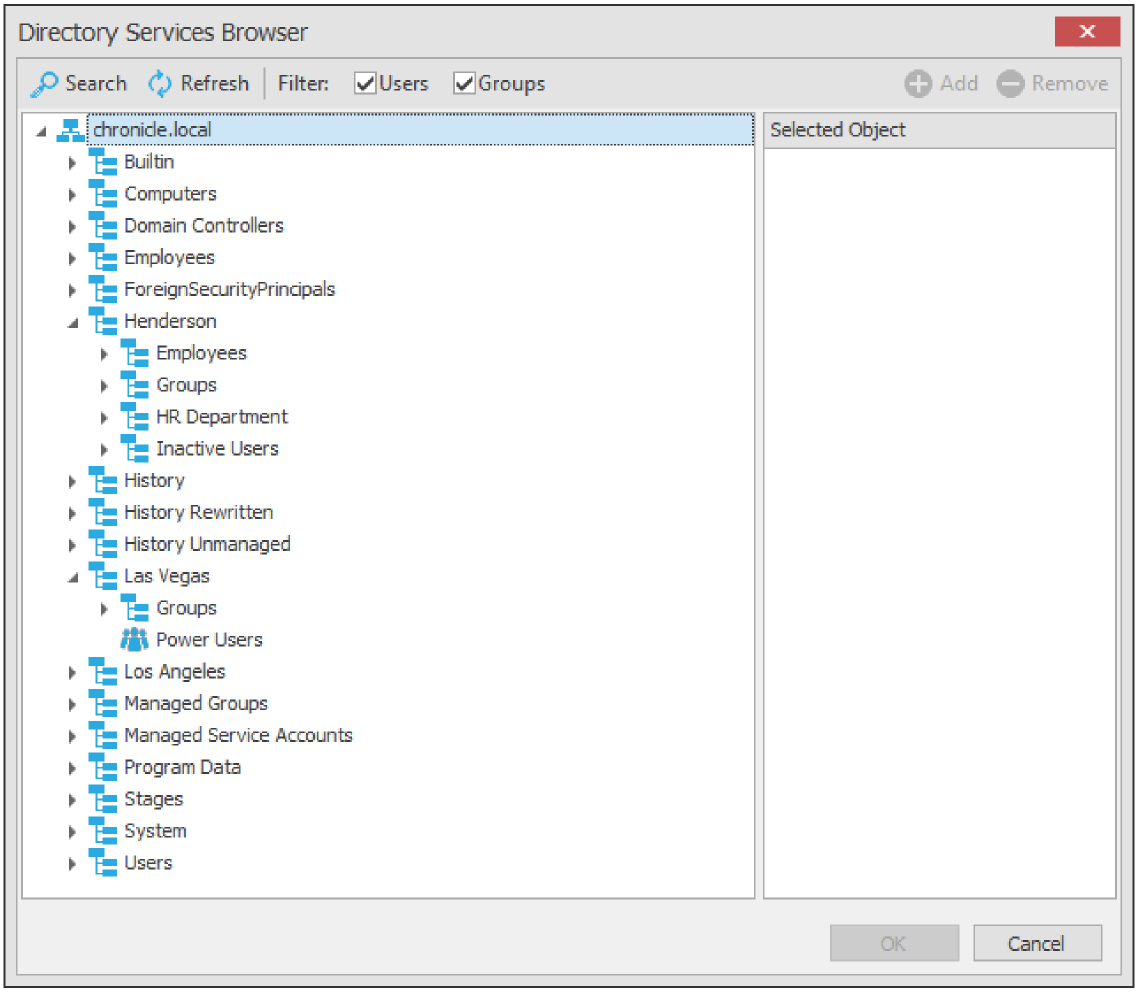
Associations is where you assign the policy you are creating to a domain, organizational unit, group, or user object.

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 domain, organizational unit, Group object, or User object you want to associate the policy to.



Filter: ☑ Users ☑ Groups

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, `CN=Tellers,OU=HR Department,OU=Henderson,DC=chronicle,DC=local`.

6 Click **OK** to close the Directory Services Browser.

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

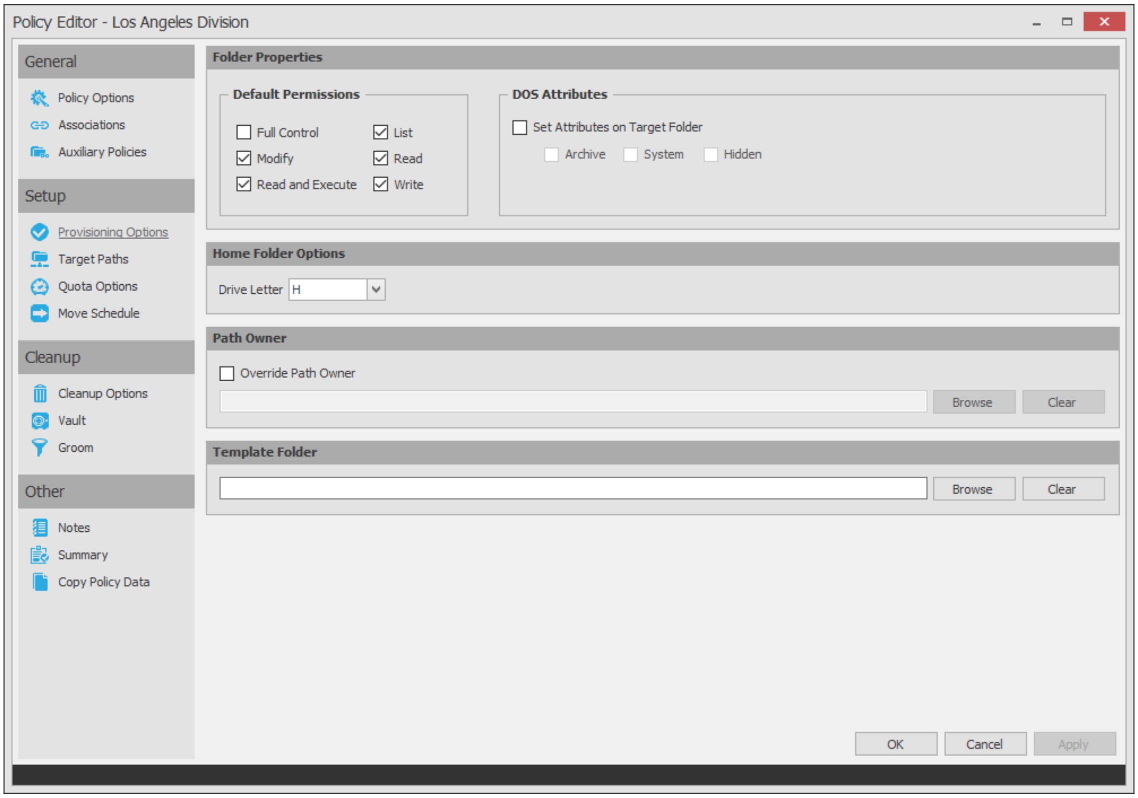
8 Proceed with Section 6.5.3, “Setting Provisioning Options,” on page 53.

## 6.5.3 Setting Provisioning Options

The Provisioning Options page is where you indicate home folder rights, 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:



Folder Properties

Default Permissions

☐ Full Control ☑ List
☑ Modify ☑ Read
☑ Read and Execute ☑ Write

DOS Attributes

☐ Set Attributes on Target Folder
☐ Archive ☐ System ☐ Hidden

Home Folder Options

Drive Letter H

Path Owner

☐ Override Path Owner

Template Folder

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

**Default Permissions:** By default, Storage Manager grants the user all file rights to the managed folder except for Full Control. Granting Full Control is not recommended because it provides administrator rights to the managed path 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, for example, you could enable the Hidden attribute by selecting the **Hidden** check box.

By default, Storage Manager 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 rights—with the exception of administrative rights—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 Click **Apply** to save your settings.

6 Proceed with Section 6.5.4, "Setting Target Paths," on page 54.

### 6.5.4 Setting Target Paths

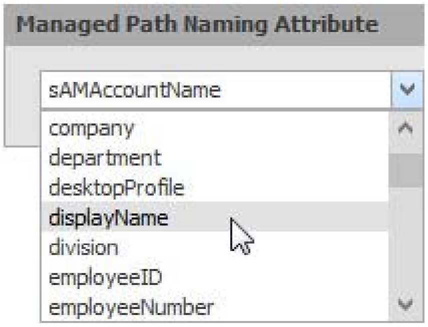
The Target Paths page is where you select the naming attribute for the managed path, as well as set the paths to the shares where user home folders will be hosted.

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

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 Storage Manager to create a home folder with a name like WSanders, rather than SA74556, you can select a different attribute from the drop-down list.



Managed Path Naming Attribute

sAMAccountName

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 Storage Manager 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 Appendix F, "Managed Path Naming Attribute Specifications," on page 357.

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\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\HOME\H\BSMITH.`

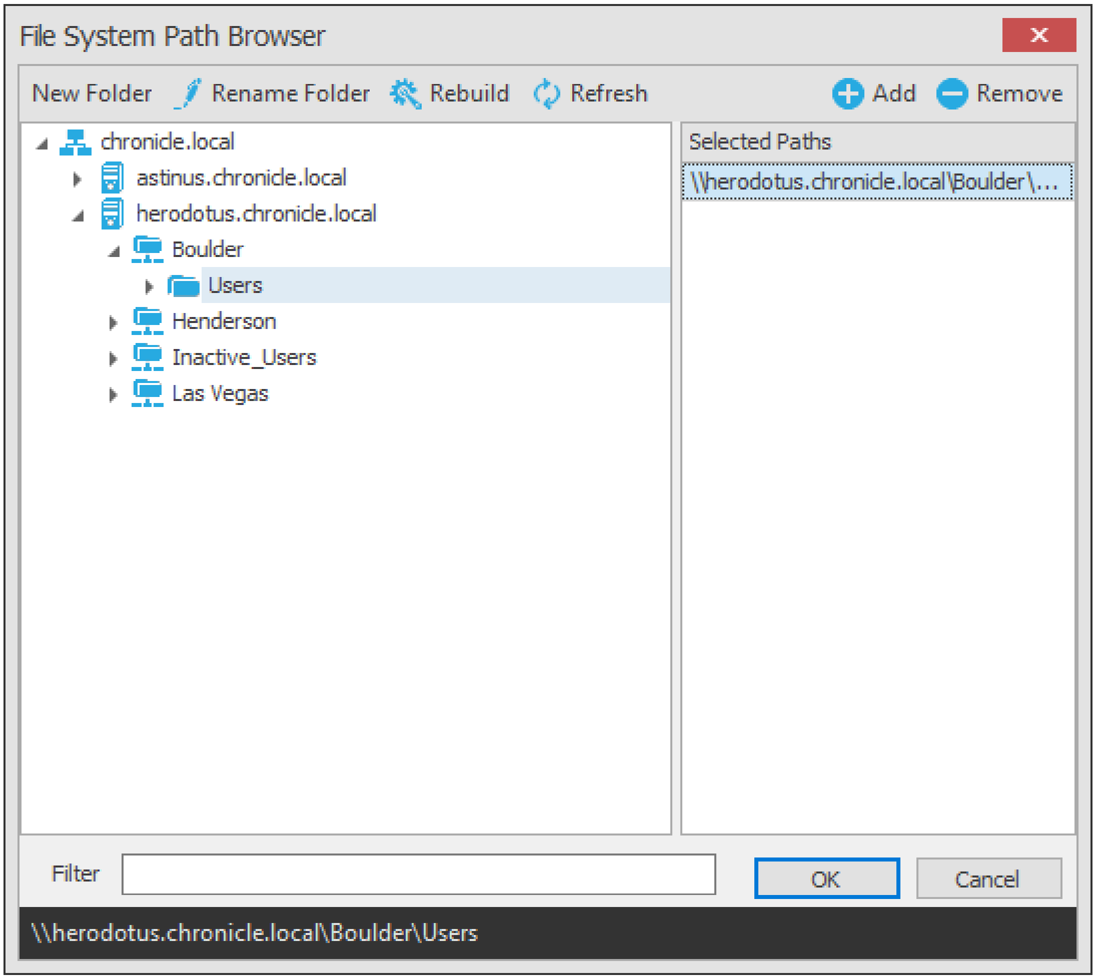
The **Last Letter** means the last character of the attribute Storage Manager uses to create storage. Once again, Storage Manager uses the SAM, not the character of the last name.

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\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 Storage Manager accesses to attempt to create a home folder before it suspends the attempt.

For example, suppose you have 100 target paths and you're using **Random Distribution** and the **Maximum Unreachable Paths** setting is 20. Storage Manager 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.



\\herodotus.chronicle.local\Boulder\...

\\herodotus.chronicle.local\Boulder\Users

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

7 Proceed to Section 6.5.5, “Setting Quota Options,” on page 56.

## 6.5.5 Setting Quota Options

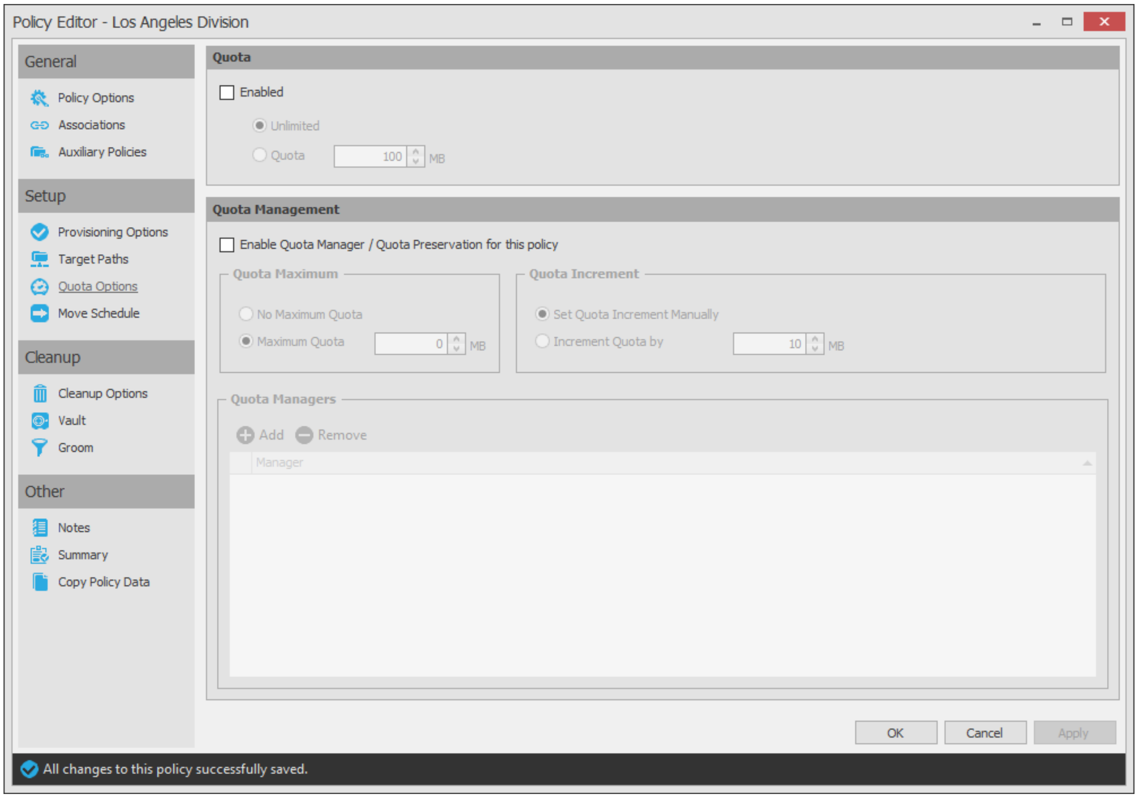
This page lets you establish user storage quotas. Until quota management is established, users have unlimited storage disk space for their home folders.

**NOTE:** 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—for example, a help desk administrator or technical support representative—who is granted the ability to increase a user’s quota, without having rights to the file system. Quota management actions are performed through Quota Manager, which is a separate Web browser-based management interface. For more information on Quota Manager, see Chapter 9, “Using Quota Manager,” on page 119.

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

The following page appears:



Quota

□ Enabled

● Unlimited

○ Quota 100 MB

Quota Management

□ Enable Quota Manager / Quota Preservation for this policy

Quota Maximum

○ No Maximum Quota

● Maximum Quota 0 MB

Quota Increment

● Set Quota Increment Manually

○ Increment Quota by 10 MB

Quota Managers

All changes to this policy successfully saved.

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 enable quota preservation.

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

**Quota Maximum:** Indicate whether the 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 SMAdmins group will be able to use the Quota Manager Web interface.

5. Click **Apply** to save your settings.
6. Proceed with Section 6.5.6, “Setting the Move Schedule,” on page 58.

## 6.5.6 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 Section 6.5.7, “Setting Cleanup Options,” on page 58.

## 6.5.7 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, weeks, or years 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 Section 6.5.8, “Setting Vault Rules,” on page 58.

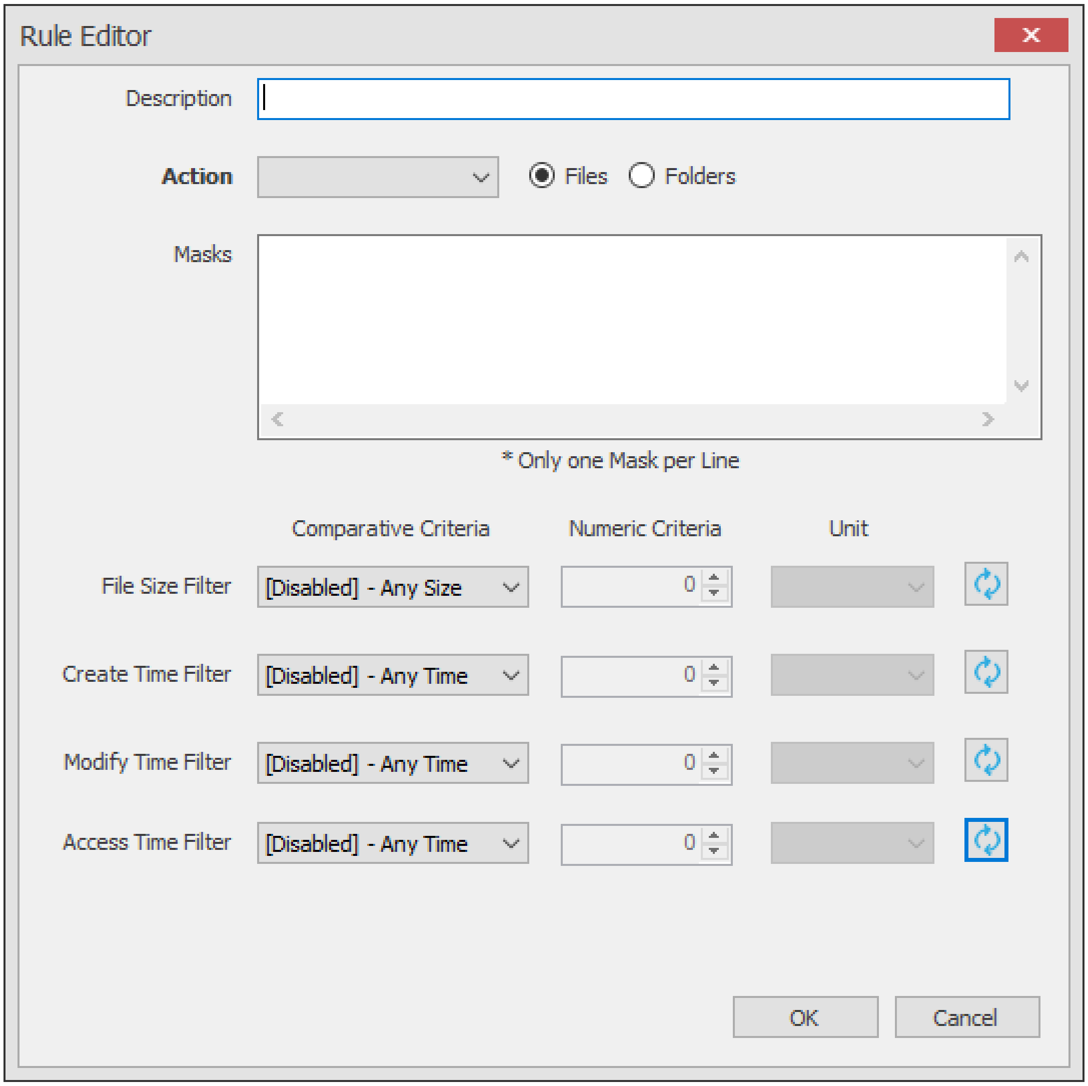
## 6.5.8 Setting Vault Rules

When a User object is removed from Active Directory, you can have Storage Manager vault the contents of the user’s home folder from primary storage to less expensive secondary storage. Storage Manager 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.



● Files ○ Folders

* Only one Mask per Line

| | Comparative Criteria | Numeric Criteria | Unit |
|---|---|---|---|
| File Size Filter | [Disabled] - Any Size | 0 | |
| Create Time Filter | [Disabled] - Any Time | 0 | |
| Modify Time Filter | [Disabled] - Any Time | 0 | |
| Access Time Filter | [Disabled] - Any Time | 0 | |

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

  For example, "Files to delete before vaulting," or "Files to vault."

4 Fill in the following fields:

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

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

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

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

Selecting **Folders** disables the filter settings in the lower portion of the 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 vault rule you are creating is specific to files, complete the applicable filter settings.

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

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

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

8 Proceed with Section 6.5.9, "Setting Groom Rules," on page 60.

### 6.5.9 Setting Groom Rules

Grooming rules in Storage Manager 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 SMAdmin. For more information, see Section 13.1.6, "Actions," on page 268.

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 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 **Mask** text box according to what is indicated in the **Action** drop-down menu. Choosing any of the other options from the drop-down menu lets you indicate files to delete or vault according to size, when created, when last modified, and when last accessed.

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

7 Proceed with Section 6.5.10, “Notes,” on page 61.

### 6.5.10 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.

### 6.5.11 Policy Summary

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

## 6.6 Creating a User Profile Path Policy

For users in Active Directory who access the network through Remote Desktop Services, Storage Manager 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, Storage Manager 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-name`*`\`*`share-name`*`\`*`users`*`\`*`user`*`\profile.V2`.

For Windows workstations running Windows XP and earlier, the path is similar to the following: `\\`*`server-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 Storage Manager 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.

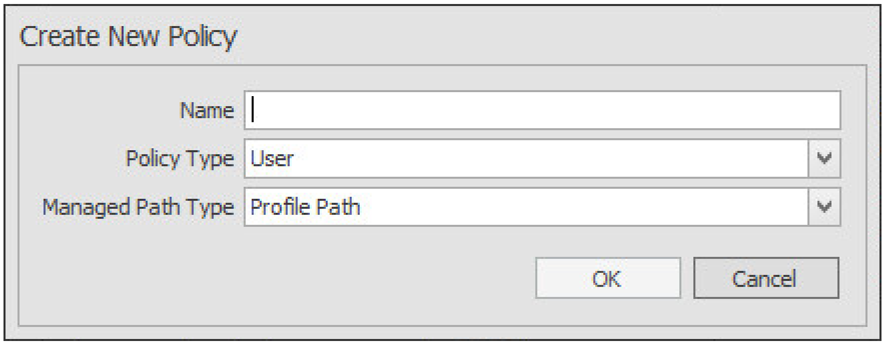
**NOTE:** The Windows Full Control NTFS permission is established and cannot be modified.

### 6.6.1 To Create a User Profile Path Policy

1 In SMAdmin, click **Policies**.

2 In the **Manage** menu, select **New > User Profile Path**.

The following dialog box appears:



Create New Policy

Name

Policy Type: User

Managed Path Type: Profile Path

3. Specify a name in the **Name** field and leave the **User** and **Profile Path** options selected.

   The Policy Options page appears.

4. 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 Section 6.5.1, “Setting Policy Options,” on page 51.

**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 Section 6.5.2, “Setting Associations,” on page 52.

**Auxiliary Policies:** Lets you link an Auxiliary policy to the profile path. For more information on Auxiliary policies, see Section 6.11, “Using a Policy to Manage Auxiliary Storage,” on page 69.

**Provisioning Options:** The Provisioning Options page provides only the Path Owner and Template Folder settings that are described in detail in Section 6.5.3, “Setting Provisioning Options,” on page 53.

**NOTE:** 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 Paths:** The fields presented on the Target Paths page are identical to those presented when you create a user home folder policy. For an explanation of the page, along with procedures for setting target paths, see Section 6.5.4, “Setting Target Paths,” on page 54.

**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 Section 6.5.5, “Setting Quota Options,” on page 56.

**Move Schedule:** The fields presented on the Move Schedule page are identical to those presented when you create a user home folder policy. For an explanation of the page, along with procedures for setting the move schedule, see Section 6.5.6, “Setting the Move Schedule,” on page 58.

**Cleanup Options:** The fields presented on the Cleanup Options page are identical to those presented when you create a user home folder policy. For an explanation of the page, along with procedures for setting cleanup options, see Section 6.5.7, “Setting Cleanup Options,” on page 58.

**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 Section 6.5.8, “Setting Vault Rules,” on page 58.

**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 Section 6.5.9, “Setting Groom Rules,” on page 60.

## 6.7 Creating a User Remote Desktop Services Home Folder Policy

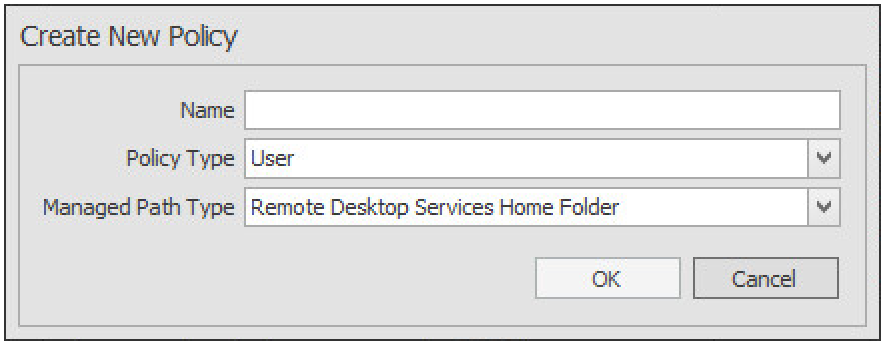
Remote Desktop Services provides users network access from remote client machines. Storage Manager provisions and manages these users’ home folders through User Remote Desktop Services Home Folder policies.

### 6.7.1 To Create a User Remote Desktop Services Home Folder Policy

1 In SMAdmin, click **Policies**.

2 In the **Manage** menu, select **New > User Remote Desktop Services Home Folder**.

The following dialog box appears:



Create New Policy

Name:

Policy Type: User

Managed Path Type: Remote Desktop Services Home Folder

3 Specify a name in the **Name** field and leave the **User** and **Remote Desktop Services Home Folder** options selected.

The Policy Options page appears.

4 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 Section 6.5.1, “Setting Policy Options,” on page 51.

**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 Section 6.5.2, “Setting Associations,” on page 52.

**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 Section 6.5.3, “Setting Provisioning Options,” on page 53.

**Target Paths:** The fields presented on the Target Paths page are identical to those presented when you create a user home folder policy. For an explanation of the page, along with procedures for setting target paths, see Section 6.5.4, “Setting Target Paths,” on page 54.

**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 Section 6.5.5, “Setting Quota Options,” on page 56.

**Move Schedule:** The fields presented on the Move Schedule page are identical to those presented when you create a user home folder policy. For an explanation of the page, along with procedures for setting the move schedule, see Section 6.5.6, “Setting the Move Schedule,” on page 58.

**Cleanup Options:** The fields presented on the Cleanup Options page are identical to those presented when you create a user home folder policy. For an explanation of the page, along with procedures for setting cleanup options, see Section 6.5.7, “Setting Cleanup Options,” on page 58.

**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 Section 6.5.8, “Setting Vault Rules,” on page 58.

**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 Section 6.5.9, “Setting Groom Rules,” on page 60.

## 6.8 Creating a User Remote Desktop Services Profile Path Policy

Storage Manager 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, Storage Manager 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, Storage Manager 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-name`*`\`*`share-name`*`\`*`users`*`\`*`user`*`\profile.V2`

For Windows workstations running Windows XP and earlier, the path is similar to: `\\`*`server-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.

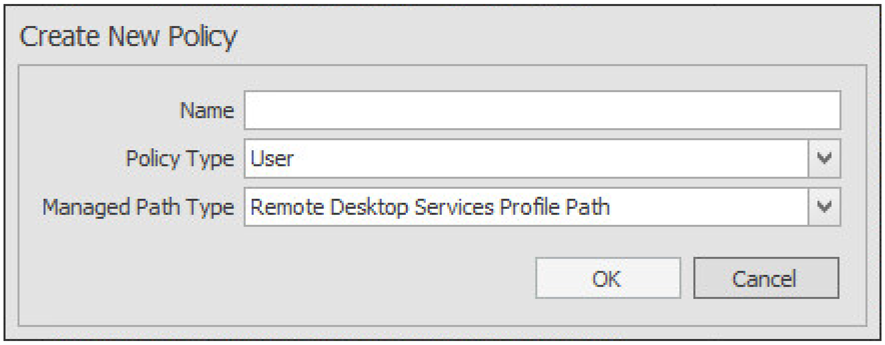
When Storage Manager has provisioned a profile path for the Remote Desktop Services user, it enters settings in the **Profile path** field of the User object’s Remote Desktop Services Profile property.

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

## 6.8.1 To Create a User Remote Desktop Services Profile Path Policy:

1. In SMAdmin, click **Policies.**
2. In the **Manage** menu, select **New > User Remote Desktop Services Profile Path**.

   The following dialog box appears:



3. Specify a name in the **Name** field and leave the **User** and **Remote Desktop Services Profile Path** options selected.

   The Policy Options page appears.
4. 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 Section 6.5.1, "Setting Policy Options," on page 51.

**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 Section 6.5.2, "Setting Associations," on page 52.

**Provisioning Options:** The Provisioning Options page provides only the Path Owner and Template Folder settings that are described in detail in Section 6.5.3, "Setting Provisioning Options," on page 53.

**NOTE:** 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 Paths:** The fields presented on the Target Paths page are identical to those presented when you create a user home folder policy. For an explanation of the page, along with procedures for setting target paths, see Section 6.5.4, "Setting Target Paths," on page 54.

**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 Section 6.5.5, "Setting Quota Options," on page 56.

**Move Schedule:** The fields presented on the Move Schedule page are identical to those presented when you create a user home folder policy. For an explanation of the page, along with procedures for setting the move schedule, see Section 6.5.6, "Setting the Move Schedule," on page 58.

**Cleanup Options:** The fields presented on the Cleanup Options page are identical to those presented when you create a user home folder policy. For an explanation of the page, along with procedures for setting cleanup options, see Section 6.5.7, "Setting Cleanup Options," on page 58.

**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 Section 6.5.8, "Setting Vault Rules," on page 58.

**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 Section 6.5.9, "Setting Groom Rules," on page 60.

## 6.9 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 Storage Manager, 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.

- Section 6.9.1, "Creating an Inactive Users Organizational Unit," on page 66
- Section 6.9.2, "Creating an Inactive Users Folder," on page 66
- Section 6.9.3, "Creating an Inactive Users Policy," on page 67
- Section 6.9.4, "Setting Inactive Users Policy Associations," on page 67
- Section 6.9.5, "Setting Inactive Users Policy Provisioning Options," on page 67
- Section 6.9.6, "Setting Inactive Users Policy Target Paths," on page 67
- Section 6.9.7, "Setting Inactive Users Policy Cleanup Options," on page 68

### 6.9.1 Creating an Inactive Users Organizational Unit

1. In SMAdmin, click the **Home** 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.

### 6.9.2 Creating an Inactive Users Folder

1. Launch Windows Explorer.
2. On a network share, create a folder to store inactive user home folders.

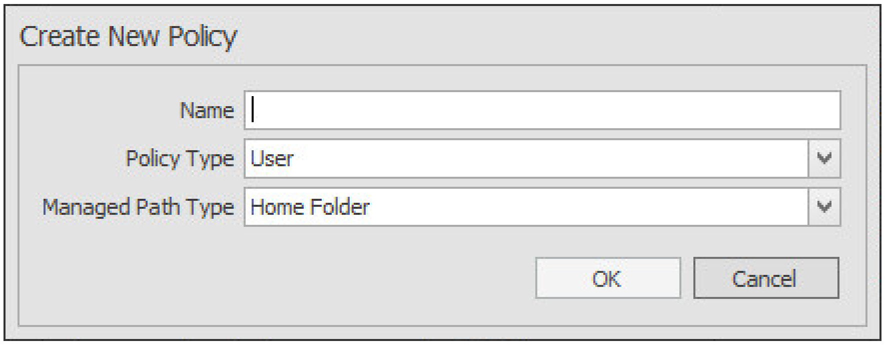
   Give the folder a descriptive name, such as "Inactive Users."

## 6.9.3 Creating an Inactive Users Policy

1 In SMAdmin, click the **Home** tab.

2 In the **Manage** menu, select **New > User Home Folder.**

The following dialog box appears:



Create New Policy

Name:

Policy Type: User

Managed Path Type: Home Folder

3 Specify a descriptive name in the **Name** field, leave the **User** and **Home Folder** options selected, then click **OK**.

The Policy Options page appears.

4 Continue with Section 6.9.4, “Setting Inactive Users Policy Associations,” on page 67.

## 6.9.4 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 on page 66.

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 Section 6.9.5, “Setting Inactive Users Policy Provisioning Options,” on page 67.

## 6.9.5 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 Section 6.9.6, “Setting Inactive Users Policy Target Paths,” on page 67.

## 6.9.6 Setting Inactive Users Policy Target Paths

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

2 Click **Add**, then browse to and select the inactive users folder that your created in Step 2 on page 66.

3 Click **Add** to add the inactive users folder to the **Selected Items** panel.

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

5 Proceed with Section 6.9.7, “Setting Inactive Users Policy Cleanup Options,” on page 68.

### 6.9.7 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 **OK** to save the settings.

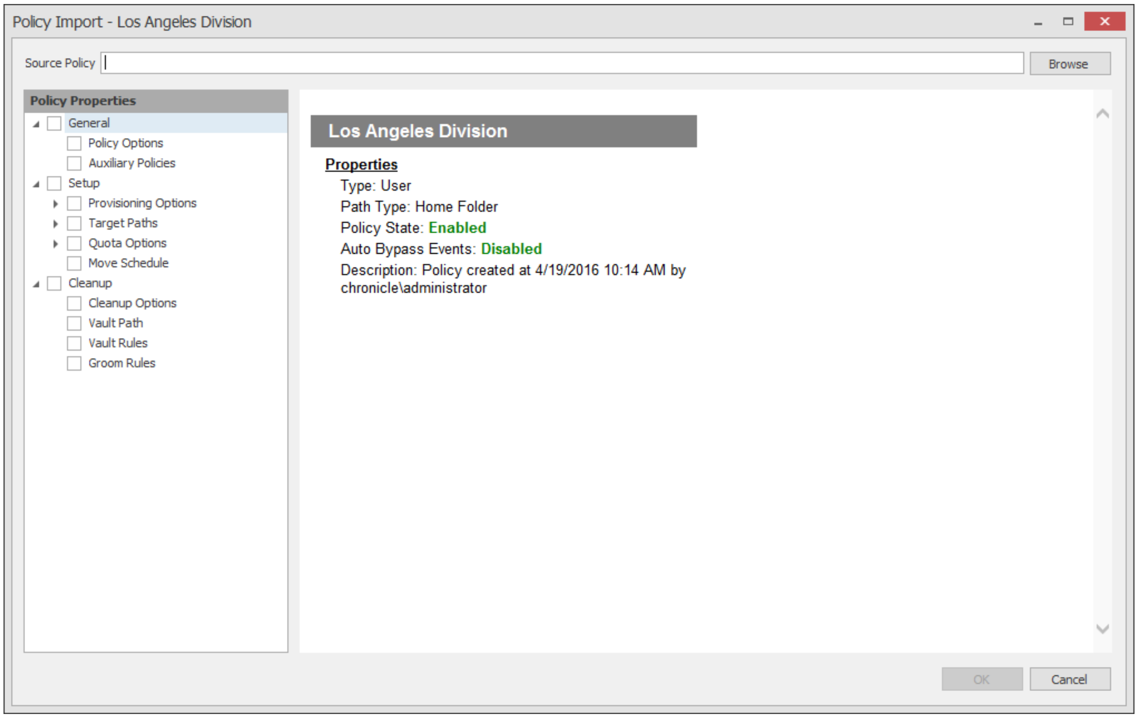
## 6.10 Copying Policy Data

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

1 In SMAdmin, click the **Home** 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.



Los Angeles Division

Properties

Type: User

Path Type: Home Folder

Policy State: Enabled

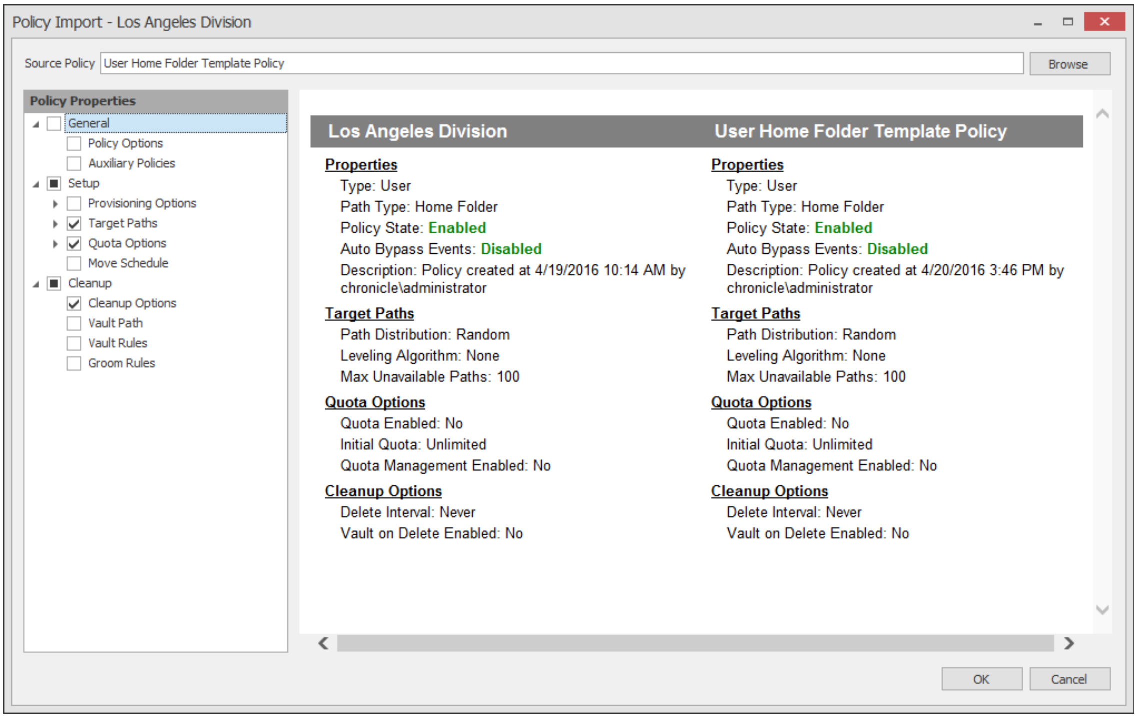
Auto Bypass Events: Disabled

Description: Policy created at 4/19/2016 10:14 AM by chronicle\administrator

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.



Source Policy: User Home Folder Template Policy

Policy Properties
- □ General
  - □ Policy Options
  - □ Auxiliary Policies
- ■ Setup
  - □ Provisioning Options
  - ☑ Target Paths
  - ☑ Quota Options
  - □ Move Schedule
- ■ Cleanup
  - ☑ Cleanup Options
  - □ Vault Path
  - □ Vault Rules
  - □ Groom Rules

| Los Angeles Division | User Home Folder Template Policy |
|---|---|
| **Properties** | **Properties** |
| Type: User | Type: User |
| Path Type: Home Folder | Path Type: Home Folder |
| Policy State: Enabled | Policy State: Enabled |
| Auto Bypass Events: Disabled | Auto Bypass Events: Disabled |
| Description: Policy created at 4/19/2016 10:14 AM by chronicle\administrator | Description: Policy created at 4/20/2016 3:46 PM by chronicle\administrator |
| **Target Paths** | **Target Paths** |
| Path Distribution: Random | Path Distribution: Random |
| Leveling Algorithm: None | Leveling Algorithm: None |
| Max Unavailable Paths: 100 | Max Unavailable Paths: 100 |
| **Quota Options** | **Quota Options** |
| Quota Enabled: No | Quota Enabled: No |
| Initial Quota: Unlimited | Initial Quota: Unlimited |
| Quota Management Enabled: No | Quota Management Enabled: No |
| **Cleanup Options** | **Cleanup Options** |
| Delete Interval: Never | Delete Interval: Never |
| Vault on Delete Enabled: No | Vault on Delete Enabled: No |

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

## 6.11 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 Storage Manager 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 directory 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.

Storage Manager's life cycle management capabilities easily manage auxiliary storage to the specific needs of the organization. For example, if a user transfers from one city to another and the user home folder is moved to a new Organizational Unit object as a result, the policy can dictate what becomes of the auxiliary storage including moving it, moving it and adjusting the quota settings, leaving it where it currently is, etc. For more information on moving Auxiliary storage, see Section 6.11.4, “Establishing Auxiliary Purpose Mappings,” on page 73.

- Section 6.11.1, “Creating an Auxiliary Storage Policy,” on page 70
- Section 6.11.2, “Linking a User Home Folder Policy to an Auxiliary Storage Policy,” on page 72
- Section 6.11.3, “Provisioning Auxiliary Storage for Existing Users,” on page 72
- Section 6.11.4, “Establishing Auxiliary Purpose Mappings,” on page 73

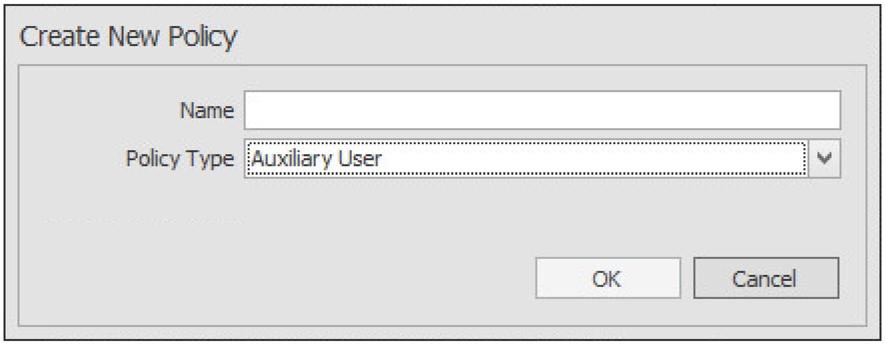
## 6.11.1 Creating an Auxiliary Storage Policy

1 In SMAdmin, click the **Home** tab.

2 Click **Policies**.

3 In the **Manage** menu, select **New > Auxiliary**.

The following dialog box appears:



Create New Policy

Name

Policy Type Auxiliary User

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” on page 70.

### Setting Auxiliary Storage Policy Options

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

2 Proceed with “Enabling Auxiliary Storage Extended Options” on page 70.

### Enabling Auxiliary Storage Extended Options

Auxiliary storage extended options help other tools, such as the AuxMap utility, identify the auxiliary storage policy through additional attributes. For information on the AuxMap utility, see Appendix E, “AuxMap,” on page 355.

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.

This field is used by the AuxMap utility to make auxiliary storage associations.

Micro Focus recommends that once you have made an entry in the **Tag** field, that you do not change it. If the value of the **Tag** field is changed after some users have already had their auxiliary storage provisioned via that policy, the new tag value does not automatically get propagated to those users. Only users who get storage provisioned after the change in the tag value will get the new tag value.

4. In the **Description** field, specify a description of the Auxiliary Storage policy.
5. Click **Apply** to save your settings.
6. Proceed with "Setting Auxiliary Storage Provisioning Options" on page 71.

## Setting Auxiliary Storage Provisioning Options

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

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

1. In the left pane, click **Provisioning Options**.
2. Do one of the following:
   - If you do not want the associated user to have access to the auxiliary storage folder, deselect all of the **Default Rights** check boxes.
   - If you want the associated user to have access to the auxiliary storage folder, select the appropriate permissions from the **Default Rights** check boxes.
3. In the **Template Folder** region, click the **Browse** button, and then specify the template path in the Path Browser dialog box.
4. Click **Apply** to save your settings.
5. Proceed with "Setting Additional Auxiliary Storage Options" on page 71.

## Setting Additional Auxiliary Storage Options

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

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

   The fields presented on the Target Paths page are identical to those presented when you create a User Home Folder policy. For an explanation of the page along with procedures for setting target paths, see Section 6.5.4, "Setting Target Paths," on page 54.

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

   The fields presented on the Quota Options page are identical to those presented when you create a User Home Folder policy. For an explanation of the page, along with procedures for setting quota options, see Section 6.5.5, "Setting Quota Options," on page 56.

**Move Schedule:** The fields presented on the Move Schedule page are identical to those presented when you create a user home folder policy. For an explanation of the page, along with procedures for setting the move schedule, see Section 6.5.6, "Setting the Move Schedule," on page 58.

**Cleanup Options:** The fields presented on the Cleanup Options page are identical to those presented when you create a User Home Folder policy. For an explanation of the page, along with procedures for setting cleanup options, see Section 6.5.7, "Setting Cleanup Options," on page 58.

**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 Section 6.5.8, "Setting Vault Rules," on page 58.

**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 Section 6.5.9, "Setting Groom Rules," on page 60.

2 Proceed with Section 6.11.2, "Linking a User Home Folder Policy to an Auxiliary Storage Policy," on page 72.

### 6.11.2 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 Section 6.11.3, "Provisioning Auxiliary Storage for Existing Users," on page 72.

1. In SMAdmin, click the **Home** 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.

### 6.11.3 Provisioning Auxiliary Storage for Existing Users

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

1. In SMAdmin, click the **Home** 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 **Action**s 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.

### 6.11.4 Establishing Auxiliary Purpose Mappings

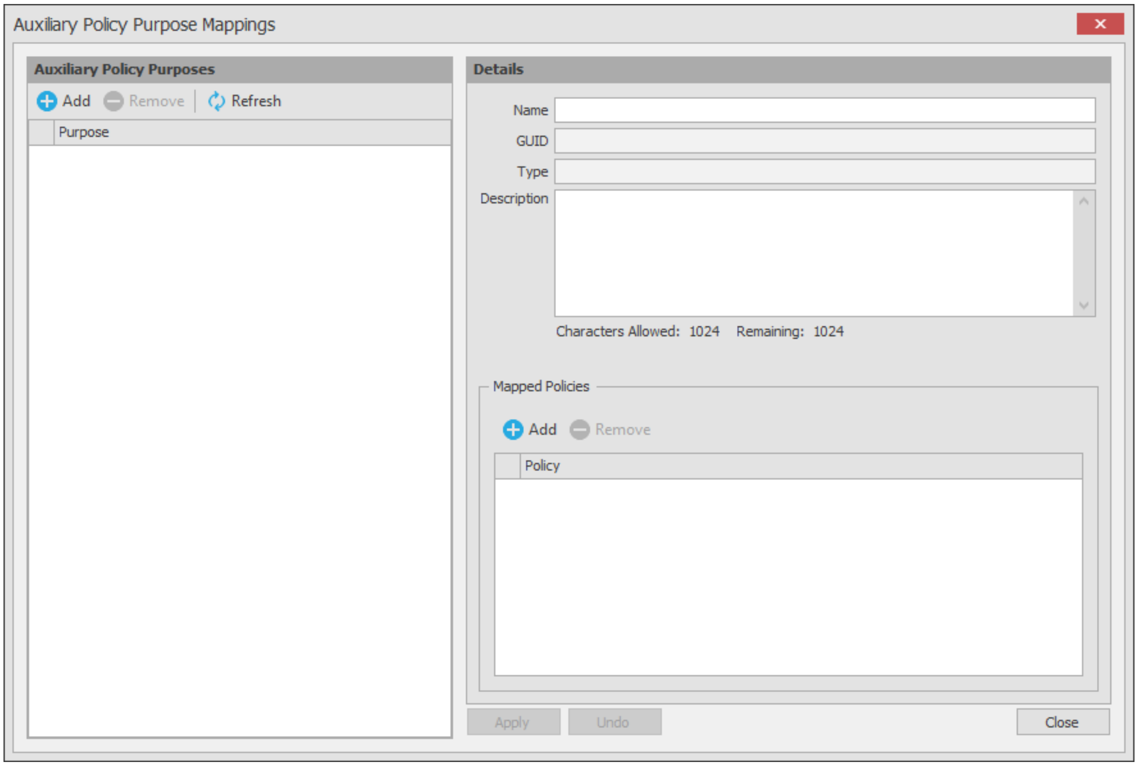
Auxiliary Purpose Mappings are the means of moving a user's auxiliary storage when a user is moved in Active Directory. For example, if a user were moved from the Atlanta container to the Detroit container, and the two container's Auxiliary Storage policies were part of the same Auxiliary Purpose Mapping,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

**WARNING:** If there is no established Auxiliary Purpose Mapping between the source and destination container, the user's Auxiliary storage is deleted once the user is moved.

1 In SMAdmin, click the **Home** tab.

2 Click **Policies**.

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


Auxiliary Policy Purpose Mappings
Auxiliary Policy Purposes
Add
Remove
Refresh
Purpose
Details
Name
GUID
Type
Description
Characters Allowed: 1024 Remaining: 1024
Mapped Policies
Add
Remove
Policy
Apply
Undo
Close

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**.

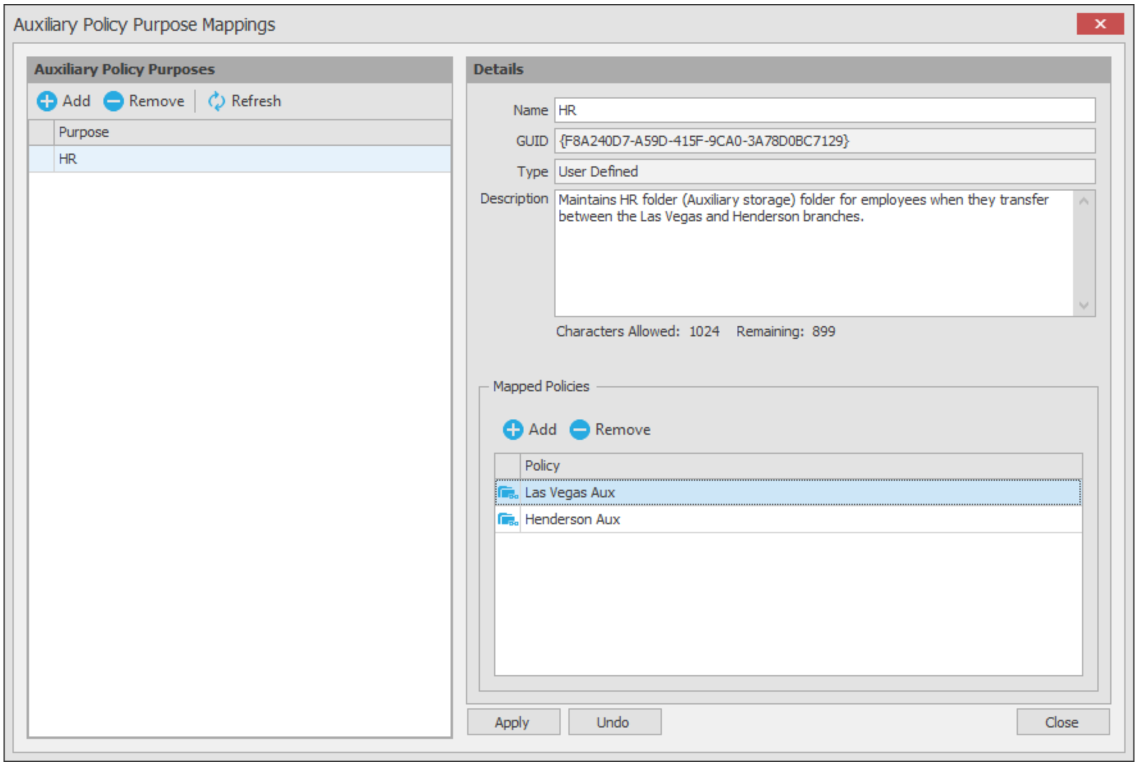
8 From the Policy Selector dialog box, hold down the Control key to select each of the Auxiliary storage policies you want associated with the Auxiliary Purpose Mapping.

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.



| Purpose |
|---|
| HR |

Name: HR

GUID: {F8A240D7-A59D-415F-9CA0-3A78D0BC7129}

Type: User Defined

Description: Maintains HR folder (Auxiliary storage) folder for employees when they transfer between the Las Vegas and Henderson branches.

Characters Allowed: 1024 Remaining: 899

| Policy |
|---|
| Las Vegas Aux |
| Henderson Aux |

11 Click **Apply**.

12 Click **Close**.

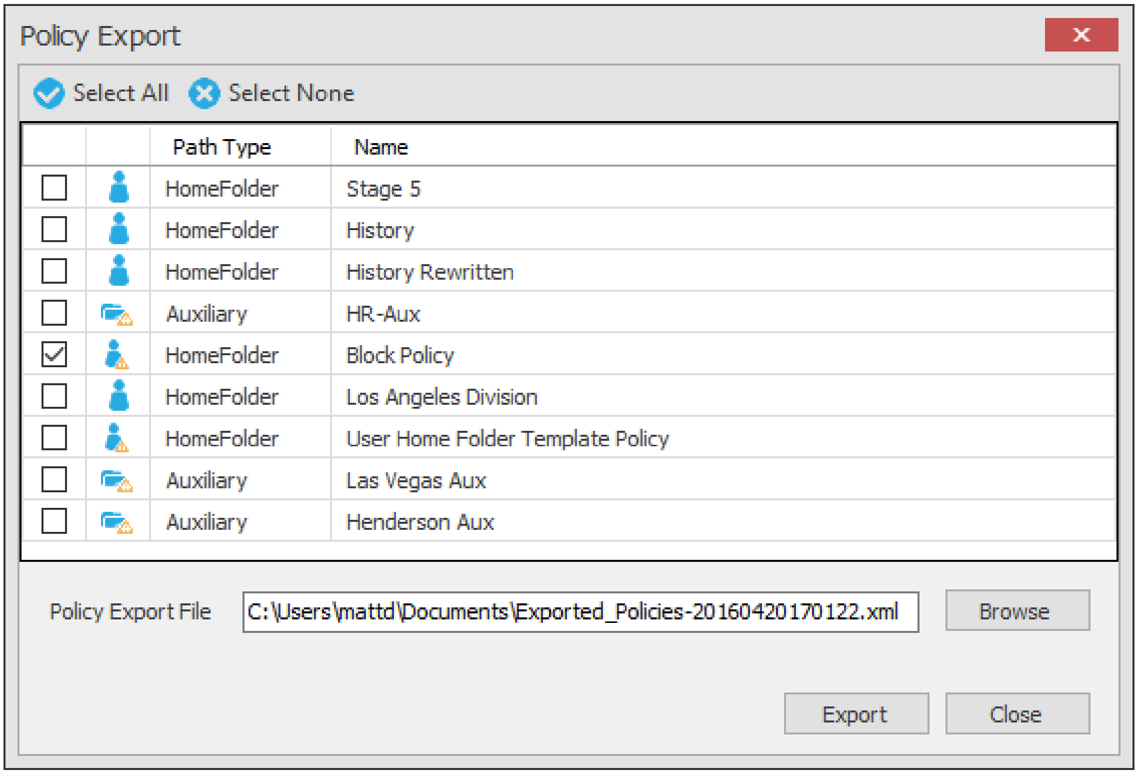
# 6.12 Exporting Policies

Storage Manager provides the ability to export policies so that they can be imported later. For example, many customers first evaluate Storage Manager 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 SMAdmin, click the **Home** tab.

2 Click **Policies**.

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



| | | Path Type | Name |
|---|---|---|---|
| ☐ | | HomeFolder | Stage 5 |
| ☐ | | HomeFolder | History |
| ☐ | | HomeFolder | History Rewritten |
| ☐ | | Auxiliary | HR-Aux |
| ☑ | | HomeFolder | Block Policy |
| ☐ | | HomeFolder | Los Angeles Division |
| ☐ | | HomeFolder | User Home Folder Template Policy |
| ☐ | | Auxiliary | Las Vegas Aux |
| ☐ | | Auxiliary | Henderson Aux |

Policy Export File: C:\Users\mattd\Documents\Exported_Policies-20160420170122.xml

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**.

## 6.13 Importing Policies

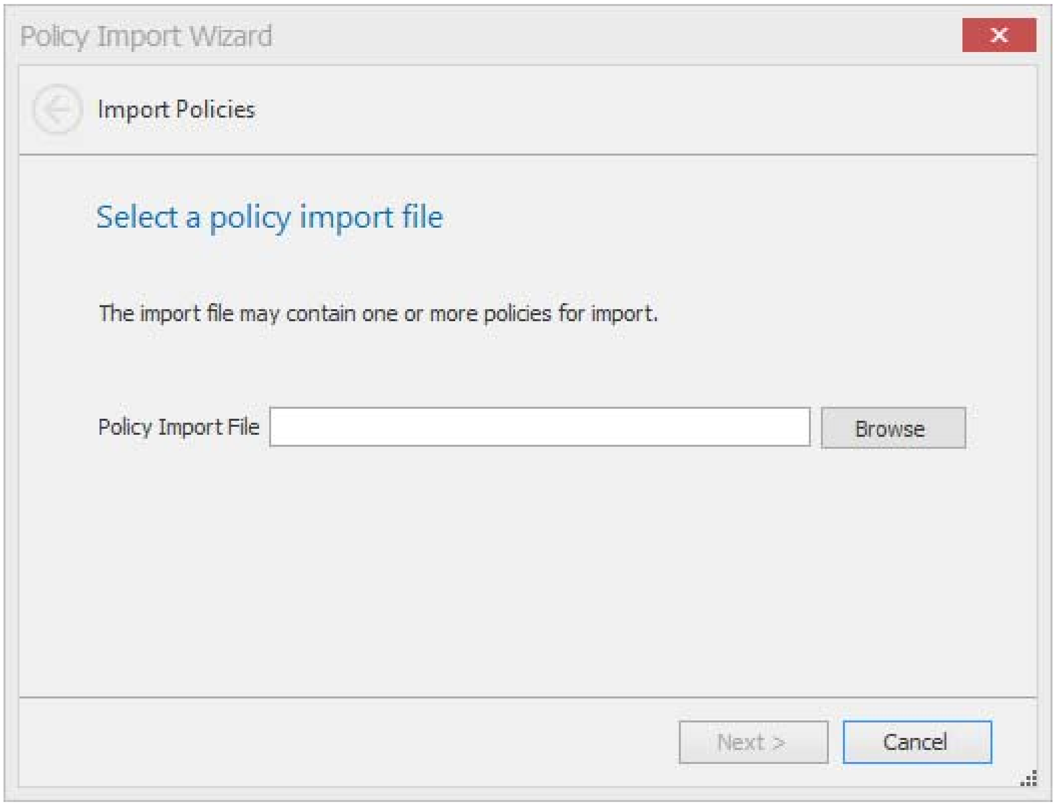
Previously exported policies are imported by using the Import Policies feature.

1 In SMAdmin, click the **Home** tab.

2 Click **Policies**.

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

The following wizard is launched.


Policy Import Wizard

Import Policies

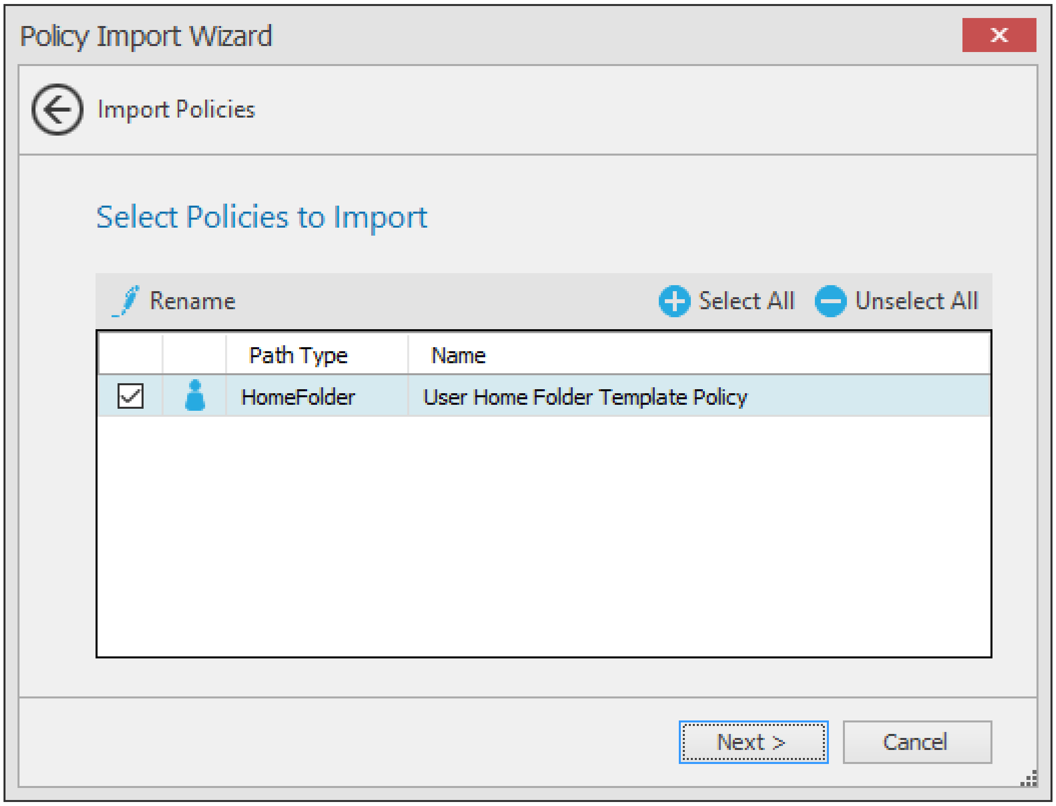
Select a policy import file

The import file may contain one or more policies for import.

Policy Import File

4 Browse to select the saved export file.

5 Click **Next**.


Policy Import Wizard

Import Policies

Select Policies to Import

| | | Path Type | Name |
|---|---|---|---|
| ☑ | 👤 | HomeFolder | User Home Folder Template Policy |

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**.

# 7 Managing Existing Collaborative Storage

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

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

Similar to Chapter 5, “Managing Existing User Storage,” on page 33, this section provides the basic procedures for managing collaborative storage, which includes associating groups and containers with shared storage, and setting the target path, quota rules, and grooming rules.

This section does not provide procedures for establishing a structured project folder with personal subfolders, which are enabled through template creation and Dynamic Template Processing. For a comprehensive discussion on managing collaborative storage, including Dynamic Template Processing, see Chapter 8, “Managing Collaborative Storage,” on page 87.

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

- Section 7.1, “Assigning a Managed Path to Existing Group-based or Container-based Storage,” on page 79
- Section 7.2, “Creating a Collaborative Storage Policy,” on page 82
- Section 7.3, “Performing Management Actions,” on page 85
- Section 7.4, “Editing Collaborative Storage Policies,” on page 86

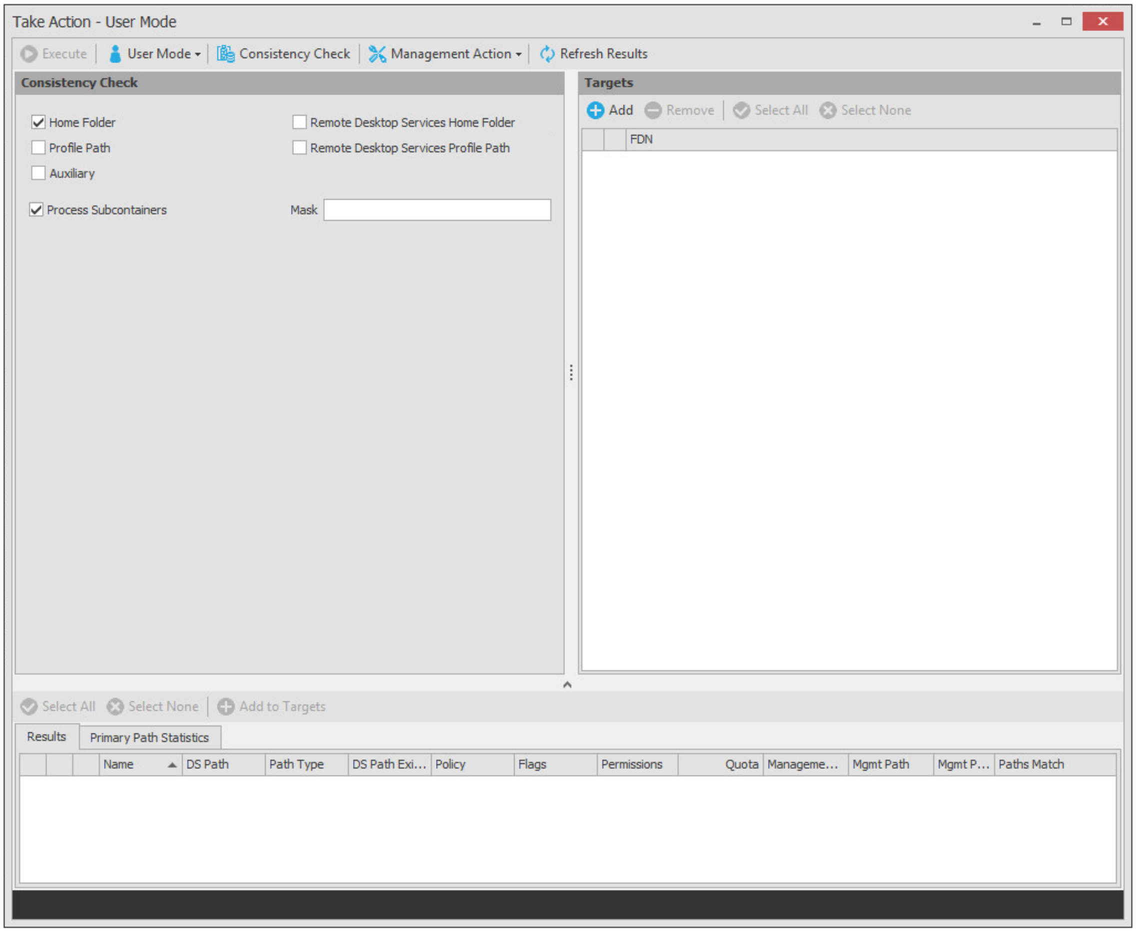
## 7.1 Assigning a Managed Path to Existing Group-based or Container-based Storage

A collaborative managed path attribute is created by Storage Manager 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 SMAdmin, click the **Home** tab.

2 Click **Actions**.

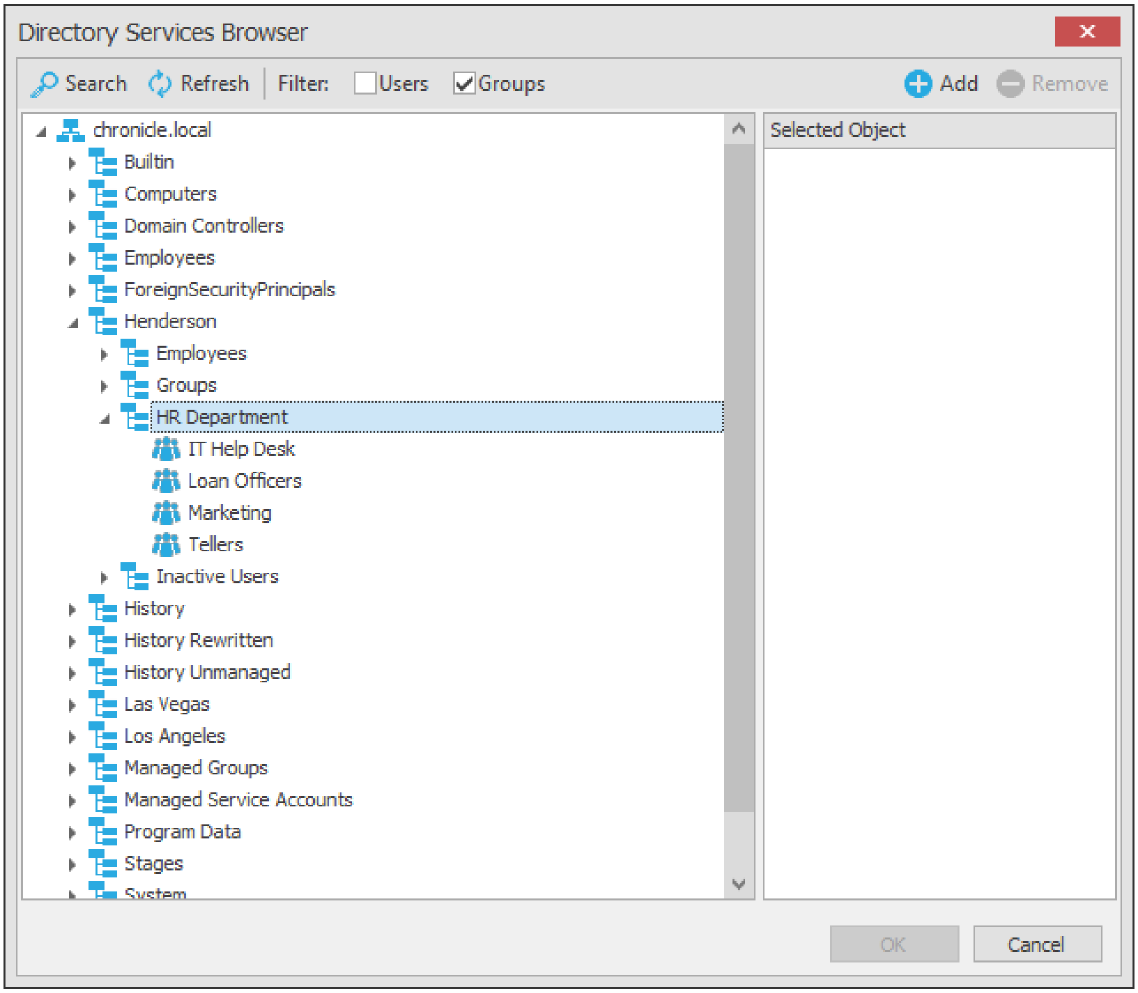


☑ Home Folder
□ Profile Path
□ Auxiliary
□ Remote Desktop Services Home Folder
□ Remote Desktop Services Profile Path
☑ Process Subcontainers
Mask

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**.



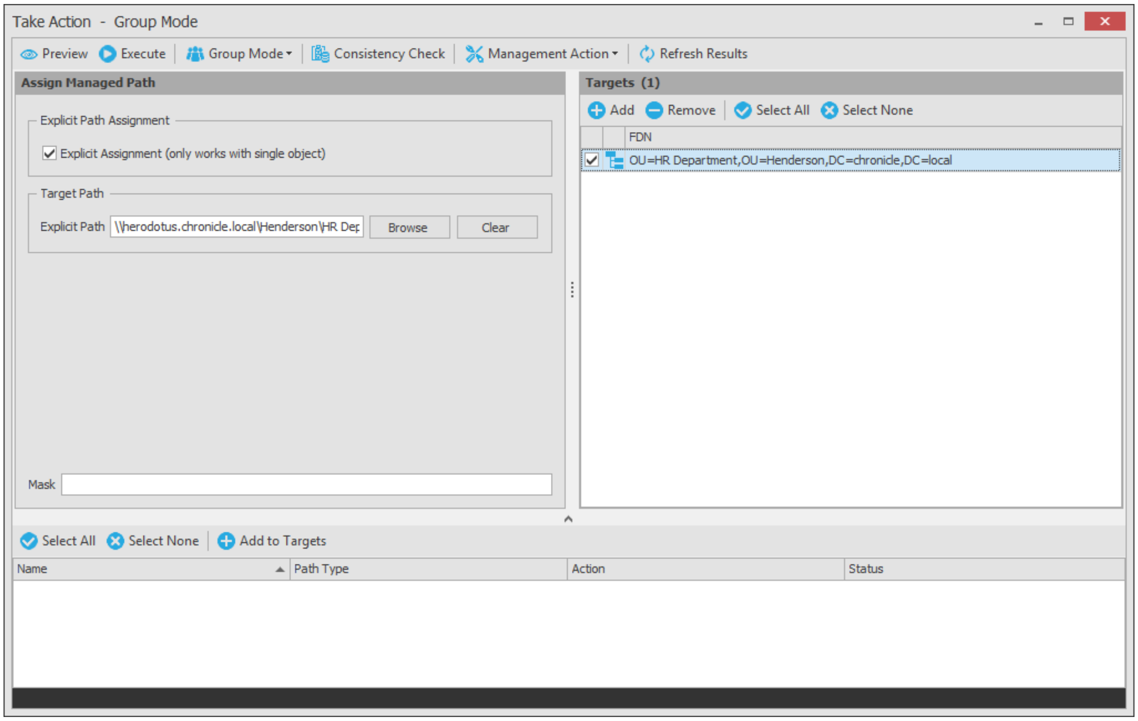
6 Click **OK**.

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 Storage Manager.

10 Click **Preview**.



Explicit Path Assignment

☑ Explicit Assignment (only works with single object)

Target Path

Explicit Path \\herodotus.chronicle.local\Henderson\HR Dep

☑ OU=HR Department,OU=Henderson,DC=chronicle,DC=local

**11** Click **Execute**.

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

**13** Continue with Section 7.2, "Creating a Collaborative Storage Policy," on page 82.

## 7.2 Creating a Collaborative Storage Policy

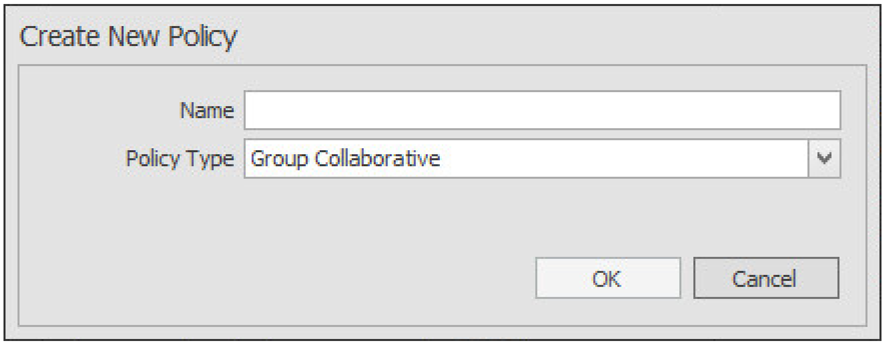
After you assign a managed path, the next step is to create a Collaborative Storage policy for the group or container you selected in Step 5 on page 80. In this procedure, the Collaborative Storage policy will apply to the Group object. However, a Collaborative Storage policy can apply to a Group's parent container thus making it applicable to all existing and new groups located therein.

**1** In SMAdmin, click the **Home** tab.

**2** Click **Policies**.

**3** Select **Manage** > **New** > **Group Collaborative**.

The following dialog box appears.



Name

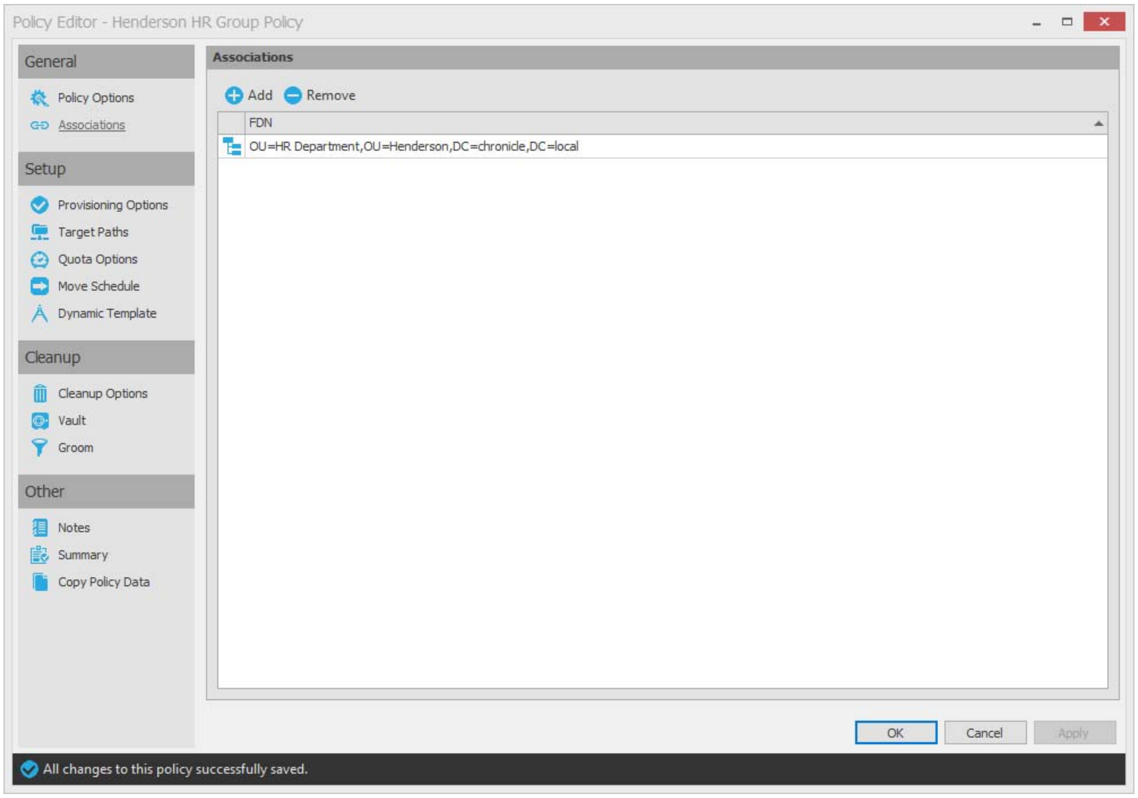
Policy Type Group Collaborative

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

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

6 At the top of the right pane, click **Add** and browse to select the group or container that you selected in Step 5 on page 80.

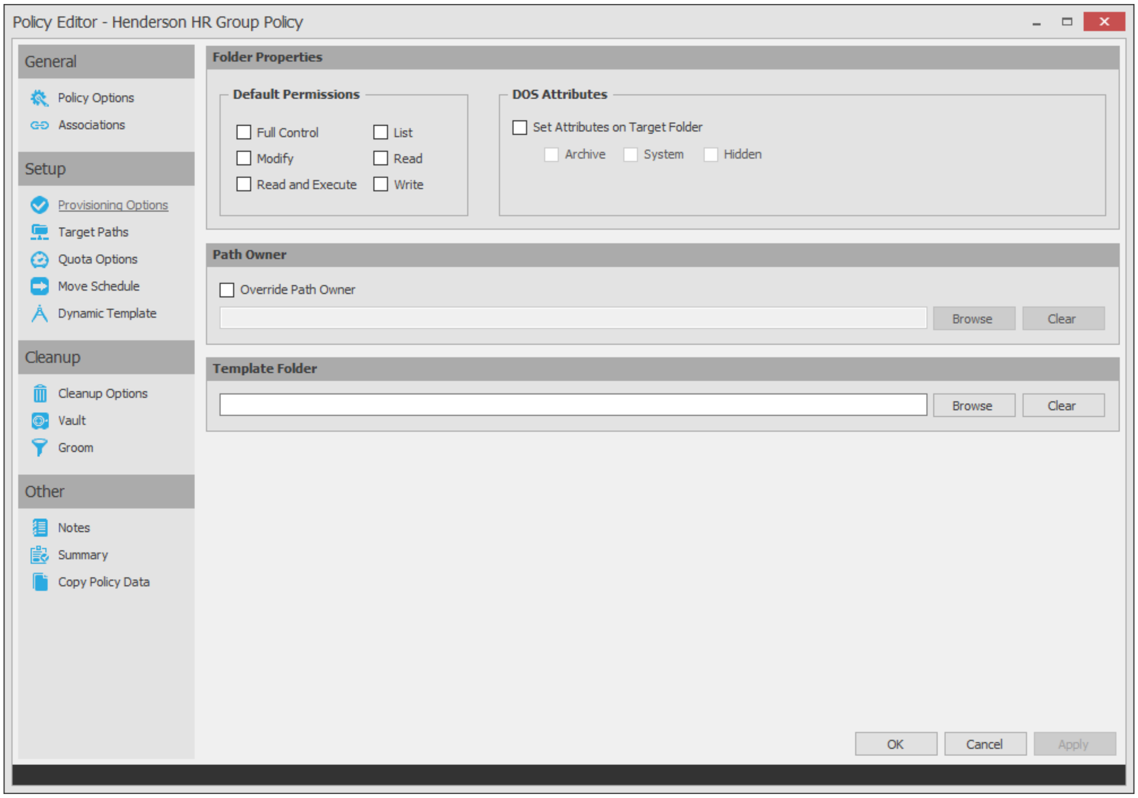
7 Click **Add**, then click **Apply** to save your changes.



OU=HR Department,OU=Henderson,DC=chronicle,DC=local

All changes to this policy successfully saved.

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 left panel, select **Target Paths**, then click **Add**.

12 Browse to and select the parent of the folder you selected in Step 9 on page 81.

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

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

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

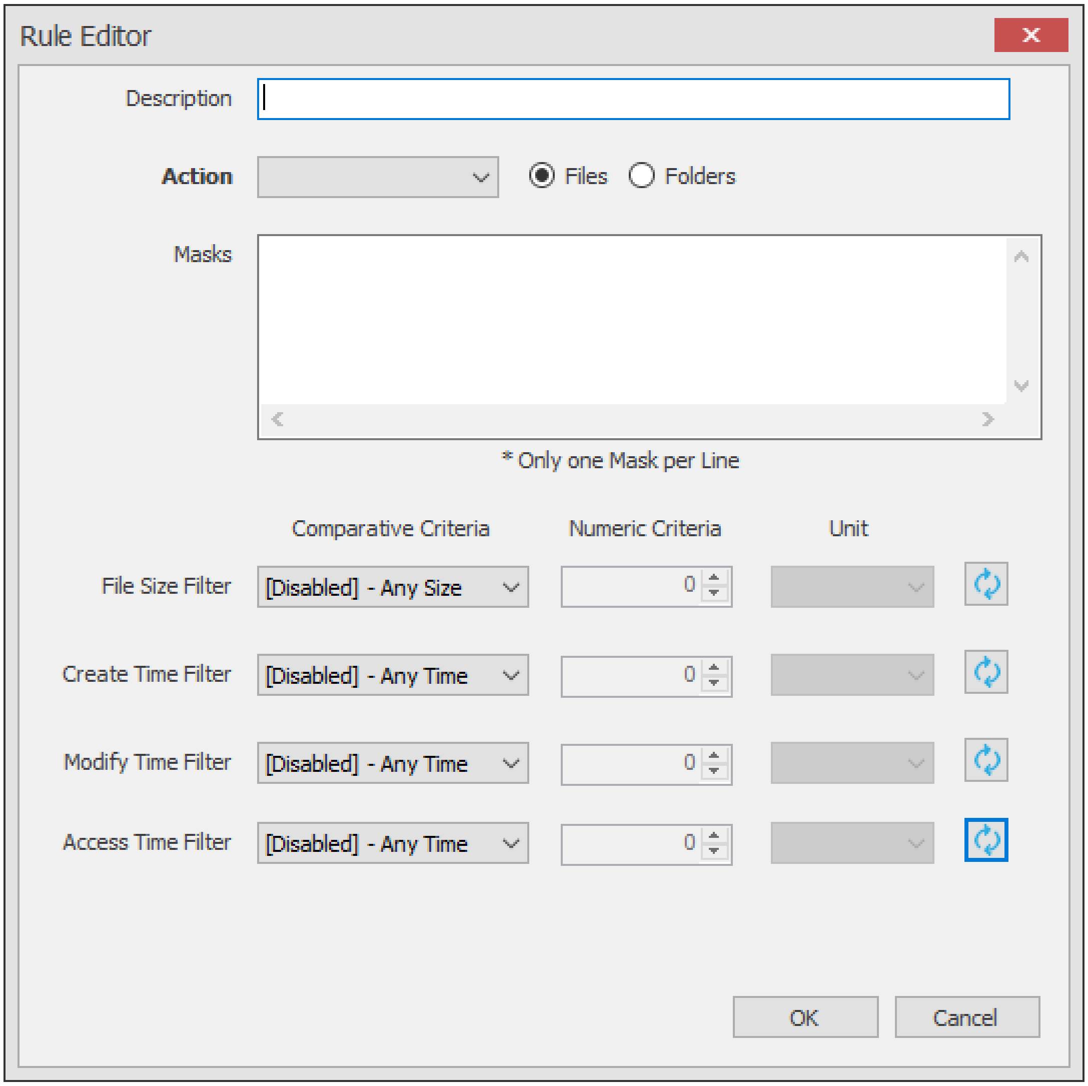
16 (Conditional) If you want to set specifications for a quota manager, select **Enable Quota Manager / Quota Preservation for this policy** and set quota maximums, increments, and managers.

17 In the left pane, select **Groom**.

18 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.

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



Rule Editor

Description

Action ● Files ○ Folders

Masks

* Only one Mask per Line

|  | Comparative Criteria | Numeric Criteria | Unit |
|---|---|---|---|
| File Size Filter | [Disabled] - Any Size | 0 |  |
| Create Time Filter | [Disabled] - Any Time | 0 |  |
| Modify Time Filter | [Disabled] - Any Time | 0 |  |
| Access Time Filter | [Disabled] - Any Time | 0 |  |

**20** In the Rule Editor dialog box, indicate the files that Storage Manager will groom from the collaborative storage pertaining to this policy.

For information on each of the fields in this dialog box, refer to Section 6.5.9, “Setting Groom Rules,” on page 60.

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

**22** Continue with Section 7.3, “Performing Management Actions,” on page 85.

## 7.3 Performing Management Actions

This procedure manages and creates collaborative storage for groups through Dynamic Template Processing. For more information on Dynamic Template Processing, see Chapter 8, “Managing Collaborative Storage,” on page 87.

**1** In SMAdmin, click the **Home** tab.

**2** Click **Objects**.

**3** Browse to and select the group or container that you specified in Step 5 on page 80.

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

5 Click **Preview**.

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

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

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 applied 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 scheduled for object.
```

25 Click **Execute**.

## 7.4 Editing Collaborative Storage Policies

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

For more comprehensive information on collaborative storage policies, including their ability to create structured group-based or container-based storage folders through Dynamic Template Processing, see Chapter 8, “Managing Collaborative Storage,” on page 87.

# 8 Managing Collaborative Storage

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

Storage Manager 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 rights.
- Creating a project folder with a specified owner. The project folder has subfolders for each of the members of the group. This configuration is done through Dynamic Template Processing. For more information on Dynamic Template Processing, see Setting Group Collaborative Storage Policy Dynamic Template Processing.
- 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 Section 8.9, "Creating a Multi-Principal Collaborative Storage Policy," on page 107.

Storage Manager 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

# 8.1 Creating Collaborative Storage Objects in Active Directory

For Storage Manager 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.

**IMPORTANT:** 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.

# 8.2 Understanding Collaborative Storage Templates

When you created user home folder policies in Chapter 6, “Managing User Home Folders,” on page 49, a field in the Provisioning Options page let you indicate the path to a template for provisioning folder structure and content in the home folder.

For collaborative storage management, you can also indicate a template path for provisioning and folder structure within the collaborative managed path. When Storage Manager creates a collaborative managed path for a group, Storage Manager 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

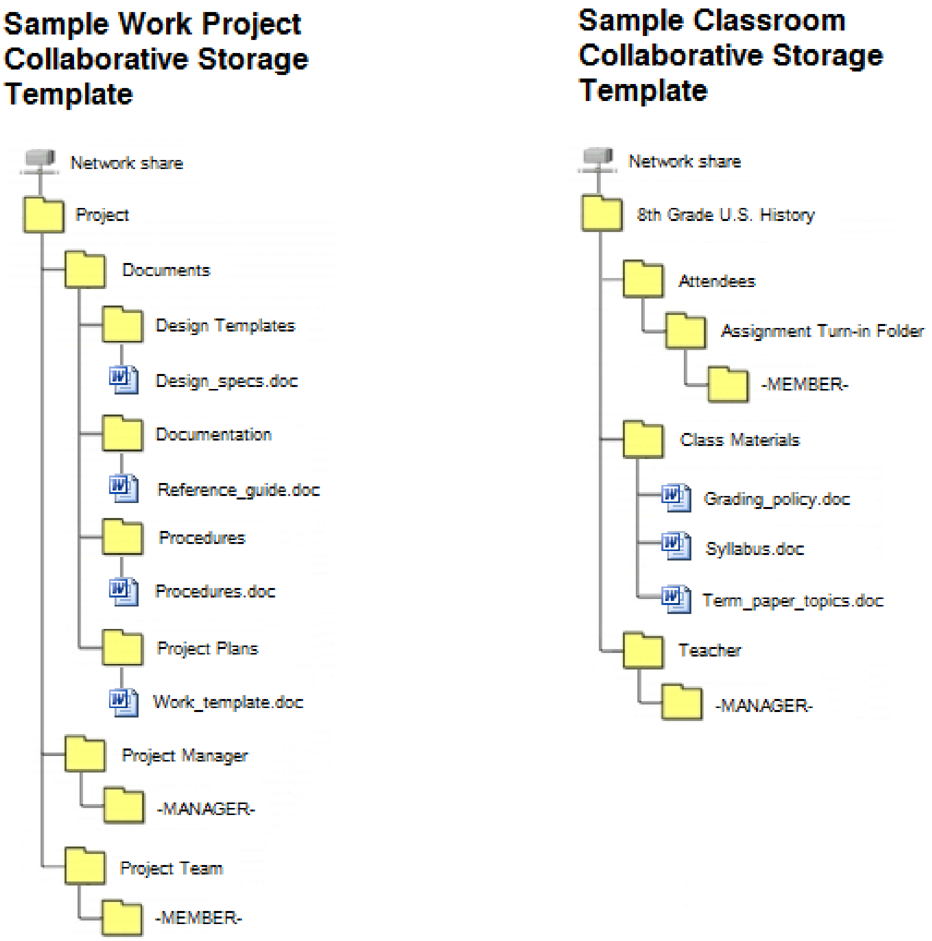
Unlike user home folders, collaborative storage managed by Storage Manager is dynamic in that the member attributes of Group objects are monitored so that the addition and deletion of members can have a direct impact on the structure of the individual file system of a group as well as the permissions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

# 8.3 Determining How You Want to Structure Your Collaborative Storage

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

Two sample designs are shown below.

*Figure 8-1 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.

## 8.4 Creating a Collaborative Storage Template

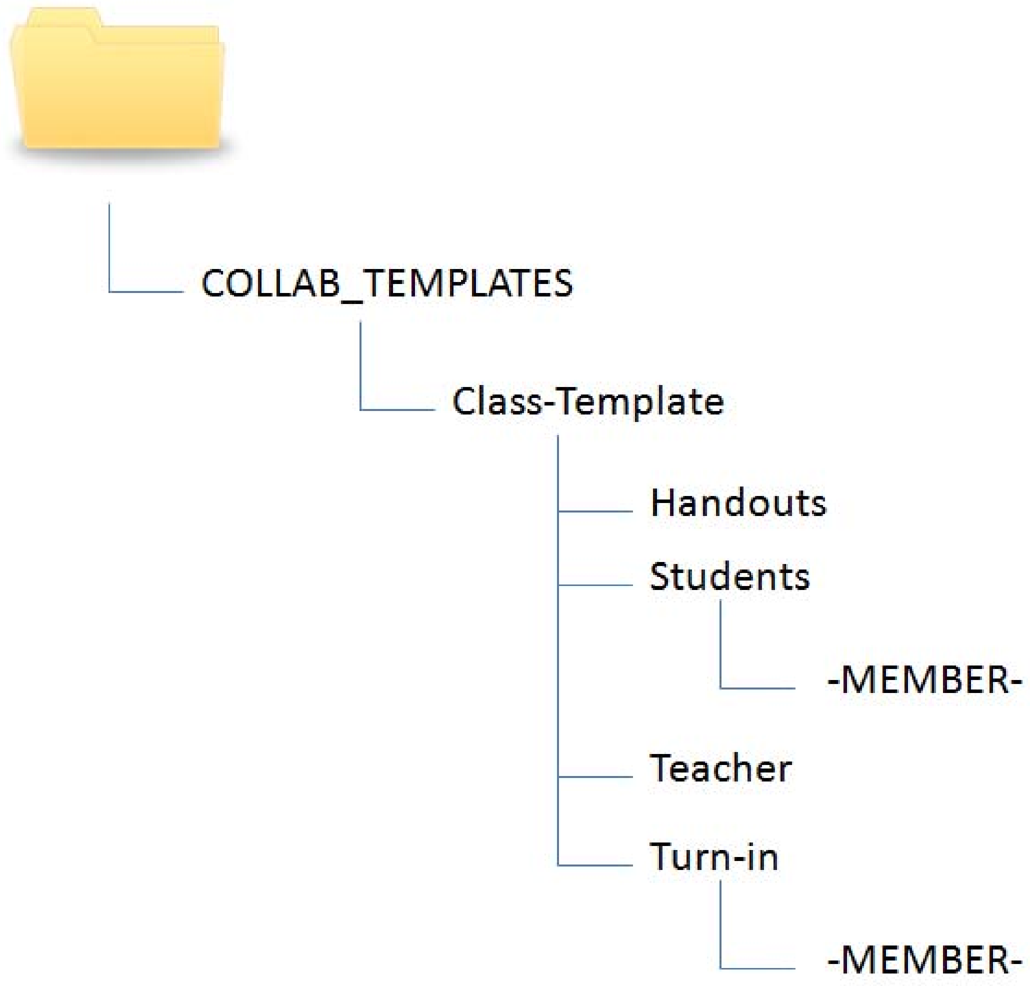
1. Launch Windows Explorer.
2. On a network share, create a file structure for a group that you will provide collaborative storage.
3. Place any documents you want available to the group in the appropriate folders.

## 8.5 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.

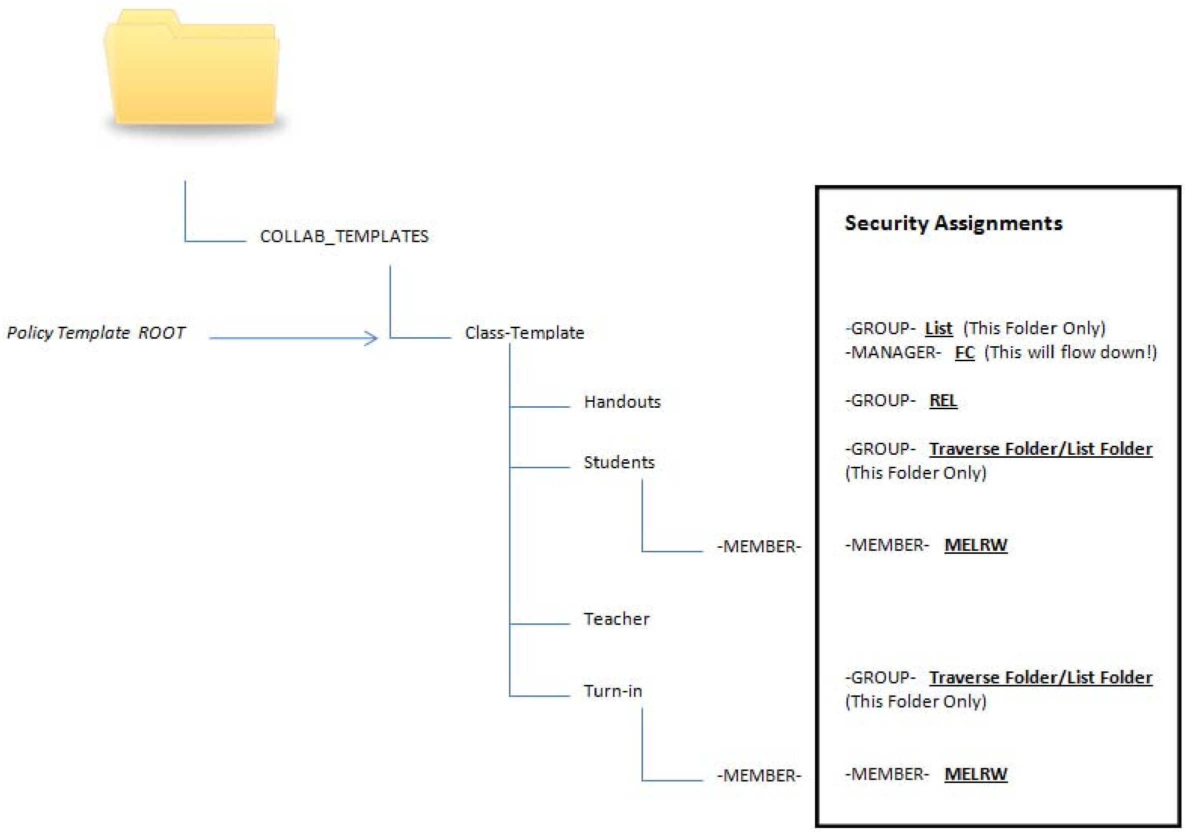
*Figure 8-2 Common Academic Setting Collaborative Storage Template Structure*



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.

***Figure 8-3*** *Security Permissions for Each Folder in the Sample Template*

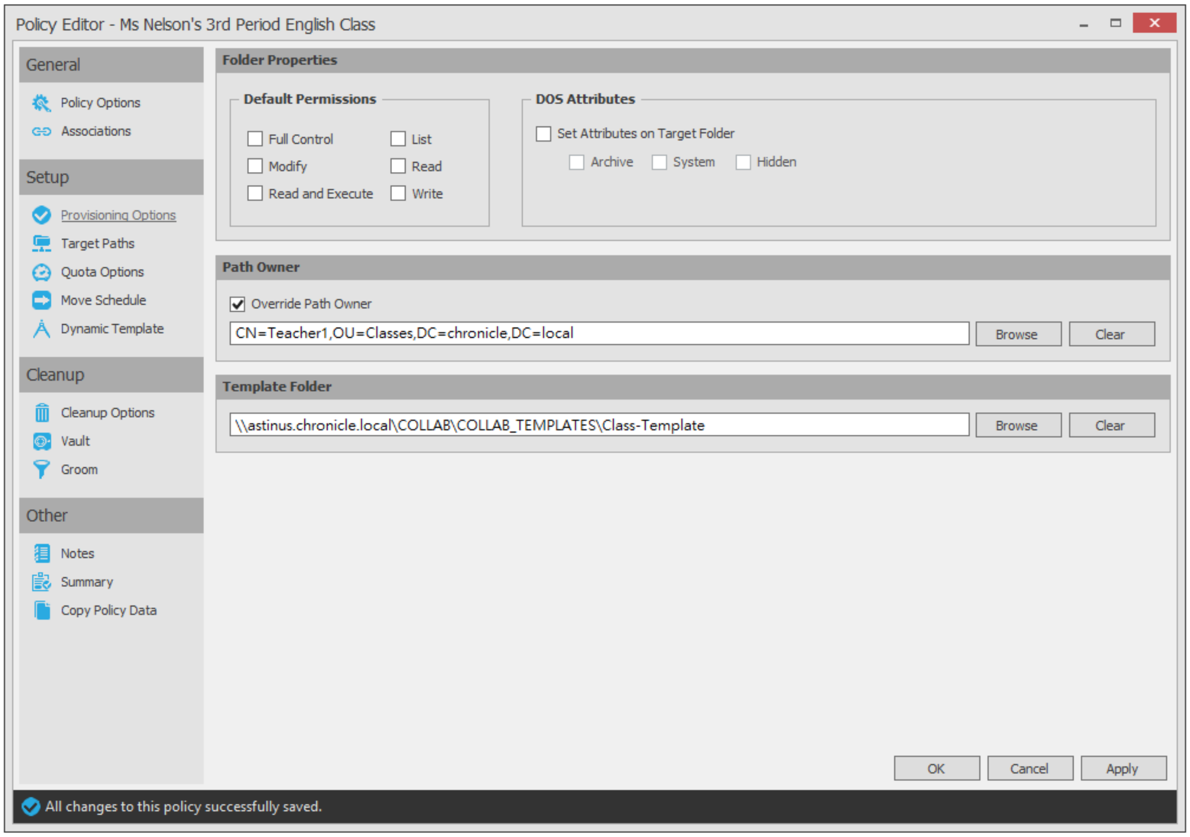

COLLAB_TEMPLATES
Policy Template ROOT
Class-Template
Handouts
Students
-MEMBER-
Teacher
Turn-in
-MEMBER-
Security Assignments
-GROUP- List (This Folder Only)
-MANAGER- FC (This will flow down!)
-GROUP- REL
-GROUP- Traverse Folder/List Folder (This Folder Only)
-MEMBER- MELRW
-GROUP- Traverse Folder/List Folder (This Folder Only)
-MEMBER- MELRW

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.

**IMPORTANT:** 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 Figure 8-3, Teacher1 is specified as the owner.

*Figure 8-4 Owner of a Collaborative Storage Folder*



Default Permissions: □ Full Control □ List □ Modify □ Read □ Read and Execute □ Write

DOS Attributes: □ Set Attributes on Target Folder □ Archive □ System □ Hidden

☑ Override Path Owner

CN=Teacher1,OU=Classes,DC=chronicle,DC=local

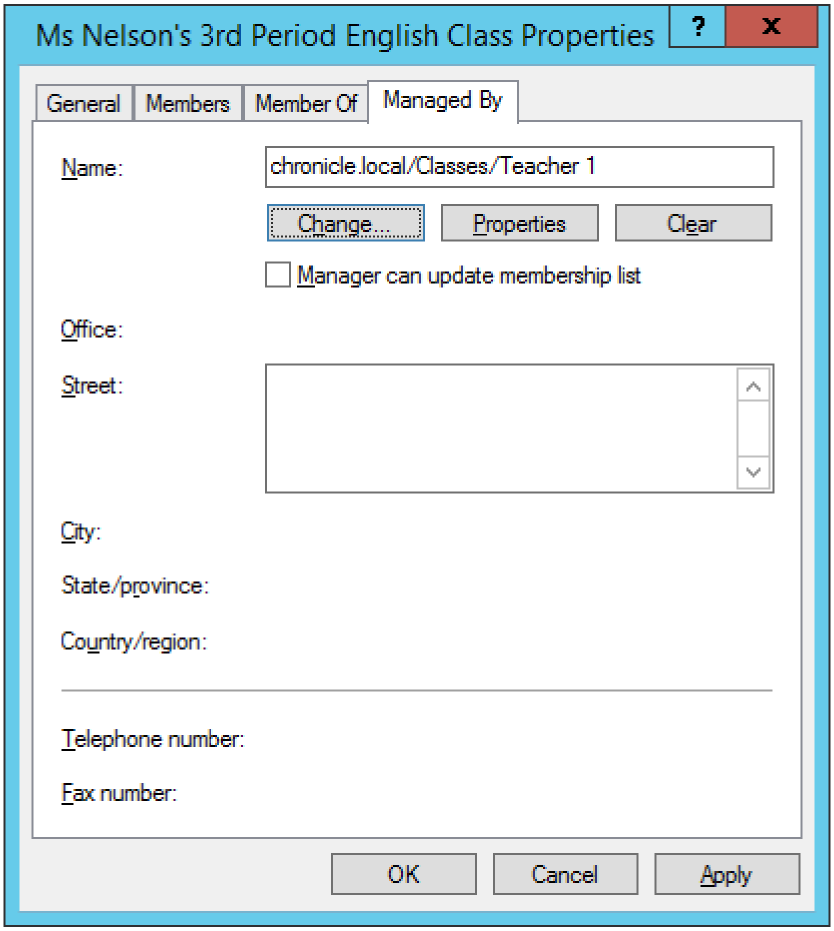
\\astinus.chronicle.local\COLLAB\COLLAB_TEMPLATES\Class-Template

All changes to this policy successfully saved.

The **Override Path Owner** check box is selected and the owner of the folder is set to TEACHER1. 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 TEACHER1.

*Figure 8-5 An Owner in the Name Field Enables -MANAGER- to Function Properly*



Ms Nelson's 3rd Period English Class Properties

Name: chronicle.local/Classes/Teacher 1

□ Manager can update membership list

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

## 8.5.1 Establishing Permissions

You establish the permissions specified for each of the folders in Figure 8-3 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**.

## 8.5.2 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 Figure 8-1 on page 89, 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.

## 8.5.3 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 in Section 8.4, "Creating a Collaborative Storage Template," on page 90, 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.

## 8.5.4 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 in Section 8.4, "Creating a Collaborative Storage Template," on page 90, browse to and right-click one of the subfolders, then click **Properties**.

For example, in the sample work project collaborative storage template example in Figure 8-1 on page 89, 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.

## 8.6 Understanding Collaborative Storage Policies

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

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

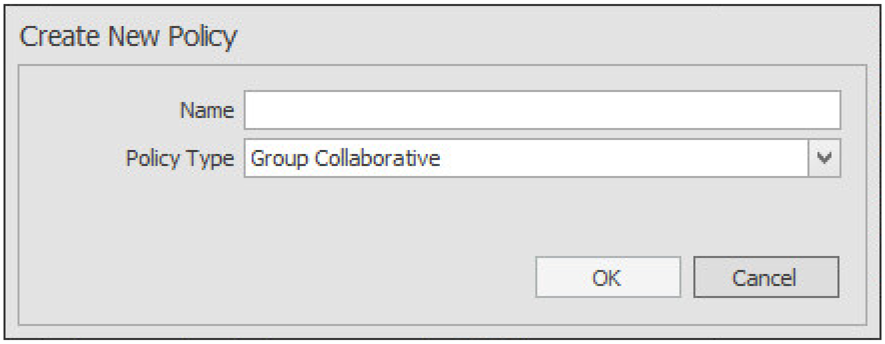
## 8.7 Creating a Group Collaborative Storage Policy

1 In SMAdmin, click the **Home** tab.

2 Click **Policies**.

3 In the **Manage** menu, select **New > Group Collaborative**.

The following dialog box appears:



Create New Policy

Name:

Policy Type: Group Collaborative

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

The Policy Options page appears.

5. Continue with Section 8.7.1, "Setting Group Collaborative Storage Policy Options," on page 96.

## 8.7.1 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.

**NOTE:** Group Policies in Storage Manager are completely independent of Microsoft Group policies.

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

   This indicates that you want the settings in this policy to be applied to all groups within the domain or organizational unit where this policy is assigned. Deselecting this check box indicates that you want to create a Blocking policy that can be applied to a specific group. For more information on blocking policies, see Section 5.6, "Creating a Blocking Policy," on page 37.
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 Section 8.7.2, "Setting Group Collaborative Storage Policy Associations," on page 96.

## 8.7.2 Setting Group Collaborative Storage Policy Associations

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

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

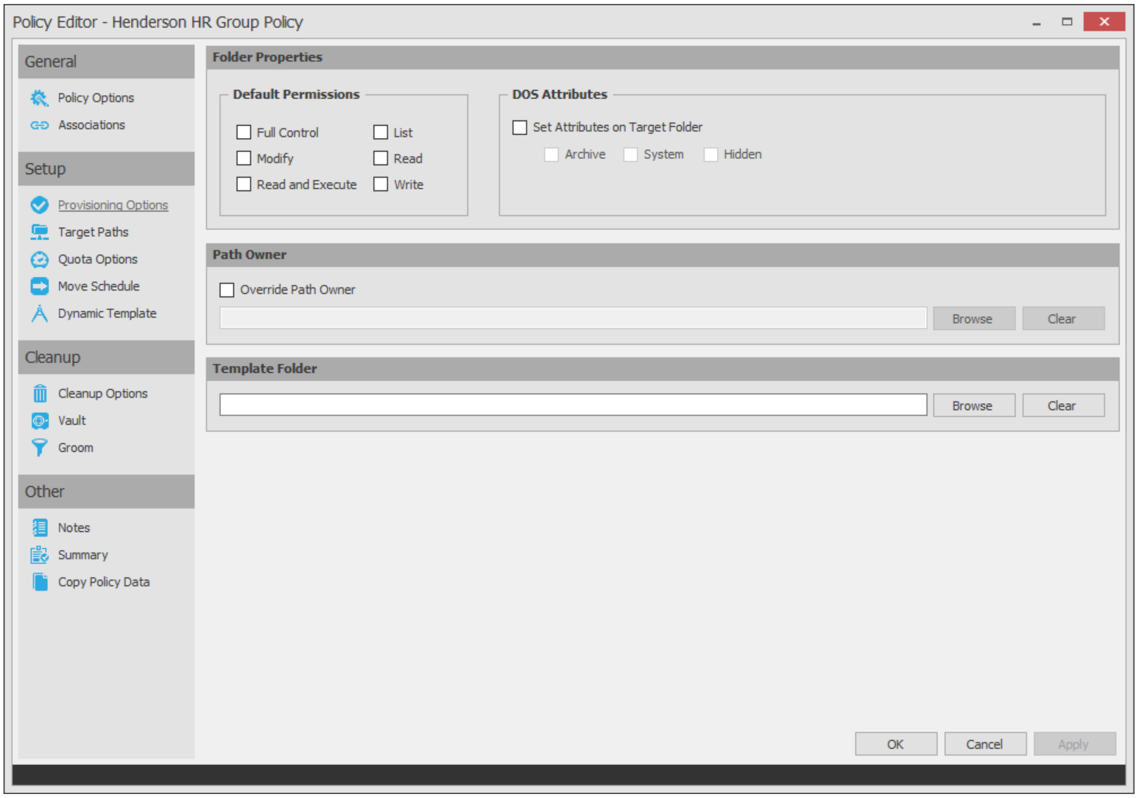
   The Directory Services Browser is closed and the object is displayed in fully qualified name format in the right pane of the window. For example, `OU=Las Vegas,DC=NVB,DC=local`.
5. Click **OK** to close the Object Browser.
6. Click **Apply** to save your settings.
7. Proceed with Section 8.7.3, "Setting Group Collaborative Storage Policy Provisioning Options," on page 97.

### 8.7.3 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 Section 8.5.3, “Configuring Permissions for the Group Members’ Personal Folders,” on page 94 and Section 8.5.4, “Configuring Group Member Permissions to Other Folders,” on page 94.

3 Select the **Override Path Owner** check box.

When you create Collaborative Storage policies, it's very important to override the path owner. By default, each group owns the entire group managed path, so all members of the group inherit Full Control of all subdirectories in the group folder, including other users' personal folders.

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

5 In the **Template Folder** region, click the **Browse** button and locate the folder structure that you created in Section 8.4, “Creating a Collaborative Storage Template,” on page 90.

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

For example, if you had a structure similar to the Sample Classroom Collaborative Storage Template in Figure 8-1 on page 89, you would select “8th Grade U.S. History.”

7. Click **Apply** to save your settings.
8. Proceed with Section 8.7.4, “Setting Group Collaborative Storage Policy Target Paths,” on page 98.

## 8.7.4 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 Paths**.
2. 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.
3. From the **Leveling** drop-down menu, choose an option.

   This setting is used 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\HOME\B\BSMITH`.

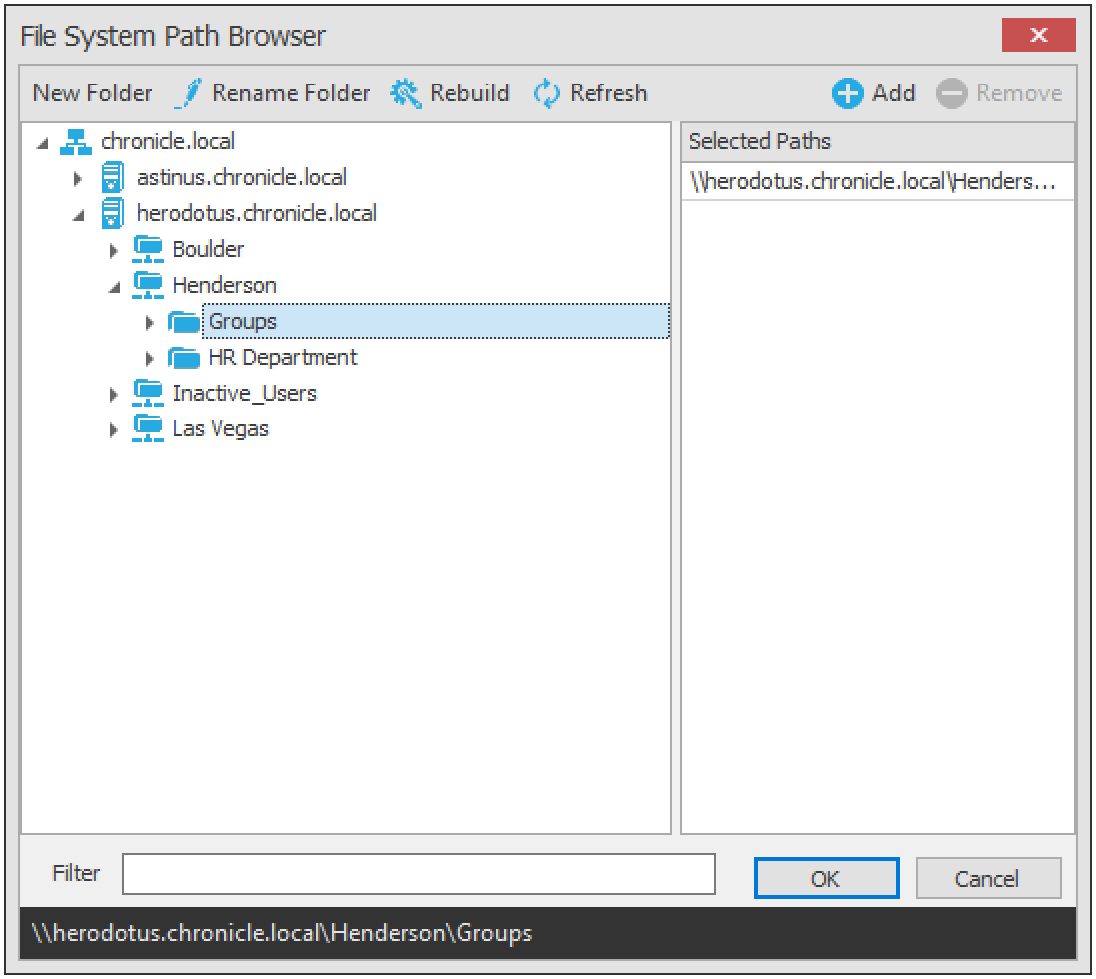
   If you choose **Last Letter**, and the **Leveling Length** field is set to 1, the same user has a home folder located in a path such as `\\SERVER1\HOME\H\BSMITH`

   The **Last Letter** means the last character of the attribute Storage Manager uses to create storage. Once again, Storage Manager 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\HOME\2014\BSMITH2014.`
4. In the Maximum Unreachable Paths field, specify a setting.

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

   For example, suppose you have 100 target paths and you're using Random Distribution and the **Maximum Unreachable Paths** setting is 20. Storage Manager 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.
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.



\\herodotus.chronicle.local\Henders...

\\herodotus.chronicle.local\Henderson\Groups

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

8 Proceed to Section 8.7.5, “Setting Group Collaborative Storage Policy Quota Options,” on page 99.

## 8.7.5 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

**NOTE:** 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.

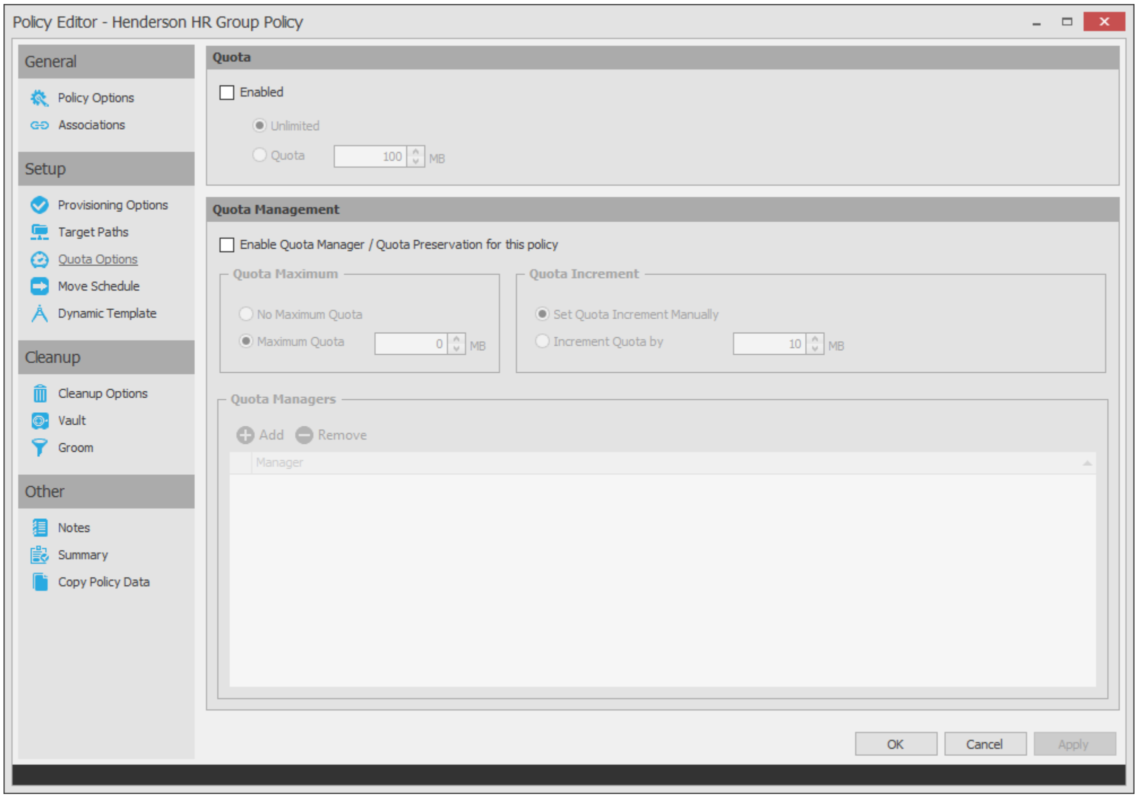
Quota management on NAS devices needs to be managed by the NAS vendor software.

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

Quota management actions are performed through Quota Manager, which is a separate Web browser-based management interface. For more information on Quota Manager, see Chapter 9, “Using Quota Manager,” on page 119.

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

The following page appears:



**Quota**

□ Enabled

● Unlimited

○ Quota 100 MB

**Quota Management**

□ Enable Quota Manager / Quota Preservation for this policy

Quota Maximum

○ No Maximum Quota

● Maximum Quota 0 MB

Quota Increment

● Set Quota Increment Manually

○ Increment Quota by 10 MB

Quota Managers

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 and to allow the Quota Manager Web interface to apply to this policy.

**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 SMAdmins group will be able to use the Quota Manager Web interface.

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

6 Proceed with Section 8.7.6, “Setting the Group Collaborative Storage Policy Move Schedule,” on page 101.

## 8.7.6 Setting the Group Collaborative Storage Policy 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.

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

1 In the left pane, click **Move Schedule**.

2 In the D**ata Move Schedule** grid, click the squares for the day and hour you want to disable for data movement.

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

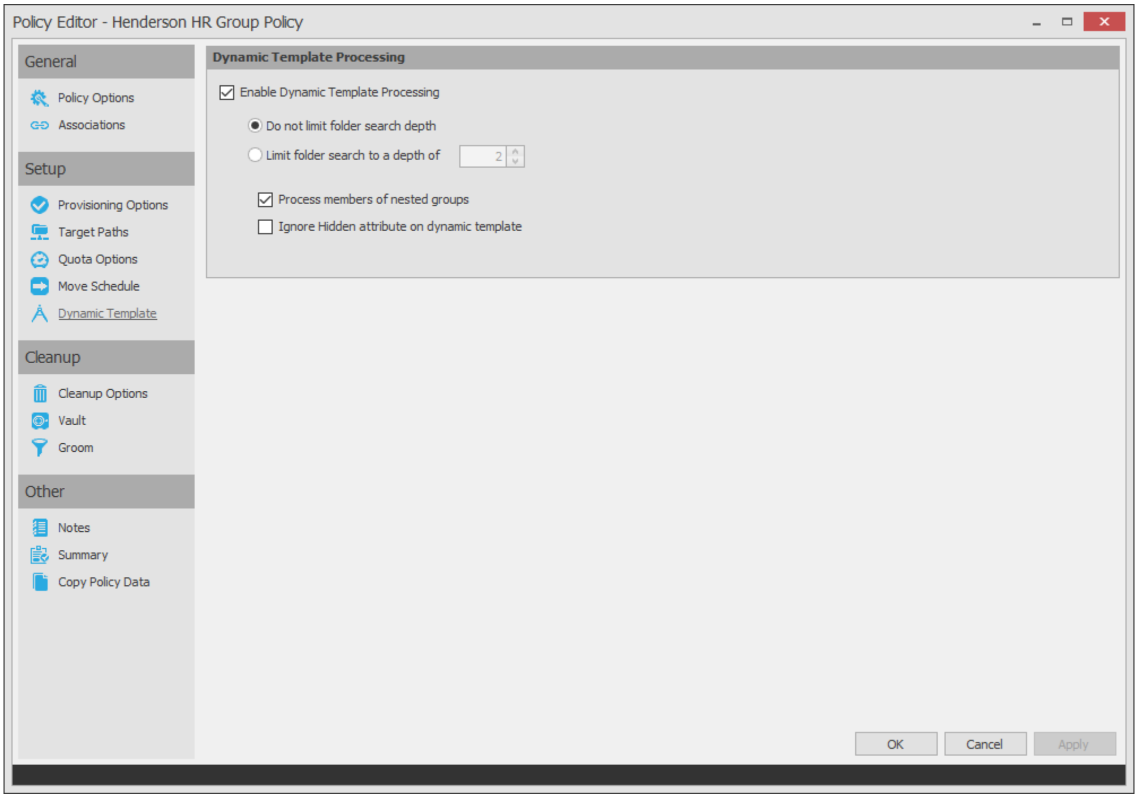
4 Proceed with Section 8.7.7, “Setting Group Collaborative Storage Policy Dynamic Template Processing,” on page 101.

## 8.7.7 Setting Group Collaborative Storage Policy Dynamic Template Processing

Dynamic Template Processing is the term used in Storage Manager 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:



**Dynamic Template Processing**

☑ Enable Dynamic Template Processing

● Do not limit folder search depth

○ Limit folder search to a depth of 2

☑ Process members of nested groups

☐ Ignore Hidden attribute on dynamic template

**2** Do one of the following:

- If the folder structure in your collaborative storage template includes a `-MEMBER-` folder, Storage Manager can create personal folders within the collaborative storage folder. Leave the **Enable Dynamic Template Processing** check box selected and proceed with Step 3.
- If your collaborative storage template does not include a `-MEMBER-` folder, Storage Manager will not create personal folders within the collaborative storage folder. Deselect the **Enable Dynamic Template Processing** check box and proceed with Section 8.7.8, “Setting Group Collaborative Storage Policy Cleanup Options,” on page 103.

**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 in Figure 8-1 on page 89, 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 Dynamic 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 Section 8.7.8, “Setting Group Collaborative Storage Policy Cleanup Options,” on page 103.

## 8.7.8 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.

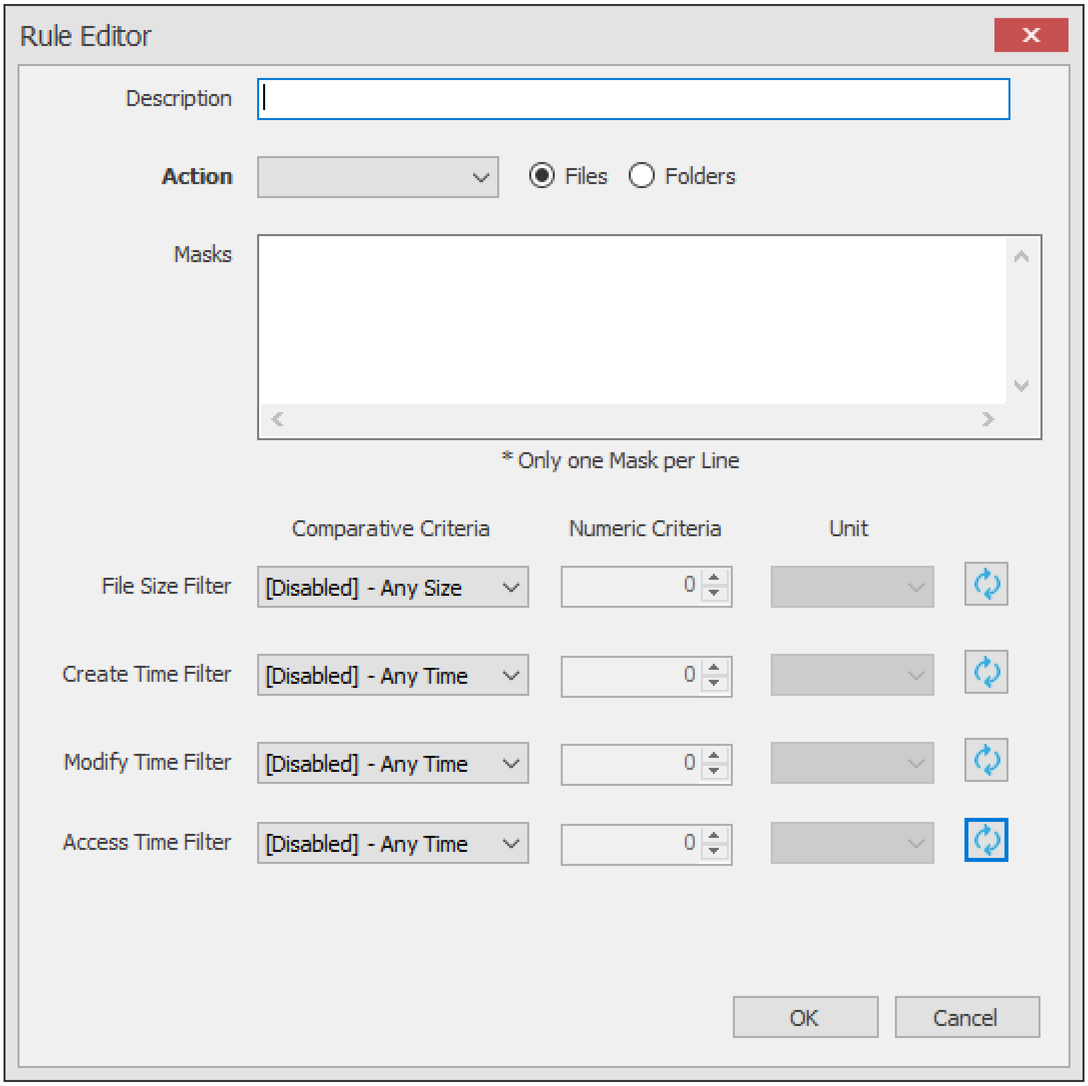
   When you indicate this path, it also appears in the **Vault Path** field of the Groom page, because groom rules and vault rules share the same vault path.
4. Click **Apply** to save the settings.
5. Proceed with Section 8.7.9, “Setting Group Collaborative Storage Policy Vault Rules,” on page 103.

## 8.7.9 Setting Group Collaborative Storage Policy Vault Rules

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

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

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



● Files ○ Folders

| | Comparative Criteria | Numeric Criteria | Unit |
|---|---|---|---|
| File Size Filter | [Disabled] - Any Size | 0 | |
| Create Time Filter | [Disabled] - Any Time | 0 | |
| Modify Time Filter | [Disabled] - Any Time | 0 | |
| Access Time Filter | [Disabled] - Any Time | 0 | |

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

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

4 Fill in the following fields:

**Action:** Select whether this vault rule deletes or vaults files.

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.

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

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

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

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

File or folder names can contain an asterisk.

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

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

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

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

8 Proceed with Section 8.7.10, "Setting Group Collaborative Storage Policy Groom Rules," on page 105.

## 8.7.10 Setting Group Collaborative Storage Policy Groom Rules

Groom rules in Storage Manager 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 SMAdmin. For more information, see Section 13.1.6, "Actions," on page 268.

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, specify a description of the groom rule.

For example, "Files to groom in Community Outreach Group."

4 Fill in the following fields:

**Action:** Select whether this groom rule will delete or vault 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.

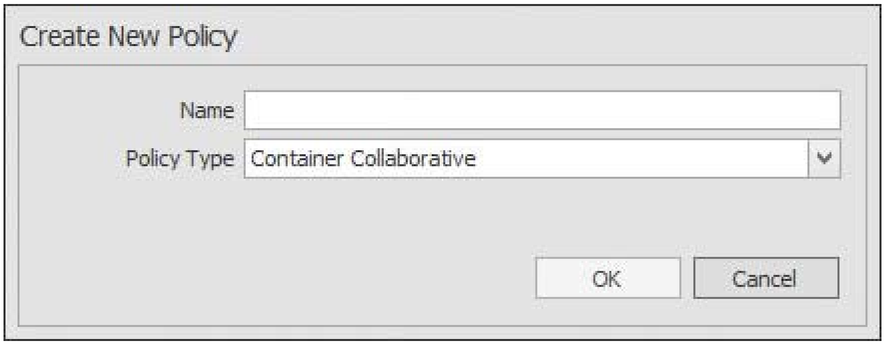
Leaving the setting as **[Disabled]-Any Size** vaults or deletes all file types listed in the **Mask** text box, according to what is indicated in the **Action** drop-down menu. Choosing any of the other options from the drop-down menu lets you indicate files to delete or vault according to size, when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

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

# 8.8 Creating a Container Collaborative Storage Policy

1. In SMAdmin, click the **Home** tab.
2. Click **Policies**.
3. In the **Manage** menu, select **New > Container Collaborative**.

   The following dialog box appears:

   Create New Policy

   Name

   Policy Type: Container Collaborative

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

   The Policy Options page appears.
5. Continue with Section 8.8.1, “Setting Container Collaborative Storage Policy Options,” on page 106.

## 8.8.1 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 Section 5.6, “Creating a Blocking Policy,” on page 37.
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 Association page presented when you create a Group Collaborative Storage policy. For an explanation of the page, along with procedures for setting associations, see Section 8.7.2, “Setting Group Collaborative Storage Policy Associations,” on page 96.

   **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 Section 8.7.3, “Setting Group Collaborative Storage Policy Provisioning Options,” on page 97.

   **Target Paths:** The fields presented on the Target Paths 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 Section 8.7.4, “Setting Group Collaborative Storage Policy Target Paths,” on page 98.

**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 Section 8.7.5, “Setting Group Collaborative Storage Policy Quota Options,” on page 99.

**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 Section 8.7.6, “Setting the Group Collaborative Storage Policy Move Schedule,” on page 101.

**Dynamic Template Processing:** The fields presented on the Dynamic Templates 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 Section 8.7.7, “Setting Group Collaborative Storage Policy Dynamic Template Processing,” on page 101.

**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 Section 8.7.8, “Setting Group Collaborative Storage Policy Cleanup Options,” on page 103.

**Vault:** The fields presented on the Vault Rules 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 Section 8.7.9, “Setting Group Collaborative Storage Policy Vault Rules,” on page 103.

**Groom:** The fields presented on the Groom Rules 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 Section 8.7.10, “Setting Group Collaborative Storage Policy Groom Rules,” on page 105.

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

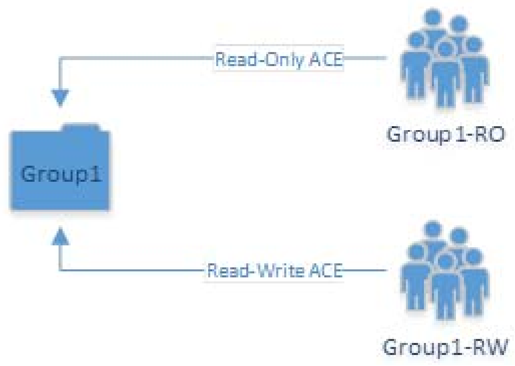
## 8.9 Creating a Multi-Principal Collaborative Storage Policy

### 8.9.1 Overview

Storage Manager for Active Directory 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 RO, another’s could RW, and another’s could be FUL. 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 Figure 8-6 on page 108 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.

*Figure 8-6 Example of a Multi-Principal Managed Path*



## 8.9.2 Group Naming Parameters

Security groups that own and access a Multi-Principal Path must be in the *`Group_Prefix_Name-Security_Suffix`* format. In Table 8-1, the naming components of the security group names in Figure 8-6 are identified.

*Table 8-1 Components of Security Group Names Owning and Accessing Multi-Principal Paths*

| Group Prefix Name | Suffix Separator Character/Sequence | 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.

## 8.9.3 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.

## 8.9.4 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.

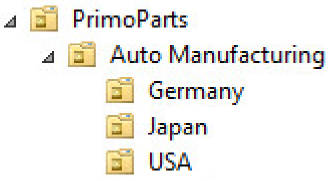
Similarly, for provisioning, the first group for which an event is received would be responsible for creating the folder based on the group name prefix and assigning its respective rights. Any other events for complimentary groups must perform the equivalent of an apply permissions (ACE) in order to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

## 8.9.5 Create a Multi-Principal Collaborative Storage Policy

### Prerequisites

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

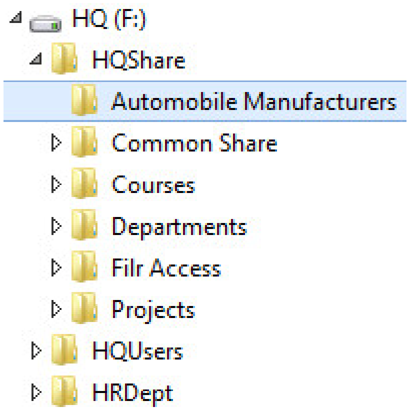
  For example, a manufacturer of automotive parts that distributes parts to Germany, Japan, and the United States might structure their Active Directory domain as follows:

  - PrimoParts
    - Auto Manufacturing
      - Germany
      - Japan
      - USA

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

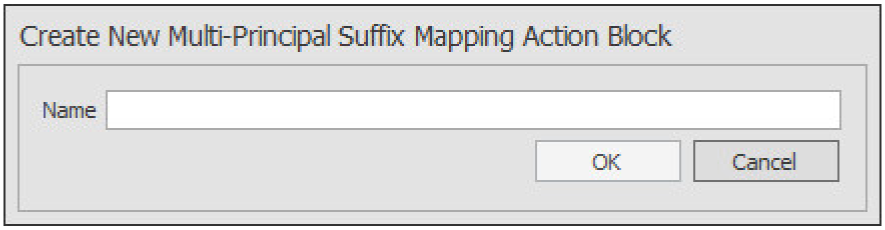
Using the auto parts manufacturer example, the file system might look like this:



## 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 Storage Manager.

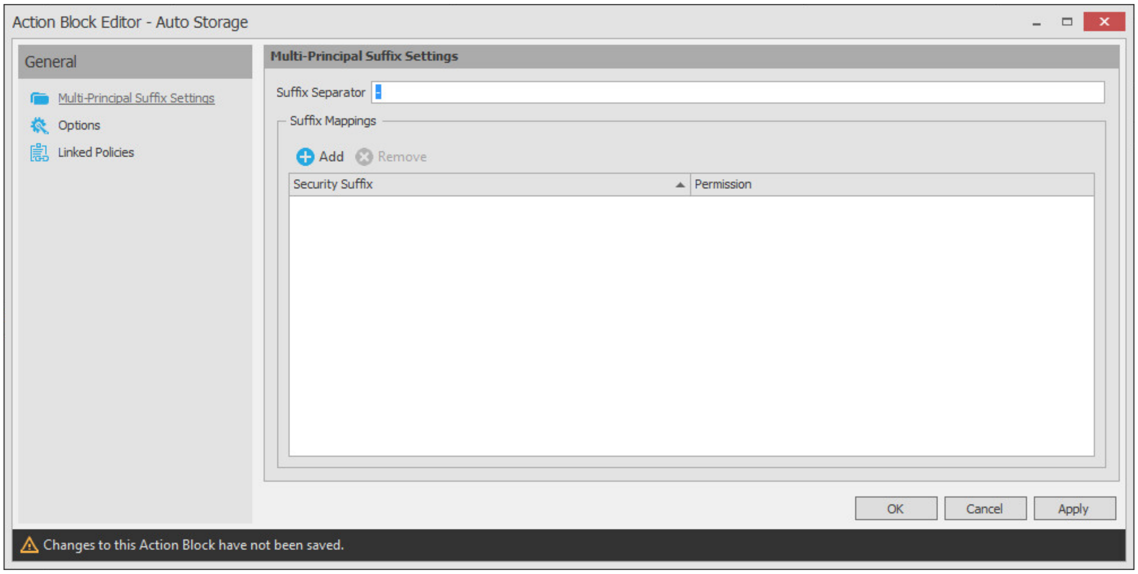
1. In SMAdmin, click the **Home** tab.
2. Click **Action Blocks**.
3. From the **Manage** menu, select **New** > **Multi-Principal Suffix Mapping**.



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

   Using the auto parts manufacturer example, the Action Block might be named something like Auto Storage.

   The following page appears:



Changes to this Action Block have not been saved.

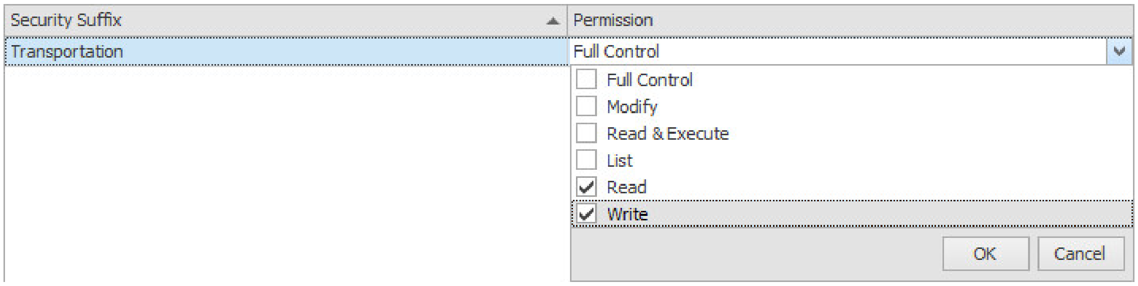
5 Click **Add**.

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.

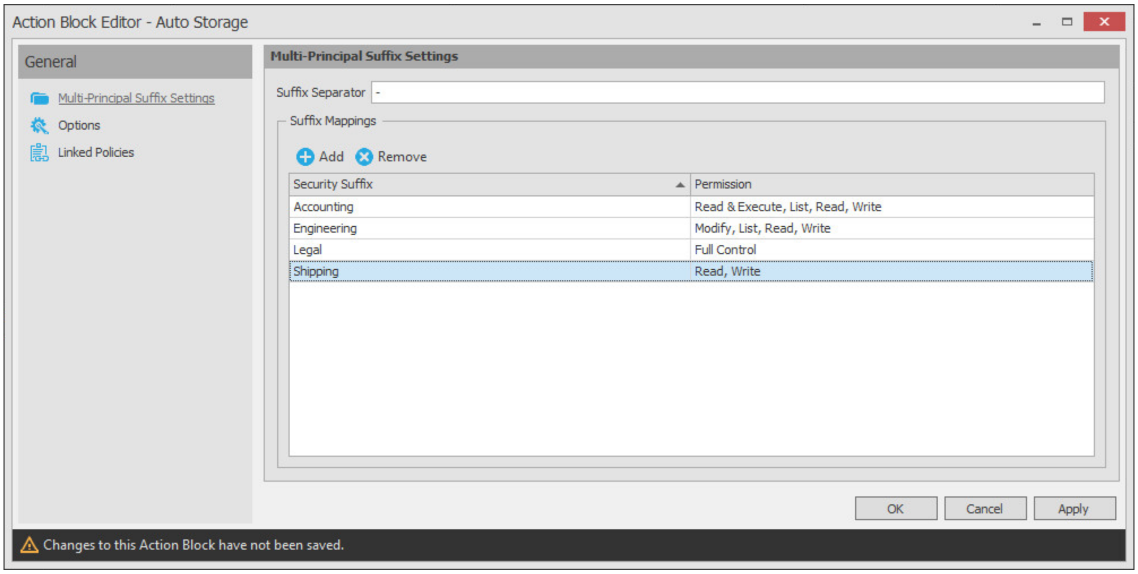
8 Specify the permissions for the particular group and click **OK**.



| Security Suffix | Permission |
|---|---|
| Transportation | Full Control |

□ Full Control
□ Modify
□ Read & Execute
□ List
☑ Read
☑ Write

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



Action Block Editor - Auto Storage

Multi-Principal Suffix Settings

Suffix Separator: -

Suffix Mappings

| Security Suffix | Permission |
|---|---|
| Accounting | Read & Execute, List, Read, Write |
| Engineering | Modify, List, Read, Write |
| Legal | Full Control |
| Shipping | Read, Write |

Changes to this Action Block have not been saved.

10 Click **Apply**.

11 Click **OK**.

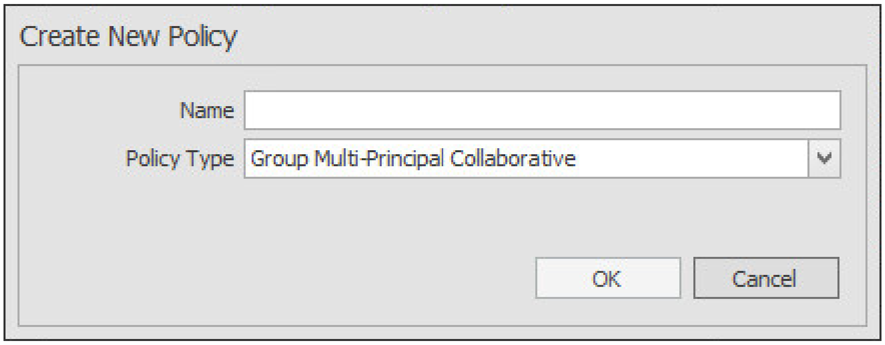
## Create a Multi-Principal Collaborative Storage Policy

1 In SMAdmin, click the **Home** tab.

2 Click **Policies**.

3 In the Manage menu, select **New** > **Group Multi-Principal Collaborative**.

The following dialog box appears:



Create New Policy

Name:

Policy Type: Group Multi-Principal Collaborative

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

For example, Auto Manufacturers.

5 Proceed with "Setting Policy Options" on page 112.

## Setting Policy Options

1 Verify that the **Process Events for Associated Managed Storage** check box is selected.

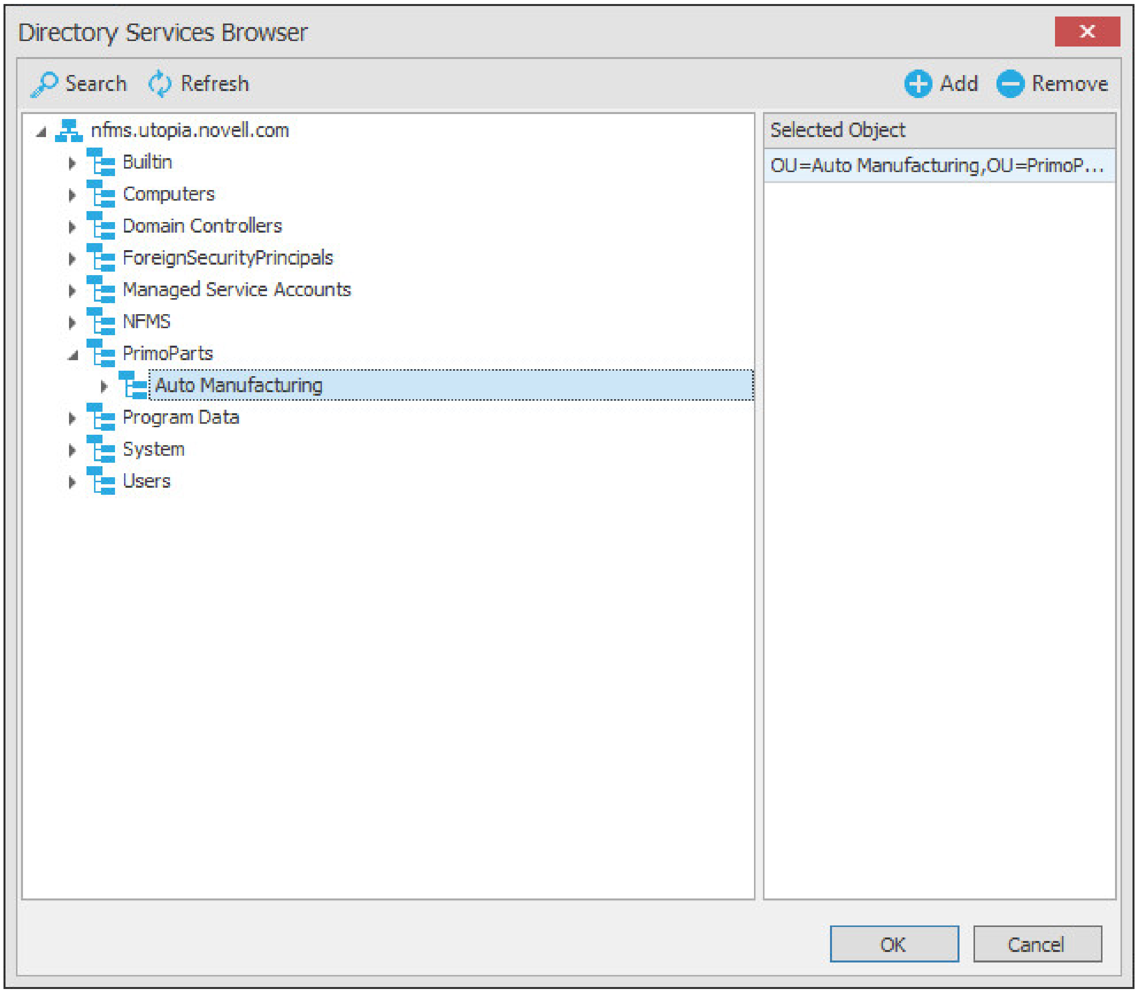
2 Verify that the **Policy applies to subcontainers** check box is selected.

3 (Optional) Enter an expanded description of the policy in the **Description** field.

4 Proceed with "Setting Associations" on page 113.

## 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.



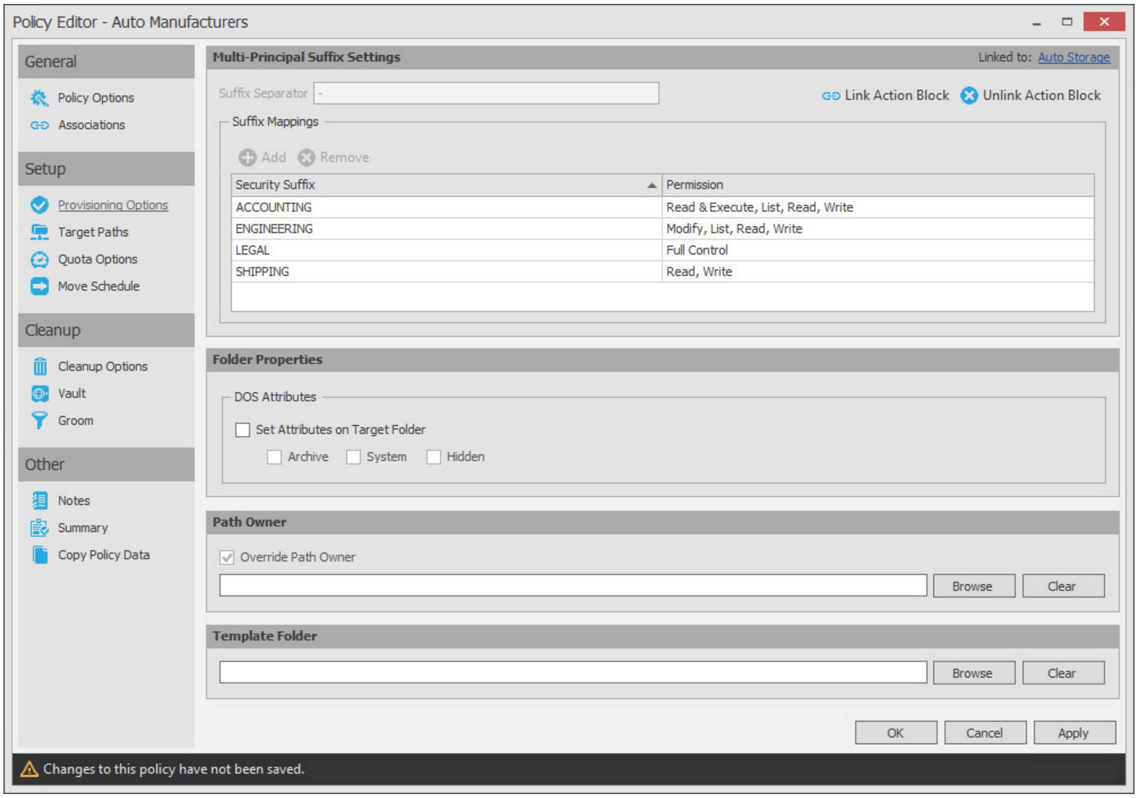
Selected Object

OU=Auto Manufacturing,OU=PrimoP...

4. Click **OK** to close the browser.
5. Proceed with "Setting Provisioning Options" on page 113.

## Setting Provisioning Options

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



**Multi-Principal Suffix Settings** Linked to: Auto Storage

Suffix Separator: -

Suffix Mappings

| Security Suffix | Permission |
|---|---|
| ACCOUNTING | Read & Execute, List, Read, Write |
| ENGINEERING | Modify, List, Read, Write |
| LEGAL | Full Control |
| SHIPPING | Read, Write |

**Folder Properties**

DOS Attributes

□ Set Attributes on Target Folder

□ Archive □ System □ Hidden

**Path Owner**

☑ Override Path Owner

**Template Folder**

Changes to this policy have not been saved.

3 In the Path Owner region of the page, click Browse and browse to specify an owner of the 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.

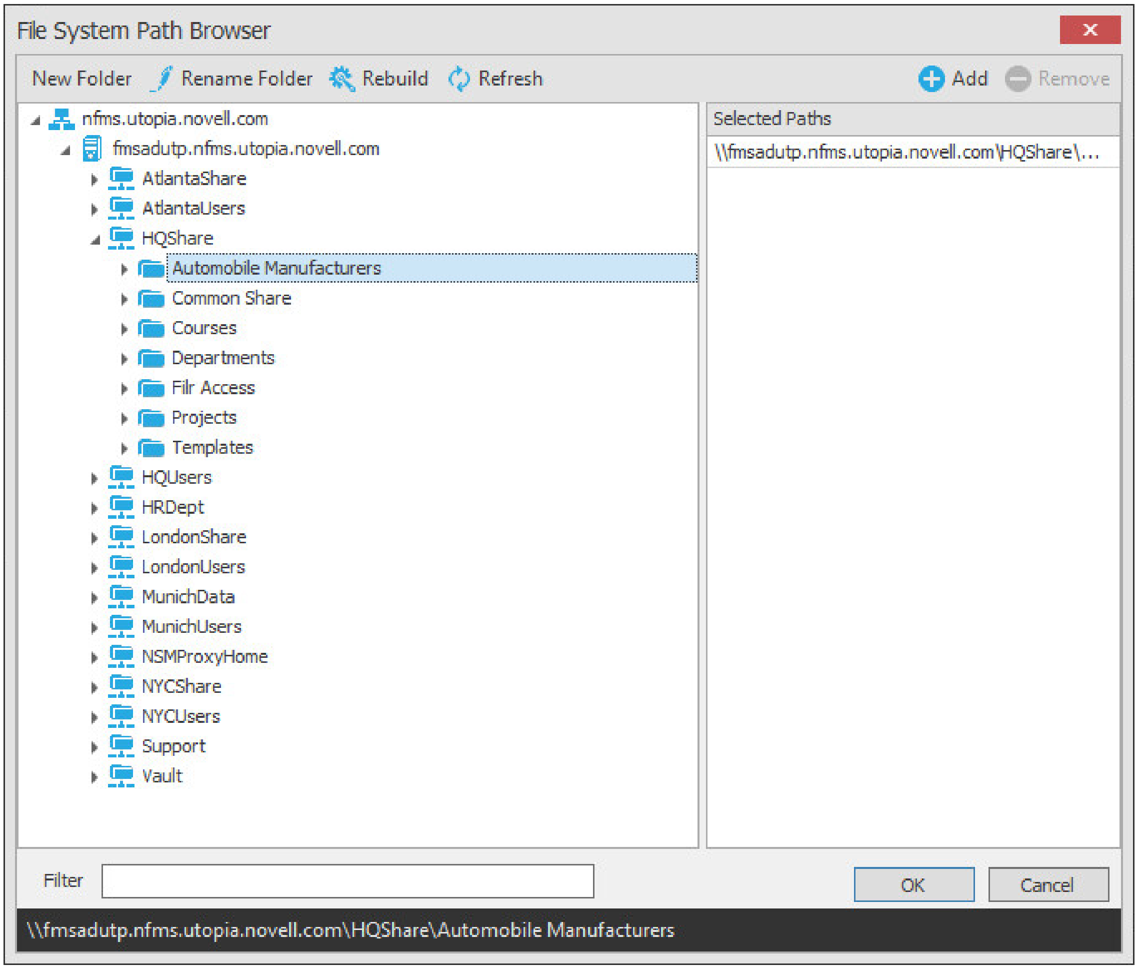
5 Proceed with "Setting the Target Path" on page 114.

## Setting the Target Path

1 Click Target Paths.

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" on page 115.

## 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.

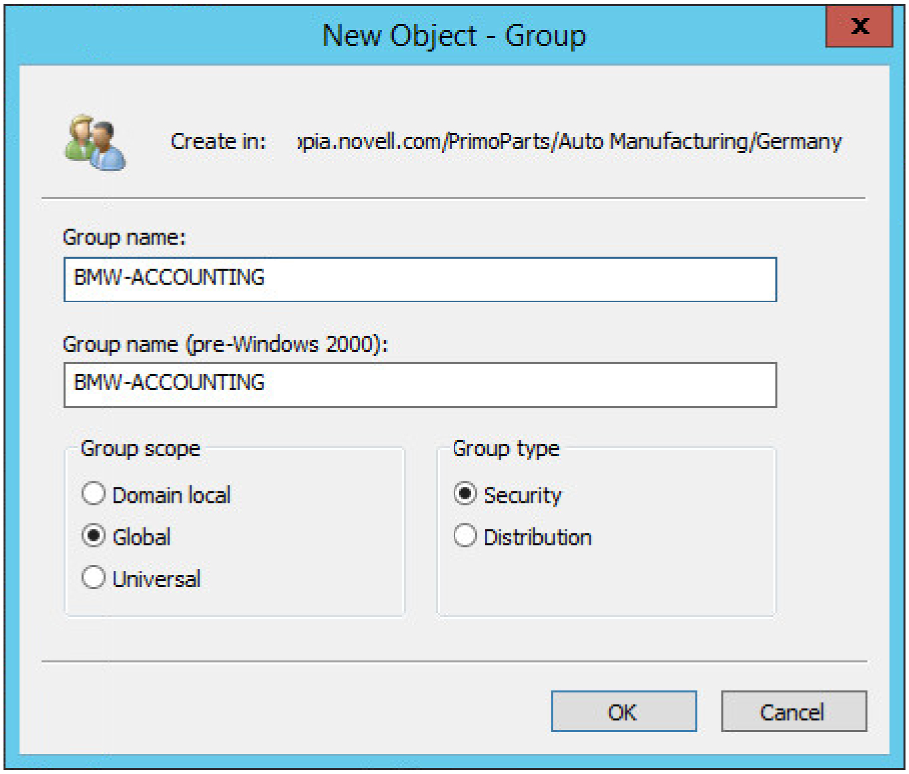
6 Proceed with "Testing the Policy" on page 116.

## 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.

Using automobile manufacturers as an example, you might create a new `BMW-ACCOUNTING` group.



Create in: ›pia.novell.com/PrimoParts/Auto Manufacturing/Germany

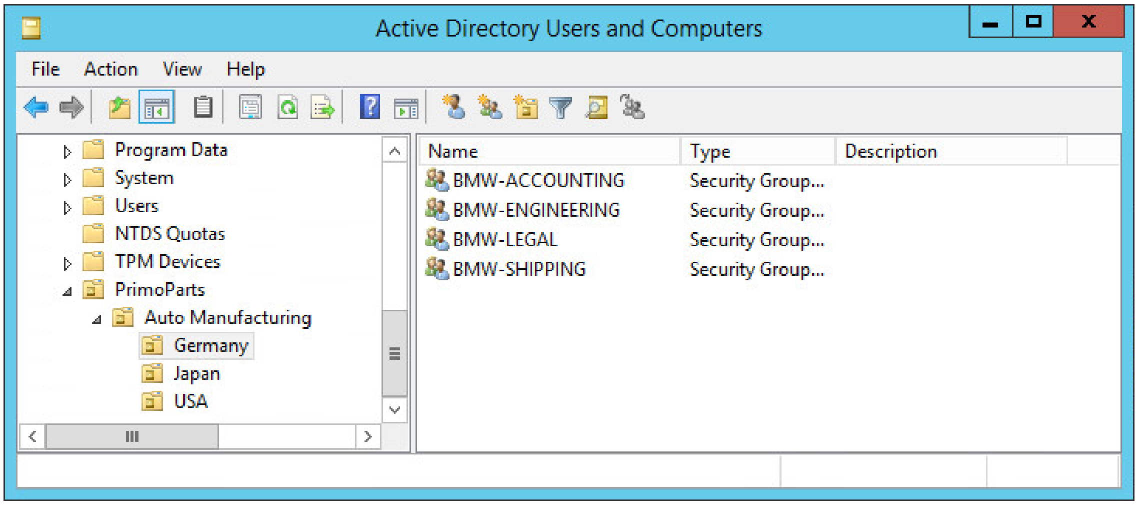
Group name: BMW-ACCOUNTING

Group name (pre-Windows 2000): BMW-ACCOUNTING

Group scope: ○ Domain local ● Global ○ Universal

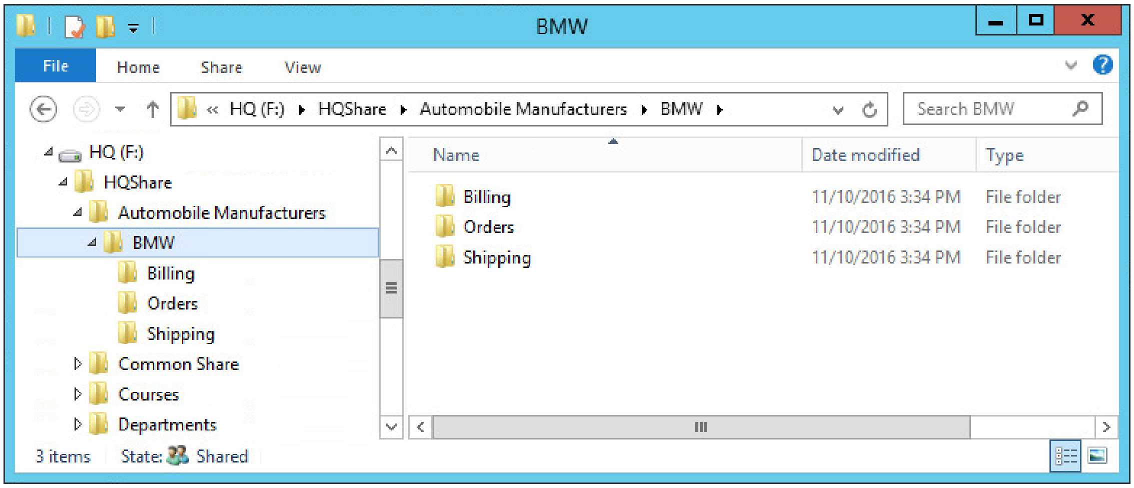
Group type: ● Security ○ Distribution

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.



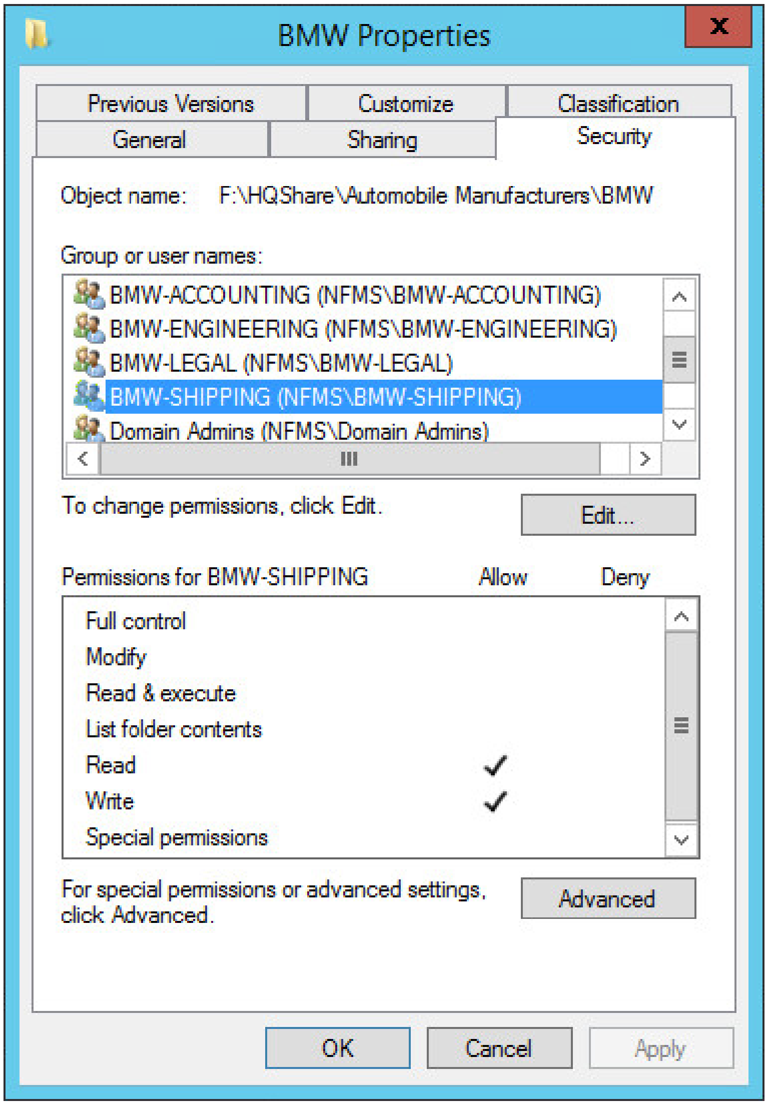
| Name | Type | Description |
|---|---|---|
| BMW-ACCOUNTING | Security Group... | |
| BMW-ENGINEERING | Security Group... | |
| BMW-LEGAL | Security Group... | |
| BMW-SHIPPING | Security Group... | |

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



| Name | Date modified | Type |
|---|---|---|
| Billing | 11/10/2016 3:34 PM | File folder |
| Orders | 11/10/2016 3:34 PM | File folder |
| Shipping | 11/10/2016 3:34 PM | File folder |

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



Object name: F:\HQShare\Automobile Manufacturers\BMW

Group or user names:

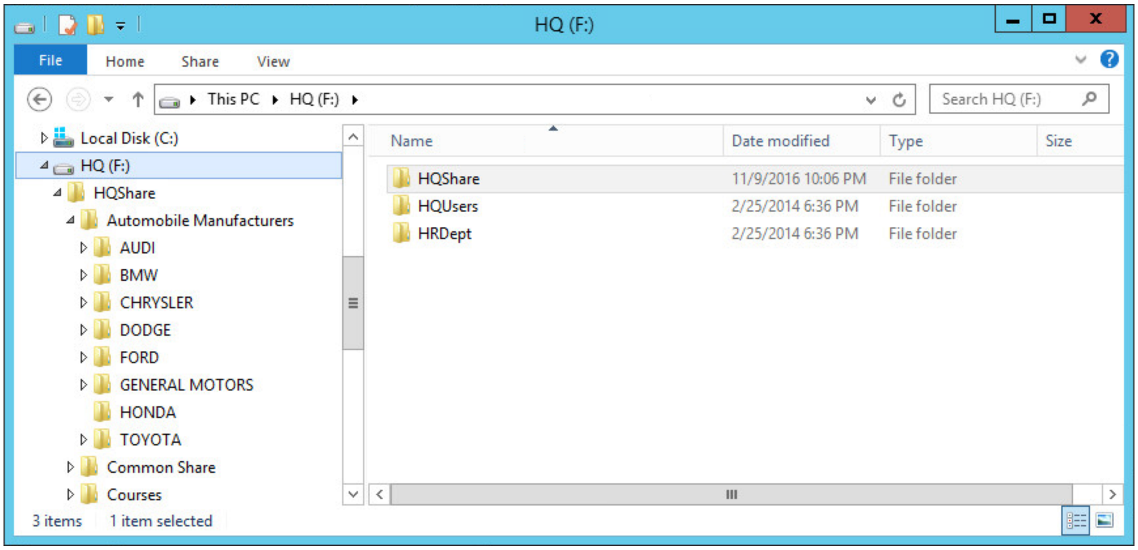
- BMW-ACCOUNTING (NFMS\BMW-ACCOUNTING)
- BMW-ENGINEERING (NFMS\BMW-ENGINEERING)
- BMW-LEGAL (NFMS\BMW-LEGAL)
- BMW-SHIPPING (NFMS\BMW-SHIPPING)
- Domain Admins (NFMS\Domain Admins)

To change permissions, click Edit.

| Permissions for BMW-SHIPPING | Allow | Deny |
|---|---|---|
| Full control | | |
| Modify | | |
| Read & execute | | |
| List folder contents | | |
| Read | ✓ | |
| Write | ✓ | |
| Special permissions | | |

For special permissions or advanced settings, click Advanced.

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.



| Name | Date modified | Type | Size |
|---|---|---|---|
| HQShare | 11/9/2016 10:06 PM | File folder | |
| HQUsers | 2/25/2014 6:36 PM | File folder | |
| HRDept | 2/25/2014 6:36 PM | File folder | |

# 9 Using Quota Manager

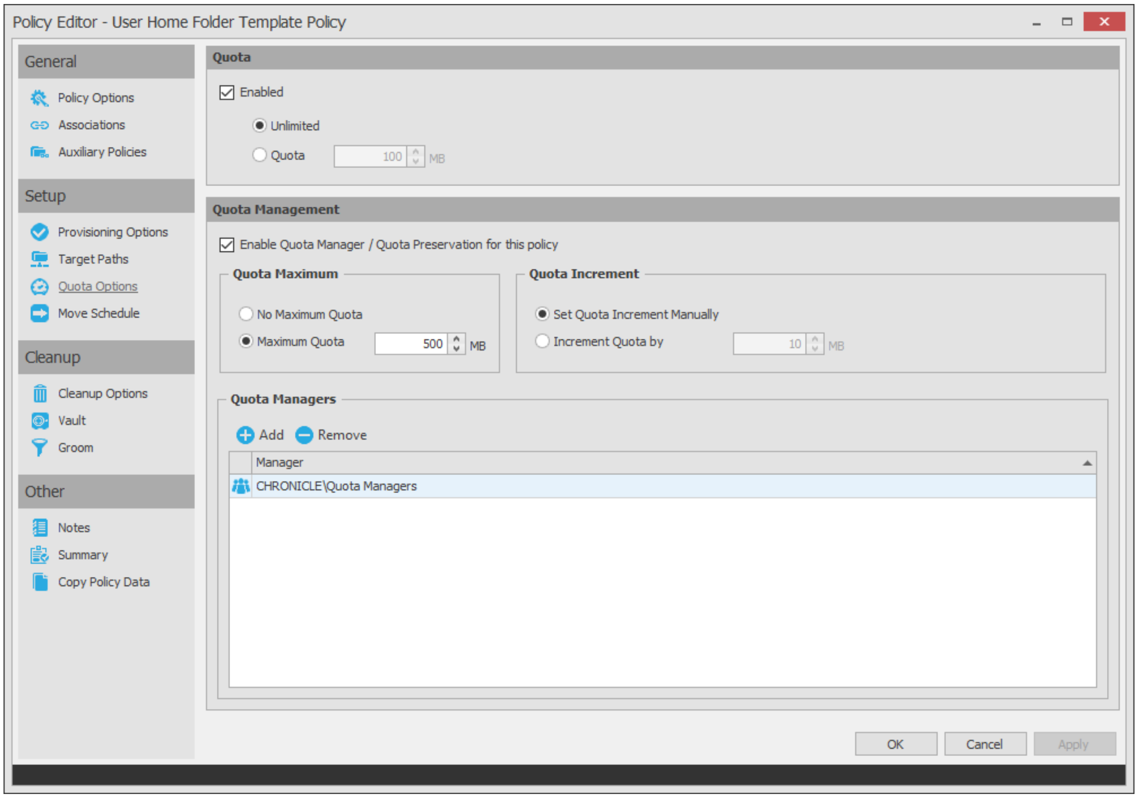
Quota Manager is a separate management interface for designated users such as help desk administrators or support personnel, to adjust user home folder or collaborative storage quota without needing permissions to the file system.

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.

- Section 9.1, “Quota Management Prerequisites,” on page 119
- Section 9.2, “Managing Quotas Through Quota Manager,” on page 120
- Section 9.3, “Understanding Quota Manager Status Indicators,” on page 122

## 9.1 Quota Management Prerequisites

1 Using SMAdmin, 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.



Quota

☑ Enabled

● Unlimited

○ Quota 100 MB

Quota Management

☑ Enable Quota Manager / Quota Preservation for this policy

Quota Maximum

○ No Maximum Quota

● Maximum Quota 500 MB

Quota Increment

● Set Quota Increment Manually

○ Increment Quota by 10 MB

Quota Managers

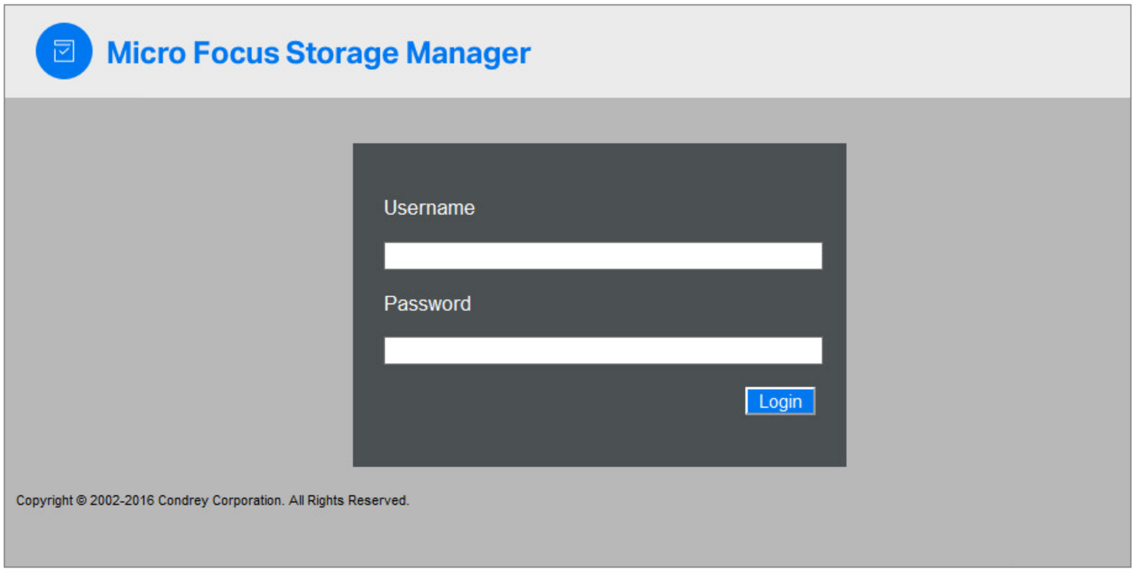
| Manager |
|---|
| CHRONICLE\Quota Managers |

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

## 9.2 Managing Quotas Through Quota Manager

1. Launch a Web browser.
2. Enter the following address: https://*ip-address-or-dns-name-of-nms-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:

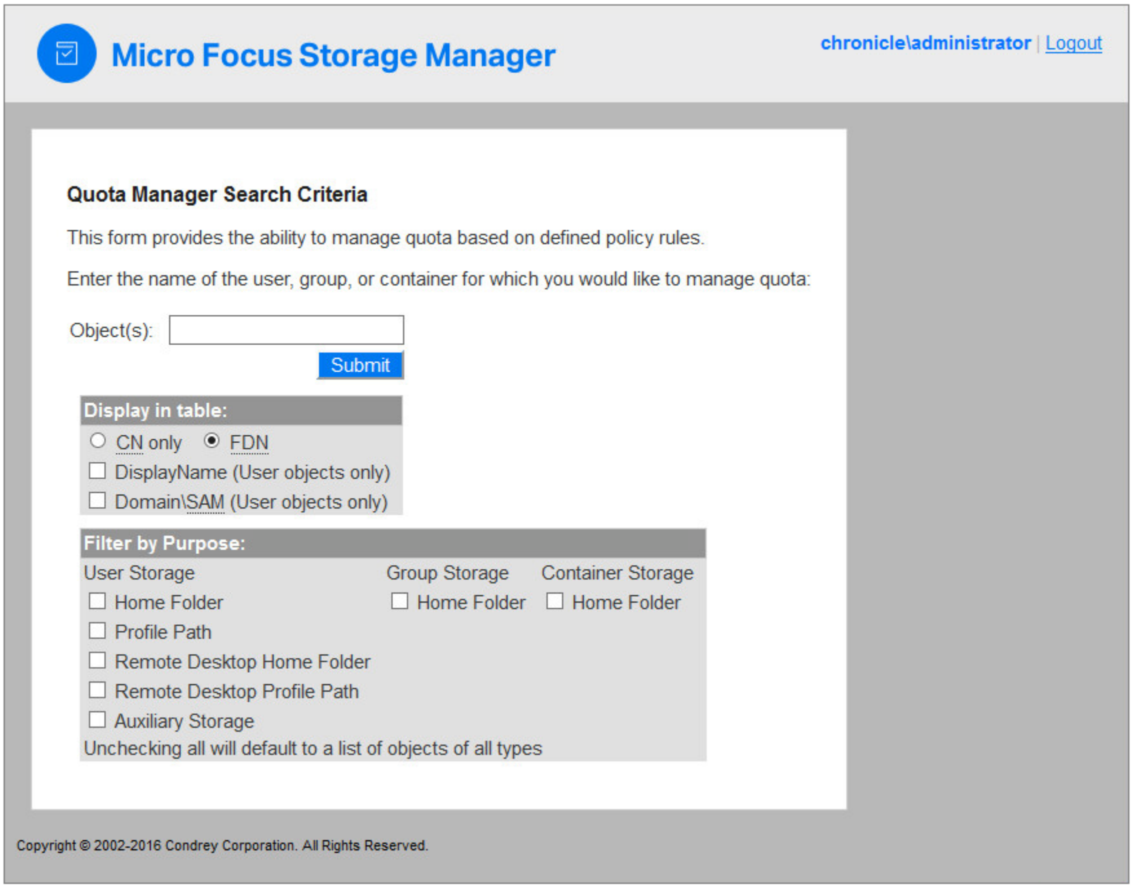


Copyright © 2002-2016 Condrey Corporation. All Rights Reserved.

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 SAM account format such as *`domain\user`* or *`user@full.domain.com`*.



Micro Focus Storage Manager

chronicle\administrator | Logout

**Quota Manager Search Criteria**

This form provides the ability to manage quota based on defined policy rules.

Enter the name of the user, group, or container for which you would like to manage quota:

Object(s): ____________

**Display in table:**

○ CN only ● FDN

□ DisplayName (User objects only)

□ Domain\SAM (User objects only)

**Filter by Purpose:**

| User Storage | Group Storage | Container Storage |
|---|---|---|
| □ Home Folder | □ Home Folder | □ Home Folder |
| □ Profile Path | | |
| □ Remote Desktop Home Folder | | |
| □ Remote Desktop Profile Path | | |
| □ Auxiliary Storage | | |

Unchecking all will default to a list of objects of all types

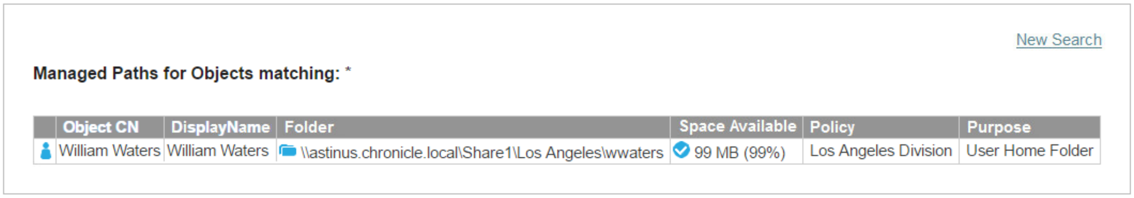
Copyright © 2002-2016 Condrey Corporation. All Rights Reserved.

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.

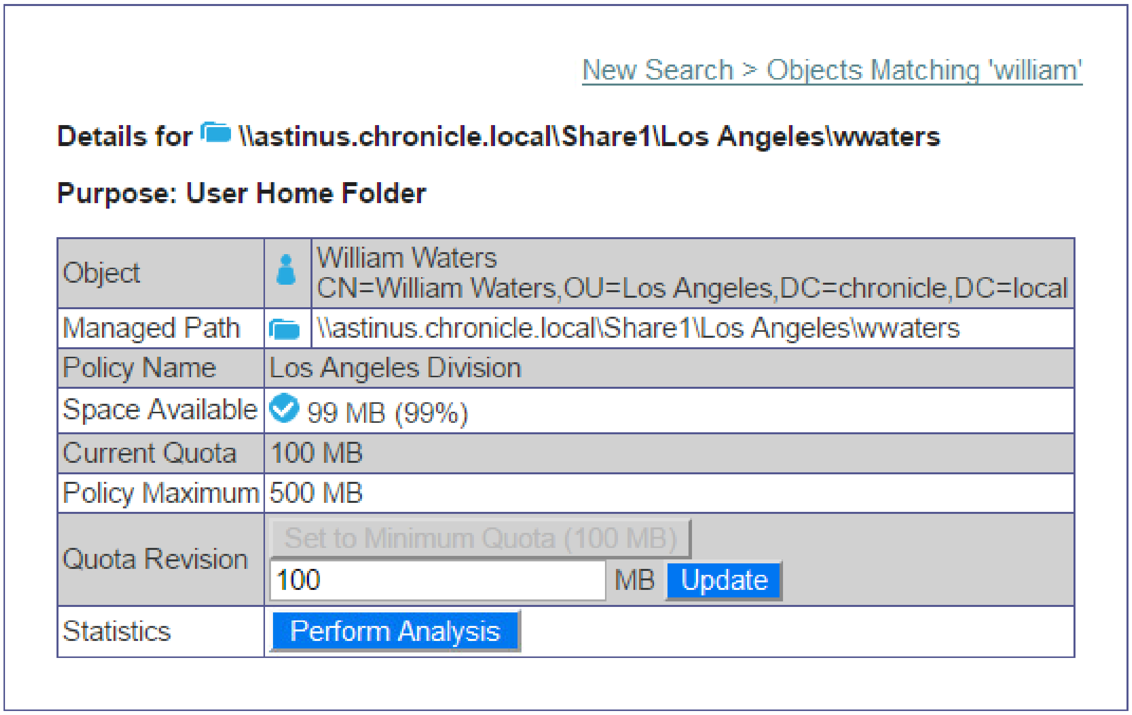
7 Click **Submit**.



**Managed Paths for Objects matching:** *

| | Object CN | DisplayName | Folder | Space Available | Policy | Purpose |
|---|---|---|---|---|---|---|
| 👤 | William Waters | William Waters | \\astinus.chronicle.local\Share1\Los Angeles\wwaters | ✓ 99 MB (99%) | Los Angeles Division | User Home Folder |

8 Click the user, group, or container you want to manage.



New Search > Objects Matching 'william'

**Details for \\astinus.chronicle.local\Share1\Los Angeles\wwaters**

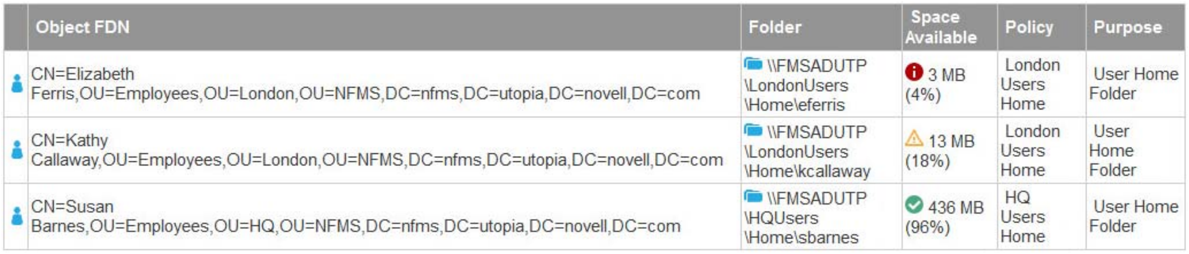
**Purpose: User Home Folder**

| | |
|---|---|
| Object | William Waters<br>CN=William Waters,OU=Los Angeles,DC=chronicle,DC=local |
| Managed Path | \\astinus.chronicle.local\Share1\Los Angeles\wwaters |
| Policy Name | Los Angeles Division |
| Space Available | ✓ 99 MB (99%) |
| Current Quota | 100 MB |
| Policy Maximum | 500 MB |
| Quota Revision | Set to Minimum Quota (100 MB)<br>100 MB Update |
| Statistics | Perform Analysis |

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

## 9.3 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.



| | Object FDN | Folder | Space Available | Policy | Purpose |
|---|---|---|---|---|---|
| | CN=Elizabeth Ferris,OU=Employees,OU=London,OU=NFMS,DC=nfms,DC=utopia,DC=novell,DC=com | \\FMSADUTP\LondonUsers\Home\eferris | ❗ 3 MB (4%) | London Users Home | User Home Folder |
| | CN=Kathy Callaway,OU=Employees,OU=London,OU=NFMS,DC=nfms,DC=utopia,DC=novell,DC=com | \\FMSADUTP\LondonUsers\Home\kcallaway | ⚠ 13 MB (18%) | London Users Home | User Home Folder |
| | CN=Susan Barnes,OU=Employees,OU=HQ,OU=NFMS,DC=nfms,DC=utopia,DC=novell,DC=com | \\FMSADUTP\HQUsers\Home\sbarnes | ✓ 436 MB (96%) | HQ Users Home | User Home 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.

# 10 Performing an eDirectory to Active Directory Cross-Empire Data Migration

**IMPORTANT:** With the release of Storage Manager 5.0, Micro Focus began providing the eDirectory to Active Directory Cross-Empire Data Migration and the new Active Directory to Active Directory Cross-Empire Data Migration subsystems only as additive support pack purchases to Storage Manager.

For example, if you wanted to migrate user data from OES to Microsoft, you would need to purchase licenses for Storage Manager 5.*x* for Active Directory + the eDirectory to Active Directory Cross-Empire Data Migration support pack.

If you do not have the additional support pack licenses, the Cross-Empire Data Migration options in SMAdmin are disabled.

eDirectory to Active Directory Cross-Empire Data Migration is a for-purchase add-on subsystem for Storage Manager that allows for the movement of file system data from the Novell or Micro Focus NSS network file system and eDirectory directory service, to the Microsoft NTFS network file system and Active Directory directory service.

Many customer initiatives can precipitate the need for such a move, including a migration to a different server operating system, a merger and acquisition by the organization, or just the consolidation of environments.

## 10.1 Understanding an eDirectory to Active Directory Cross-Empire Data Migration

The mission of Cross-Empire Data Migration is to quickly and easily perform automated movement of data, based on a variety of scenarios, including the movement of data for multiple users and groups directly to its intended location across multiple servers or shares in a single operation, all while preserving certain file system metadata. Further, Cross-Empire Data Migration lets you leverage the policies provided in Storage Manager to allow you to move to a managed storage environment on the target system and optionally restructure and reorganize data in the process.

A wizard in SMAdmin allows you to implement a phased approach to migration by incorporating one or more migration types offered through the interface to add work onto the Storage Manager event queue. In taking advantage of the dispatching and state machine architecture features of the event queue, the migration effort can be enhanced both in terms of performance through the Agent subsystem and in terms of reliability in overcoming outages and other factors that occur in real-world environments. Additionally, other options involving copying permissions, file ownership, filtering of the files to be copied and more, allow for greater control and flexibility during a data migration operation.

In addition to the eDirectory to Active Directory Cross-Empire Data Migration, there is a separate for-purchase Active Directory to Active Directory Cross-Empire Data Migration offering. For more information, see Chapter 11, “Performing an Active Directory to Active Directory Cross-Empire Data Migration,” on page 207.

Cross-Empire Data Migration generally supports three constructs for movement:

- Section 10.1.1, “User Storage Migration,” on page 126
- Section 10.1.2, “Collaborative or Group Storage Migration,” on page 127
- Section 10.1.3, “Direct Folder Migration,” on page 128

## 10.1.1 User Storage Migration

Cross-Empire Data Migration can be used to copy User object personal file data from the source platform to the target platform. In an eDirectory to Active Directory scenario, this would likely be a migration of the data from the Novell or Micro Focus home directory to the Microsoft home folder. There are two options for migrating personal storage. The difference between the two is related to how Storage Manager determines the path to a specific user’s data on the source network. These options can be used exclusively or in combination with one another during a migration project:

- “User to User” on page 126
- “Folder to User” on page 126

### User to User

This option allows you to instruct Storage Manager to determine the source location for user data by using the Home Directory attribute in eDirectory. As part of the migration wizard, you specify a source eDirectory container. The User objects within that container are listed for matching with the target, and you can select one or more users for migration. For each user selected, the Home Directory attribute provides the source file system path to be used. This option is very useful when the Home Directory attribute in the source tree is populated correctly and there is a need to migrate data simultaneously from multiple locations on the source network. It is also very useful if the user directory name on the source does not match the account name on the target.

For procedures on performing a user to user data migration, see Section 10.8, “Performing a User to User Data Migration,” on page 151.

### Folder to User

This option allows you to specify the location of user data by providing a file system path as the source. Instead of specifying an eDirectory container, you specify a parent folder location on the file system in the source network. From this folder, all immediate subfolders are listed for matching with the target, and you can select one or more for migration. This option is useful when the Home Directory attribute in the source tree is not populated or reliable, or there is a need to migrate a set of users with folders in a single path on a single volume.

For procedures on performing a folder to user data migration, see Section 10.9, “Performing a Folder to User Data Migration,” on page 159.

## 10.1.2 Collaborative or Group Storage Migration

File system data used by groups can also be copied by using the eDirectory to Active Directory Cross-Empire Data Migration subsystem. The options available to the administrator are similar to those available for user storage, but are different in whether to rely on data in directory services or specify the file system paths directly.

The underlying concept behind both options is that the collaborative storage is being moved to a managed storage environment on the target network, which means that the collaborative managed path attribute is being populated and managed in directory services in the target. If you don’t want to move some of the collaborative group directories, you should consider using direct folder storage migration., which is documented at Section 10.1.3, “Direct Folder Migration,” on page 128.

The following options are available for moving collaborative storage:

- “Group to Group” on page 127
- “Folder to Group” on page 127

### Group to Group

This option allows you to instruct Storage Manager to determine the source location for user data by using the group managed path attribute in eDirectory. As part of the migration wizard, you specify a source eDirectory container. The Group objects within that container are listed for matching with the target, and you can select one or more groups for migration. For each group selected, the group managed path attribute provides the source file system path to be used. This option is very useful when Storage Manager has been used to manage collaborative storage in the source tree.

For procedures on performing a group to group data migration, see Section 10.10, “Performing a Group to Group Data Migration,” on page 166.

### Folder to Group

This option allows you to specify the location of group data by providing a file system path. Instead of specifying an eDirectory container, you specify a parent folder location on the file system in the source network. From this folder, all immediate subfolders are listed for matching with the target, and you can select one or more for migration. This option is useful when Storage Manager has not been used in the source tree to manage collaborative group storage or when you are migrating only some of the group storage.

For procedures on performing a folder to group data migration, see Section 10.11, “Performing a Folder to Group Migration,” on page 173.

### 10.1.3 Direct Folder Migration

A major benefit in using Storage Manager is that your organization can move to a managed storage environment for its file system data. Storage Manager allows you to define and enforce policies on the data by driving management of it throughout the life cycle of the user or group associated with the data. The architecture of the Cross-Empire Data Migration subsystem allows organizations to move to this paradigm for both user and group storage.

However, you are not required to use this method during the migration process. You might not want to move to managed storage for all of the data, or you might want to move to it in phases. For this reason, the Cross-Empire Data Migration subsystem has provisions for direct movement of data outside of the policy construct by performing a folder to folder data migration.

#### Folder to Folder

A folder to folder migration allows you to move a folder and its contents directly from the source network to a designated location on the target network. Selecting this method in the wizard allows you to specify distinct file system paths on both the source and the target networks. All file system contents and metadata are copied during the operation.

For your convenience, there is a **Skip Open Files** option that will migrate all unopened files located in a folder. Open files are not migrated, but the filenames and paths of all of the open files are logged in a delta file. You can then ensure that all open files are closed and do a follow-up migration of these remaining files by simply specifying the location of the delta file.

You can identify and move all files that are new or have been modified from a given date. Additionally, you can verify that all of the files you wanted to migrate from a source server have been migrated.

Following the folder to folder migration, use the CEDMScanCompare utility to scan the NetWare or Open Enterprise Server source for all new and modified folders and files. Once these new folders and files have been migrated, use CEDMScanCompare again to generate a folder and file content list for both the source server and the target server, then use the application to compare the two lists to verify that all folders and files migrated properly.

For procedures on performing a folder to folder migration, see Section 10.12, “Performing a Folder to Folder Migration,” on page 180

## 10.2 Security and Ownership

Moving to a managed storage environment presents an opportunity to refine the security on the data itself. By defining the security that should be on the file system as a part of the policy, you are assured that the security of the data on the target network is in line with the security and governance requirements that your organization wants to employ. This can also contribute to present and future compliance requirements for your organization. Avoiding these types of exposure is another benefit of moving to a managed storage environment.

However, in many environments, there is a desire to migrate security and ownership assignments directly from the source environment to the target. This capability is accomplished through the creation and optional usage of an Identity Map as a part of a migration operation.

- Section 10.2.1, “Defining an Identity Map for Security and Ownership Migration,” on page 129
- Section 10.2.2, “Using an Identity Map,” on page 129

## 10.2.1 Defining an Identity Map for Security and Ownership Migration

For security and ownership information to be migrated between environments, the Cross-Empire Data Migration subsystem requires a series of object equivalence definitions to identify an object in the source environment as equivalent to an analogous object in the target environment. In other words, if an object in the source environment is given rights to a file or folder, and you want that trustee assignment to be migrated along with the data, then Storage Manager must be told which object in the target environment is equivalent to it so that the appropriate rights assignment can be made. An identity map is a construct for creating and managing these equivalence definitions.

You can create and populate an identity map within the Cross-Empire Data Migration subsystem of the SMAdmin interface. There are various options for automatically locating and matching objects based on a number of matching rules. There are options for creating manual assignments as well as for editing assignments.

However, some objects that are assigned rights in the source environment might not have an analogous object that already exists in the target environment. These objects need to be created before they can be defined to an identity map.

In addition, an analogous object might exist in the target environment, but might not be able to be assigned as a trustee, such as a container that is given rights in the source environment. The same container might exist in the target environment (Active Directory), but Active Directory does not support the assignment of a container as a security object. In these instances, a group representing the container is usually created for assigning permissions.

You can import data into an identity map. This can be useful when you already have a data set defining equivalences, or you can easily create one using data from an external system.

In general, it is standard practice to iteratively evolve an identity map as needed to perform a migration. Within the interface, you can run a check scan against a given source file system path to check rights and ownership assignments against an identity map. This identifies which objects still need a definition within the map in order for a migration to finish with 100 percent coverage for security and ownership.

## 10.2.2 Using an Identity Map

When you are satisfied with the coverage within the identity map for a given file system path, you can use the identity map as a part of a migration. You can optionally use the identity map in conjunction with any migration operation type supported by the Cross-Empire Data Migration subsystem:

- User storage migration
- Collaborative or group storage migration
- Direct folder storage migration

The system supports a single identity map within the framework at any one time. When the map is created or edited, the master copy is held by the Engine and is automatically distributed to Agents as necessary.

**IMPORTANT:** Certain operations during a Cross-Empire Data Migration involve building a cache on the local workstation or the Engine. If the identity map contains more than 20,000 objects, the time it takes to cache all of the objects could significantly inhibit the speed of the migration.

Once the cache has been built the first time on the workstation or Engine, it does not have to be rebuilt again.

## 10.3 Prerequisites

The server on which the Engine in Active Directory is installed must have the Client for OES installed while the migration is being performed. After the migration is complete, the client can be removed. Additionally, the Engine can delegate migration operations to Agents for improved migration performance. If Agents are deployed as a part of a Storage Manager installation, these Agents are individually used for migration if the Client for OES is installed on them. In order for an Agent to participate in a migration, the server that has the Agent installed must also have the Client for OES installed. This determination is made automatically within Storage Manager as a part of Agent/Engine communications and no additional configuration is required in order to use this feature.

The Client for OES installed on the Engine in Active Directory should be properly configured to use SLP (Service Location Protocol) for the eDirectory tree source of a data migration. For information on SLP configuration, see “Setting Client Properties” (https://www.novell.com/documentation/windows_client/windows_client_admin/data/hbqx7szx.html) in the *Novell Client 2 SP3 for Windows Administration Guide*.

### 10.3.1 Prerequisite Tasks

Before you proceed with an eDirectory to Active Directory Cross-Empire Data Migration, perform the following tasks:

1. Log in with Administrative access to the Domain.
2. Install the Storage Manager Engine on the target Windows server.

   See “Installing the Engine” in the *Micro Focus Storage Manager 5.2 for Active Directory Installation Guide.*
3. Install the Client for OES with the NMAS installation default option on the Engine server.

   The Client for OES can be removed after you have completed your migrations.
4. Extend the Active Directory schema.

   This is required only if you are migrating to a target share managed by a collaborative storage policy.

   See “Active Directory Schema” in the *Micro Focus Storage Manager 5.2 for Active Directory Installation Guide*.
5. Install SMAdmin.

   See “Installing SMAdmin” in the *Micro Focus Storage Manager 5.2 for Active Directory Installation Guide*.
6. (Optional) Install and authorize the Event Monitor.

   The Event Monitor is not needed for a Cross-Empire Data Migration, but is needed for managing storage once your data has been migrated to the Microsoft network.

   See “Installing and Configuring the Event Monitor” and “Authorizing the Event Monitor” in the *Micro Focus Storage Manager 5.2 for Active Directory Installation Guide*.
7. Assign SMProxyRights group Full Control permission to the shares to which you will be migrating data.

   See “Setting Rights and Privileges on Managed Storage” in the *Micro Focus Storage Manager 5.2 for Active Directory Installation Guide*.
8. Install and authorize Agents and configure Proxy Agents for all servers that will be target servers for Cross-Empire Data Migrations.

   See “Installing and Configuring the Agents” and “Authorizing the Agents ” in the *Micro Focus Storage Manager 5.2 for Active Directory Installation Guide*.

9. (Conditional) If you plan to migrate data to a NAS device, make the SMProxyRights group a member of the Local Administrators group on each NAS device.

   See "Setting Rights and Privileges on Managed Storage" in the *Micro Focus Storage Manager 5.2 for Active Directory Installation Guide*.

10. Install the Client for OES and configure SLP on any Agent servers that will be involved in a Cross-Empire Data Migration.

    The Client for OES can be removed after you have completed your migrations.

11. Create Storage Manager policies for the migration of storage.

    These policies are needed if the Cross-Empire Data Migrations will be driven by Storage Manager policies, which we recommend for migrating user data.

12. For all objects in eDirectory that have rights assigned to the file system, create matching objects in Active Directory.

    To migrate rights assigned to containers, you must create an equivalent Group object in Active Directory for each container object in eDirectory,.

## 10.4 Creating the Migration Proxy Account

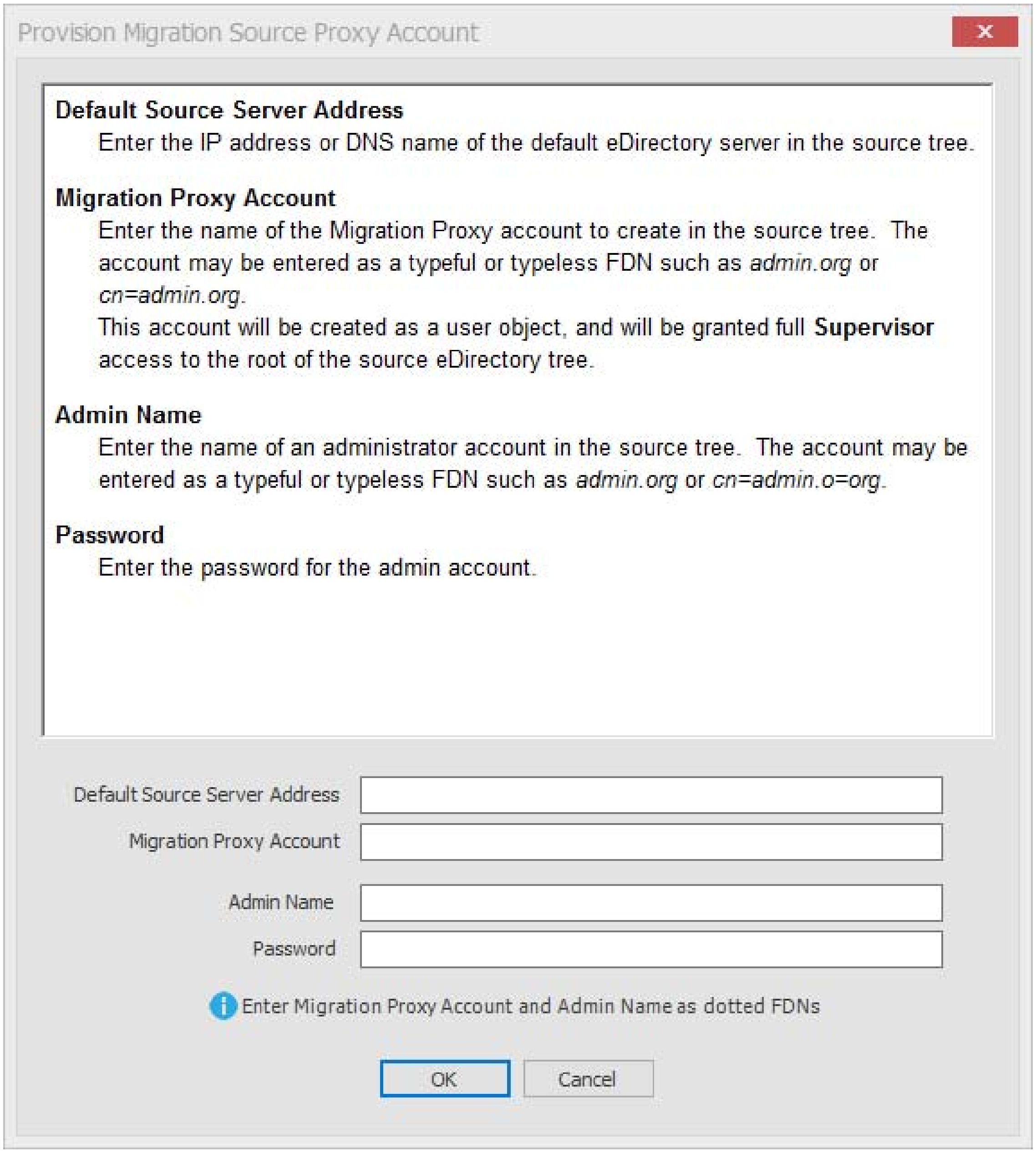
The Engine running in Active Directory uses a migration proxy account to log in to the eDirectory tree. Any time you perform a migration from the eDirectory tree to the Active Directory domain, SMAdmin uses the migration proxy account that you establish in this procedure.

**IMPORTANT:** This process creates a new User object in eDirectory with a 32-character password that is generated automatically by Storage Manager. If your Universal Password policy does not accommodate 32-character passwords, you must modify or create a new Universal Password policy before proceeding. For more information, refer to Section 3.4, "Creating Password Policies," (http://www.novell.com/documentation/password_management33/pwm_administration/data/an4bun5.html) in the *Novell Password Management 3.3.1 Administration Guide*, especially the information in Figure 3.3, "Advanced Password Rules Continued."

**1** Launch SMAdmin.

**2** From the **Home** tab, click **Cross-Empire Data Migrations** > **eDirectory to Active Directory**.

**3** From the **Proxy Account Management** drop-down menu, select **Provision Source Proxy Account**.



Provision Migration Source Proxy Account

**Default Source Server Address**
Enter the IP address or DNS name of the default eDirectory server in the source tree.

**Migration Proxy Account**
Enter the name of the Migration Proxy account to create in the source tree. The account may be entered as a typeful or typeless FDN such as *admin.org* or *cn=admin.org*.
This account will be created as a user object, and will be granted full **Supervisor** access to the root of the source eDirectory tree.

**Admin Name**
Enter the name of an administrator account in the source tree. The account may be entered as a typeful or typeless FDN such as *admin.org* or *cn=admin.o=org*.

**Password**
Enter the password for the admin account.

Default Source Server Address
Migration Proxy Account
Admin Name
Password

Enter Migration Proxy Account and Admin Name as dotted FDNs

**4** Fill in the following fields:

**Default source Server Address:** Specify the IP address or DNS name of a server in the eDirectory tree where the files you want to migrate are located. The Engine in the Active Directory environment must be able to communicate with this server when performing data migrations.

**Migration Proxy Account:** Provision a migration proxy account by specifying the typeless fully distinguished name (FDN) of the proxy account that you want to provision.

The Engine running in Active Directory uses the migration proxy account to log in to the eDirectory tree. Any time you perform a migration from the eDirectory tree to the Active Directory domain, the Engine uses the migration proxy account that you establish in this step.

**Admin Name:** Specify the typeless FDN of an account in the source eDirectory tree that has the appropriate right to provision the Migration Proxy Account (MPA).

**Password:** Specify the password for the typeless FDN provided above.

5 Click **OK**

6 When the confirmation dialog box appears, click **Yes**.

The information entered in the Provision Migration Source Proxy Account dialog box is now displayed in the fields of the **Migration Source Information** region of the page.

The Engine logs in as the Admin account provided and provisions the MPA as a User object in the source eDirectory tree. It also grants the MPA object full rights to the root of the source tree, which allows Storage Manager to pull eDirectory and file system information during the course of migration operations.

# 10.5 Creating and Modifying an Identity Map

Micro Focus Storage Manager for Active Directory uses an identity map to make associations between the users, groups, and containers that are the owners and trustees of the Novell or Micro Focus network data and the corresponding data owners on the Microsoft network target.

You create a single identity map for each eDirectory tree that you are migrating.

**IMPORTANT:** You must create an identity map so that file and folder rights, trustee assignments, and other metadata are maintained during the migration. If you do not want to maintain these rights, trustee assignments, and other metadata, you can skip this section and migrate through using the **Data Only** option from the **Migration Wizards** menu.

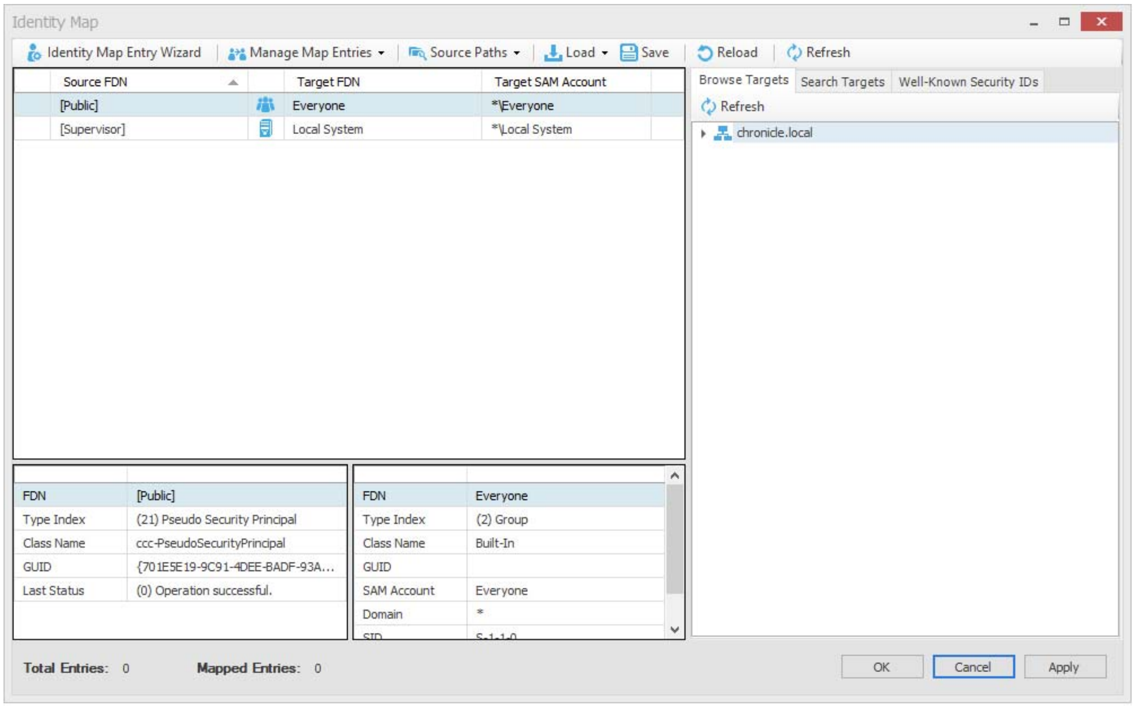
## 10.5.1 Creating an Identity Map

1 In SMAdmin, click the **Home** tab.

2 Click **Cross-Empire Data Migration > eDirectory to Active Directory.**

3 Click **Identity Map Management** > **Edit Identity Map**.

The following page appears:



| Source FDN | Target FDN | Target SAM Account |
|---|---|---|
| [Public] | Everyone | *\Everyone |
| [Supervisor] | Local System | *\Local System |

| | |
|---|---|
| FDN | [Public] |
| Type Index | (21) Pseudo Security Principal |
| Class Name | ccc-PseudoSecurityPrincipal |
| GUID | {701E5E19-9C91-4DEE-BADF-93A… |
| Last Status | (0) Operation successful. |

| | |
|---|---|
| FDN | Everyone |
| Type Index | (2) Group |
| Class Name | Built-In |
| GUID | |
| SAM Account | Everyone |
| Domain | * |
| SID | S-1-1-0 |

Total Entries: 0 Mapped Entries: 0

The page displays an initial identity map with a small number of suggested entries that you can append.

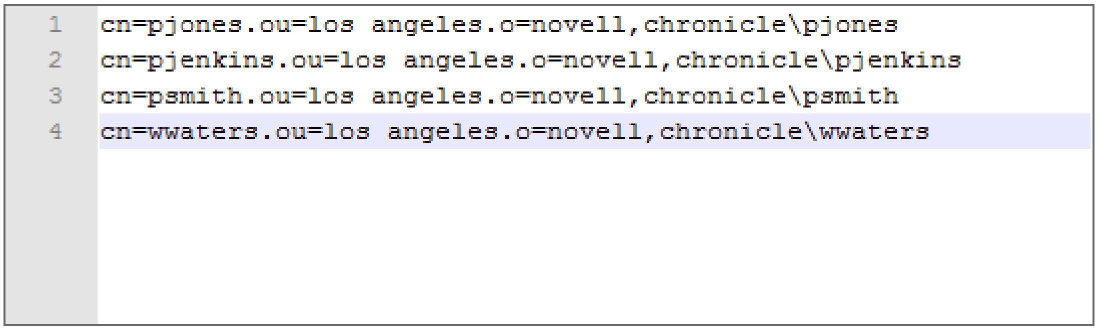
4 Do one of the following:

- To import associations between users in eDirectory and Active Directory using a delimited text CSV file, go to “Importing Identity Associations through Delimited Text” on page 134.
- To associate the users between the two directory services yourself, go to “Creating Object Associations” on page 138.

## Importing Identity Associations through Delimited Text

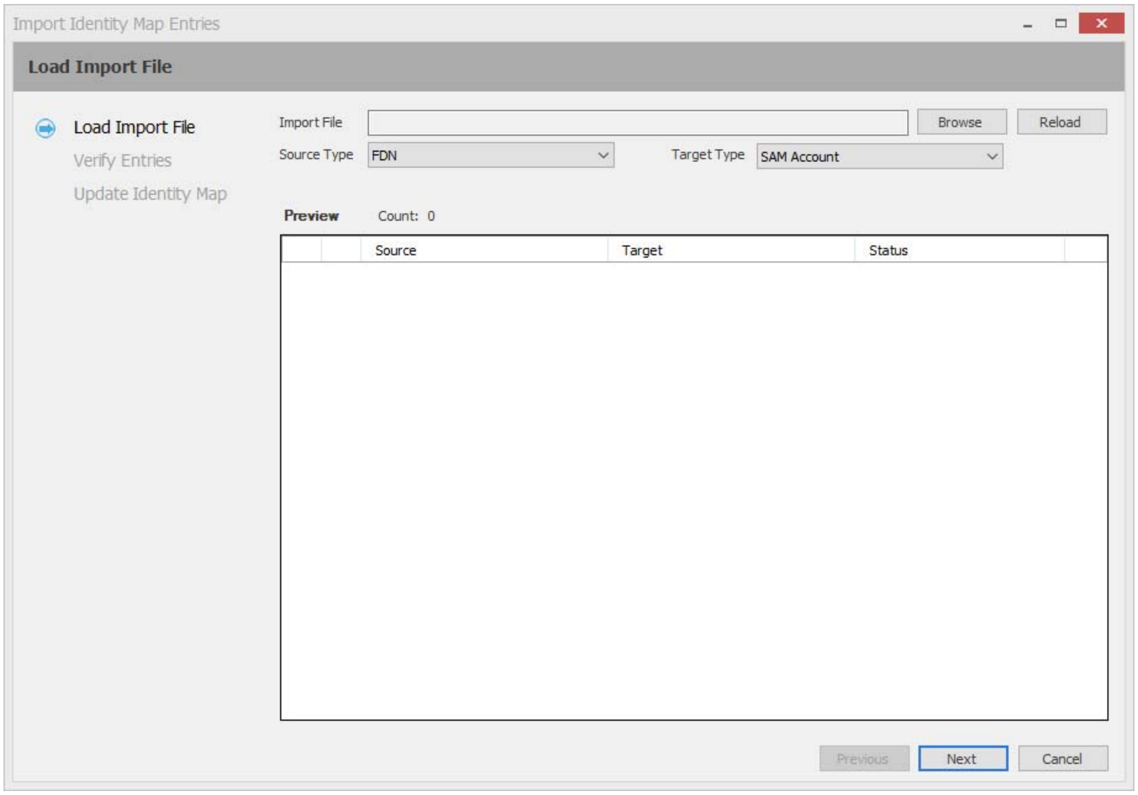
If you have a delimited text CSV file that associates eDirectory user and group objects with Active directory user and group objects, you can import it into the identity map using the **Import Identity Map from Delimited Text** option.

The CSV file can have entries using either typeful or typeless Fully Distinguished Names (FDNs).



```
cn=pjones.ou=los angeles.o=novell,chronicle\pjones
cn=pjenkins.ou=los angeles.o=novell,chronicle\pjenkins
cn=psmith.ou=los angeles.o=novell,chronicle\psmith
cn=wwaters.ou=los angeles.o=novell,chronicle\wwaters
```

1 Select **Load** > **Import Identity Map from Delimited Text**.



**Load Import File**

- Load Import File
- Verify Entries
- Update Identity Map

Import File

Source Type: FDN

Target Type: SAM Account

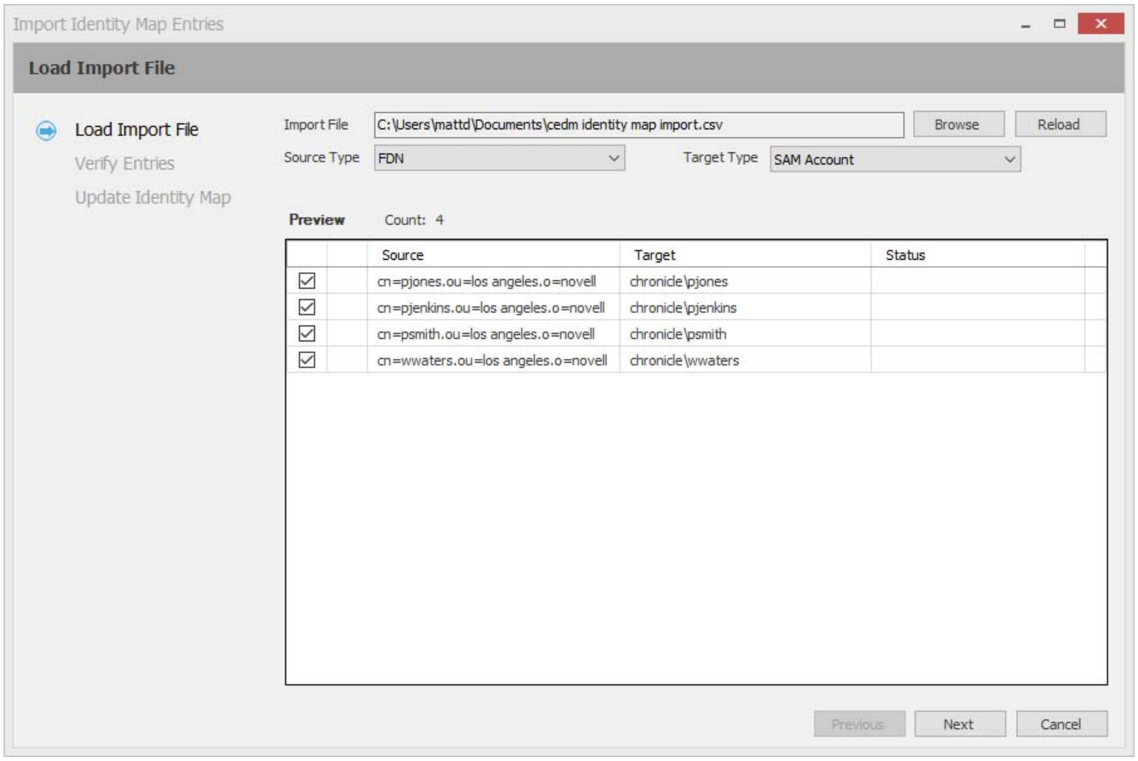
**Preview** Count: 0

| | | Source | Target | Status |
|---|---|---|---|---|

2 Click **Browse**.

3 Select the CSV file, then click **Open**.

The following page appears and specifies whether the names in the CSV file are formatted properly.



**Load Import File**

- Load Import File
- Verify Entries
- Update Identity Map

Import File: C:\Users\mattd\Documents\cedm identity map import.csv

Source Type: FDN

Target Type: SAM Account

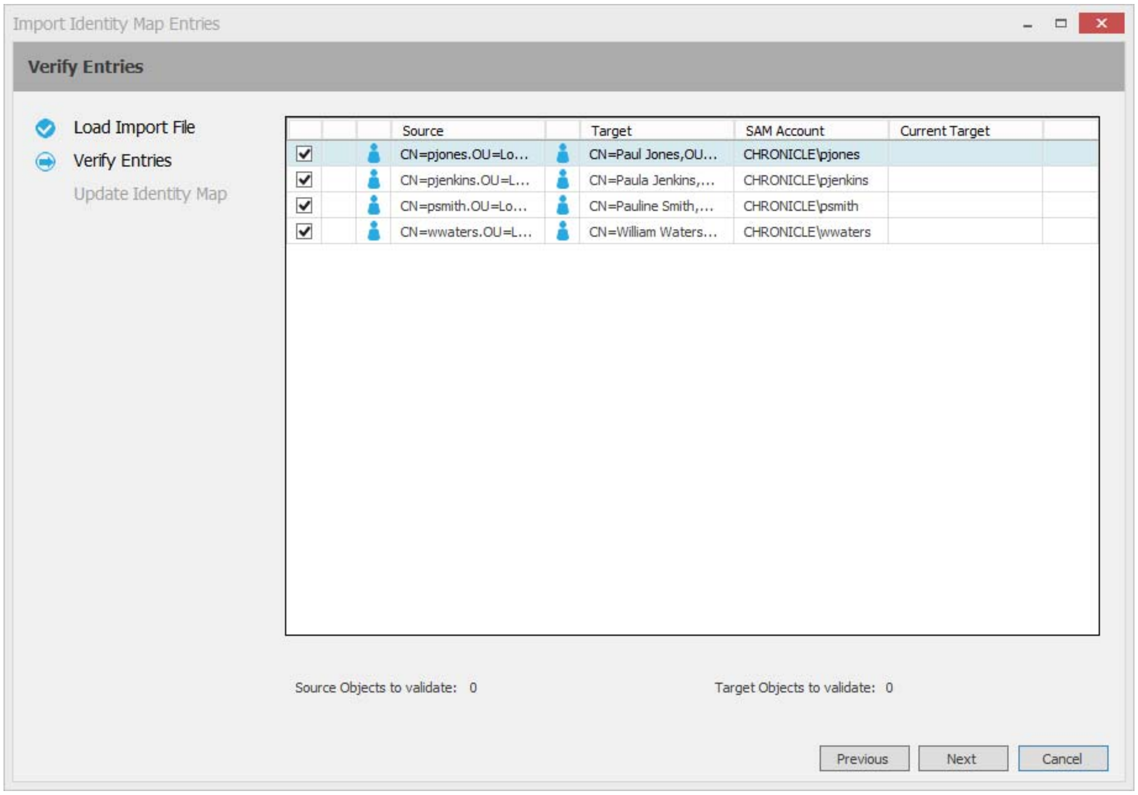
**Preview** Count: 4

| | | Source | Target | Status |
|---|---|---|---|---|
| ☑ | | cn=pjones.ou=los angeles.o=novell | chronicle\pjones | |
| ☑ | | cn=pjenkins.ou=los angeles.o=novell | chronicle\pjenkins | |
| ☑ | | cn=psmith.ou=los angeles.o=novell | chronicle\psmith | |
| ☑ | | cn=wwaters.ou=los angeles.o=novell | chronicle\wwaters | |

**4** (Conditional) If incorrect options in the **Source Type** or **Target Type** fields are displayed, select the correct options.

**5** Click **Next**.

The following page appears and specifies whether the user and group objects exist in eDirectory and Active Directory.

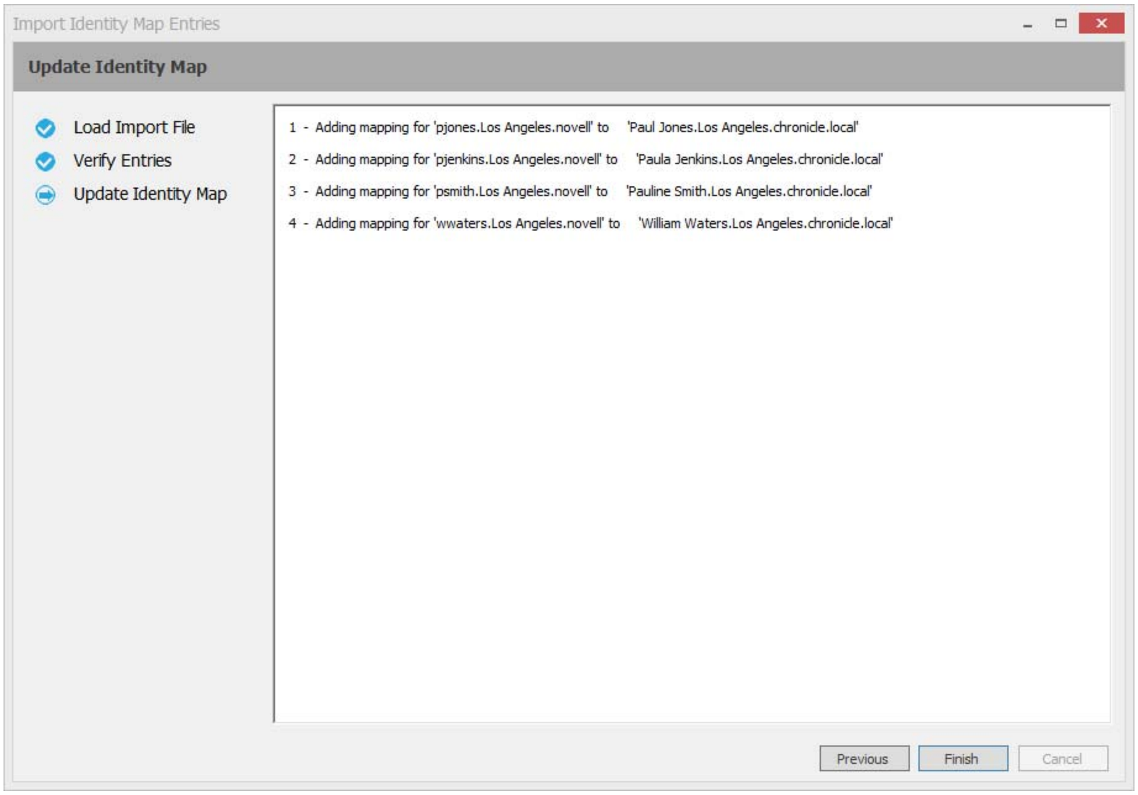


| | Source | Target | SAM Account | Current Target |
|---|---|---|---|---|
| ☑ | CN=pjones.OU=Lo… | CN=Paul Jones,OU… | CHRONICLE\pjones | |
| ☑ | CN=pjenkins.OU=L… | CN=Paula Jenkins,… | CHRONICLE\pjenkins | |
| ☑ | CN=psmith.OU=Lo… | CN=Pauline Smith,… | CHRONICLE\psmith | |
| ☑ | CN=wwaters.OU=L… | CN=William Waters… | CHRONICLE\wwaters | |

Source Objects to validate: 0

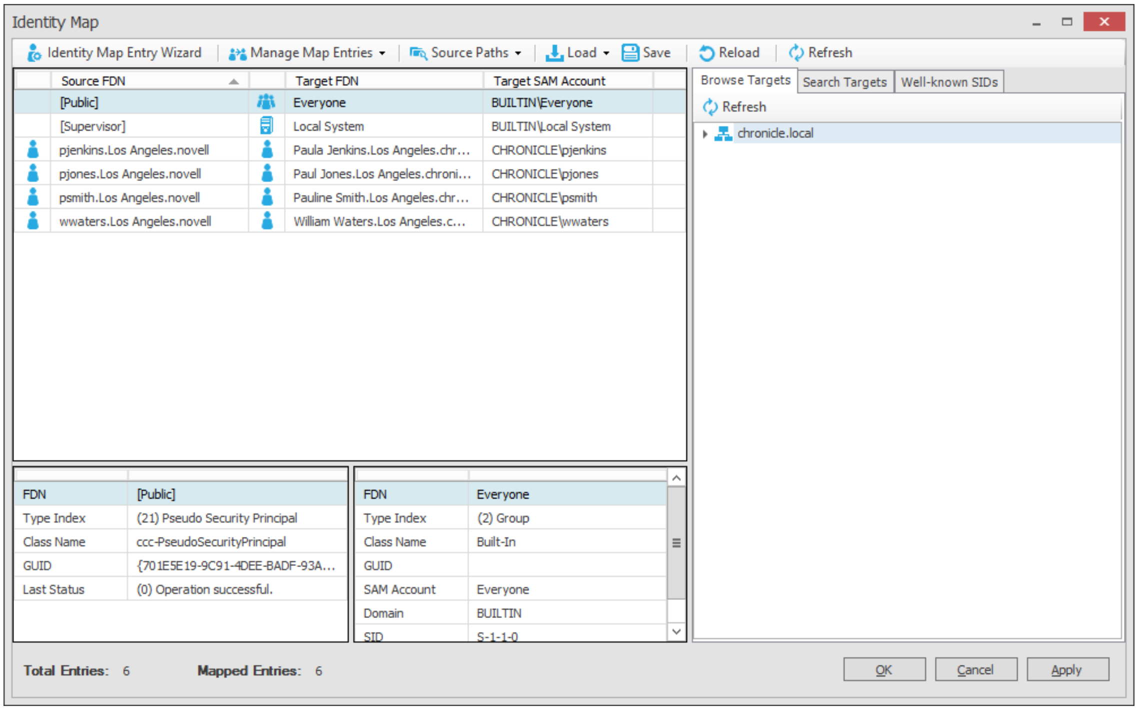
Target Objects to validate: 0

**6** Click **Next**.



```
1 - Adding mapping for 'pjones.Los Angeles.novell' to  'Paul Jones.Los Angeles.chronicle.local'
2 - Adding mapping for 'pjenkins.Los Angeles.novell' to  'Paula Jenkins.Los Angeles.chronicle.local'
3 - Adding mapping for 'psmith.Los Angeles.novell' to  'Pauline Smith.Los Angeles.chronicle.local'
4 - Adding mapping for 'wwaters.Los Angeles.novell' to  'William Waters.Los Angeles.chronicle.local'
```

7 Click **Finish**.



| Source FDN | Target FDN | Target SAM Account |
|---|---|---|
| [Public] | Everyone | BUILTIN\Everyone |
| [Supervisor] | Local System | BUILTIN\Local System |
| pjenkins.Los Angeles.novell | Paula Jenkins.Los Angeles.chr… | CHRONICLE\pjenkins |
| pjones.Los Angeles.novell | Paul Jones.Los Angeles.chroni… | CHRONICLE\pjones |
| psmith.Los Angeles.novell | Pauline Smith.Los Angeles.chr… | CHRONICLE\psmith |
| wwaters.Los Angeles.novell | William Waters.Los Angeles.c… | CHRONICLE\wwaters |

| | |
|---|---|
| FDN | [Public] |
| Type Index | (21) Pseudo Security Principal |
| Class Name | ccc-PseudoSecurityPrincipal |
| GUID | {701E5E19-9C91-4DEE-BADF-93A… |
| Last Status | (0) Operation successful. |

| | |
|---|---|
| FDN | Everyone |
| Type Index | (2) Group |
| Class Name | Built-In |
| GUID | |
| SAM Account | Everyone |
| Domain | BUILTIN |
| SID | S-1-1-0 |

**Total Entries:** 6 **Mapped Entries:** 6

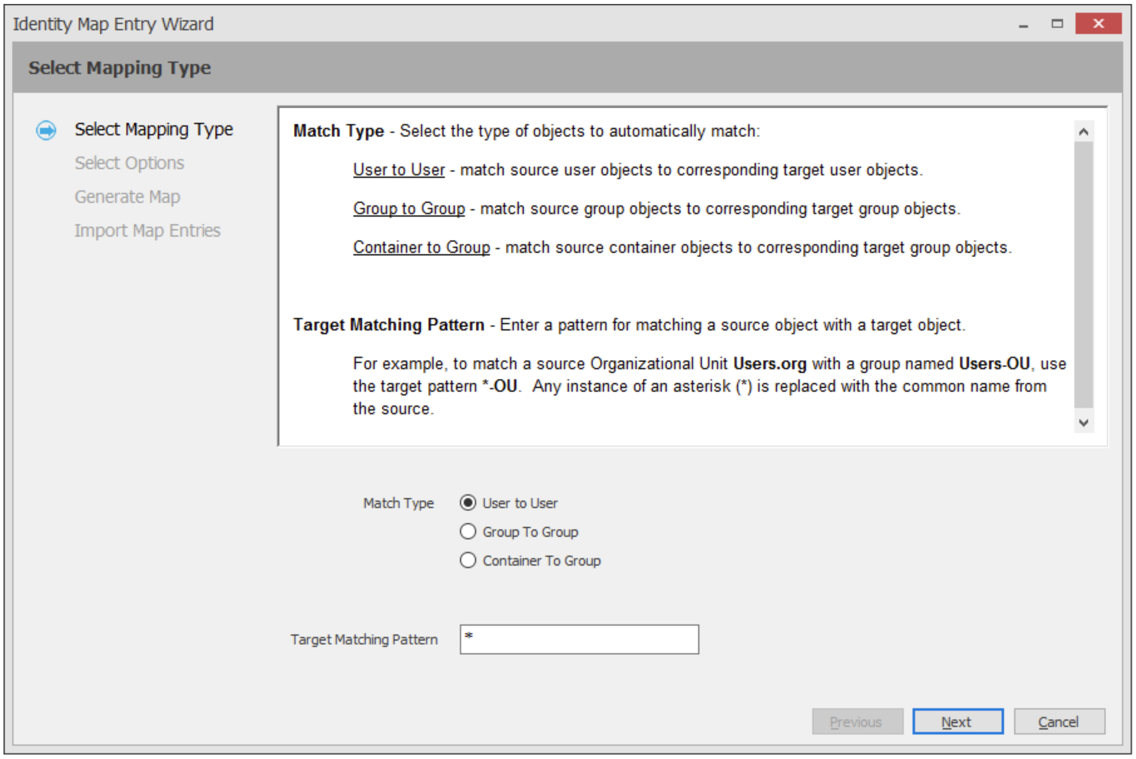
8 Click **Apply** to save the updated identity map.

9 (Conditional) If you have additional users to import from another delimited text CSV file, select the new CSV file and repeat the procedures in this section.

10 (Conditional) If you need to add additional users that were not listed in the CSV file, proceed to "Creating Object Associations" on page 138.

## Creating Object Associations

1 Click **Identity Map Entry Wizard**.



**Match Type** - Select the type of objects to automatically match:

User to User - match source user objects to corresponding target user objects.

Group to Group - match source group objects to corresponding target group objects.

Container to Group - match source container objects to corresponding target group objects.

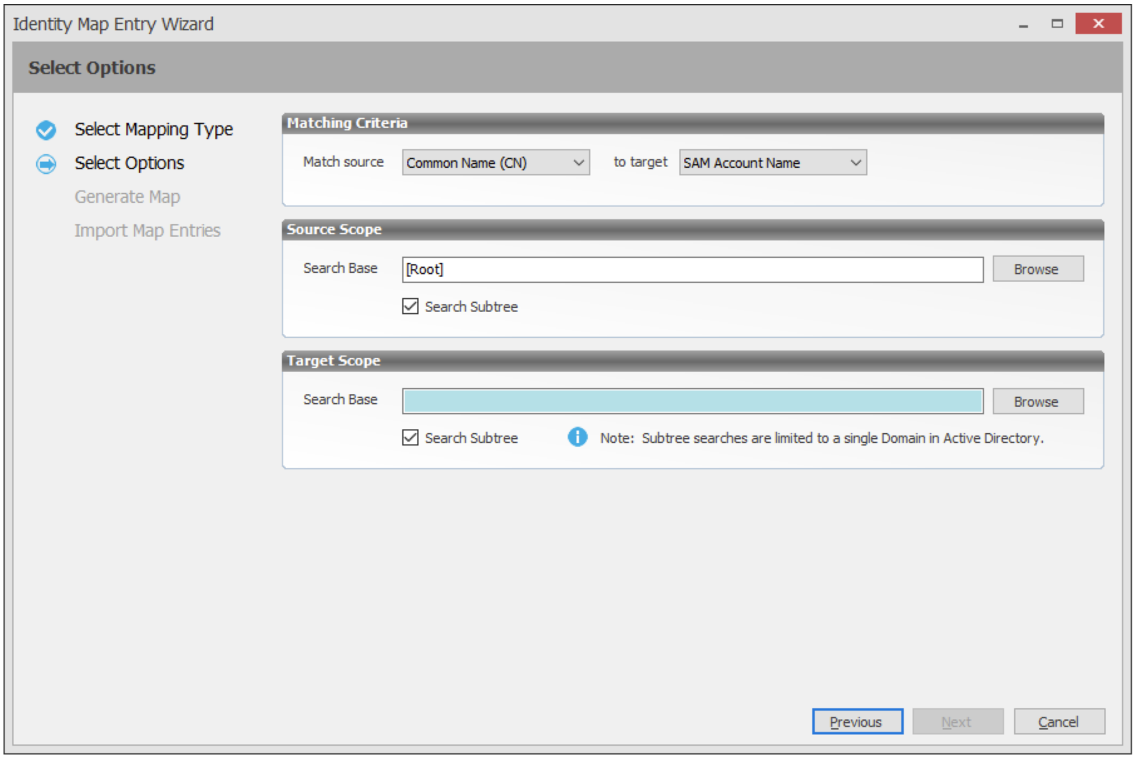
**Target Matching Pattern** - Enter a pattern for matching a source object with a target object.

For example, to match a source Organizational Unit **Users.org** with a group named **Users-OU**, use the target pattern ***-OU**. Any instance of an asterisk (*) is replaced with the common name from the source.

Match Type ● User to User ○ Group To Group ○ Container To Group

Target Matching Pattern *

2 Leave the **User to User** option selected and click **Next**.



Matching Criteria

Match source: Common Name (CN) to target: SAM Account Name

Source Scope

Search Base: [Root]

☑ Search Subtree

Target Scope

Search Base:

☑ Search Subtree

Note: Subtree searches are limited to a single Domain in Active Directory.

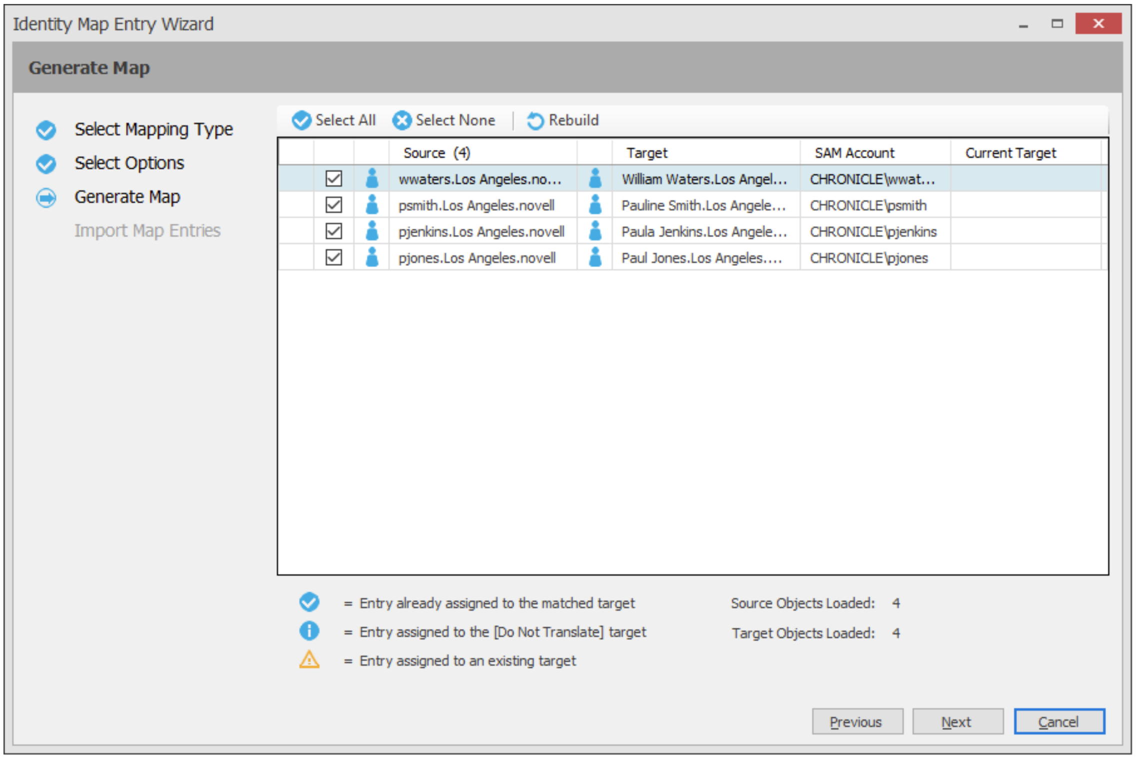
3 In the **Matching Criteria** region of the page, use the **target** drop-down menu to specify if the target accounts to locate are SAM accounts or Common Name (CN) accounts.

If you need to match using both account types on your target server, you can choose one option now and then run the wizard again and choose the other option. You might need to run the wizard multiple times in order to add all of the users, groups, and containers to the identity map.

4 In the **Source Scope** region, browse to and select the source container with the users you want included in the identity map.

5 In the **Target Scope** region, browse to and select the target container with the users you want included in the identity map.

6 Click **Next**.



|  |  |  | Source (4) |  | Target | SAM Account | Current Target |
|---|---|---|---|---|---|---|---|
|  | ☑ |  | wwaters.Los Angeles.no... |  | William Waters.Los Angel... | CHRONICLE\wwat... |  |
|  | ☑ |  | psmith.Los Angeles.novell |  | Pauline Smith.Los Angele... | CHRONICLE\psmith |  |
|  | ☑ |  | pjenkins.Los Angeles.novell |  | Paula Jenkins.Los Angele... | CHRONICLE\pjenkins |  |
|  | ☑ |  | pjones.Los Angeles.novell |  | Paul Jones.Los Angeles.... | CHRONICLE\pjones |  |

✓ = Entry already assigned to the matched target

ⓘ = Entry assigned to the [Do Not Translate] target

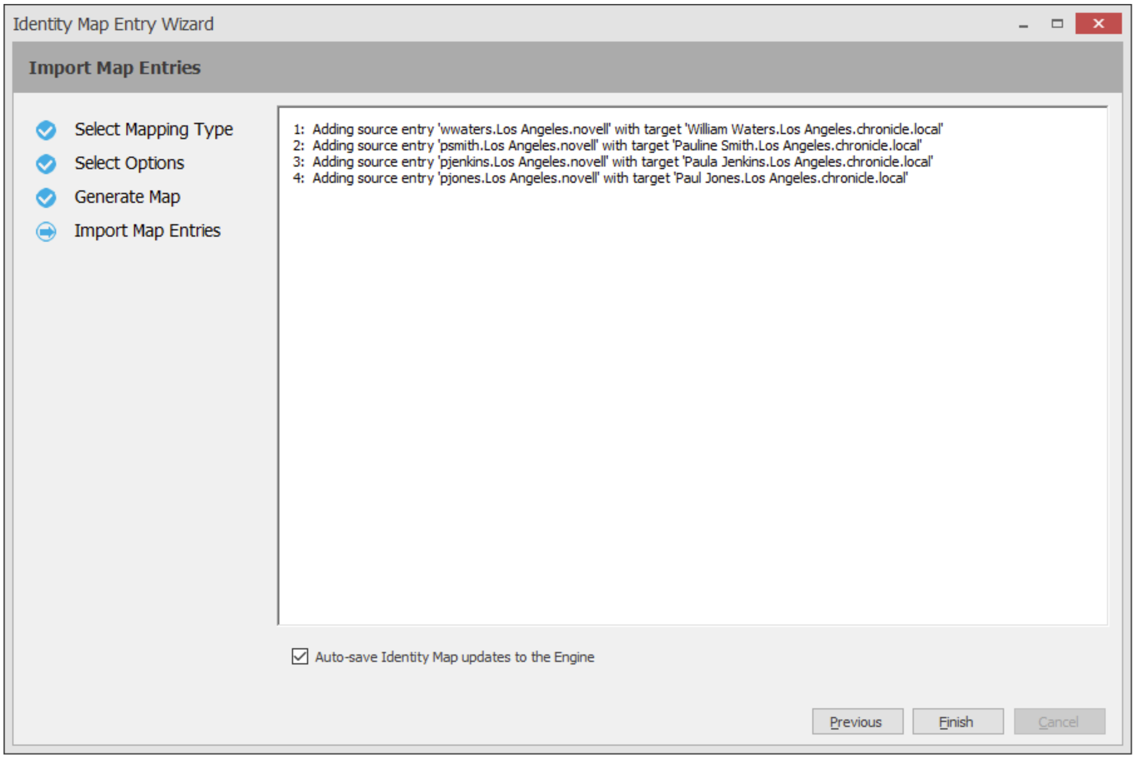
⚠ = Entry assigned to an existing target

Source Objects Loaded: 4

Target Objects Loaded: 4

7 (Conditional) Deselect any names you do not want appended to the identity map file.

8 Click **Next**.

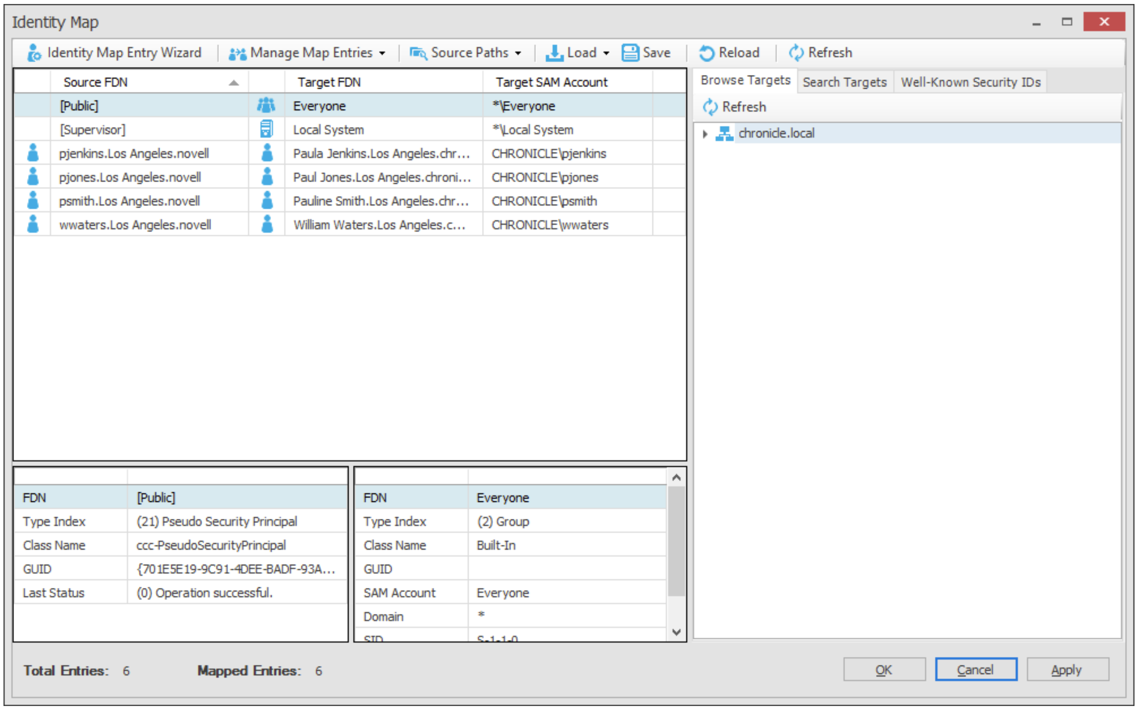


```
1:  Adding source entry 'wwaters.Los Angeles.novell' with target 'William Waters.Los Angeles.chronicle.local'
2:  Adding source entry 'psmith.Los Angeles.novell' with target 'Pauline Smith.Los Angeles.chronicle.local'
3:  Adding source entry 'pjenkins.Los Angeles.novell' with target 'Paula Jenkins.Los Angeles.chronicle.local'
4:  Adding source entry 'pjones.Los Angeles.novell' with target 'Paul Jones.Los Angeles.chronicle.local'
```

☑ Auto-save Identity Map updates to the Engine

9 Click **Finish**.

The identity map is appended with the new entries.



| Source FDN | Target FDN | Target SAM Account |
|---|---|---|
| [Public] | Everyone | *\Everyone |
| [Supervisor] | Local System | *\Local System |
| pjenkins.Los Angeles.novell | Paula Jenkins.Los Angeles.chr… | CHRONICLE\pjenkins |
| pjones.Los Angeles.novell | Paul Jones.Los Angeles.chroni… | CHRONICLE\pjones |
| psmith.Los Angeles.novell | Pauline Smith.Los Angeles.chr… | CHRONICLE\psmith |
| wwaters.Los Angeles.novell | William Waters.Los Angeles.c… | CHRONICLE\wwaters |

| FDN | [Public] |
|---|---|
| Type Index | (21) Pseudo Security Principal |
| Class Name | ccc-PseudoSecurityPrincipal |
| GUID | {701E5E19-9C91-4DEE-BADF-93A… |
| Last Status | (0) Operation successful. |

| FDN | Everyone |
|---|---|
| Type Index | (2) Group |
| Class Name | Built-In |
| GUID | |
| SAM Account | Everyone |
| Domain | * |
| SID | S-1-1-0 |

Total Entries: 6 Mapped Entries: 6

10 Click **OK** to save the updated identity map.

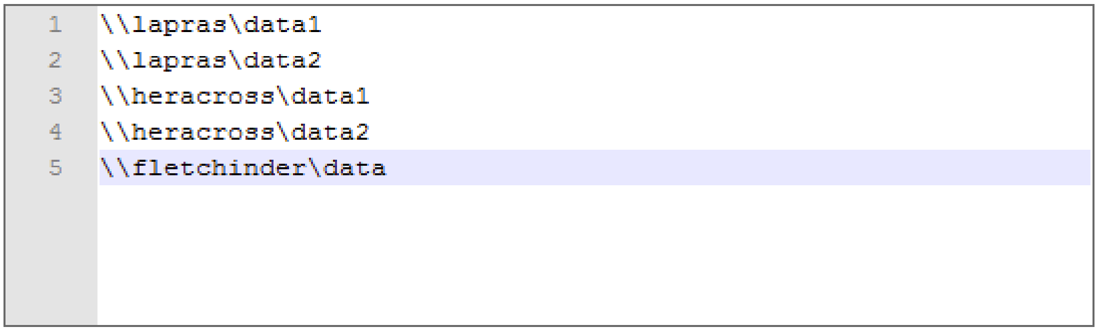
11 Repeat Step 4 and Step 5 and select the account type you did not select previously.

12 Repeat Step 6 through Step 10.

## 10.5.2 Importing a Source Path List

Depending on the size of your network, you might need to specify a significant number of different source paths as you build your identity map. You can easily import a list of your UNC paths from a text file so that these paths are accessible from a drop-down menu. Additionally, the search is filtered so that it can locate the specific UNC path as you type.

1 Using a text editor, create a file with UNC paths for each server and volume that you want to import, then save the file.



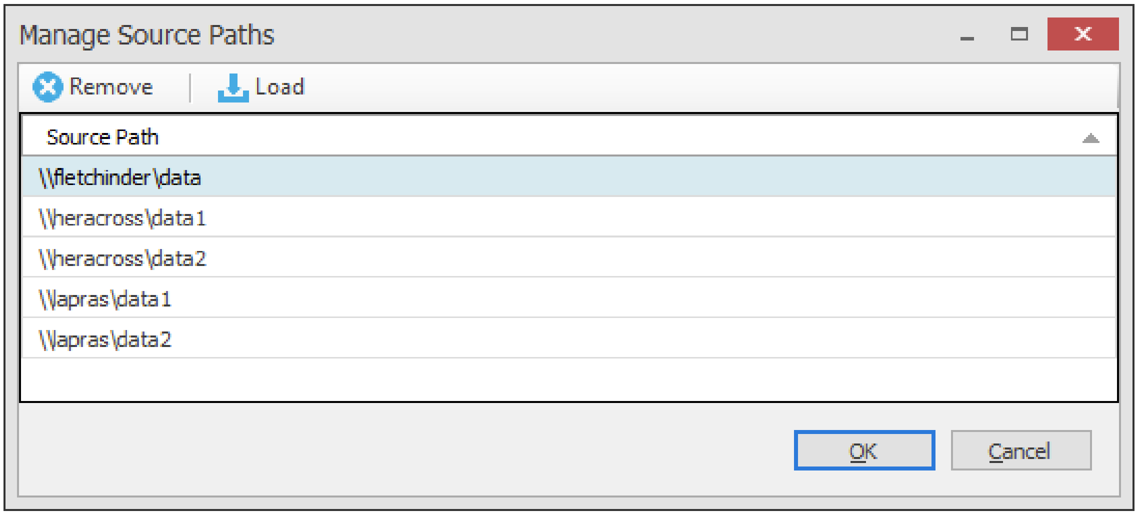
```
\\lapras\data1
\\lapras\data2
\\heracross\data1
\\heracross\data2
\\fletchinder\data
```

2 In SMAdmin, click the **Home** tab.

3 Click **Cross-Empire Data Migrations** > **eDirectory to Active Directory.**

4 Select **Source Management** > **Source Path Cache**.

5 Click **Load**, browse to and select the text file, then click **Open**.



| Source Path |
|---|
| \\fletchinder\data |
| \\heracross\data1 |
| \\heracross\data2 |
| \\lapras\data1 |
| \\lapras\data2 |

6 Click **OK**.

### 10.5.3 Adding Source Entries to the Identity Map

Once the identity map has been created, you can add new users or groups at any time.

1 In SMAdmin, click the **Home** tab.

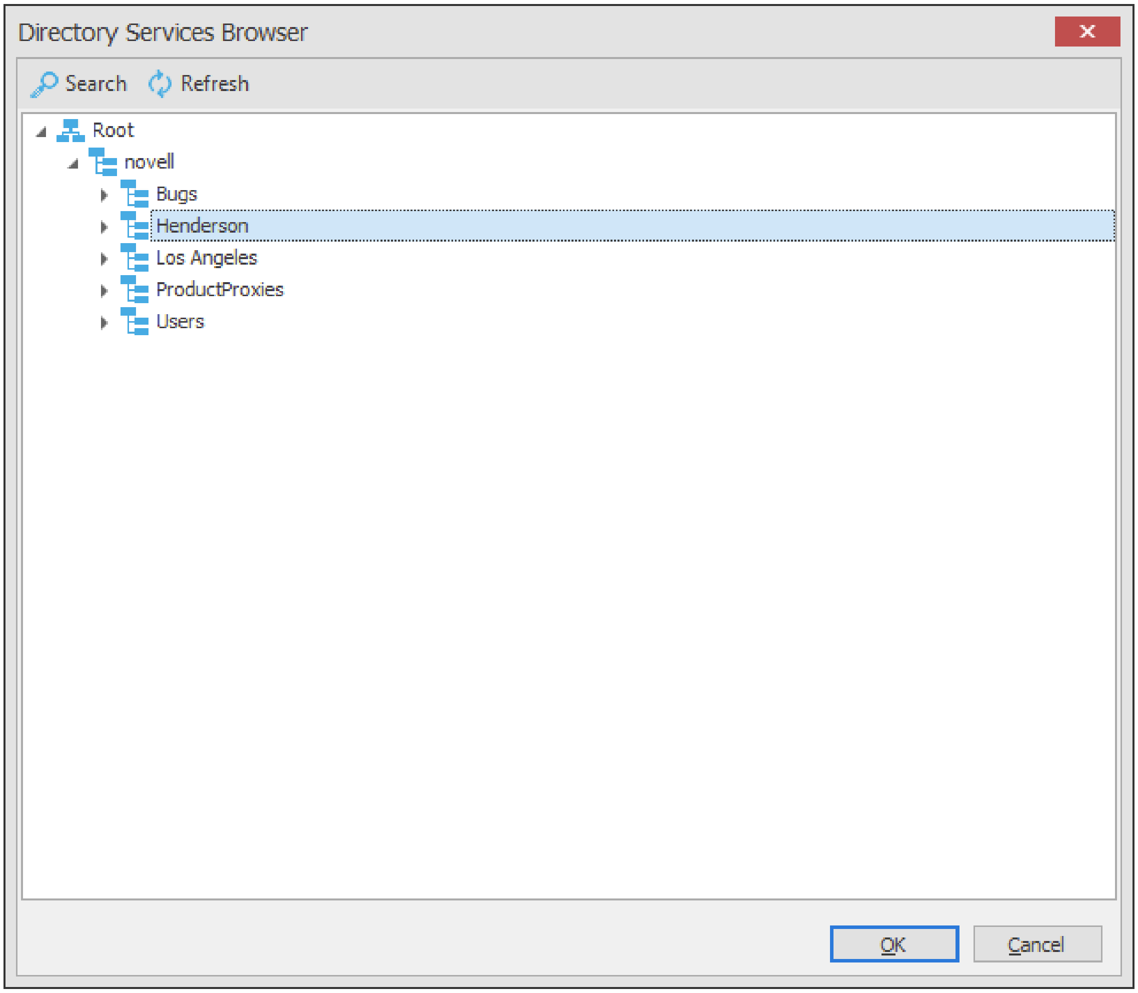
2 Select **Cross-Empire Data Migrations** > **eDirectory to Active Directory**.

3 Select **Identity Map Management** > **Edit Identity Map**.

4 Select **Manage Map Entries** > **Add Source Entries**.

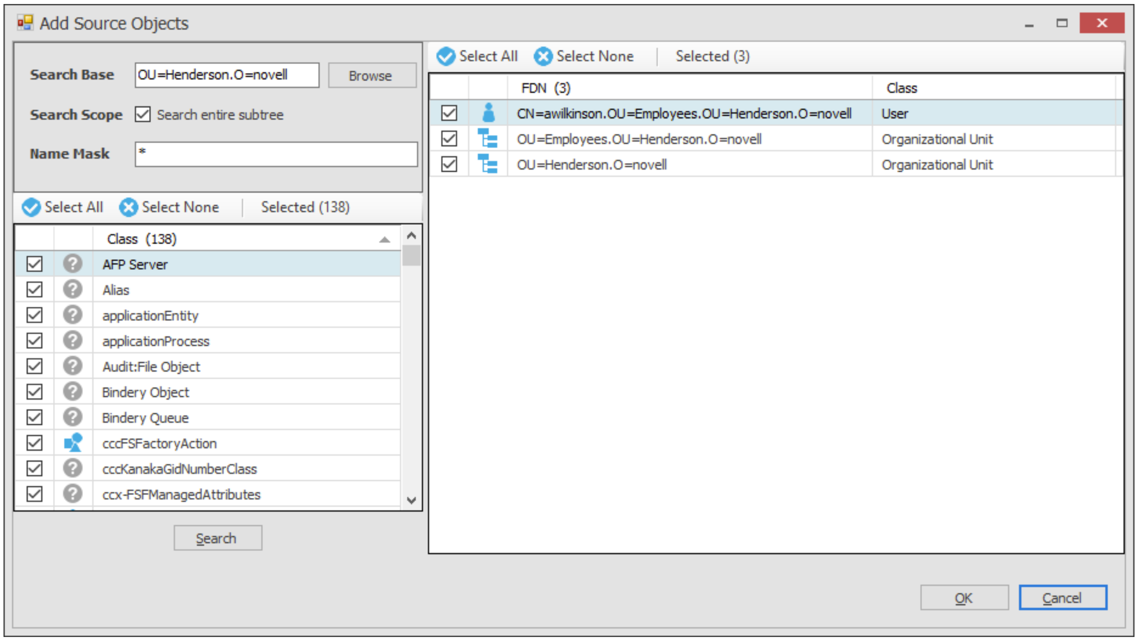
5 In the Add Source Objects page, use the **Search Base**, **Browse** button, **Search Scope**, and **Name Mask** fields to locate and select the container you want to use for your search.

If you wish to limit your search to a selected set of object types, under the **Class** heading, deselect those object types you do not want included in the search.



6 Click **OK**.

7 On the Add Source Object page, click **Search**.



Search Base: OU=Henderson.O=novell

Search Scope: ☑ Search entire subtree

Name Mask: *

Selected (138)

| | | Class (138) |
|---|---|---|
| ☑ | ? | AFP Server |
| ☑ | ? | Alias |
| ☑ | ? | applicationEntity |
| ☑ | ? | applicationProcess |
| ☑ | ? | Audit:File Object |
| ☑ | ? | Bindery Object |
| ☑ | ? | Bindery Queue |
| ☑ | | cccFSFactoryAction |
| ☑ | ? | cccKanakaGidNumberClass |
| ☑ | ? | ccx-FSFManagedAttributes |

Selected (3)

| | | FDN (3) | Class |
|---|---|---|---|
| ☑ | | CN=awilkinson.OU=Employees.OU=Henderson.O=novell | User |
| ☑ | | OU=Employees.OU=Henderson.O=novell | Organizational Unit |
| ☑ | | OU=Henderson.O=novell | Organizational Unit |

By default, all located objects are selected.

8 Deselect the objects you do not want to append to the identity map.

9 Click **OK**.

## 10.5.4 Adding or Modifying Target Entries to the Identity Map

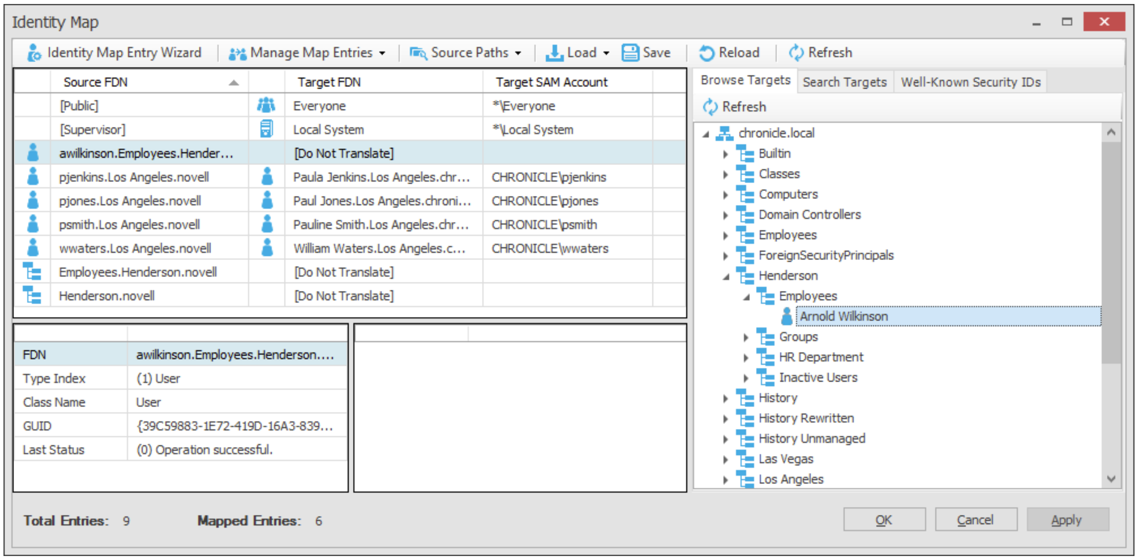
1 In SMAdmin, click the **Home** tab.

2 Select **Cross-Empire Data Migrations** > **eDirectory to Active Directory**.

3 Select **Identity Map Management** > **Edit Identity Map**.

4 In the Identity Map page, select the listing for the source entry to which you want to add a target or that you want to modify.

5 Use one of the tabs in the right panel of the Identity Map page to locate and select the desired target.



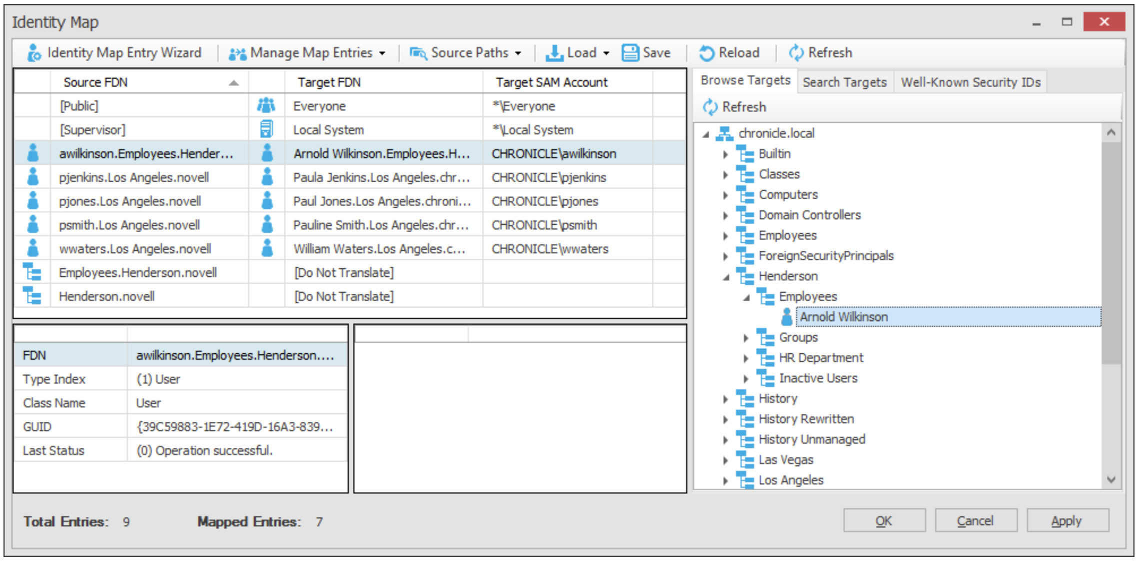
| Source FDN | Target FDN | Target SAM Account |
|---|---|---|
| [Public] | Everyone | *\Everyone |
| [Supervisor] | Local System | *\Local System |
| awilkinson.Employees.Hender… | [Do Not Translate] | |
| pjenkins.Los Angeles.novell | Paula Jenkins.Los Angeles.chr… | CHRONICLE\pjenkins |
| pjones.Los Angeles.novell | Paul Jones.Los Angeles.chroni… | CHRONICLE\pjones |
| psmith.Los Angeles.novell | Pauline Smith.Los Angeles.chr… | CHRONICLE\psmith |
| wwaters.Los Angeles.novell | William Waters.Los Angeles.c… | CHRONICLE\wwaters |
| Employees.Henderson.novell | [Do Not Translate] | |
| Henderson.novell | [Do Not Translate] | |

| | |
|---|---|
| FDN | awilkinson.Employees.Henderson.… |
| Type Index | (1) User |
| Class Name | User |
| GUID | {39C59883-1E72-419D-16A3-839… |
| Last Status | (0) Operation successful. |

**Total Entries:** 9 **Mapped Entries:** 6

6 Specify the object as the new target object.

For example, if you were using the **Browse Targets** tab in the example above, you could right-click or drag the object to place it in the **Target SAM Account** field of the selected source object.



| Source FDN | Target FDN | Target SAM Account |
|---|---|---|
| [Public] | Everyone | *\Everyone |
| [Supervisor] | Local System | *\Local System |
| awilkinson.Employees.Hender... | Arnold Wilkinson.Employees.H... | CHRONICLE\awilkinson |
| pjenkins.Los Angeles.novell | Paula Jenkins.Los Angeles.chr... | CHRONICLE\pjenkins |
| pjones.Los Angeles.novell | Paul Jones.Los Angeles.chroni... | CHRONICLE\pjones |
| psmith.Los Angeles.novell | Pauline Smith.Los Angeles.chr... | CHRONICLE\psmith |
| wwaters.Los Angeles.novell | William Waters.Los Angeles.c... | CHRONICLE\wwaters |
| Employees.Henderson.novell | [Do Not Translate] | |
| Henderson.novell | [Do Not Translate] | |

| | |
|---|---|
| FDN | awilkinson.Employees.Henderson.... |
| Type Index | (1) User |
| Class Name | User |
| GUID | {39C59883-1E72-419D-16A3-839... |
| Last Status | (0) Operation successful. |

**Total Entries:** 9 **Mapped Entries:** 7

7 Click **Apply** to save the modified identity map.

## 10.5.5 Saving a Local Instance of the Identity Map

When working with identity maps, you might find that you want to experiment with different associations. In such cases, you should have multiple identity maps. To save an identity map that differs from the original, you must save it locally.

1 Click **Save**.

2 Save the XML formatted identity map file to a location you prefer.

## 10.5.6 Loading a Saved Identity Map

This action retrieves saved versions of identity maps.

1 Select **Load** > **Import Identity Map File**.

2 Select the file, then click **Open**.

## 10.5.7 Generating a Migration Preview Report

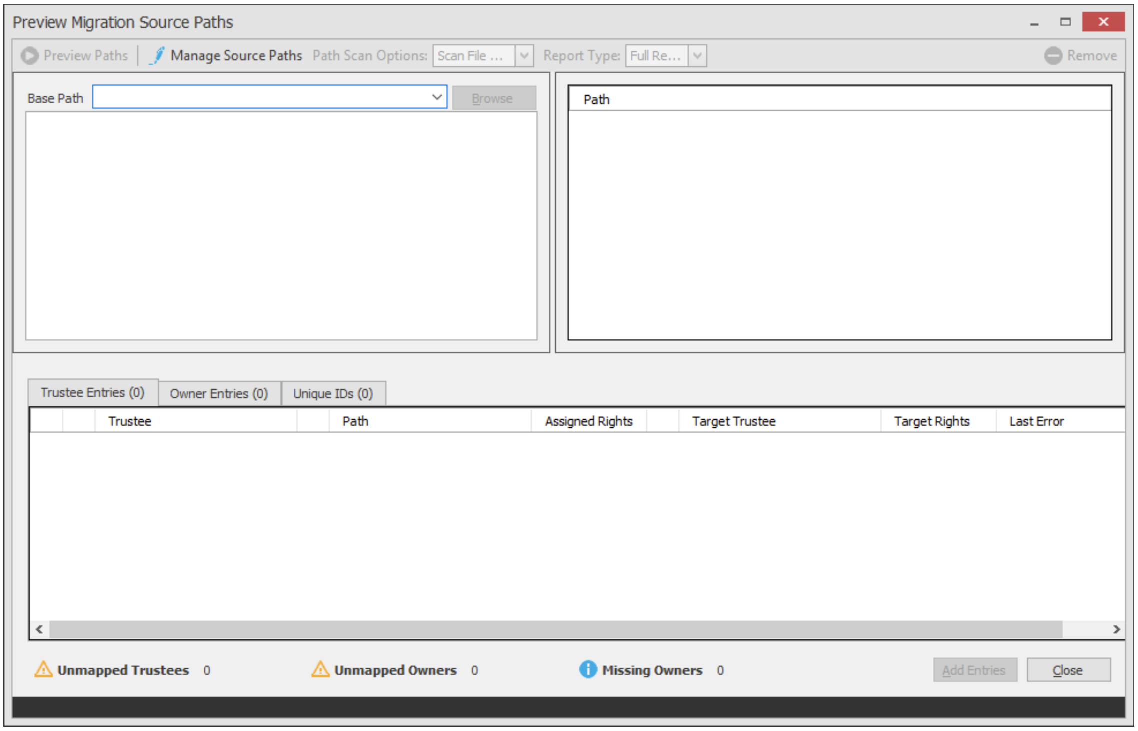
Before performing a Cross-Empire Data Migration, you should generate a preview report. The report indicates any concerns that might need to be addressed such as objects which have file rights but which have not yet been mapped in the identity map.

The preview report uses your identity map, and searches file and folder rights assignments and ownership of the actual data which you will be migrating to indicate which objects actually have ownership or rights, and if an object is mapped in the identity map.

1 In SMAdmin, click the **Home** tab.

2 Select **Cross-Empire Data Migrations** > **eDirectory to Active Directory**.

3 Select **Source Paths** > **Generate Preview Report**.



4 In the **Base Path** field, specify an initial UNC path for a server and volume to browse.

For example, `\\server_name\volume_name\ or \\ip_address\volume_name`.

After you enter a path, you can click the **Browse** button to browse to the folder you want, such as the `Users` folder.

5 Drag the selected folder to the **Path** pane.

6 From the **Path Scan Options** drop-down menu, choose one of the following:

- **Scan Folders Only**: Select this option to view the trustee assignments and owners of folders.
- **Scan File Owners**: Select this option to view the trustee assignments and owners of folders, along with the owners of files.
- **Scan File Owners and Trustees**: Select this option to view the trustee assignments and owners of folders, as well as the trustee assignments and owners of files.

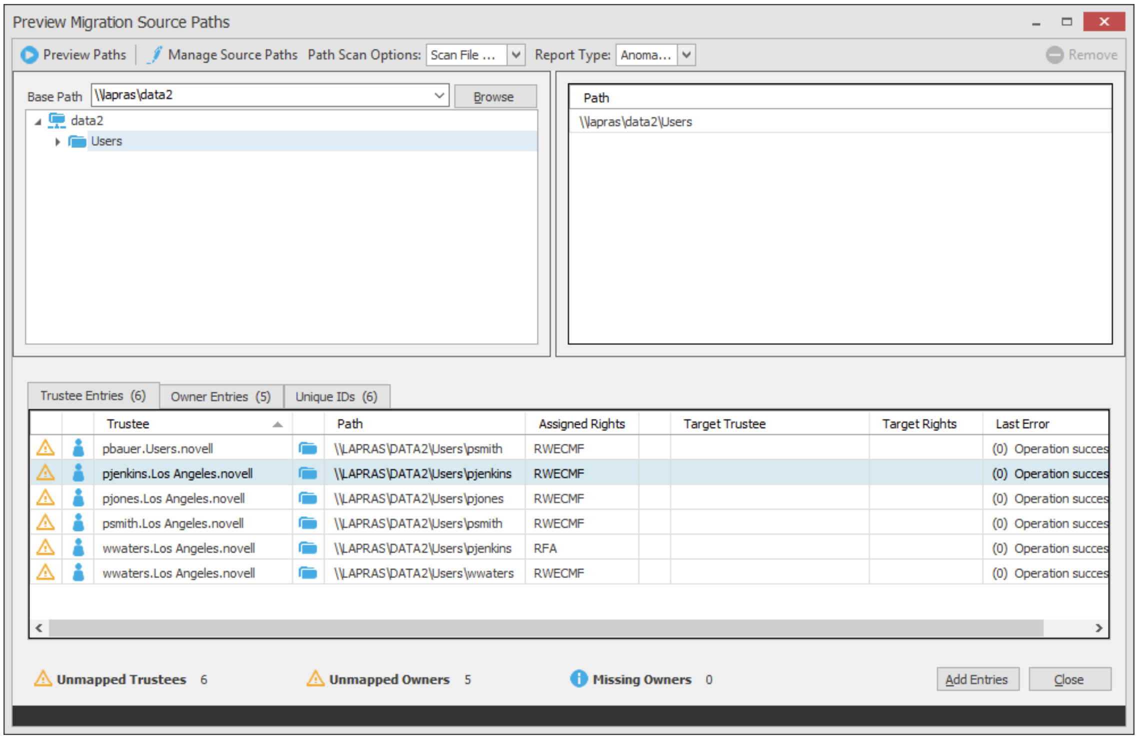
  Depending on the number of files and folders on your Novell or Micro Focus network, the **Scan File Owners and Trustees** option can take a significant amount of time to generate. We recommend using one of the other options first.

7 From the **Report Type** drop-down menu, choose one of the following:

- **Anomaly Report**: Depending on which of the **File Scan Options** is selected, this generates a report of all of the folders and files that have trustees or owners that are *not* mapped to a target object in the identity map.
- **Full Report**: Depending on which of the **File Scan Options** are selected, this generates a report of all of the folders and files, along with their corresponding owners and trustees, and indicates whether they are mapped to a target object in the identity map or not.

  Depending on the number of files and folders on your Novell or Micro Focus network, generating a full report can take a significant amount of time. We recommend generating an Anomaly report instead.

8 Click **Preview Paths**.



Path Scan Options: Scan File ...

Report Type: Anoma...

Base Path: \\lapras\data2

data2
Users

Path
\\lapras\data2\Users

Trustee Entries (6) | Owner Entries (5) | Unique IDs (6)

| | Trustee | Path | Assigned Rights | Target Trustee | Target Rights | Last Error |
|---|---|---|---|---|---|---|
| ⚠ | pbauer.Users.novell | \\LAPRAS\DATA2\Users\psmith | RWECMF | | | (0) Operation succes |
| ⚠ | pjenkins.Los Angeles.novell | \\LAPRAS\DATA2\Users\pjenkins | RWECMF | | | (0) Operation succes |
| ⚠ | pjones.Los Angeles.novell | \\LAPRAS\DATA2\Users\pjones | RWECMF | | | (0) Operation succes |
| ⚠ | psmith.Los Angeles.novell | \\LAPRAS\DATA2\Users\psmith | RWECMF | | | (0) Operation succes |
| ⚠ | wwaters.Los Angeles.novell | \\LAPRAS\DATA2\Users\pjenkins | RFA | | | (0) Operation succes |
| ⚠ | wwaters.Los Angeles.novell | \\LAPRAS\DATA2\Users\wwaters | RWECMF | | | (0) Operation succes |

⚠ Unmapped Trustees 6 ⚠ Unmapped Owners 5 ℹ Missing Owners 0

9 Use the tabbed reports to preview targets according to trustees, owners, and unique IDs.

For example, in the graphic above, the **Trustee Entries** tab displays the source IDs that have a trustee assignment to a folder but a target ID has not yet been created in the identity map.

The **Owner Entries** tab displays owners of files and folders that do not have a corresponding target in the identity map.

The **Unique IDs** tab displays a single entry for each ID that is mapped in the identity report.

10 Click **Add Entries** to add the entries to the identity map.

The entries are added to the identity map and you can now add target entries by following the procedures in Section 10.5.4, “Adding or Modifying Target Entries to the Identity Map,” on page 144.

### 10.5.8 Adding Entries from Preview Reports

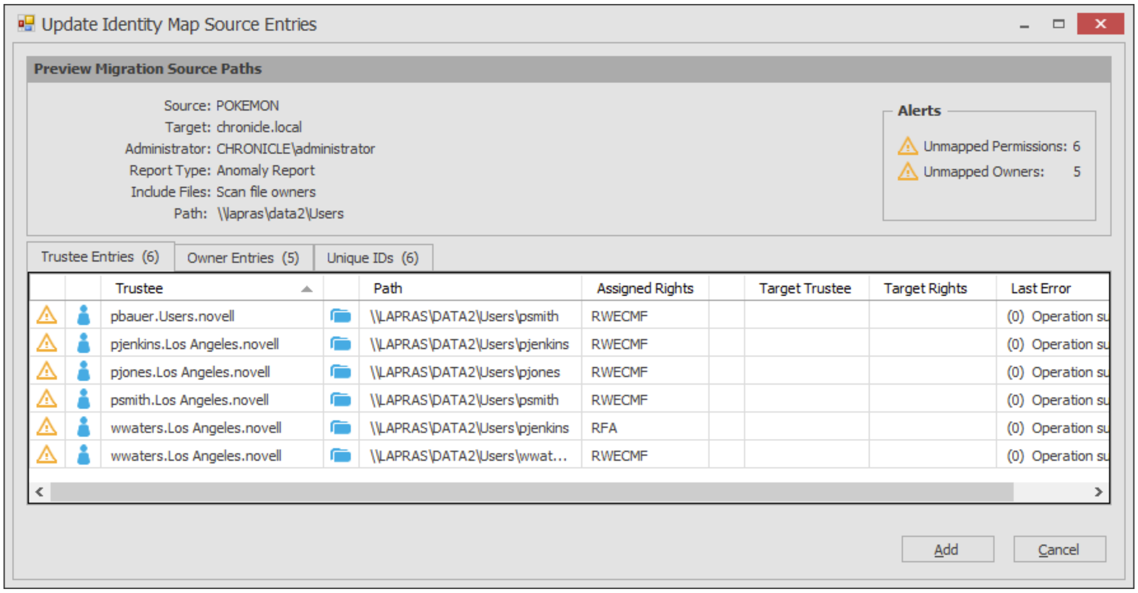
In Step 10 on page 147, you added entries to the identity map by using the Preview Migration Source Path page’s **Add Entries** button. You can also use the **Add Entries from Preview Report** option to retrieve any preview report that you have generated for the directory tree you are working with, and add those entries to the identity map.

1 In SMAdmin, click the **Home** tab.

2 Select **Cross-Empire Data Migrations** > **eDirectory to Active Directory**.

3 Select **Source Paths** > **Add Entries from Preview Report**.

4 From the Browse Migration Preview Reports dialog box, select the preview report you want to add, then click **OK**.



Update Identity Map Source Entries

**Preview Migration Source Paths**

Source: POKEMON
Target: chronicle.local
Administrator: CHRONICLE\administrator
Report Type: Anomaly Report
Include Files: Scan file owners
Path: \\lapras\data2\Users

**Alerts**

⚠ Unmapped Permissions: 6
⚠ Unmapped Owners: 5

Trustee Entries (6) | Owner Entries (5) | Unique IDs (6)

| | Trustee | Path | Assigned Rights | Target Trustee | Target Rights | Last Error |
|---|---|---|---|---|---|---|
| ⚠ | pbauer.Users.novell | \\LAPRAS\DATA2\Users\psmith | RWECMF | | | (0) Operation su |
| ⚠ | pjenkins.Los Angeles.novell | \\LAPRAS\DATA2\Users\pjenkins | RWECMF | | | (0) Operation su |
| ⚠ | pjones.Los Angeles.novell | \\LAPRAS\DATA2\Users\pjones | RWECMF | | | (0) Operation su |
| ⚠ | psmith.Los Angeles.novell | \\LAPRAS\DATA2\Users\psmith | RWECMF | | | (0) Operation su |
| ⚠ | wwaters.Los Angeles.novell | \\LAPRAS\DATA2\Users\pjenkins | RFA | | | (0) Operation su |
| ⚠ | wwaters.Los Angeles.novell | \\LAPRAS\DATA2\Users\wwat... | RWECMF | | | (0) Operation su |

At this point, you can view the preview report according to the tabbed options.

5 Click **Add** to add the entries to the identity map.

The entries are added to the identity map and you can now add target entries to each by following the procedures under Section 10.5.4, “Adding or Modifying Target Entries to the Identity Map,” on page 144.

## 10.5.9 Review Rights and Trustee Assignment Mappings

Despite the inherent differences in rights, trustee assignments, and permissions between Novell or Micro Focus and Microsoft networks, the Cross-Empire Data Migration subsystem of Storage Manager for Active Directory does its best to match the Novell or Micro Focus rights and trustee assignments with the equivalent Microsoft permissions and advanced permissions.

When you generate a Preview Report, you should pay particular attention to the actual rights in the **Assigned Rights** column and the proposed file and folder rights listed in the **Target Rights** column.

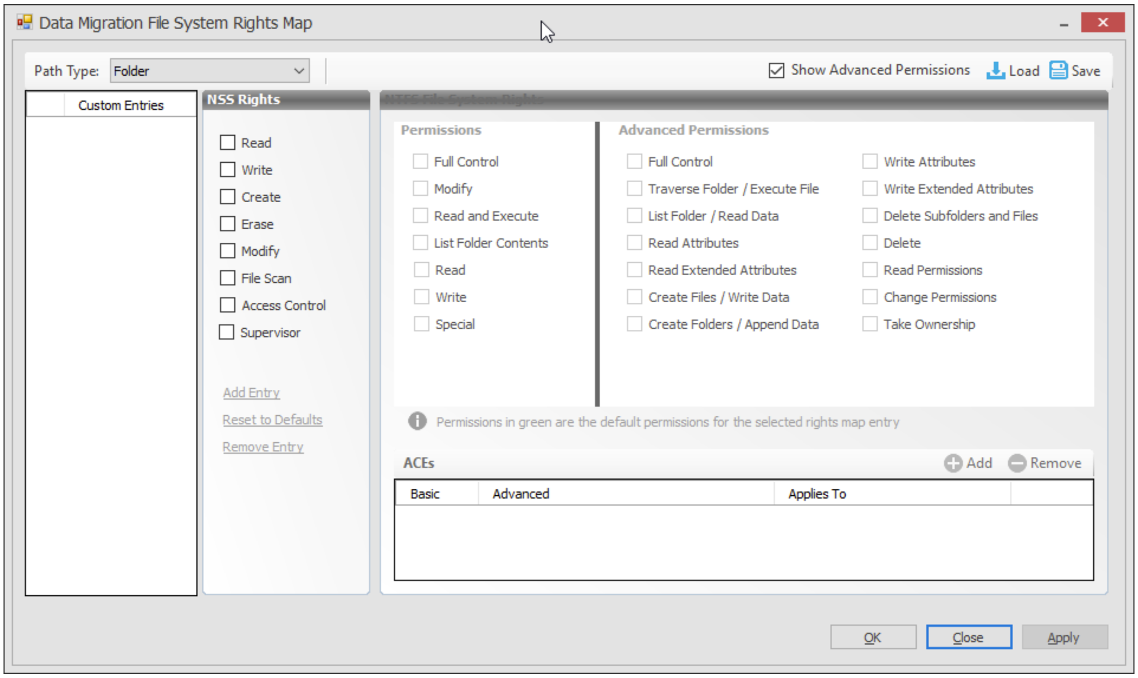
You can modify the rights mappings by using the File System Rights Map. When you do this, you specify a mapping between one particular set of rights on the Novell or Micro Focus servers to one particular set of rights on the Microsoft Windows servers. As an example, the default mapping is to map the Novell or Micro Focus NSS rights RWECMF to the Windows NTFS rights MELRW. As a further example, perhaps when files have this set of rights you do not want to grant the E (erase) right to files on the target. You could modify the mapping using the procedures below to change the mapping of Novell or Micro Focus NSS rights RWECMF to the Windows NTFS rights MLRW. When you do this, you change the mapping for every file that has that exact set of rights, but it does not change the E mapping in any other set of rights. For instance, if you had trustees that had RWCEF, that mapping would not be changed because you changed the mapping for RWCEMF.

To view or modify these rights:

1 In SMAdmin, click the **Home** tab.

2 Select **Cross-Empire Data Migrations** > **eDirectory to Active Directory.**

3 Select **Identity Map Management** > **File System Rights Map**.



Path Type: Folder

☑ Show Advanced Permissions

NSS Rights: □ Read □ Write □ Create □ Erase □ Modify □ File Scan □ Access Control □ Supervisor

Permissions: □ Full Control □ Modify □ Read and Execute □ List Folder Contents □ Read □ Write □ Special

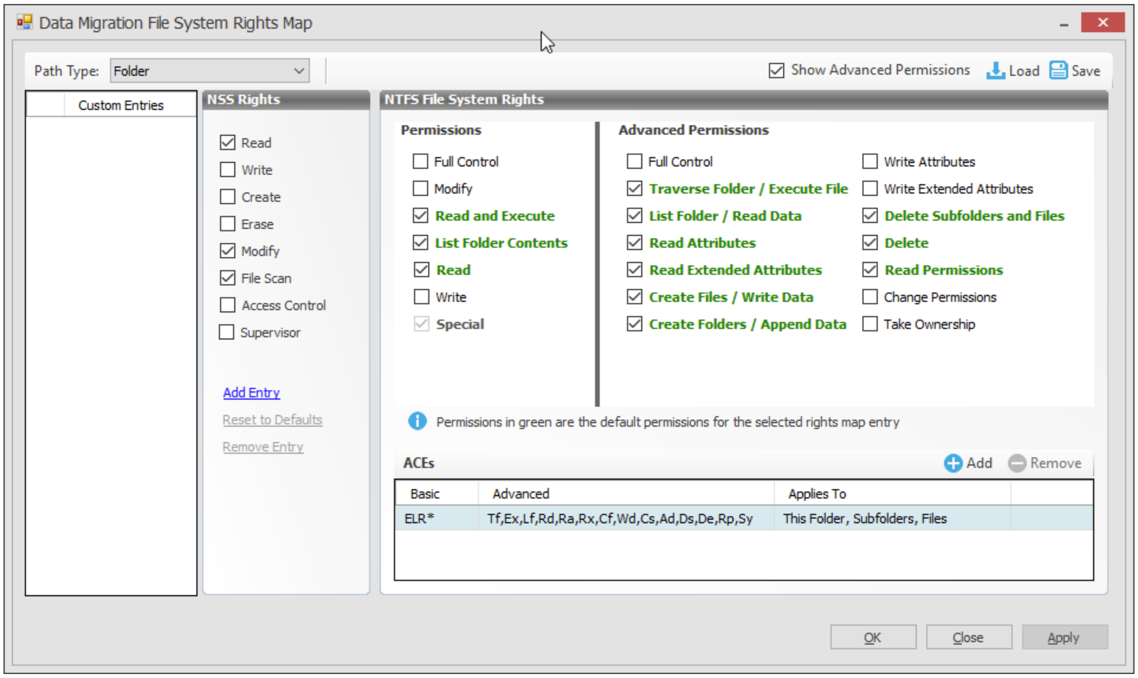
Advanced Permissions: □ Full Control □ Traverse Folder / Execute File □ List Folder / Read Data □ Read Attributes □ Read Extended Attributes □ Create Files / Write Data □ Create Folders / Append Data □ Write Attributes □ Write Extended Attributes □ Delete Subfolders and Files □ Delete □ Read Permissions □ Change Permissions □ Take Ownership

Permissions in green are the default permissions for the selected rights map entry

ACEs

| Basic | Advanced | Applies To |
|---|---|---|

4 In the **NSS Rights** column, click the rights to see the equivalent NTFS permissions and advanced permissions.



Path Type: Folder

☑ Show Advanced Permissions

NSS Rights: ☑ Read □ Write □ Create □ Erase ☑ Modify ☑ File Scan □ Access Control □ Supervisor

Permissions: □ Full Control □ Modify ☑ Read and Execute ☑ List Folder Contents ☑ Read □ Write ☑ Special

Advanced Permissions: □ Full Control ☑ Traverse Folder / Execute File ☑ List Folder / Read Data ☑ Read Attributes ☑ Read Extended Attributes ☑ Create Files / Write Data ☑ Create Folders / Append Data □ Write Attributes □ Write Extended Attributes ☑ Delete Subfolders and Files ☑ Delete ☑ Read Permissions □ Change Permissions □ Take Ownership

Permissions in green are the default permissions for the selected rights map entry

ACEs

| Basic | Advanced | Applies To |
|---|---|---|
| ELR* | Tf,Ex,Lf,Rd,Ra,Rx,Cf,Wd,Cs,Ad,Ds,De,Rp,Sy | This Folder, Subfolders, Files |

The default permissions are indicated in green.

5 Select or deselect permissions as needed.

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

# 10.6 Migration Options

The Cross-Empire Data Migration subsystem of Storage Manager for Active Directory provides the following options for migration:

- Section 10.6.1, “Data and Security,” on page 150
- Section 10.6.2, “Data Only,” on page 150
- Section 10.6.3, “Security Only,” on page 150

## 10.6.1 Data and Security

This option migrates the data and the associated folder and file rights and trustee assignments specified in the identity map.

**NOTE:** The initial identity map referenced in Step 3 on page 133 does not function as an identity map until you have appended entries to it.

The procedures that begin in Section 10.8, “Performing a User to User Data Migration,” on page 151 use the Data and Security option.

## 10.6.2 Data Only

This option migrates only the data and not the associated rights and trustee assignments. After you have migrated the data, you can later go back and apply the file rights and trustee assignments to the data through the **Security Only** option.

When data is migrated by using this option, file ownership is set according to the Storage Manager policy for the migration target. If there is no policy in place, the owner is the Storage Manager proxy user in Active Directory.

In the procedures included in the remainder of this section, the **Copy Options - Rights and Ownership** page is not applicable for a Data Only migration.

## 10.6.3 Security Only

This option migrates the rights and trustee assignments of data that has already been migrated. If the data to which the trustee assignments are assigned has not been migrated, the associated rights and trustee assignments for those files or folders are not migrated.

If you attempt to use this option and you have not created an identity map, you cannot proceed.

This option is frequently used when migrating the rights and trustee assignments from a single Novell or Micro Focus source to a remote Windows Server that does not have an installed Client for OES.

# 10.7 Viewing the Migration Log File

The migration log file can be used to track the status of the migration. You can view the file by using a Windows tail program or an application such as `dbgview.exe`.

To view the log file using `dgbview.exe`, refer to the application’s documentation for configuring and viewing log file data.

Procedures for viewing the log file data using a Windows tail program follow:

1. Download a Windows tail program and install it on the Engine host or the Cross-Empire Data Migration enabled Agent tasked with the migration.

   To verify that the Agent is Cross-Empire Data Migration enabled, refer to the Agent page in SMAdmin. For more information, see Section 13.1.16, "Agents," on page 310.

2. Do one of the following:

   - If the server to which you are migrating data is running a Cross-Empire Data Migration capable Agent, or is set up to be proxied by a Cross-Empire Data Migration capable Agent, at the Agent server, use the Windows tail application to open the log file at:

     ```
     C:\ProgramData\Micro Focus\Storage Manager\Agent\log\smagent.log
     ```

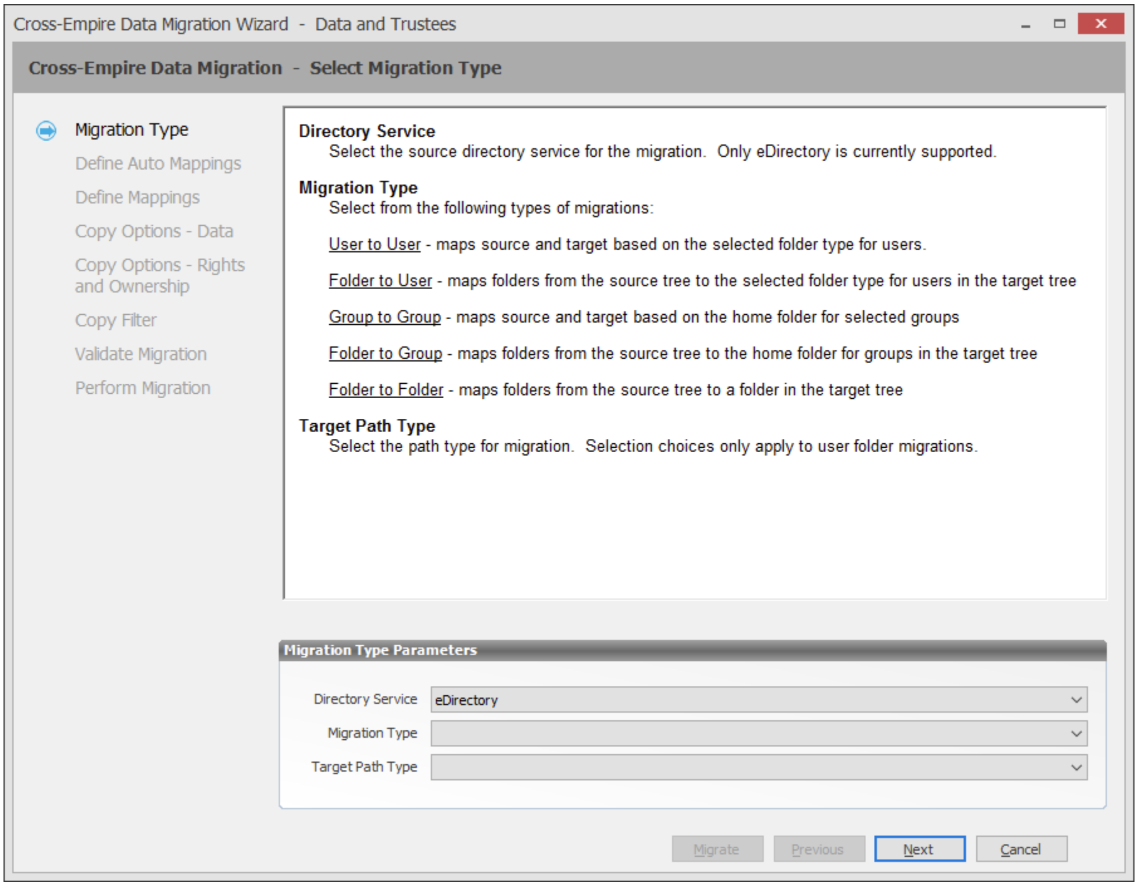
   - If the server to which you are migrating data is not running a Cross-Empire Data Migration capable Agent, and is not set up to be proxied by a Cross-Empire Data Migration capable Agent, at the Engine server, use the Windows tail application to open the log file at:

     ```
     C:\ProgramData\Micro Focus\Storage Manager\Engine\log\smengine.log
     ```

3. Refer to the log file during the migration to view the status.

## 10.8 Performing a User to User Data Migration

1. Make sure you have completed the prerequisites and have created a migration proxy account. For more information on the prerequisites, see Section 10.3, "Prerequisites," on page 130. For more information on creating a migration proxy account, see Section 10.4, "Creating the Migration Proxy Account," on page 131.
2. In SMAdmin, click the **Home** tab.
3. Select **Cross-Empire Data Migrations** > **eDirectory to Active Directory**.
4. Select **Migration Wizards** > **Data and Security**.


Cross-Empire Data Migration Wizard - Data and Trustees
Cross-Empire Data Migration - Select Migration Type
Migration Type
Define Auto Mappings
Define Mappings
Copy Options - Data
Copy Options - Rights and Ownership
Copy Filter
Validate Migration
Perform Migration
Migration Type Parameters
Migrate
Previous
Next
Cancel

**Directory Service**
Select the source directory service for the migration. Only eDirectory is currently supported.

**Migration Type**
Select from the following types of migrations:

User to User - maps source and target based on the selected folder type for users.

Folder to User - maps folders from the source tree to the selected folder type for users in the target tree

Group to Group - maps source and target based on the home folder for selected groups

Folder to Group - maps folders from the source tree to the home folder for groups in the target tree

Folder to Folder - maps folders from the source tree to a folder in the target tree

**Target Path Type**
Select the path type for migration. Selection choices only apply to user folder migrations.

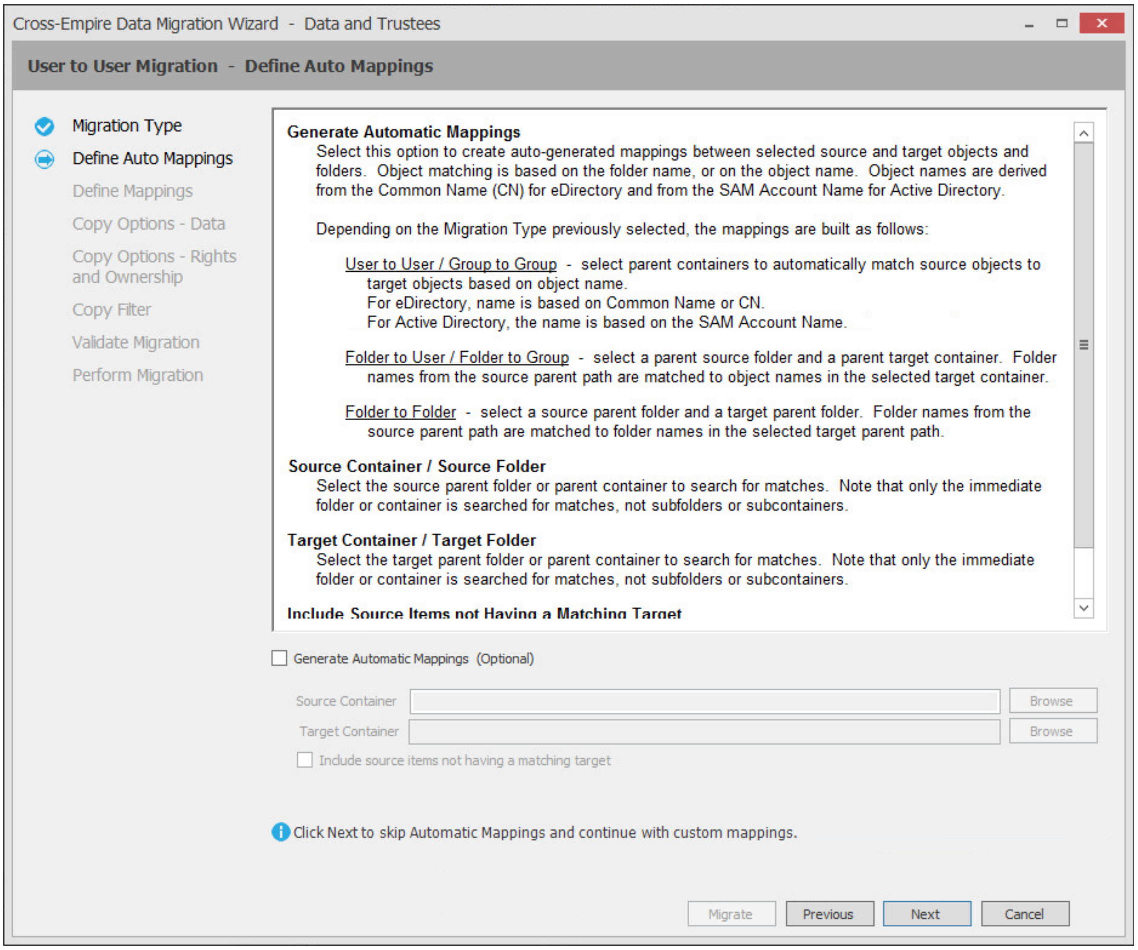
Directory Service: eDirectory
Migration Type:
Target Path Type:

5 From the **Migration Type** drop-down menu, select **User to User.**

6 From the **Target Path Type** drop-down menu, select the target path type for the data that you will migrate.

For example, if you select **Home Folder**, the data is copied to each user’s home folder path as defined in directory services.

7 Click **Next**.



User to User Migration - Define Auto Mappings

**Generate Automatic Mappings**
Select this option to create auto-generated mappings between selected source and target objects and folders. Object matching is based on the folder name, or on the object name. Object names are derived from the Common Name (CN) for eDirectory and from the SAM Account Name for Active Directory.

Depending on the Migration Type previously selected, the mappings are built as follows:

User to User / Group to Group - select parent containers to automatically match source objects to target objects based on object name.
For eDirectory, name is based on Common Name or CN.
For Active Directory, the name is based on the SAM Account Name.

Folder to User / Folder to Group - select a parent source folder and a parent target container. Folder names from the source parent path are matched to object names in the selected target container.

Folder to Folder - select a source parent folder and a target parent folder. Folder names from the source parent path are matched to folder names in the selected target parent path.

**Source Container / Source Folder**
Select the source parent folder or parent container to search for matches. Note that only the immediate folder or container is searched for matches, not subfolders or subcontainers.

**Target Container / Target Folder**
Select the target parent folder or parent container to search for matches. Note that only the immediate folder or container is searched for matches, not subfolders or subcontainers.

**Include Source Items not Having a Matching Target**

□ Generate Automatic Mappings (Optional)

Source Container

Target Container

□ Include source items not having a matching target

Click Next to skip Automatic Mappings and continue with custom mappings.

8 Do one of the following:

- Fill in the following fields:

  **Generate Automatic Mappings:** If you are migrating a large number of users, select this check box to activate the other fields.

  **Source Container:** Browse to select the source container.

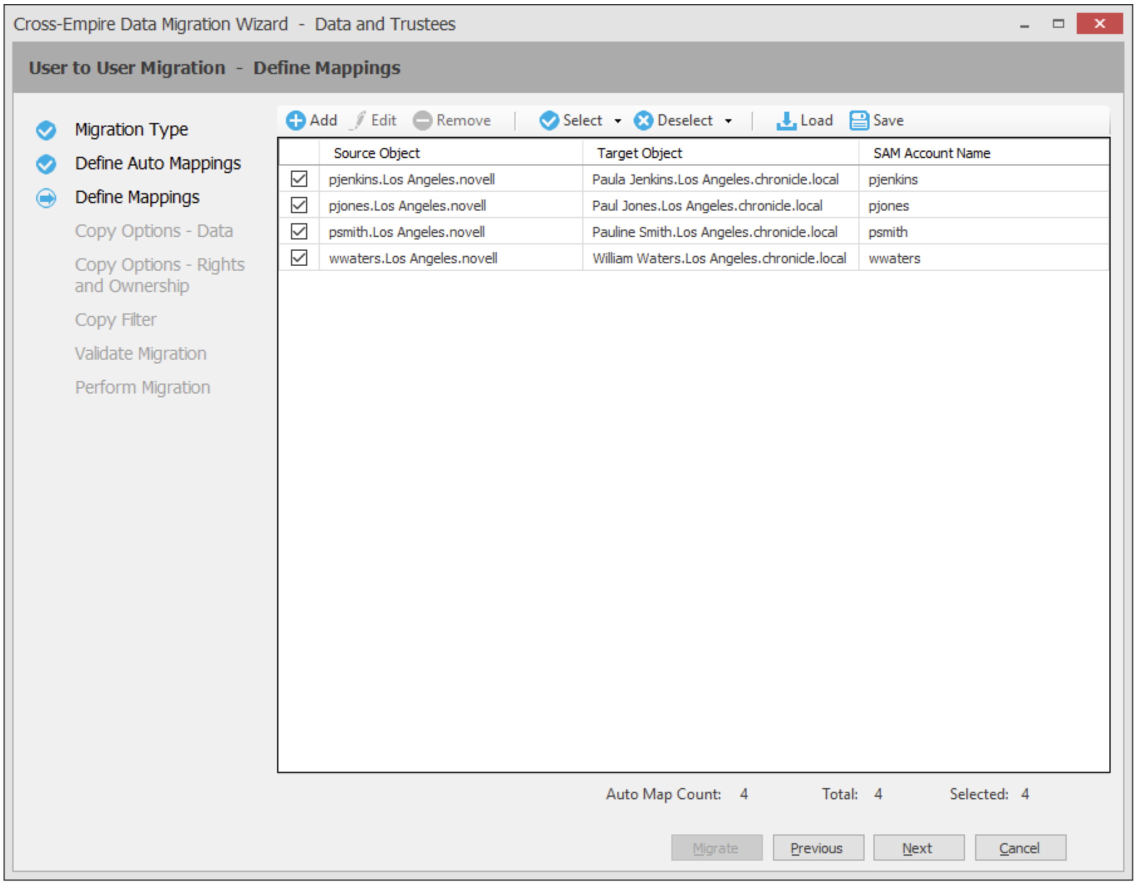
  **Target Container:** Browse to select the target container.

  **Include Source items not having a matching target:** Indicate if you want to identify source objects not having a matching target object.

- If you are migrating only a few users, use the **Add** button on the next wizard page to add the users individually.

9 Click **Next**.

The Data Migration Wizard attempts to match the Common Name (CN) of objects from the eDirectory source with the SAM (Security Accounts Manager) Account Names in the Active Directory target. If there is a match, the listed object in the **Source Object** field is selected and a corresponding match is listed in the Target Object column.



Cross-Empire Data Migration Wizard - Data and Trustees

User to User Migration - Define Mappings

| | Source Object | Target Object | SAM Account Name |
|---|---|---|---|
| ☑ | pjenkins.Los Angeles.novell | Paula Jenkins.Los Angeles.chronicle.local | pjenkins |
| ☑ | pjones.Los Angeles.novell | Paul Jones.Los Angeles.chronicle.local | pjones |
| ☑ | psmith.Los Angeles.novell | Pauline Smith.Los Angeles.chronicle.local | psmith |
| ☑ | wwaters.Los Angeles.novell | William Waters.Los Angeles.chronicle.local | wwaters |

Auto Map Count: 4 Total: 4 Selected: 4

**10** Specify a target object for each source object that is not automatically matched by double-clicking the name to bring up the Modify Data Map Entry dialog box.

**11** Click **Browse**, specify the target object, then click **OK**.

The target object is displayed in the **Target Object** column.

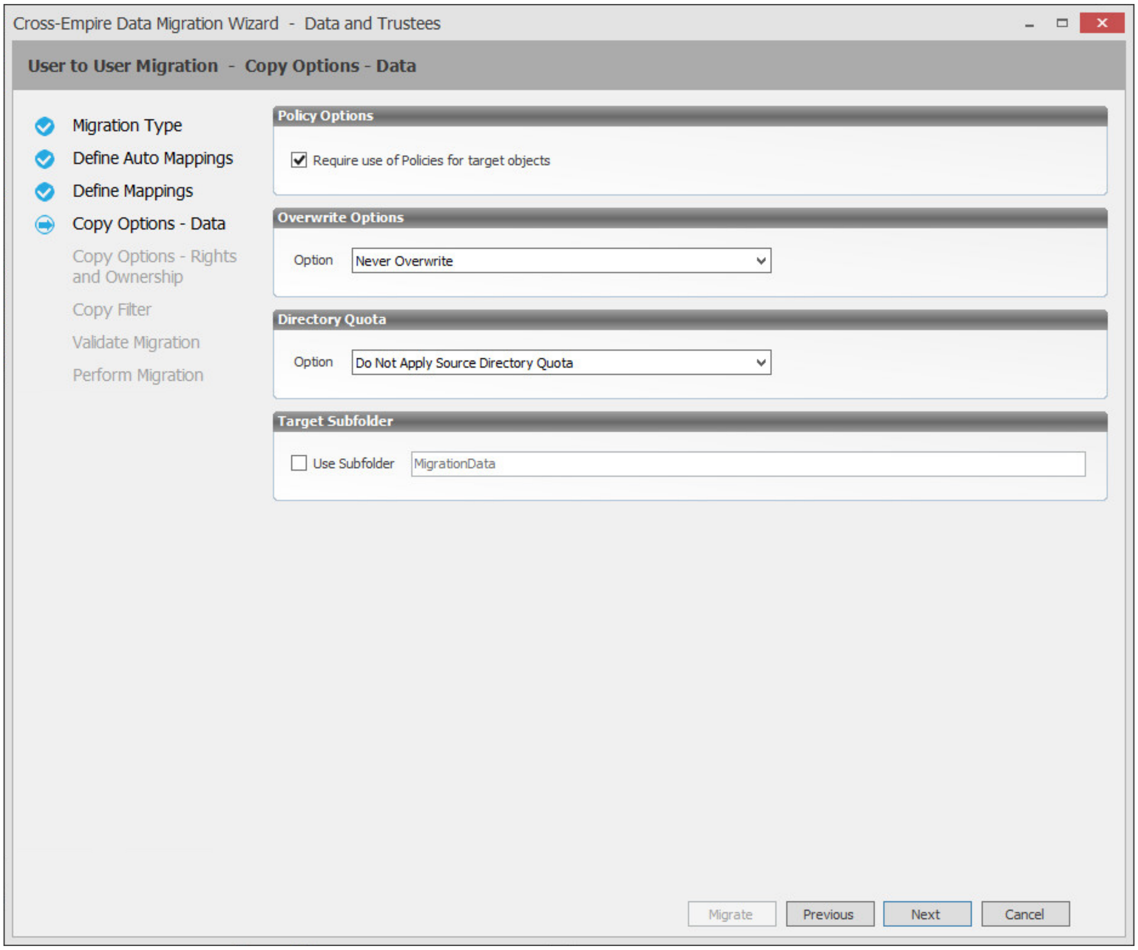
**12** Click the check box corresponding to the listing with the new target.

**13** Repeat Step 10 and Step 11 to specify all target objects that are not listed.

To change the specified target object, use the **Edit** button.

To add an object to the Source Object column, use the **Add** button.

**14** When all of the objects you want to migrate are selected and have an associated target object, click **Next**.



Policy Options

☑ Require use of Policies for target objects

Overwrite Options

Option: Never Overwrite

Directory Quota

Option: Do Not Apply Source Directory Quota

Target Subfolder

☐ Use Subfolder: MigrationData

15 Fill in the following fields:

**Require use of Policies for target objects:** If you are migrating data for objects to an Active Directory container that has an associated Storage Manager policy, leave this check box selected.

If this check box is selected and there is no associated Storage Manager policy, the object's data is not eligible for migration.

Additionally, if you are migrating a user and the target user is not currently managed by an associated policy, but the object does have a policy that would apply to it, then Storage Manager automatically applies that policy to the target user.

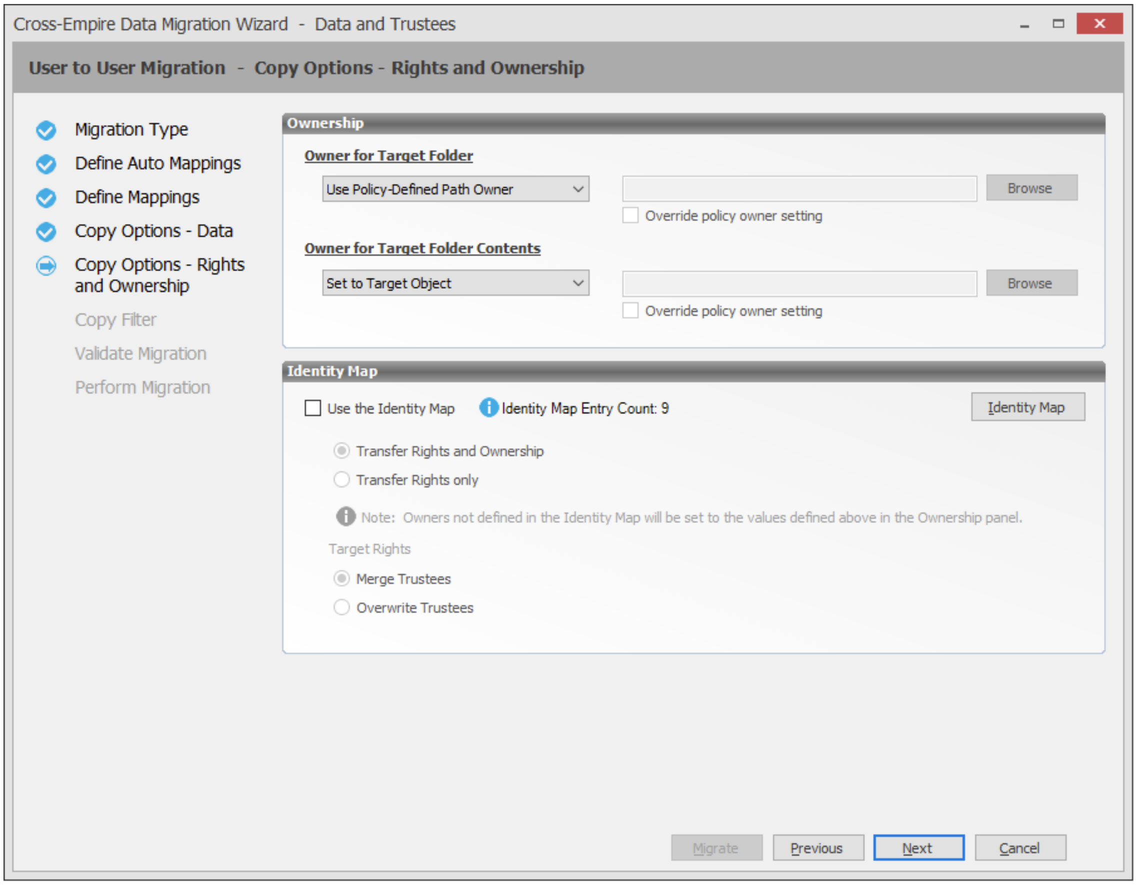
If you are migrating object data to an Active Directory container that does not have an associated Storage Manager policy, deselect this check box.

**Overwrite Options:** Indicate what you want to take place when duplicate filenames are encountered in the source and target.

**Directory Quota:** Specify how quota settings from the source Novell or Micro Focus file system should be applied after the migration.

**Target Subfolder:** If you want migrated data to be placed in a subfolder, select the **Use Subfolder** check box and specify the subfolder name in the field.

16 Click **Next**.



Owner for Target Folder: Use Policy-Defined Path Owner

□ Override policy owner setting

Owner for Target Folder Contents: Set to Target Object

□ Override policy owner setting

□ Use the Identity Map

Identity Map Entry Count: 9

● Transfer Rights and Ownership

○ Transfer Rights only

Note: Owners not defined in the Identity Map will be set to the values defined above in the Ownership panel.

Target Rights

● Merge Trustees

○ Overwrite Trustees

**17** Fill in the following fields:

**Owner for Target Folder:** Use these settings to specify how ownership of the migrated folder is determined.

If you selected the **Require use of Policies for target objects** check box in the previous wizard page, only the **Use Policy-Defined Path Owner** and **Set Explicit Owner** options are available on the drop-down menu.

- **Use Operating System Defaults:** This default setting allows the target Microsoft Windows Server to adjust the file ownership according to the settings on the target server.
- **Set to Target Object:** Specifies the target object as the owner of the migrated files. If the policy specifies a different owner, the policy's owner is applied.
- **Use Policy-Defined Path Owner:** Ownership of the files is determined according to the settings in the Storage Manager policy associated with the container where the object is managed.
- **Set Explicit Owner:** Allows you to browse and select an object as the explicit owner of the migrated folder, unless the policy specifies another object as the owner. To override the policy's configuration, select the **Override policy owner setting** check box.

**Owner for Target Folder Contents:** Use these settings to specify how ownership of the migrated folder contents is determined.

If you selected the **Require use of Policies for target objects** check box in the previous wizard page, only the **Set to Target Object** and **Set Explicit Owner** options are available on the drop-down menu.

- **Use Operating System Defaults:** This default setting allows the target Microsoft Windows Server to adjust the file ownership according to the settings on the target server.
- **Set to Target Object:** Specifies the target object as the owner of the migrated files. If the policy specifies a different owner, the policy's owner is applied.
- **Set Explicit Owner:** Allows you to browse and select an object as the explicit owner of the migrated files, unless the policy specifies another object as the owner. To override the policy's configuration, select the **Override policy owner setting** check box.

**Use the Identity Map:** Selecting this check box indicates that you want Storage Manager to utilize the identity map you created earlier and use the corresponding IDs to copy security rights and file ownership from the Novell or Micro Focus network file system to the Windows network file system.

- **Transfer Rights and Ownership:** Selecting this option indicates that you want to transfer the file and folder security rights along with the ownership settings.

  Be aware that when you transfer the ownership of a file or folder in a Windows network, you are granting the owner Full Rights, which you might not want to provide.
- **Transfer Rights Only:** Selecting this option indicates that you want to transfer only the file and folder security rights.
- **Overwrite Trustees:** Selecting this option indicates that you want any existing trustee assignments for a target file or folder, to be overridden by the established eDirectory trustee assignments for those files and folders.
- **Merge Trustees:** Selecting this option indicates that you want the established eDirectory trustee assignments merged with those of the target files or folders in the Windows file system.

**Identity Map:** Clicking this button opens your identity map where you can make any desired changes.

**18** Click **Next**.

**19** (Conditional) If you want to use a filter to include or exclude specific files, select the **Use Copy Filter** check box and click the **Add** button.

**19a** Fill in the following fields:

**Description:** Specify a description of the filter.

**Action:** From the drop-down menu, select either **Migrate** or **Ignore**, based on whether the filter specifies to migrate files or folders or to ignore them.

**Files, Folders:** Specify if the filter applies to files or folders.

**Masks:** List the file types to migrate or ignore.

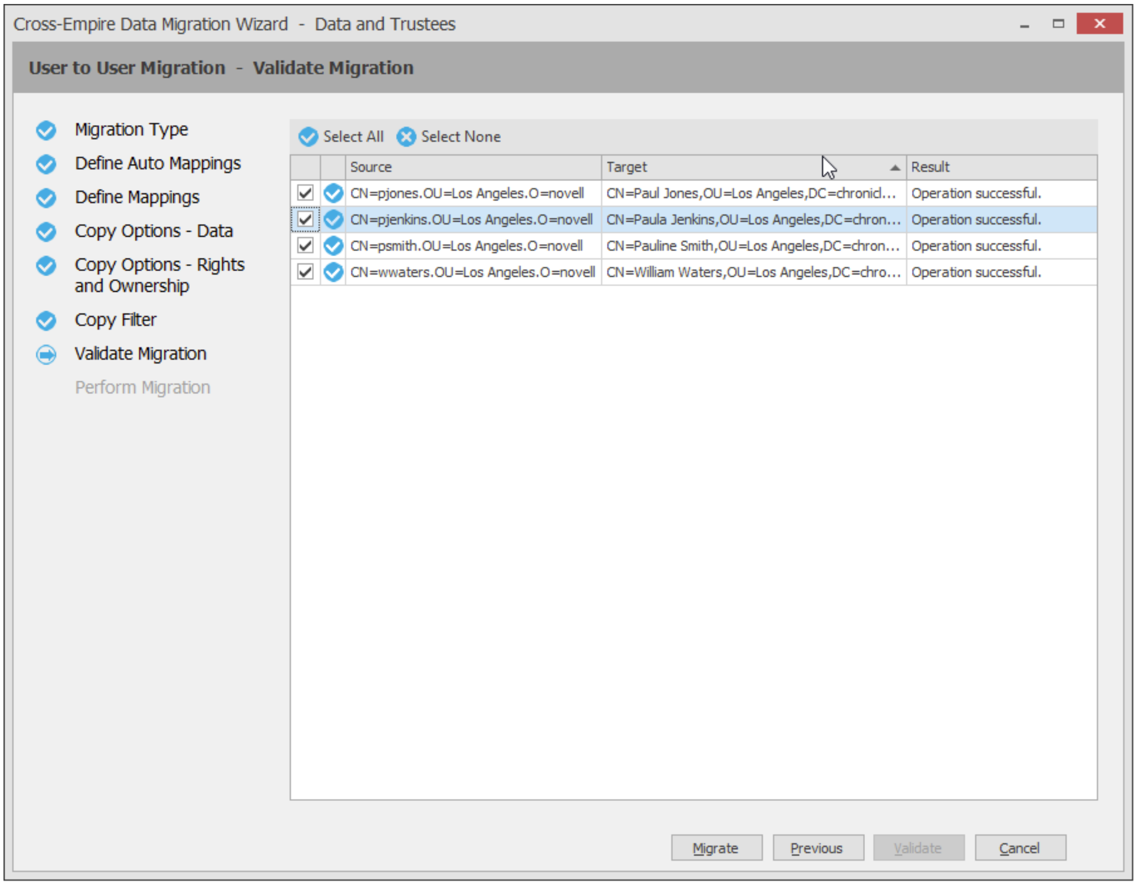
**19b** Specify any additional filter criteria in the menus and fields that remain.

For a detailed explanation of this region of the dialog box, see Section 6.5.8, "Setting Vault Rules," on page 58

**19c** Click **OK**.

**20** Click **Validate**.

**Validate** shows the result of certain checks that can be run prior to the migration. The **Result** column shows the status of the validation checks. If errors are displayed, you can choose to correct those errors prior to running the migration.

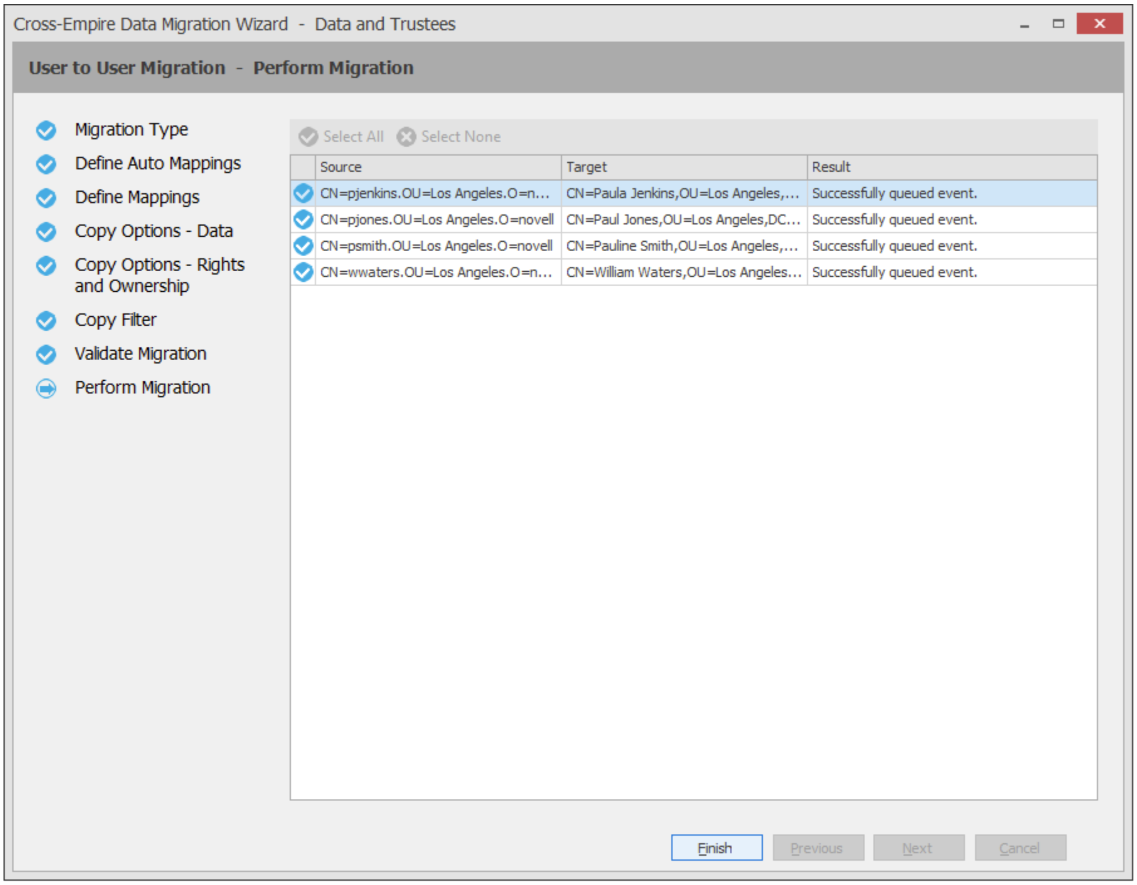


| | | Source | Target | Result |
|---|---|---|---|---|
| ☑ | ✓ | CN=pjones.OU=Los Angeles.O=novell | CN=Paul Jones,OU=Los Angeles,DC=chronicl... | Operation successful. |
| ☑ | ✓ | CN=pjenkins.OU=Los Angeles.O=novell | CN=Paula Jenkins,OU=Los Angeles,DC=chron... | Operation successful. |
| ☑ | ✓ | CN=psmith.OU=Los Angeles.O=novell | CN=Pauline Smith,OU=Los Angeles,DC=chron... | Operation successful. |
| ☑ | ✓ | CN=wwaters.OU=Los Angeles.O=novell | CN=William Waters,OU=Los Angeles,DC=chro... | Operation successful. |

**21** (Conditional) Take any necessary action in the Windows network file system target and click **Previous** and then **Validate** again.

**22** Click **Migrate**.

A page appears with details of the data migration events that are queued for processing. To view the status of migration events, click **Pending Events**. For more information on Pending Events, see Section 13.1.7, “Events,” on page 274.

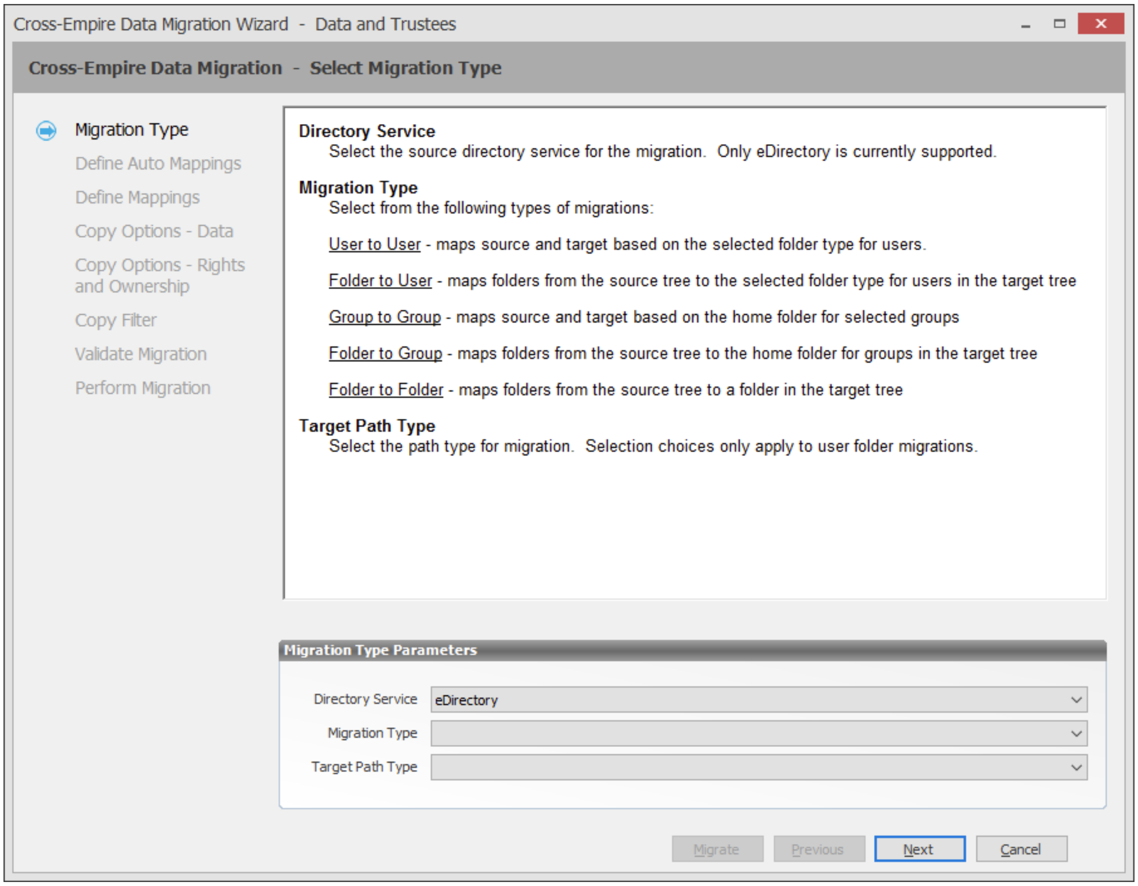


| | Source | Target | Result |
|---|---|---|---|
| ✓ | CN=pjenkins.OU=Los Angeles.O=n… | CN=Paula Jenkins,OU=Los Angeles,… | Successfully queued event. |
| ✓ | CN=pjones.OU=Los Angeles.O=novell | CN=Paul Jones,OU=Los Angeles,DC… | Successfully queued event. |
| ✓ | CN=psmith.OU=Los Angeles.O=novell | CN=Pauline Smith,OU=Los Angeles,… | Successfully queued event. |
| ✓ | CN=wwaters.OU=Los Angeles.O=n… | CN=William Waters,OU=Los Angeles… | Successfully queued event. |

**23** Click **Finish** to close the Data Migration Wizard.

## 10.9 Performing a Folder to User Data Migration

1. Make sure you have completed the prerequisites and have created a migration proxy account. For more information on the prerequisites, see Section 10.3, “Prerequisites,” on page 130. For more information on creating a migration proxy account, see Section 10.4, “Creating the Migration Proxy Account,” on page 131.
2. In SMAdmin, click the **Home** tab.
3. Select **Cross-Empire Data Migrations** > **eDirectory to Active Directory**.
4. Select **Migration Wizards** > **Data and Security**.


Cross-Empire Data Migration Wizard - Data and Trustees
Cross-Empire Data Migration - Select Migration Type
Migration Type
Define Auto Mappings
Define Mappings
Copy Options - Data
Copy Options - Rights and Ownership
Copy Filter
Validate Migration
Perform Migration
Migration Type Parameters
Migrate
Previous
Next
Cancel

**Directory Service**
Select the source directory service for the migration. Only eDirectory is currently supported.

**Migration Type**
Select from the following types of migrations:

User to User - maps source and target based on the selected folder type for users.

Folder to User - maps folders from the source tree to the selected folder type for users in the target tree

Group to Group - maps source and target based on the home folder for selected groups

Folder to Group - maps folders from the source tree to the home folder for groups in the target tree

Folder to Folder - maps folders from the source tree to a folder in the target tree

**Target Path Type**
Select the path type for migration. Selection choices only apply to user folder migrations.

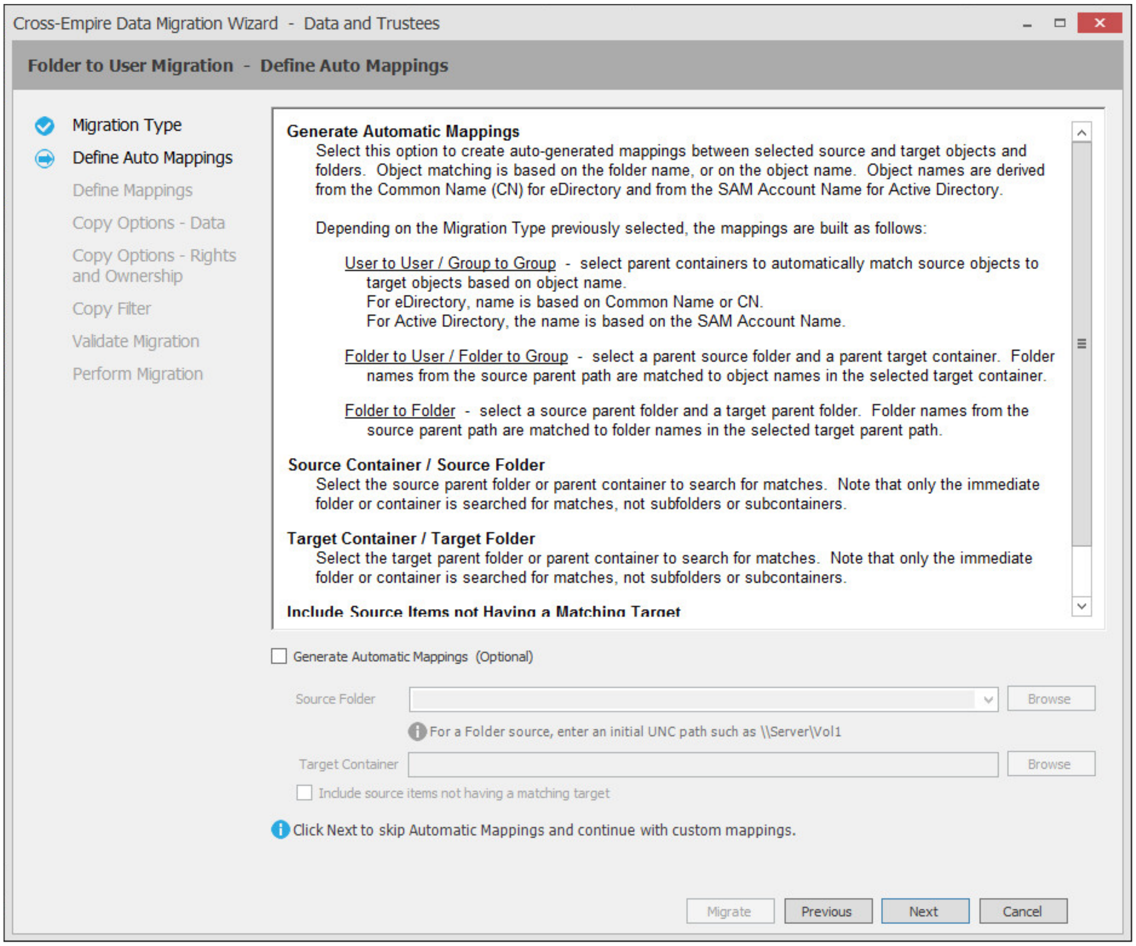
Directory Service: eDirectory
Migration Type:
Target Path Type:

5 From the **Migration Type** drop-down menu, select **Folder to User.**

6 From the **Target Path Type** drop-down menu, select the target path type for the data that you will migrate.

For example, if you select **Home Folder**, the data is copied to each user's home folder path as defined in directory services.

7 Click **Next**.



**Generate Automatic Mappings**
Select this option to create auto-generated mappings between selected source and target objects and folders. Object matching is based on the folder name, or on the object name. Object names are derived from the Common Name (CN) for eDirectory and from the SAM Account Name for Active Directory.

Depending on the Migration Type previously selected, the mappings are built as follows:

User to User / Group to Group - select parent containers to automatically match source objects to target objects based on object name.
For eDirectory, name is based on Common Name or CN.
For Active Directory, the name is based on the SAM Account Name.

Folder to User / Folder to Group - select a parent source folder and a parent target container. Folder names from the source parent path are matched to object names in the selected target container.

Folder to Folder - select a source parent folder and a target parent folder. Folder names from the source parent path are matched to folder names in the selected target parent path.

**Source Container / Source Folder**
Select the source parent folder or parent container to search for matches. Note that only the immediate folder or container is searched for matches, not subfolders or subcontainers.

**Target Container / Target Folder**
Select the target parent folder or parent container to search for matches. Note that only the immediate folder or container is searched for matches, not subfolders or subcontainers.

**Include Source Items not Having a Matching Target**

□ Generate Automatic Mappings (Optional)

Source Folder [ ] Browse

For a Folder source, enter an initial UNC path such as \\Server\Vol1

Target Container [ ] Browse

□ Include source items not having a matching target

Click Next to skip Automatic Mappings and continue with custom mappings.

8 Do one of the following:

- Fill in the following fields:

  **Generate Automatic Mappings:** If you are migrating a large number of folders, select this check box to activate the other fields.

  **Source Folder:** Specify an initial UNC path for a server and volume to browse.

  For example, `\\server_name\volume_name\` or `\\ip_address\volume_name`.

  After a path is entered, you can click the **Browse** button to browse to the folder you want.

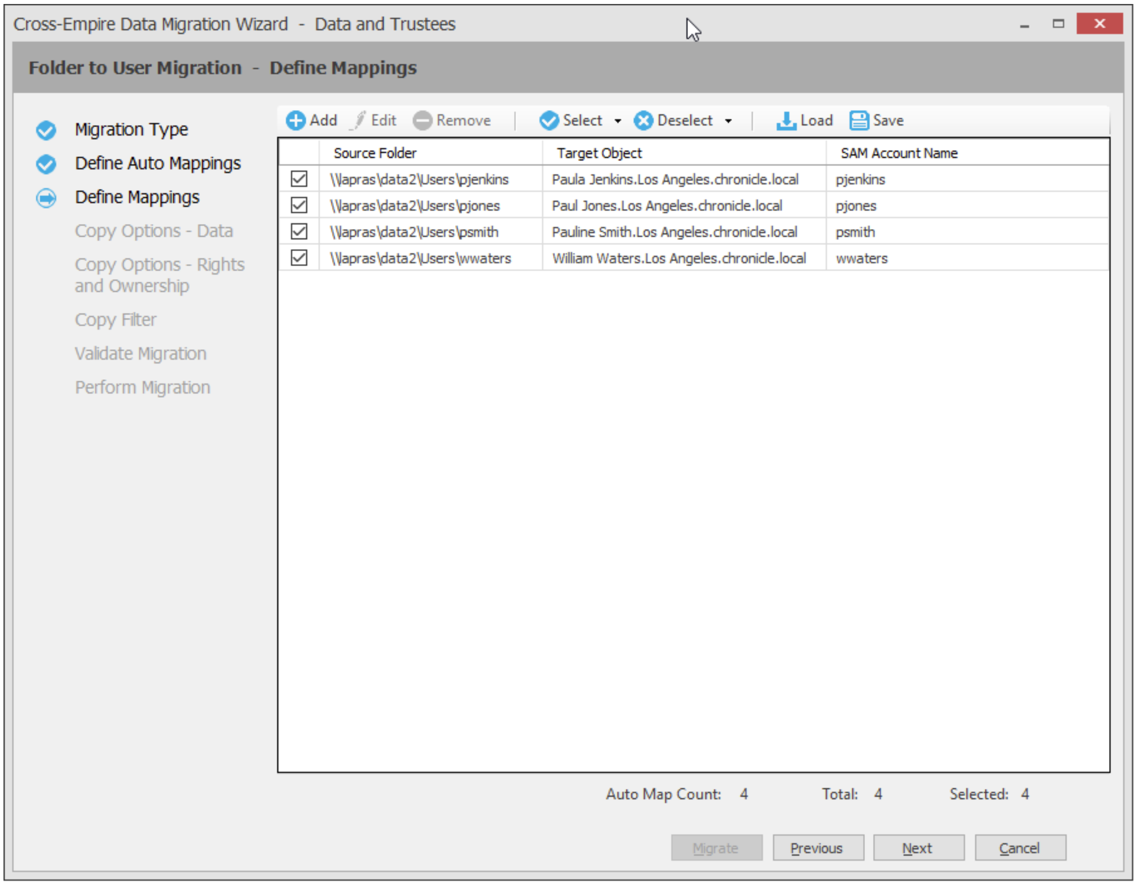
  **Target Container:** Browse to select the target container.

  **Include source items not having a matching target:** Indicate if you want to identify source data not having a matching target.

- If you are migrating only a few users, use the **Add** button on the next wizard page to add the users individually.

9 Click **Next**.

The Data Migration Wizard attempts to match the names of the subfolders of the source path with the SAM (Security Accounts Manager) Account Names in the Active Directory target. If there is a match, the listed folder in the **Source Folder** field is selected and a corresponding match is listed in the Target Object column.



| | Source Folder | Target Object | SAM Account Name |
|---|---|---|---|
| ☑ | \\apras\data2\Users\pjenkins | Paula Jenkins.Los Angeles.chronicle.local | pjenkins |
| ☑ | \\apras\data2\Users\pjones | Paul Jones.Los Angeles.chronicle.local | pjones |
| ☑ | \\apras\data2\Users\psmith | Pauline Smith.Los Angeles.chronicle.local | psmith |
| ☑ | \\apras\data2\Users\wwaters | William Waters.Los Angeles.chronicle.local | wwaters |

Auto Map Count: 4 Total: 4 Selected: 4

10 Specify a target object for each source object that is not automatically matched by double-clicking the name to bring up the Modify Data Map Entry dialog box.

11 Click **Browse**, specify the target object, then click **OK**.

The target object is displayed in the Target Object column.

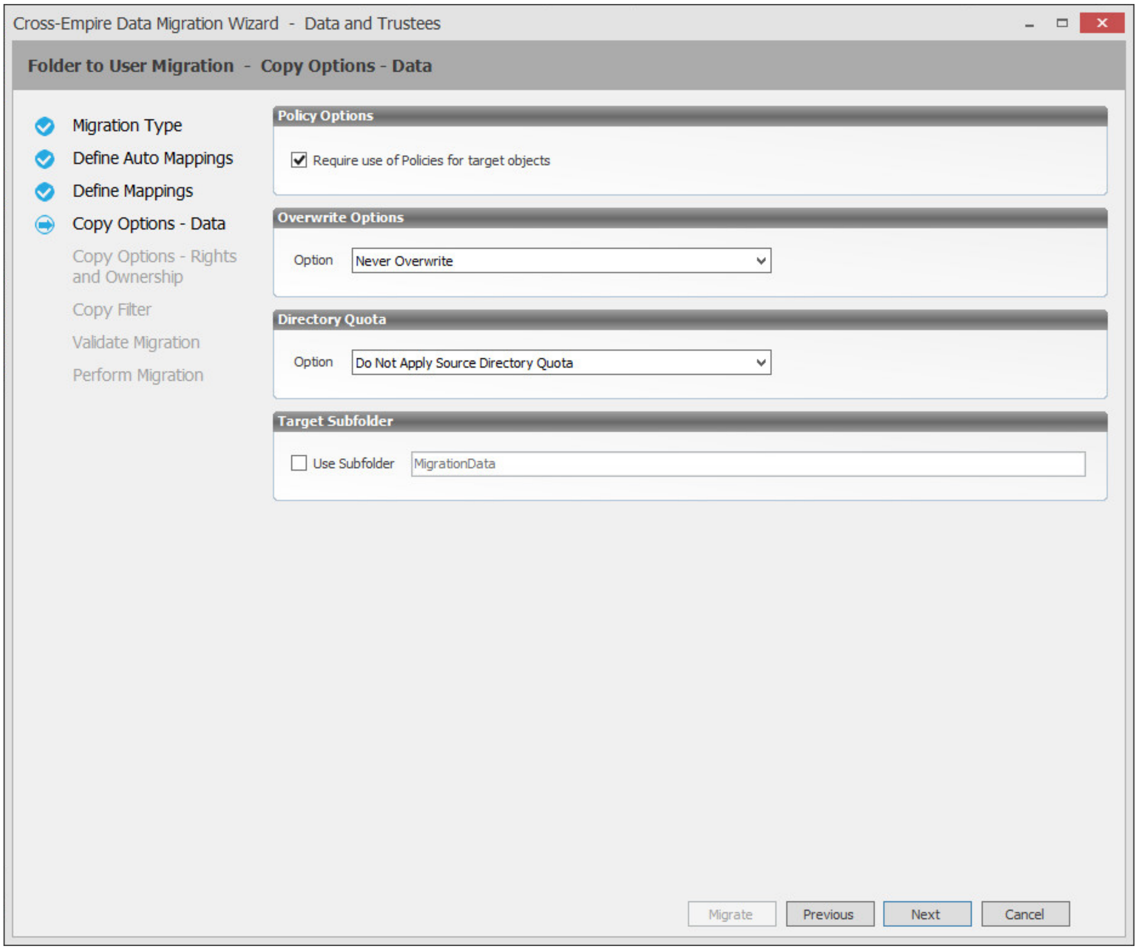
12 Click the check box corresponding to the listing with the new target.

13 Repeat Step 10 and Step 11 to specify all target objects that are not listed.

To change the specified target object, use the **Edit** button.

To add an object to the Source Object column, use the **Add** button.

14 When all of the objects you want to migrate are selected and have an associated target object, click **Next**.



Policy Options

☑ Require use of Policies for target objects

Overwrite Options

Option: Never Overwrite

Directory Quota

Option: Do Not Apply Source Directory Quota

Target Subfolder

☐ Use Subfolder: MigrationData

**15** Fill in the following fields:

**Require use of Policies for target objects:** If you are migrating data for objects to an Active Directory container that has an associated Storage Manager policy, leave this check box selected.

If this check box is selected and there is no associated Storage Manager policy, the object's data is not eligible for migration.

Additionally, if you are migrating a folder and the target user is not currently managed by an associated policy, but the user does have a policy that would apply to it, Storage Manager automatically applies that policy to the target user.

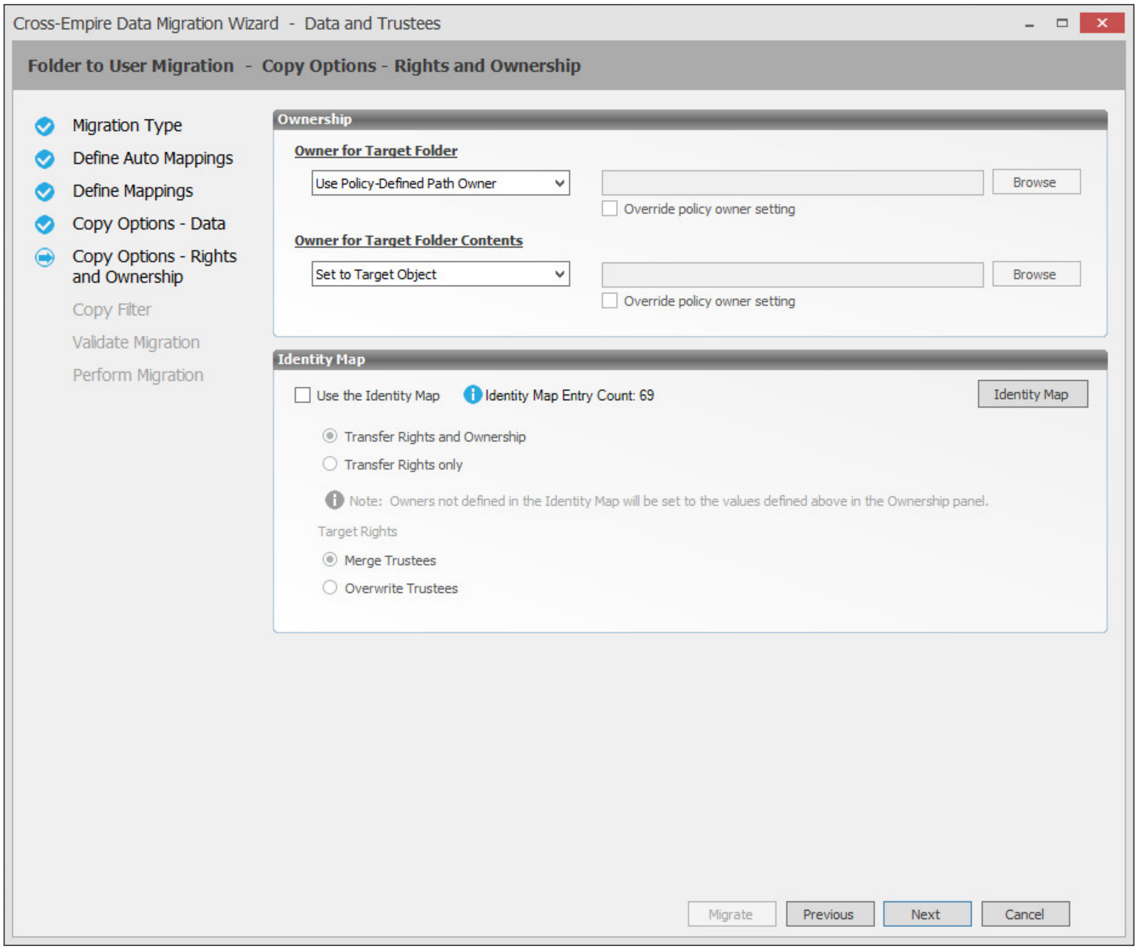
If you are migrating folders to an Active Directory container that does not have an associated Storage Manager policy, deselect this check box.

**Overwrite Options:** Indicate what you want to take place when duplicate filenames are encountered in the source and target.

**Directory Quota:** Specify how quota settings from the source Novell or Micro Focus file system should be applied after the migration.

**Target Subfolder:** If you want migrated data to be placed in a subfolder, select the **Use subfolder** check box and specify the subfolder name in the field.

**16** Click **Next**.



Cross-Empire Data Migration Wizard - Data and Trustees

Folder to User Migration - Copy Options - Rights and Ownership

Ownership

Owner for Target Folder: Use Policy-Defined Path Owner

□ Override policy owner setting

Owner for Target Folder Contents: Set to Target Object

□ Override policy owner setting

Identity Map

□ Use the Identity Map — Identity Map Entry Count: 69

● Transfer Rights and Ownership

○ Transfer Rights only

Note: Owners not defined in the Identity Map will be set to the values defined above in the Ownership panel.

Target Rights

● Merge Trustees

○ Overwrite Trustees

17 Fill in the following fields:

**Owner for Target Folder:** Use these settings to specify how ownership of the migrated folder is determined.

If you selected the **Require use of Policies for target objects** check box in the previous wizard page, only the **Use Policy-Defined Path Owner** and **Set Explicit Owner** options are available on the drop-down menu.

- **Use Operating System Defaults:** This default setting allows the target Microsoft Windows Server to adjust the file ownership according to the settings on the target server.
- **Set to Target Object:** Specifies the target object as the owner of the migrated files. If the policy specifies a different owner, the policy's owner is applied.
- **Use Policy-Defined Path Owner:** Ownership of the files is determined according to the settings in the Storage Manager policy associated with the container where the object is managed.
- **Set Explicit Owner:** Allows you to browse and select an object as the explicit owner of the migrated folder, unless the policy specifies another object as the owner. To override the policy's configuration, select the **Override policy owner setting** check box.

**Owner for Target Folder Contents:** Use these settings to specify how ownership of the migrated folder contents is determined.

If you selected the **Require use of Policies for target objects** check box in the previous wizard page, only the **Set to Target Object,** and **Set Explicit Owner** options are available on the drop-down menu.

- **Use Operating System Defaults:** This default setting allows the target Microsoft Windows Server to adjust the file ownership according to the settings on the target server.
- **Set to Target Object:** Specifies the target object as the owner of the migrated files. If the policy specifies a different owner, the policy's owner is applied.
- **Set Explicit Owner:** Allows you to browse and select an object as the explicit owner of the migrated folder, unless the policy specifies another object as the owner. To override the policy's configuration, select the **Override policy owner setting** check box.

**Use the Identity Map:** Selecting this check box indicates that you want Storage Manager to utilize the identity map you created earlier and use the corresponding IDs to copy security rights and file ownership from the Novell or Micro Focus network file system to the Windows network file system.

- **Transfer Rights and Ownership:** Selecting this option indicates that you want to transfer the file and folder security rights along with the ownership settings.

  Be aware that when you transfer the ownership of a file or folder in a Windows network, you are granting the owner Full Rights, which you might not want to provide.
- **Transfer Rights Only:** Selecting this option indicates that you want to transfer only the file and folder security rights.
- **Overwrite Trustees:** Selecting this option indicates that you want any existing trustee assignments for a target file or folder, to be overridden by the established eDirectory trustee assignments for those files and folders.
- **Merge Trustees:** Selecting this option indicates that you want the established eDirectory trustee assignments merged with those of the target files or folders in the Windows network file system.

**Identity Map:** Clicking this button opens your identity map where you can make any desired changes.

**18** Click **Next**.

**19** (Conditional) If you want to use a filter to include or exclude specific files, select the **Use Copy Filter** check box and click the **Add** button.

**19a** Fill in the following fields:

**Description:** Specify a description of the filter.

**Action:** From the drop-down menu, select either **Migrate** or **Ignore**, based on whether the filter specifies to migrate files or folders or to ignore them.

**Files, Folders:** Specify if the filter applies to files or folders.

**Masks:** List the file types to migrate or ignore.

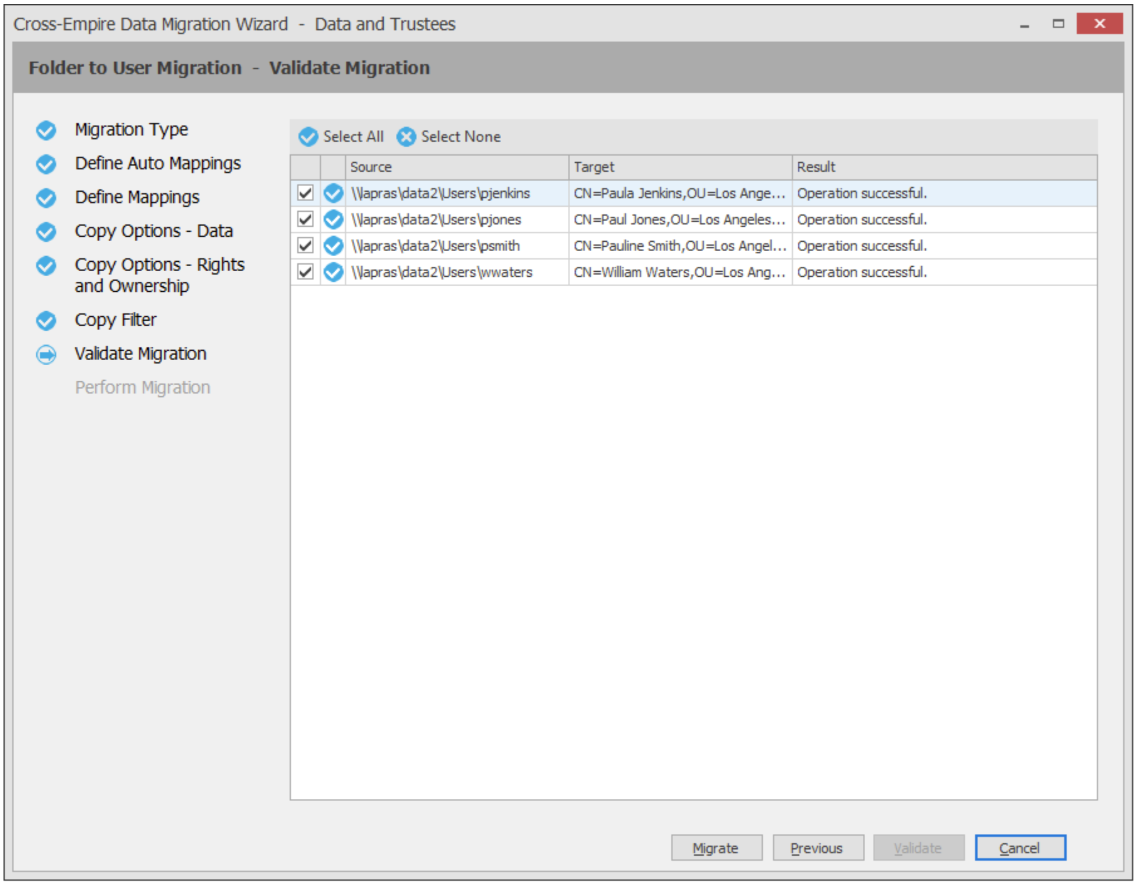
**19b** Specify any additional filter criteria in the menus and fields that remain.

For a detailed explanation of this region of the dialog box, see Section 6.5.8, "Setting Vault Rules," on page 58.

**19c** Click **OK**.

**20** Click **Validate**.

**Validate** shows the result of certain checks that can be run prior to the migration. The **Result** column shows the status of the validation checks. If errors are displayed, you can choose to correct those errors prior to running the migration.



| | | Source | Target | Result |
|---|---|---|---|---|
| ☑ | ✓ | \\apras\data2\Users\pjenkins | CN=Paula Jenkins,OU=Los Ange... | Operation successful. |
| ☑ | ✓ | \\apras\data2\Users\pjones | CN=Paul Jones,OU=Los Angeles... | Operation successful. |
| ☑ | ✓ | \\apras\data2\Users\psmith | CN=Pauline Smith,OU=Los Angel... | Operation successful. |
| ☑ | ✓ | \\apras\data2\Users\wwaters | CN=William Waters,OU=Los Ang... | Operation successful. |

21 (Conditional) Take any necessary action in the Windows network file system target and click **Previous** and then **Validate** again.

22 Click **Migrate**.

A page appears with details of the data migration events that are queued for processing. To view the status of migration events, click **Pending Events**. For more information on Pending Events, see Section 13.1.7, “Events,” on page 274.

23 Click **Finish** to close the Data Migration Wizard.

## 10.10 Performing a Group to Group Data Migration

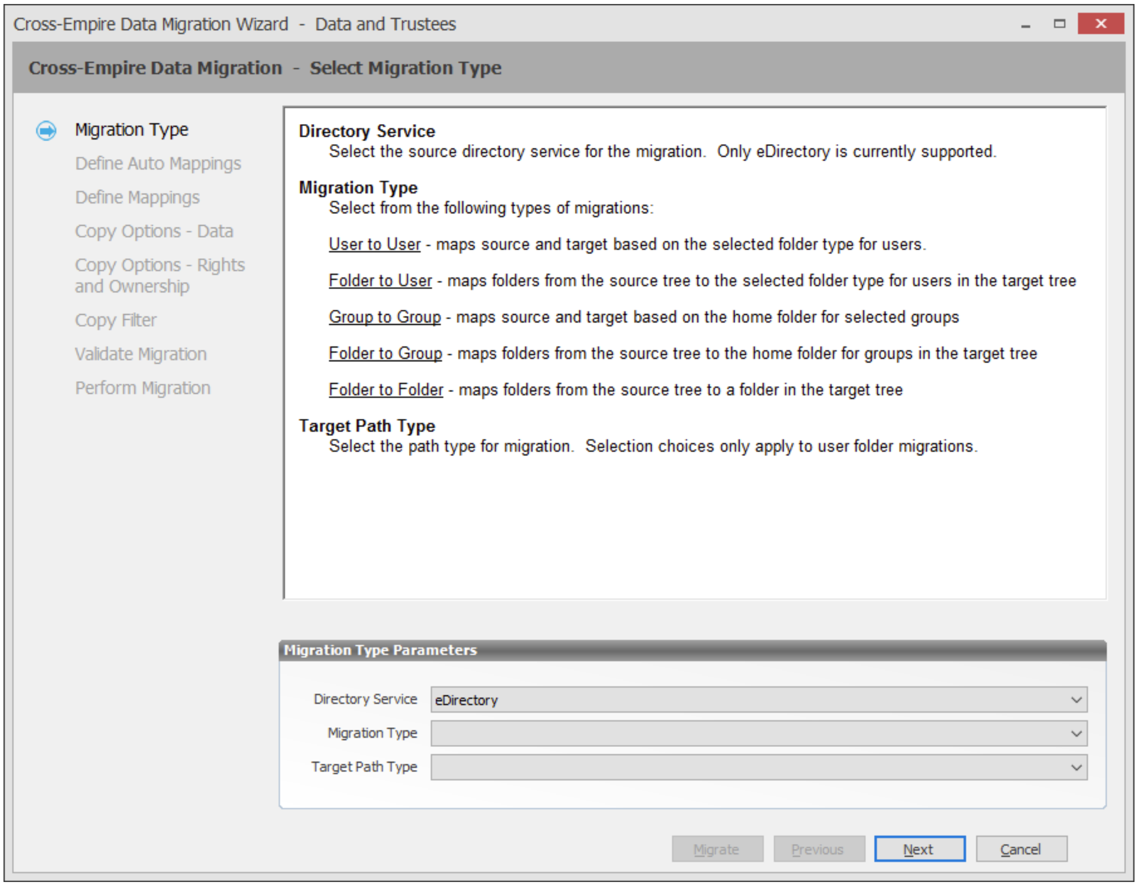
**IMPORTANT:** This migration option can be performed only if the source volume from which you are migrating has group home folders being managed by Micro Focus Storage Manager for eDirectory group-based collaborative storage policies.

1 Make sure you have completed the prerequisites and have created a migration proxy account. For more information on the prerequisites, see Section 10.3, “Prerequisites,” on page 130. For more information on creating a migration proxy account, see Section 10.4, “Creating the Migration Proxy Account,” on page 131.

2 In SMAdmin, click the **Home** tab.

3 Select **Cross-Empire Data Migrations** > **eDirectory to Active Directory**.

4 Select **Migration Wizards** > **Data and Security**.


Cross-Empire Data Migration Wizard - Data and Trustees
Cross-Empire Data Migration - Select Migration Type
Migration Type
Define Auto Mappings
Define Mappings
Copy Options - Data
Copy Options - Rights and Ownership
Copy Filter
Validate Migration
Perform Migration
Migrate
Previous
Next
Cancel

**Directory Service**
Select the source directory service for the migration. Only eDirectory is currently supported.

**Migration Type**
Select from the following types of migrations:

User to User - maps source and target based on the selected folder type for users.

Folder to User - maps folders from the source tree to the selected folder type for users in the target tree

Group to Group - maps source and target based on the home folder for selected groups

Folder to Group - maps folders from the source tree to the home folder for groups in the target tree

Folder to Folder - maps folders from the source tree to a folder in the target tree

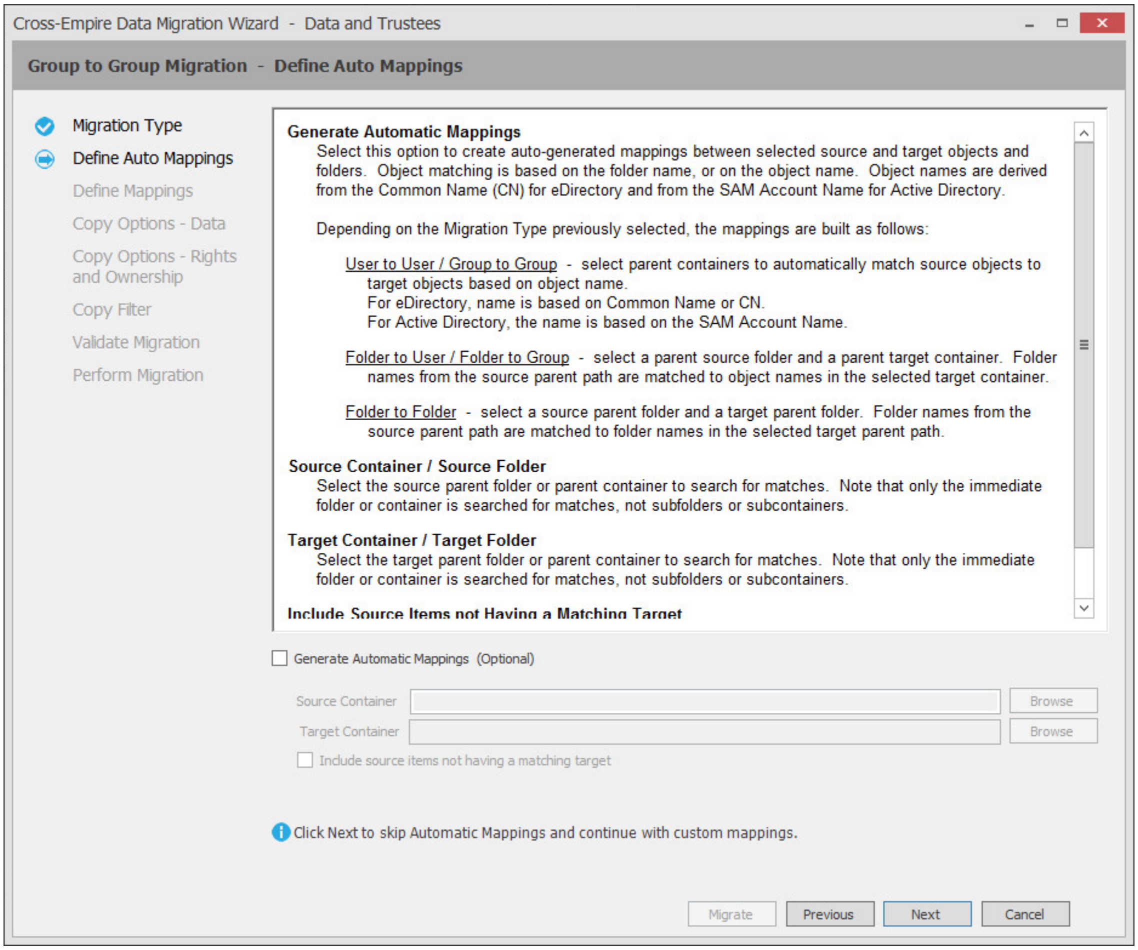
**Target Path Type**
Select the path type for migration. Selection choices only apply to user folder migrations.

**Migration Type Parameters**

| | |
|---|---|
| Directory Service | eDirectory |
| Migration Type | |
| Target Path Type | |

5 From the **Migration Type** drop-down menu, select **Group to Group**.

6 Click **Next**.



**Generate Automatic Mappings**
Select this option to create auto-generated mappings between selected source and target objects and folders. Object matching is based on the folder name, or on the object name. Object names are derived from the Common Name (CN) for eDirectory and from the SAM Account Name for Active Directory.

Depending on the Migration Type previously selected, the mappings are built as follows:

User to User / Group to Group - select parent containers to automatically match source objects to target objects based on object name.
For eDirectory, name is based on Common Name or CN.
For Active Directory, the name is based on the SAM Account Name.

Folder to User / Folder to Group - select a parent source folder and a parent target container. Folder names from the source parent path are matched to object names in the selected target container.

Folder to Folder - select a source parent folder and a target parent folder. Folder names from the source parent path are matched to folder names in the selected target parent path.

**Source Container / Source Folder**
Select the source parent folder or parent container to search for matches. Note that only the immediate folder or container is searched for matches, not subfolders or subcontainers.

**Target Container / Target Folder**
Select the target parent folder or parent container to search for matches. Note that only the immediate folder or container is searched for matches, not subfolders or subcontainers.

**Include Source Items not Having a Matching Target**

□ Generate Automatic Mappings (Optional)

Source Container

Target Container

□ Include source items not having a matching target

Click Next to skip Automatic Mappings and continue with custom mappings.

**7** Do one of the following:

- Fill in the following fields:

  **Generate Automatic Mappings:** If you are migrating a large number of groups, select this check box to activate the other fields.

  **Source Container:** Browse to select the source container.

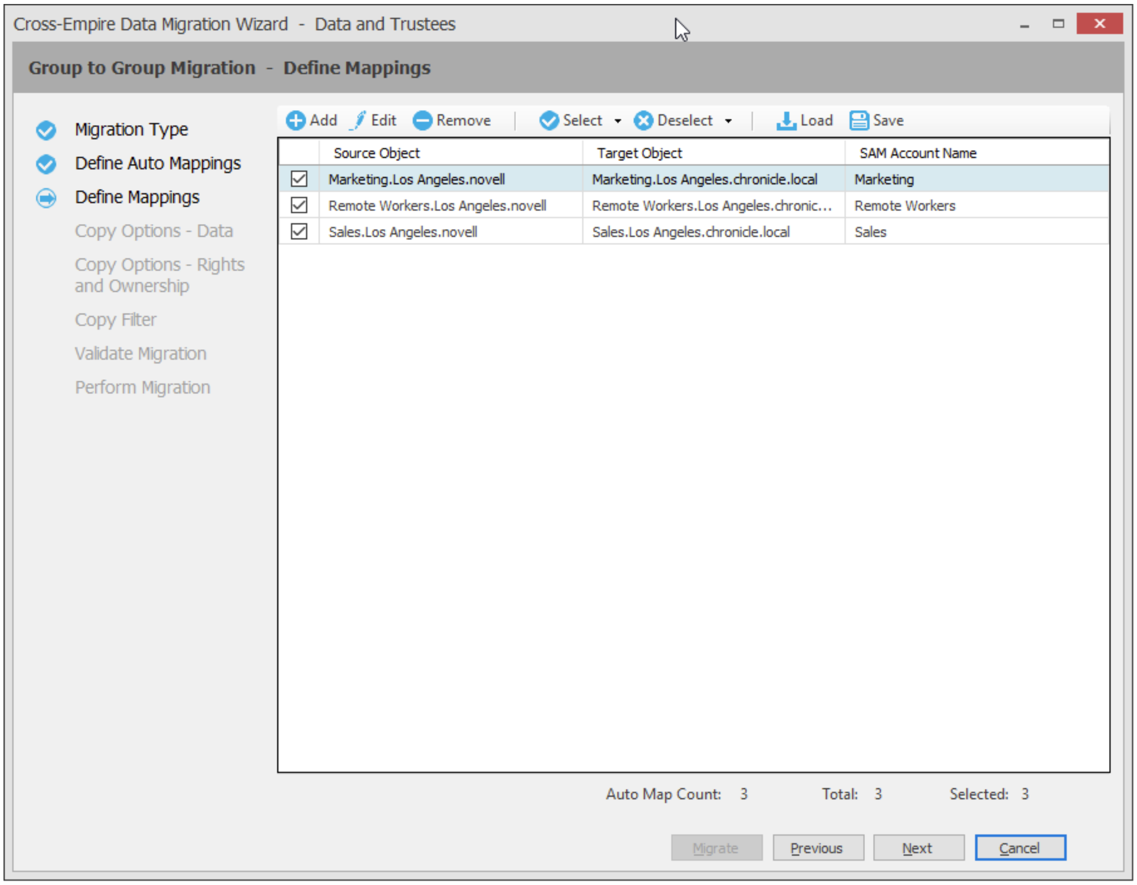
  **Target Container:** Browse to select the target container.

  **Include source items not having a matching target:** Indicate if you want to identify source data not having a matching target.

- If you are migrating only a few groups, use the **Add** button in the next wizard page to add the groups individually.

**8** Click **Next**.

The Data Migration Wizard attempts to match the Common Names (CN) of objects from the eDirectory source with the SAM (Security Accounts Manager) Account Names in the Active Directory target. If there is a match, the listed object in the **Source Object** field is selected and a corresponding match is listed in the **Target Object** column.



| | Source Object | Target Object | SAM Account Name |
|---|---|---|---|
| ☑ | Marketing.Los Angeles.novell | Marketing.Los Angeles.chronicle.local | Marketing |
| ☑ | Remote Workers.Los Angeles.novell | Remote Workers.Los Angeles.chronic… | Remote Workers |
| ☑ | Sales.Los Angeles.novell | Sales.Los Angeles.chronicle.local | Sales |

Auto Map Count: 3 Total: 3 Selected: 3

9 Specify a target object for each source object that is not automatically matched by double-clicking the name to bring up the Modify Data Map Entry dialog box.

10 Click **Browse**, specify the target object, then click **OK**.

The target object is displayed in the **Target Object** column.

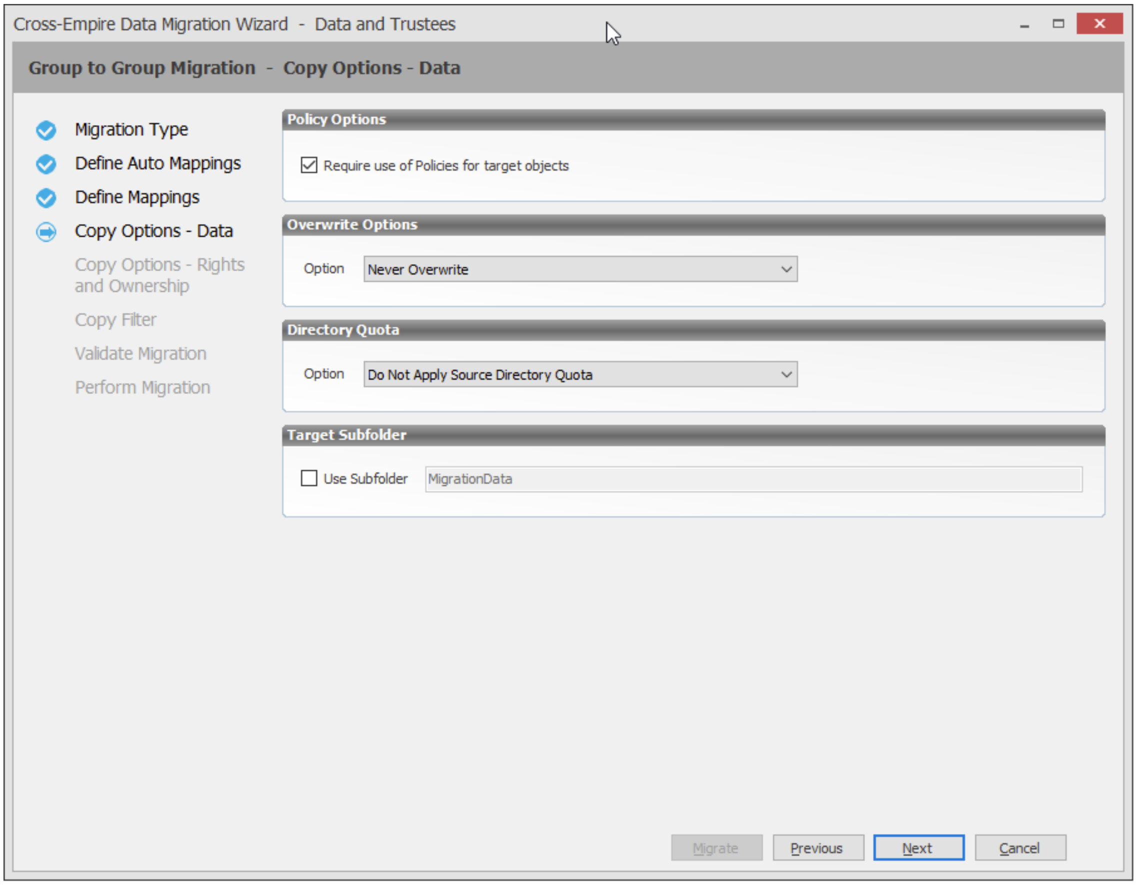
11 Click the check box corresponding to the listing with the new target.

12 Repeat Step 9 and Step 10 to specify all target objects that are not listed.

To change the specified target object, use the **Edit** button.

To add an object to the Source Object column, use the **Add** button.

13 When all of the objects you want to migrate are selected and have an associated target object, click **Next**.



Cross-Empire Data Migration Wizard - Data and Trustees

Group to Group Migration - Copy Options - Data

Policy Options

☑ Require use of Policies for target objects

Overwrite Options

Option: Never Overwrite

Directory Quota

Option: Do Not Apply Source Directory Quota

Target Subfolder

□ Use Subfolder: MigrationData

**14** Fill in the following fields:

**Require use of Policies for target objects:** If you are migrating data for objects to an Active Directory container that has an associated Storage Manager policy, leave this check box selected.

If this check box is selected and there is no associated Storage Manager policy, the object's data is not eligible for migration.

Additionally, if you are migrating a group folder and the target group is not currently managed by an associated policy, but the object does have a policy that would apply to it, Storage Manager will automatically apply that policy to the target object.

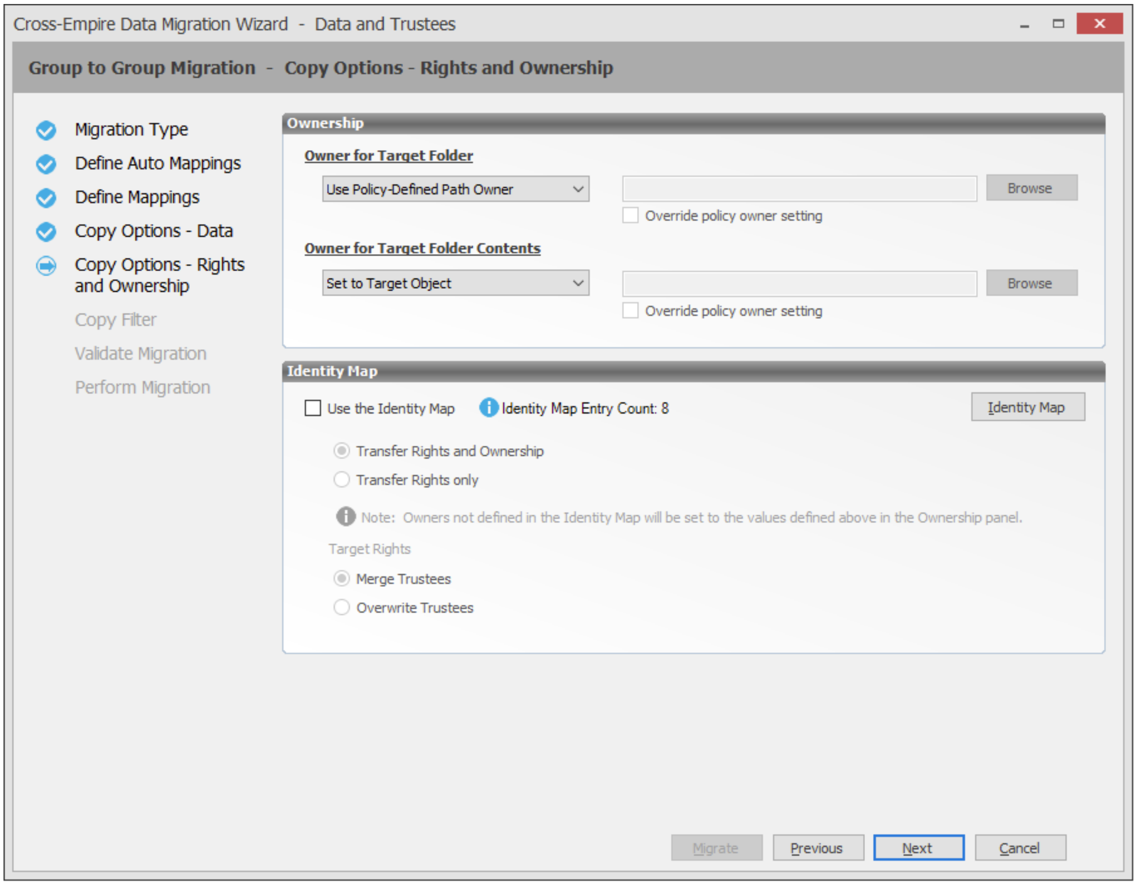
If you are migrating group folders data to Active Directory objects that do not have policy associations, deselect this check box.

**Overwrite Options:** Indicate what you want to take place when duplicate filenames are encountered in the source and target.

**Directory Quota:** Specify how quota settings from the source Novell or Micro Focus file system should be applied after the migration.

**Target Subfolder:** If you want migrated data to be placed in a subfolder, select the **Use subfolder** check box and specify the subfolder name in the field.

**15** Click **Next**.


Cross-Empire Data Migration Wizard - Data and Trustees

Group to Group Migration - Copy Options - Rights and Ownership

- ✓ Migration Type
- ✓ Define Auto Mappings
- ✓ Define Mappings
- ✓ Copy Options - Data
- Copy Options - Rights and Ownership
- Copy Filter
- Validate Migration
- Perform Migration

Ownership

Owner for Target Folder: Use Policy-Defined Path Owner

□ Override policy owner setting

Owner for Target Folder Contents: Set to Target Object

□ Override policy owner setting

Identity Map

□ Use the Identity Map

Identity Map Entry Count: 8

● Transfer Rights and Ownership

○ Transfer Rights only

Note: Owners not defined in the Identity Map will be set to the values defined above in the Ownership panel.

Target Rights

● Merge Trustees

○ Overwrite Trustees

**16** Fill in the following fields:

**Owner for Target Folder:** Use these settings to specify how ownership of the migrated folder is determined.

If you selected the **Require use of Policies for target objects** check box in the previous wizard page, only the **Use Policy-Defined Path Owner** and **Set Explicit Owner** options are available on the drop-down menu.

- **Use Operating System Defaults:** This default setting allows the target Microsoft Windows Server to adjust the file ownership according to the settings on the target server.
- **Set to Target Object:** Specifies the target object as the owner of the migrated files. If the policy specifies a different owner, the policy's owner is applied.
- **Use Policy-Defined Path Owner:** Ownership of the files is determined according to the settings in the Storage Manager policy associated with the container where the object is managed.
- **Set Explicit Owner:** Allows you to browse and select an object as the explicit owner of the migrated folder, unless the policy specifies another object as the owner. To override the policy's configuration, select the **Override policy owner setting** check box.

**Owner for Target Folder Contents:** Use these settings to specify how ownership of the migrated folder contents is determined.

If you selected the **Require use of Policies for target objects** check box in the previous wizard page, only the **Set to Target Object** and **Set Explicit Owner** options are available on the drop-down menu.

- **Use Operating System Defaults:** This default setting allows the target Microsoft Windows Server to adjust the file ownership according to the settings on the target server.
- **Set to Target Object:** Specifies the target object as the owner of the migrated files. If the policy specifies a different owner, the policy's owner is applied.
- **Set Explicit Owner:** Allows you to browse and select an object as the explicit owner of all of the migrated files, unless the policy specifies another object as the owner. To override the policy's configuration, select the **Override policy owner setting** check box.

**Use the Identity Map:** Selecting this check box indicates that you want Storage Manager to utilize the identity map you created earlier and use the corresponding IDs to copy security rights and file ownership from the Novell or Micro Focus network file system to the Windows network file system.

- **Transfer Rights and Ownership:** Selecting this option indicates that you want to transfer the file and folder security rights along with the ownership settings.

  Be aware that when you transfer the ownership of a file or folder in a Windows network, you are granting the owner Full Rights, which you might not want to provide.
- **Transfer Rights Only:** Selecting this option indicates that you want to transfer only the file and folder security rights.
- **Overwrite Trustees:** Selecting this option indicates that you want any existing trustee assignments for a target file or folder to be overridden by the established eDirectory trustee assignments for those files and folders.
- **Merge Trustees:** Selecting this option indicates that you want the established eDirectory trustee assignments merged with those of the target files or folders in the Windows network file system.

**Identity Map:** Clicking this button opens your identity map where you can make any desired changes.

17 Click **Next**.

18 (Conditional) If you want to use a filter to include or exclude specific files, select the **Use Copy Filter** check box and click the **Add** button.

18a Fill in the following fields:

**Description:** Specify a description of the filter.

**Action:** From the drop-down menu, select either **Migrate** or **Ignore**, based on whether the filter specifies to migrate files or folders or to ignore them.

**Files, Folders:** Specify if the filter applies to files or folders.

**Masks:** List the file types to migrate or ignore.

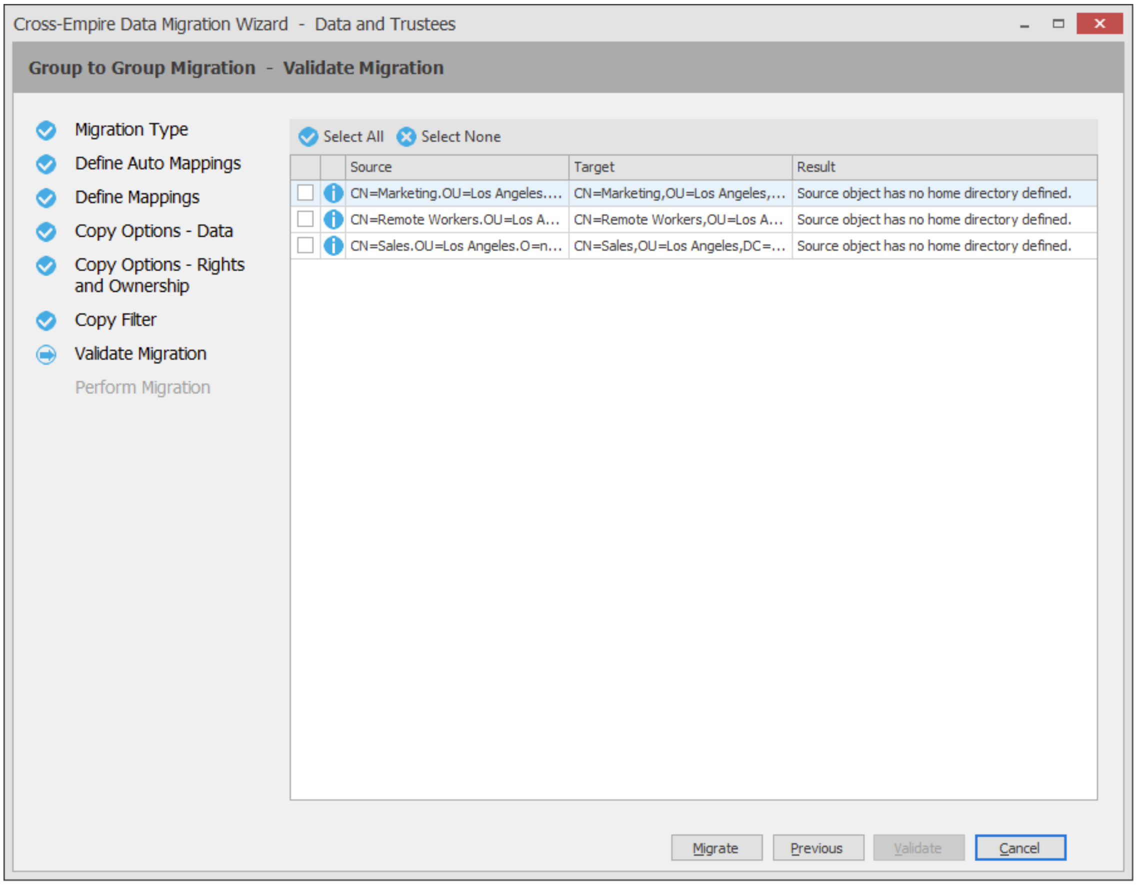
18b Specify any additional filter criteria in the menus and fields that remain.

For a detailed explanation of this region of the dialog box, see Section 6.5.8, "Setting Vault Rules," on page 58.

18c Click **OK**.

19 Click **Validate**.

**Validate** shows the result of certain checks that can be run prior to the migration. The **Result** column shows the status of the validation checks. If errors are displayed, you can choose to correct those errors prior to running the migration.



| | | Source | Target | Result |
|---|---|---|---|---|
| □ | ⓘ | CN=Marketing.OU=Los Angeles.… | CN=Marketing,OU=Los Angeles,… | Source object has no home directory defined. |
| □ | ⓘ | CN=Remote Workers.OU=Los A… | CN=Remote Workers,OU=Los A… | Source object has no home directory defined. |
| □ | ⓘ | CN=Sales.OU=Los Angeles.O=n… | CN=Sales,OU=Los Angeles,DC=… | Source object has no home directory defined. |

20 (Conditional) Take any necessary action in the Windows network file system target and click **Previous** and then **Validate** again.

21 Click **Migrate**.

A page appears with details of the data migration events that are queued for processing. To view the status of migration events, click **Pending Events**. For more information on Pending Events, see Section 13.1.7, “Events,” on page 274.

22 Click **Finish** to close the Data Migration Wizard.

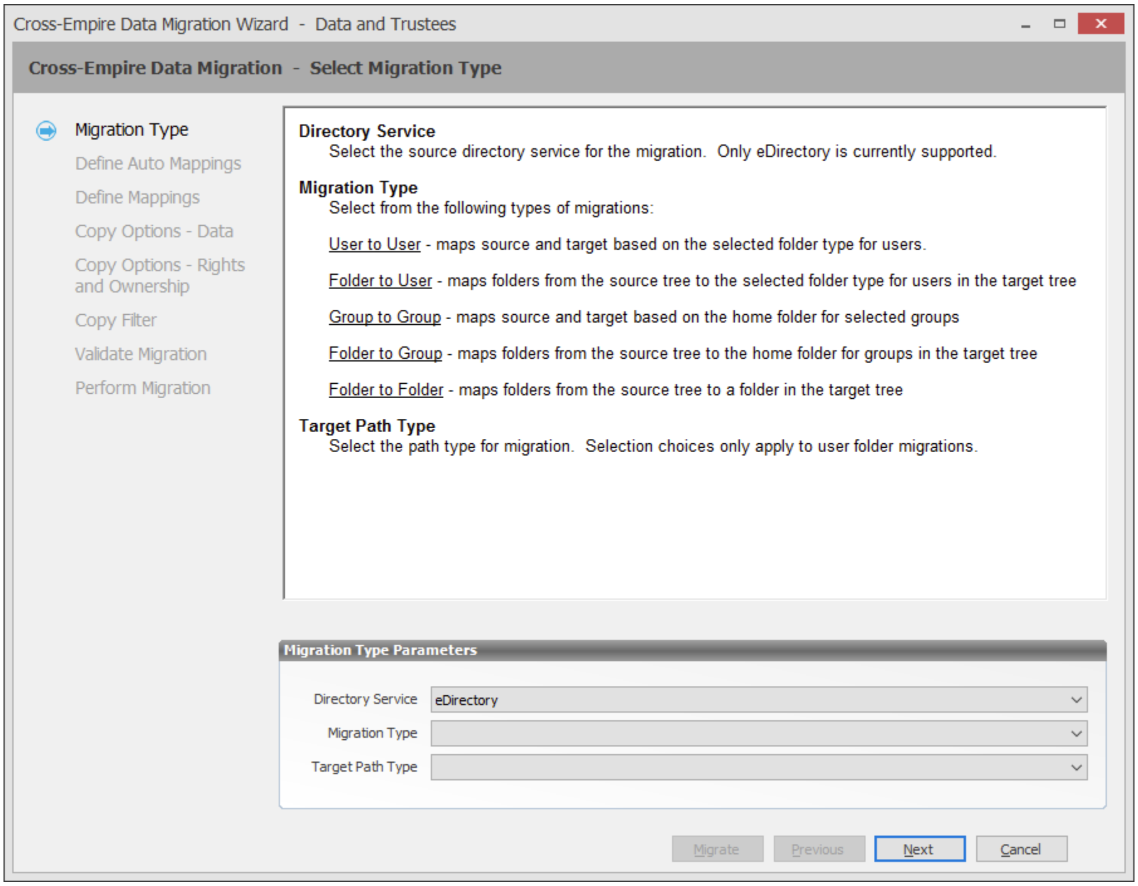
## 10.11 Performing a Folder to Group Migration

1 Make sure you have completed the prerequisites and have created a migration proxy account. For more information on the prerequisites, see Section 10.3, “Prerequisites,” on page 130. For more information on creating a migration proxy account, see Section 10.4, “Creating the Migration Proxy Account,” on page 131.

2 In SMAdmin, click the **Home** tab.

3 Select **Cross-Empire Data Migrations** > **eDirectory to Active Directory**.

4 Select **Migration Wizards** > **Data and Security**.


Cross-Empire Data Migration Wizard - Data and Trustees
Cross-Empire Data Migration - Select Migration Type
Migration Type
Define Auto Mappings
Define Mappings
Copy Options - Data
Copy Options - Rights and Ownership
Copy Filter
Validate Migration
Perform Migration
Migration Type Parameters
Migrate
Previous
Next
Cancel

**Directory Service**

Select the source directory service for the migration. Only eDirectory is currently supported.

**Migration Type**

Select from the following types of migrations:

User to User - maps source and target based on the selected folder type for users.

Folder to User - maps folders from the source tree to the selected folder type for users in the target tree

Group to Group - maps source and target based on the home folder for selected groups

Folder to Group - maps folders from the source tree to the home folder for groups in the target tree

Folder to Folder - maps folders from the source tree to a folder in the target tree

**Target Path Type**

Select the path type for migration. Selection choices only apply to user folder migrations.

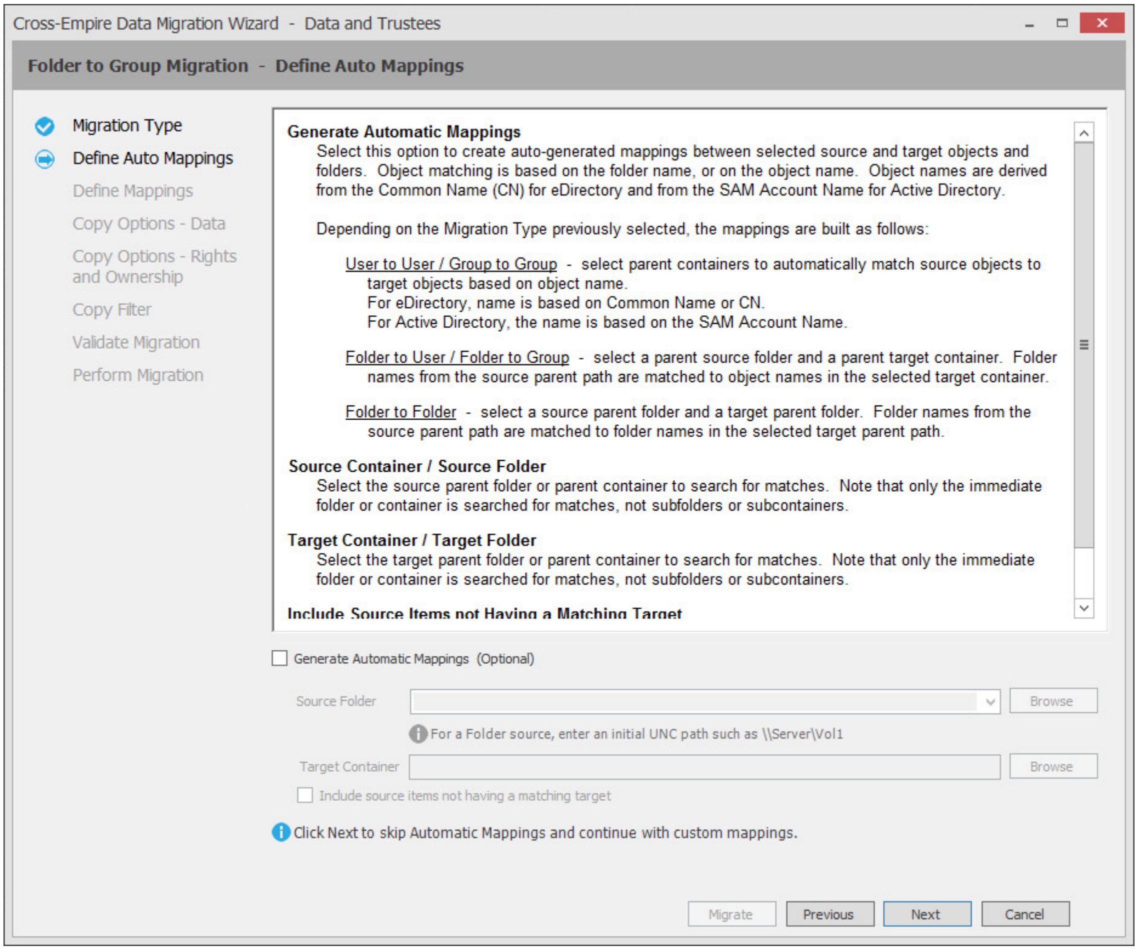
Directory Service: eDirectory

Migration Type:

Target Path Type:

5 From the **Migration Type** drop-down menu, select **Folder to Group.**

6 Click **Next**.



**Generate Automatic Mappings**
Select this option to create auto-generated mappings between selected source and target objects and folders. Object matching is based on the folder name, or on the object name. Object names are derived from the Common Name (CN) for eDirectory and from the SAM Account Name for Active Directory.

Depending on the Migration Type previously selected, the mappings are built as follows:

User to User / Group to Group - select parent containers to automatically match source objects to target objects based on object name.
For eDirectory, name is based on Common Name or CN.
For Active Directory, the name is based on the SAM Account Name.

Folder to User / Folder to Group - select a parent source folder and a parent target container. Folder names from the source parent path are matched to object names in the selected target container.

Folder to Folder - select a source parent folder and a target parent folder. Folder names from the source parent path are matched to folder names in the selected target parent path.

**Source Container / Source Folder**
Select the source parent folder or parent container to search for matches. Note that only the immediate folder or container is searched for matches, not subfolders or subcontainers.

**Target Container / Target Folder**
Select the target parent folder or parent container to search for matches. Note that only the immediate folder or container is searched for matches, not subfolders or subcontainers.

**Include Source Items not Having a Matching Target**

□ Generate Automatic Mappings (Optional)

Source Folder

For a Folder source, enter an initial UNC path such as \\Server\Vol1

Target Container

□ Include source items not having a matching target

Click Next to skip Automatic Mappings and continue with custom mappings.

7 Do one of the following:

- Fill in the following fields:

  **Generate Automatic Mappings:** If you are migrating a large number of folders, select this check box to activate the other fields.

  **Source Folder:** Specify an initial UNC path for a server and volume to browse.

  For example `\\server_name\volume_name\` or `\\ip_address\volume_name`.

  After a path is entered, you can click the **Browse** button to browse to the folder you want.

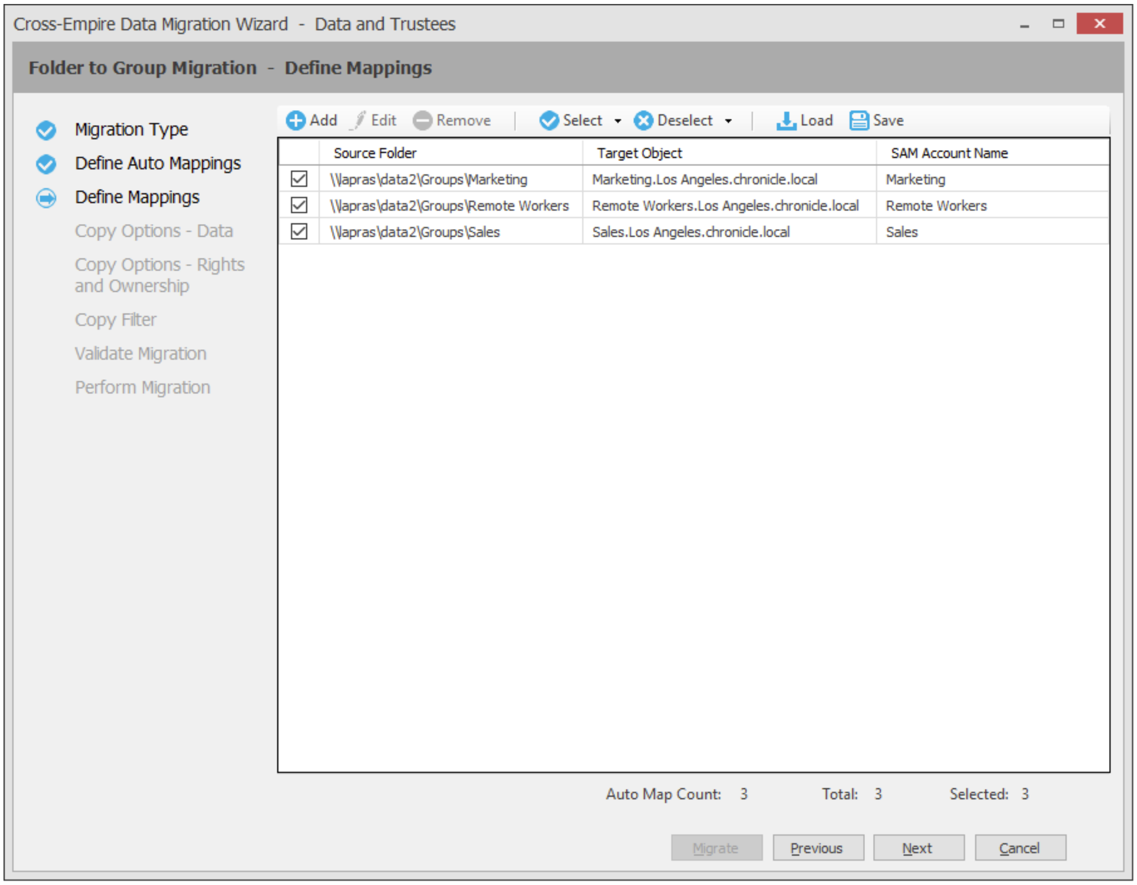
  **Target Container:** Browse to select the target container.

  **Include source items not having a matching target:** Indicate if you want to identify source data not having a matching target object.

- If you are migrating only a few users, use the **Add** button on the next wizard page to add the users individually.

8 Click **Next**.

The Data Migration Wizard attempts to match the names of subfolders of the source path with the SAM (Security Accounts Manager) Account Names in the Active Directory target. If there is a match, the listed folder in the **Source Folder** field is selected and a corresponding match is listed in the **Target Object** column.



| | Source Folder | Target Object | SAM Account Name |
|---|---|---|---|
| ☑ | \\lapras\data2\Groups\Marketing | Marketing.Los Angeles.chronicle.local | Marketing |
| ☑ | \\lapras\data2\Groups\Remote Workers | Remote Workers.Los Angeles.chronicle.local | Remote Workers |
| ☑ | \\lapras\data2\Groups\Sales | Sales.Los Angeles.chronicle.local | Sales |

Auto Map Count: 3 Total: 3 Selected: 3

**9** Specify a target object for each source folder that is not automatically matched by double-clicking the name to bring up the Modify Data Map Entry dialog box.

**10** Click **Browse**, specify the target object, then click **OK**.

The target object is displayed in the **Target Object** column.

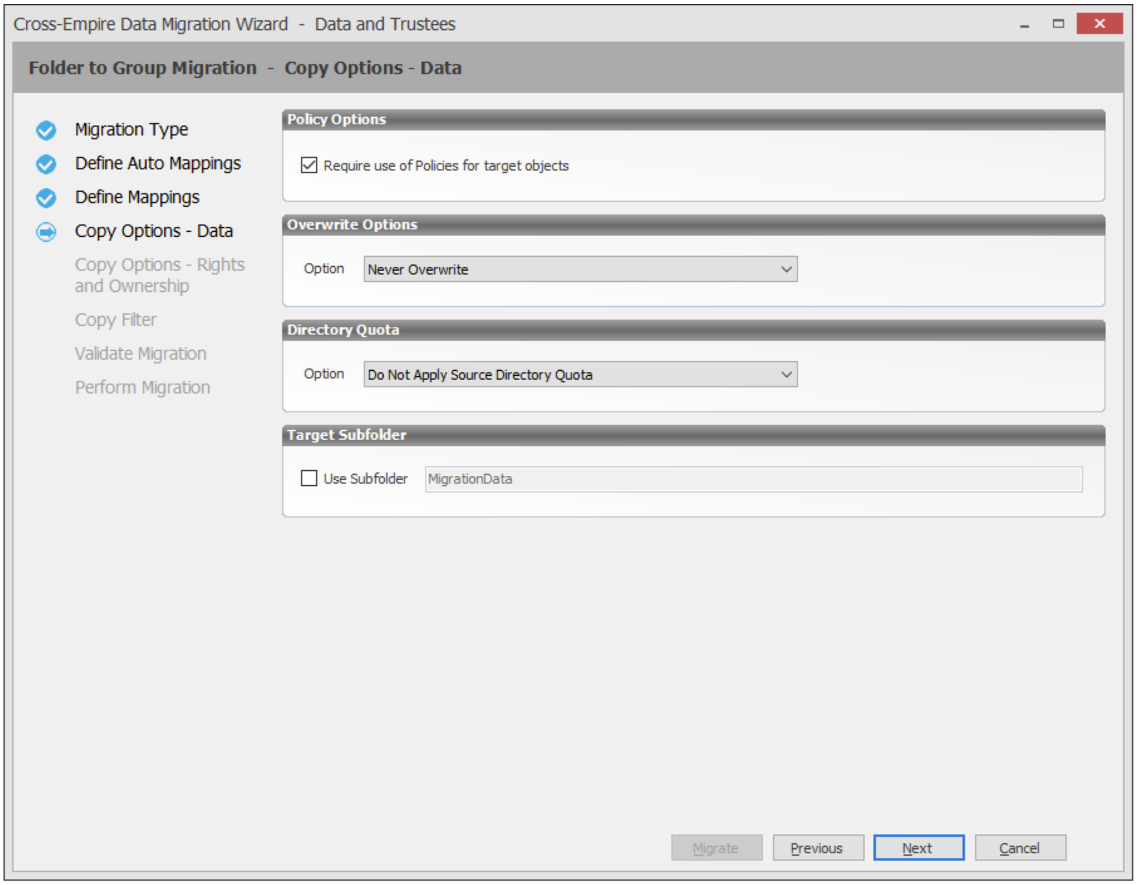
**11** Click the check box corresponding to the listing with the new target.

**12** Repeat Step 9 and Step 10 to specify all target objects that are not listed.

To change the specified target object, use the **Edit** button.

To add an object to the **Source Object** column, use the **Add** button.

**13** When all of the objects you want to migrate are selected and have an associated target object, click **Next**.



Policy Options

☑ Require use of Policies for target objects

Overwrite Options

Option: Never Overwrite

Directory Quota

Option: Do Not Apply Source Directory Quota

Target Subfolder

☐ Use Subfolder: MigrationData

14 Fill in the following fields:

**Require use of Policies for target objects:** If you are migrating data for objects to an Active Directory container that has an associated Storage Manager policy, leave this check box selected.

If this check box is selected and there is no associated Storage Manager policy, the object’s data is not eligible for migration.

Additionally, if you are migrating a folder and the target group is not currently managed by an associated policy, but the group does have a policy that would apply to it, Storage Manager automatically applies that policy to the target group.

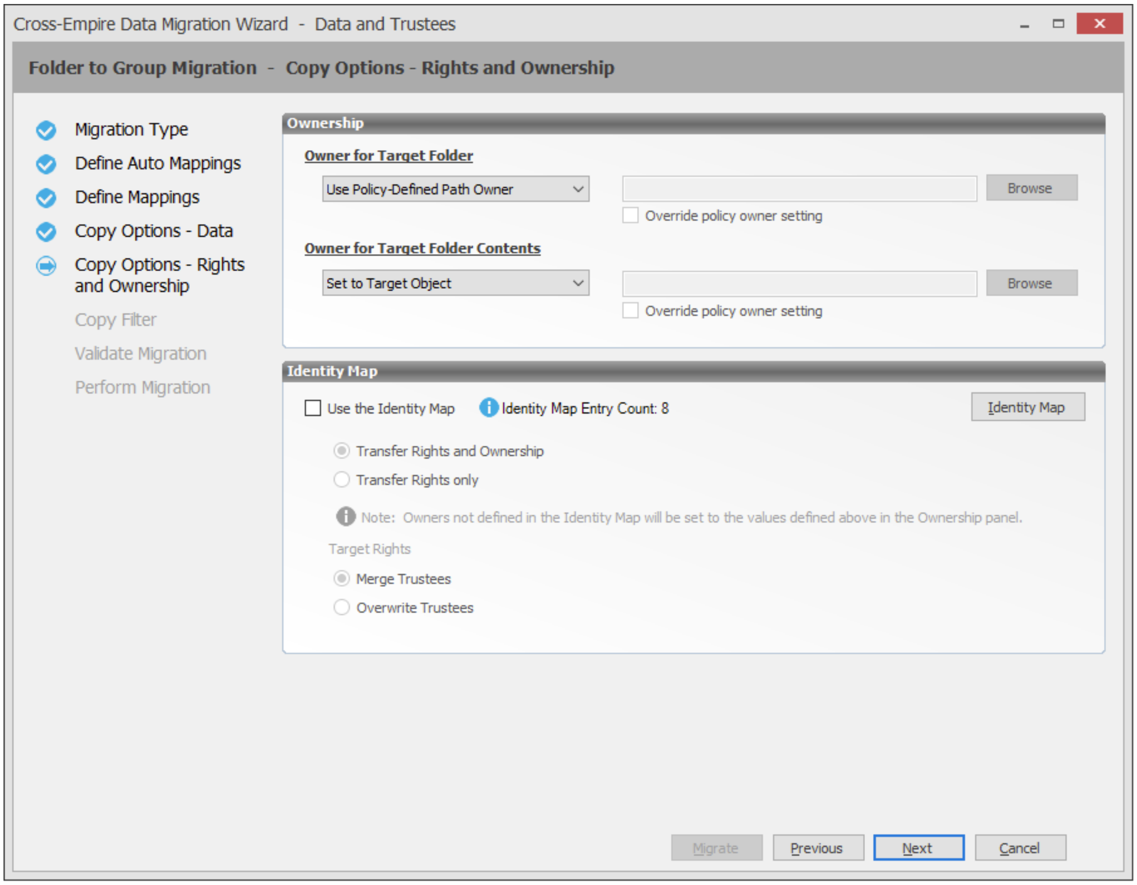
If you are migrating folder data to Active Directory objects that do not have policy associations, deselect this check box.

**Overwrite Options:** Indicate what you want to take place when duplicate filenames are encountered in the source and target.

**Directory Quota:** Specify how quota settings from the source Novell or Micro Focus file system should be applied after the migration.

**Target Subfolder:** If you want migrated data to be placed in a subfolder, select the **Use subfolder** check box and specify the subfolder name in the field.

15 Click **Next**.



Cross-Empire Data Migration Wizard - Data and Trustees

Folder to Group Migration - Copy Options - Rights and Ownership

- Migration Type
- Define Auto Mappings
- Define Mappings
- Copy Options - Data
- Copy Options - Rights and Ownership
- Copy Filter
- Validate Migration
- Perform Migration

Ownership

Owner for Target Folder: Use Policy-Defined Path Owner [Browse]
□ Override policy owner setting

Owner for Target Folder Contents: Set to Target Object [Browse]
□ Override policy owner setting

Identity Map

□ Use the Identity Map — Identity Map Entry Count: 8 [Identity Map]

● Transfer Rights and Ownership
○ Transfer Rights only

Note: Owners not defined in the Identity Map will be set to the values defined above in the Ownership panel.

Target Rights
● Merge Trustees
○ Overwrite Trustees

**16** Fill in the following fields:

**Owner for Target Folder:** Use these settings to specify how ownership of the migrated folder is determined.

If you selected the **Require use of Policies for target objects** check box in the previous wizard page, only the **Use Policy-Defined Path Owner** and **Set Explicit Owner** options are available on the drop-down menu.

- **Use Operating System Defaults:** This default setting allows the target Microsoft Windows Server to adjust the file ownership according to the settings on the target server.
- **Set to Target Object:** Specifies the target object as the owner of the migrated files. If the policy specifies a different owner, the policy's owner is applied.
- **Use Policy-Defined Path Owner:** Ownership of the files is determined according to the settings in the Storage Manager policy associated with the container where the object is managed.
- **Set Explicit Owner:** Allows you to browse and select an object as the explicit owner of the migrated folder, unless the policy specifies another object as the owner. To override the policy's configuration, select the **Override policy owner setting** check box.

**Owner for Target Folder Contents:** Use these settings to specify how ownership of the migrated folder contents is determined.

If you selected the **Require use of Policies for target objects** check box in the previous wizard page, only the **Set to Target Object** and **Set Explicit Owner** options are available on the drop-down menu.

- **Use Operating System Defaults:** This default setting allows the target Microsoft Windows Server to adjust the file ownership according to the settings on the target server.
- **Set to Target Object:** Specifies the target object as the owner of the migrated files. If the policy specifies a different owner, the policy's owner is applied.
- **Set Explicit Owner:** Allows you to browse and select an object as the explicit owner of the migrated files, unless the policy specifies another object as the owner. To override the policy's configuration, select the **Override policy owner setting** check box.

**Use the Identity Map:** Selecting this check box indicates that you want Storage Manager to utilize the identity map you created earlier and use the corresponding IDs to copy security rights and file ownership from the Novell or Micro Focus network file system to the Windows network file system.

- **Transfer Rights and Ownership:** Selecting this option indicates that you want to transfer the file and folder security rights along with the ownership settings.

  Be aware that when you transfer the ownership of a file or folder in a Windows network, you are granting the owner Full Rights, which you might not want to provide.
- **Transfer Rights Only:** Selecting this option indicates that you want to transfer only the file and folder security rights.
- **Overwrite Trustees:** Selecting this option indicates that you want any existing trustee assignments for a target file or folder to be overridden by the established eDirectory trustee assignments for those files and folders.
- **Merge Trustees:** Selecting this option indicates that you want the established eDirectory trustee assignments merged with those of the target files or folders in the Windows network file system.

**Identity Map:** Clicking this button opens your identity map where you can make any desired changes.

**17** Click **Next**.

**18** (Conditional) If you want to use a filter to include or exclude specific files, select the **Use Copy Filter** check box and click the **Add** button.

**18a** Fill in the following fields:

**Description:** Specify a description of the filter.

**Action:** From the drop-down menu, select either **Migrate** or **Ignore**, based on whether the filter specifies to migrate files or folders or to ignore them.

**Files, Folders:** Specify if the filter applies to files or folders.

**Masks:** List the file types to migrate or ignore.

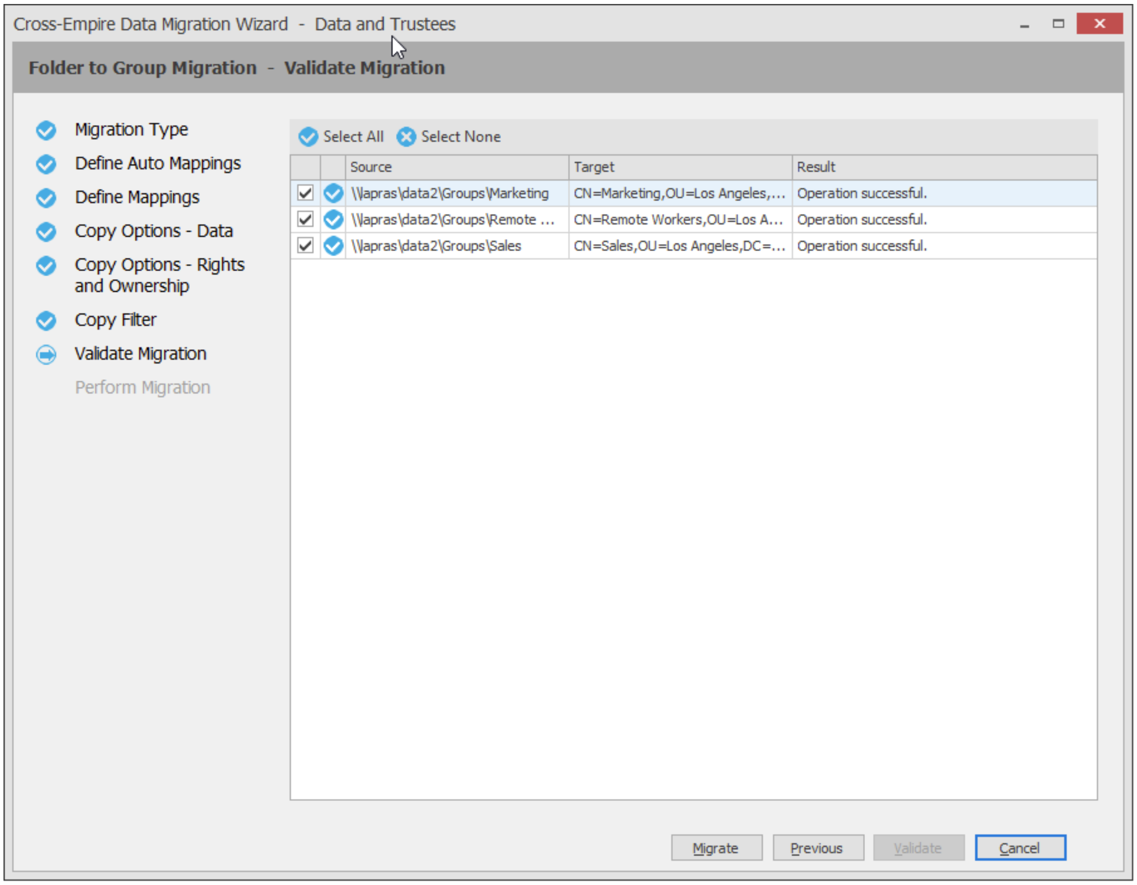
**18b** Specify any additional filter criteria in the menus and fields that remain.

For a detailed explanation of this region of the dialog box, see Section 6.5.8, "Setting Vault Rules," on page 58.

**18c** Click **OK**.

**19** Click **Validate**.

**Validate** shows the result of certain checks that can be run prior to the migration. The **Result** column shows the status of the validation checks. If errors are displayed, you can choose to correct those errors prior to running the migration.



| | | Source | Target | Result |
|---|---|---|---|---|
| ☑ | ✓ | \\apras\data2\Groups\Marketing | CN=Marketing,OU=Los Angeles,... | Operation successful. |
| ☑ | ✓ | \\apras\data2\Groups\Remote ... | CN=Remote Workers,OU=Los A... | Operation successful. |
| ☑ | ✓ | \\apras\data2\Groups\Sales | CN=Sales,OU=Los Angeles,DC=... | Operation successful. |

**20** (Conditional) Take any needed action that needs to be corrected and click **Previous** and then **Validate** again.

**21** Click **Migrate**.

A page appears with details of the data migration events that are queued for processing. To view the status of migration events, click **Pending Events**. For more information on Pending Events, see Section 13.1.7, “Events,” on page 274.

**22** Click **Finish** to close the Data Migration Wizard.

# 10.12 Performing a Folder to Folder Migration

A folder to folder migration has flexible target specification options that are not available in the other migration options. When you perform a folder to folder migration, you can either specify an existing target folder or create a target folder in the Data Migration Wizard. You can also decide whether to migrate all of the files at once, or skip some files and migrate them later.

The preferred time for performing a folder to folder migration is when all files located in the folders to be migrated are closed, such as during the weekend. However, if you have large data sets to migrate, some folder to folder migrations might need to be started during the week, when some of the files intended for migration are open. In cases such as these, we recommend a two-phased folder to folder migration:

**Migrating Unopened Files:** While users are still logged in, you migrate all of the unopened files in the source location. This will be the vast majority of your network files. Because the **Skip Open Files** option is selected, open files are not migrated, but the filenames and paths of all of the open files are logged in a text file.

---

**NOTE:** If you perform a Cross-Empire Data Migration when all users are logged off, you do not need to migrate skipped files.

---

**Migrating Skipped, New, and Modified Files:** After having all users log off or all previously open files have been closed, migrate the skipped files, migrate the new and modified files, then compare the files on the source and target servers to verify that everything migrated correctly.

- Section 10.12.1, "Determine Whether You Will Be Migrating to an Existing Target Folder or Creating a Target Folder During the Migration," on page 181
- Section 10.12.2, "Migrating to an Existing Target Folder," on page 181
- Section 10.12.3, "Scanning the Source Server for New or Modified Directories and Files," on page 192
- Section 10.12.4, "Migrating the New and Modified Directories and Files," on page 195
- Section 10.12.5, "Verifying that All Directories and Files were Migrated by Comparing Source Server and Target Server Contents," on page 198
- Section 10.12.6, "Creating a Target Folder in the Data Migration Wizard," on page 200

## 10.12.1 Determine Whether You Will Be Migrating to an Existing Target Folder or Creating a Target Folder During the Migration

You have the option of migrating data to an existing target folder on the target server, or creating the target folder on the target server during the migration. The procedures differ for both, so at this point you must decide and then follow the appropriate procedures.

If you are plan to migrate folder data to an existing target folder on the target server, proceed with Section 10.12.2, "Migrating to an Existing Target Folder," on page 181.

If you plan to migrate folder data to a target folder that you create during the migration, proceed with Section 10.12.6, "Creating a Target Folder in the Data Migration Wizard," on page 200.

## 10.12.2 Migrating to an Existing Target Folder

- "Migrating Unopened Files" on page 181
- "Migrating Skipped Files" on page 188

### Migrating Unopened Files

1 Make sure you have completed the prerequisites and have created a migration proxy account.

  For more information on the prerequisites, see Section 10.3, "Prerequisites," on page 130. For more information on creating a migration proxy account, see Section 10.4, "Creating the Migration Proxy Account," on page 131.

**2** (Conditional) If you want to migrate closed files now and skip some files to migrate later:

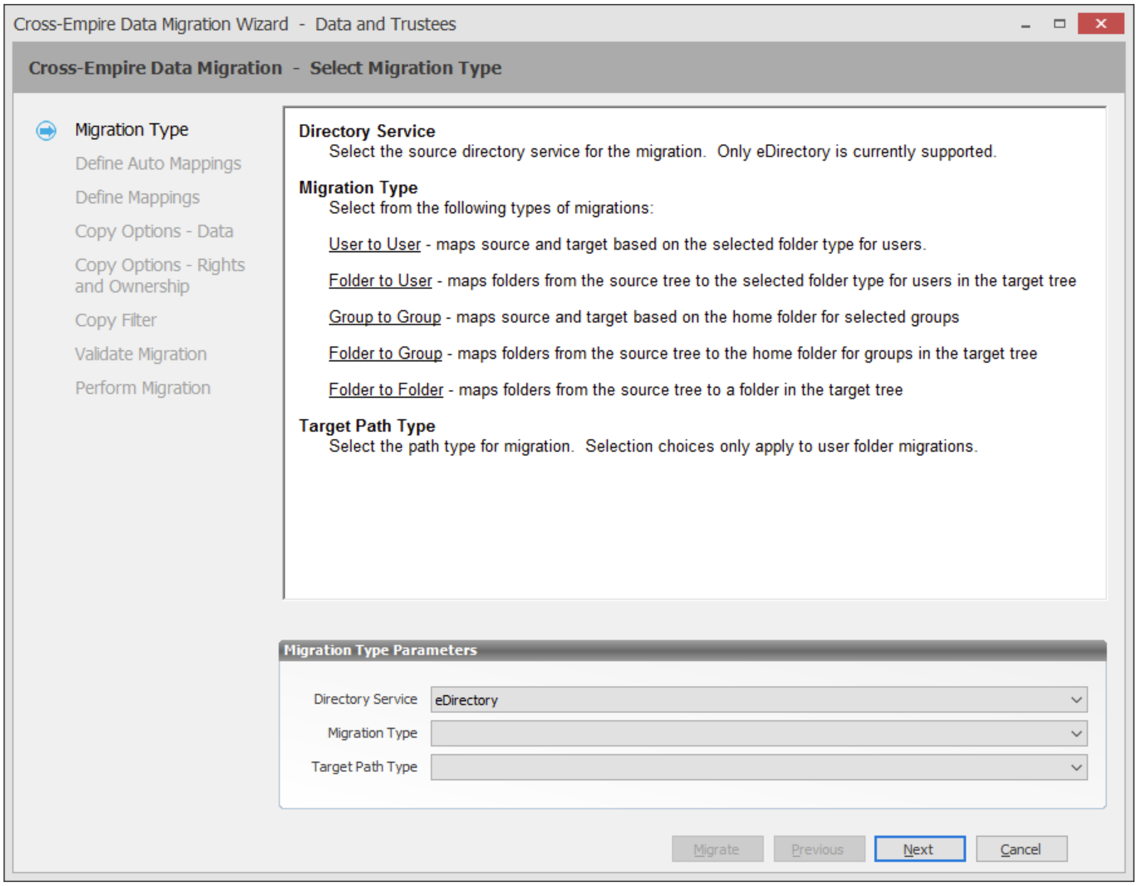
**2a** From the `Utilities\CEDM` folder on the Storage Manager ISO image, copy the `CEDMScanCompare.exe` utility to either the Windows target server or to a Windows server where you are going to administer the migration.

**2b** On each NetWare or Open Enterprise Server from which you are going to migrate data, create a new subdirectory and name it `Open`.

**3** In SMAdmin, click the **Home** tab.

**4** Select **Cross-Empire Data Migrations** > **eDirectory to Active Directory**.

**5** Select **Migration Wizards** > **Data and Security**.



Cross-Empire Data Migration Wizard - Data and Trustees

**Cross-Empire Data Migration - Select Migration Type**

**Directory Service**
Select the source directory service for the migration. Only eDirectory is currently supported.

**Migration Type**
Select from the following types of migrations:

User to User - maps source and target based on the selected folder type for users.

Folder to User - maps folders from the source tree to the selected folder type for users in the target tree

Group to Group - maps source and target based on the home folder for selected groups

Folder to Group - maps folders from the source tree to the home folder for groups in the target tree

Folder to Folder - maps folders from the source tree to a folder in the target tree

**Target Path Type**
Select the path type for migration. Selection choices only apply to user folder migrations.

**Migration Type Parameters**

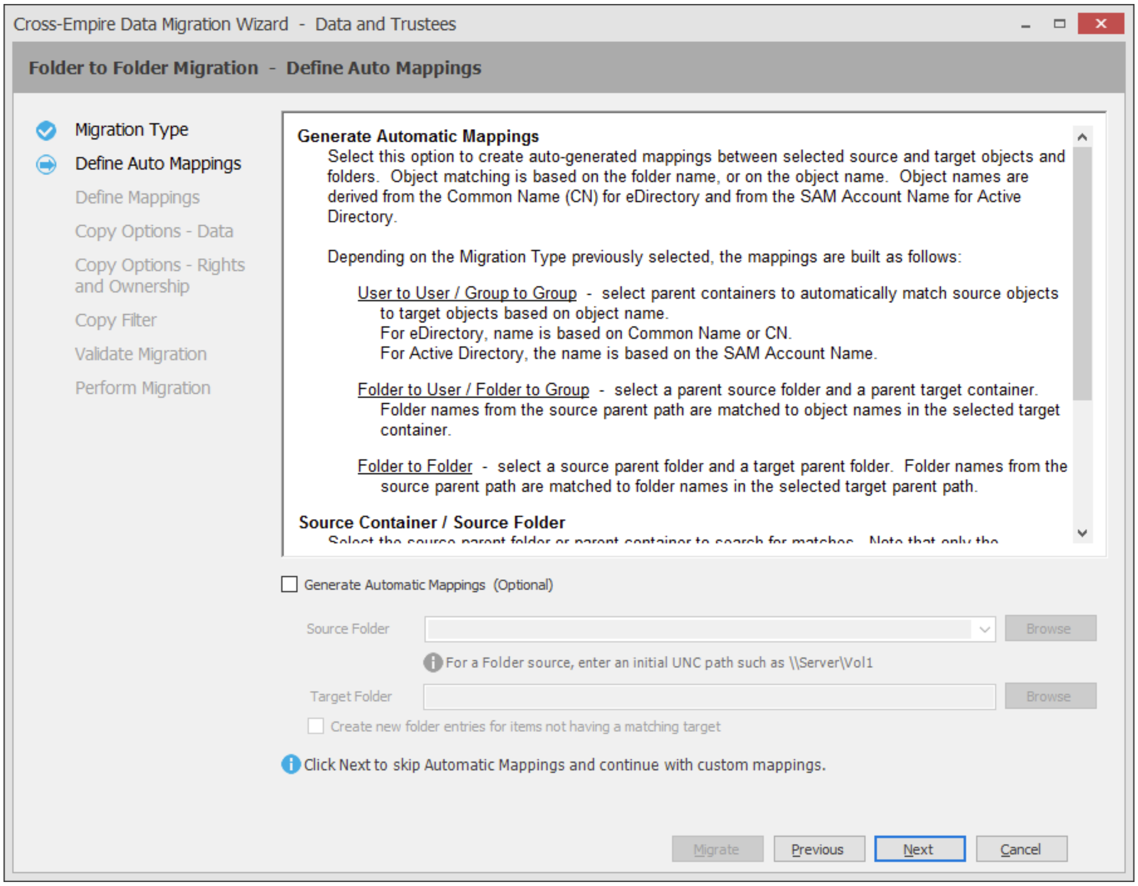
Directory Service: eDirectory

Migration Type:

Target Path Type:

**6** From the **Migration Type** drop-down menu, select **Folder to Folder.**

**7** Click **Next**.



**Generate Automatic Mappings**

Select this option to create auto-generated mappings between selected source and target objects and folders. Object matching is based on the folder name, or on the object name. Object names are derived from the Common Name (CN) for eDirectory and from the SAM Account Name for Active Directory.

Depending on the Migration Type previously selected, the mappings are built as follows:

User to User / Group to Group - select parent containers to automatically match source objects to target objects based on object name.
For eDirectory, name is based on Common Name or CN.
For Active Directory, the name is based on the SAM Account Name.

Folder to User / Folder to Group - select a parent source folder and a parent target container. Folder names from the source parent path are matched to object names in the selected target container.

Folder to Folder - select a source parent folder and a target parent folder. Folder names from the source parent path are matched to folder names in the selected target parent path.

**Source Container / Source Folder**

Select the source parent folder or parent container to search for matches. Note that only the

□ Generate Automatic Mappings (Optional)

Source Folder

For a Folder source, enter an initial UNC path such as \\Server\Vol1

Target Folder

□ Create new folder entries for items not having a matching target

Click Next to skip Automatic Mappings and continue with custom mappings.

8 Fill in the following fields:

**Generate Automatic Mappings:** Select this check box to activate the other fields.

**Source Folder:** Specify an initial UNC path for a server and volume to browse.

For example, `\\server_name\volume_name\` or `\\ip_address\volume_name`.

After a path is entered, you can click the **Browse** button to browse to the folder you want.

**Target Folder:** Browse to select the target folder.

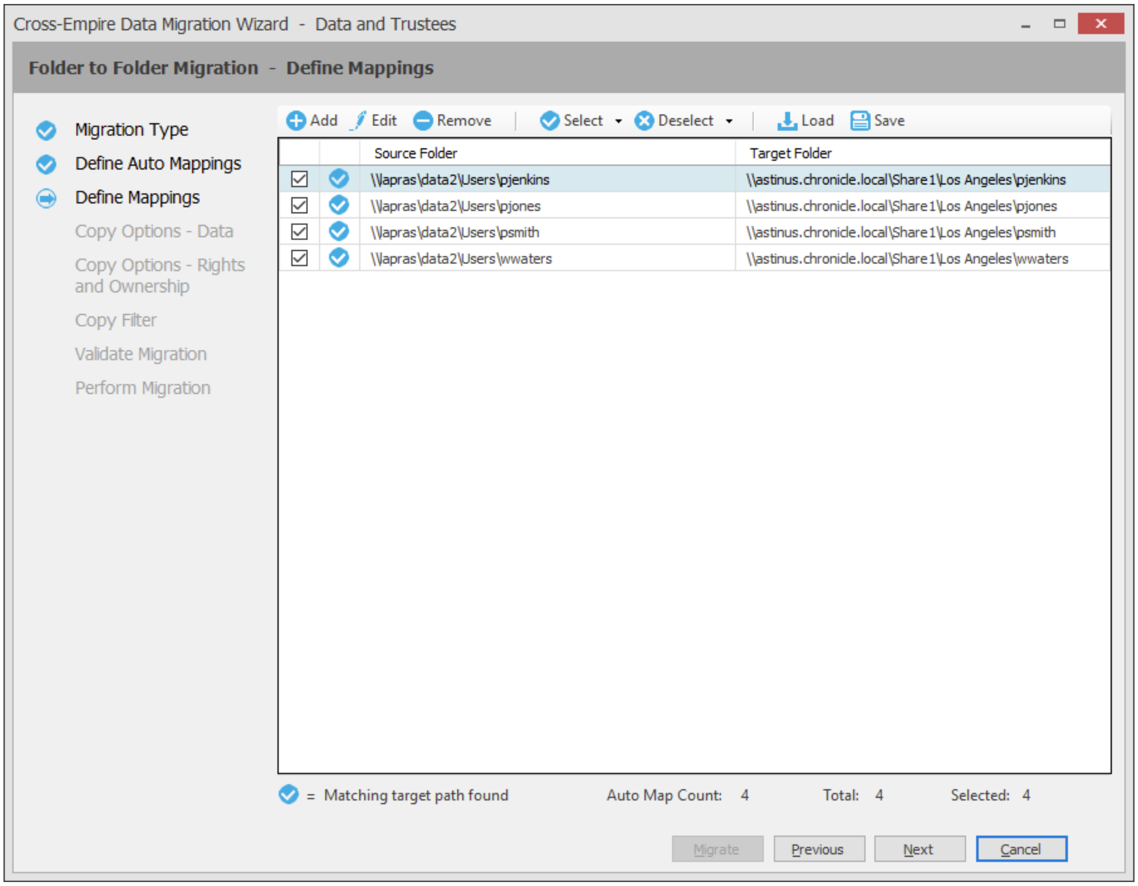
**Create new folder entries for items not having a matching target:** Selecting this check box indicates that you want Storage Manager to display both matching and non-matching source and target folders.

Selecting this check box also indicates that you want Storage Manager to create and populate any subfolders that do not exist in the target folder.

For example, assume that the source path at `\\10.10.10.233\Vol2\Projects` is being migrated to `\\Corpserver\Projects` and the `Projects` directory on the source server has a `Stategov` subfolder. If there is no `Stategov` subfolder in the target folder, a `Stategov` subdirectory is created to include the directory contents.

9 Click **Next**.

The Data Migration Wizard attempts to match the names of the subfolders of the source path with the subfolders of the specified target directory. If there is a match, the listed folder in the **Source Folder** field is selected and a corresponding match is listed in the **Target Folder** column.



Cross-Empire Data Migration Wizard - Data and Trustees

Folder to Folder Migration - Define Mappings

- Migration Type
- Define Auto Mappings
- Define Mappings
- Copy Options - Data
- Copy Options - Rights and Ownership
- Copy Filter
- Validate Migration
- Perform Migration

| | | Source Folder | Target Folder |
|---|---|---|---|
| ☑ | ✓ | \\lapras\data2\Users\pjenkins | \\astinus.chronicle.local\Share1\Los Angeles\pjenkins |
| ☑ | ✓ | \\lapras\data2\Users\pjones | \\astinus.chronicle.local\Share1\Los Angeles\pjones |
| ☑ | ✓ | \\lapras\data2\Users\psmith | \\astinus.chronicle.local\Share1\Los Angeles\psmith |
| ☑ | ✓ | \\lapras\data2\Users\wwaters | \\astinus.chronicle.local\Share1\Los Angeles\wwaters |

✓ = Matching target path found    Auto Map Count: 4    Total: 4    Selected: 4

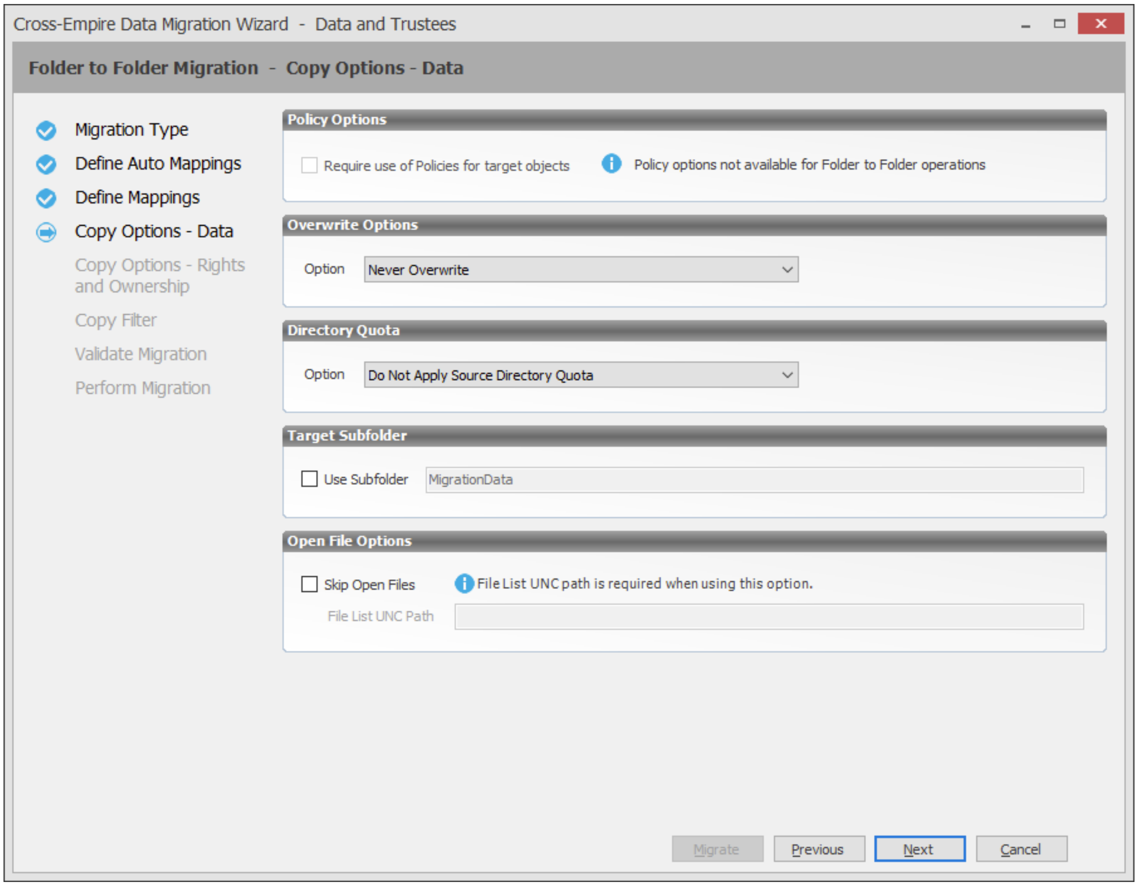
**10** Specify a target folder for each source folder that is not automatically matched by double-clicking the name to bring up the Modify Data Map Entry dialog box.

**11** Click **Browse**, specify the target folder, then click **OK**.

The target folder is placed in the **Target Folder** column.

**12** Click the check box corresponding to the listing with the new target.

**13** When all of the folders you want to migrate are selected and have an associated target folder, click **Next**.



Policy Options

□ Require use of Policies for target objects

Policy options not available for Folder to Folder operations

Overwrite Options

Option: Never Overwrite

Directory Quota

Option: Do Not Apply Source Directory Quota

Target Subfolder

□ Use Subfolder: MigrationData

Open File Options

□ Skip Open Files

File List UNC path is required when using this option.

File List UNC Path:

**14** Fill in the following fields:

**Overwrite Options:** Indicate what you want to take place when duplicate filenames are encountered in the source and target.

**Directory Quota:** Specify how quota settings from the source NSS file system should be applied after the migration.

**Target Subfolder:** If you want migrated data to be placed in a subfolder, select the **Use subfolder** check box and specify the subfolder name in the field.

**Open File Options:** If you want the Cross-Empire Data Migration subsystem to skip all open files on the network and not migrate them, select **Skip Open Files**.

Selecting **Skip Open Files** activates the **File List UNC Path** field where you specify the name and location of the log file listing all of the open files that are skipped during the migration.

Specify the UNC path for the `Open` directory you created along with a filename for the text file that will list the skipped files.

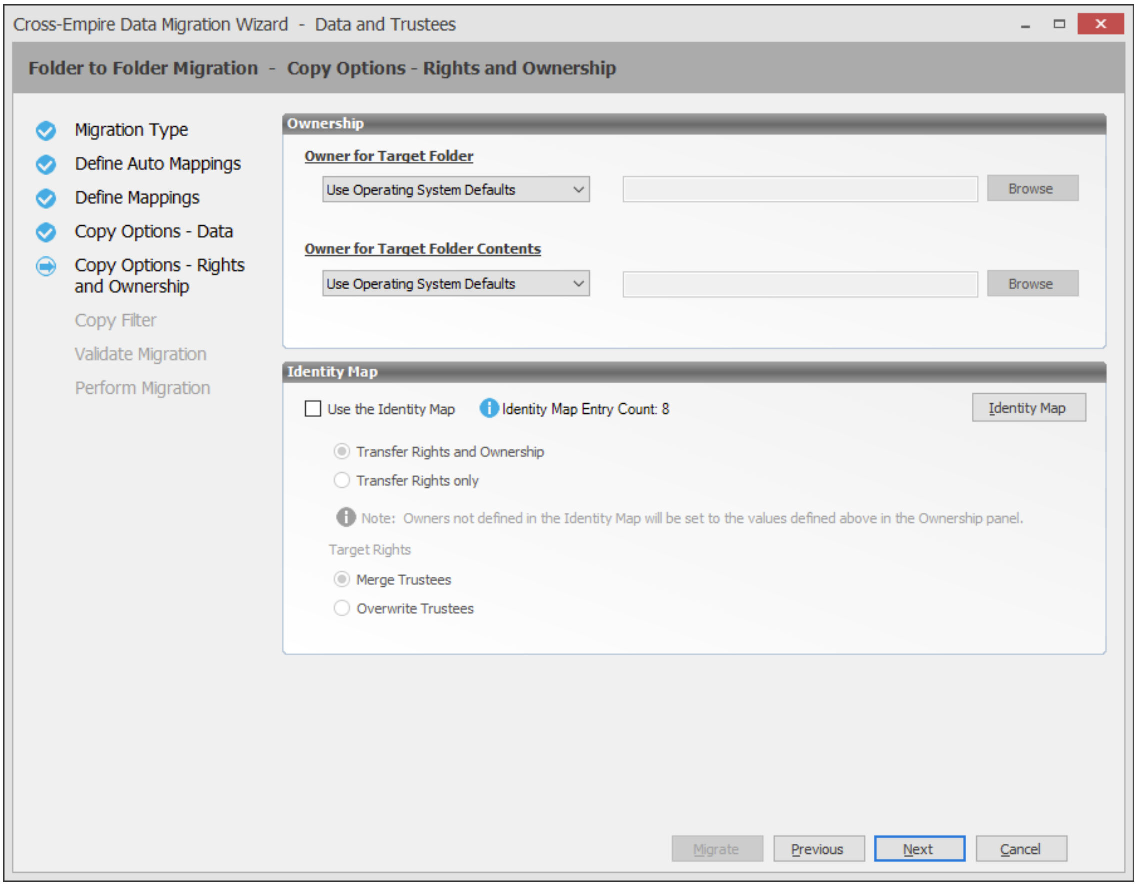
For example, `\\server_name\volume_name\directory_name\Open\skip.txt`

or

`\\ip_address\volume_name\Open\skip.txt`

The Cross-Empire Data Migration subsystem does not validate the path, so you must make sure that the path entered is correct. Otherwise, the migration fails.

**15** Click **Next**.



Cross-Empire Data Migration Wizard - Data and Trustees

Folder to Folder Migration - Copy Options - Rights and Ownership

- Migration Type
- Define Auto Mappings
- Define Mappings
- Copy Options - Data
- Copy Options - Rights and Ownership
- Copy Filter
- Validate Migration
- Perform Migration

Ownership

Owner for Target Folder: Use Operating System Defaults

Owner for Target Folder Contents: Use Operating System Defaults

Identity Map

□ Use the Identity Map

Identity Map Entry Count: 8

○ Transfer Rights and Ownership
○ Transfer Rights only

Note: Owners not defined in the Identity Map will be set to the values defined above in the Ownership panel.

Target Rights

○ Merge Trustees
○ Overwrite Trustees

16 Fill in the following fields:

**Owner for Target Folder:** Use these settings to specify how ownership of the migrated folder is determined.

- **Use Operating System Defaults:** This default setting allows the target Microsoft Windows Server to adjust the file ownership according to the setting on the target server.
- **Set Explicit Owner:** Allows you to browse and select an object as the explicit owner of the migrated folder.

**Owner for Target Folder Contents:** Use these settings to specify how ownership of the migrated folder contents is determined.

- **Use Operating System Defaults:** This default setting allows the target Microsoft Windows Server to adjust the file ownership according to the settings on the target server.
- **Set Explicit Owner:** Allows you to browse and select an object as the explicit owner of all of the migrated files.

**Use the Identity Map:** Select this check box if you want Storage Manager to utilize the identity map you created earlier and use the corresponding IDs to copy security rights and file ownership from the Novell or Micro Focus network file system to the Windows network file system.

- **Transfer Rights and Ownership:** Select this option if you want to transfer the file and folder security rights along with the ownership settings.

  Be aware that when you transfer the ownership of a file or folder in a Windows network, you are granting the owner Full Rights, which you might not want to provide.
- **Transfer Rights Only:** Select this option to transfer only the file and folder security rights.
- **Overwrite Trustees:** Select this option to override any existing trustee assignments for a target file or folder with the established eDirectory trustee assignments for those files and folders.
- **Merge Trustees:** Select this option to merge the established eDirectory trustee assignments with those of the target files or folders in the Windows network file system.

**Identity Map:** Clicking this button opens your identity map where you can make any desired changes.

**17** Click **Next**.

**18** (Conditional) If you want to use a filter to include or exclude specific files, select the **Use Copy Filter** check box and click the **Add** button.

**18a** Fill in the following fields:

**Description:** Specify a description of the filter.

**Action:** From the drop-down menu, select either **Migrate** or **Ignore**, based on whether the filter specifies to migrate files or folders or to ignore them.

**Files, Folders:** Specify if the filter applies to files or folders.

**Masks:** List the file types to migrate or ignore.

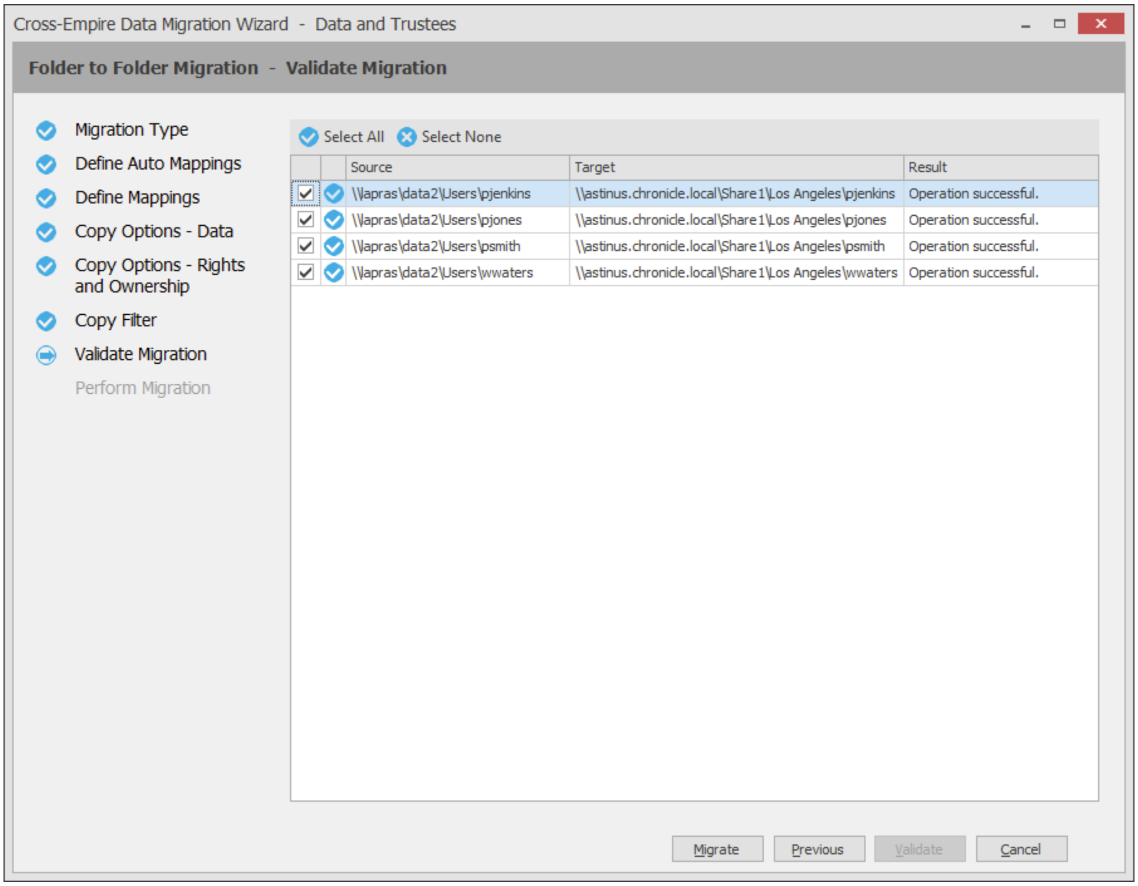
**18b** Specify any additional filter criteria in the menus and fields that remain.

For a detailed explanation of this region of the dialog box, see Section 6.5.8, “Setting Vault Rules,” on page 58.

**18c** Click **OK**.

**19** Click **Validate**.

**Validate** shows the result of certain checks that can be run prior to the migration. The **Result** column shows the status of the validation checks. If errors are displayed, you can choose to correct those errors prior to running the migration.



| | | Source | Target | Result |
|---|---|---|---|---|
| ☑ | ✓ | \\apras\data2\Users\pjenkins | \\astinus.chronicle.local\Share1\Los Angeles\pjenkins | Operation successful. |
| ☑ | ✓ | \\apras\data2\Users\pjones | \\astinus.chronicle.local\Share1\Los Angeles\pjones | Operation successful. |
| ☑ | ✓ | \\apras\data2\Users\psmith | \\astinus.chronicle.local\Share1\Los Angeles\psmith | Operation successful. |
| ☑ | ✓ | \\apras\data2\Users\wwaters | \\astinus.chronicle.local\Share1\Los Angeles\wwaters | Operation successful. |

20 (Conditional) Take any necessary corrective action, click **Previous** and then click **Validate** again.

21 Click **Migrate**.

A page appears with details of the data migration events that are queued for processing. To view the status of migration events, click **Events**. For more information on Pending Events, see Section 13.1.7, “Events,” on page 274.

22 Do one of the following:

- If you skipped some files to migrate later, click **Finish** and then continue with “Migrating Skipped Files” on page 188.
- If you have migrated all of your data, click **Finish**.

  You are now finished with the folder to folder migration.

## Migrating Skipped Files

The second phase of a folder to folder data migration is conducted when all of the users are logged off the network, so all network files are closed.

1 Have everyone log off the network so that there are no open files on the source NetWare or Open Enterprise Server machines.

2 Open the text file that you created in Step 14 on page 185 and view the files that were skipped.

Do not make any changes to the file. Doing so causes errors during the migration.

3 Save a copy of the text file.

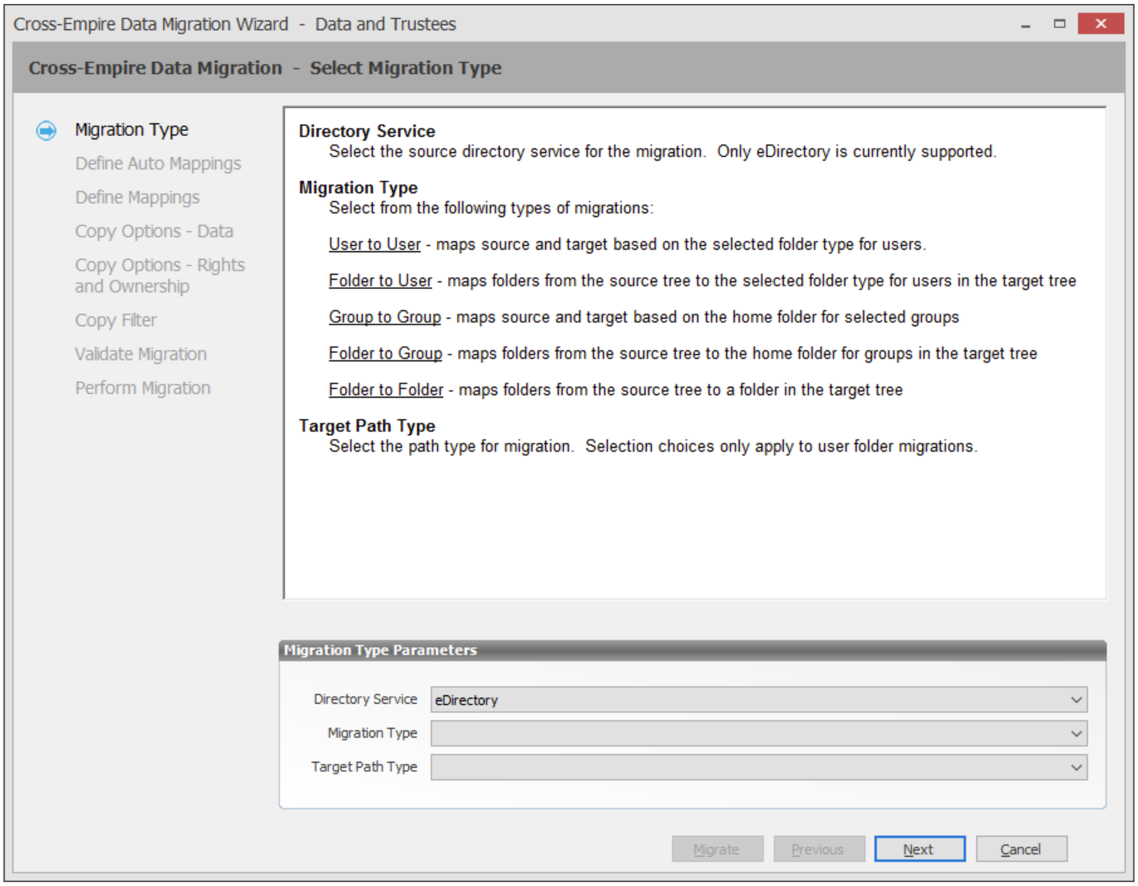
For example, if you named the file `skip.txt`, save a copy as `skip_copy.txt`.

After the Cross-Empire Data Migration subsystem migrates the skipped files, it deletes the text file. You can use the copy to verify that the files were migrated.

4 In SMAdmin, click the **Home** tab.

5 Select **Cross-Empire Data Migrations** > **eDirectory to Active Directory**.

6 Select **Migration Wizards** > **Data and Security**.


Cross-Empire Data Migration Wizard - Data and Trustees
Cross-Empire Data Migration - Select Migration Type
Migration Type
Define Auto Mappings
Define Mappings
Copy Options - Data
Copy Options - Rights and Ownership
Copy Filter
Validate Migration
Perform Migration
Migration Type Parameters
Migrate
Previous
Next
Cancel

**Directory Service**
Select the source directory service for the migration. Only eDirectory is currently supported.

**Migration Type**
Select from the following types of migrations:

User to User - maps source and target based on the selected folder type for users.

Folder to User - maps folders from the source tree to the selected folder type for users in the target tree

Group to Group - maps source and target based on the home folder for selected groups

Folder to Group - maps folders from the source tree to the home folder for groups in the target tree

Folder to Folder - maps folders from the source tree to a folder in the target tree

**Target Path Type**
Select the path type for migration. Selection choices only apply to user folder migrations.

Directory Service: eDirectory
Migration Type:
Target Path Type:

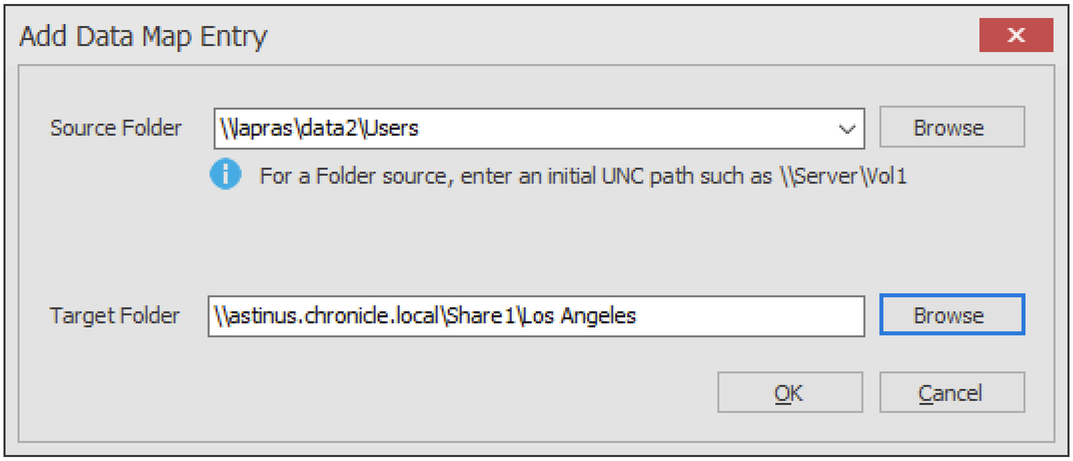
7 From the **Migration Type** drop-down menu, select **Delta File**.

8 Click **Next**.

9 Skip the Automatic Mappings settings by clicking **Next**.

10 On the Define Mappings wizard page, click **Add**.

11 In the Add Data Entry dialog box, browse to and select the source and target folders.



Add Data Map Entry

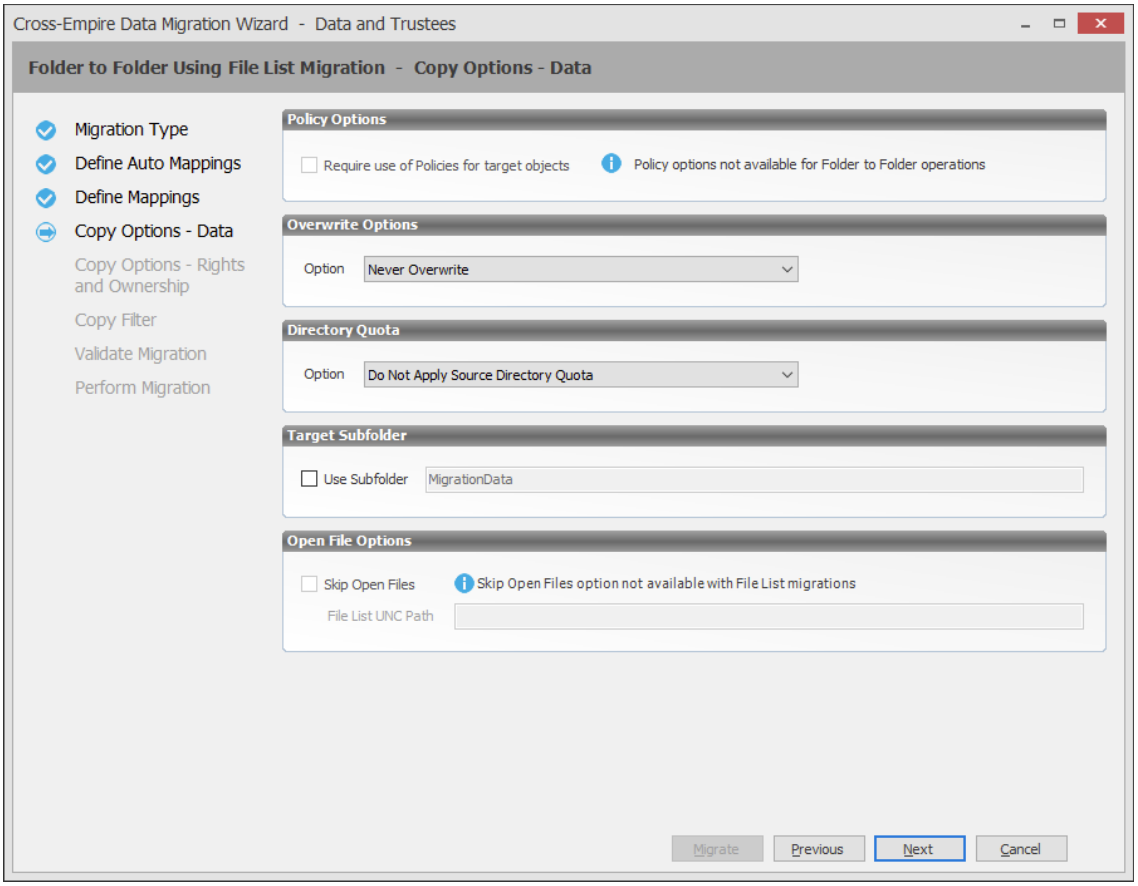
Source Folder: \\apras\data2\Users

For a Folder source, enter an initial UNC path such as \\Server\Vol1

Target Folder: \\astinus.chronicle.local\Share1\Los Angeles

12 Click **OK**.

13 On the Define Mappings wizard page, verify the source folder and the destination folder and click **Next**.



Cross-Empire Data Migration Wizard - Data and Trustees

Folder to Folder Using File List Migration - Copy Options - Data

Policy Options

□ Require use of Policies for target objects

Policy options not available for Folder to Folder operations

Overwrite Options

Option: Never Overwrite

Directory Quota

Option: Do Not Apply Source Directory Quota

Target Subfolder

□ Use Subfolder: MigrationData

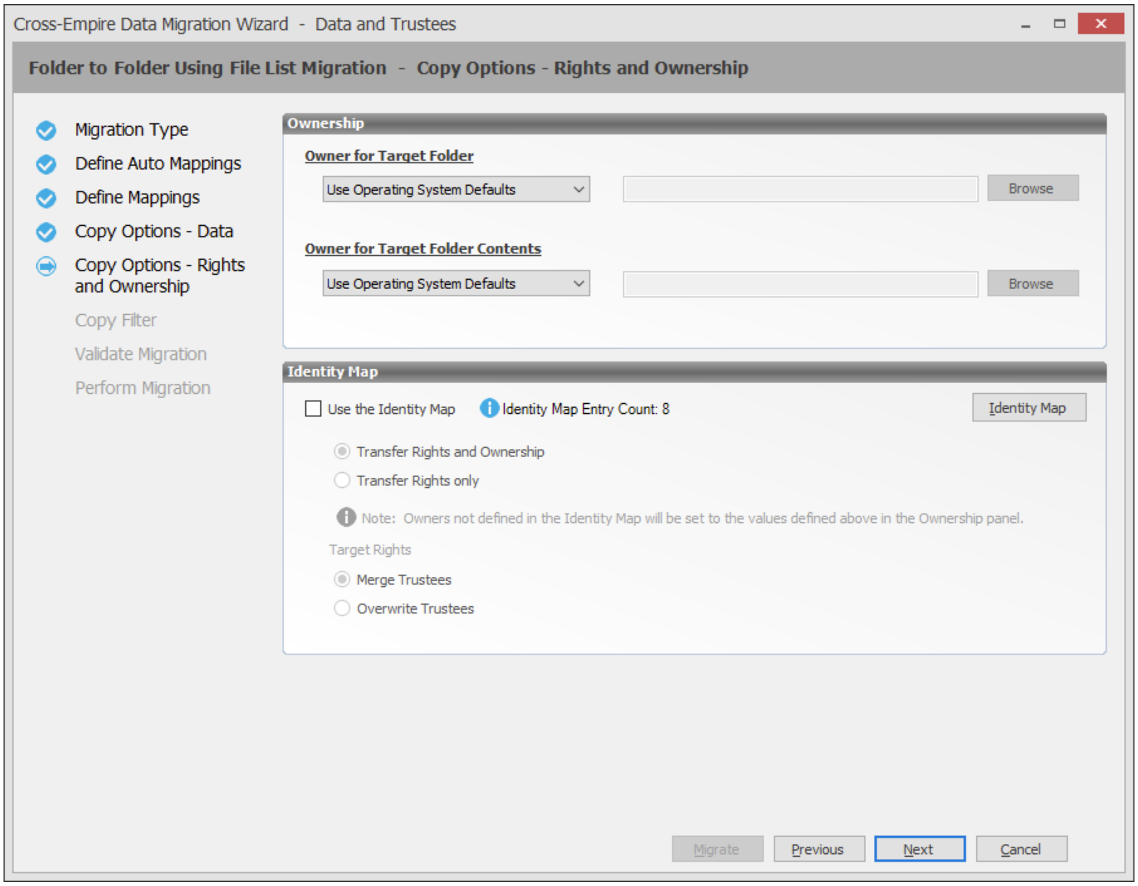
Open File Options

□ Skip Open Files

Skip Open Files option not available with File List migrations

File List UNC Path:

14 On the Copy Options - Data wizard page, from the **Option** drop-down menu in the **Overwrite Options** region, select **Overwrite if Newer** and click **Next**.



Cross-Empire Data Migration Wizard - Data and Trustees

Folder to Folder Using File List Migration - Copy Options - Rights and Ownership

Ownership

Owner for Target Folder: Use Operating System Defaults

Owner for Target Folder Contents: Use Operating System Defaults

Identity Map

□ Use the Identity Map

Identity Map Entry Count: 8

● Transfer Rights and Ownership
○ Transfer Rights only

Note: Owners not defined in the Identity Map will be set to the values defined above in the Ownership panel.

Target Rights

● Merge Trustees
○ Overwrite Trustees

15 (Optional) On the Copy Options - Rights and Owners wizard page, from the drop-down menu of the **Owner for Target Folder** region, select **Set Explicit Owner.**

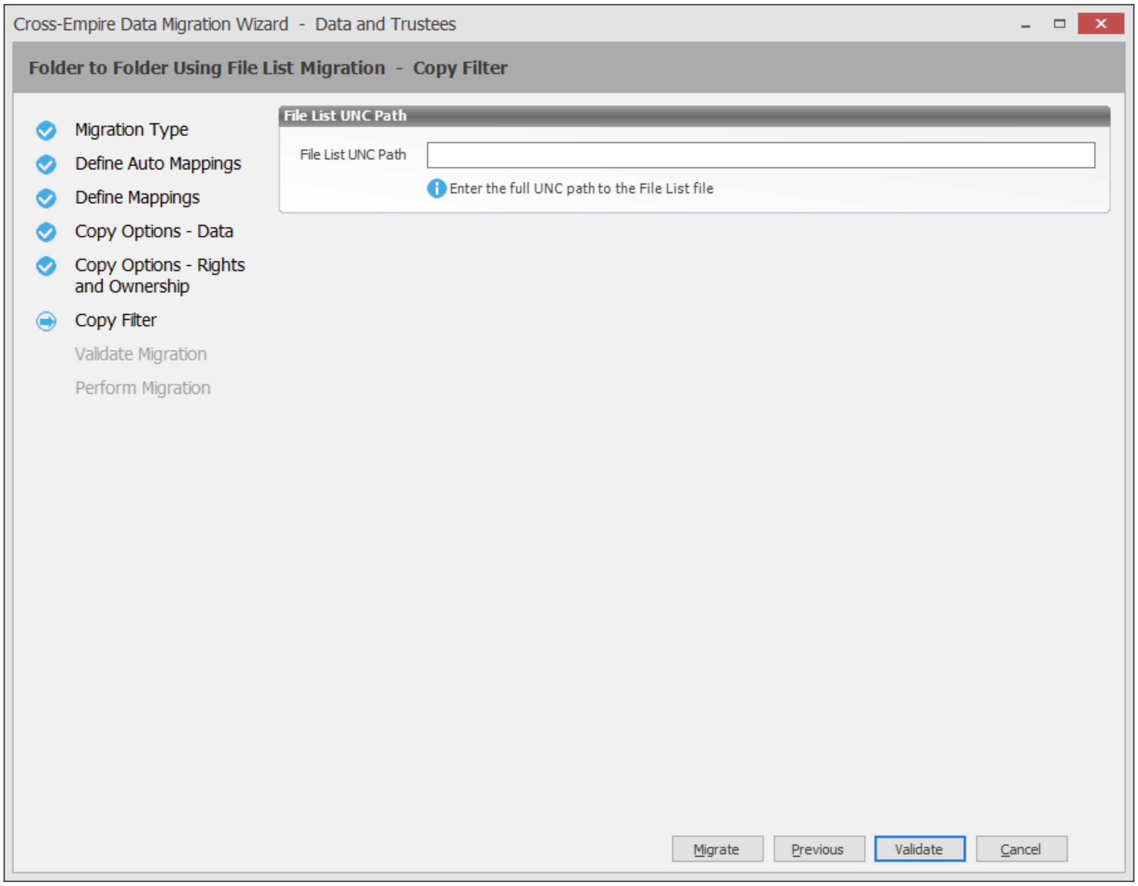
16 (Conditional) If you chose to set an explicit owner for the folder, click the corresponding **Browse** button and browse to specify an owner for the target folder.

17 (Optional) From the drop-down menu of the **Owner for Target Folder Contents** region, select **Set Explicit Owner**.

18 (Conditional) if you chose to set an explicit owner for the folder contents, click the corresponding **Browse** button and browse to specify an owner for the target folder contents.

19 Select the **Use Identity Map** check box and click **Next**.

20 On the Copy Filter wizard page, specify the UNC path to the file you created in Step 14 on page 185.



File List UNC Path

Enter the full UNC path to the File List file

21 Click **Validate** to confirm that the path is correct.

22 Click **Migrate**.

The skipped files are migrated and the text file that you created in Step 14 on page 185 is deleted.

23 Click **Finish**.

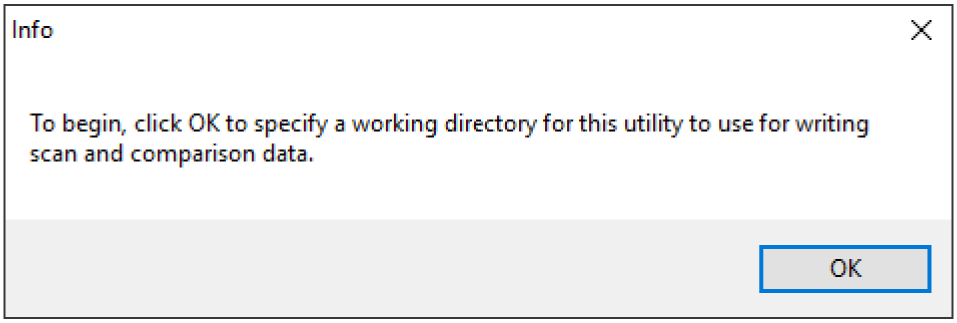
24 Continue with "Scanning the Source Server for New or Modified Directories and Files" on page 192.

## 10.12.3 Scanning the Source Server for New or Modified Directories and Files

Before you can migrate all of the new and modified directories and files since the first phase of the migration, you must first generate a list of these new and modified directories and files. This is done using the CEDMScanCompare utility.

1 Launch the CEDMScanCompare utility.

The following message appears:

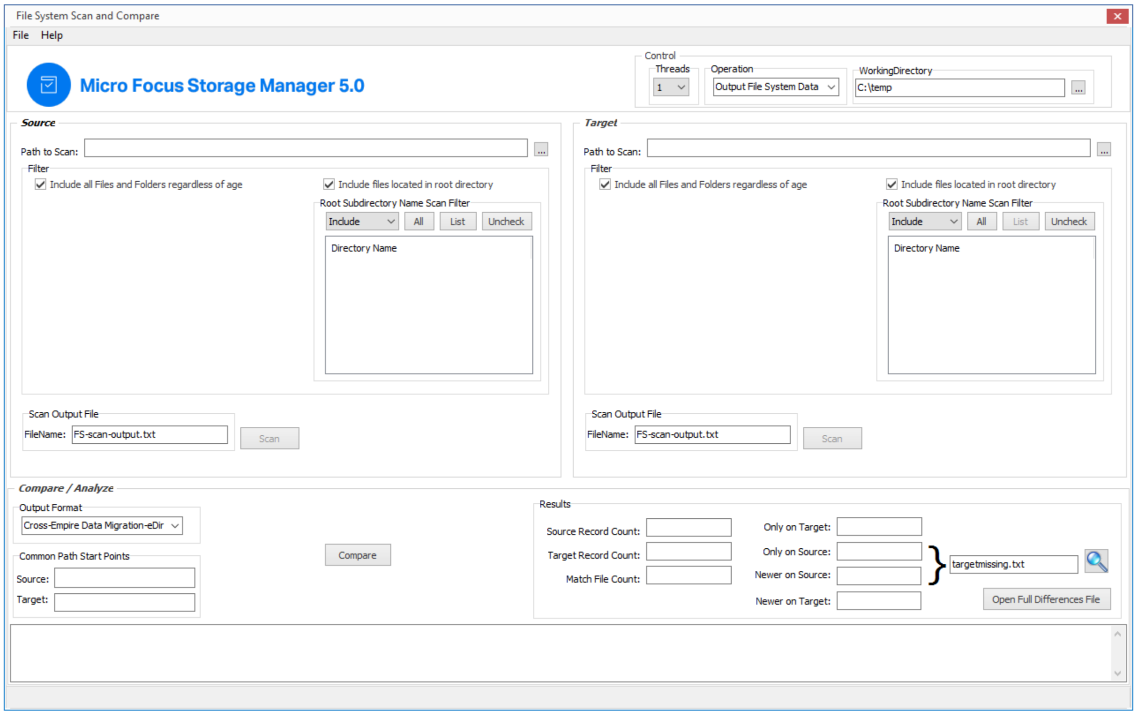


To begin, click OK to specify a working directory for this utility to use for writing scan and comparison data.

2 Click **OK**.

3 Browse to a folder where you want to store the comparison data and click **Select Folder**.

The CEDMScanCompare utility interface is launched.



Threads: 1

Operation: Output File System Data

WorkingDirectory: C:\temp

Source:

☑ Include all Files and Folders regardless of age

☑ Include files located in root directory

Include

FileName: FS-scan-output.txt

Target:

☑ Include all Files and Folders regardless of age

☑ Include files located in root directory

Include

FileName: FS-scan-output.txt

Output Format: Cross-Empire Data Migration-eDir

targetmissing.txt

The selected folder location is specified in the **Working Directory** field.

4 In the **Source** region, for the **Path to Scan** field, browse to specify the UNC path to the directory on the NetWare or Open Enterprise Server you want to scan.

For example: `\\oesnw\vol2\dept_shares`

You can scan both NetWare and OES Linux servers in your tree by using the above syntax. For example, to scan Vol2 of an OES Linux server, you would use a syntax like the following:

```
\\oeslinux\vol2
```

5 In the **Target** region, for the **Path to Scan** field, browse to specify the UNC path to the folder in the target forest you want to scan.

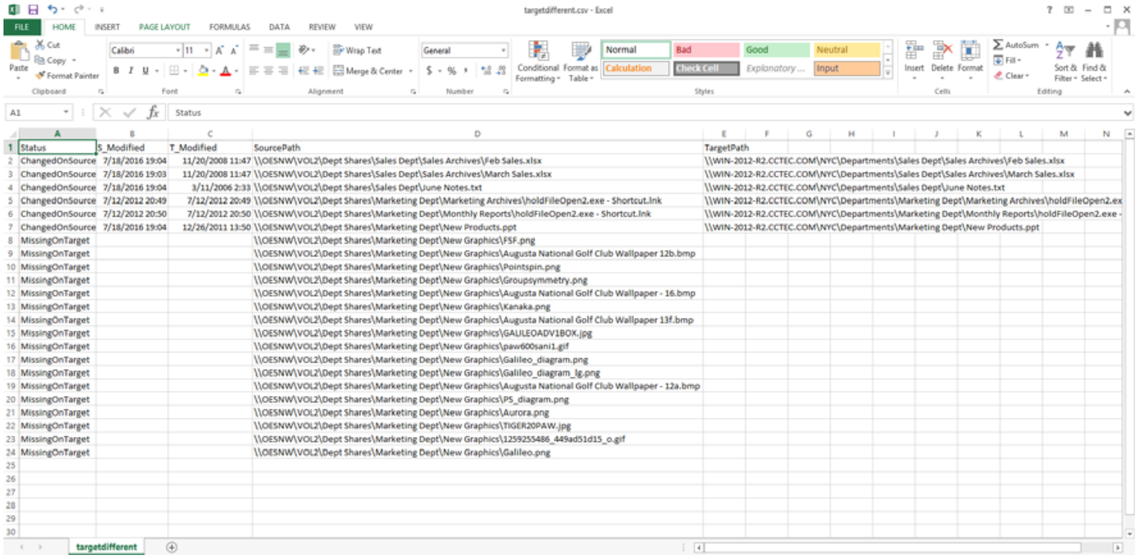
6 In the **Source** region, click **Scan**.

7 In the **Scan Result** region, note the findings in the **Folders** and **Files** fields.

8 In the **Target** region, click **Scan**.

9. In the **Scan Result** region, note the findings in the **Folders** and **Files** fields.
10. In the **Compare / Analyze** region, from the **FileName** drop-down menu, select **Cross-Empire Data Migration-eDir**.
11. Click **Compare**.
12. Do one of the following:
    - If the results show no discrepancies between the source and target, there are no new or modified directories and files. You are finished with the folder to folder data migration.
    - If the results show discrepancies between the source and target, follow the remaining procedures in this section.
13. Click **Open Full Differences File**.

    A spreadsheet appears listing:
    - All files on the source that are newer than the same named files on the target, along with the source and target path of each file.
    - All files on the source that are missing from the target.



| Status | S_Modified | T_Modified | SourcePath | TargetPath |
|---|---|---|---|---|
| ChangedOnSource | 7/18/2016 19:04 | 11/20/2008 11:47 | \\OESNW\VOL2\Dept Shares\Sales Dept\Sales Archives\Feb Sales.xlsx | \\WIN-2012-R2.CCTEC.COM\NYC\Departments\Sales Dept\Sales Archives\Feb Sales.xlsx |
| ChangedOnSource | 7/18/2016 19:03 | 11/20/2008 11:47 | \\OESNW\VOL2\Dept Shares\Sales Dept\Sales Archives\March Sales.xlsx | \\WIN-2012-R2.CCTEC.COM\NYC\Departments\Sales Dept\Sales Archives\March Sales.xlsx |
| ChangedOnSource | 7/18/2016 19:04 | 3/11/2006 2:33 | \\OESNW\VOL2\Dept Shares\Sales Dept\June Notes.txt | \\WIN-2012-R2.CCTEC.COM\NYC\Departments\Sales Dept\June Notes.txt |
| ChangedOnSource | 7/12/2012 20:49 | 7/12/2012 20:49 | \\OESNW\VOL2\Dept Shares\Marketing Dept\Marketing Archives\holdFileOpen2.exe - Shortcut.lnk | \\WIN-2012-R2.CCTEC.COM\NYC\Departments\Marketing Dept\Marketing Archives\holdFileOpen2.ex |
| ChangedOnSource | 7/12/2012 20:50 | 7/12/2012 20:50 | \\OESNW\VOL2\Dept Shares\Marketing Dept\Monthly Reports\holdFileOpen2.exe - Shortcut.lnk | \\WIN-2012-R2.CCTEC.COM\NYC\Departments\Marketing Dept\Monthly Reports\holdFileOpen2.exe - |
| ChangedOnSource | 7/18/2016 19:04 | 12/26/2011 13:50 | \\OESNW\VOL2\Dept Shares\Marketing Dept\New Products.ppt | \\WIN-2012-R2.CCTEC.COM\NYC\Departments\Marketing Dept\New Products.ppt |
| MissingOnTarget | | | \\OESNW\VOL2\Dept Shares\Marketing Dept\New Graphics\FSF.png | |
| MissingOnTarget | | | \\OESNW\VOL2\Dept Shares\Marketing Dept\New Graphics\Augusta National Golf Club Wallpaper 12b.bmp | |
| MissingOnTarget | | | \\OESNW\VOL2\Dept Shares\Marketing Dept\New Graphics\Pointspin.png | |
| MissingOnTarget | | | \\OESNW\VOL2\Dept Shares\Marketing Dept\New Graphics\Groupsymmetry.png | |
| MissingOnTarget | | | \\OESNW\VOL2\Dept Shares\Marketing Dept\New Graphics\Augusta National Golf Club Wallpaper - 16.bmp | |
| MissingOnTarget | | | \\OESNW\VOL2\Dept Shares\Marketing Dept\New Graphics\Kanaka.png | |
| MissingOnTarget | | | \\OESNW\VOL2\Dept Shares\Marketing Dept\New Graphics\Augusta National Golf Club Wallpaper 13f.bmp | |
| MissingOnTarget | | | \\OESNW\VOL2\Dept Shares\Marketing Dept\New Graphics\GALILEOADV1BOX.jpg | |
| MissingOnTarget | | | \\OESNW\VOL2\Dept Shares\Marketing Dept\New Graphics\paw600sani1.gif | |
| MissingOnTarget | | | \\OESNW\VOL2\Dept Shares\Marketing Dept\New Graphics\Galileo_diagram.png | |
| MissingOnTarget | | | \\OESNW\VOL2\Dept Shares\Marketing Dept\New Graphics\Galileo_diagram_lg.png | |
| MissingOnTarget | | | \\OESNW\VOL2\Dept Shares\Marketing Dept\New Graphics\Augusta National Golf Club Wallpaper - 12a.bmp | |
| MissingOnTarget | | | \\OESNW\VOL2\Dept Shares\Marketing Dept\New Graphics\PS_diagram.png | |
| MissingOnTarget | | | \\OESNW\VOL2\Dept Shares\Marketing Dept\New Graphics\Aurora.png | |
| MissingOnTarget | | | \\OESNW\VOL2\Dept Shares\Marketing Dept\New Graphics\TIGER20PAW.jpg | |
| MissingOnTarget | | | \\OESNW\VOL2\Dept Shares\Marketing Dept\New Graphics\1259255486_449ad51d15_o.gif | |
| MissingOnTarget | | | \\OESNW\VOL2\Dept Shares\Marketing Dept\New Graphics\Galileo.png | |

14. View the files that are newer on the source server as well as those files on the source server that were not migrated.
15. In the CEDMScanCompare utility interface, note the `targetmissing.txt` output file.

    This is the file listing all of the new and modified directories and files on the source server.
16. Locate the `targetmissing.txt` file in the folder you specified earlier and copy the file to a location on the source server.
17. Have all of your network users close any open files in the source area, and then proceed to "Migrating the New and Modified Directories and Files" on page 195.

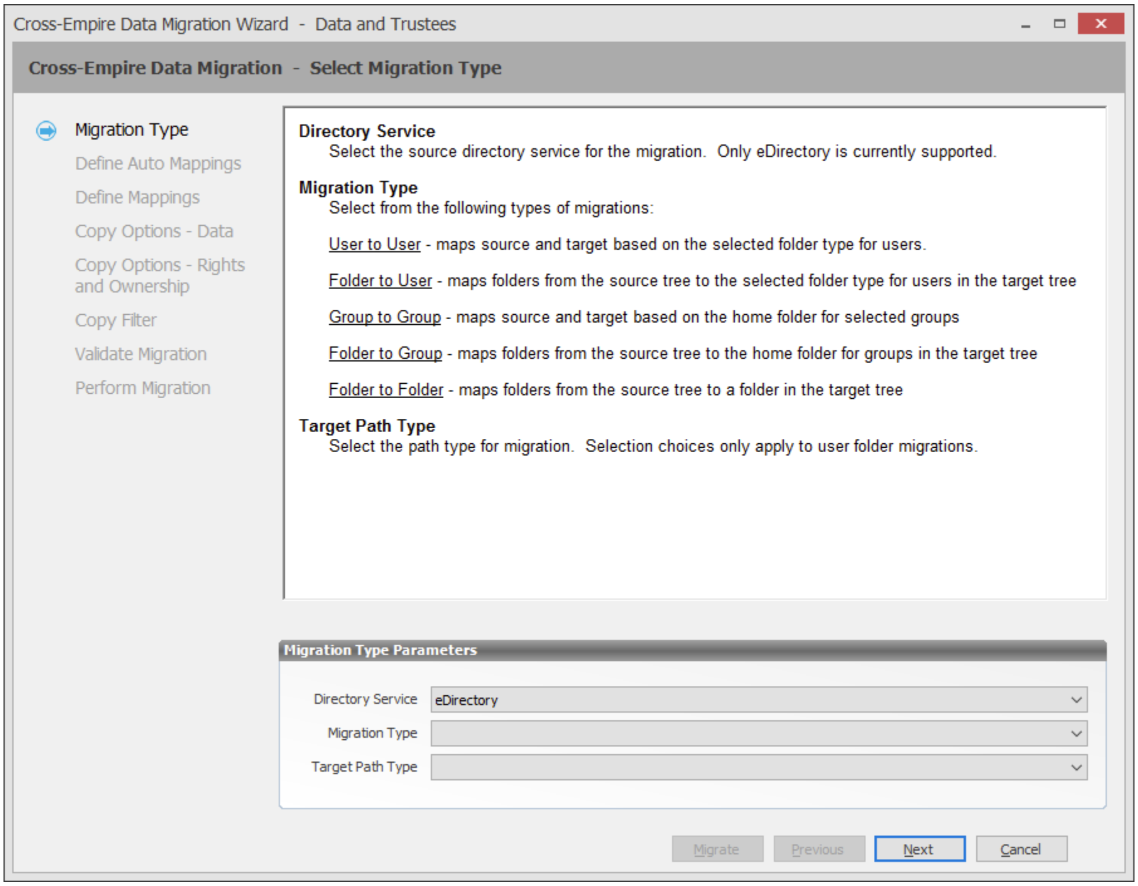
## 10.12.4 Migrating the New and Modified Directories and Files

Migrating all of the directories and files that are new or modified since the first phase of the folder to folder migration follows the same process as migrating the skipped files. The only difference is that you enter a different UNC path.

1 In SMAdmin, click the **Home** tab.

2 Select **Cross-Empire Data Migrations** > **eDirectory to Active Directory**.

3 Select **Migration Wizards** > **Data and Security**.


Cross-Empire Data Migration Wizard - Data and Trustees
Cross-Empire Data Migration - Select Migration Type
Migration Type
Define Auto Mappings
Define Mappings
Copy Options - Data
Copy Options - Rights and Ownership
Copy Filter
Validate Migration
Perform Migration
Migration Type Parameters
Migrate
Previous
Next
Cancel

**Directory Service**
Select the source directory service for the migration. Only eDirectory is currently supported.

**Migration Type**
Select from the following types of migrations:

User to User - maps source and target based on the selected folder type for users.

Folder to User - maps folders from the source tree to the selected folder type for users in the target tree

Group to Group - maps source and target based on the home folder for selected groups

Folder to Group - maps folders from the source tree to the home folder for groups in the target tree

Folder to Folder - maps folders from the source tree to a folder in the target tree

**Target Path Type**
Select the path type for migration. Selection choices only apply to user folder migrations.

Directory Service: eDirectory
Migration Type:
Target Path Type:

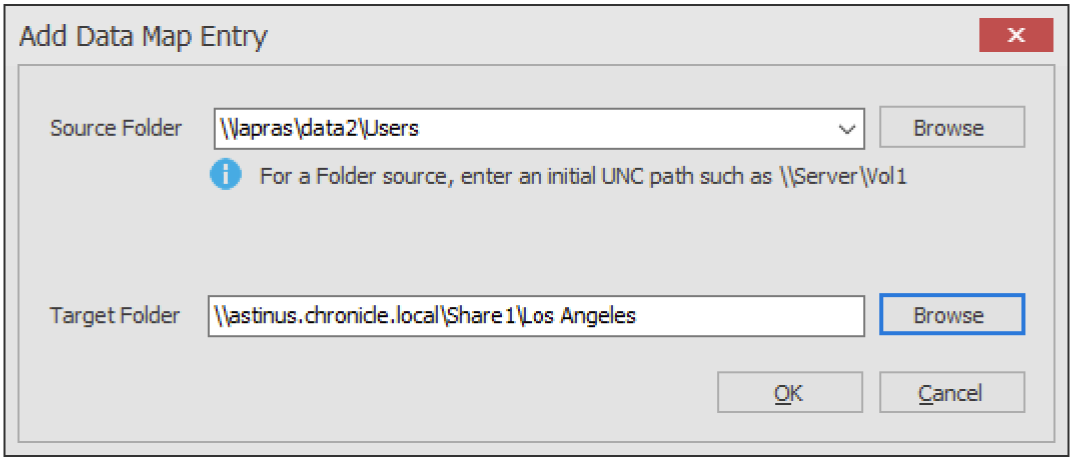
4 From the **Migration Type** drop-down menu, select **Delta File**.

5 Click **Next**.

6 Skip the Automatic Mappings settings by clicking **Next**.

7 On the Define Mappings wizard page, click **Add**.

8 In the Add Data Entry dialog box, browse to and select the source and target folders.


Add Data Map Entry

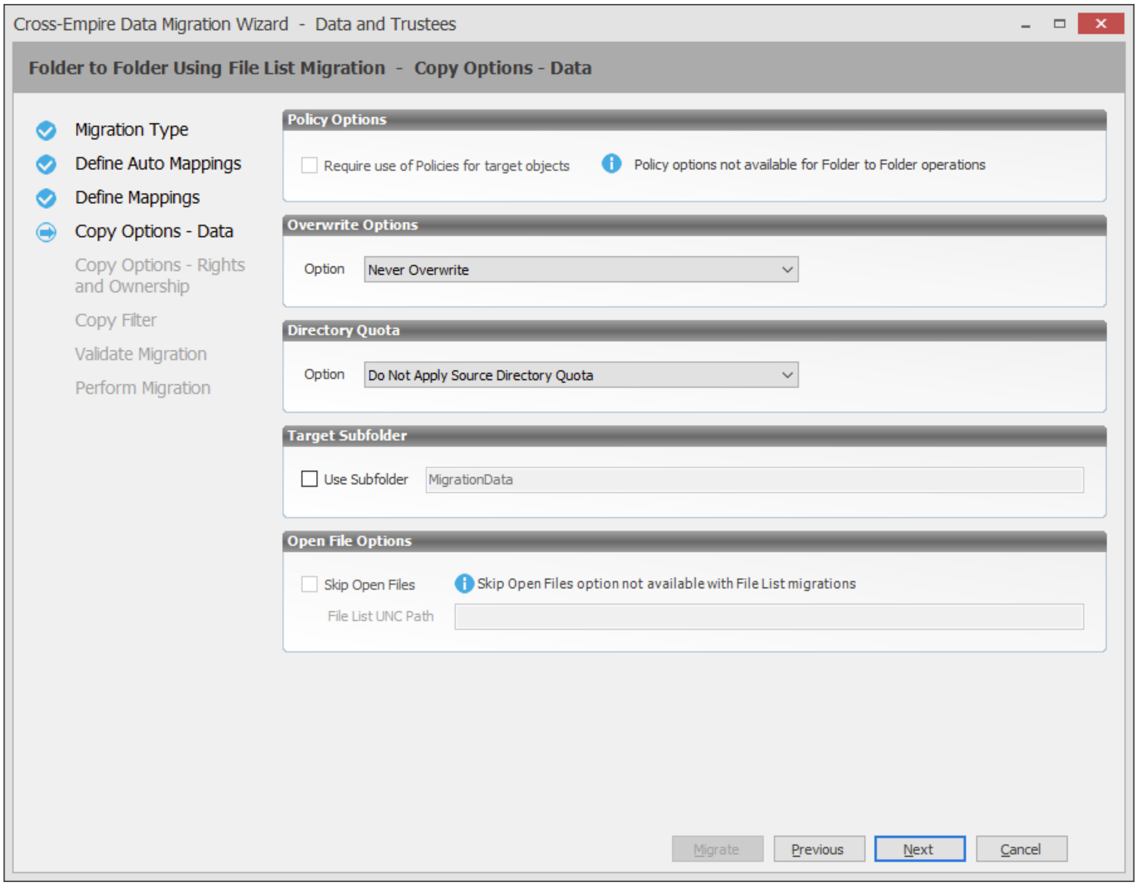
Source Folder: \\apras\data2\Users

For a Folder source, enter an initial UNC path such as \\Server\Vol1

Target Folder: \\astinus.chronicle.local\Share1\Los Angeles

9 Click **OK**.

10 On the Define Mappings wizard page, verify the source folder and the destination folder and click **Next**.


Cross-Empire Data Migration Wizard - Data and Trustees

Folder to Folder Using File List Migration - Copy Options - Data

Policy Options

□ Require use of Policies for target objects

Policy options not available for Folder to Folder operations

Overwrite Options

Option: Never Overwrite

Directory Quota

Option: Do Not Apply Source Directory Quota

Target Subfolder

□ Use Subfolder: MigrationData

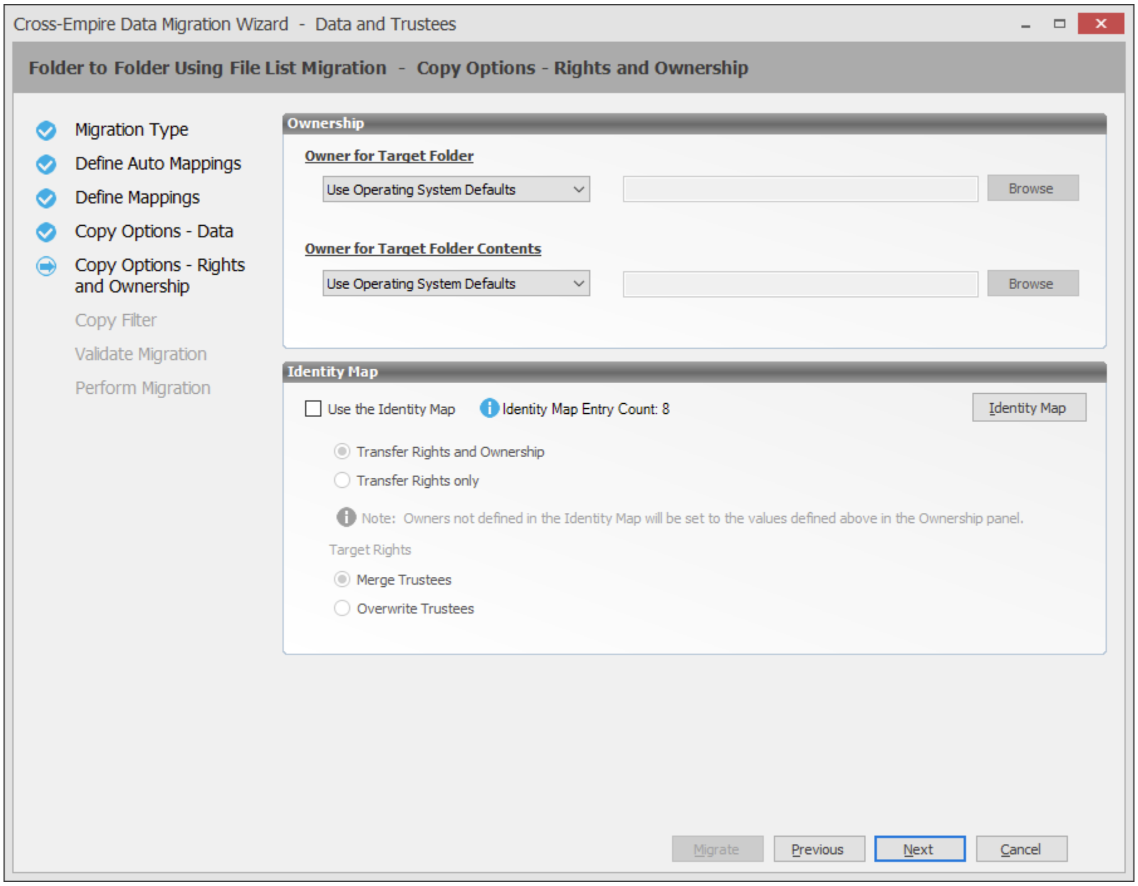
Open File Options

□ Skip Open Files

Skip Open Files option not available with File List migrations

File List UNC Path

11 On the Copy Options - Data wizard page, from the **Option** drop-down menu in the **Overwrite Options** region, select **Overwrite if Newer**, then click **Next**.



Folder to Folder Using File List Migration - Copy Options - Rights and Ownership

Ownership

Owner for Target Folder: Use Operating System Defaults

Owner for Target Folder Contents: Use Operating System Defaults

Identity Map

□ Use the Identity Map

Identity Map Entry Count: 8

● Transfer Rights and Ownership

○ Transfer Rights only

Note: Owners not defined in the Identity Map will be set to the values defined above in the Ownership panel.

Target Rights

● Merge Trustees

○ Overwrite Trustees

**12** (Optional) On the Copy Options - Rights and Owners wizard page, from the drop-down menu of the **Owner for Target Folder** region, select **Set Explicit Owner**.

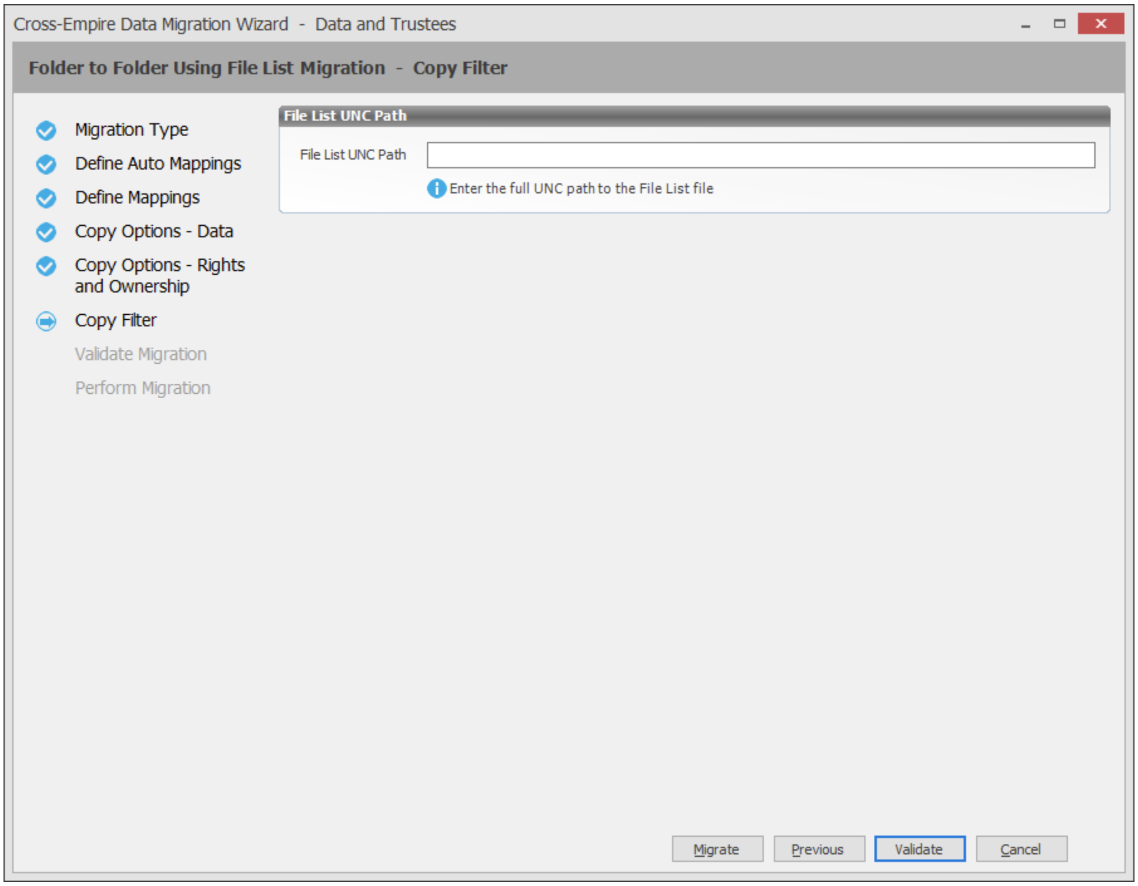
**13** (Conditional) If you chose to set an explicit owner for the folder, click the corresponding **Browse** button and browse to specify an owner for the target folder.

**14** (Optional) From the drop-down menu of the **Owner for Target Folder Contents** region, select **Set Explicit Owner**.

**15** (Conditional) If you chose to set an explicit owner for the folder contents, click the corresponding **Browse** button and browse to specify an owner for the target folder contents.

**16** Select the **Use Identity Map** check box and click **Next**.

**17** On the **Copy Filter** wizard page, specify the UNC path to the `targetmissing.txt` file that you copied to the source server.


Cross-Empire Data Migration Wizard - Data and Trustees
Folder to Folder Using File List Migration - Copy Filter
Migration Type
Define Auto Mappings
Define Mappings
Copy Options - Data
Copy Options - Rights and Ownership
Copy Filter
Validate Migration
Perform Migration
File List UNC Path
File List UNC Path
Enter the full UNC path to the File List file
Migrate
Previous
Validate
Cancel

18 Click **Validate** to confirm that the path is correct.

19 Click **Migrate**.

The new and modified files are migrated.

20 Continue with Section 10.12.5, "Verifying that All Directories and Files were Migrated by Comparing Source Server and Target Server Contents," on page 198.

## 10.12.5 Verifying that All Directories and Files were Migrated by Comparing Source Server and Target Server Contents

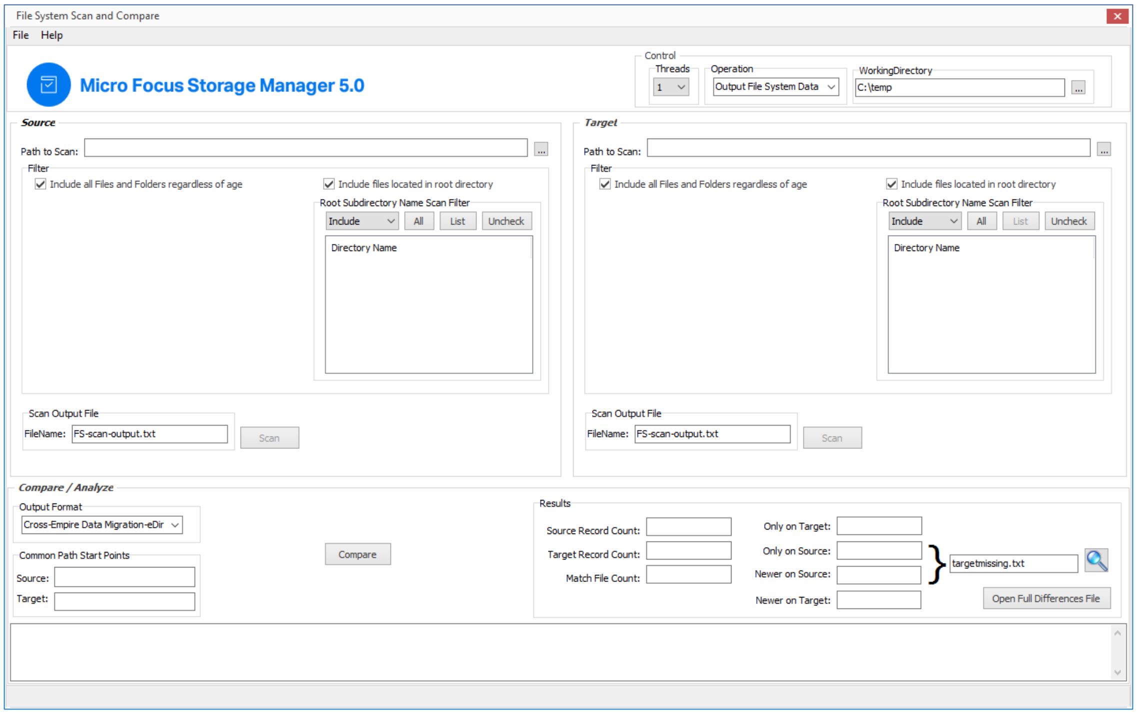
With all of the directories and files now migrated, you should now compare the contents of the source server and target server to verify that everything migrated properly. The process is as follows:

1 Launch the CEDMScanCompare utility.

2 When the message appears about the need to specify a working directory for the scan and comparison data, click **OK**.

3 Browse to a folder where you want to store the comparison data and click **Select Folder**.

The CEDMScanCompare utility interface is launched.



Threads: 1

Operation: Output File System Data

WorkingDirectory: C:\temp

☑ Include all Files and Folders regardless of age

☑ Include files located in root directory

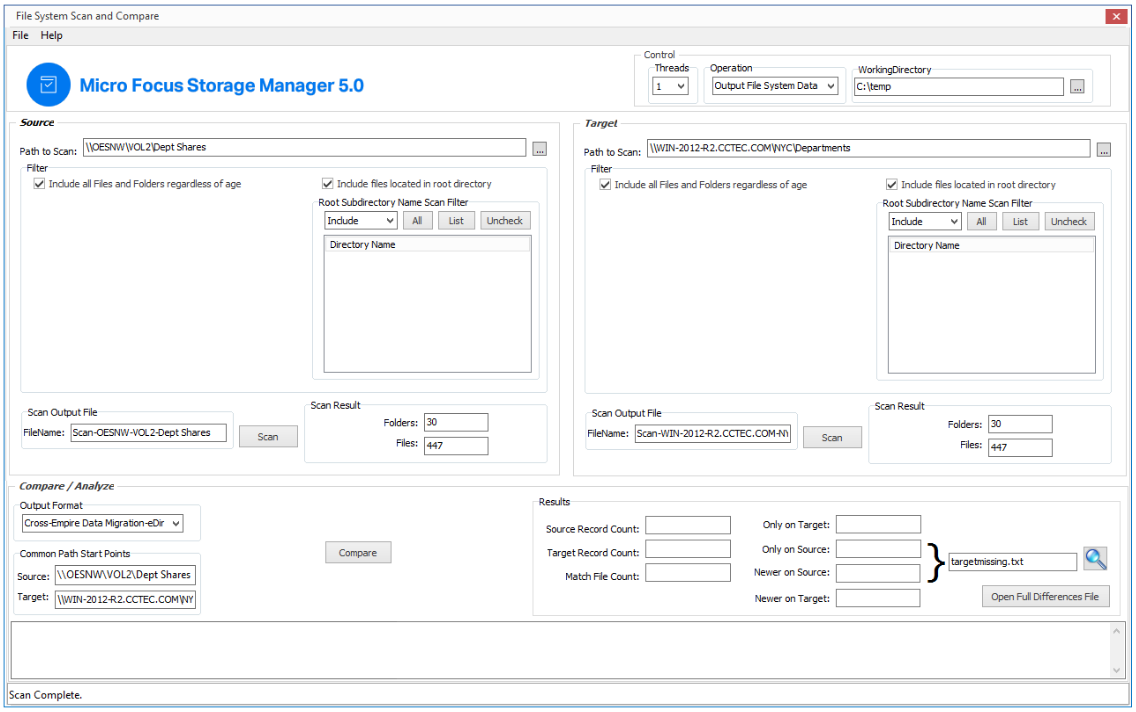
Root Subdirectory Name Scan Filter: Include

FileName: FS-scan-output.txt

Output Format: Cross-Empire Data Migration-eDir

targetmissing.txt

4. In the **Source** region, for the **Path to Scan** field, browse to specify the UNC path to the folder from the source server you want to scan.
5. In the **Target** region, for the **Path to Scan** field, browse to specify the UNC path to the folder in the target server you want to scan.
6. In the Source region, click **Scan**.
7. In the Target region, click **Scan**.
8. In the **Compare / Analyze** region, from the **FileName** drop-down menu, select **Cross-Empire Data Migration-eDir**.
9. Click **Compare**.



Threads: 1

Operation: Output File System Data

WorkingDirectory: C:\temp

Source

Path to Scan: \\OESNW\VOL2\Dept Shares

☑ Include all Files and Folders regardless of age

☑ Include files located in root directory

Root Subdirectory Name Scan Filter: Include

FileName: Scan-OESNW-VOL2-Dept Shares

Folders: 30

Files: 447

Target

Path to Scan: \\WIN-2012-R2.CCTEC.COM\NYC\Departments

☑ Include all Files and Folders regardless of age

☑ Include files located in root directory

Root Subdirectory Name Scan Filter: Include

FileName: Scan-WIN-2012-R2.CCTEC.COM-NY

Folders: 30

Files: 447

Output Format: Cross-Empire Data Migration-eDir

Source: \\OESNW\VOL2\Dept Shares

Target: \\WIN-2012-R2.CCTEC.COM\NY

targetmissing.txt

Scan Complete.

**10** Do one of the following:

- If the results show no discrepancies between the source and target, all of the folders and files were migrated. You can close the CEDMScanCompare utility as you are now finished with the folder to folder data migration.
- If the results show discrepancies between the source and target, take measures to close the open files and repeat the procedures in "Migrating the New and Modified Directories and Files" on page 195.

## 10.12.6 Creating a Target Folder in the Data Migration Wizard

**1** Make sure you have completed the prerequisites and have created a migration proxy account.

For more information on the prerequisites, see Section 10.3, "Prerequisites," on page 130. For more information on creating a migration proxy account, see Section 10.4, "Creating the Migration Proxy Account," on page 131.

**2** (Conditional) If you want to migrate closed files now and skip some files to migrate later:

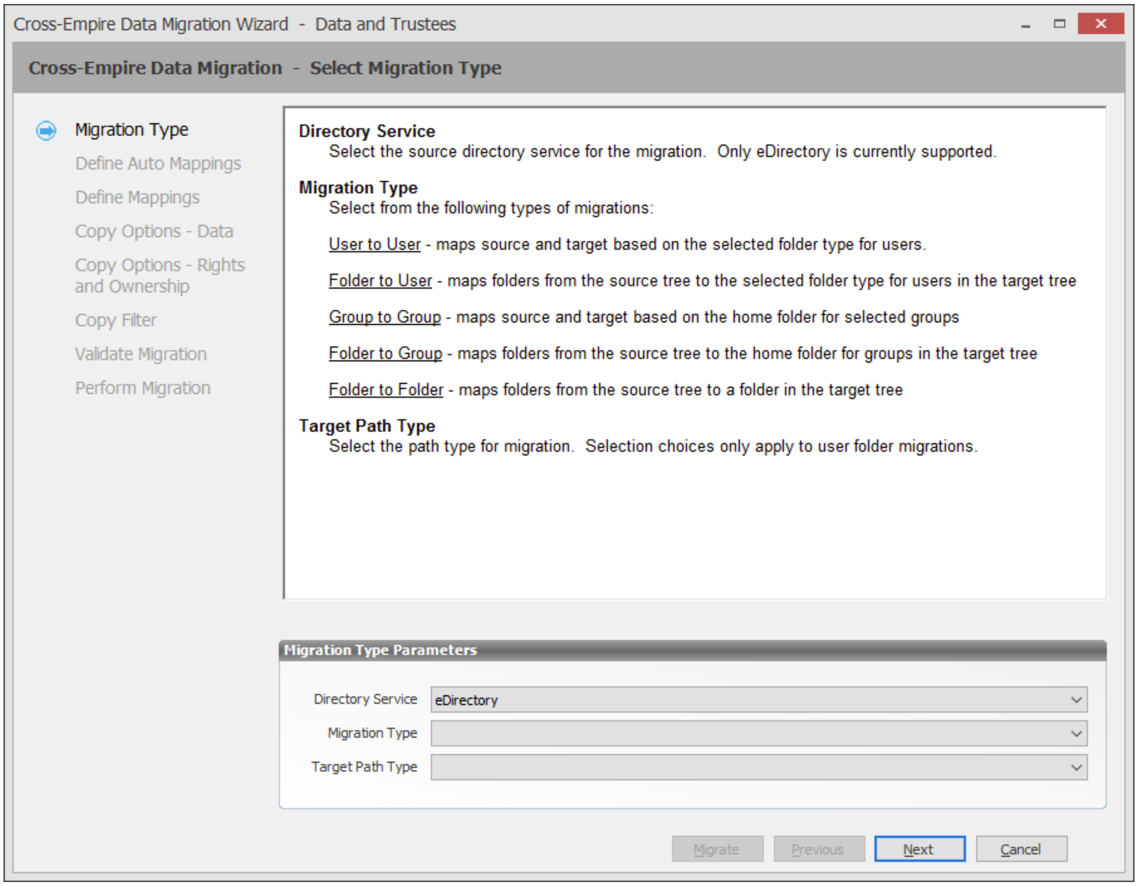
**2a** From the `Utilities\CEDM` folder on the Storage Manager ISO image, copy the `CEDMScanCompare.exe` utility to either the Windows target server or to a Windows server where you are going to administer the migration.

**2b** On each NetWare or Open Enterprise Server from which you are going to migrate data, create a new subdirectory and name it `Open`.

**3** In SMAdmin, click the **Home** tab.

**4** Select **Cross-Empire Data Migrations** > **eDirectory to Active Directory**.

**5** Select **Migration Wizards** > **Data and Security**.


Cross-Empire Data Migration Wizard - Data and Trustees
Cross-Empire Data Migration - Select Migration Type
Migration Type
Define Auto Mappings
Define Mappings
Copy Options - Data
Copy Options - Rights and Ownership
Copy Filter
Validate Migration
Perform Migration
Migration Type Parameters
Migrate
Previous
Next
Cancel

**Directory Service**
Select the source directory service for the migration.  Only eDirectory is currently supported.

**Migration Type**
Select from the following types of migrations:

User to User - maps source and target based on the selected folder type for users.

Folder to User - maps folders from the source tree to the selected folder type for users in the target tree

Group to Group - maps source and target based on the home folder for selected groups

Folder to Group - maps folders from the source tree to the home folder for groups in the target tree

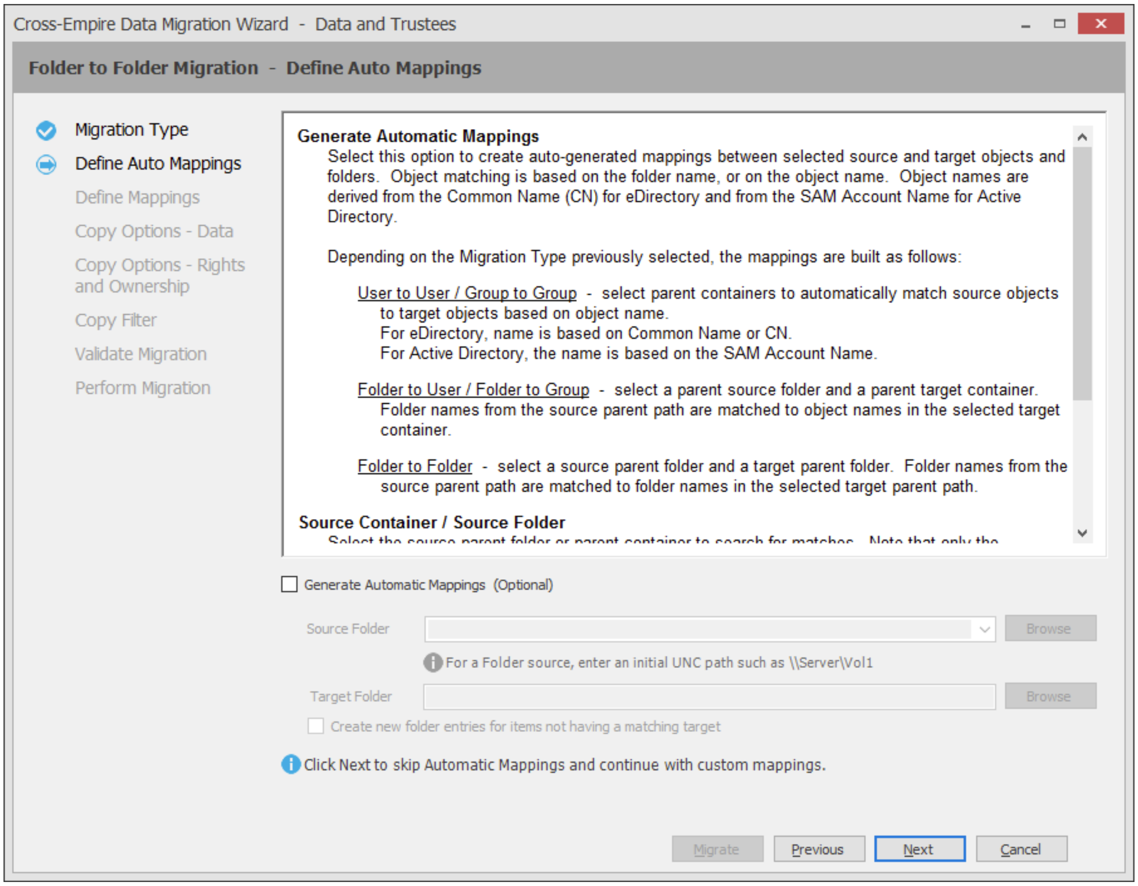
Folder to Folder - maps folders from the source tree to a folder in the target tree

**Target Path Type**
Select the path type for migration.  Selection choices only apply to user folder migrations.

Directory Service: eDirectory
Migration Type:
Target Path Type:

6 From the **Migration Type** drop-down menu, select **Folder to Folder**.

7 Click **Next**.



**Generate Automatic Mappings**

Select this option to create auto-generated mappings between selected source and target objects and folders. Object matching is based on the folder name, or on the object name. Object names are derived from the Common Name (CN) for eDirectory and from the SAM Account Name for Active Directory.

Depending on the Migration Type previously selected, the mappings are built as follows:

User to User / Group to Group - select parent containers to automatically match source objects to target objects based on object name.
For eDirectory, name is based on Common Name or CN.
For Active Directory, the name is based on the SAM Account Name.

Folder to User / Folder to Group - select a parent source folder and a parent target container. Folder names from the source parent path are matched to object names in the selected target container.

Folder to Folder - select a source parent folder and a target parent folder. Folder names from the source parent path are matched to folder names in the selected target parent path.

**Source Container / Source Folder**

Select the source parent folder or parent container to search for matches. Note that only the

☐ Generate Automatic Mappings (Optional)

Source Folder

For a Folder source, enter an initial UNC path such as \\Server\Vol1

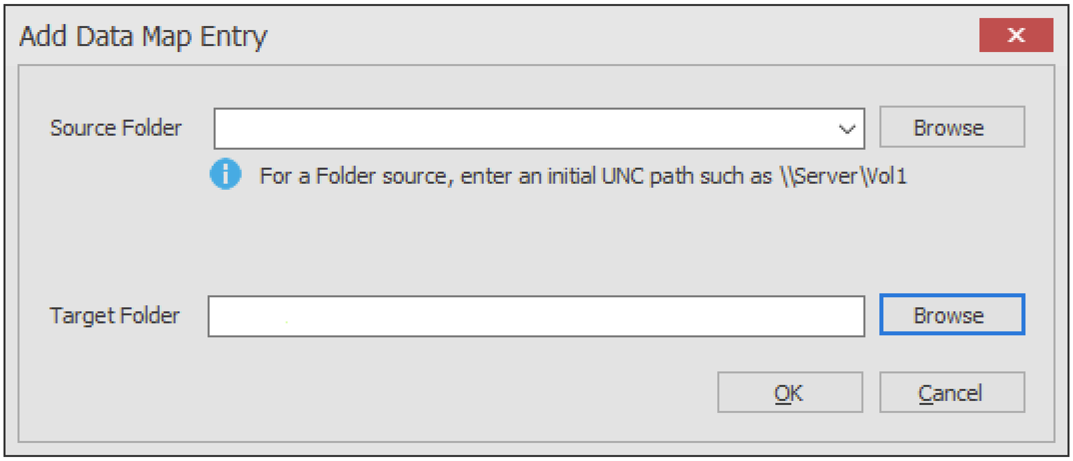
Target Folder

☐ Create new folder entries for items not having a matching target

Click Next to skip Automatic Mappings and continue with custom mappings.

8 Click **Next**.

9 Click **Add**.



Source Folder

For a Folder source, enter an initial UNC path such as \\Server\Vol1

Target Folder

10 In the **Source Folder** field, specify an initial UNC path for a server and volume to browse.

For example, `\\server_name\volume_name\` or `\\ip_address\volume_name`.

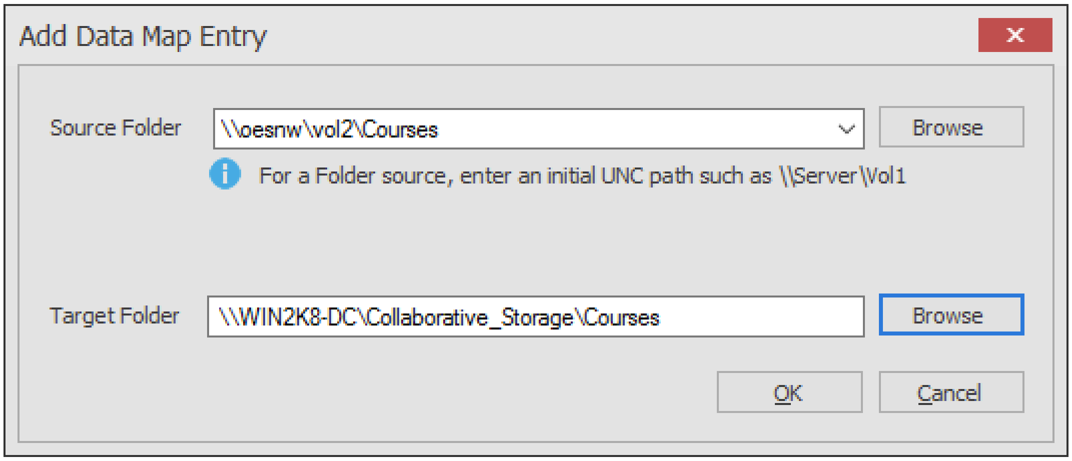
After a path is entered, you can click the **Browse** button to browse to the folder you want.

11 Click the **Browse** button that corresponds to the **Target Folder** field to locate the share where you want to create the new folder for the migrated data.

12 Right-click the share, select **Create Folder**, name the new folder, and click **OK**.

**13** Click **OK** to close the Target File System Path Browser.

**14** In the Add Data Map Entry dialog box, click the **Browse** button that corresponds to the **Target Folder** field again, browse to and select the new folder, then click **OK**.



Add Data Map Entry

Source Folder \\oesnw\vol2\Courses

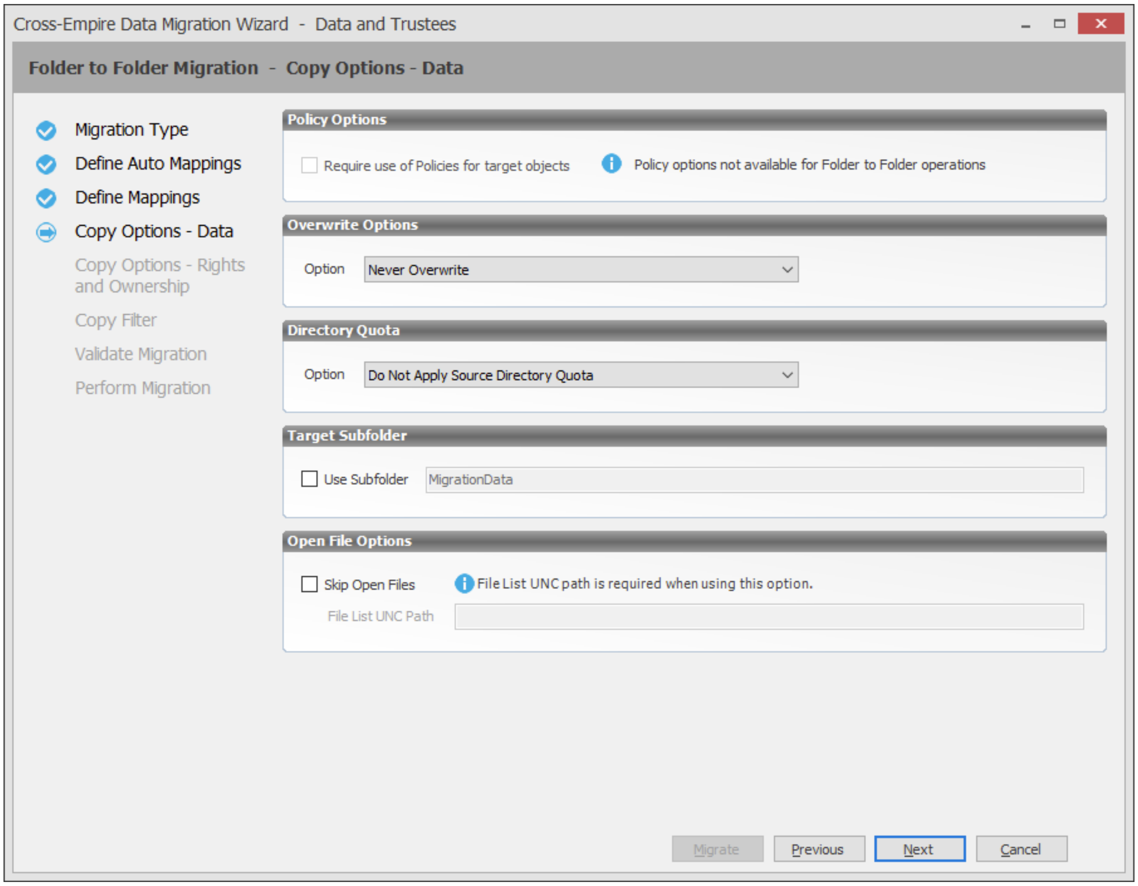
For a Folder source, enter an initial UNC path such as \\Server\Vol1

Target Folder \\WIN2K8-DC\Collaborative_Storage\Courses

**15** Click **OK**.

The defined source and target mappings are displayed.

**16** Click **Next**.



Cross-Empire Data Migration Wizard - Data and Trustees

**Folder to Folder Migration - Copy Options - Data**

- Migration Type
- Define Auto Mappings
- Define Mappings
- Copy Options - Data
- Copy Options - Rights and Ownership
- Copy Filter
- Validate Migration
- Perform Migration

**Policy Options**

□ Require use of Policies for target objects

Policy options not available for Folder to Folder operations

**Overwrite Options**

Option: Never Overwrite

**Directory Quota**

Option: Do Not Apply Source Directory Quota

**Target Subfolder**

□ Use Subfolder MigrationData

**Open File Options**

□ Skip Open Files

File List UNC path is required when using this option.

File List UNC Path

**17** Fill in the following fields:

**Overwrite Options:** Indicate what you want to take place when duplicate filenames are encountered in the source and target.

**Directory Quota:** Specify how quota settings from the source NSS file system should be applied after the migration.

**Target Subfolder:** If you want migrated data to be placed in a subfolder, select the **Use subfolder** check box and specify the subfolder name in the field.

**Open File Options:** If you want the Cross-Empire Data Migration subsystem to skip all open files on the network and not migrate them, select **Skip Open Files**.

Selecting **Skip Open Files** activates the **File List UNC Path** field where you specify the name and location of the log file listing all of the open files that are skipped during the migration.

Specify the UNC path for the Open directory you created along with a filename for the text file that will list the skipped files.

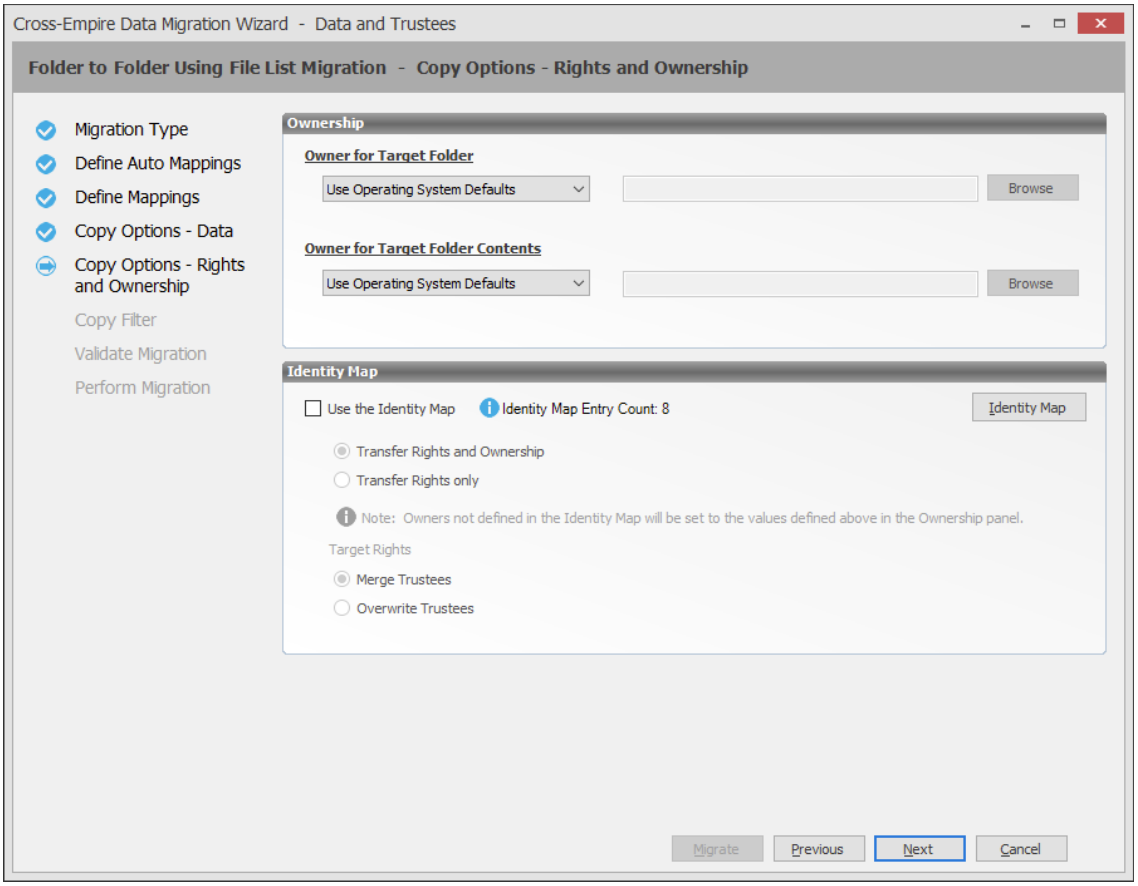
For example, `\\server_name\volume_name\directory_name\Open\skip.txt`

or

`\\ip_address\volume_name\Open\skip.txt`

The Cross-Empire Data Migration subsystem does not validate the path, so you must make sure that the path entered is correct. Otherwise, the migration fails.

**18** Click **Next**.



Cross-Empire Data Migration Wizard - Data and Trustees

**Folder to Folder Using File List Migration - Copy Options - Rights and Ownership**

**Ownership**

Owner for Target Folder: Use Operating System Defaults

Owner for Target Folder Contents: Use Operating System Defaults

**Identity Map**

□ Use the Identity Map

Identity Map Entry Count: 8

● Transfer Rights and Ownership

○ Transfer Rights only

Note: Owners not defined in the Identity Map will be set to the values defined above in the Ownership panel.

Target Rights

● Merge Trustees

○ Overwrite Trustees

**19** Fill in the following fields:

**Owner for Target Folder:** Use these settings to specify how ownership of the migrated folder is determined.

- **Use Operating System Defaults:** This default setting allows the target Microsoft Windows Server to adjust the file ownership according to the setting on the target server.
- **Set Explicit Owner:** Allows you to browse and select an object as the explicit owner of the migrated folder.

**Owner for Target Folder Contents:** Use these settings to specify how ownership of the migrated folder contents is determined.

- **Use Operating System Defaults:** This default setting allows the target Microsoft Windows Server to adjust the file ownership according to the settings on the target server.
- **Set Explicit Owner:** Allows you to browse and select an object as the explicit owner of the migrated folder.

**Use the Identity Map:** Select this check box if you want Storage Manager to utilize the identity map you created earlier and use the corresponding IDs to copy security rights and file ownership from the Novell or Micro Focus network file system to the Windows network file system.

- **Transfer Rights and Ownership:** Select this option if you want to transfer the file and folder security rights along with the ownership settings.

  Be aware that when you transfer the ownership of a file or folder in a Windows network, you are granting the owner Full Rights, which you might not want to provide.
- **Transfer Rights Only:** Select this option to transfer only the file and folder security rights.
- **Overwrite Trustees:** Select this option to override any existing trustee assignments for a target file or folder with the established eDirectory trustee assignments for those files and folders.
- **Merge Trustees:** Select this option to merge the established eDirectory trustee assignments with those of the target files or folders in the Windows network file system.

**Identity Map:** Clicking this button opens your identity map where you can make any desired changes.

**20** Click **Next**.

**21** (Conditional) If you want to use a filter to include or exclude specific files, select the **Use Copy Filter** check box and click the **Add** button.

**21a** Fill in the following fields:

**Description:** Specify a description of the filter.

**Action:** From the drop-down menu, select either **Migrate** or **Ignore**, based on whether the filter specifies to migrate files or folders or to ignore them.

**Files, Folders:** Specify if the filter applies to files or folders.

**Masks:** List the file types to migrate or ignore.

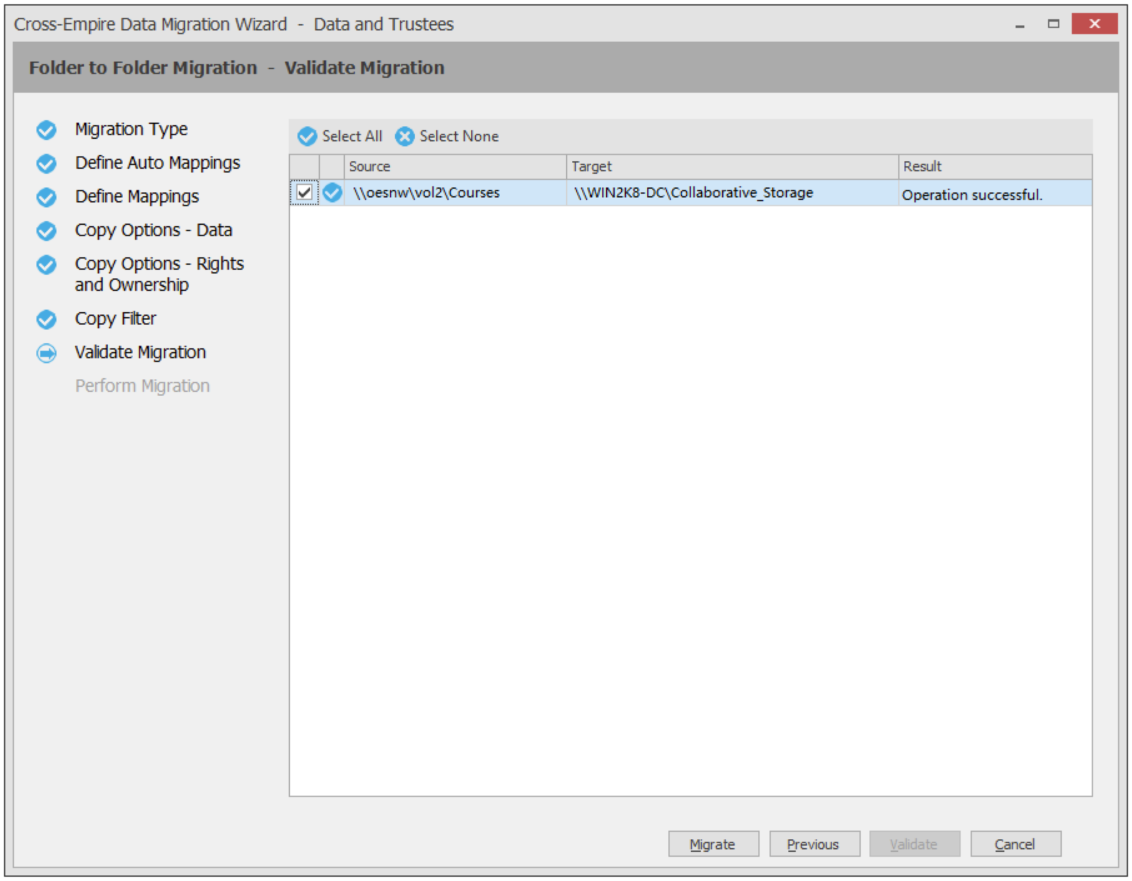
**21b** Specify any additional filter criteria in the menus and fields that remain.

For a detailed explanation of this region of the dialog box, see Section 6.5.8, “Setting Vault Rules,” on page 58.

**21c** Click **OK**.

**22** Click **Validate**.

**Validate** shows the result of certain checks that can be run prior to the migration. The **Result** column shows the status of the validation checks. If errors are displayed, you can choose to correct those errors prior to running the migration.



Cross-Empire Data Migration Wizard - Data and Trustees

Folder to Folder Migration - Validate Migration

| | | Source | Target | Result |
|---|---|---|---|---|
| ☑ | ✓ | \\oesnw\vol2\Courses | \\WIN2K8-DC\Collaborative_Storage | Operation successful. |

23 (Conditional) Take any necessary action in the Windows network file system target and then re-run the Data Migration Wizard.

24 Click **Migrate**.

A page appears with details of the data migration events that are queued for processing. To view the status of migration events, click **Events**. For more information on Pending Events, see Section 13.1.7, “Events,” on page 274.

25 Do one of the following:

- If you skipped some files to migrate later, click **Finish** and then continue with “Migrating Skipped Files” on page 188.
- If you have migrated all of you data, click **Finish**.

26 Scan the source server for new of modified directories and files by following the procedures in Section 10.12.3, “Scanning the Source Server for New or Modified Directories and Files,” on page 192.

27 Migrate all new and modified directories and files by following the procedures in Section 10.12.4, “Migrating the New and Modified Directories and Files,” on page 195.

28 Verify that all directories and files were migrated by following the procedures in Section 10.12.5, “Verifying that All Directories and Files were Migrated by Comparing Source Server and Target Server Contents,” on page 198.

# 11 Performing an Active Directory to Active Directory Cross-Empire Data Migration

**IMPORTANT:** With the release of Storage Manager 5.0, Micro Focus began providing the eDirectory to Active Directory Cross-Empire Data Migration and the new AD to AD Cross-Empire Data Migration subsystems only as additive support pack purchases to Storage Manager.

For example, if you wanted to migrate user data from one Active Directory forest to another, you would need to purchase licenses for Storage Manager 5.*x* for Active Directory + the AD to AD Cross-Empire Data Migration support pack.

If you do not have the additional support pack licenses, the Cross-Empire Data Migration options in SMAdmin are disabled.

## 11.1 Overview

The AD to AD Cross-Empire Data Migration Support Pack enables you to migrate user and group folders from one Active Directory forest to another, and in the process, maintain the original permissions, ownership, and disk quota settings.

Of course, you can modify the permissions, ownership, and disk quota settings automatically following the migration through Storage Manager policies and Management Actions.

**IMPORTANT:** Because of the potential complexity of an AD to AD Cross-Empire Data Migration, Micro Focus highly recommends that you utilize the expertise of a Micro Focus Support representative or a qualified partner.

## 11.2 Prerequisite Tasks

Before you can perform an AD to AD Cross-Empire Data Migration, you must first perform some prerequisite tasks on the source and target servers, along with establishing a configured trust relationship between the two.

1. Create matching user and group objects in the target forest for objects in the source forest.
2. Make sure you have installed all Storage Manager for Active Directory components in the target forest.
3. Disable file screening and virus protection software on the target server during the migration.
4. Configure DNS so that the source and target forest can communicate.
5. Configure a forest trust between the source and target forest.

   At a minimum, a one-way trust is required so that the target forest can access the source forest.

For a detailed explanation of forest trust requirements, see Section 13.1.14, “Forest Trusts,” on page 290.

6. From the `Utilities\CEDM` folder on the Storage Manager ISO image, copy the `CEDMScanCompare.exe` utility to either the Windows target server or to a Windows server where you are going to administer the migration.

## 11.3 Perform an AD to AD Cross-Empire Data Migration

### 11.3.1 Establish a Forest Trust Configuration in SMAdmin

1. Launch SMAdmin and click the **Home** tab.
2. Click **Forest Trusts** and select the check box next to the displayed source forest.
3. Close out of SMAdmin.
4. Launch SMAdmin and log in.
5. Click **Forest Trusts** and verify that the status for forest trust reads:

   ```
   Trust is fully configured and usable.
   ```

### 11.3.2 Assign Administrative Rights to the SMProxyRights Group

Follow these procedures to add the SMProxyRights group of the target forest as a member of the local administrators group on the server or appliance in the source forest.

1. On the source server, launch Active Directory Users and Computers.
2. From the `Builtin` directory of the forest, double-click `Administrators`.
3. Click the **Members** tab.

4 Click **Add**.

This opens the Select Users, Contacts, Computers, Service Accounts, or Groups dialog box.

5 Click **Locations**.

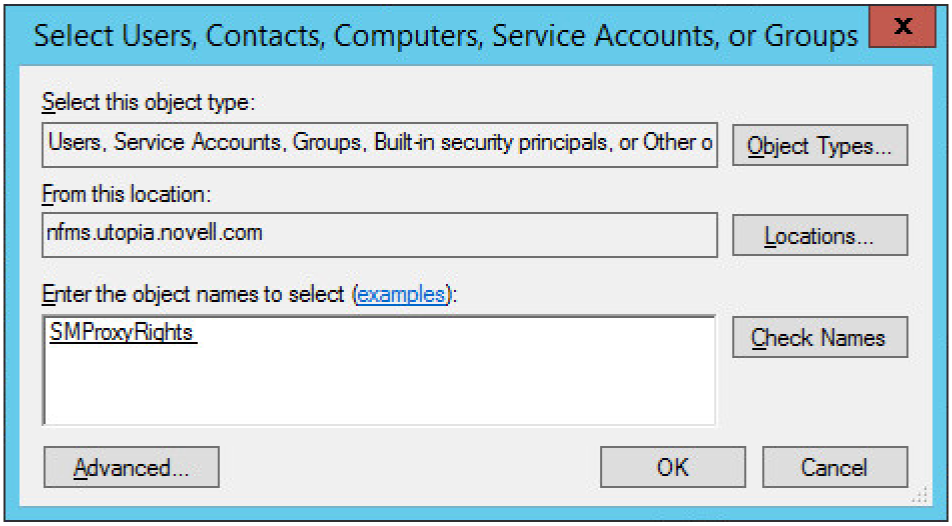
This opens the Locations dialog box.

6 Select the target forest and click **OK**.

7 In the **Enter the object names to select** field of the Select Users, Contacts, Computers, Service Accounts, or Groups dialog box, type `smp` and click **check names**.

This opens the Multiple Names Found dialog box.

8 Select `SMProxyRights` and click **OK**.



Select Users, Contacts, Computers, Service Accounts, or Groups

Select this object type:
Users, Service Accounts, Groups, Built-in security principals, or Other o

From this location:
nfms.utopia.novell.com

Enter the object names to select (examples):
SMProxyRights

9 Click **OK** to close the Select Users, Contact, Computers, Service Accounts, or Groups dialog box.

SMProxyRights is added to the list of members in the Administrators dialog box.

10 Click **OK** to close the Administrators dialog box.

### 11.3.3 Assign Permissions to the SMProxyRights Group

Follow these procedures to assign the SMProxyRights group of the target server, FULL Share Permissions to shares that Storage Manager will be migrating from the source forest.

1 Using Windows Explorer on the source server, right-click the shares you plan to migrate and select **Properties**.

This opens the Properties dialog box.

2 Click the **Sharing** tab and click **Advanced Sharing**.

This opens the Advanced Sharing dialog box.

3 Click **Permissions**.

This opens the Permissions dialog box.

4 Click **Add**.

This opens the Select Users, Computers, Service Accounts, or Groups dialog box.

5 Click **Locations**.

This opens the Locations dialog box.

6 Select the target forest and click **OK**.

7 In the **Enter the object names to select** field of the Select Users, Computers, Service Accounts, or Groups dialog box, type `smp` and click **Check names**.

This opens the Multiple Names Found dialog box.

8 Select `SMProxyRights` and click **OK**.

9 In the Permissions dialog box pertaining to the share you selected previously, assign SMProxyRights Full Control.

10 Click **OK** to save the setting and close the Permission dialog box.

11 Repeat these steps for all other shares you plan to migrate.

12 Close the Advanced Sharing and Properties dialog boxes.

## 11.3.4 Verify that SMAdmin Can See Shares on the Source Server

Follow these procedures to verify that SMAdmin can see the shares that you plan to migrate.

1 Launch SMAdmin and click the **Home** tab.

2 Click **Storage Resources**.

3 Verify that the shares you want to migrate are listed.

If the shares are not listed click **Rebuild**.

## 11.3.5 Create an Identity Map

Storage Manager for Active Directory uses an identity map to specify associations between the users and groups of the source forest with the users and groups of the target forest.

As specified in Section 11.2, "Prerequisite Tasks," on page 207, you must create the associated target server users, groups, and shares before you migrate as the AD to AD Cross-Empire Data Migration Solution Pack does not create these associated objects on the target server.

**IMPORTANT:** If you are creating an identity map of more than 25,000 objects, we recommend 8GB to 12GB of memory for the workstation or server running SMAdmin.

1 Launch SMAdmin and click the **Home** tab.

2 Click **Cross-Empire Data Migrations** > **Active Directory to Active Directory**.

3 Click **Edit Identity Map**.

4 Click **Identity Map Entry Wizard**.

5 Select both the **User to User** and **Group to Group** check boxes.

6 From the **Match Attribute** drop-down menu, select on of the following options:

**SAM-Account-Name:** This attribute can be used when you want to populate the identity map with objects in the source and target forest that have the same corresponding attribute value. By choosing **SAM-Account-Name** (SAM) as the Match Attribute, (depending on your Source and Target Scopes) the engine will search the source and target forests for objects whose SAM are the same value.

**Common-Name:** This attribute selection functions in the same manner as the SAM-Account Name, but for Common-Names(CN).

**Object-SID:** This option is only applicable in the case where accounts have been migrated from the source to the target using a tool such as Active Directory Migration Tool (ADMT). When ADMT is used, you can opt to copy the Object-Sid. This results in the target object containing the Object-Sid of the originating source object in the SID-History attribute.

For more information, refer to these Microsoft documents:

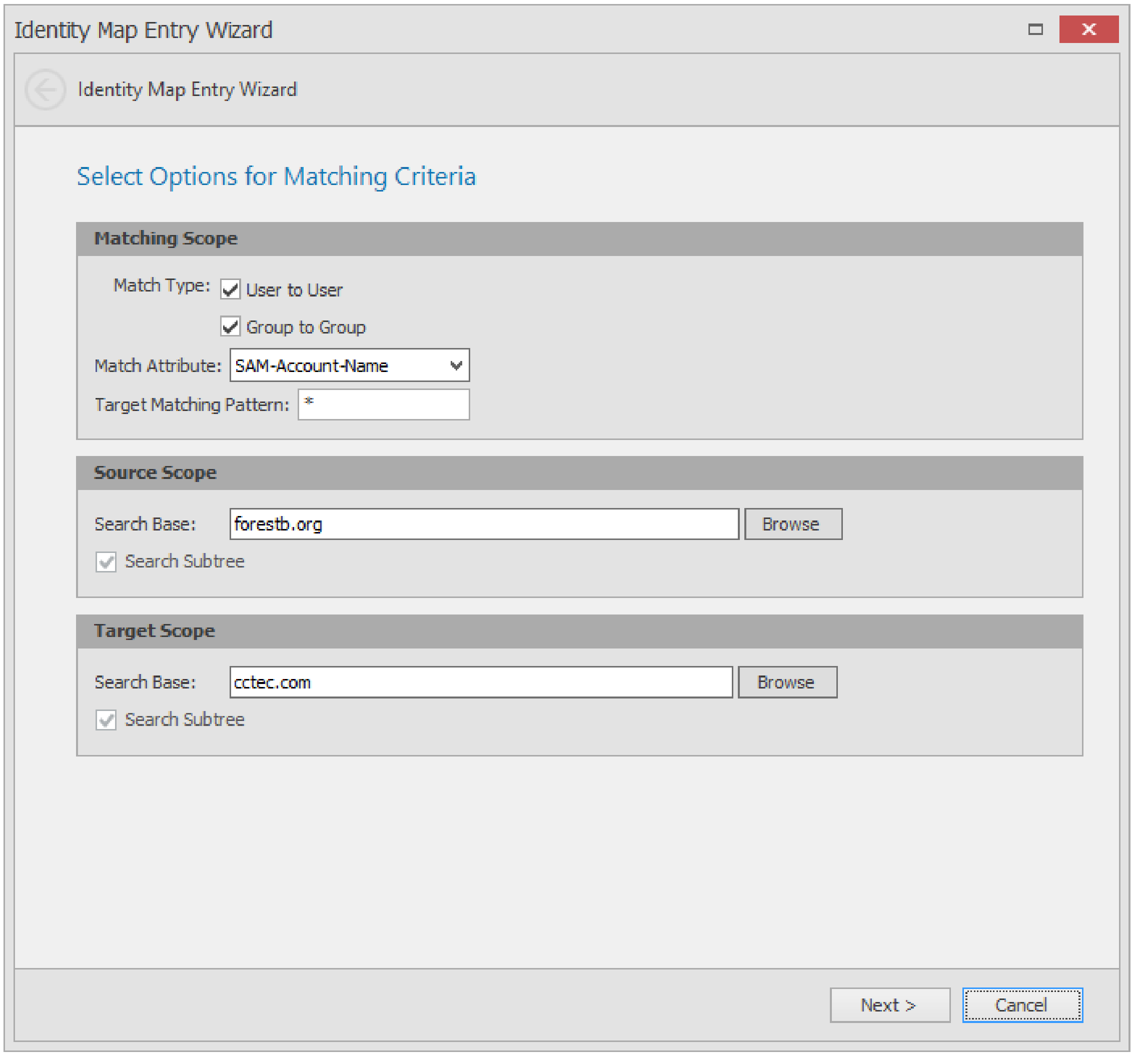
- https://msdn.microsoft.com/en-us/library/ms679833(v=vs.85).aspx
- https://technet.microsoft.com/en-us/library/cc778824(v=ws.10).aspx

When this Match Attribute is chosen, the engine will enumerate objects in the source and then search for objects whose SID-History attribute contains the source object's Object-Sid. If objects have not been migrated such that the source's Object-Sid is in the target's SID-History, you must use either SAM-Account-Name or Common-Name to populate the identity map.

**Well-known SIDS:** This option should be used when you want to populate the identity map with well-known SIDs whose relative identifiers (RIDs) are relative to each domain (e.g. `chronicle\administrator`) and whose domain identifier is not "Builtin" (32).

For more information, refer to this Microsoft document: https://msdn.microsoft.com/en-us/library/windows/desktop/aa379649(v=vs.85).aspx

Builtin well-known SIDs can be added and mapped manually in the Identity Map editor by selecting an object from the Well-known SIDs tab, right-clicking and selecting **Add Identity Map Entry**.



Select Options for Matching Criteria

Matching Scope

Match Type: ☑ User to User

☑ Group to Group

Match Attribute: SAM-Account-Name

Target Matching Pattern: *

Source Scope

Search Base: forestb.org Browse

☑ Search Subtree

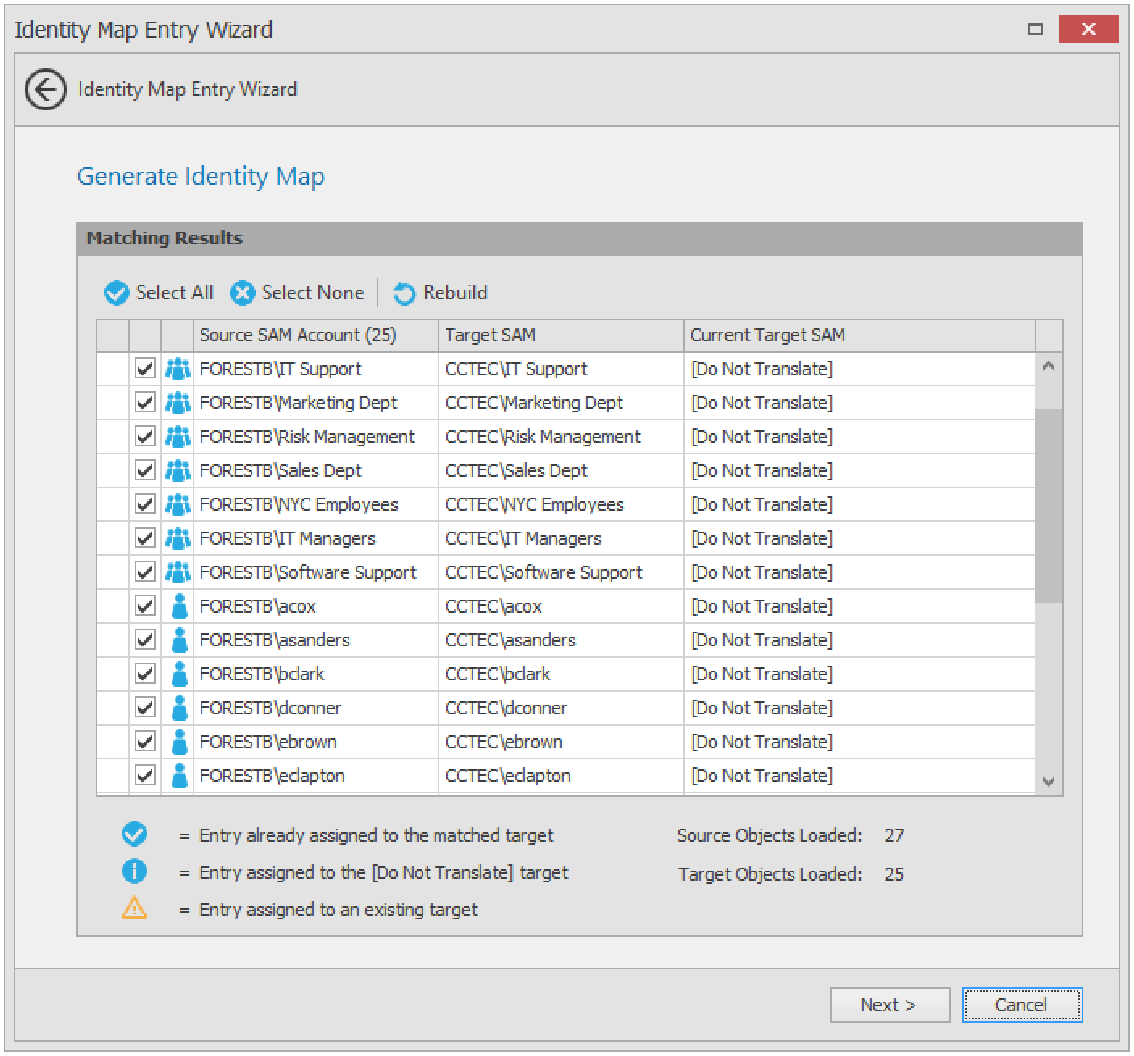
Target Scope

Search Base: cctec.com Browse

☑ Search Subtree

7 Verify that the source forest and target forest in the Source Scope and Target Scope regions respectively, are correct and click **Next**.

8 Observe the matching results of source and target groups and users.



| | | | Source SAM Account (25) | Target SAM | Current Target SAM |
|---|---|---|---|---|---|
| | ☑ | | FORESTB\IT Support | CCTEC\IT Support | [Do Not Translate] |
| | ☑ | | FORESTB\Marketing Dept | CCTEC\Marketing Dept | [Do Not Translate] |
| | ☑ | | FORESTB\Risk Management | CCTEC\Risk Management | [Do Not Translate] |
| | ☑ | | FORESTB\Sales Dept | CCTEC\Sales Dept | [Do Not Translate] |
| | ☑ | | FORESTB\NYC Employees | CCTEC\NYC Employees | [Do Not Translate] |
| | ☑ | | FORESTB\IT Managers | CCTEC\IT Managers | [Do Not Translate] |
| | ☑ | | FORESTB\Software Support | CCTEC\Software Support | [Do Not Translate] |
| | ☑ | | FORESTB\acox | CCTEC\acox | [Do Not Translate] |
| | ☑ | | FORESTB\asanders | CCTEC\asanders | [Do Not Translate] |
| | ☑ | | FORESTB\bclark | CCTEC\bclark | [Do Not Translate] |
| | ☑ | | FORESTB\dconner | CCTEC\dconner | [Do Not Translate] |
| | ☑ | | FORESTB\ebrown | CCTEC\ebrown | [Do Not Translate] |
| | ☑ | | FORESTB\eclapton | CCTEC\eclapton | [Do Not Translate] |

✓ = Entry already assigned to the matched target

ⓘ = Entry assigned to the [Do Not Translate] target

⚠ = Entry assigned to an existing target

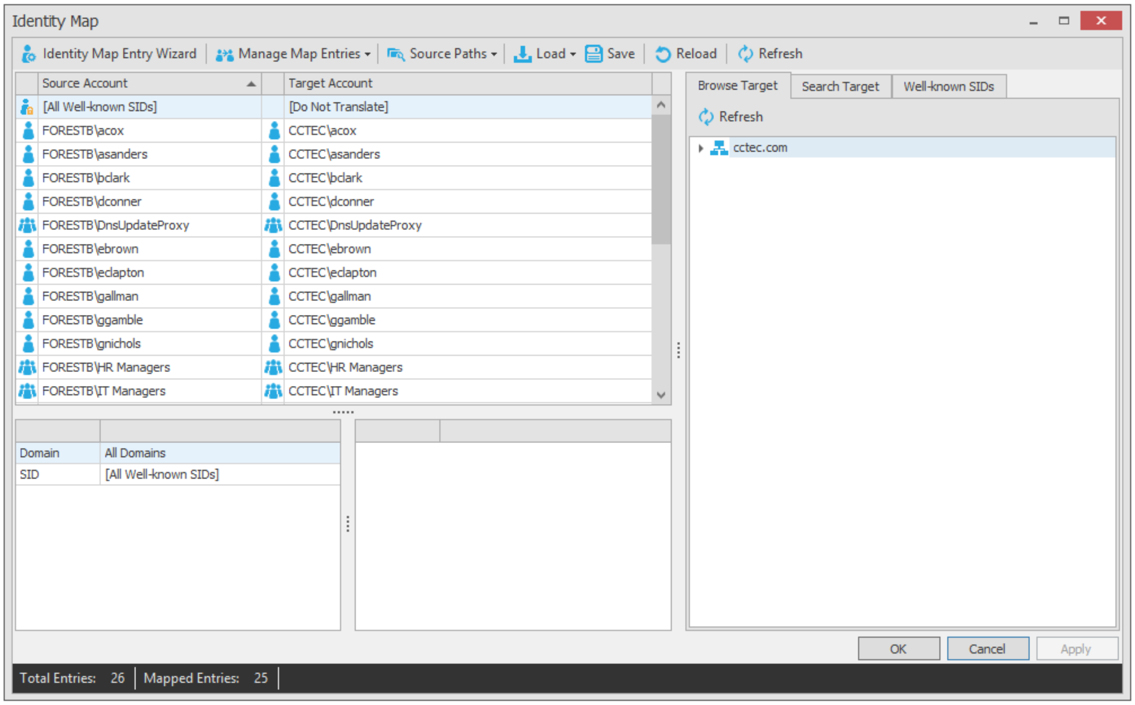
Source Objects Loaded: 27

Target Objects Loaded: 25

9 Click **Next**.

10 In the Import Map Entries page, leave the **Auto-save Identity Map updates to Engine** check box selected and click **Finish**.

The users and groups on the source and target forests are now matched.



| Source Account | Target Account |
|---|---|
| [All Well-known SIDs] | [Do Not Translate] |
| FORESTB\acox | CCTEC\acox |
| FORESTB\asanders | CCTEC\asanders |
| FORESTB\bclark | CCTEC\bclark |
| FORESTB\dconner | CCTEC\dconner |
| FORESTB\DnsUpdateProxy | CCTEC\DnsUpdateProxy |
| FORESTB\ebrown | CCTEC\ebrown |
| FORESTB\eclapton | CCTEC\eclapton |
| FORESTB\gallman | CCTEC\gallman |
| FORESTB\ggamble | CCTEC\ggamble |
| FORESTB\gnichols | CCTEC\gnichols |
| FORESTB\HR Managers | CCTEC\HR Managers |
| FORESTB\IT Managers | CCTEC\IT Managers |

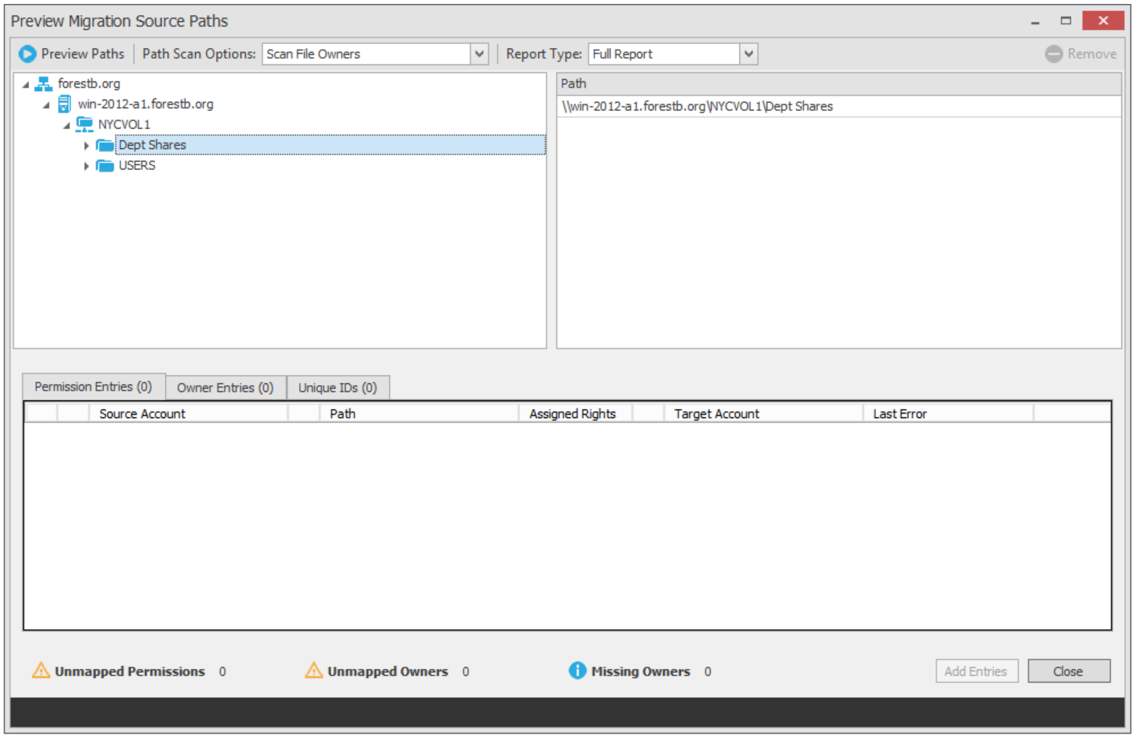
| | |
|---|---|
| Domain | All Domains |
| SID | [All Well-known SIDs] |

Total Entries: 26 | Mapped Entries: 25

## 11.3.6 Preview the Source Paths for the Migration

Follow these procedures to preview the migration source paths as well as add and match any missing objects to the identity map.

1. In the Identity Map interface, click **Source Paths** > **Generate Preview Report**.
2. In the Preview Migration Source Paths dialog box, in the upper left-hand pane, navigate to the desired share and double-click it to add it to the **Path** window to the right.



Preview Migration Source Paths

Preview Paths | Path Scan Options: Scan File Owners | Report Type: Full Report | Remove

- forestb.org
  - win-2012-a1.forestb.org
    - NYCVOL1
      - Dept Shares
      - USERS

Path: \\win-2012-a1.forestb.org\NYCVOL1\Dept Shares

Permission Entries (0) | Owner Entries (0) | Unique IDs (0)

| Source Account | Path | Assigned Rights | Target Account | Last Error |
|---|---|---|---|---|

Unmapped Permissions 0 | Unmapped Owners 0 | Missing Owners 0 | Add Entries | Close

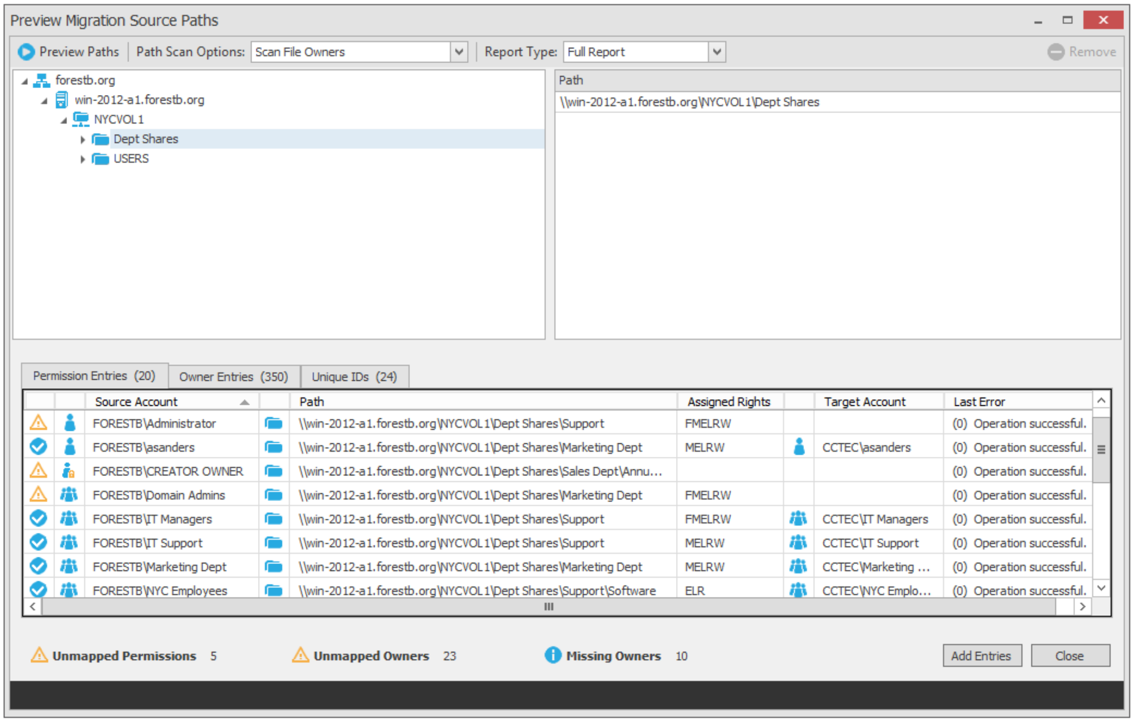
3 From the **Path Scan Options** drop-down menu, select from the following options:

**Scan Folders Only:** Scans only the folder permissions in the specified paths.

**Scan File Owners:** Scans the folder permissions and the file owners in the specified paths.

**Scan File Owners and Permissions:** Scans the folder permissions, file owners, and file permissions in the specified paths.

4 Click **Preview Paths**.



Preview Migration Source Paths

Preview Paths | Path Scan Options: Scan File Owners | Report Type: Full Report | Remove

- forestb.org
  - win-2012-a1.forestb.org
    - NYCVOL1
      - Dept Shares
      - USERS

Path: \\win-2012-a1.forestb.org\NYCVOL1\Dept Shares

Permission Entries (20) | Owner Entries (350) | Unique IDs (24)

| | Source Account | Path | Assigned Rights | Target Account | Last Error |
|---|---|---|---|---|---|
| ⚠ | FORESTB\Administrator | \\win-2012-a1.forestb.org\NYCVOL1\Dept Shares\Support | FMELRW | | (0) Operation successful. |
| ✓ | FORESTB\asanders | \\win-2012-a1.forestb.org\NYCVOL1\Dept Shares\Marketing Dept | MELRW | CCTEC\asanders | (0) Operation successful. |
| ⚠ | FORESTB\CREATOR OWNER | \\win-2012-a1.forestb.org\NYCVOL1\Dept Shares\Sales Dept\Annu... | | | (0) Operation successful. |
| ⚠ | FORESTB\Domain Admins | \\win-2012-a1.forestb.org\NYCVOL1\Dept Shares\Marketing Dept | FMELRW | | (0) Operation successful. |
| ✓ | FORESTB\IT Managers | \\win-2012-a1.forestb.org\NYCVOL1\Dept Shares\Support | FMELRW | CCTEC\IT Managers | (0) Operation successful. |
| ✓ | FORESTB\IT Support | \\win-2012-a1.forestb.org\NYCVOL1\Dept Shares\Support | MELRW | CCTEC\IT Support | (0) Operation successful. |
| ✓ | FORESTB\Marketing Dept | \\win-2012-a1.forestb.org\NYCVOL1\Dept Shares\Marketing Dept | MELRW | CCTEC\Marketing ... | (0) Operation successful. |
| ✓ | FORESTB\NYC Employees | \\win-2012-a1.forestb.org\NYCVOL1\Dept Shares\Support\Software | ELR | CCTEC\NYC Emplo... | (0) Operation successful. |

Unmapped Permissions 5 | Unmapped Owners 23 | Missing Owners 10 | Add Entries | Close

For ease in identifying all unmapped (orphaned) SIDs, use the sort arrow which is located on the first column heading in the lower portion of the interface.

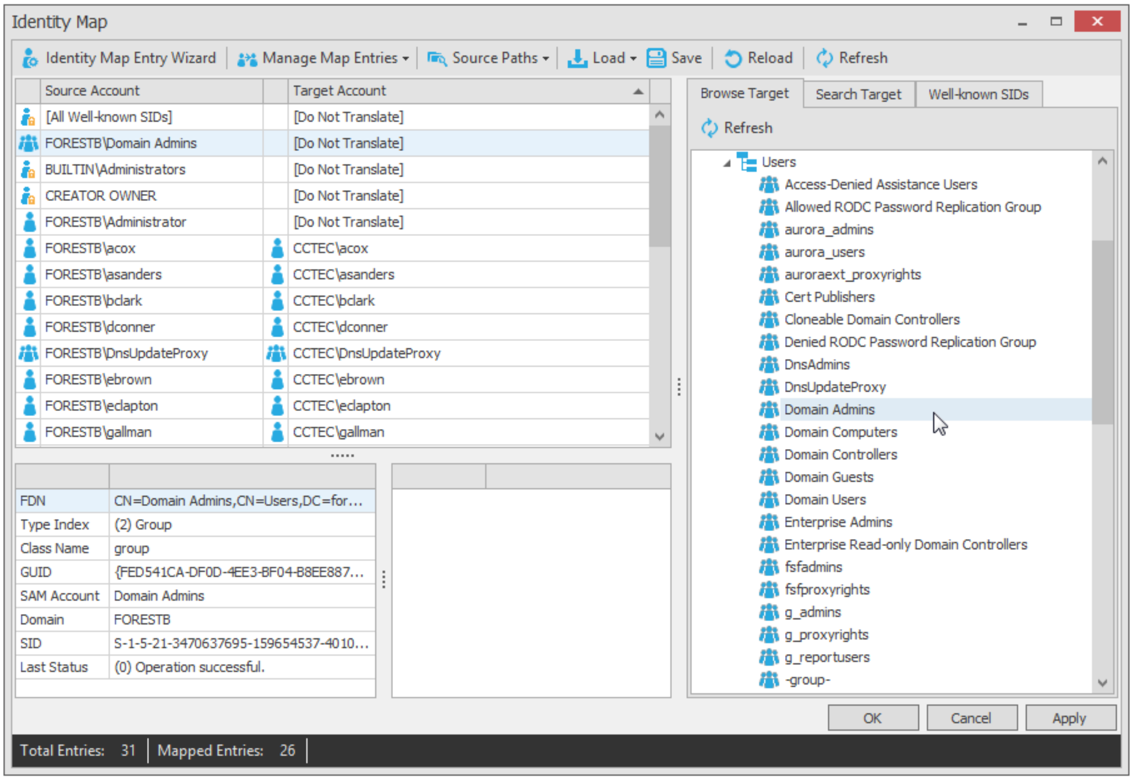
5. Click the **Owner Entries** tab and view the orphaned SIDs, meaning all of the folders and files without owners.
6. Click the **Unique IDs** tab and view the unmatched objects.

   These are objects that you will need to add to the identity map.

## 11.3.7 Add Unmapped Objects to the Identity Map

Follow these procedures to add any unmapped objects listed in the Unique IDs tab to the identity map.

1. In the identity map, click the **Target Account** column heading to sort unmapped objects so they are all listed as a group at the top of the list.
2. From the **Browser Target** tab on the right pane, locate an object you want to indicate as an owner for an unmapped object and drag the object up to the unmapped object's corresponding **Target Account** column entry.



| Source Account | Target Account |
|---|---|
| [All Well-known SIDs] | [Do Not Translate] |
| FORESTB\Domain Admins | [Do Not Translate] |
| BUILTIN\Administrators | [Do Not Translate] |
| CREATOR OWNER | [Do Not Translate] |
| FORESTB\Administrator | [Do Not Translate] |
| FORESTB\acox | CCTEC\acox |
| FORESTB\asanders | CCTEC\asanders |
| FORESTB\bclark | CCTEC\bclark |
| FORESTB\dconner | CCTEC\dconner |
| FORESTB\DnsUpdateProxy | CCTEC\DnsUpdateProxy |
| FORESTB\ebrown | CCTEC\ebrown |
| FORESTB\eclapton | CCTEC\eclapton |
| FORESTB\gallman | CCTEC\gallman |

| | |
|---|---|
| FDN | CN=Domain Admins,CN=Users,DC=for… |
| Type Index | (2) Group |
| Class Name | group |
| GUID | {FED541CA-DF0D-4EE3-BF04-B8EE887… |
| SAM Account | Domain Admins |
| Domain | FORESTB |
| SID | S-1-5-21-3470637695-159654537-4010… |
| Last Status | (0) Operation successful. |

Users
- Access-Denied Assistance Users
- Allowed RODC Password Replication Group
- aurora_admins
- aurora_users
- auroraext_proxyrights
- Cert Publishers
- Cloneable Domain Controllers
- Denied RODC Password Replication Group
- DnsAdmins
- DnsUpdateProxy
- Domain Admins
- Domain Computers
- Domain Controllers
- Domain Guests
- Domain Users
- Enterprise Admins
- Enterprise Read-only Domain Controllers
- fsfadmins
- fsfproxyrights
- g_admins
- g_proxyrights
- g_reportusers
- -group-

Total Entries: 31 | Mapped Entries: 26

   This changes the unmapped object's Target Account listing from [Do Not Translate] to the new owner object.

3. When you are finished specifying owners for your unmapped objects, click **Apply**.

## 11.3.8 Generating a Preview Report Before Migrating

You can easily generate a preview report as a CSV file before you migrate. This might be useful if you needed to provide a report to a CIP or other members of the migration team.

1. Launch SMAdmin and click the **Reports** tab.
2. Click **Preview Source Path**.
3. Double-click the top entry in the list.
4. From the View Report page, click the **CSV** icon to save the report as a CSV file.

## 11.3.9 Determine If You Are Going to Migrate the Data in Two Phases or One

Before you migrate data from the source to the target forest, you must determine if you will be migrating in two phases or one.

### Two-Phase Migration

In the first phase, you migrate all unopened files while skipping all opened files. In the second phase, you get all of your users to log off of the network (assuring that they have no files opened), then you migrate all of the skipped files, then all of the new and modified files.

A two-phased migration is more suitable to organizations with data sets to large to migrate over a weekend.

### Single-Phase Migration

This approach lets you migrate all of the data in one phase. You must have all users logged off of the network and be able to migrate the data before the users return to work.

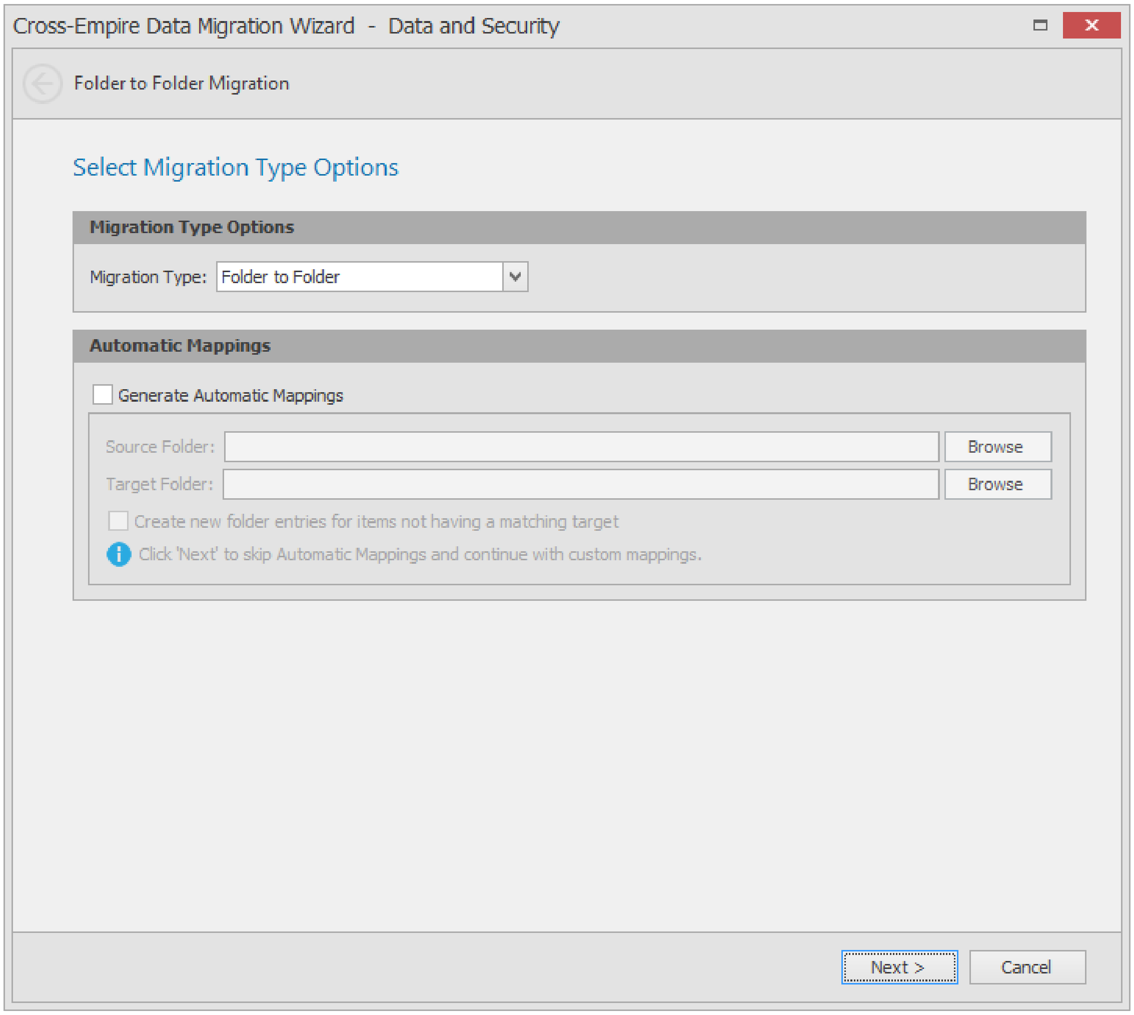
## 11.3.10 Migrate Group Data

**TIP:** To view the status of the migration, we recommend that you install and run a Tail program and use it to tail the Agent log path located at: `"%programdata%\Micro Focus\Storage Manager\Agent\log\smagent.log”`

Follow these procedures to migrate group data from the source forest to the target forest.

1. In SMAdmin, click the **Home** tab.
2. Select **Cross-Empire Data Migration** > **Active Directory to Active Directory**.
3. Select **Migration Wizards** > **Data and Security**.

   This launches the Folder to Folder Migration wizard.



Cross-Empire Data Migration Wizard - Data and Security

Folder to Folder Migration

Select Migration Type Options

Migration Type Options

Migration Type: Folder to Folder

Automatic Mappings

□ Generate Automatic Mappings

Source Folder:

Target Folder:

□ Create new folder entries for items not having a matching target

Click 'Next' to skip Automatic Mappings and continue with custom mappings.

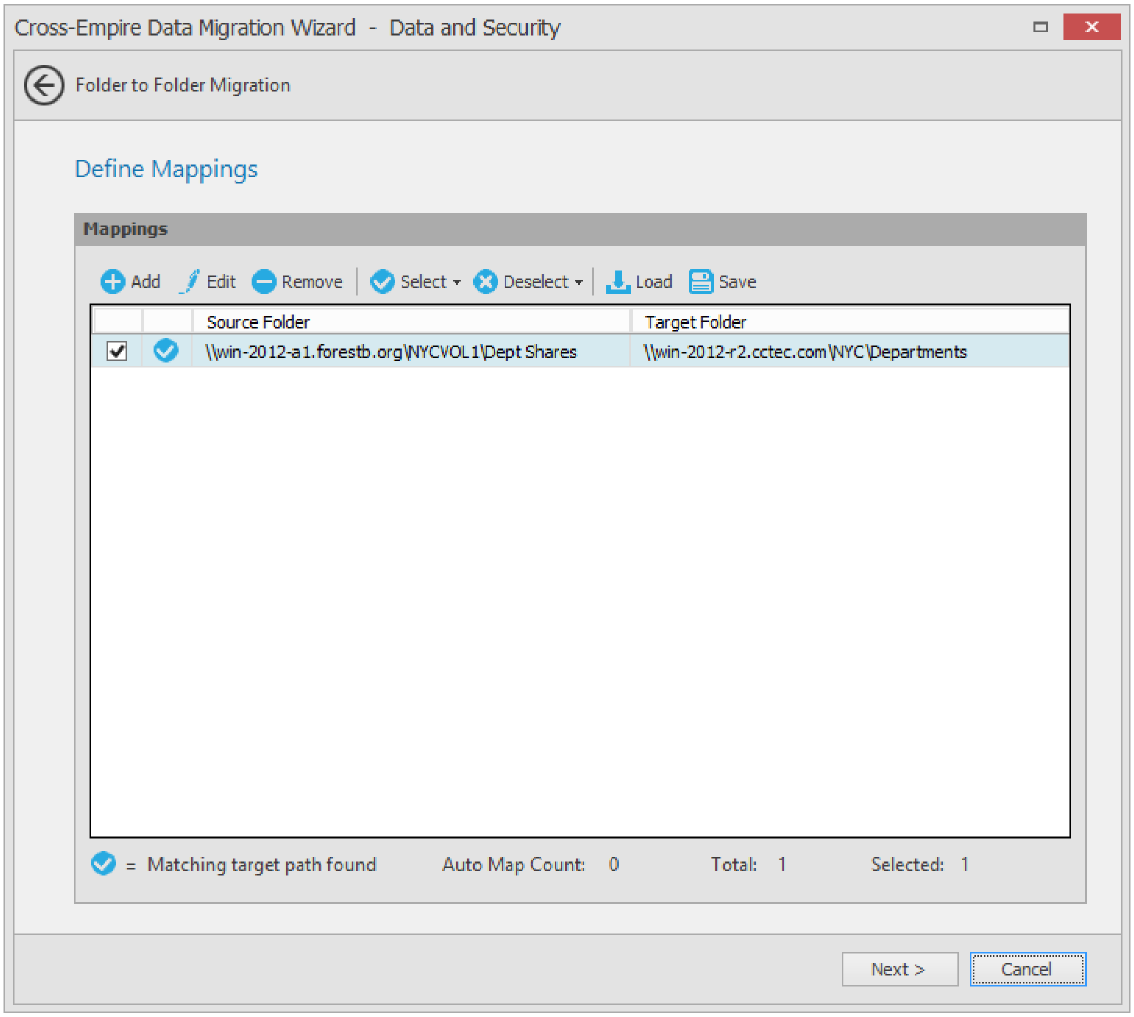
4 Do one of the following:

- If you plan to do a two-phase migration by skipping open files, leave the **Generate Automatic Mappings** check box deselected and click **Next**. Browse to specify the source and target folders and click **Next**.

  This method will create a single source path and single target path, which alleviates potential problems that can surface when skipping open files during a migration.

- If you plan to do a single-phase migration, you can select the **Generate Automatic Mappings** check box to create any needed subfolders on the target that do not already exist. Browse to specify the source and target folders and click **Next**.

5 In the Define Mappings page of the wizard, observe the migration events that are now queued up.



Cross-Empire Data Migration Wizard - Data and Security

Folder to Folder Migration

Define Mappings

Mappings

| | | Source Folder | Target Folder |
|---|---|---|---|
| ☑ | ✓ | \\win-2012-a1.forestb.org\NYCVOL1\Dept Shares | \\win-2012-r2.cctec.com\NYC\Departments |

✓ = Matching target path found  Auto Map Count: 0  Total: 1  Selected: 1

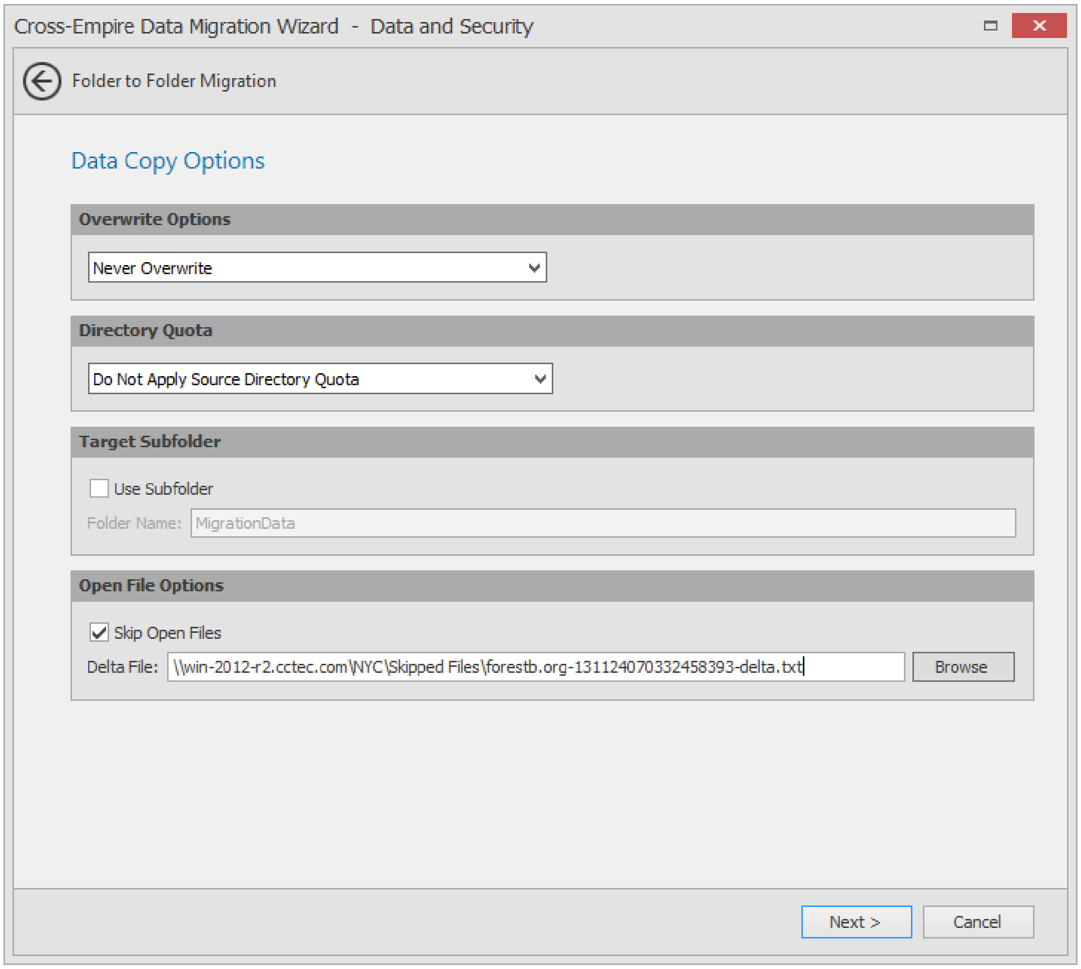
6 Click **Next**.

7 (Conditional) If you are doing a two-phase migration, in the Data Copy Options page, select the **Skip Open Files** check box.

7a Click the **Browse** button that corresponds to the **Delta File** field and through the path browser, select the folder where you want to store the delta file.

7b Right-click and select **New Folder** and click **OK**.

The delta file name is created and displayed in the **Delta File** field.



Cross-Empire Data Migration Wizard - Data and Security

Folder to Folder Migration

Data Copy Options

**Overwrite Options**

Never Overwrite

**Directory Quota**

Do Not Apply Source Directory Quota

**Target Subfolder**

□ Use Subfolder

Folder Name: MigrationData

**Open File Options**

☑ Skip Open Files

Delta File: \\win-2012-r2.cctec.com\NYC\Skipped Files\forestb.org-131124070332458393-delta.txt

8 Click **Next**.

9 In the Security and Ownership page, select the **Use the Identity Map** check box.

10 Select either the **Merge Security** or **Overwrite Security** option.

**Merge Security:** This option merges the permissions of the source folder with those of the target folder.

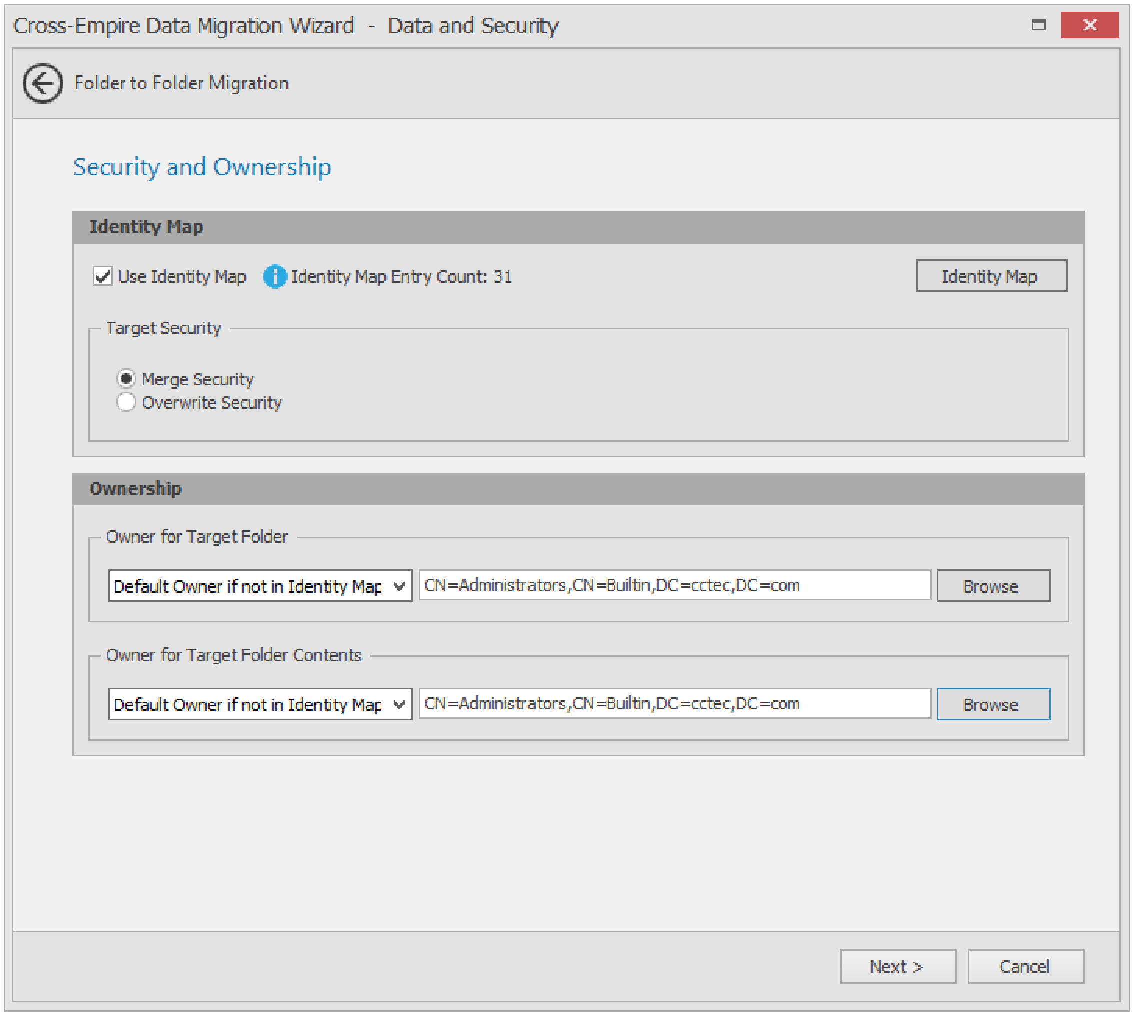
**Overwrite Security:** This option overwrites the permissions of the target folder with those of the source folder.

**11** From the **Owner for Target Folder** drop-down menu, select your preferred option.

**11a** If you select either **Default Owner if not in Identity Map** or **Set Explicit Owner,** browse to assign an owner.

**12** From the **Owner for Target Folder Contents** drop-down menu, select your preferred option.

**12a** If you select either **Default Owner if not in Identity Map** or **Set Explicit Owner,** browse to assign an owner.



Cross-Empire Data Migration Wizard - Data and Security

Folder to Folder Migration

Security and Ownership

**Identity Map**

☑ Use Identity Map   Identity Map Entry Count: 31

Target Security

● Merge Security
○ Overwrite Security

**Ownership**

Owner for Target Folder: Default Owner if not in Identity Map   CN=Administrators,CN=Builtin,DC=cctec,DC=com

Owner for Target Folder Contents: Default Owner if not in Identity Map   CN=Administrators,CN=Builtin,DC=cctec,DC=com

**13** Click **Next**.

**14** Click **Migrate**.

The queued migration events are listed.

**15** Click **Finish**.

**16** In SMAdmin, from the **Home** tab, click **Events** to view the status of the migration.

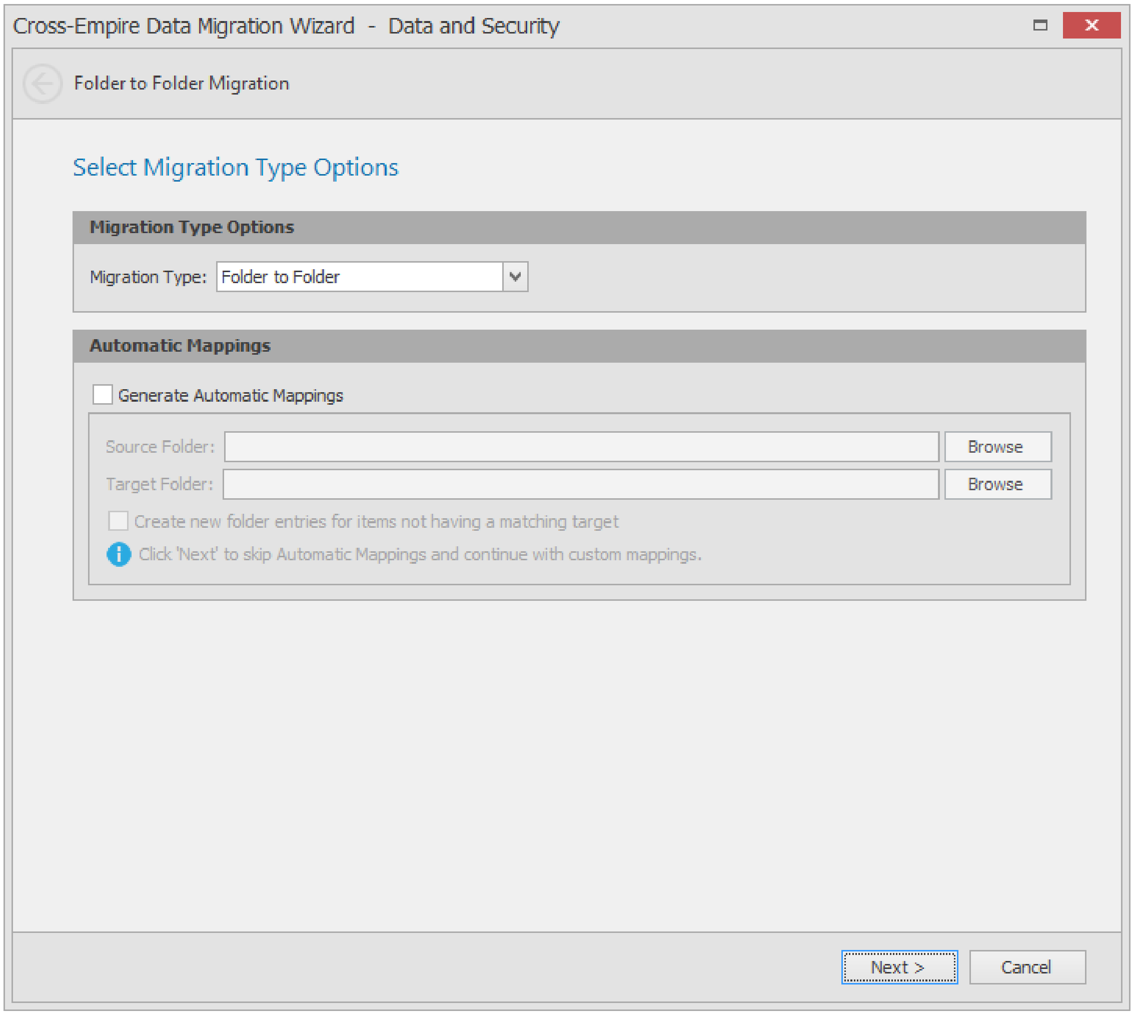
**17** (Optional) If you have a Tail program, you can view the status of the migration.

## 11.3.11 Migrate User Data

Use these procedures to migrate user home folders from the source forest to the target forest.

1. In SMAdmin, click the **Home** tab.
2. Select **Cross-Empire Data Migration** > **Active Directory to Active Directory**.
3. Select **Migration Wizards** > **Data and Security**.

   This launches the Folder to Folder Migration wizard.



Cross-Empire Data Migration Wizard - Data and Security

Folder to Folder Migration

Select Migration Type Options

Migration Type Options

Migration Type: Folder to Folder

Automatic Mappings

□ Generate Automatic Mappings

Source Folder:

Target Folder:

□ Create new folder entries for items not having a matching target

Click 'Next' to skip Automatic Mappings and continue with custom mappings.

4. Do one of the following:
   - If you plan to do a two-phase migration by skipping open files, leave the **Generate Automatic Mappings** check box deselected and click **Next**. Browse to specify the source and target folders and click **Next**.

     This method will create a single source path and single target path, which alleviates potential problems that can surface when skipping open files during a migration.
   - If you plan to do a single-phase migration, you can select the **Generate Automatic Mappings** check box to create any needed subfolders on the target that do not already exist. Browse to specify the source and target folders and click **Next**.
5. In the Define Mappings page of the wizard, observe the migration events that are now queued up.

6 Click **Next**.

7 (Conditional) If you are doing a two-phase migration, in the Data Copy Options page, select the **Skip Open Files** check box.

  7a Click the **Browse** button that corresponds to the **Delta File** field and through the path browser, select the folder of the delta file that you created previously for your group data.

8 Click **Next**.

9 In the Security and Ownership page, select the **Use the Identity Map** check box.

10 Select either the **Merge Security** or **Overwrite Security** option.

11 From the **Owner for Target Folder** and **Owner for Target Contents** drop-down menus, select **Copy Existing Source Owner**.

   As a best practice, each user should be established as the owner of their files and folders. For those instances where folders and files that aren't owned by the users, we will address them later once we create a policy and then perform Management Actions following the migration.

12 Click **Next**.

13 In the Copy Filter page, select the **User Copy Filter** check box.

14 Click **Add** to create a copy filter of those files you do not want to copy to the target forest.

   For example, you probably want to avoid copying .TMP files.

15 Click **Validate** and observe what will be migrated.

   If you observe any potential problems, you will want to correct them at this time.

16 Click **Migrate**.

   The queued migration events are listed.

17 Click **Finish**.

18 In SMAdmin, from the **Home** tab, click **Events** to view the status of the migration.

19 (Optional) If you have a Tail program, you can view the status of the migration.

## 11.3.12 Determine If Any Files Were Skipped

Follow these procedures to see if the Delta file lists any skipped files.

1 From the location where you saved the Delta file, open it to see if any files are listed.

  If any are listed, those are all of the files that were skipped during the first phase of the migration.

2 (Conditional) If files are listed, you must have the owners of these files close the files before proceeding with Section 11.3.13, "Migrate Skipped, Modified and New Files," on page 223

## 11.3.13 Migrate Skipped, Modified and New Files

Follow these procedures to migrate any files that were skipped, modified or that were created since the first phase of the migration.

1 In SMAdmin, click the **Home** tab.

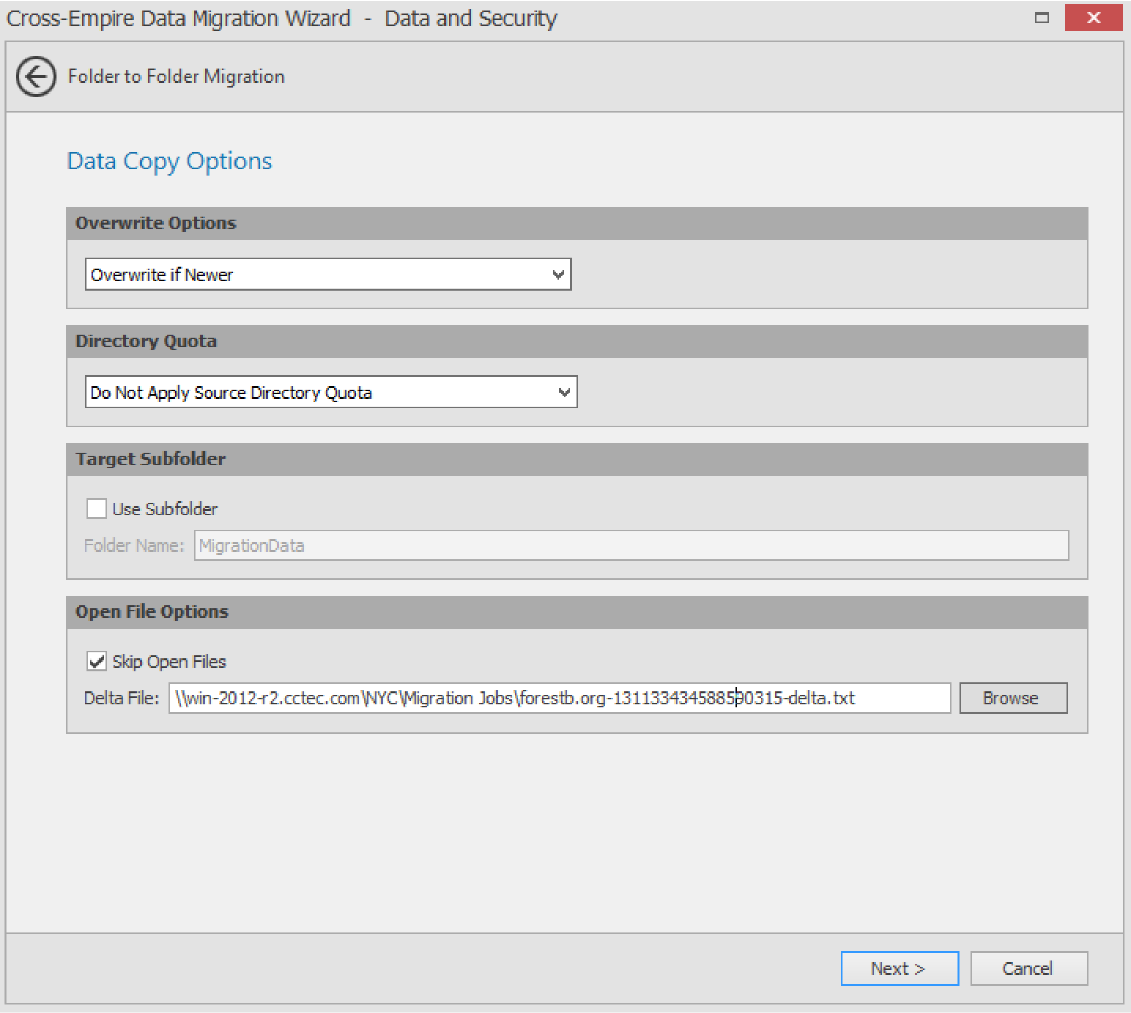
2 Select **Cross-Empire Data Migration** > **Active Directory to Active Directory**.

3 Select **Migration Wizards** > **Data and Security**.

4 In the Select Migration Type Options page, click **Next**.

5 In the Define Mappings page, specify the same source and target paths that you specified in Section 11.3.11, "Migrate User Data," on page 222 and click **Next**.

6 In the Data Copy Options page, from the **Overwrite Options** drop-down menu, select **Overwrite if Newer**, select the **Skip Open Files** check box, and browse to the location where you stored your original Delta file to create a new Delta file.


Cross-Empire Data Migration Wizard - Data and Security
Folder to Folder Migration

Data Copy Options

Overwrite Options

Overwrite if Newer

Directory Quota

Do Not Apply Source Directory Quota

Target Subfolder

□ Use Subfolder

Folder Name: MigrationData

Open File Options

☑ Skip Open Files

Delta File: \\win-2012-r2.cctec.com\NYC\Migration Jobs\forestb.org-13113343458855 0315-delta.txt

7 Click **Next**.

8 In the Security and Ownership page, select the **Use Identity Map** check box, and specify the same **Owner for Target Folder**, **Owner for Target Folder Contents**, and related paths as you did in Section 11.3.11, "Migrate User Data," on page 222.

9 Click **Next**.

10 Click **Validate** and observe what will be migrated.

If you observe any potential problems, you will want to correct them at this time.

11 Click **Migrate**.

The queued migration events are listed.

12 Click **Finish**.

13 In SMAdmin, from the **Home** tab, click **Events** to view the status of the migration.

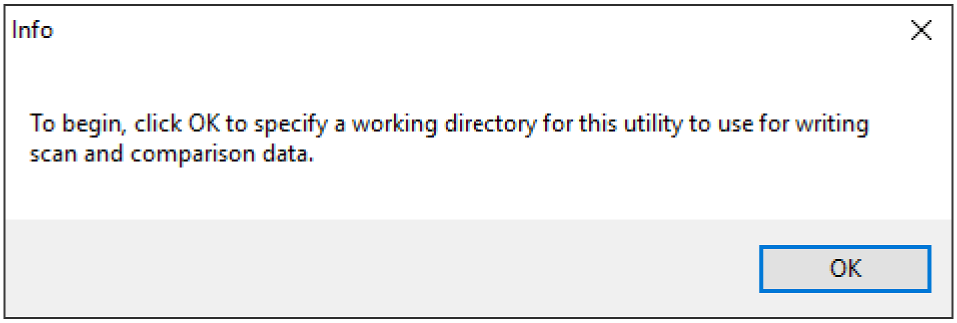
14 (Optional) If you have a Tail program, you can view the status of the migration.

## 11.3.14 Using CEDMScanCompare.exe to Compare Folders and Files Between the Source and Target

With the skipped, modified, and new files and folders migrated, you are now ready to compare the folders and files between the source and target forests to verify that everything migrated properly.

1 Launch the CEDMScanCompare utility that you copied earlier.

The following message appears:



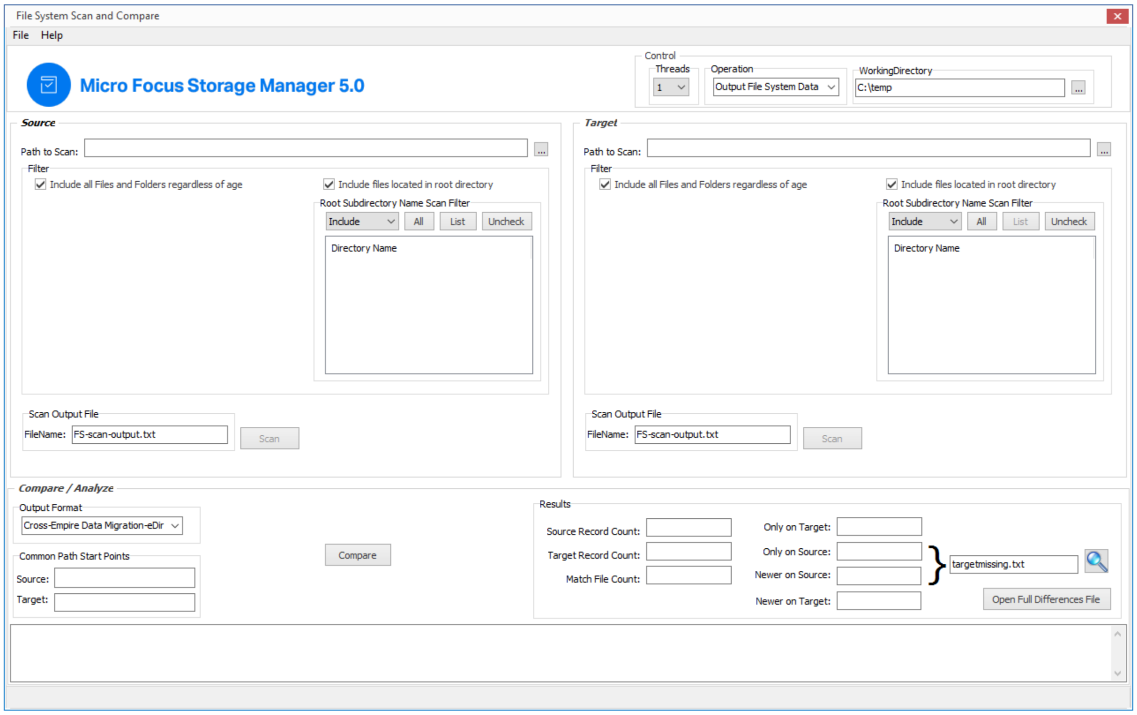
Info

To begin, click OK to specify a working directory for this utility to use for writing scan and comparison data.

2 Click **OK**.

3 Browse to a folder where you want to store the comparison data and click **Select Folder**.

The CEDMScanCompare utility interface is launched.



File System Scan and Compare

Micro Focus Storage Manager 5.0

Control: Threads: 1; Operation: Output File System Data; WorkingDirectory: C:\temp

Source: Path to Scan:

Filter: ☑ Include all Files and Folders regardless of age; ☑ Include files located in root directory

Root Subdirectory Name Scan Filter: Include

Scan Output File: FileName: FS-scan-output.txt

Target: Path to Scan:

Filter: ☑ Include all Files and Folders regardless of age; ☑ Include files located in root directory

Root Subdirectory Name Scan Filter: Include

Scan Output File: FileName: FS-scan-output.txt

Compare / Analyze: Output Format: Cross-Empire Data Migration-eDir

Common Path Start Points: Source: ; Target:

Results: Source Record Count: ; Target Record Count: ; Match File Count: ; Only on Target: ; Only on Source: ; Newer on Source: ; Newer on Target: ; targetmissing.txt

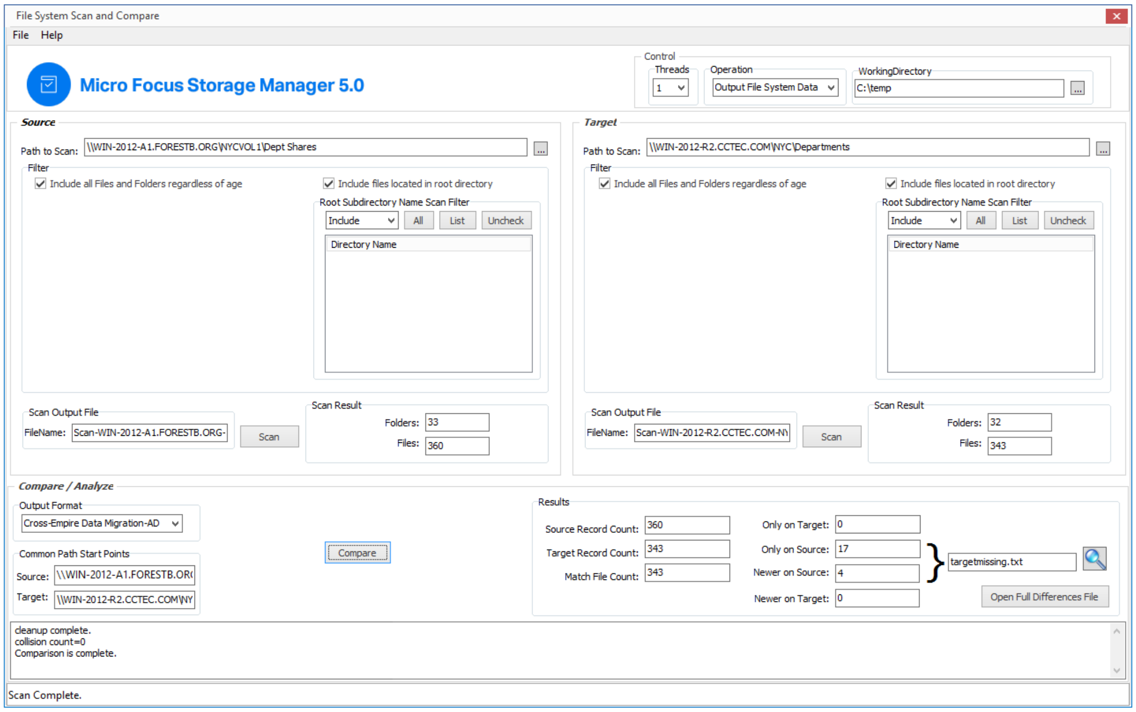
The selected folder location is specified in the **Working Directory** field.

4 In the **Source** region, for the **Path to Scan** field, browse to specify the UNC path to the folder in the source forest you want to scan.

For example: `\\WIN-2012-A1ForestB.ORG\NYCvol1\DeptShares`

5. In the **Target** region, for the **Path to Scan** field, browse to specify the UNC path to the folder in the target forest you want to scan.

   For example: `\\WIN-2012-R2.CCTEC.COM\NYC\Departments`
6. In the **Source** region, click **Scan**.
7. In the **Scan Result** region, note the findings in the **Folders** and **Files** fields.
8. In the **Target** region, click **Scan**.
9. In the **Scan Result** region, note the findings in the **Folders** and **Files** fields.
10. In the **Compare / Analyze** region, from the **FileName** drop-down menu, select **Cross-Empire Data Migration-AD**.
11. Click **Compare**.



File System Scan and Compare

Threads: 1
Operation: Output File System Data
WorkingDirectory: C:\temp

**Source**

Path to Scan: \\WIN-2012-A1.FORESTB.ORG\NYCVOL1\Dept Shares

Filter
☑ Include all Files and Folders regardless of age
☑ Include files located in root directory
Root Subdirectory Name Scan Filter: Include

Scan Output File
FileName: Scan-WIN-2012-A1.FORESTB.ORG-

Scan Result
Folders: 33
Files: 360

**Target**

Path to Scan: \\WIN-2012-R2.CCTEC.COM\NYC\Departments

Filter
☑ Include all Files and Folders regardless of age
☑ Include files located in root directory
Root Subdirectory Name Scan Filter: Include

Scan Output File
FileName: Scan-WIN-2012-R2.CCTEC.COM-NY

Scan Result
Folders: 32
Files: 343

**Compare / Analyze**

Output Format: Cross-Empire Data Migration-AD

Common Path Start Points
Source: \\WIN-2012-A1.FORESTB.ORG
Target: \\WIN-2012-R2.CCTEC.COM\NY

Results
Source Record Count: 360
Target Record Count: 343
Match File Count: 343
Only on Target: 0
Only on Source: 17
Newer on Source: 4
Newer on Target: 0
targetmissing.txt

```
cleanup complete.
collision count=0
Comparison is complete.
```

Scan Complete.

12. Do one of the following:
    - If the results show no discrepancies between the source and target, all of the folders and files were migrated. Proceed with Section 11.3.15, "Manage the Migrated User Folders through a Storage Manager Home Folder Policy," on page 227.
    - If the results show discrepancies between the source and target, follow the remaining procedures in this section.
13. Click **Open Full Differences File**.

    A spreadsheet appears listing:
    - All files on the source that are newer than the same named files on the target, along with the source and target path of each file.
    - All files on the source that are missing from the target.
14. View the files that are newer on the source server as well as those files on the source server that were not migrated.

15 Have all of your network users close any open files in the source area, and once again, follow the procedures in Section 11.3.13, “Migrate Skipped, Modified and New Files,” on page 223.

16 Run the CEDMScanCompare utility again. When the you have verified that all of the folders and files have migrated, proceed with Section 11.3.15, “Manage the Migrated User Folders through a Storage Manager Home Folder Policy,” on page 227.

## 11.3.15 Manage the Migrated User Folders through a Storage Manager Home Folder Policy

Once you have migrated all of the user data, you will want to manage it through Storage Manager. Follow these procedures to create a Home Folder policy and then enforce the policies settings through Management Actions.

### Prerequisite

If the container where you migrated the user home folders does not already have a Storage Manager policy, create a Home Folder policy by following the procedures in Section 6.5, “Creating a User Home Folder Policy,” on page 50.

### Enforcing the Policy through Management Actions

Perform the following tasks and Management Actions to enforce the policy settings on the migrated home folders.

1 Run a Consistency Check.

For more information, see Section 5.3, “Running Consistency Check Reports on Existing Storage,” on page 35.

2 Preform the following Management Actions:

- Assign Managed Path

  See “Assign Managed Path” on page 274.

- Manage

  See “Manage” on page 270.

- Apply Permissions

  See “Apply Permissions” on page 273.

- Apply Owner

  See “Apply Owner” on page 271.

# 12 Work Log Reports

## 12.1 Overview

The Work Log is a mechanism that maintains a history of Storage Manager 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 Storage Manager and requires you to install Apache CouchDB.

### 12.1.1 Restrictions

The current Work Log implementation has the following restrictions:

- 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 Storage Manager version that does not support the Work Log, 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.

### 12.1.2 Database

Due to the potentially large amount of data that can be logged, the Work Log leverages Apache CouchDB, an open source NoSQL database. The use of CouchDB is intended to provide you with the flexibility to scale your Work Log needs outside of SQL Server and to the cloud, if you prefer.

**NOTE:** Additional NoSQL databases might be supported in the future.

Figure 12-1 on page 230 depicts an environment where CouchDB is installed and deployed on a separate server in an on-premise network:

***Figure 12-1** CouchDB Deployed on a Separate, On-premise Server*

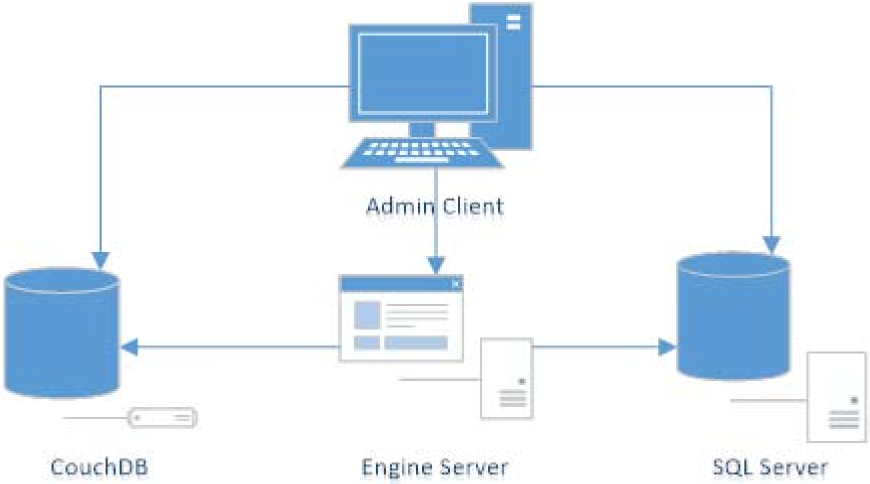
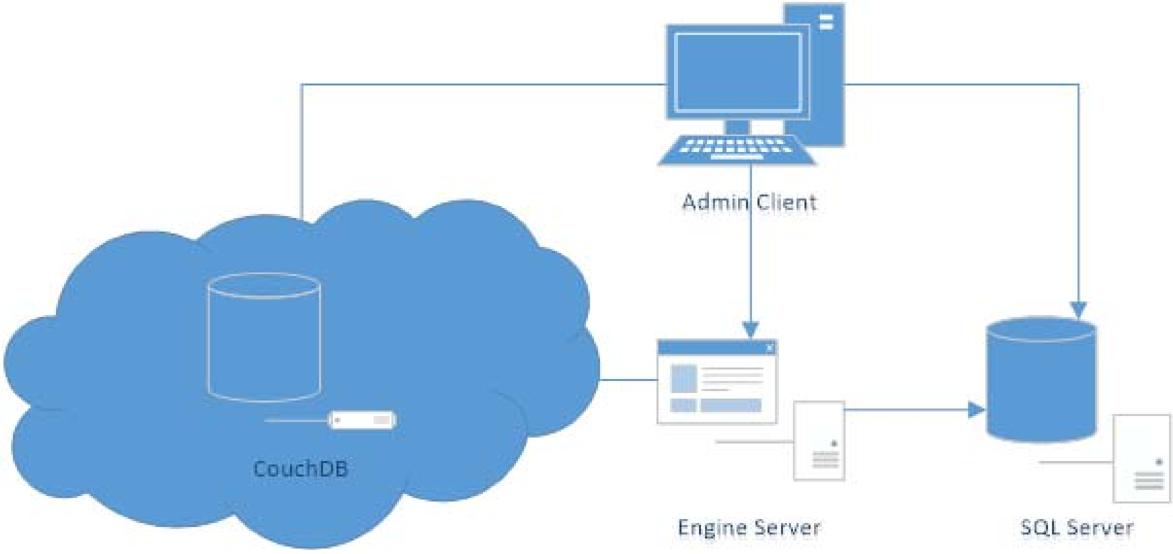


Figure 12-2 on page 230 depicts an environment where CouchDB is installed and deployed in the cloud:

***Figure 12-2** CouchDB Deployed in the Cloud*



In each deployment scenario, care must be taken to deploy CouchDB such that sufficient disk space and processing resources are available. For recommended disk space and RAM allocations, see Section 12.2, “Installing CouchDB,” on page 231.

## 12.1.3 Configuration

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

Similar to Storage Manager SQL Server configuration, the following will be created and managed for you via the Storage Manager 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

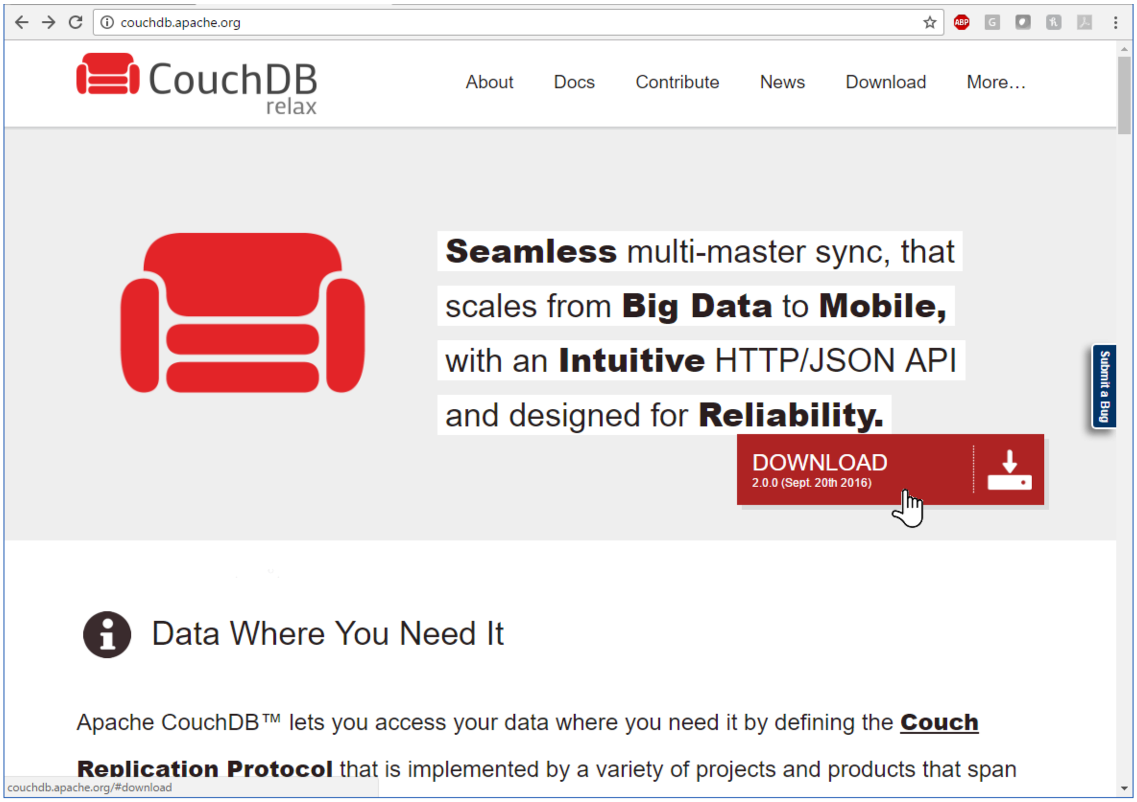
## 12.2 Installing CouchDB

### Recommendations

- Disk space requirements depend on how many events are being recorded and will vary based on the number of objects that are managed and how dynamic your environment is. A good estimate is allocating 30 MB per 100,000 stored events.
- Micro Focus recommends that the CouchDB host be a multi-processor system with a minimum of 4 GB of RAM. If you host CouchDB on a server that also hosts the Engine, Event Monitor, or SQL Server, the RAM requirements are in addition to the RAM for those services.

The following are a minimal set of procedures for installing CouchDB. For more detailed procedures, refer to the Apache CouchDB installation documentation.

1 From couchdb.apache.org, download the platform version of Couch DB 2.0 for the server that will host the CouchDB database.



**Seamless** multi-master sync, that scales from **Big Data** to **Mobile,** with an **Intuitive** HTTP/JSON API and designed for **Reliability.**

Data Where You Need It

Apache CouchDB™ lets you access your data where you need it by defining the **Couch Replication Protocol** that is implemented by a variety of projects and products that span

2 Launch the downloaded installation file.

3 Follow the wizard steps to complete the installation.

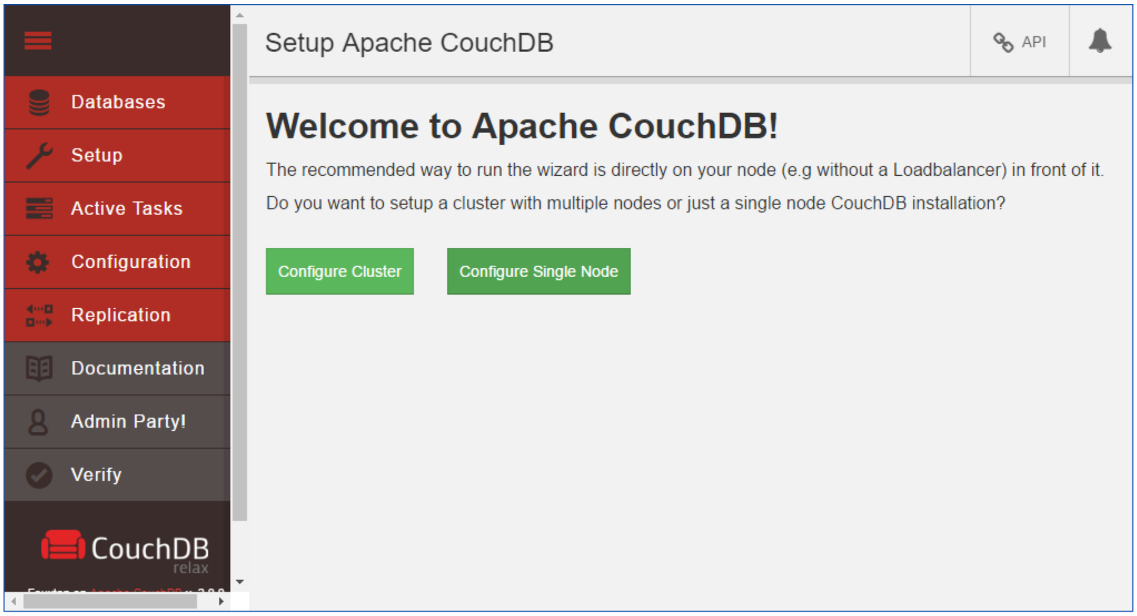
4 (Conditional) if you are logged in as a built-in administrator, you must log out and then log in as a user with administrative permissions.

CouchDB requires that the database be administered through a user account with administrative permissions rather than through the server's built-in administrator.

5 Launch Apache CouchDB Fauxton.

This launches the Apache CouchDB administrative interface in a web browser.

6 Click **Setup**.

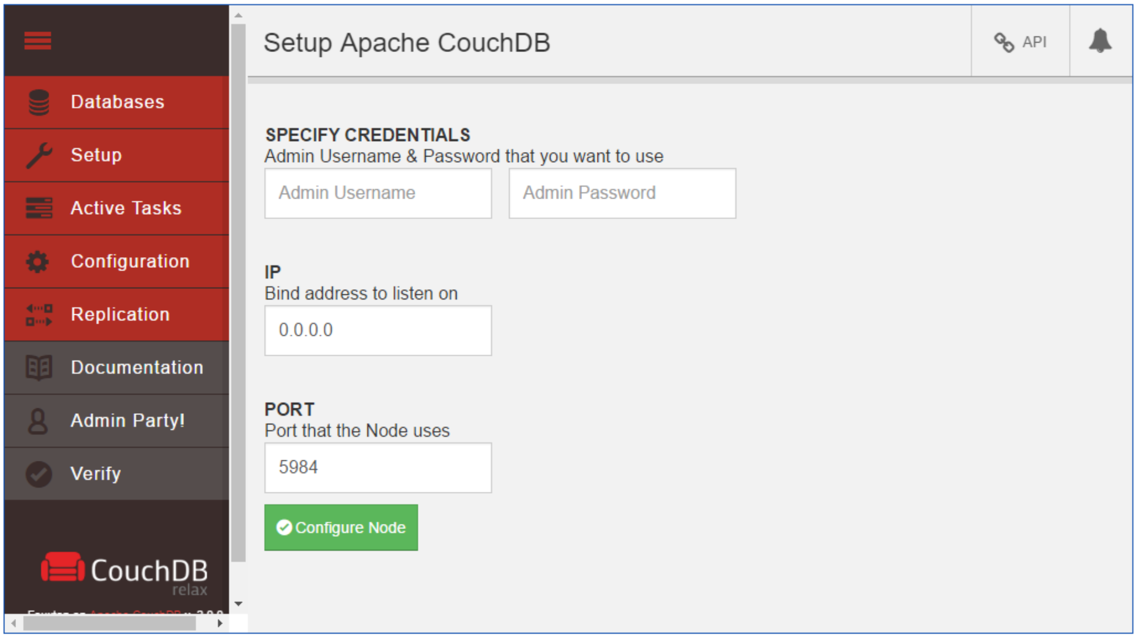


**Welcome to Apache CouchDB!**

The recommended way to run the wizard is directly on your node (e.g without a Loadbalancer) in front of it.

Do you want to setup a cluster with multiple nodes or just a single node CouchDB installation?

7 Click **Configure Single Node**.



SPECIFY CREDENTIALS
Admin Username & Password that you want to use
Admin Username
Admin Password

IP
Bind address to listen on
0.0.0.0

PORT
Port that the Node uses
5984

8 Specify a new administrator username and password, leave the **IP** address setting open, and leave the **Port** setting at 5984, then click **Configure Node**.

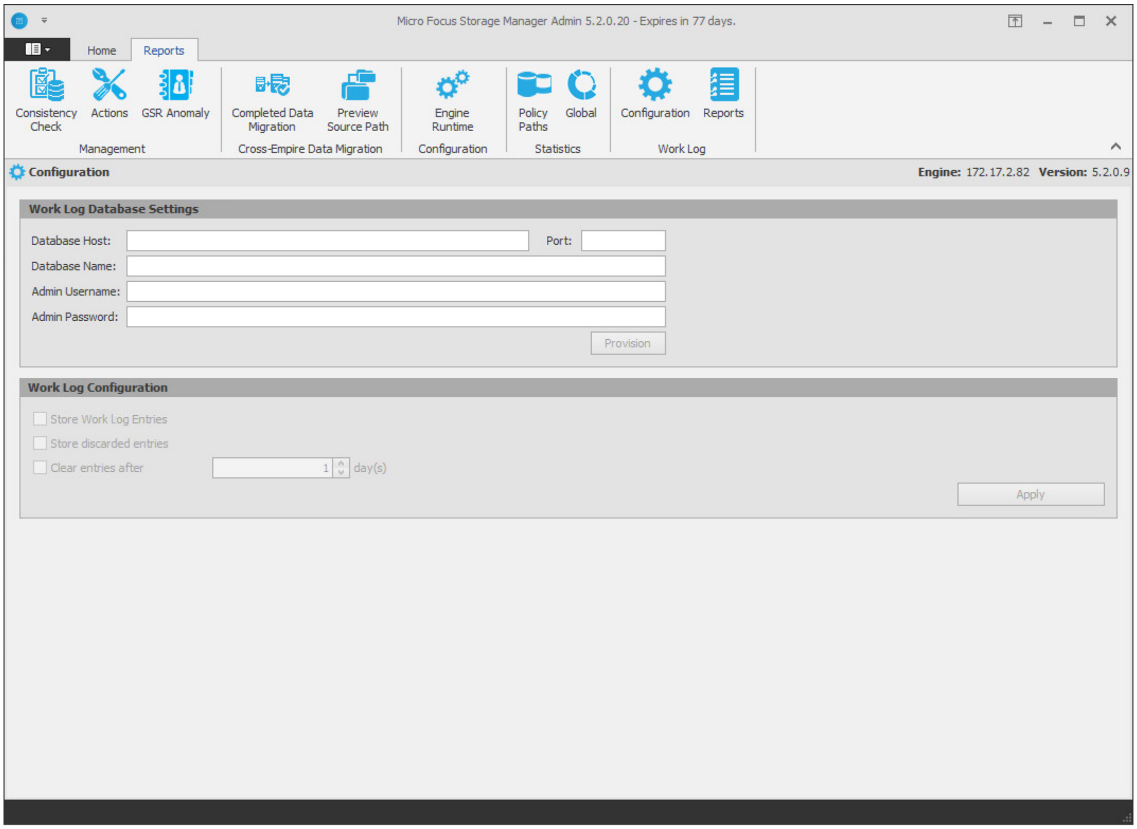
9 Proceed with Section 12.3, “Establishing the Work Log Database Settings in SMAdmin,” on page 233

## 12.3 Establishing the Work Log Database Settings in SMAdmin

Follow these procedures to establish the CouchDB settings in SMAdmin.

1 In SMAdmin, click the **Reports** tab.

2 Click **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 Step 8 on page 233.

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 SMAdmin and in the **Work Log Configuration** region, specify the settings you want for Work Log entries.

9 Click **Apply**.

# 12.4 Building Work Log Reports

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

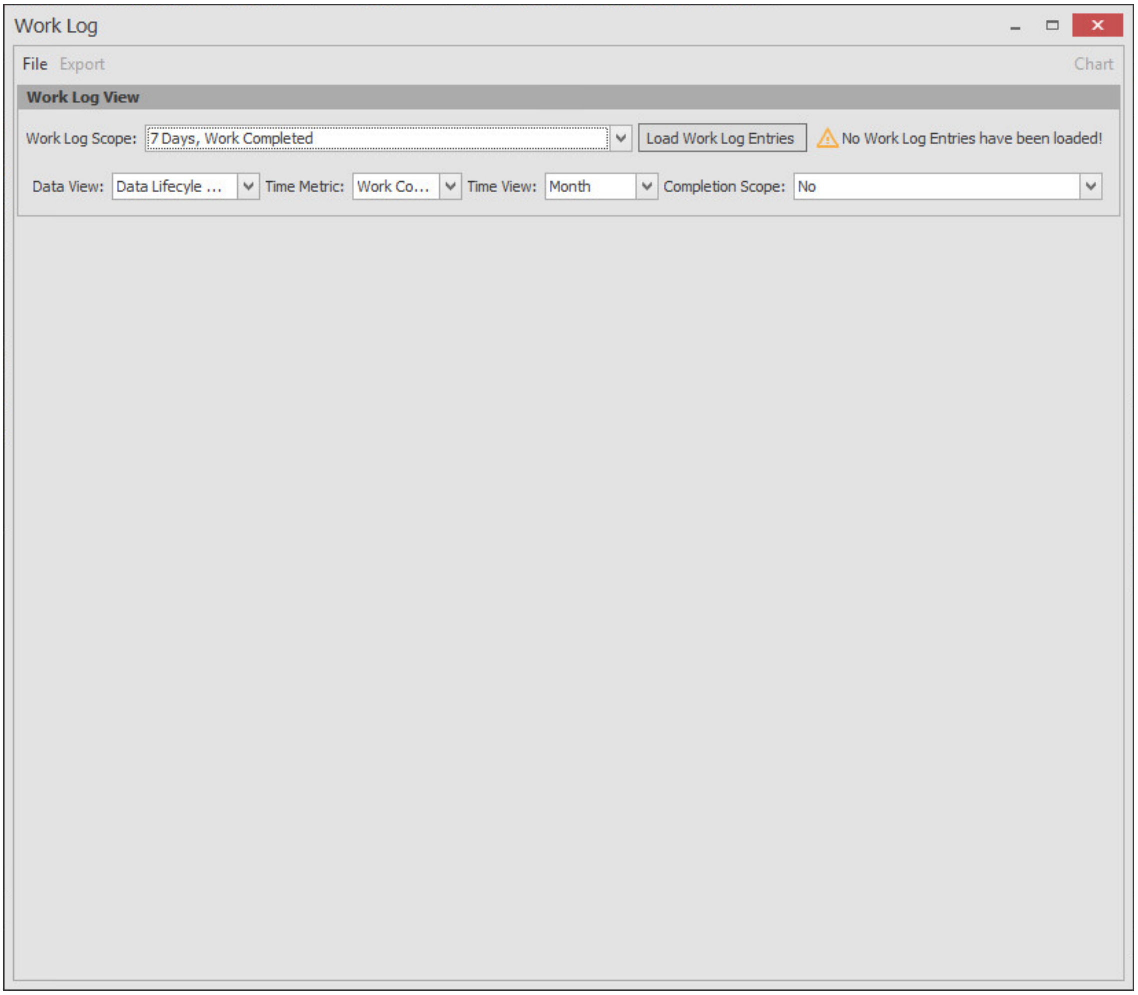
Work Log reports are built in SMAdmin using a pivot grid interface. There are four preset options for viewing data, along with a playground option that lets you choose the parameters and presentation of the report.

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

## 12.4.1 Loading Work Log Entries

1 In SMAdmin, click the **Reports** tab.

2 Click **Reports**.

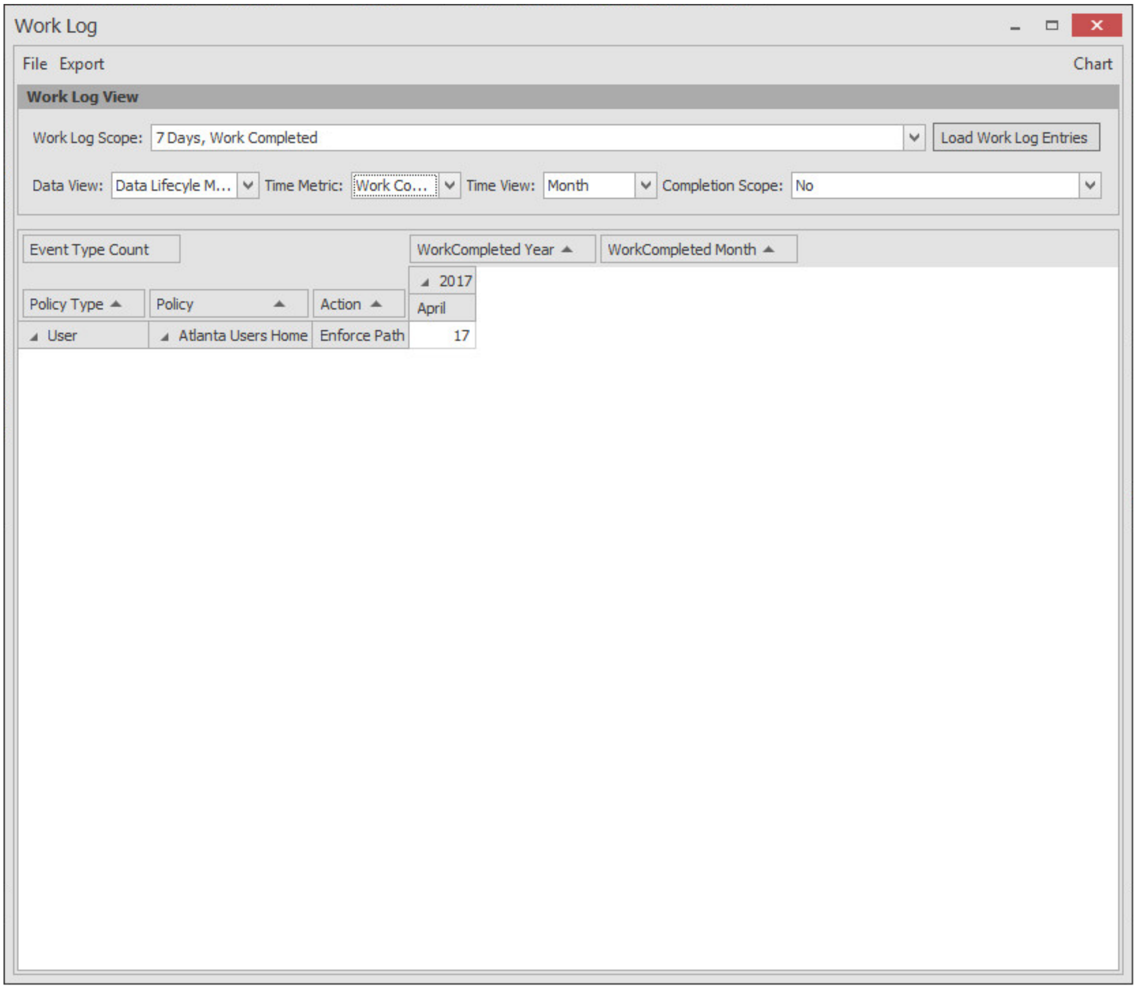


Work Log Scope: 7 Days, Work Completed

⚠ No Work Log Entries have been loaded!

Data View: Data Lifecyle ... Time Metric: Work Co... Time View: Month Completion Scope: No

3 Click Load **Work Log Entries**.



Work Log Scope: 7 Days, Work Completed

Data View: Data Lifecyle M… Time Metric: Work Co… Time View: Month Completion Scope: No

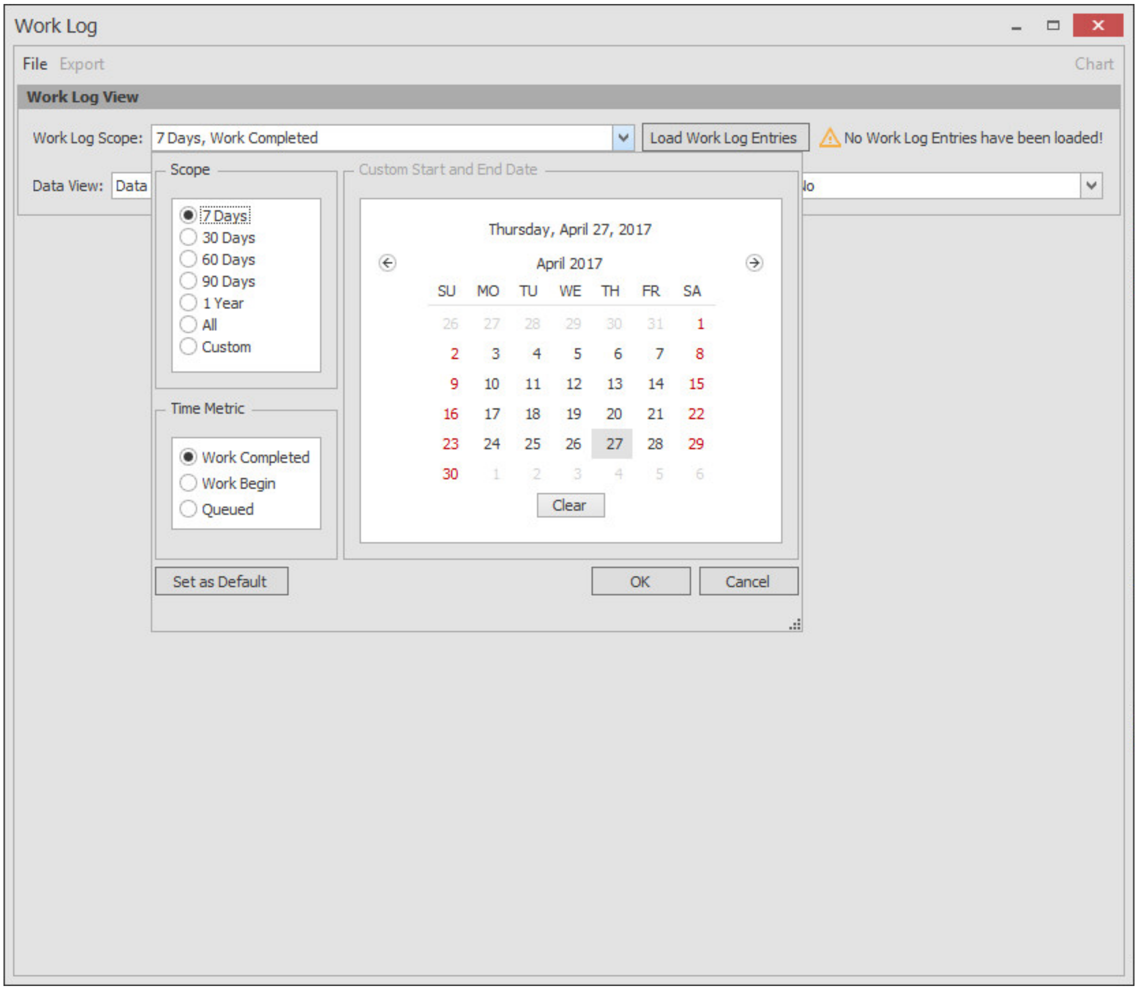
Event Type Count

| | | | WorkCompleted Year / WorkCompleted Month |
|---|---|---|---|
| | | | 2017 |
| Policy Type | Policy | Action | April |
| User | Atlanta Users Home | Enforce Path | 17 |

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

## 12.4.2 Setting the Work Log Scope

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



Work Log Scope: 7 Days, Work Completed

No Work Log Entries have been loaded!

Scope: ● 7 Days

Time Metric: ● Work Completed

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.

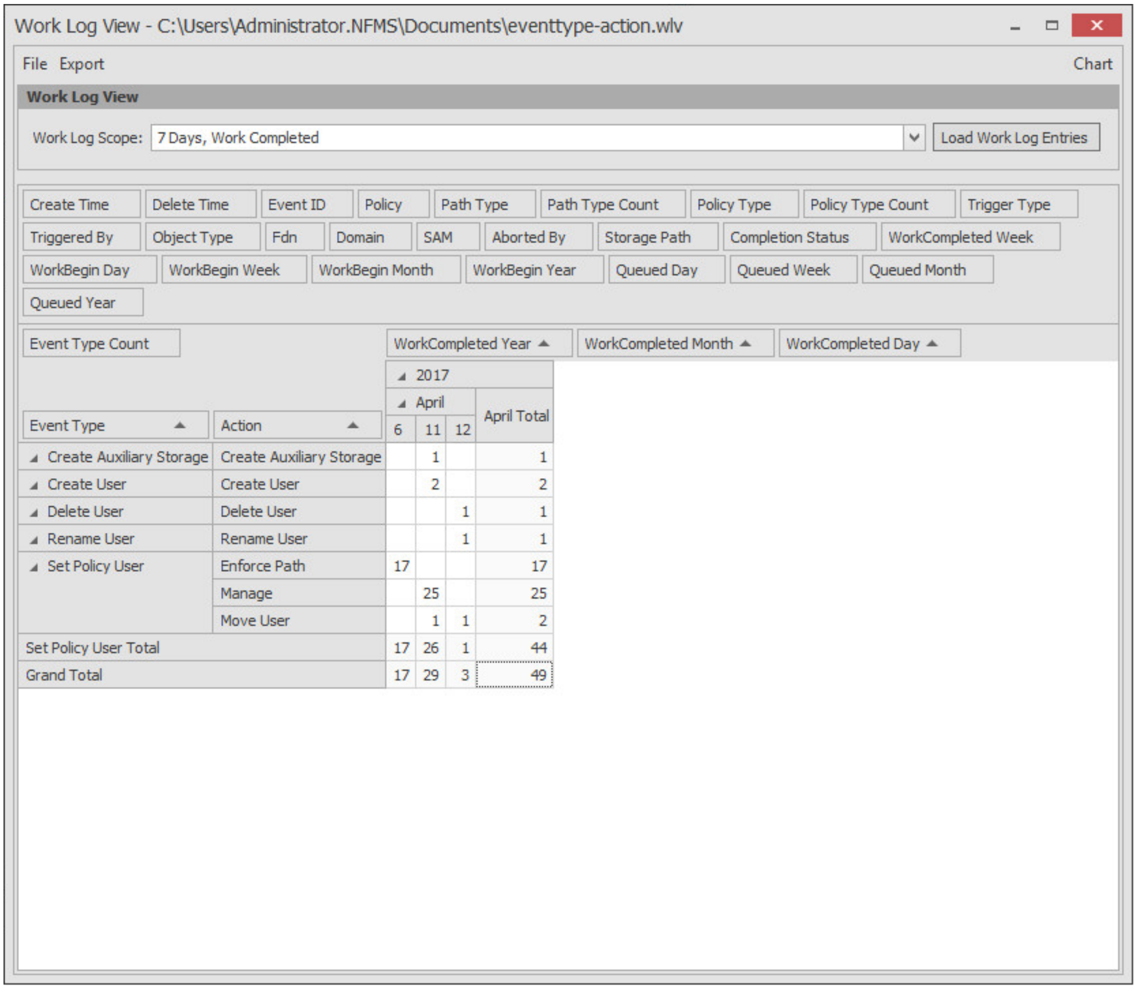
3 Click **OK**.

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

## 12.4.3 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.



Work Log Scope: 7 Days, Work Completed

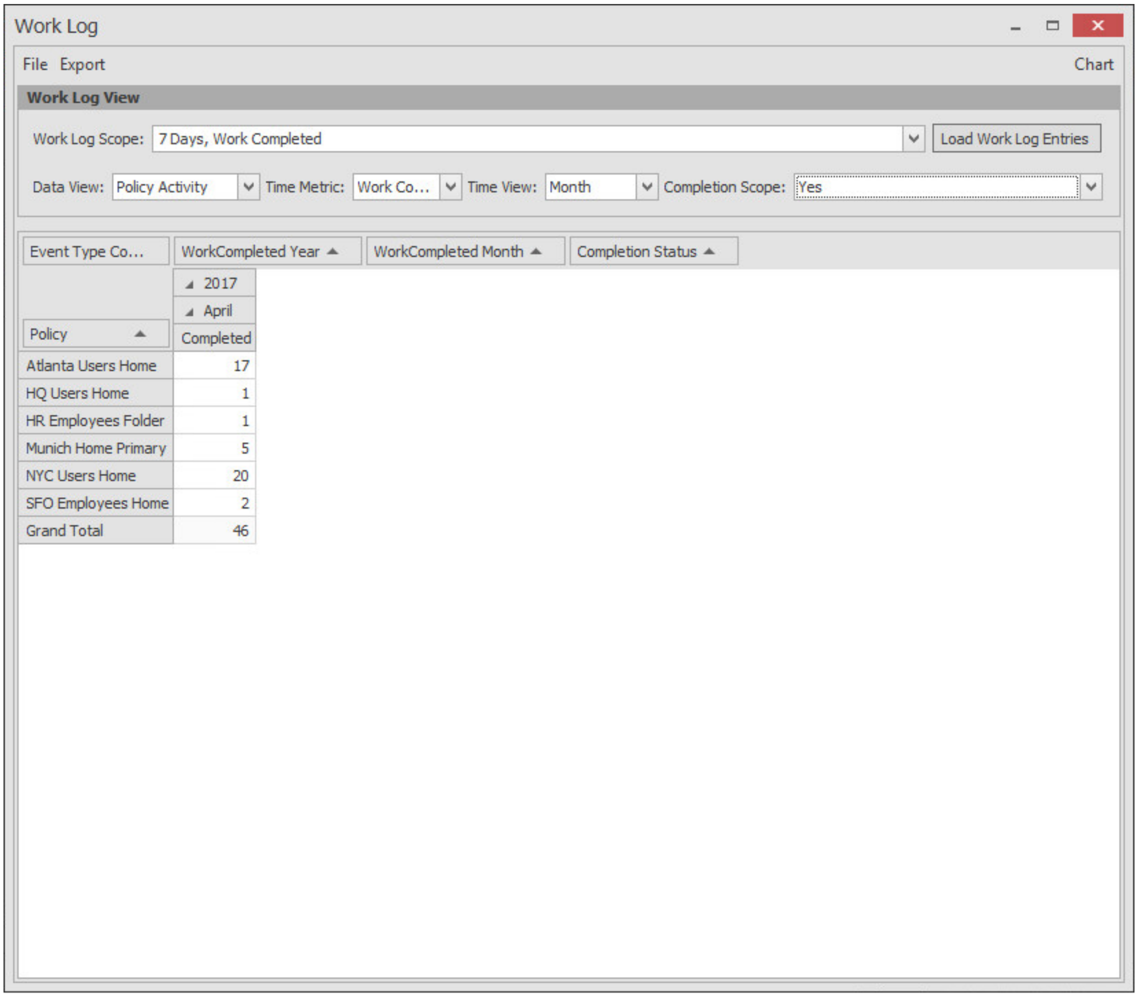
| Event Type Count | | 2017 | | | |
|---|---|---|---|---|---|
| | | April | | | April Total |
| Event Type | Action | 6 | 11 | 12 | |
| Create Auxiliary Storage | Create Auxiliary Storage | | 1 | | 1 |
| Create User | Create User | | 2 | | 2 |
| Delete User | Delete User | | | 1 | 1 |
| Rename User | Rename User | | | 1 | 1 |
| Set Policy User | Enforce Path | 17 | | | 17 |
| | Manage | | 25 | | 25 |
| | Move User | | 1 | 1 | 2 |
| Set Policy User Total | | 17 | 26 | 1 | 44 |
| Grand Total | | 17 | 29 | 3 | 49 |

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 Storage Manager events for the Month of April 2017.



Work Log Scope: 7 Days, Work Completed

Data View: Policy Activity  Time Metric: Work Co...  Time View: Month  Completion Scope: Yes

Event Type Co... | WorkCompleted Year | WorkCompleted Month | Completion Status

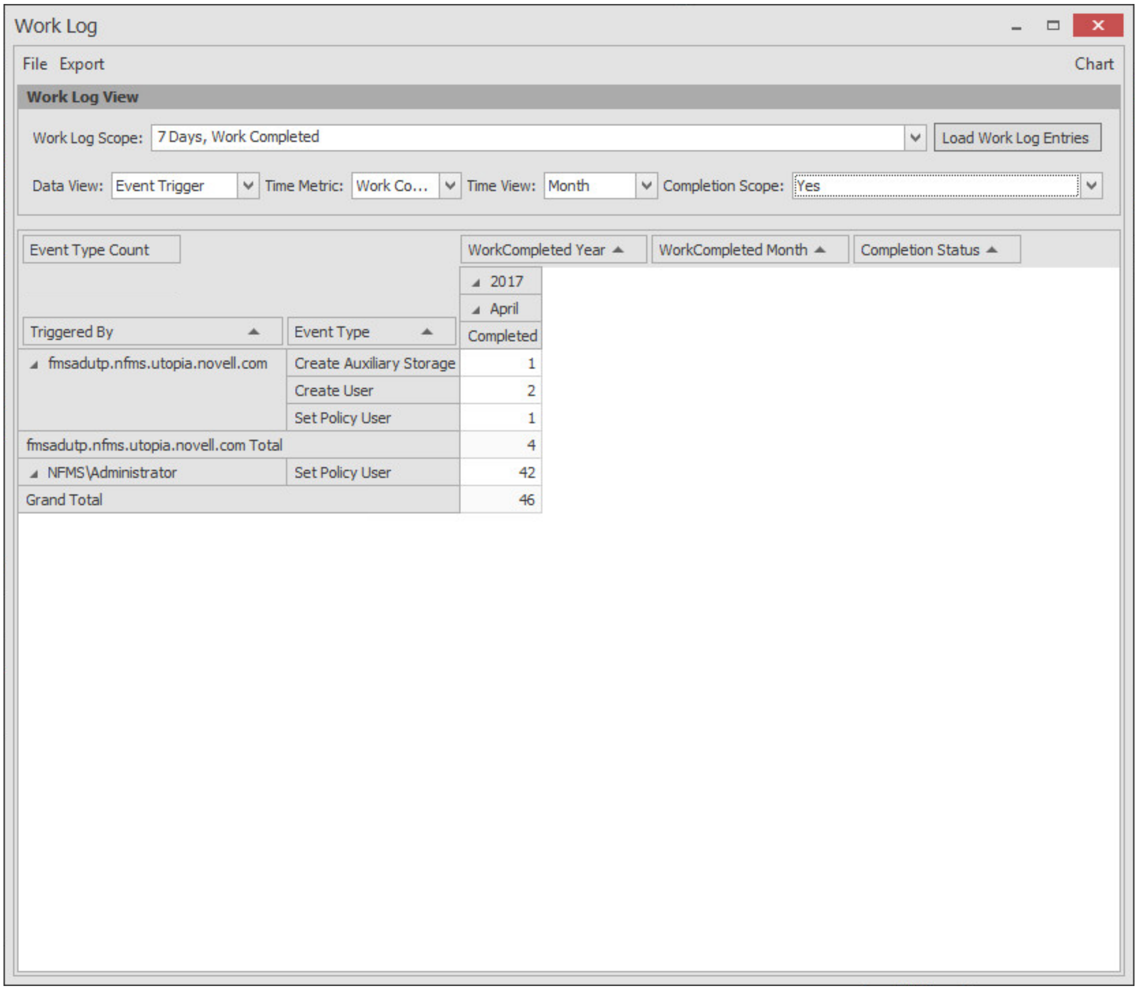
| Policy | 2017<br>April<br>Completed |
|---|---|
| Atlanta Users Home | 17 |
| HQ Users Home | 1 |
| HR Employees Folder | 1 |
| Munich Home Primary | 5 |
| NYC Users Home | 20 |
| SFO Employees Home | 2 |
| Grand Total | 46 |

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 Storage Manager 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 April 2017.



Work Log Scope: 7 Days, Work Completed

Data View: Event Trigger  Time Metric: Work Co...  Time View: Month  Completion Scope: Yes

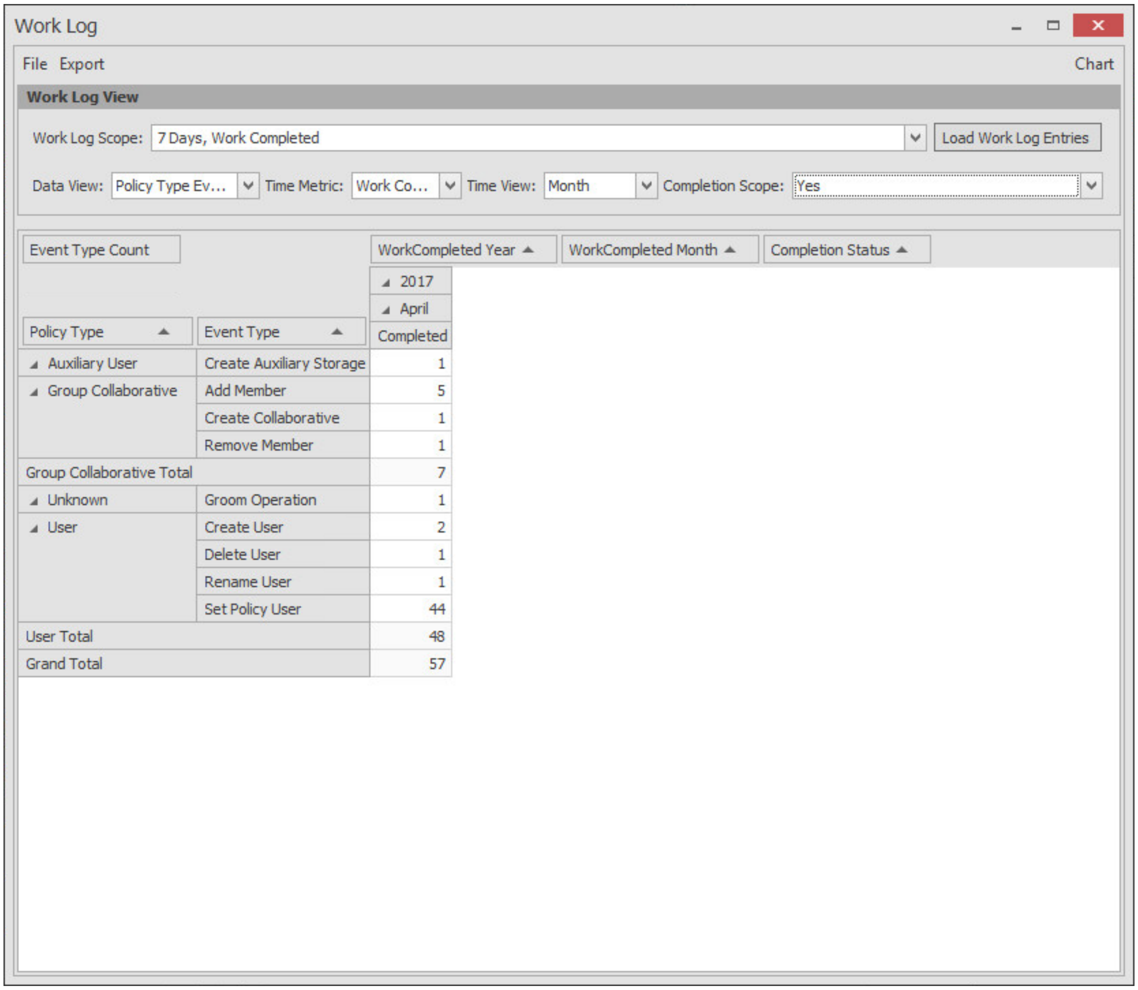
| Event Type Count | | 2017 |
|---|---|---|
| | | April |
| Triggered By | Event Type | Completed |
| fmsadutp.nfms.utopia.novell.com | Create Auxiliary Storage | 1 |
| | Create User | 2 |
| | Set Policy User | 1 |
| fmsadutp.nfms.utopia.novell.com Total | | 4 |
| NFMS\Administrator | Set Policy User | 42 |
| Grand Total | | 46 |

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 Storage Manager 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 April 2017.



Work Log Scope: 7 Days, Work Completed

Data View: Policy Type Ev… Time Metric: Work Co… Time View: Month Completion Scope: Yes

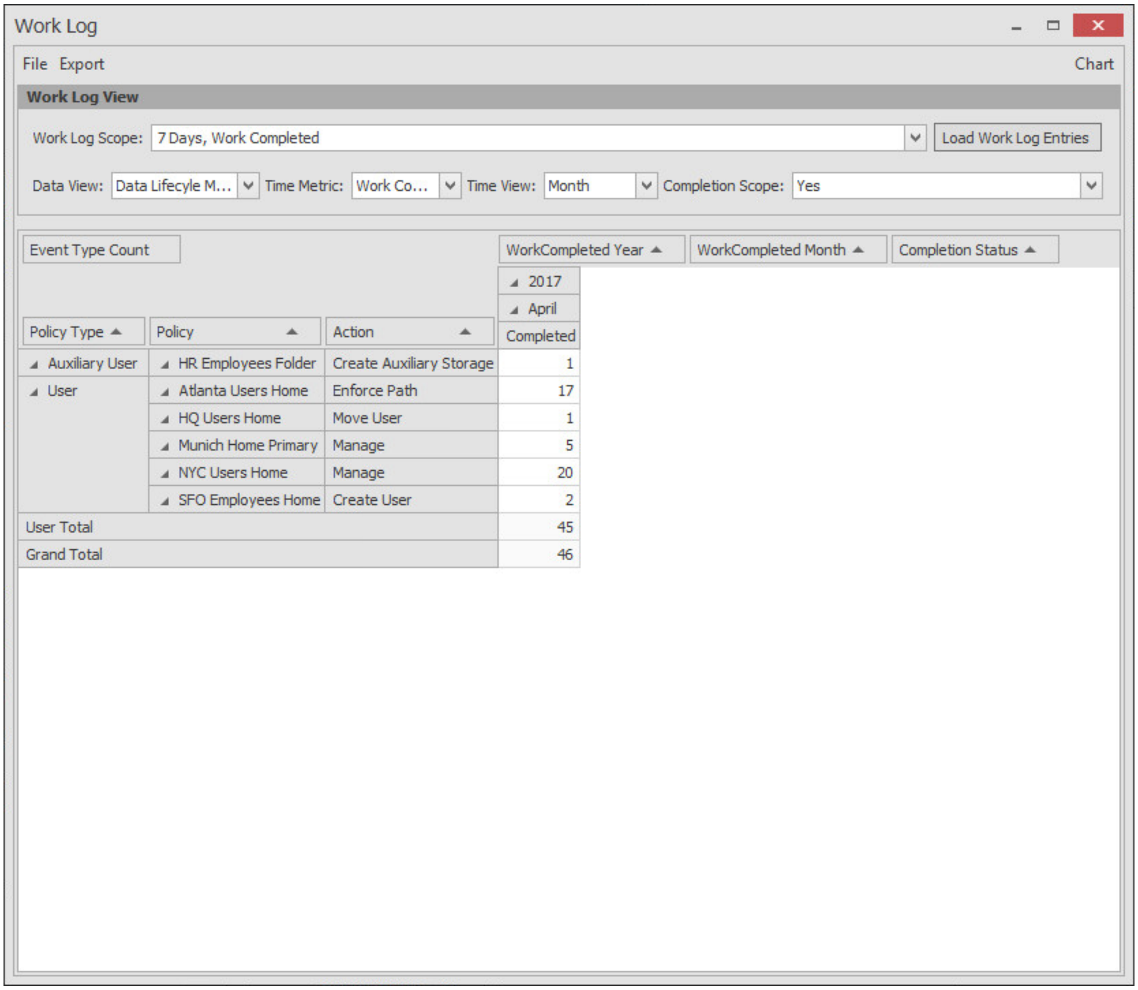
| | | 2017 |
|---|---|---|
| | | April |
| Policy Type | Event Type | Completed |
| Auxiliary User | Create Auxiliary Storage | 1 |
| Group Collaborative | Add Member | 5 |
| | Create Collaborative | 1 |
| | Remove Member | 1 |
| Group Collaborative Total | | 7 |
| Unknown | Groom Operation | 1 |
| User | Create User | 2 |
| | Delete User | 1 |
| | Rename User | 1 |
| | Set Policy User | 44 |
| User Total | | 48 |
| Grand Total | | 57 |

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 April 2017.



Work Log View

Work Log Scope: 7 Days, Work Completed

Data View: Data Lifecyle M... Time Metric: Work Co... Time View: Month Completion Scope: Yes

Event Type Count

WorkCompleted Year ▲ WorkCompleted Month ▲ Completion Status ▲

| Policy Type ▲ | Policy ▲ | Action ▲ | 2017<br>April<br>Completed |
|---|---|---|---|
| Auxiliary User | HR Employees Folder | Create Auxiliary Storage | 1 |
| User | Atlanta Users Home | Enforce Path | 17 |
| | HQ Users Home | Move User | 1 |
| | Munich Home Primary | Manage | 5 |
| | NYC Users Home | Manage | 20 |
| | SFO Employees Home | Create User | 2 |
| User Total | | | 45 |
| Grand Total | | | 46 |

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.

## 12.4.4 Build a Work Log Report

1. In SMAdmin, click the **Reports** 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.

## 12.4.5 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 SMAdmin, click the **Reports** 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.

## 12.4.6 Exporting a Work Log Report

Storage Manager enables you to export Work Log reports to the following formats:

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

1. In SMAdmin, click the **Reports** 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.

# 13 Reference

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

## 13.1 Home Tab

The **Home** tab provides access to the active management interfaces for Storage Manager. You use the **Home** tab to create, edit, deploy, and analyze Storage Manager policies, as well as perform a variety of other management tasks.

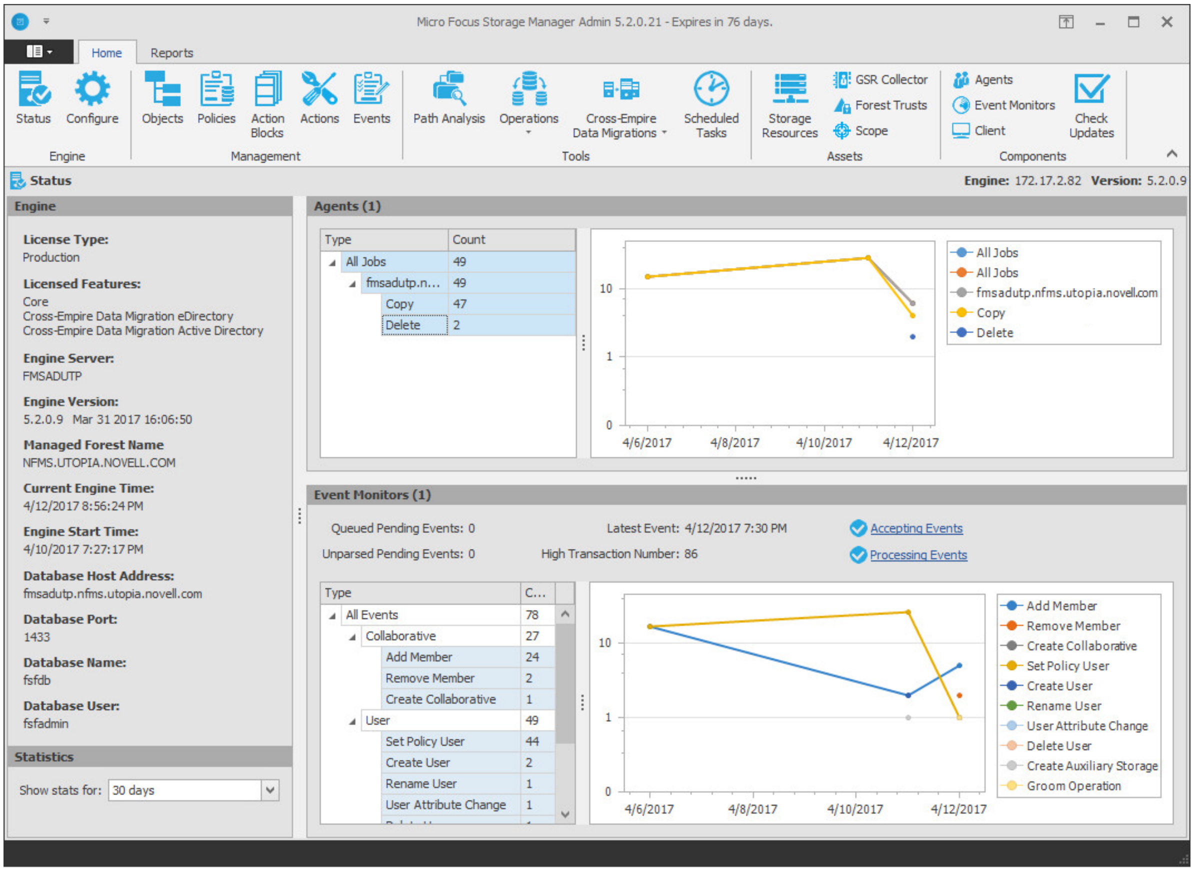
### 13.1.1 Status

The Status page provides status information on the Engine and the database.

If you are not seeing Storage Manager enact actions after events in Active Directory take place, viewing whether the Engine is processing and accepting events through this page is a good first step in troubleshooting.

Details pertaining to events are indicated in different regions of the page. The **Agents** region enumerates events enacted by the Agents. The **Event Monitors** region enumerates events enacted as a result of Active Directory events. By holding down the Control key and selecting table cells, you can specify what parameters are graphed over a selected number of days. The **Engine** region provides a summary of details pertaining to the Engine.

***Figure 13-1*** *Status Page*



**Engine:** 172.17.2.82 **Version:** 5.2.0.9

**Engine**

**License Type:**
Production

**Licensed Features:**
Core
Cross-Empire Data Migration eDirectory
Cross-Empire Data Migration Active Directory

**Engine Server:**
FMSADUTP

**Engine Version:**
5.2.0.9 Mar 31 2017 16:06:50

**Managed Forest Name**
NFMS.UTOPIA.NOVELL.COM

**Current Engine Time:**
4/12/2017 8:56:24 PM

**Engine Start Time:**
4/10/2017 7:27:17 PM

**Database Host Address:**
fmsadutp.nfms.utopia.novell.com

**Database Port:**
1433

**Database Name:**
fsfdb

**Database User:**
fsfadmin

Show stats for: 30 days

| Type | Count |
|---|---|
| All Jobs | 49 |
| fmsadutp.n... | 49 |
| Copy | 47 |
| Delete | 2 |

Queued Pending Events: 0 Latest Event: 4/12/2017 7:30 PM Accepting Events

Unparsed Pending Events: 0 High Transaction Number: 86 Processing Events

| Type | C... |
|---|---|
| All Events | 78 |
| Collaborative | 27 |
| Add Member | 24 |
| Remove Member | 2 |
| Create Collaborative | 1 |
| User | 49 |
| Set Policy User | 44 |
| Create User | 2 |
| Rename User | 1 |
| User Attribute Change | 1 |

## 13.1.2 Configure

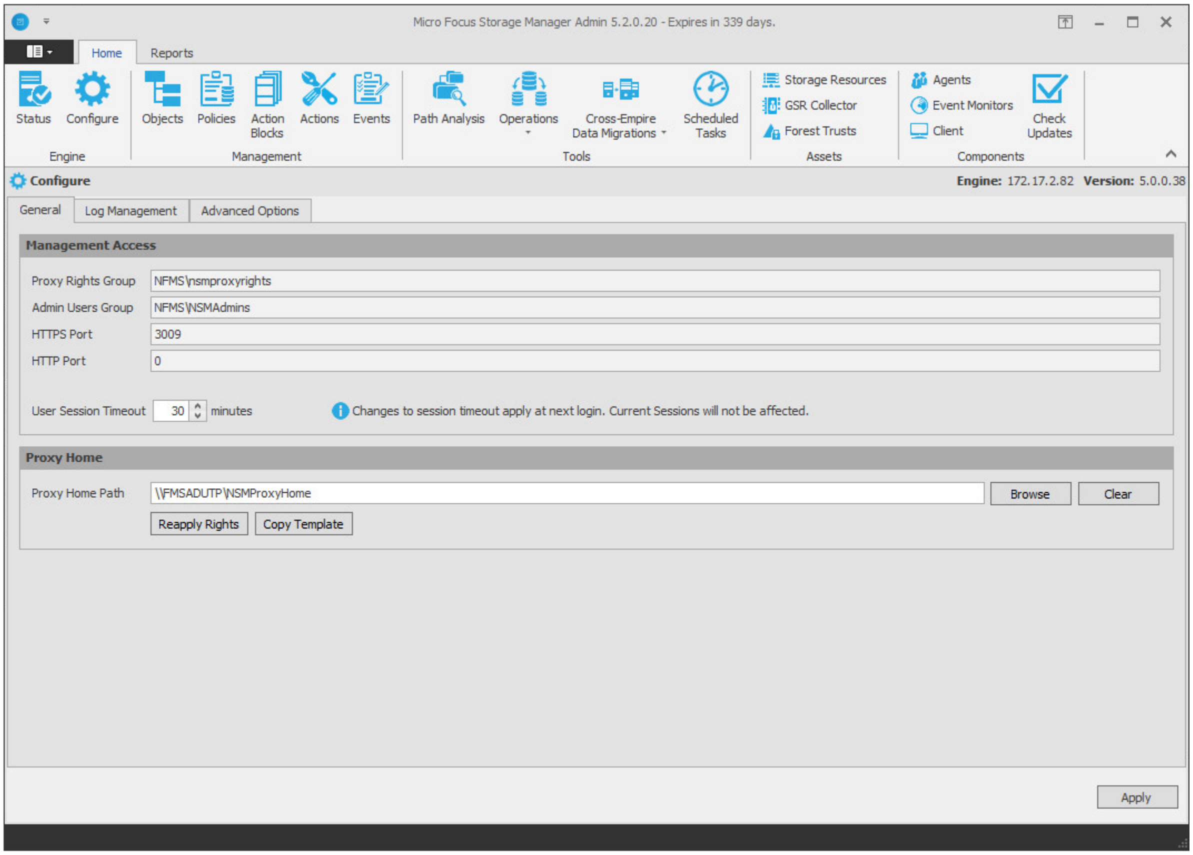
This page lets you view and set Engine configuration settings.

- "General" on page 246
- "Log Management" on page 248
- "Advanced Options" on page 249

### General

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

***Figure 13-2*** *The General Tab of the Configure Page*



Micro Focus Storage Manager Admin 5.2.0.20 - Expires in 339 days.

**Engine:** 172.17.2.82 **Version:** 5.0.0.38

Proxy Rights Group: NFMS\nsmproxyrights

Admin Users Group: NFMS\NSMAdmins

HTTPS Port: 3009

HTTP Port: 0

User Session Timeout: 30 minutes

Changes to session timeout apply at next login. Current Sessions will not be affected.

Proxy Home Path: \\FMSADUTP\NSMProxyHome

**Proxy Rights Group:** Displays the Proxy Rights Group that you established when you installed Storage Manager.

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

**HTTPS Port:** Displays the HTTPS port that you chose when you installed Storage Manager.

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

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

**Proxy Home Path:** This path was established during the installation of SMAdmin. 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.

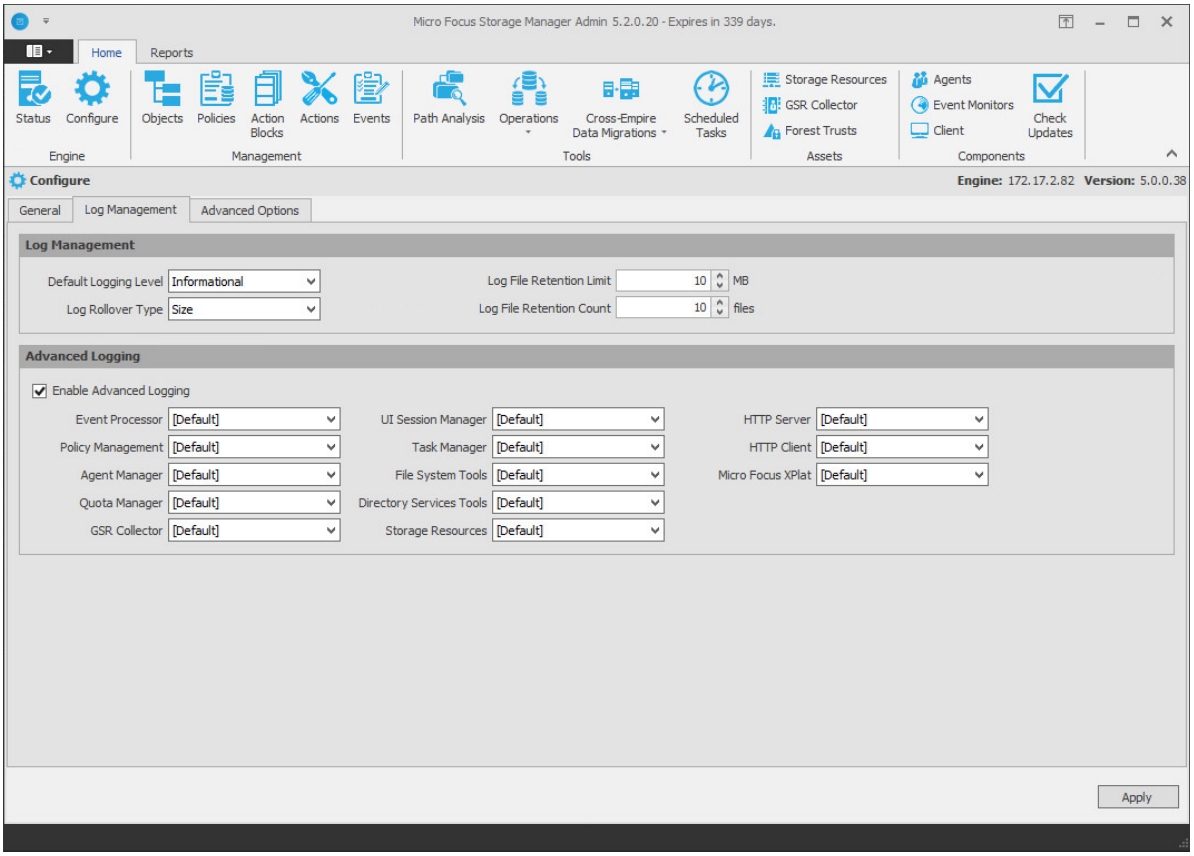
**Copy Template:** Clicking this button recopies files located in `C:ProgramData\Micro Focus\Storage Manager\Engine\data\ProxyHome` to the location specified by the share. If the proxy home is not located on the server hosting the Engine, this makes it so you can recopy the template files without having to do it manually.

## Log Management

The Log Management tab includes settings specific to log files. Log files are accessible only from the server hosting the Engine at `C:\ProgramData\Micro Focus\Storage Manager\Engine\log`.

Each of the fields is described below.

***Figure 13-3** The Log Tab of the Configure Page*



**Engine:** 172.17.2.82 **Version:** 5.0.0.38

**Log Management**

Default Logging Level: Informational
Log Rollover Type: Size
Log File Retention Limit: 10 MB
Log File Retention Count: 10 files

**Advanced Logging**

☑ Enable Advanced Logging

| | | | | | |
|---|---|---|---|---|---|
| Event Processor | [Default] | UI Session Manager | [Default] | HTTP Server | [Default] |
| Policy Management | [Default] | Task Manager | [Default] | HTTP Client | [Default] |
| Agent Manager | [Default] | File System Tools | [Default] | Micro Focus XPlat | [Default] |
| Quota Manager | [Default] | Directory Services Tools | [Default] | | |
| GSR Collector | [Default] | Storage Resources | [Default] | | |

**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.

---

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

---

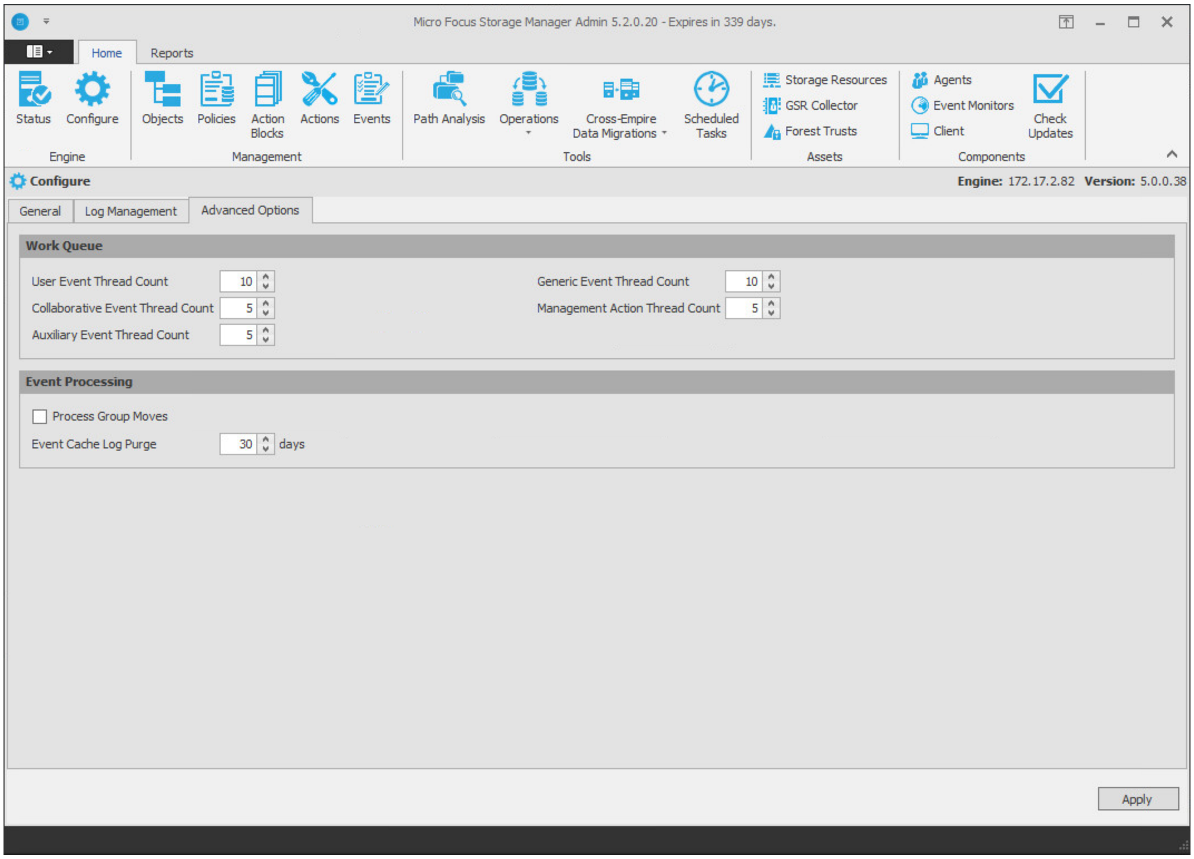
**Log File Retention Count:** By default, Storage Manager retains the 10 most recent log files, according to the **Log Rollover Type** setting. For example, if the **Log Rollover Type** setting is set to Daily, the retained log files are from the last 10 days.

**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 Storage Manager performs.

***Figure 13-4*** *The Advanced Options Tab of the Configure Page*



Engine: 172.17.2.82 Version: 5.0.0.38

**Work Queue**

| | | | |
|---|---|---|---|
| User Event Thread Count | 10 | Generic Event Thread Count | 10 |
| Collaborative Event Thread Count | 5 | Management Action Thread Count | 5 |
| Auxiliary Event Thread Count | 5 | | |

**Event Processing**

☐ Process Group Moves

Event Cache Log Purge 30 days

**Work Queue:** These settings are optimized for a normal Storage Manager workload.

**Process Group Moves:** Click this box to enable Storage Manager to move collaborative storage.

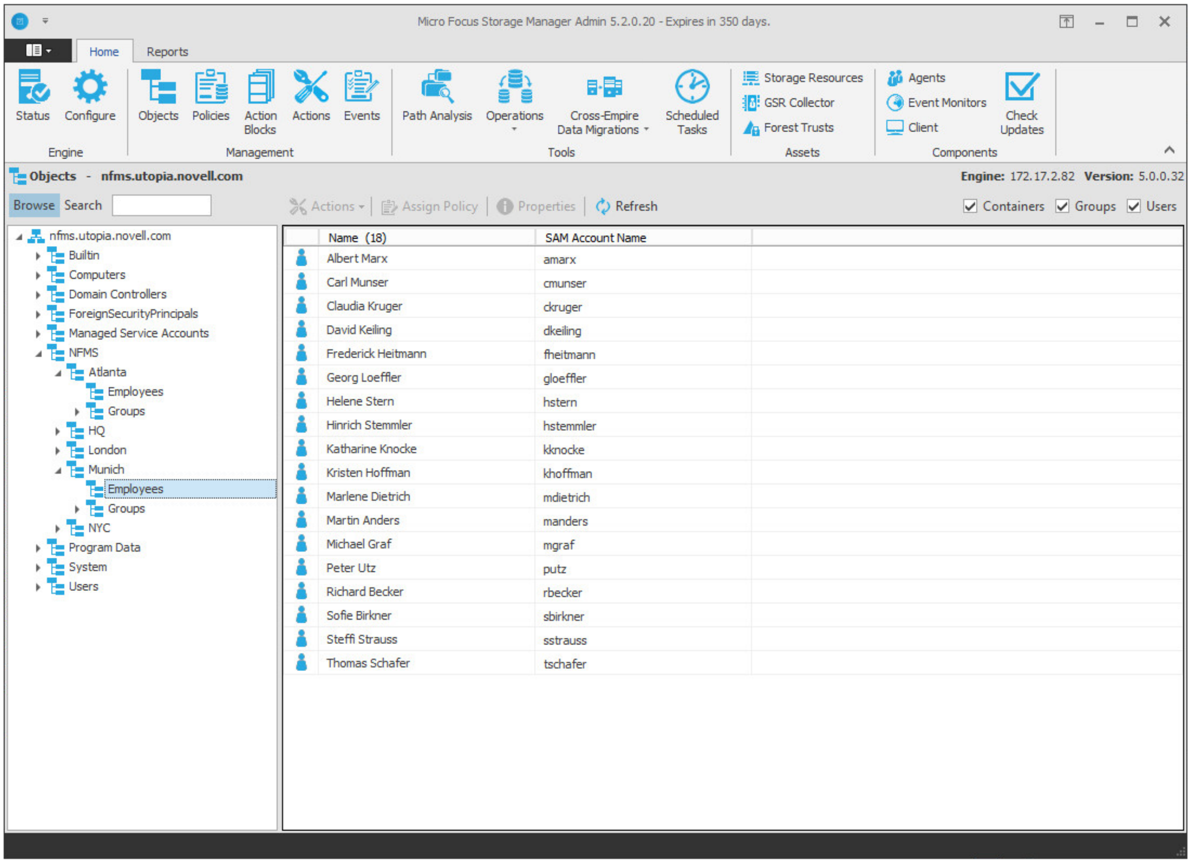
**Event Cache Log Purge:** By default, Storage Manager keeps the most recent 30 days of event entries in cache. You can adjust the setting in the **Days** field.

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

## 13.1.3 Objects

The Objects page lets you manage the associations between Storage Manager 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.

***Figure 13-5** Objects Page*



Objects - nfms.utopia.novell.com

Engine: 172.17.2.82 Version: 5.0.0.32

- nfms.utopia.novell.com
  - Builtin
  - Computers
  - Domain Controllers
  - ForeignSecurityPrincipals
  - Managed Service Accounts
  - NFMS
    - Atlanta
      - Employees
      - Groups
    - HQ
    - London
    - Munich
      - Employees
      - Groups
    - NYC
  - Program Data
  - System
  - Users

| Name (18) | SAM Account Name |
|---|---|
| Albert Marx | amarx |
| Carl Munser | cmunser |
| Claudia Kruger | ckruger |
| David Keiling | dkeiling |
| Frederick Heitmann | fheitmann |
| Georg Loeffler | gloeffler |
| Helene Stern | hstern |
| Hinrich Stemmler | hstemmler |
| Katharine Knocke | kknocke |
| Kristen Hoffman | khoffman |
| Marlene Dietrich | mdietrich |
| Martin Anders | manders |
| Michael Graf | mgraf |
| Peter Utz | putz |
| Richard Becker | rbecker |
| Sofie Birkner | sbirkner |
| Steffi Strauss | sstrauss |
| Thomas Schafer | tschafer |

## 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

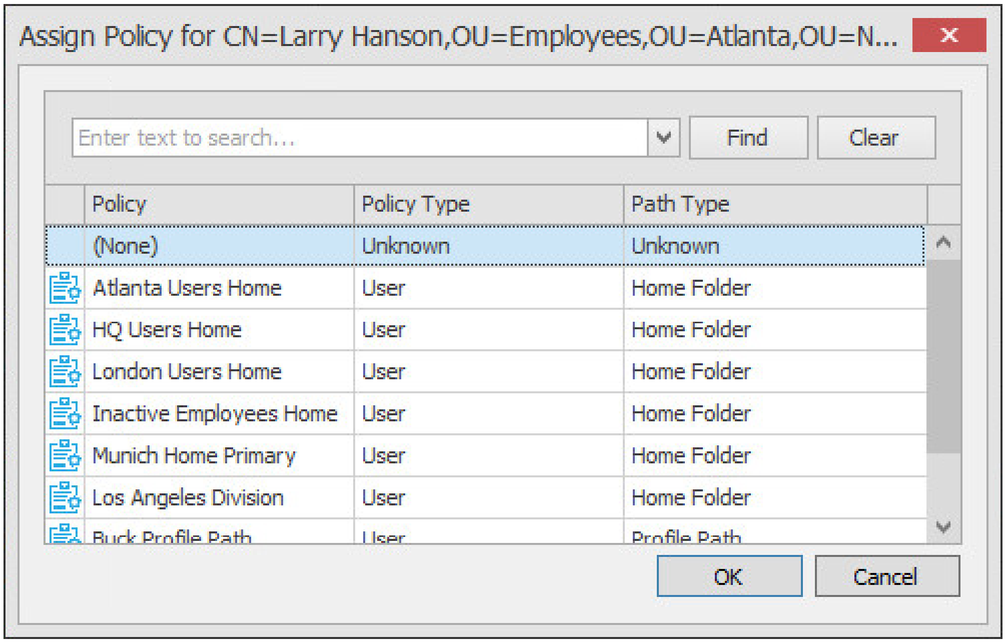
Use the right pane to view the objects within a selected organizational unit as well as view properties, perform Management Actions, and assign policies. The right pane displays containers (organizational units), groups, and users, according to what you have selected in the Filter check boxes.

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

***Figure 13-6*** *Policy Selector Dialog Box*



Assign Policy for CN=Larry Hanson,OU=Employees,OU=Atlanta,OU=N...

| Policy | Policy Type | Path Type |
|---|---|---|
| (None) | Unknown | Unknown |
| Atlanta Users Home | User | Home Folder |
| HQ Users Home | User | Home Folder |
| London Users Home | User | Home Folder |
| Inactive Employees Home | User | Home Folder |
| Munich Home Primary | User | Home Folder |
| Los Angeles Division | User | Home Folder |
| Buck Profile Path | User | Profile Path |

## 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. If you are working with a Micro Focus Support representative to resolve a problem, you might need to provide information from this page.

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

**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 Storage Manager. 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 Section 13.1.13, “GSR Collector,” on page 283.

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.

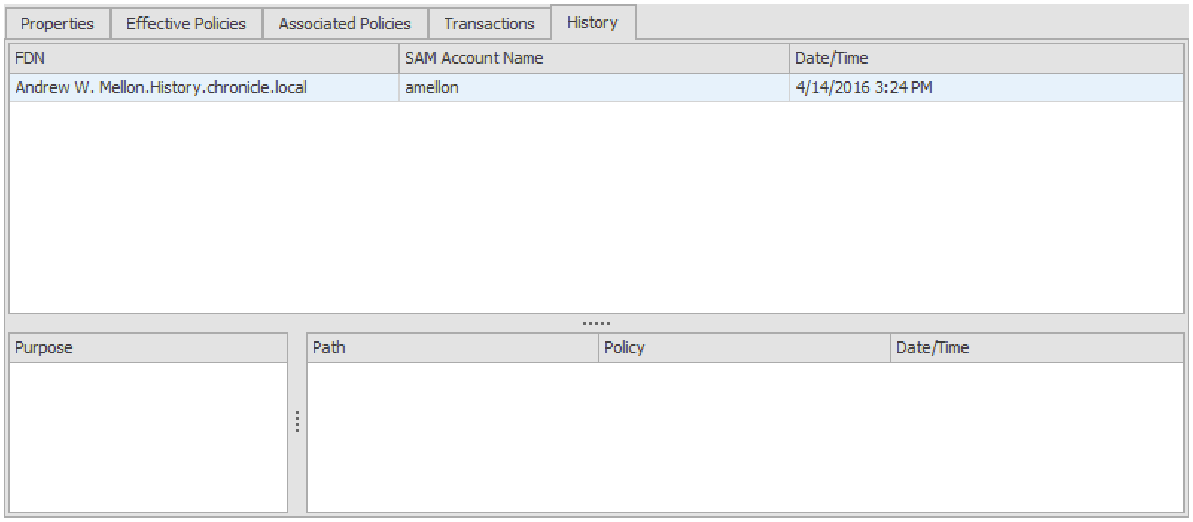
The GSR Collector's historical data can be especially useful when managed paths are moved based on policy.

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.

***Figure 13-7*** *Example of an Unmanaged User without a Cataloged Path*



| FDN | SAM Account Name | Date/Time |
|---|---|---|
| Andrew W. Mellon.History.chronicle.local | amellon | 4/14/2016 3:24 PM |

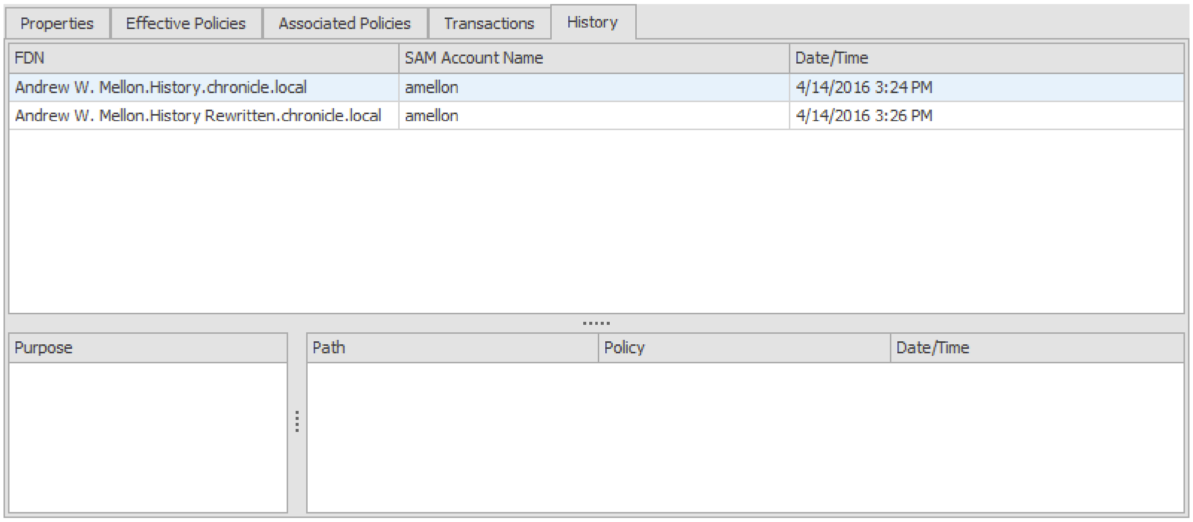
| Purpose |
|---|

| Path | Policy | Date/Time |
|---|---|---|

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.

***Figure 13-8** Example of a Moved Unmanaged User*



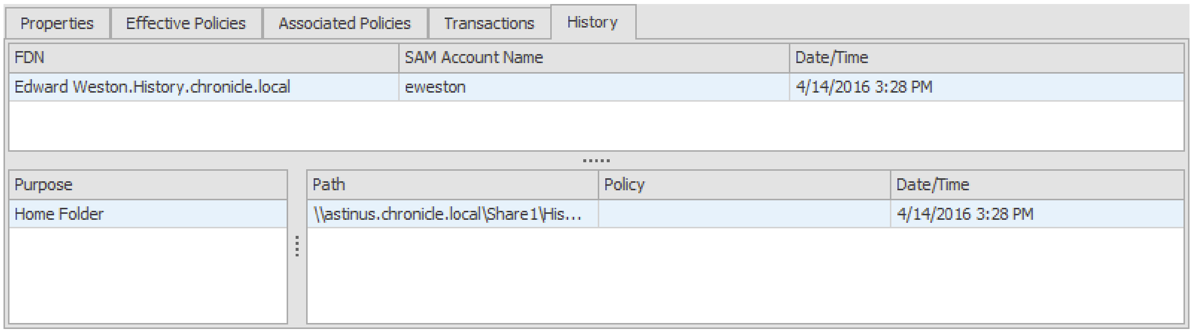
| FDN | SAM Account Name | Date/Time |
|---|---|---|
| Andrew W. Mellon.History.chronicle.local | amellon | 4/14/2016 3:24 PM |
| Andrew W. Mellon.History Rewritten.chronicle.local | amellon | 4/14/2016 3:26 PM |

| Purpose |
|---|

| Path | Policy | Date/Time |
|---|---|---|

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.

***Figure 13-9** Example of an Unmanaged User with a Home Folder*



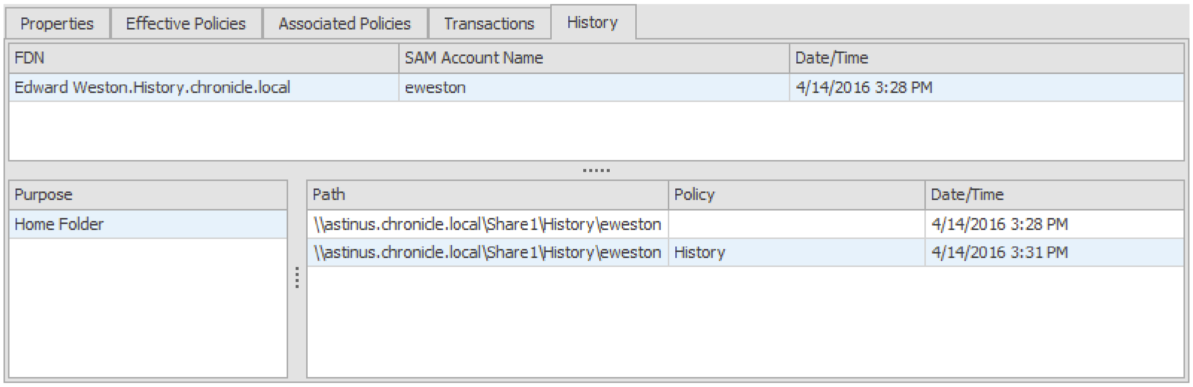
| FDN | SAM Account Name | Date/Time |
|---|---|---|
| Edward Weston.History.chronicle.local | eweston | 4/14/2016 3:28 PM |

| Purpose |
|---|
| Home Folder |

| Path | Policy | Date/Time |
|---|---|---|
| \\astinus.chronicle.local\Share1\His... | | 4/14/2016 3:28 PM |

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.

*Figure 13-10 Example of a Managed User*



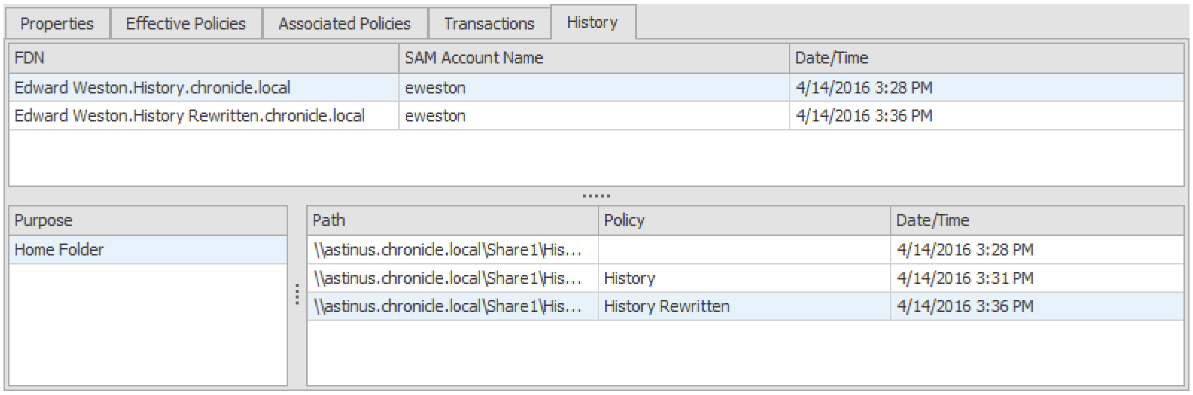
| FDN | SAM Account Name | Date/Time |
|---|---|---|
| Edward Weston.History.chronicle.local | eweston | 4/14/2016 3:28 PM |

| Purpose |
|---|
| Home Folder |

| Path | Policy | Date/Time |
|---|---|---|
| \\astinus.chronicle.local\Share1\History\eweston | | 4/14/2016 3:28 PM |
| \\astinus.chronicle.local\Share1\History\eweston | History | 4/14/2016 3:31 PM |

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.

*Figure 13-11 Example of a Moved Managed User*



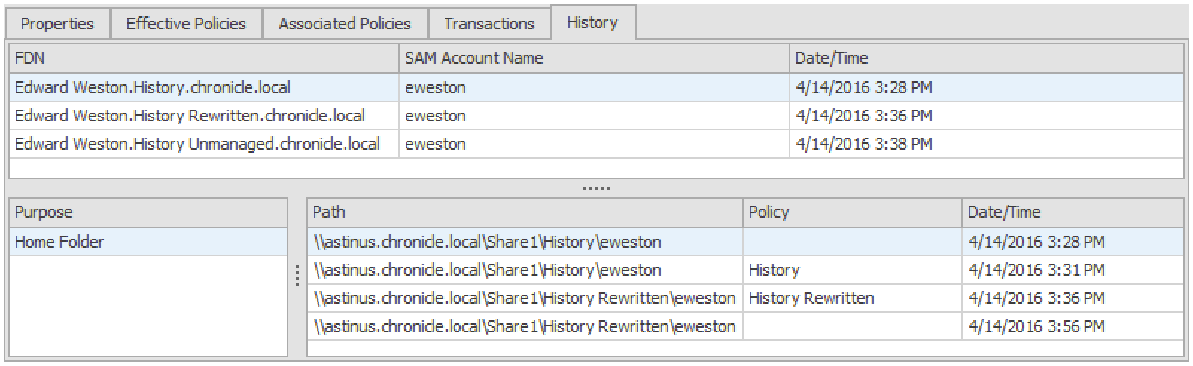
| FDN | SAM Account Name | Date/Time |
|---|---|---|
| Edward Weston.History.chronicle.local | eweston | 4/14/2016 3:28 PM |
| Edward Weston.History Rewritten.chronicle.local | eweston | 4/14/2016 3:36 PM |

| Purpose |
|---|
| Home Folder |

| Path | Policy | Date/Time |
|---|---|---|
| \\astinus.chronicle.local\Share1\His... | | 4/14/2016 3:28 PM |
| \\astinus.chronicle.local\Share1\His... | History | 4/14/2016 3:31 PM |
| \\astinus.chronicle.local\Share1\His... | History Rewritten | 4/14/2016 3:36 PM |

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.

*Figure 13-12 Example of a Moved User to a Container Not Managed by a Policy*



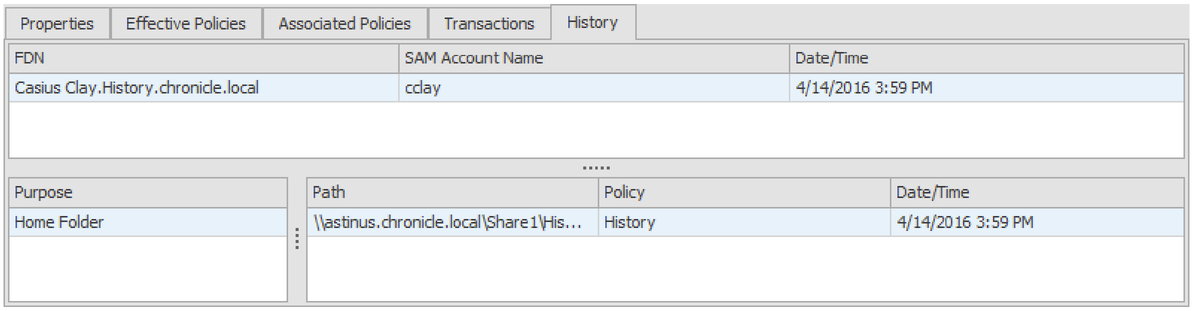
| FDN | SAM Account Name | Date/Time |
|---|---|---|
| Edward Weston.History.chronicle.local | eweston | 4/14/2016 3:28 PM |
| Edward Weston.History Rewritten.chronicle.local | eweston | 4/14/2016 3:36 PM |
| Edward Weston.History Unmanaged.chronicle.local | eweston | 4/14/2016 3:38 PM |

| Purpose |
|---|
| Home Folder |

| Path | Policy | Date/Time |
|---|---|---|
| \\astinus.chronicle.local\Share1\History\eweston | | 4/14/2016 3:28 PM |
| \\astinus.chronicle.local\Share1\History\eweston | History | 4/14/2016 3:31 PM |
| \\astinus.chronicle.local\Share1\History Rewritten\eweston | History Rewritten | 4/14/2016 3:36 PM |
| \\astinus.chronicle.local\Share1\History Rewritten\eweston | | 4/14/2016 3:56 PM |

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.

***Figure 13-13*** *Example of a Managed User Before Being Renamed*



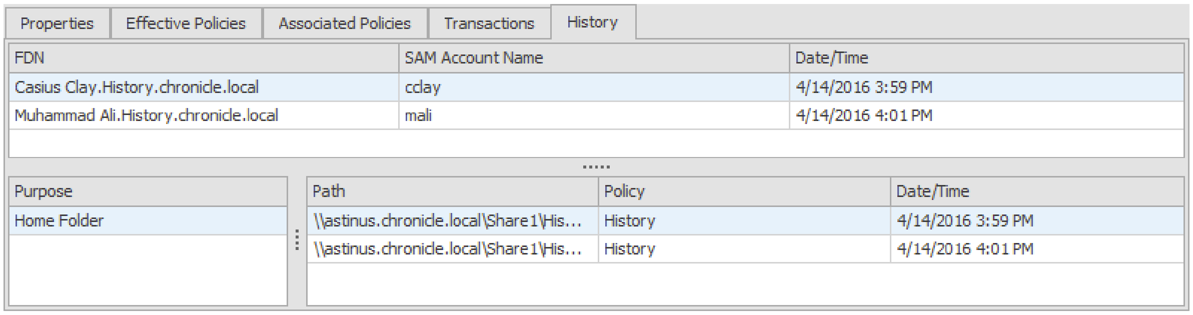
| FDN | SAM Account Name | Date/Time |
|---|---|---|
| Casius Clay.History.chronicle.local | cclay | 4/14/2016 3:59 PM |

| Purpose |
|---|
| Home Folder |

| Path | Policy | Date/Time |
|---|---|---|
| \\astinus.chronicle.local\Share1\His... | History | 4/14/2016 3:59 PM |

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

***Figure 13-14*** *Example of a Managed User After Being Renamed*



| FDN | SAM Account Name | Date/Time |
|---|---|---|
| Casius Clay.History.chronicle.local | cclay | 4/14/2016 3:59 PM |
| Muhammad Ali.History.chronicle.local | mali | 4/14/2016 4:01 PM |

| Purpose |
|---|
| Home Folder |

| Path | Policy | Date/Time |
|---|---|---|
| \\astinus.chronicle.local\Share1\His... | History | 4/14/2016 3:59 PM |
| \\astinus.chronicle.local\Share1\His... | History | 4/14/2016 4:01 PM |

## 13.1.4 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.

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

**Manage:** Lets you create any of the following policies:

- User Home Folder policy
- User Profile Path policy
- User Remote Desktop Services Home Folder policy
- User Remote Desktop Services Profile Path policy
- Group policy
- Container policy
- Auxiliary policy

**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 and 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 Storage Manager 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, seeSection 6.11.4, "Establishing Auxiliary Purpose Mappings," on page 73.

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

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

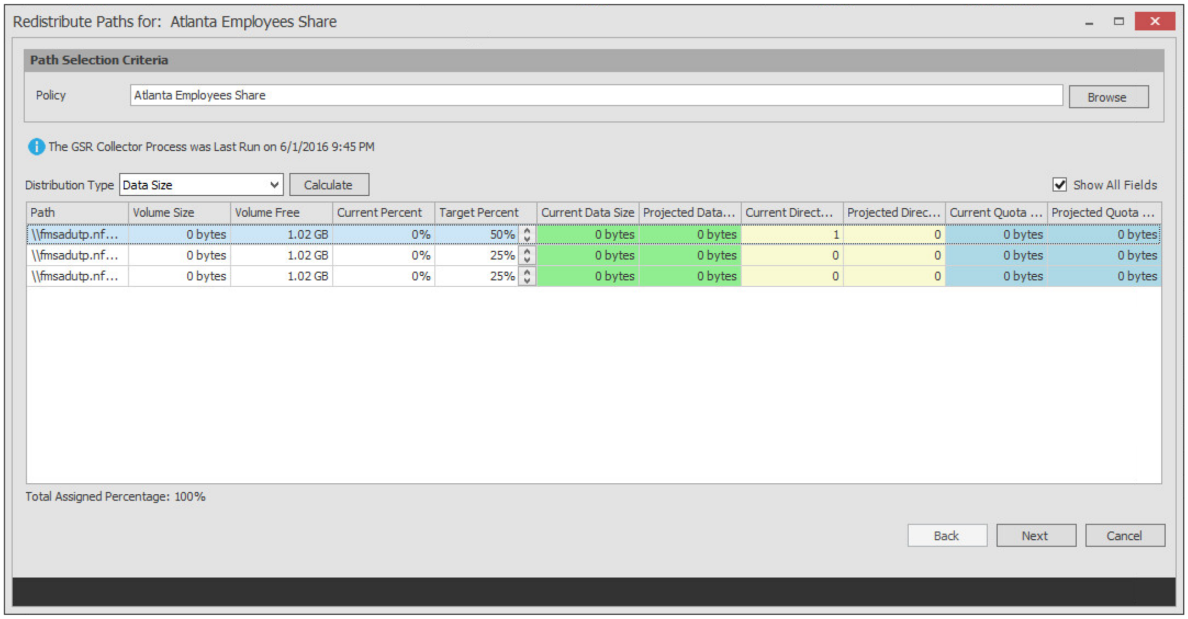
For more information on importing policies, see Section 6.13, "Importing Policies," on page 75.

**Export:** Provides the ability to export policies so that they can be imported later. For example, many customers first evaluate Storage Manager 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 Section 6.12, "Exporting Policies," on page 74.

**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.

***Figure 13-15*** *Redistribute Policy Paths Dialog Box*



Redistribute Paths for: Atlanta Employees Share

Path Selection Criteria

Policy: Atlanta Employees Share

The GSR Collector Process was Last Run on 6/1/2016 9:45 PM

Distribution Type: Data Size

☑ Show All Fields

| Path | Volume Size | Volume Free | Current Percent | Target Percent | Current Data Size | Projected Data... | Current Direct... | Projected Direc... | Current Quota ... | Projected Quota ... |
|---|---|---|---|---|---|---|---|---|---|---|
| \\fmsadutp.nf... | 0 bytes | 1.02 GB | 0% | 50% | 0 bytes | 0 bytes | 1 | 0 | 0 bytes | 0 bytes |
| \\fmsadutp.nf... | 0 bytes | 1.02 GB | 0% | 25% | 0 bytes | 0 bytes | 0 | 0 | 0 bytes | 0 bytes |
| \\fmsadutp.nf... | 0 bytes | 1.02 GB | 0% | 25% | 0 bytes | 0 bytes | 0 | 0 | 0 bytes | 0 bytes |

Total Assigned Percentage: 100%

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

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

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

Click **Next** to view the current locations of the home folders and collaborative storage folders, and the location where Storage Manager 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.

**NOTE:** 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:** SMAdmin shows only the policy types that are checked.

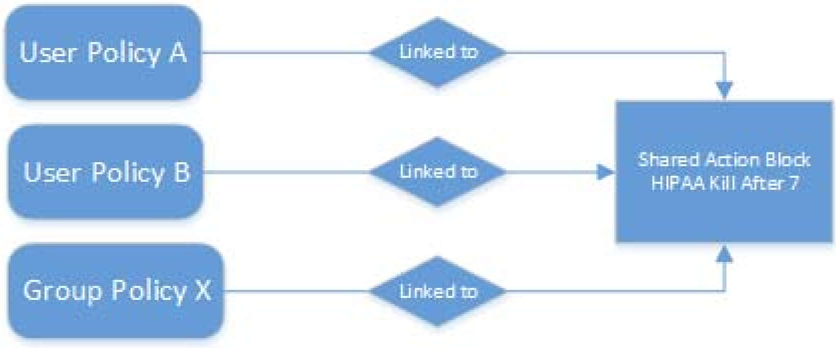
## 13.1.5 Action Blocks

This page lets you create Action Blocks that can be linked to a policy or that can be associated with a Groom operation not associated with a policy.

### 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.

***Figure 13-16*** *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.

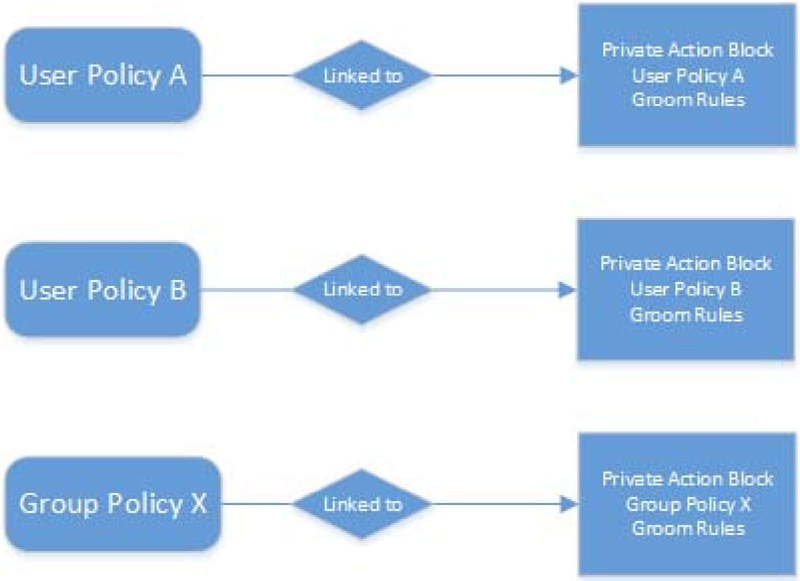
An Action Block can have a many-to-one relationship. This means that any number of policies can share any particular Action Block for a given policy option. Action Block inheritance cannot be chained. That is to say, “Policy A” cannot inherit the Filter rules from “Groom Block A” and “Groom Block B”. “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.

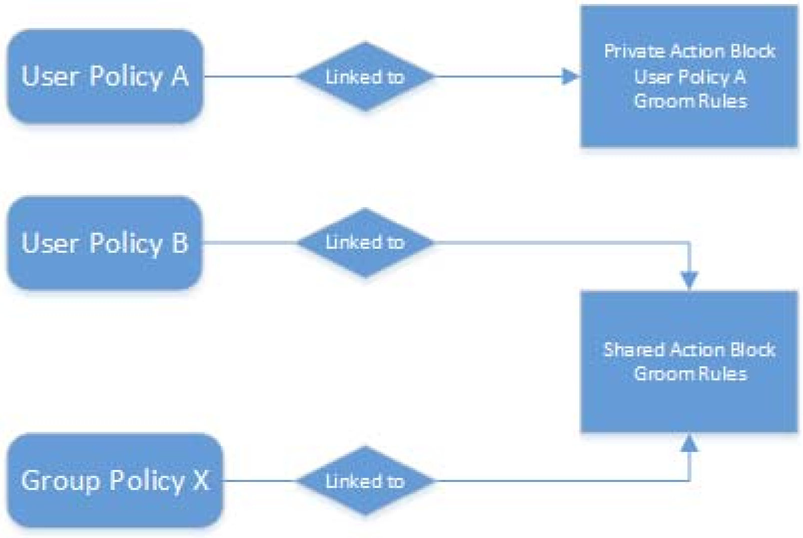
A Private Action Block represents a set of policy options that aren’t shared, yet have been migrated to the Action Block architecture. Private Action Blocks are also created and associated to a policy when the policy is upgraded as new Action Block types are supported. Below is an example of the relationships 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.

***Figure 13-17*** *Relationships Between Policies and their Private Action Blocks for Filters*


User Policy A
Linked to
Private Action Block User Policy A Groom Rules
User Policy B
Linked to
Private Action Block User Policy B Groom Rules
Group Policy X
Linked to
Private Action Block Group Policy X Groom Rules

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.

***Figure 13-18*** *Shared and Private Action Block Associations*

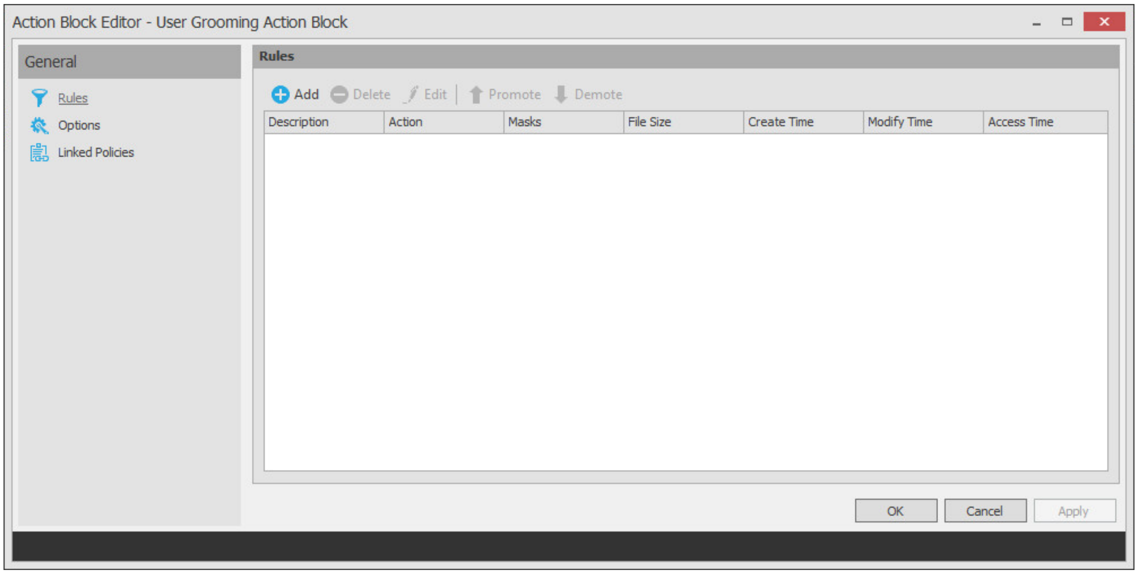


By default, a Private Action Block is not viewable in the list of Shared Action Blocks.

## Creating a Filter Action Block

1. In SMAdmin, click the **Home** 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 Storage Manager 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 Section 6.5.8, "Setting Vault Rules," on page 58.
7. Click **OK** to close the Action Block Editor dialog box.

### Linking Filter Action Blocks

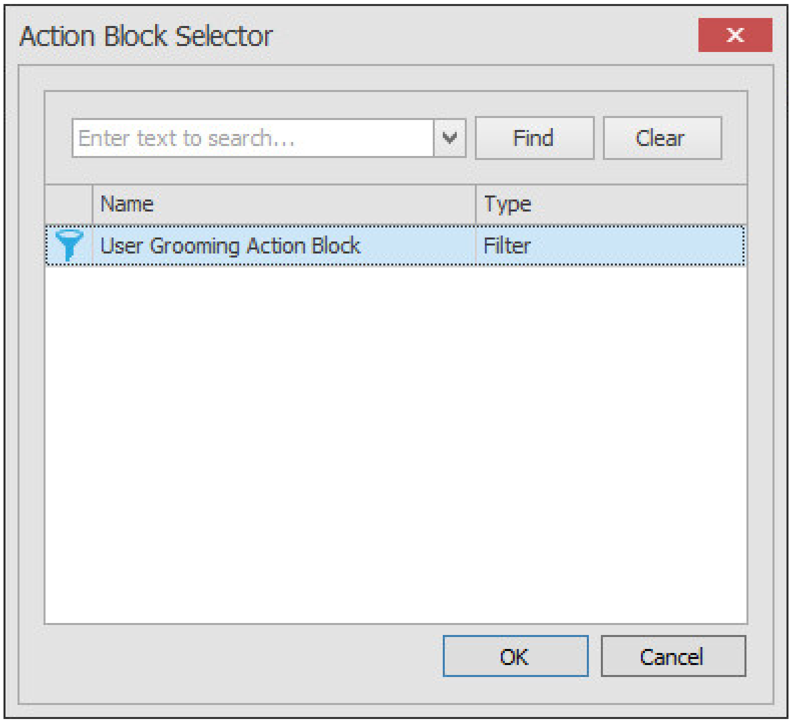
Filter Action Blocks can be linked to the following:

- Policy-based Vault
- Policy-based Groom
- Groom Operations

### 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 SMAdmin, click the **Home** 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.



| Name | Type |
|---|---|
| User Grooming Action Block | Filter |

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.

### Linking a Filter Action Block to a Groom Operation

Non-policy based Groom Operations require a linked Filter Action Block. For procedures on linking a Filter Action Block with a Groom Operation, see “Performing a Groom Operation” on page 278.

## 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 Appendix F, “Managed Path Naming Attribute Specifications,” on page 357.

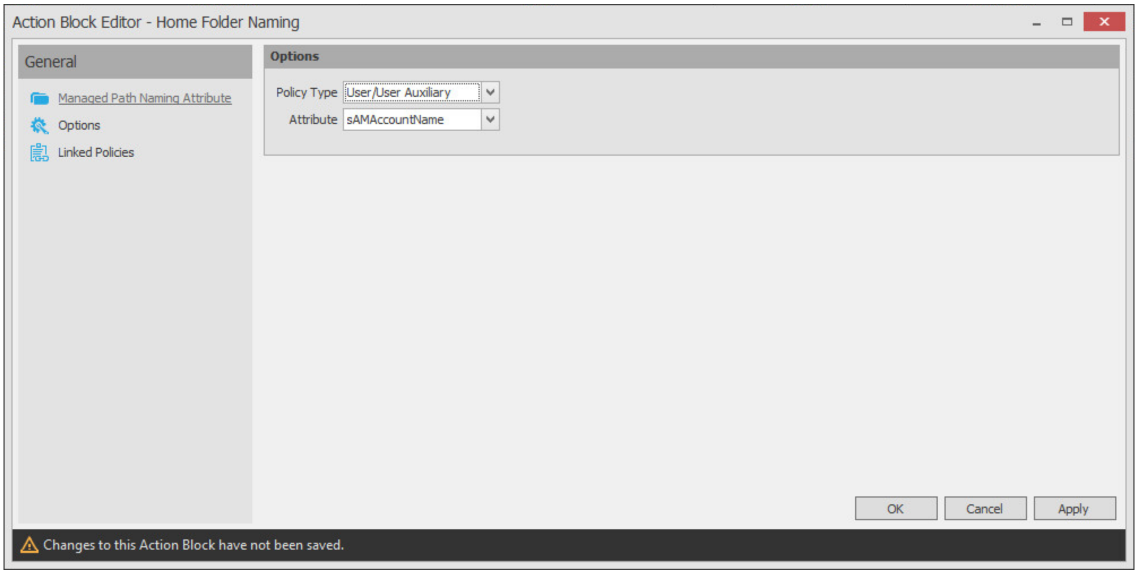
1 In SMAdmin, click the **Home** tab.

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:


Action Block Editor - Home Folder Naming
General
Managed Path Naming Attribute
Options
Linked Policies
Options
OK
Cancel
Apply

Policy Type: User/User Auxiliary

Attribute: sAMAccountName

Changes to this Action Block have not been saved.

**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 of group object.

With the introduction of Storage Manager for Active Directory 5.1, 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 Storage Manager will automatically provision the home folder based on this attribute setting.

For more information, see Section 6.5.4, “Setting Target Paths,” on page 54.

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.

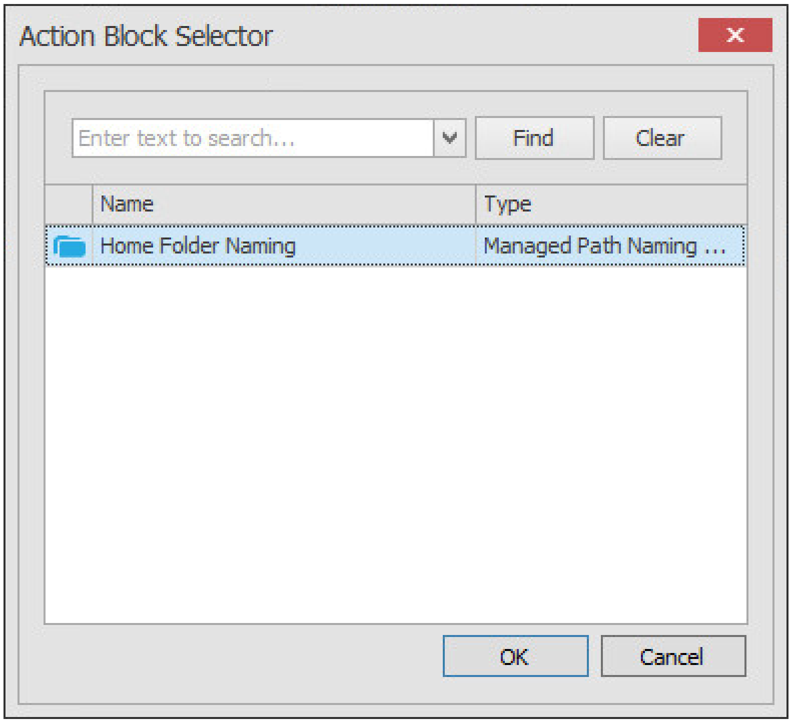
1 In SMAdmin, click the **Home** tab.

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**.



| Name | Type |
|---|---|
| Home Folder Naming | Managed Path Naming ... |

6 Select the Action Block you want to link.

7 Click **OK**.

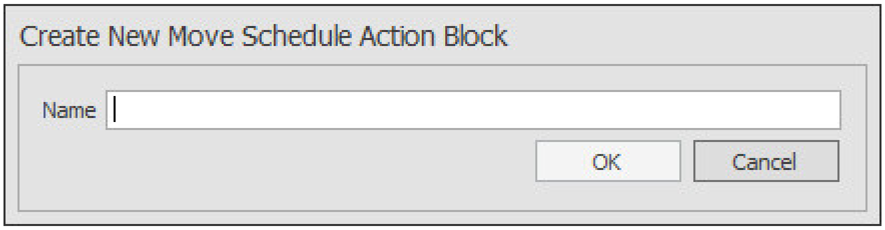
## Creating a Move Schedule Action Block

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

1 In SMAdmin, click the **Home** tab.

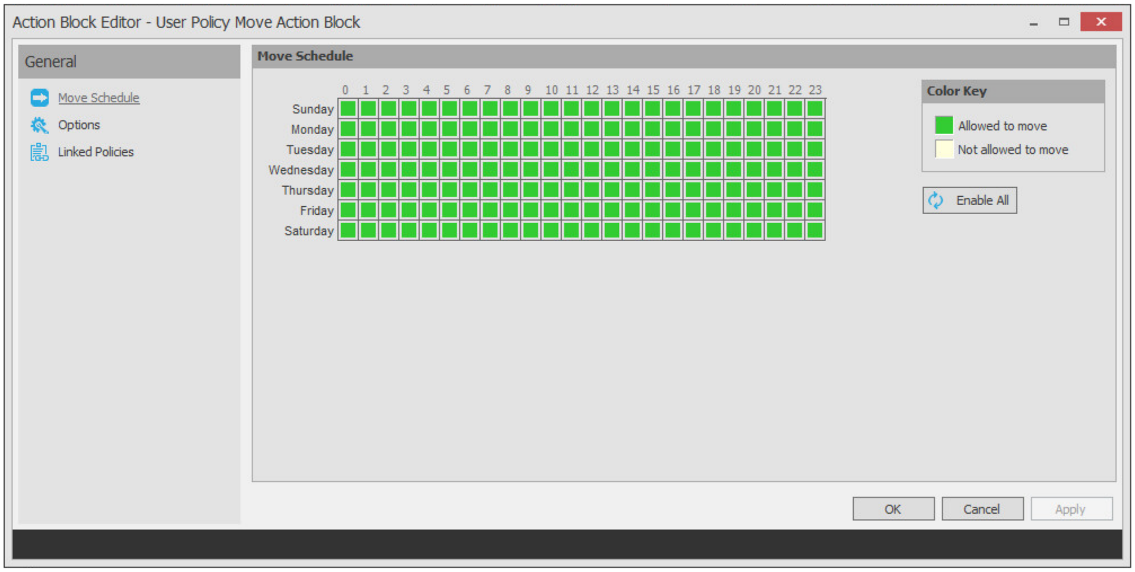
2 Click **Action Blocks**.

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:



| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Sunday | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Monday | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Tuesday | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Wednesday | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Thursday | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Friday | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Saturday | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |

🟩 Allowed to move
□ Not allowed to move

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

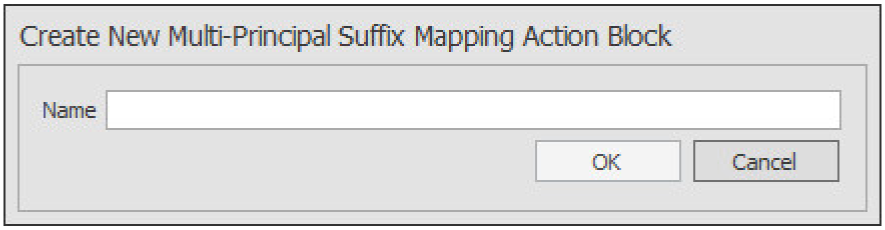
These procedures specify how to link a Move Schedule Action Block to an existing policy. You can also link a Move Schedule Action Block to a new policy as you create one.

1. In SMAdmin, click the **Home** 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 **OK**.

## Creating a Multi-Principal Suffix Mapping Action Block

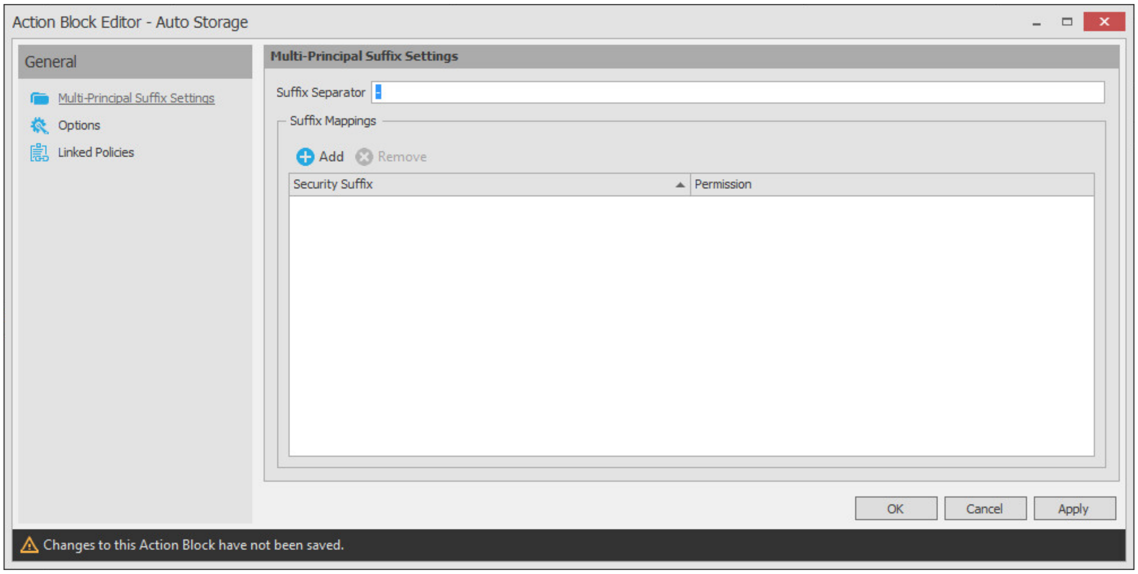
Use Multi-Principal Suffix Mapping Action Blocks to standardize the groups and their associated permissions for the collaborative storage folders that are provisioned by Storage Manager.

1. In SMAdmin, click the **Home** 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:



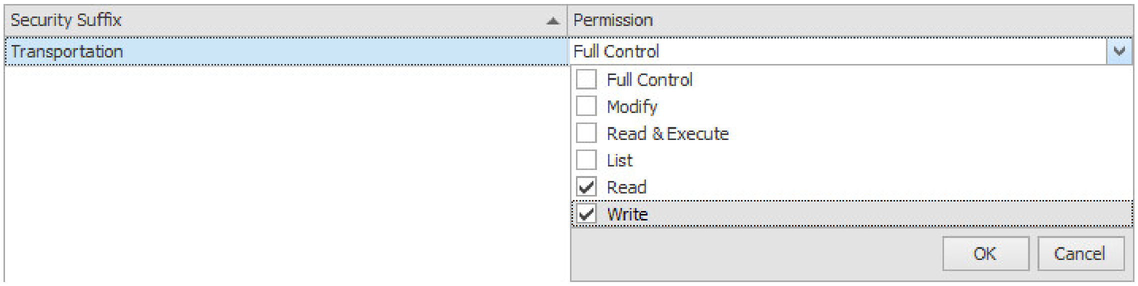
⚠ Changes to this Action Block have not been saved.

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.

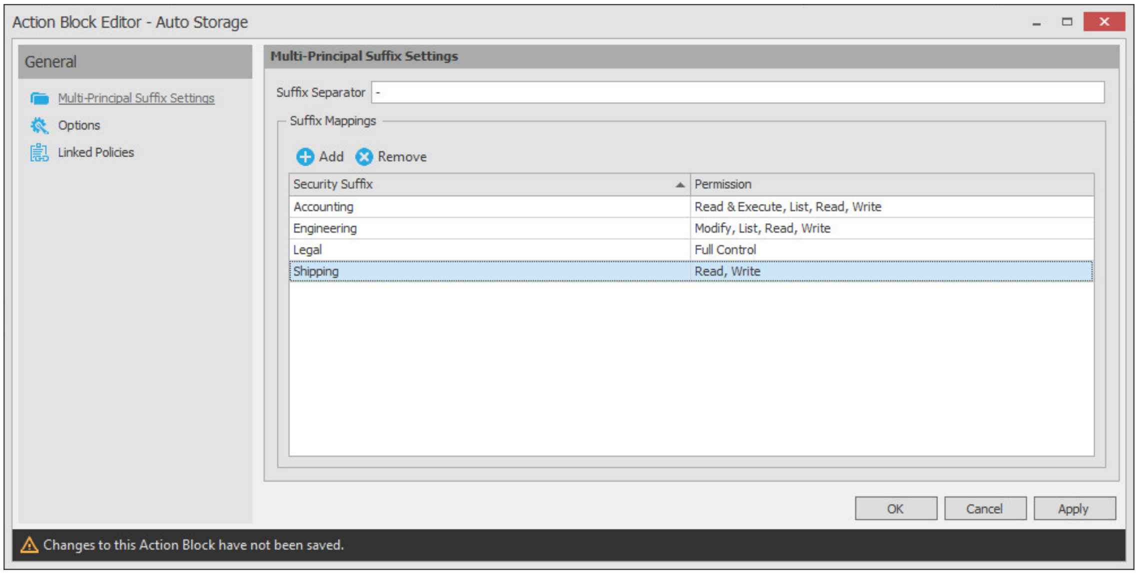
8 Specify the permissions for the particular group and click **OK**.



| Security Suffix | Permission |
|---|---|
| Transportation | Full Control |

□ Full Control
□ Modify
□ Read & Execute
□ List
☑ Read
☑ Write

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


Action Block Editor - Auto Storage
General
Multi-Principal Suffix Settings
Options
Linked Policies
Multi-Principal Suffix Settings
Suffix Mappings
Add
Remove
OK
Cancel
Apply

Suffix Separator: -

| Security Suffix | Permission |
|---|---|
| Accounting | Read & Execute, List, Read, Write |
| Engineering | Modify, List, Read, Write |
| Legal | Full Control |
| Shipping | Read, Write |

Changes to this Action Block have not been saved.

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 SMAdmin, click the **Home** 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 **OK**.

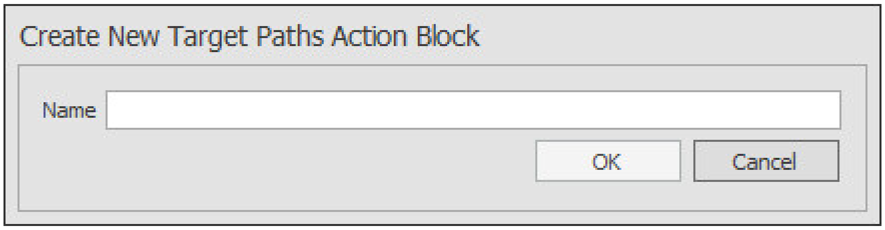
## Creating a Target Paths Action Block

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 SMAdmin, click the **Home** tab.

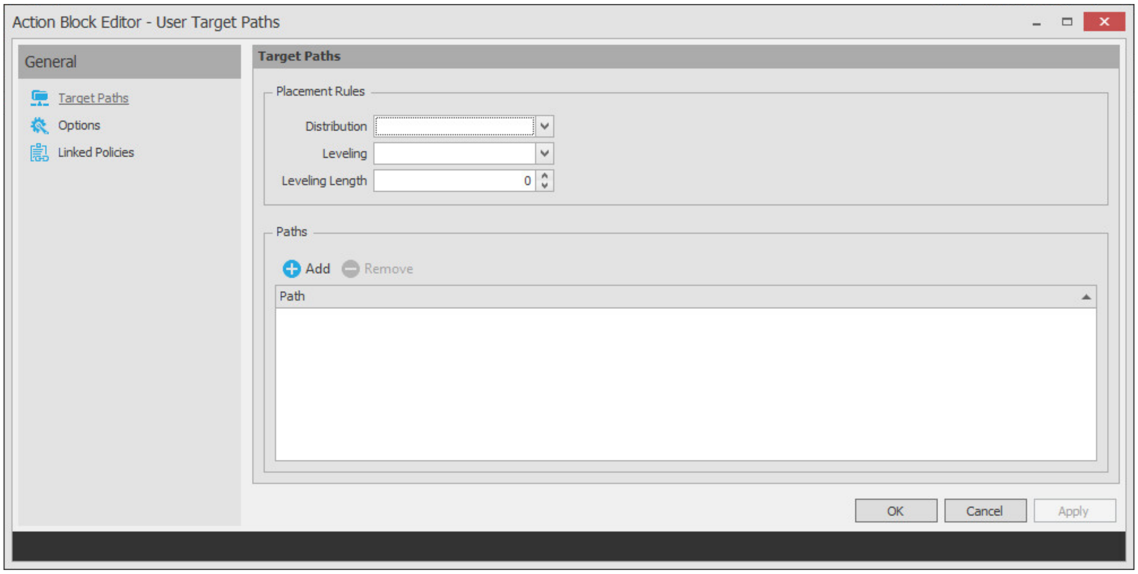
2 Click **Action Blocks**.

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 Section 6.5.4, "Setting Target Paths," on page 54.

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 SMAdmin, click the **Home** 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 **OK**.

## 13.1.6 Actions

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

In Storage Manager, 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.

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

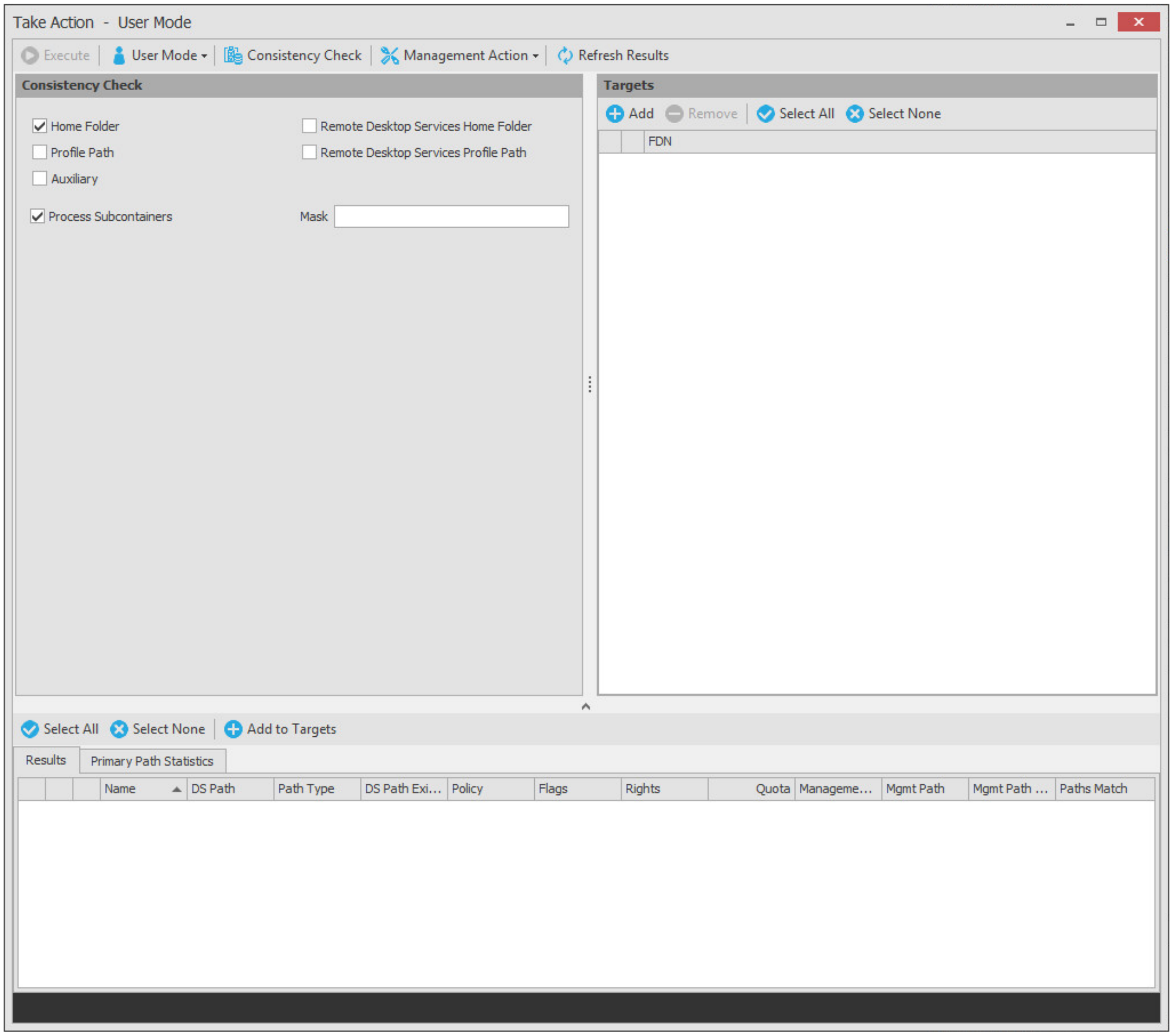
Storage Manager analyzes each User object independently, regardless of whether the Management Action is initiated via organizational unit, Group objects, or User objects.

- "Management Actions Dialog Box" on page 268
- "Available Management Actions" on page 270

### Management Actions Dialog Box

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

*Figure 13-19 Management Action Dialog Box*



☑ Home Folder
□ Profile Path
□ Auxiliary
☑ Process Subcontainers
□ Remote Desktop Services Home Folder
□ Remote Desktop Services Profile Path

**Execute:** Clicking this button executes the management 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 Storage Manager. These potential problems might be missing storage quotas, inconsistent directory attributes, missing and inconsistent managed paths, and more.

In addition to reporting on storage issues, consistency check reports let you review current quota assignments and can help you with the design and planning of storage policies. In Section 5.3, “Running Consistency Check Reports on Existing Storage,” on page 35, 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, Storage Manager 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 Storage Manager 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

- “Manage” on page 270
- “Enforce Policy Path” on page 271
- “Groom” on page 271
- “Apply Attributes” on page 271
- “Apply Home Drive” on page 271
- “Apply Members” on page 271
- “Apply Owner” on page 271
- “Apply Quota” on page 273
- “Apply Permissions” on page 273
- “Apply Template” on page 273
- “Clear Managed Path Attribute” on page 273
- “Recover Managed Path Attribute” on page 274
- “Assign Managed Path” on page 274
- “Directory Merge” on page 274
- “Remove from Engine Database” on page 274

### Manage

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

If the existing objects already have established managed paths, attributes, and rights, Storage Manager 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.

## Groom

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

## Apply Attributes

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

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

## Apply Home Drive

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

If you have a Storage Manager 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.

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

## Apply Members

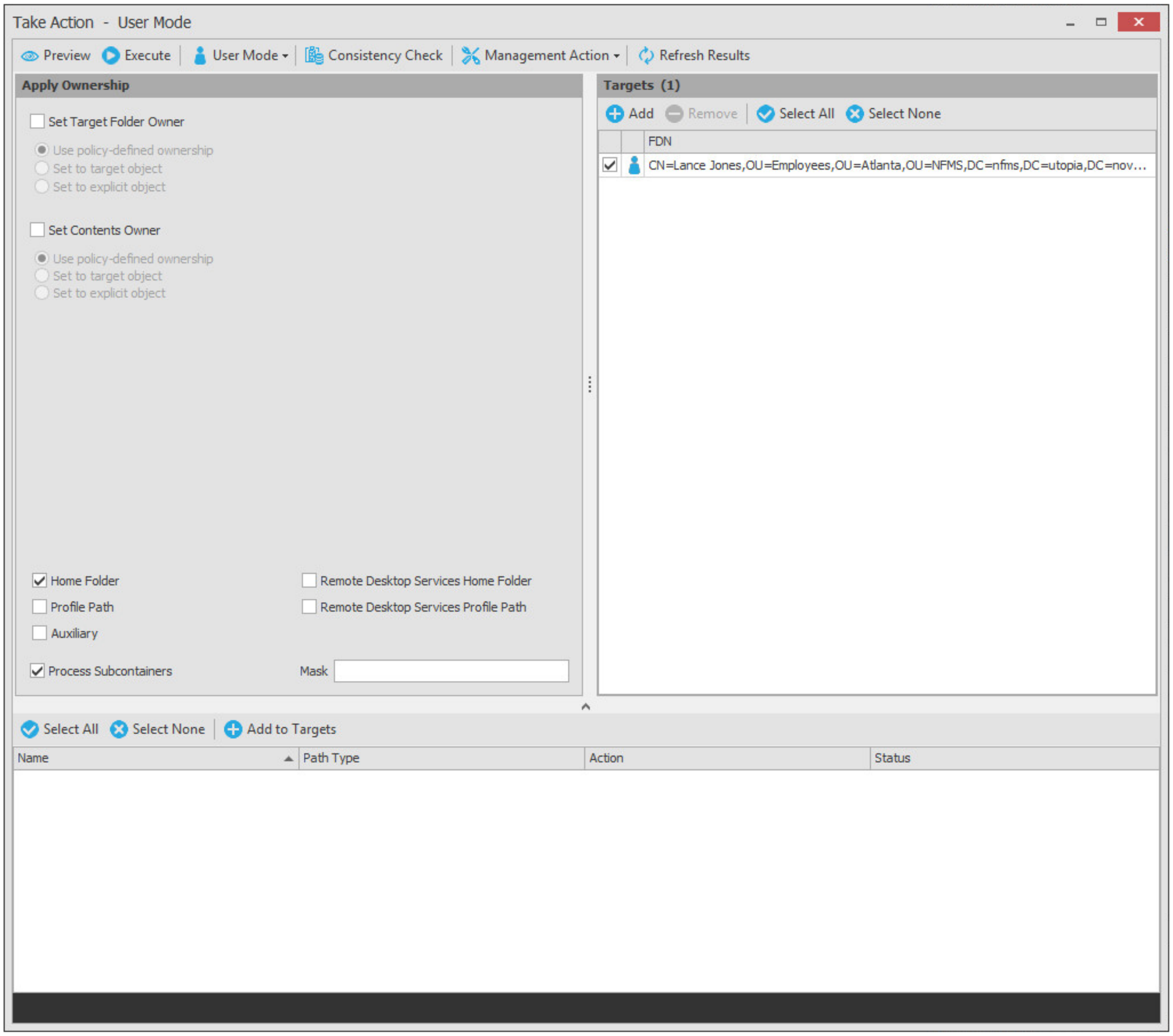
This Management Action is included to create the owner folder and personal folders in a collaborative storage area, where these folders did not exist previously. You must first modify the collaborative storage template in the policy to include -OWNER- and -MEMBER-. For more information, see Chapter 8, "Managing Collaborative Storage," on page 87.

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.

*Figure 13-20 Apply Ownership Management Action Page*



Apply Ownership

□ Set Target Folder Owner

● Use policy-defined ownership
○ Set to target object
○ Set to explicit object

□ Set Contents Owner

● Use policy-defined ownership
○ Set to target object
○ Set to explicit object

☑ Home Folder
□ Profile Path
□ Auxiliary
□ Remote Desktop Services Home Folder
□ Remote Desktop Services Profile Path

☑ Process Subcontainers

Mask

Targets (1)

| | FDN |
|---|---|
| ☑ | CN=Lance Jones,OU=Employees,OU=Atlanta,OU=NFMS,DC=nfms,DC=utopia,DC=nov… |

| Name | Path Type | Action | Status |
|---|---|---|---|

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

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

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

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

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

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

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

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

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

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 Storage Manager 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 above). If you want to modify the original file structure for the home folder, you can do so through the settings in the in the left pane of the Apply Template dialog box.

## Clear Managed Path Attribute

This Management Action 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 Storage Manager 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 Storage Manager database and makes the object unmanaged.

## 13.1.7 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.

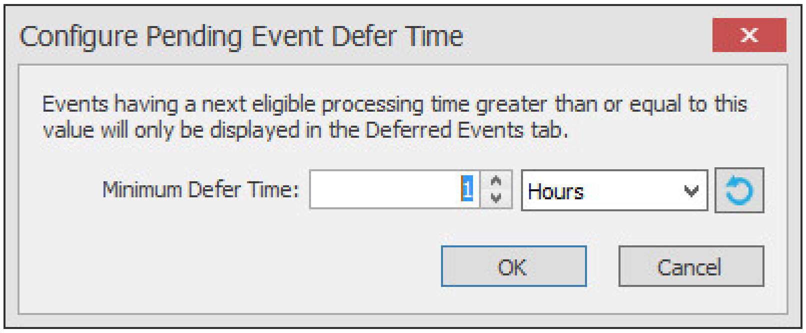
**Make Eligible:** If an event is deferred, you can click this option to make the event eligible immediately.

**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.

*Figure 13-21 Configure Pending Event Defer Time Dialog Box*



Configure Pending Event Defer Time

Events having a next eligible processing time greater than or equal to this value will only be displayed in the Deferred Events tab.

Minimum Defer Time: 1 Hours

**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.

---

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

---

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

## 13.1.8 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.

---

**NOTE:** Whether managed by Storage Manager 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.

## 13.1.9 Operations

The Operations page provides you the ability to perform operations outside of policy-based managed storage. The available Operation types are:

- **Copy:** A copy operation can be used to copy the data of any arbitrary path to another.
- **Groom:** A groom operation can be used to vault data from any arbitrary path to a vault location.

Operations can be run once, scheduled to run once in the future, or can be run on a regular occurrence. Each operation has a specific event and their status can be monitored via Events. Multiple operations can be created and run in parallel. Likewise, any number of scheduled operations can be created and run in parallel.

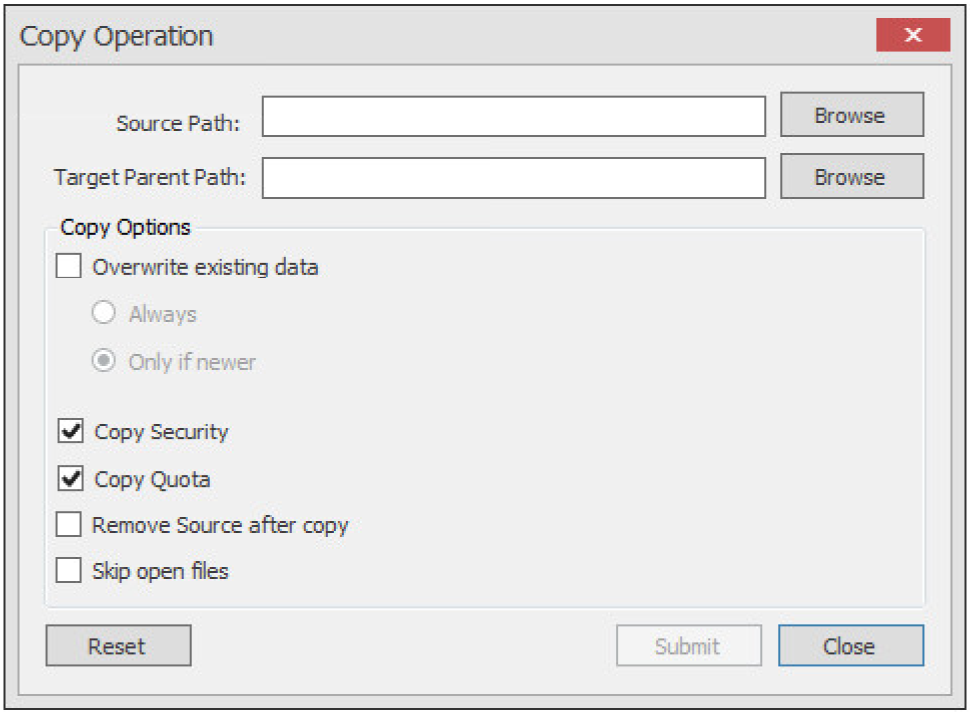
Unless an operation is scheduled, the copy or groom operation takes place immediately. To check on its status, click Events.

### Performing a Copy Operation

Copy operations copy folders and their contents to a target parent folder. If the parent folder does not have a subfolder with the name of the folder being copied, it will create a new subfolder with that name. If it already has a subfolder with the same name, it will merge the contents of the folder into the existing subfolder with the same name and then, based on your overwrite settings, either overwrite the same named files or not copy the same named files.

**NOTE:** In previous versions of Storage Manager, this operation was called a “Data Management” operation. If you have previously scheduled Data Management tasks, they will still continue to work. They have just been renamed to Copy Operation.

1. In SMAdmin, click the Home tab.
2. Click Operations > Copy.



Source Path:

Target Parent Path:

Copy Options

☐ Overwrite existing data

○ Always

● Only if newer

☑ Copy Security

☑ Copy Quota

☐ Remove Source after copy

☐ Skip open files

3 Click the **Browse** button to select a folder for the **Source Path** field.

4 Click the **Browse** button to select a folder for the **Target Parent Path** field.

This is the parent folder where the copied folder will be structured as a subfolder.

5 (Conditional) If you want to overwrite the existing data in the target folder, select the **Overwrite existing data** check box, and then specify either the **Always** or **Only if newer** option.

- **Always:** Duplicate named files on the target will always be overwritten by the source file.
- **Only if newer:** Duplicate named files on the target will only be overwritten if the modification timestamp on the source is newer than the timestamp of the file on the target.

If no option is selected, all duplicate named files will not be copied.

6 Select from the following options:

- **Copy Security:** Maintains the file permissions from the source location to the destination location.
- **Copy Quota:** If the target supports quota management, maintains the disk quota settings from the source location to the destination location.
- **Remove Source after copy:** Removes the folder from its original location in the file system after it has been copied.
- **Skip open files:** Skips all of the files that are opened from the source folder.

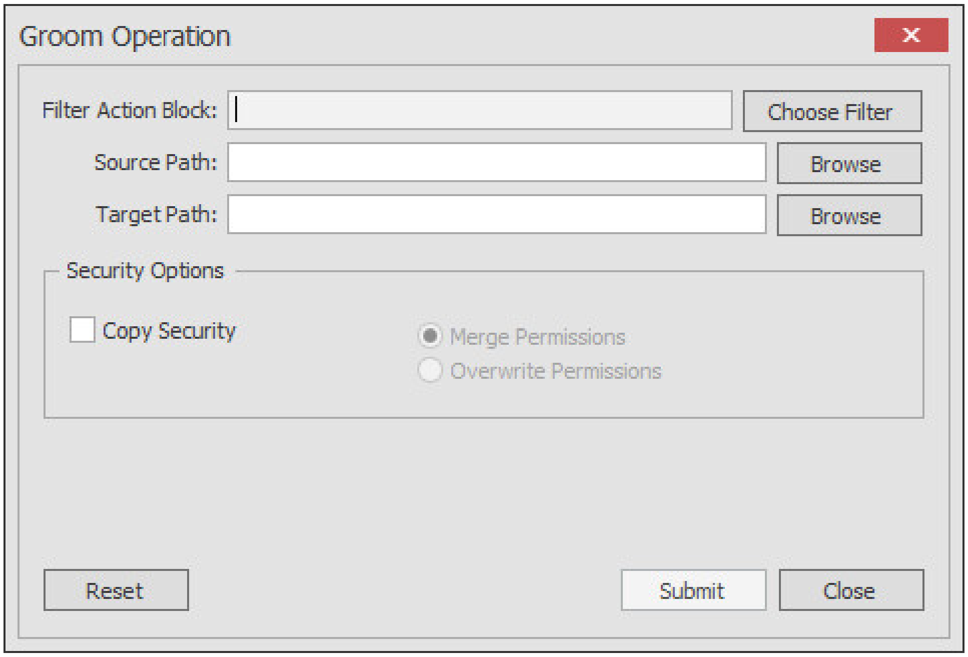
  With copy operations, Storage Manager does not attempt to copy skipped files later. You might want to therefore schedule a copy operation during a time when users are logged out. For procedures on scheduling a copy operation, see Section 13.1.11, “Scheduled Tasks,” on page 279.

## Performing a Groom Operation

Groom operations remove files from any arbitrary path to a vault location. The files that are groomed are in accordance to the specifications that you establish in an Action Block. For more information on Action Blocks, see Section 13.1.5, “Action Blocks,” on page 257.

1 In SMAdmin, click the **Home** tab.

2 Click **Operations** > **Groom**.



□ Copy Security

● Merge Permissions

○ Overwrite Permissions

3 Click **Choose Filter**, select an Action Block, and click **OK**.

4 Click the **Browse** button to select a folder for the **Source Path** field.

5 Click the **Browse** button to select the vault location for the **Target Path** field.

6 (Conditional) If you want you 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.

7 Click **Submit**.

## Scheduling Operations

Operations are scheduled through the Scheduled Tasks page. For information on scheduling copy and groom operations see Section 13.1.11, “Scheduled Tasks,” on page 279.

## 13.1.10 Cross-Empire Data Migrations

For customers who have purchased either the eDirectory to Active Directory Cross-Empire Data Migration Solution Pack, or the Active Directory to Active Directory Cross-Empire Data Migration Solution Pack, this page is the means of launching either Cross-Empire Data Migration project.

- For information and procedures on performing an eDirectory to Active Directory Cross-Empire Data Migration, see Chapter 10, “Performing an eDirectory to Active Directory Cross-Empire Data Migration,” on page 125.
- For information and procedures on performing an Active Directory to Active Directory Cross-Empire Data Migration, see Chapter 11, “Performing an Active Directory to Active Directory Cross-Empire Data Migration,” on page 207.

## 13.1.11 Scheduled Tasks

Use the Scheduled Tasks page to schedule storage resources discoveries and database cleanup tasks as well as schedule copy and groom operations.

### 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 SMAdmin, click the **Home** 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 SMAdmin, click the **Home** tab.
2. Click **Scheduled Tasks**.
3. From the list of scheduled tasks, right-click S**torage 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 Storage Manager 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 SMAdmin, click the **Home** 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**.

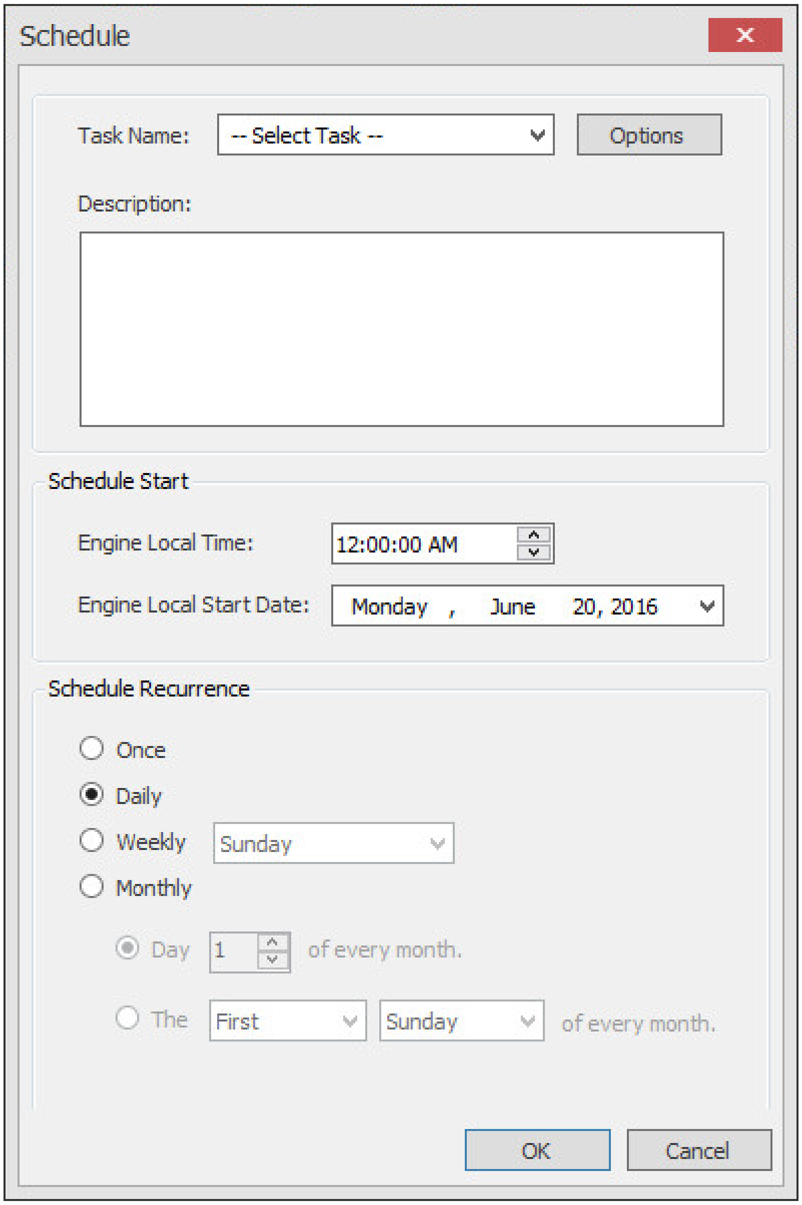
## Run a Database Cleanup

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

1. In SMAdmin, click the **Home** tab.
2. Click **Scheduled Tasks**.
3. From the list of scheduled tasks, right-click D**atabase Cleanup** and select **Run**.
4. Click **Yes** in the confirmation dialog box.

## Schedule an Operation

1. In SMAdmin, click the **Home** tab.
2. Click **Scheduled Tasks**.
3. Click **Add**.



Schedule

Task Name: -- Select Task --

Description:

Schedule Start

Engine Local Time: 12:00:00 AM

Engine Local Start Date: Monday , June 20, 2016

Schedule Recurrence

○ Once

● Daily

○ Weekly Sunday

○ Monthly

● Day 1 of every month.

○ The First Sunday of every month.

4 From the **Task Name** drop-down menu, select an operation.

5 Click **Options** to access the task-specific dialog box.

6 Enter the settings in the dialog box and click **Save** or **OK**.

7 In the **Description** field, enter a description of the operation.

8 In the **Schedule Start** region, set the time and data parameters when you want the operation to take place.

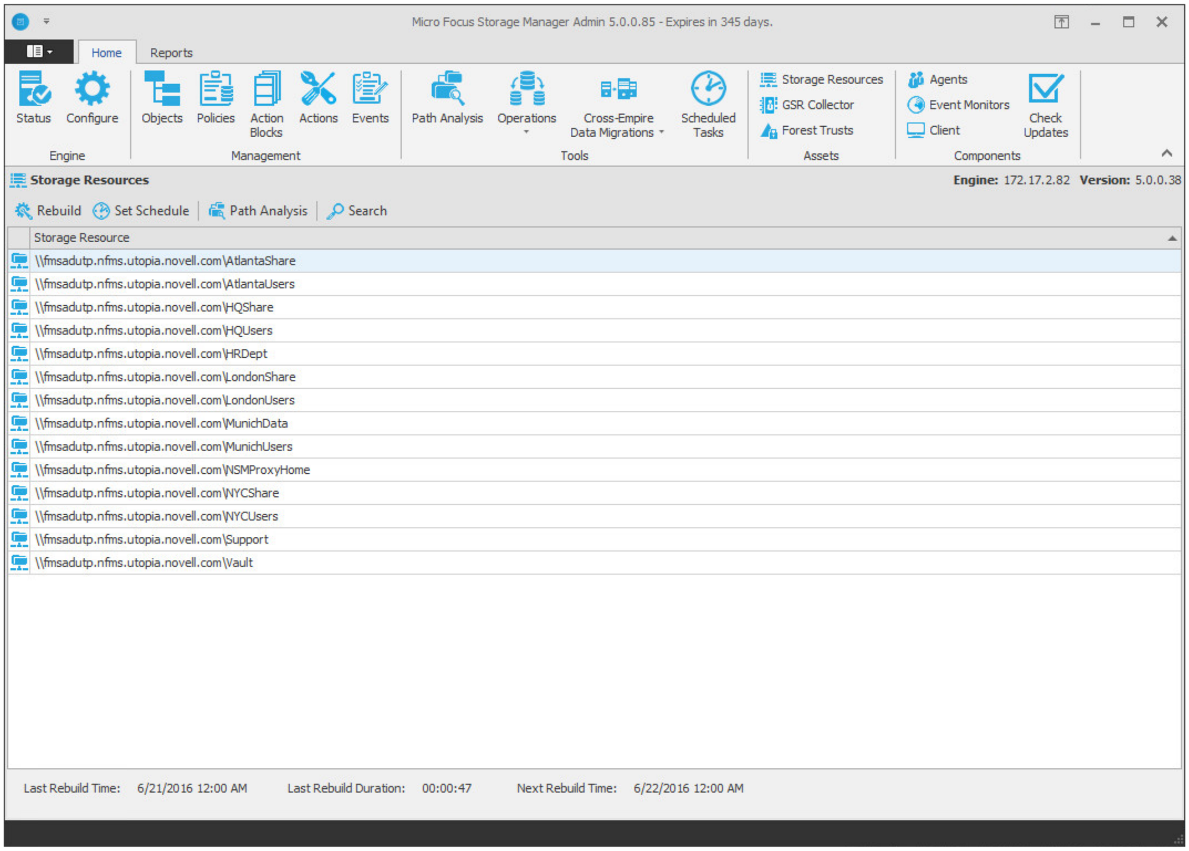
9 In the **Schedule Recurrence** region, specify the frequency of the operation.

10 Click **OK**.

## 13.1.12 Storage Resources

This page lets you rebuild the storage resource cache used in Storage Manager. Because Storage Manager 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.

*Figure 13-22 Storage Resources Page*



**Engine:** 172.17.2.82 **Version:** 5.0.0.38

\\fmsadutp.nfms.utopia.novell.com\AtlantaShare
\\fmsadutp.nfms.utopia.novell.com\AtlantaUsers
\\fmsadutp.nfms.utopia.novell.com\HQShare
\\fmsadutp.nfms.utopia.novell.com\HQUsers
\\fmsadutp.nfms.utopia.novell.com\HRDept
\\fmsadutp.nfms.utopia.novell.com\LondonShare
\\fmsadutp.nfms.utopia.novell.com\LondonUsers
\\fmsadutp.nfms.utopia.novell.com\MunichData
\\fmsadutp.nfms.utopia.novell.com\MunichUsers
\\fmsadutp.nfms.utopia.novell.com\NSMProxyHome
\\fmsadutp.nfms.utopia.novell.com\NYCShare
\\fmsadutp.nfms.utopia.novell.com\NYCUsers
\\fmsadutp.nfms.utopia.novell.com\Support
\\fmsadutp.nfms.utopia.novell.com\Vault

Last Rebuild Time: 6/21/2016 12:00 AM Last Rebuild Duration: 00:00:47 Next Rebuild Time: 6/22/2016 12:00 AM

**Rebuild:** Clicking this button initiates a search within the entire forest domain 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.

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

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

**Search:** Provides a search field for storage resources.

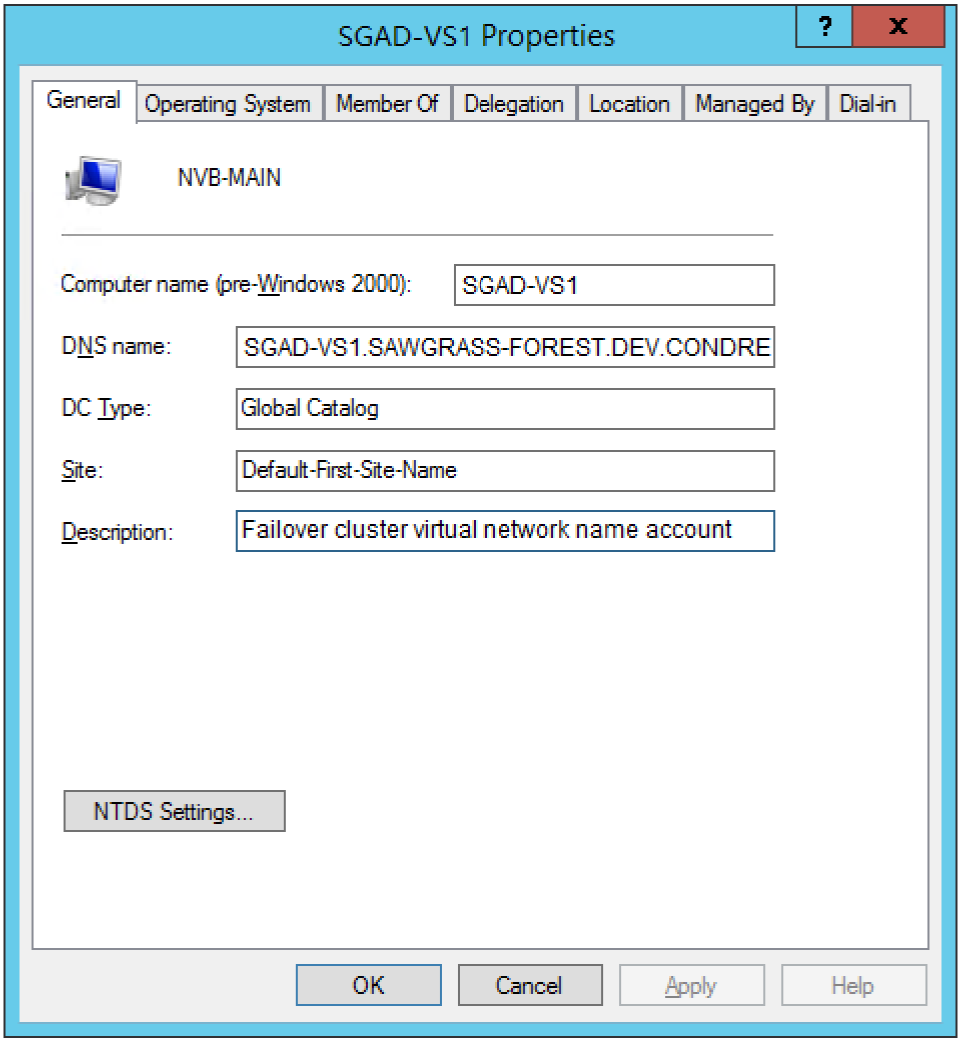
**Last Rebuild Time:** Displays the last date and time that the storage resource list was rebuilt.

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

**Next Rebuild Time:** Displays the date and time when Storage Manager 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, Storage Manager cannot see it as a storage resource.



NVB-MAIN

Computer name (pre-Windows 2000): SGAD-VS1

DNS name: SGAD-VS1.SAWGRASS-FOREST.DEV.CONDRE

DC Type: Global Catalog

Site: Default-First-Site-Name

Description: Failover cluster virtual network name account

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” on page 279.

## 13.1.13 GSR Collector

- “GSR Collector Configuration” on page 284
- “GSR Collector Configuration Scenarios” on page 287

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 Storage Manager. 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.

**NOTE:** GSR Anomaly Analysis is discussed in Section 13.2.3, "GSR Anomaly," on page 318.

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.

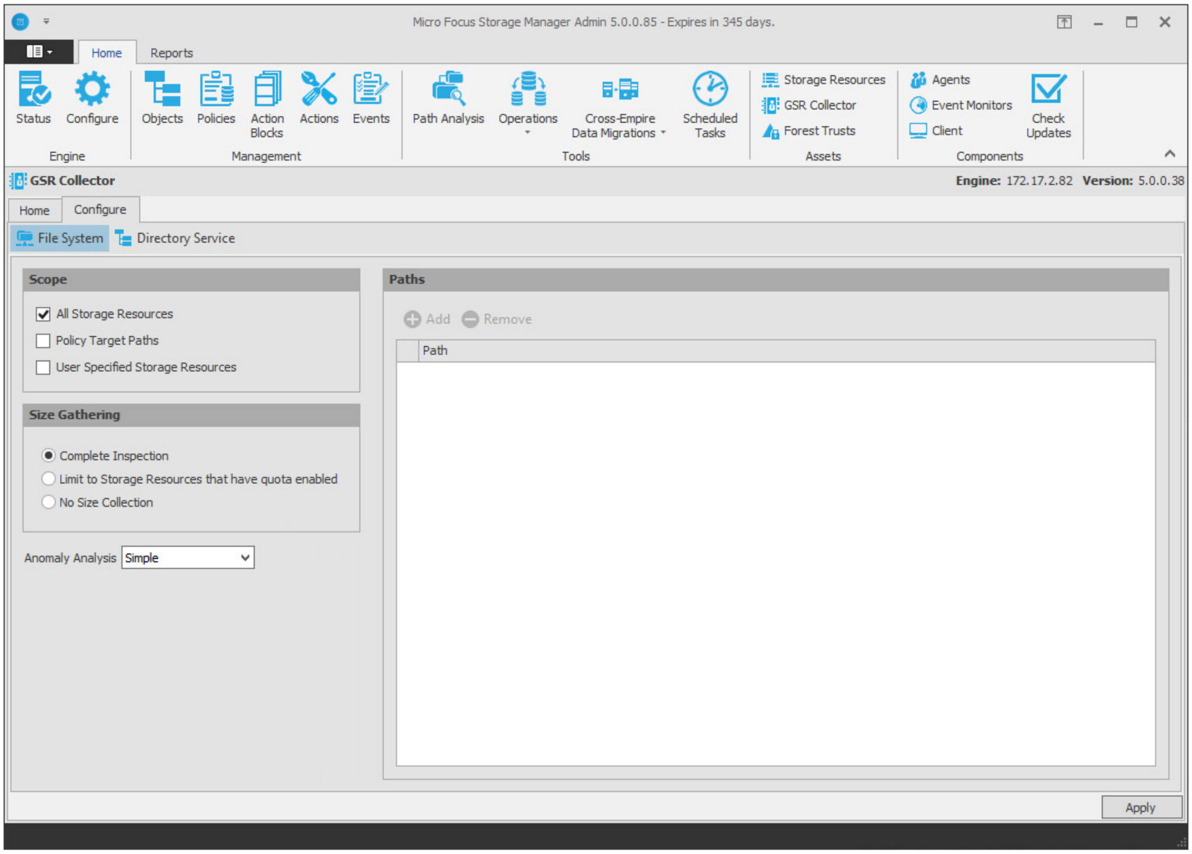
### Performance Caveats

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 Storage Manager 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 Storage Manager. You should be careful when running the GSR Collector during peak traffic load on the Engine.

## GSR Collector 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.

***Figure 13-23** File System Configuration Settings for the GSR Collector*



Micro Focus Storage Manager Admin 5.0.0.85 - Expires in 345 days.

GSR Collector

**Engine:** 172.17.2.82 **Version:** 5.0.0.38

Scope

☑ All Storage Resources

□ Policy Target Paths

□ User Specified Storage Resources

Size Gathering

● Complete Inspection

○ Limit to Storage Resources that have quota enabled

○ No Size Collection

Anomaly Analysis: Simple

Paths

## File System

**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 User 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 User 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.
- **User Specified 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

**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 **User 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 U**ser 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.
- **User 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)

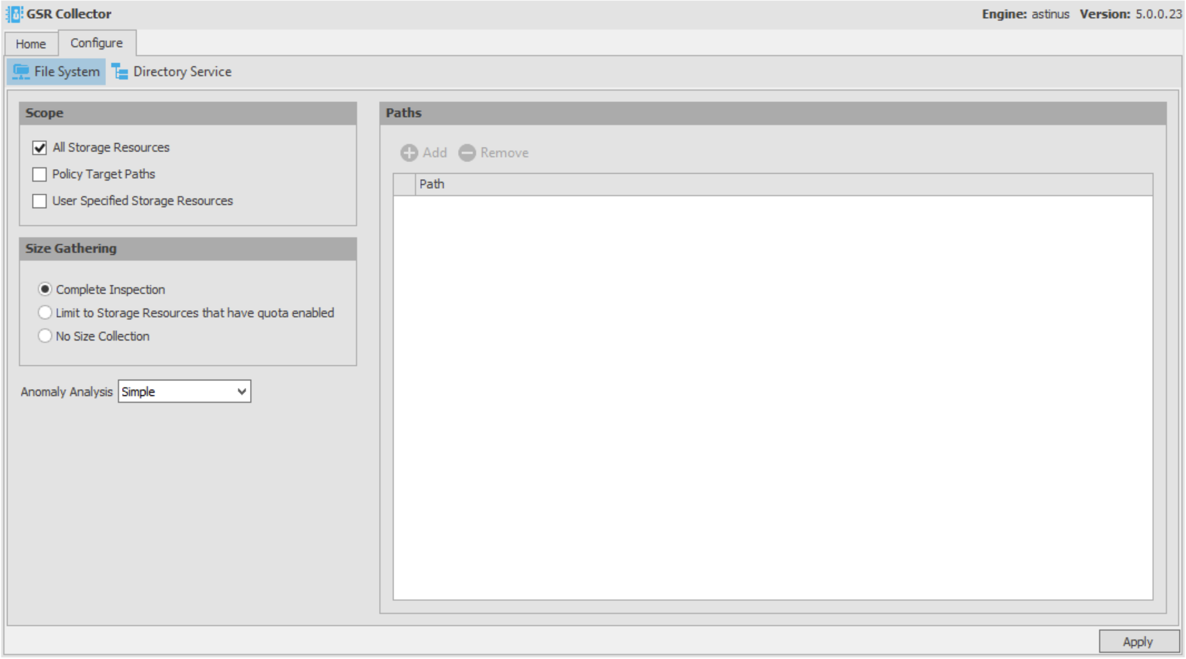
## GSR Collector Configuration Scenarios

- “All Storage Resources + Complete Inspection” on page 287
- “All Storage Resources + Limited to Storage Resources that Have Quota Enabled” on page 288
- “All Storage Resources + No Size Collection” on page 289

### 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.

***Figure 13-24*** *All Storage Resources + Complete Inspection*



Engine: astinus Version: 5.0.0.23

Scope

☑ All Storage Resources
□ Policy Target Paths
□ User Specified Storage Resources

Size Gathering

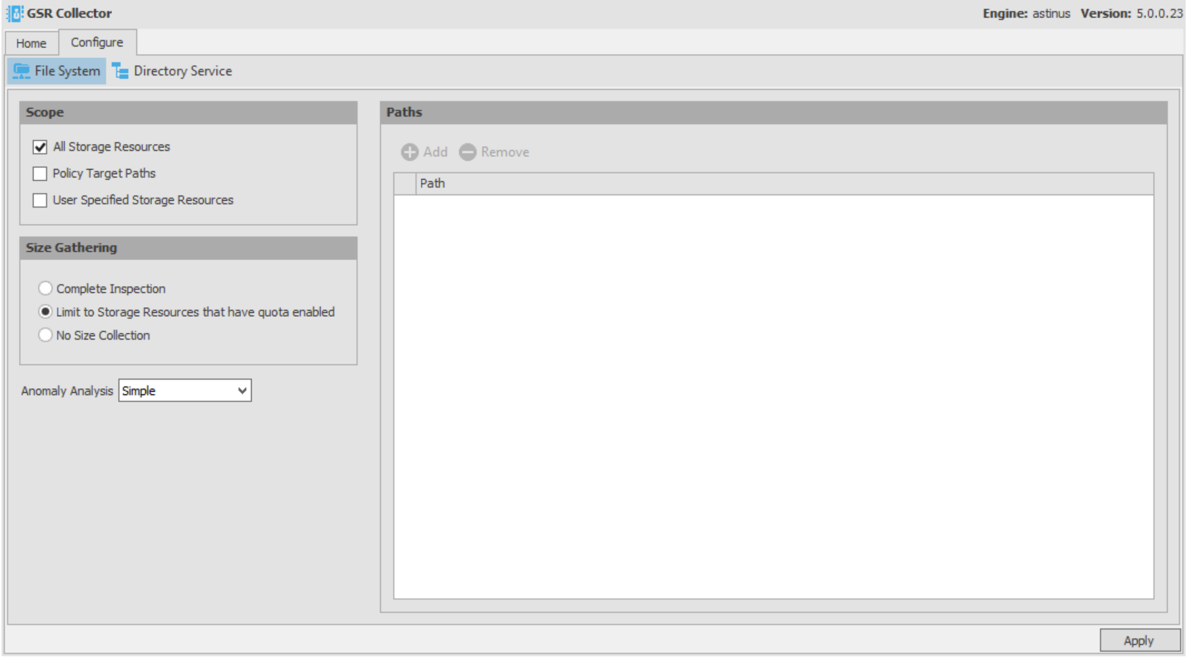
● Complete Inspection
○ Limit to Storage Resources that have quota enabled
○ No Size Collection

Anomaly Analysis: Simple

## 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.

*Figure 13-25 All Storage Resources + Limited to Storage Resources that Have Quota Enabled*



Scope

☑ All Storage Resources
□ Policy Target Paths
□ User Specified Storage Resources

Size Gathering

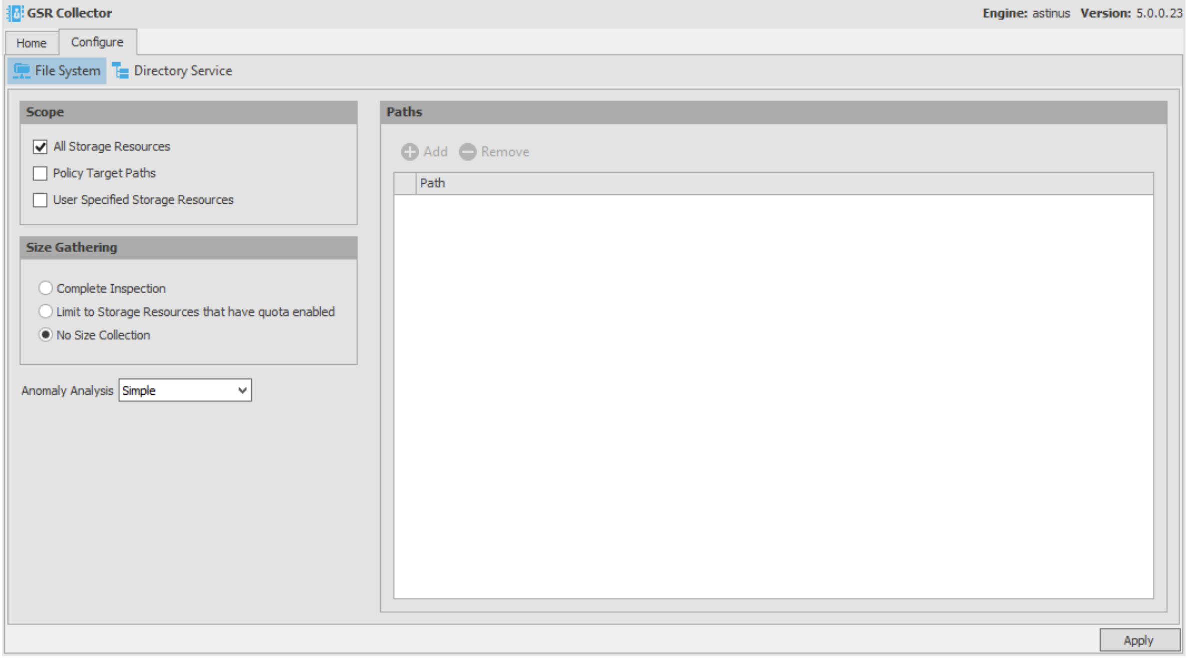
○ Complete Inspection
● Limit to Storage Resources that have quota enabled
○ No Size Collection

Anomaly Analysis: Simple

## 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.

*Figure 13-26 All Storage Resources + No Size Collection*



Scope

☑ All Storage Resources
□ Policy Target Paths
□ User Specified Storage Resources

Size Gathering

○ Complete Inspection
○ Limit to Storage Resources that have quota enabled
● No Size Collection

Anomaly Analysis: Simple

# 13.1.14 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.

## Overview

Storage Manager has limited support for forest trusts for Active Directory to Active Directory Cross-Empire Data Migration and for managing storage resources in another forest. The trust cannot be leveraged to monitor for events in another forest.

To configure a supported forest trust, see "Configuring a Forest Trust" on page 291. After a forest trust is configured for use, you will need to set the appropriate permissions on shares so that they can be made available for access and management.

After a supported forest trust is established, SMAdmin can be used to enable it for use. Multiple forest trusts can be established and configured for use.To enable an established forest trust for use, refer to "Managing Forest Trusts" on page 300.

***Table 13-1*** *Supported Trusts*

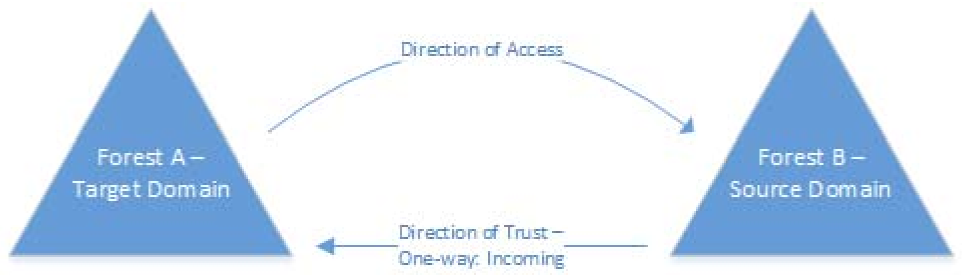
| Trust Type | Direction | Scope of Authentication | Supported |
|---|---|---|---|
| External | One-way or two-way | Selective or Forest-wide | No |
| Realm | One-way or two-way | Selective or Forest-wide | No |
| Forest | One-way or two-way | Selective | No |
| Forest | One-way incoming or two-way |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

### Active Directory Cross-Empire Data Migration Trust Scenarios

### One-way Incoming

In this scenario, a one-way incoming trust has been established between Forest A and Forest B. Here, Storage Manager will copy data and permissions from storage resources in Forest B to Forest A.

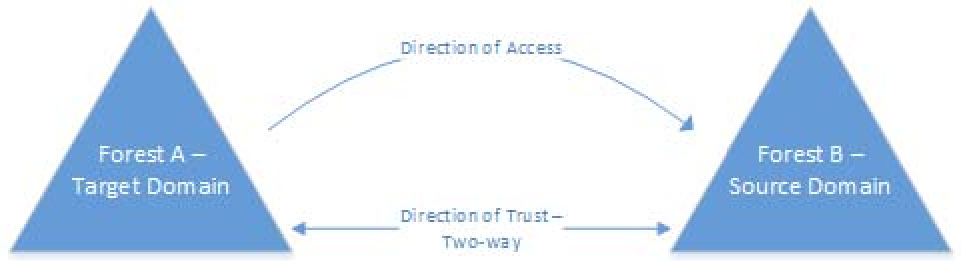
*Figure 13-27 One-way: Incoming Forest Trust*



### Two-way

In this scenario, a two-way trust has been established between Forest A and Forest B. Here, Storage Manager will copy data and permissions from storage resources in Forest B to Forest A.

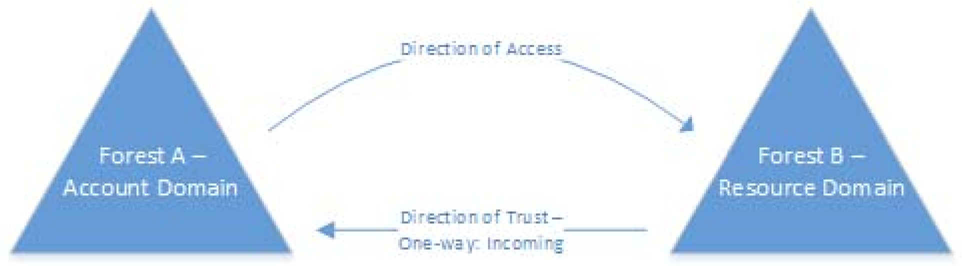
*Figure 13-28 Two-way Forest Trust*



### Trusted Resource Management Scenario

In this scenario, a one-way incoming trust has been established between Forest A and Forest B. Here, Storage Manager will monitor for events in Forest A account forest and manage data in the Forest B resource forest.

*Figure 13-29 One-way: Incoming Trust*



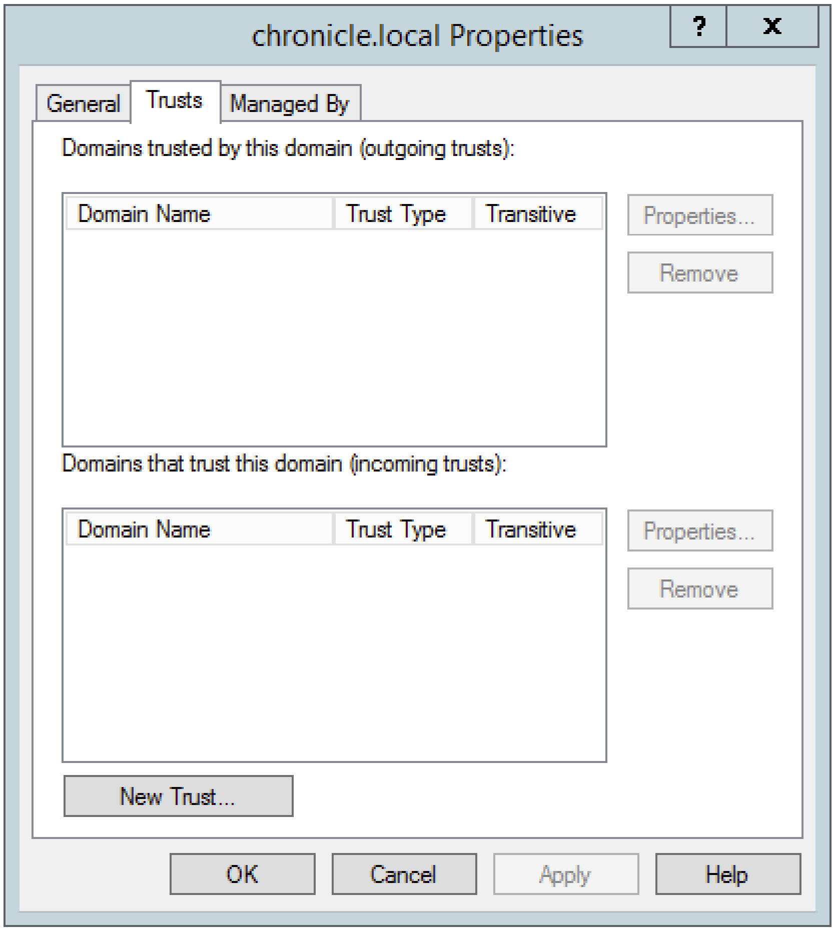
For more information on Active Directory Domains and Trusts, see https://technet.microsoft.com/en-us/library/cc770299.aspx.

## Configuring a Forest Trust

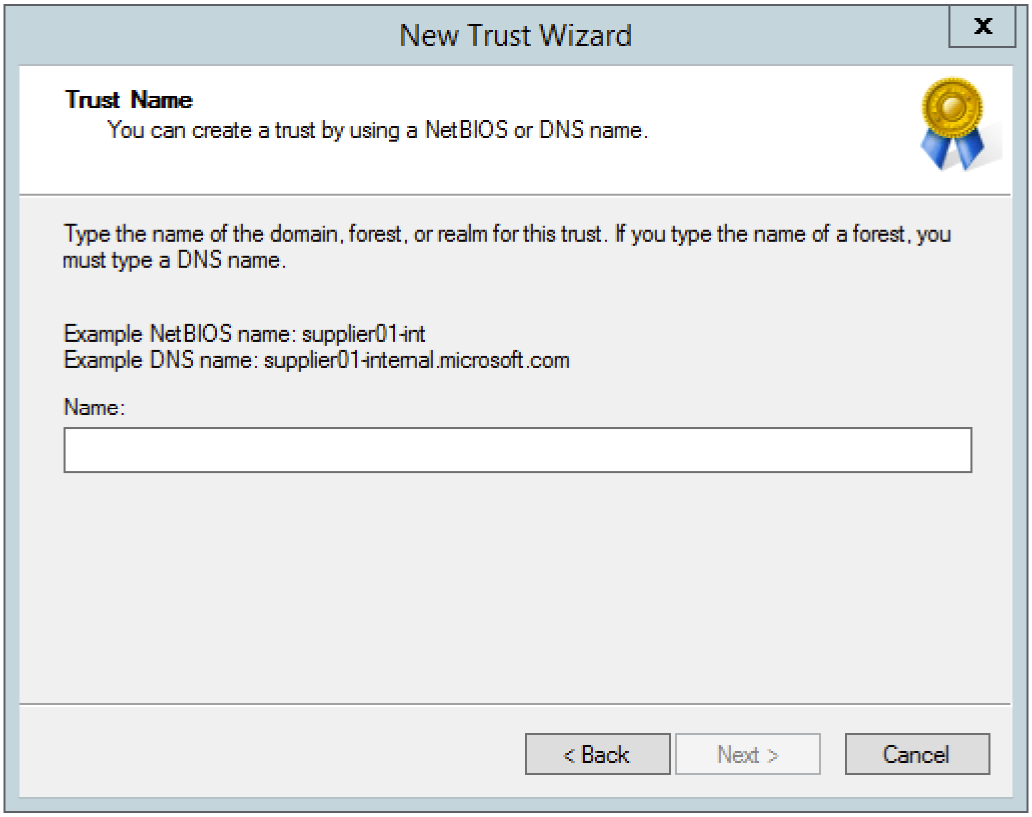
1 On a server in the target forest in which Storage Manager is installed, open Active Directory Domains and Trusts.

2 Right click the target forest in which Storage Manager is installed and click **Properties**.

3 In the properties dialog box, click **New Trust**.



4 In the New Trust Wizard dialog box, enter the DNS name for the incoming forest trust and click **Next**.



New Trust Wizard

**Trust Name**

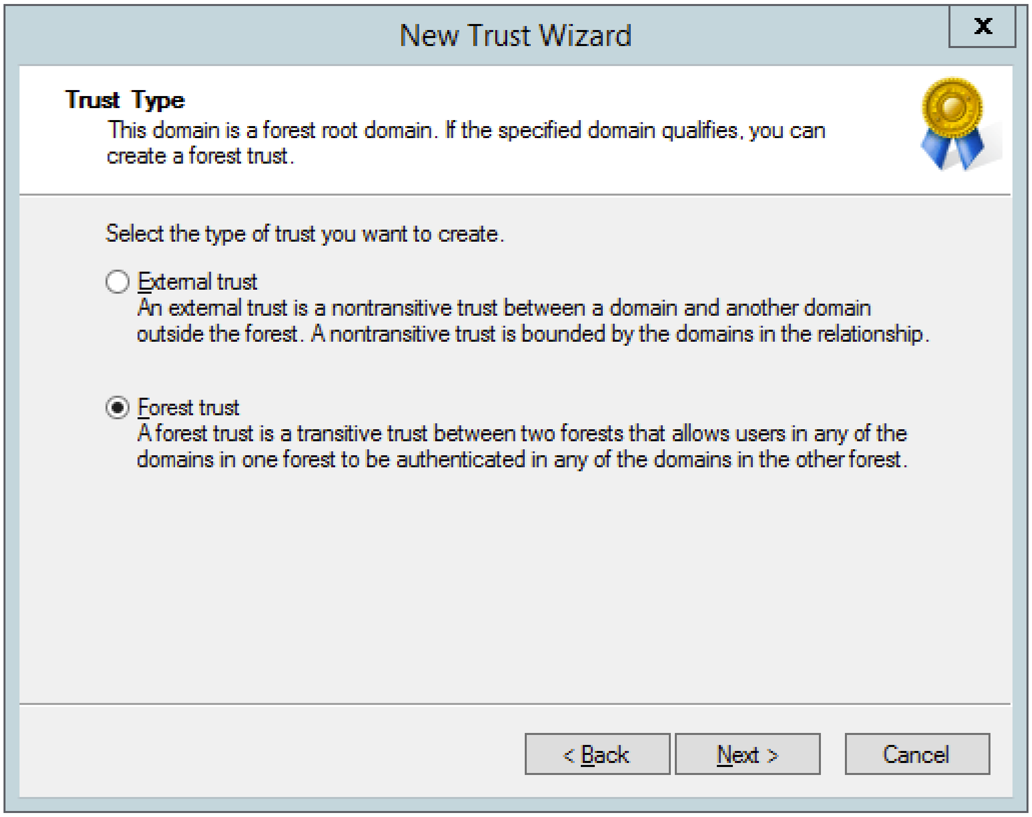
You can create a trust by using a NetBIOS or DNS name.

Type the name of the domain, forest, or realm for this trust. If you type the name of a forest, you must type a DNS name.

Example NetBIOS name: supplier01-int
Example DNS name: supplier01-internal.microsoft.com

Name:

5 For the Trust Type, select **Forest trust** and click **Next**.



New Trust Wizard

**Trust Type**

This domain is a forest root domain. If the specified domain qualifies, you can create a forest trust.

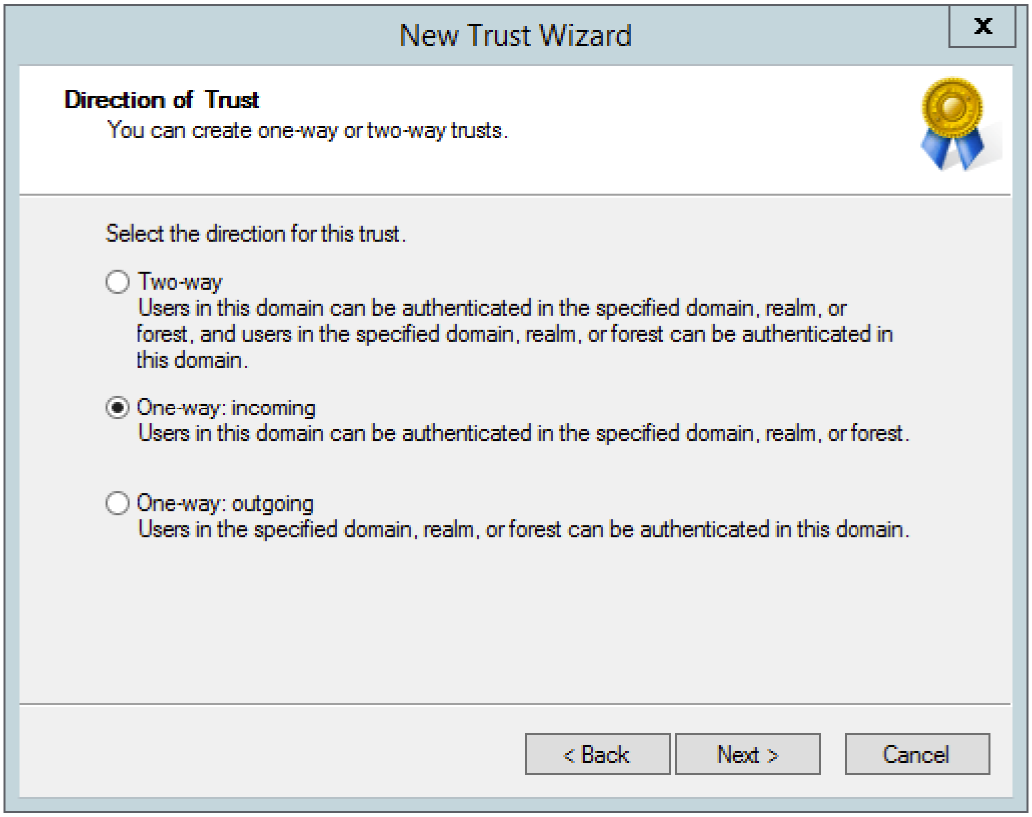
Select the type of trust you want to create.

○ External trust
An external trust is a nontransitive trust between a domain and another domain outside the forest. A nontransitive trust is bounded by the domains in the relationship.

● Forest trust
A forest trust is a transitive trust between two forests that allows users in any of the domains in one forest to be authenticated in any of the domains in the other forest.

6 Unless you need a two-way trust, select **One-way: incoming** and click **Next**.

Storage Manager supports Two-way or One-way: incoming directional trusts.



New Trust Wizard

**Direction of Trust**

You can create one-way or two-way trusts.

Select the direction for this trust.

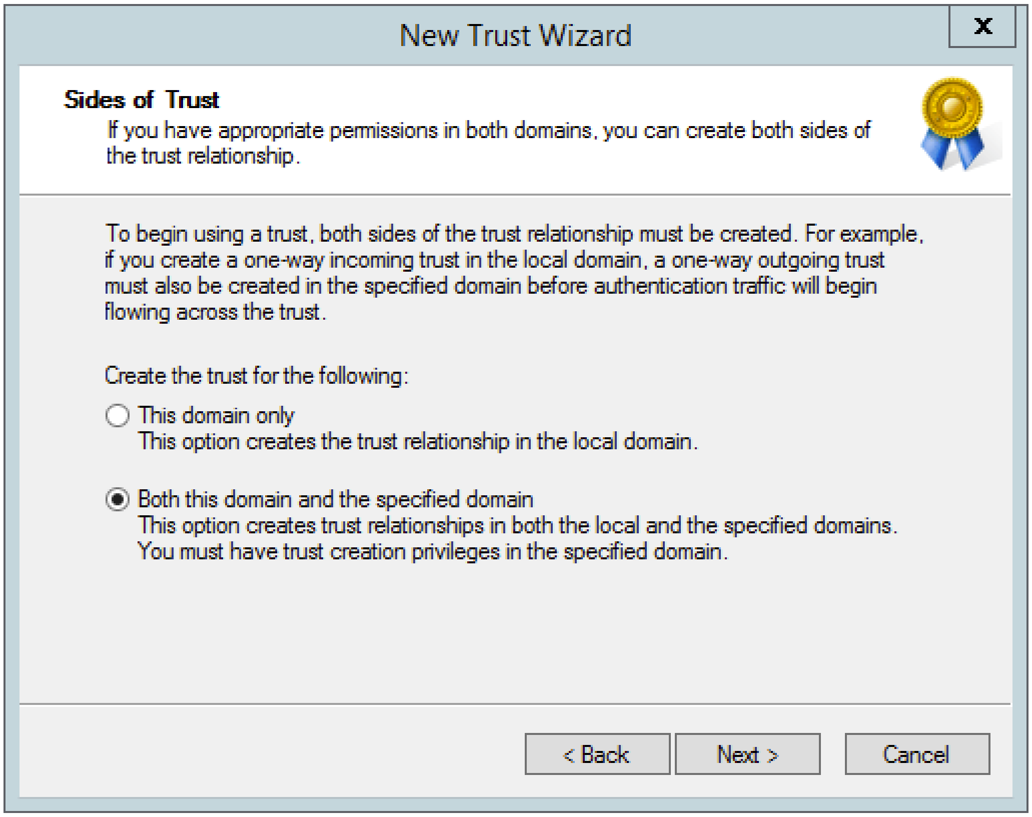
○ Two-way
Users in this domain can be authenticated in the specified domain, realm, or forest, and users in the specified domain, realm, or forest can be authenticated in this domain.

● One-way: incoming
Users in this domain can be authenticated in the specified domain, realm, or forest.

○ One-way: outgoing
Users in the specified domain, realm, or forest can be authenticated in this domain.

7 (Conditional) If you have the necessary permissions, specify **Both this domain and the specified domain** and click **Next**.

Depending on the appropriate permissions that you have as the user you're logged in as, you can create both sides of the trust relationship.



**Sides of Trust**

If you have appropriate permissions in both domains, you can create both sides of the trust relationship.

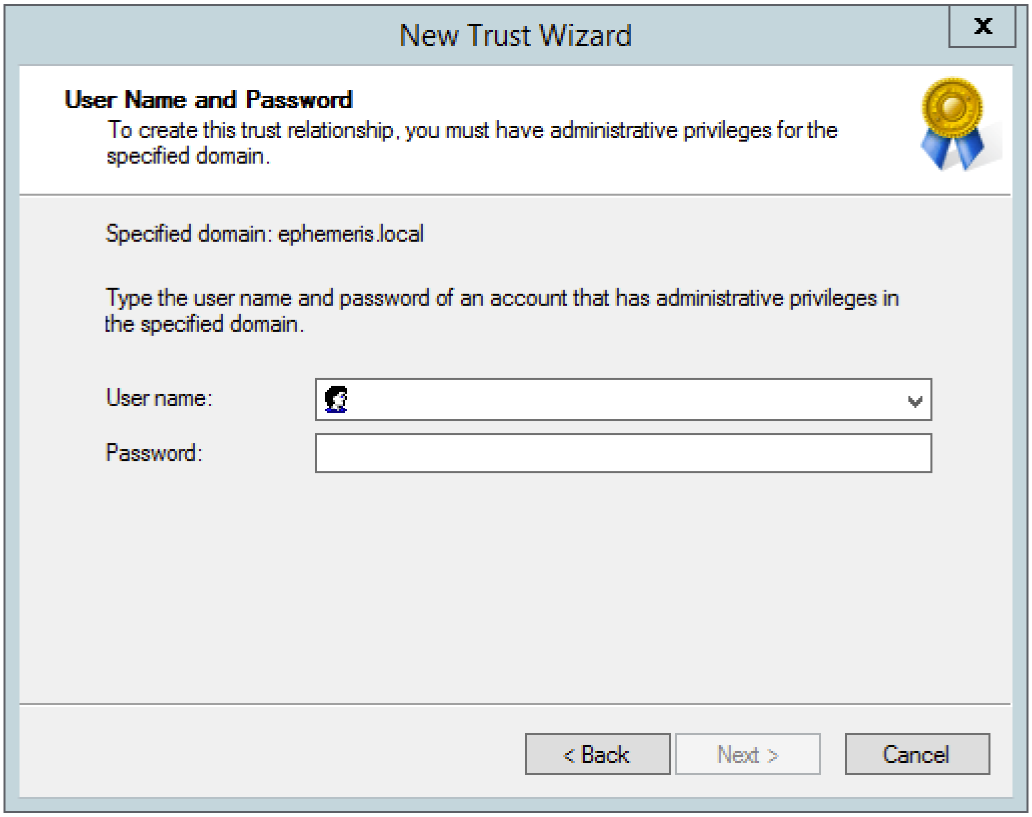
To begin using a trust, both sides of the trust relationship must be created. For example, if you create a one-way incoming trust in the local domain, a one-way outgoing trust must also be created in the specified domain before authentication traffic will begin flowing across the trust.

Create the trust for the following:

○ This domain only
This option creates the trust relationship in the local domain.

● Both this domain and the specified domain
This option creates trust relationships in both the local and the specified domains. You must have trust creation privileges in the specified domain.

8 Enter credentials for the specified source domain and click **Next**.



**User Name and Password**

To create this trust relationship, you must have administrative privileges for the specified domain.

Specified domain: ephemeris.local

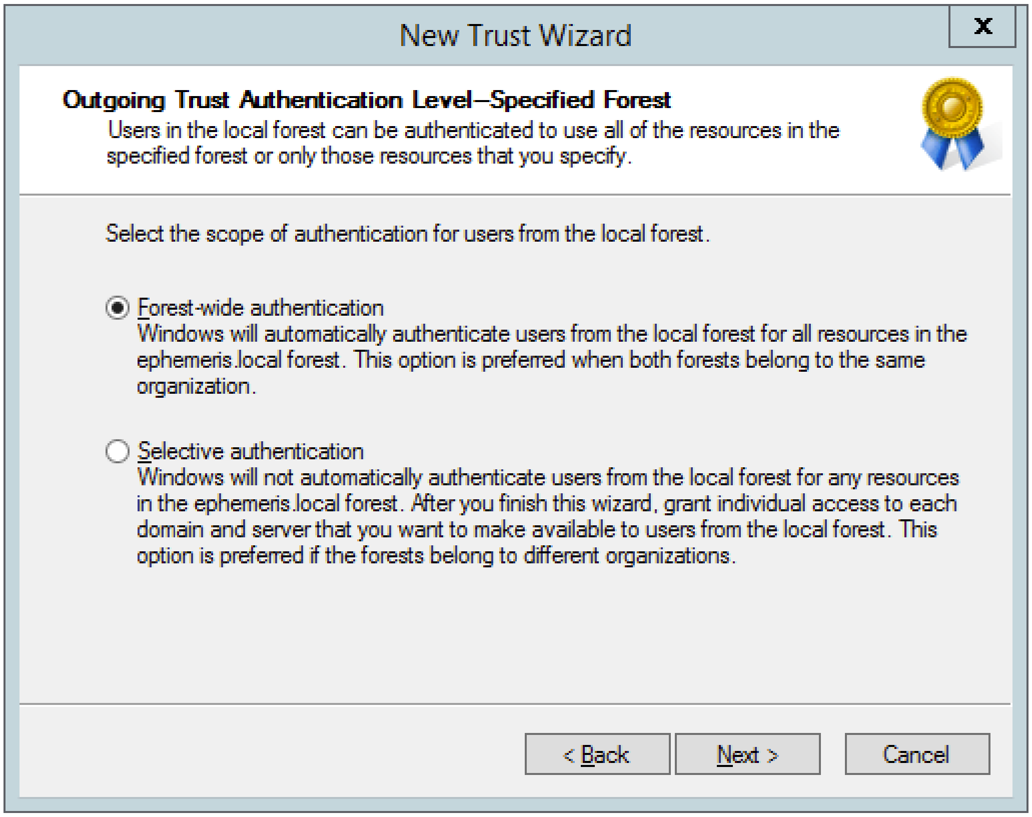
Type the user name and password of an account that has administrative privileges in the specified domain.

User name:

Password:

9 Specify **Forest-wide authentication** and click **Next**

Storage Manager requires Forest-wide authentication.



**Outgoing Trust Authentication Level—Specified Forest**

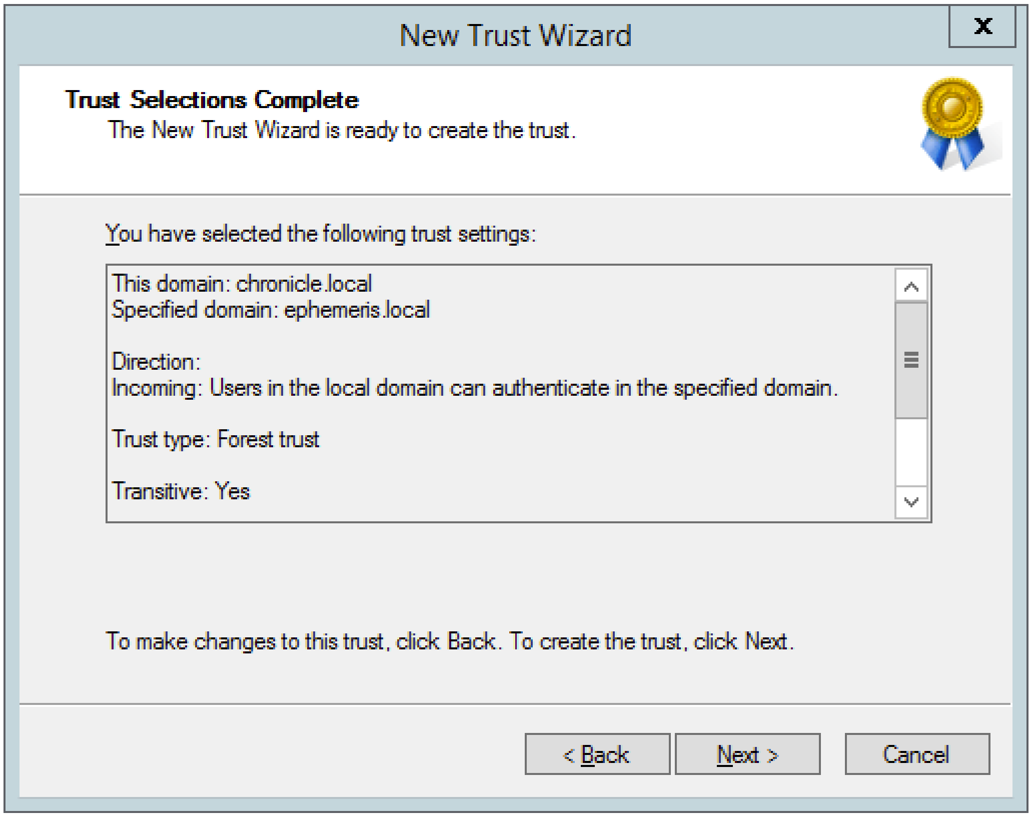
Users in the local forest can be authenticated to use all of the resources in the specified forest or only those resources that you specify.

Select the scope of authentication for users from the local forest.

● Forest-wide authentication
Windows will automatically authenticate users from the local forest for all resources in the ephemeris.local forest. This option is preferred when both forests belong to the same organization.

○ Selective authentication
Windows will not automatically authenticate users from the local forest for any resources in the ephemeris.local forest. After you finish this wizard, grant individual access to each domain and server that you want to make available to users from the local forest. This option is preferred if the forests belong to different organizations.

10 Review the selected trust settings. If everything is correct, click **Next**.



**Trust Selections Complete**

The New Trust Wizard is ready to create the trust.

You have selected the following trust settings:

This domain: chronicle.local
Specified domain: ephemeris.local

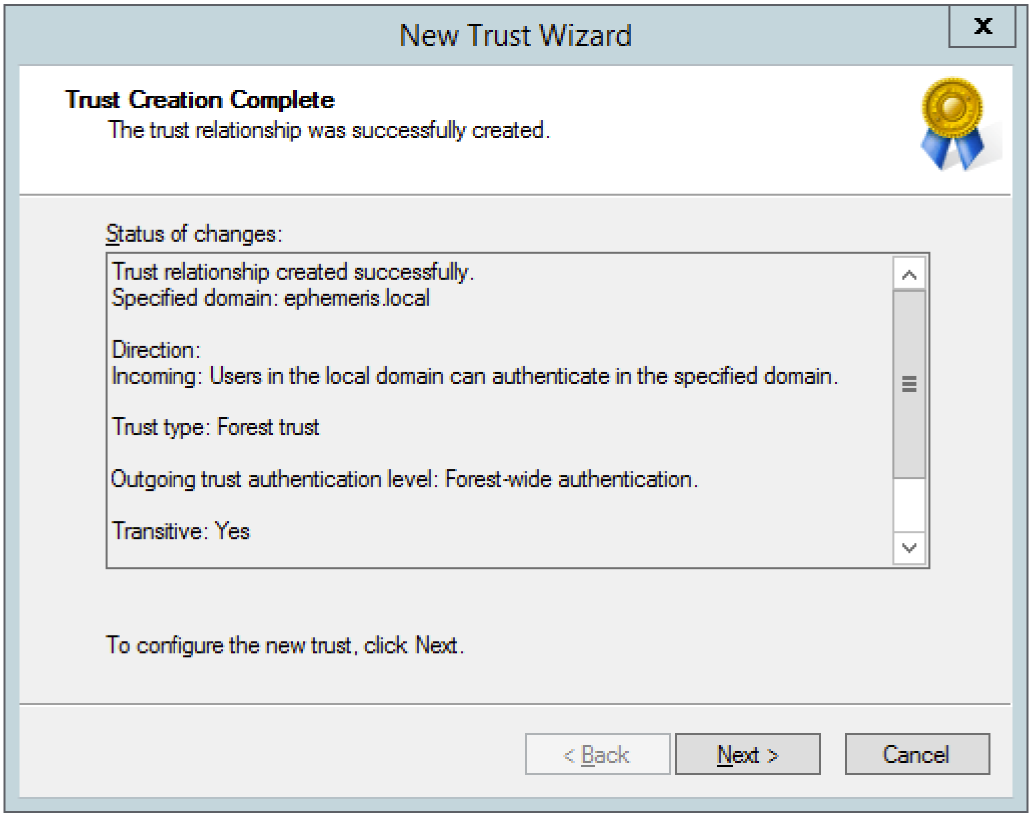
Direction:
Incoming: Users in the local domain can authenticate in the specified domain.

Trust type: Forest trust

Transitive: Yes

To make changes to this trust, click Back. To create the trust, click Next.

**11** Once the trust is successfully created, click **Next**.



**Trust Creation Complete**

The trust relationship was successfully created.

Status of changes:

Trust relationship created successfully.
Specified domain: ephemeris.local

Direction:
Incoming: Users in the local domain can authenticate in the specified domain.

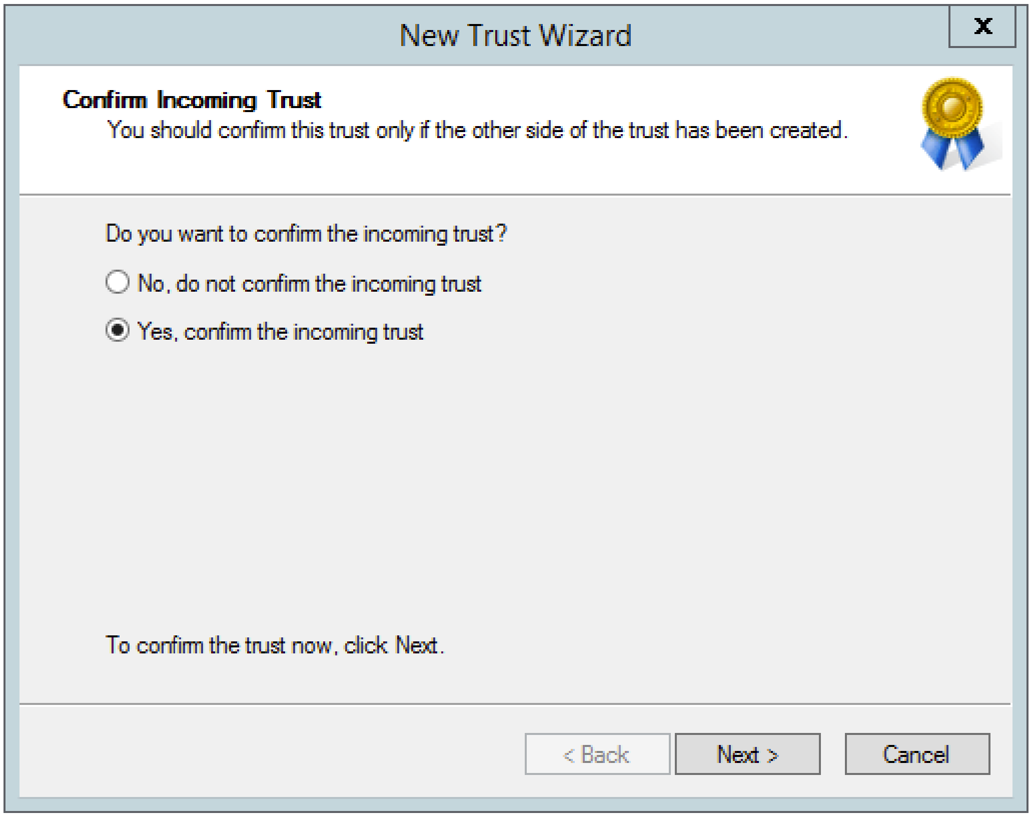
Trust type: Forest trust

Outgoing trust authentication level: Forest-wide authentication.

Transitive: Yes

To configure the new trust, click Next.

**12** To validate the trust, specify **Yes**, confirm the incoming trust and click **Next**.



**Confirm Incoming Trust**

You should confirm this trust only if the other side of the trust has been created.

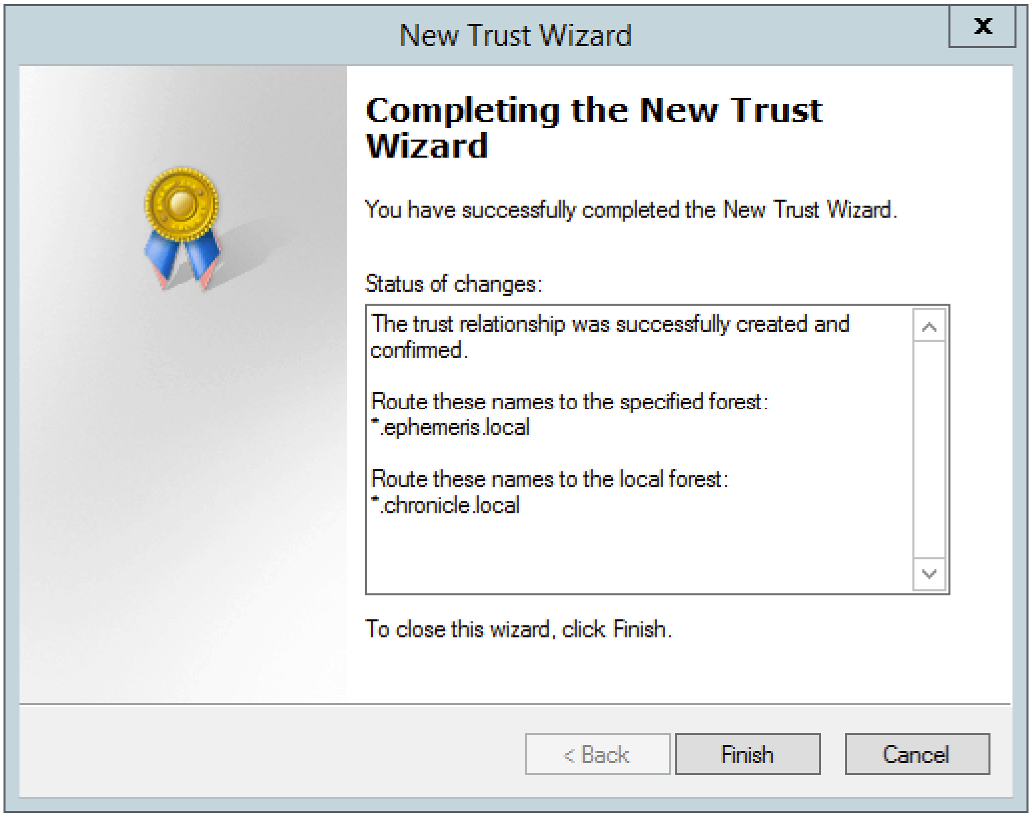
Do you want to confirm the incoming trust?

○ No, do not confirm the incoming trust

● Yes, confirm the incoming trust

To confirm the trust now, click Next.

**13** View the updated status of changes and click **Finish**.



Completing the New Trust Wizard

You have successfully completed the New Trust Wizard.

Status of changes:

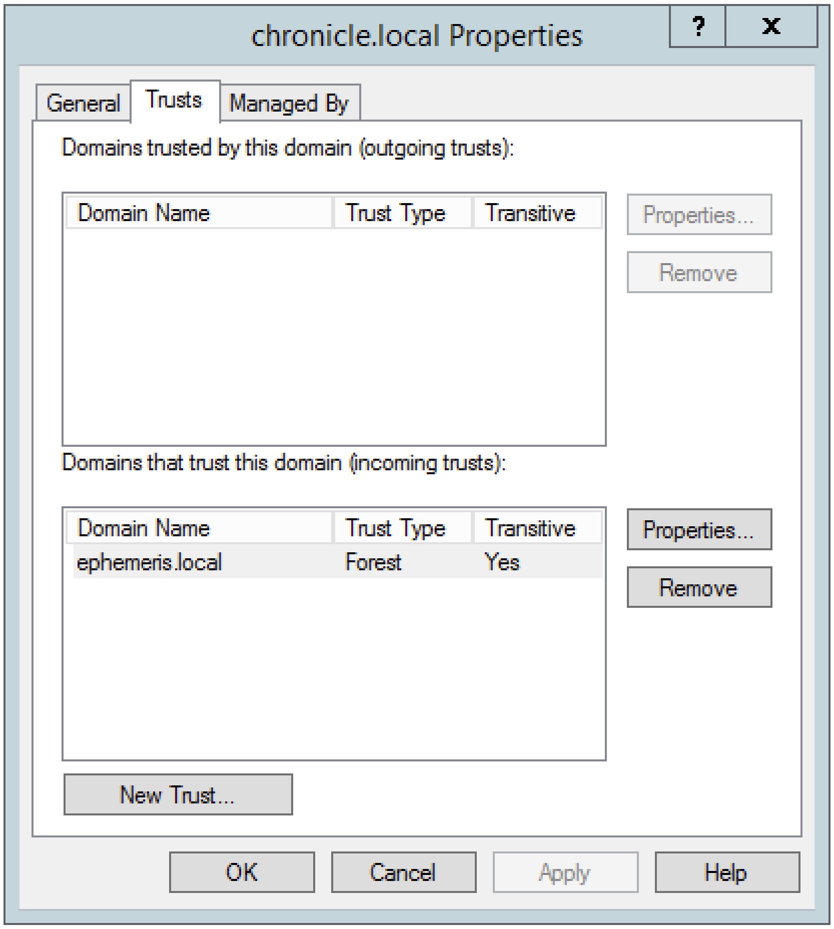
The trust relationship was successfully created and confirmed.

Route these names to the specified forest:
*.ephemeris.local

Route these names to the local forest:
*.chronicle.local

To close this wizard, click Finish.

**14** In the Properties dialog box, view the new Transitive Forest Trust.



Domains trusted by this domain (outgoing trusts):

| Domain Name | Trust Type | Transitive |
|---|---|---|

Domains that trust this domain (incoming trusts):

| Domain Name | Trust Type | Transitive |
|---|---|---|
| ephemeris.local | Forest | Yes |

15 In the Properties dialog box, examine the properties of the trust by selecting the trust and clicking **Properties**.

16 Click **OK** to close the trust properties dialog box.

17 Click **OK** to close the domain properties dialog box.

Storage Manager can now be configured to use the trust for Active Directory to Active Directory Cross-Empire Data Migrations.

## Managing Forest Trusts

Once a supported forest trust is established, SMAdmin can be used to enable it for use. Forest trusts are primarily used for Active Directory to Active Directory Cross-Empire Data Migrations. However, they can also be used in a scenario where a storage resource resides in a trusted forest.

After a forest trust is configured for use, you will need to set the appropriate permissions on shares so that they can be made available for access and management.

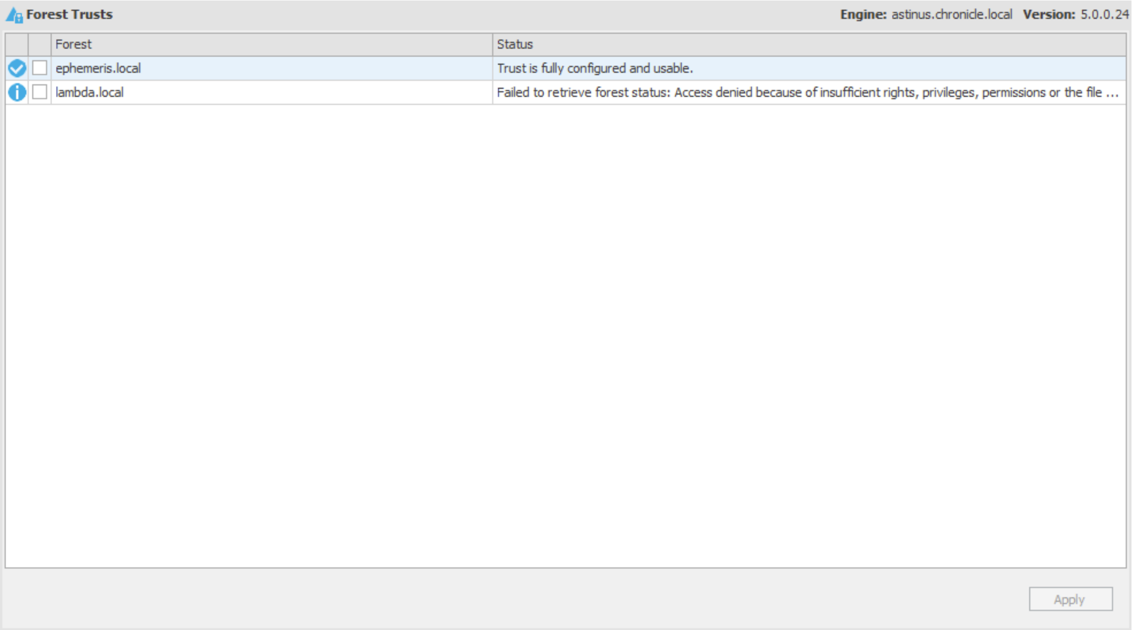
Multiple forest trusts can be established and configured for use.

### Example 1

1 In SMAdmin, click the **Home** tab.

2 Click **Forest Trusts**.

If you have configured forest trusts, they will appear in the list of Forest Trusts.

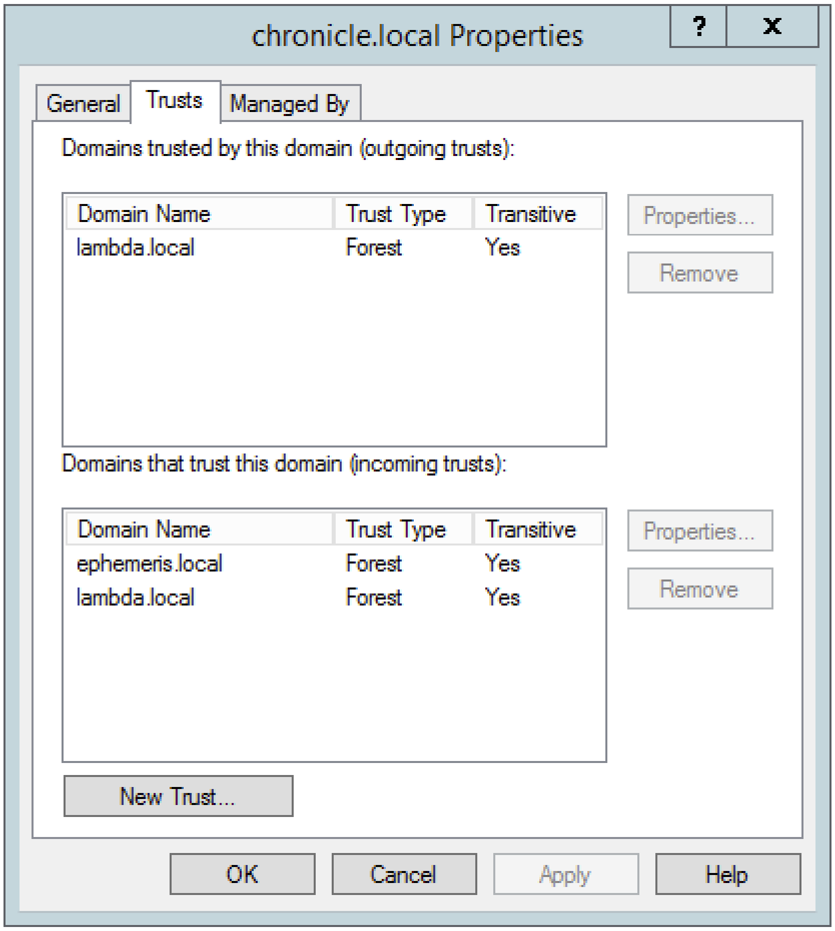


**Forest Trusts** **Engine:** astinus.chronicle.local **Version:** 5.0.0.24

|  |  | Forest | Status |
|---|---|---|---|
| ✓ | □ | ephemeris.local | Trust is fully configured and usable. |
| ⓘ | □ | lambda.local | Failed to retrieve forest status: Access denied because of insufficient rights, privileges, permissions or the file ... |

Supported forest trusts will have a check mark next to them. Unsupported forest trusts will be designated with an exclamation point. The **Status** column provides descriptive text as to why the forest trust is unsupported. If you select the check box to enable an unsupported forest trust, you will receive an error dialog indicating that the forest trust cannot be managed.

The properties for the chronicle.local forest are shown below.



chronicle.local Properties

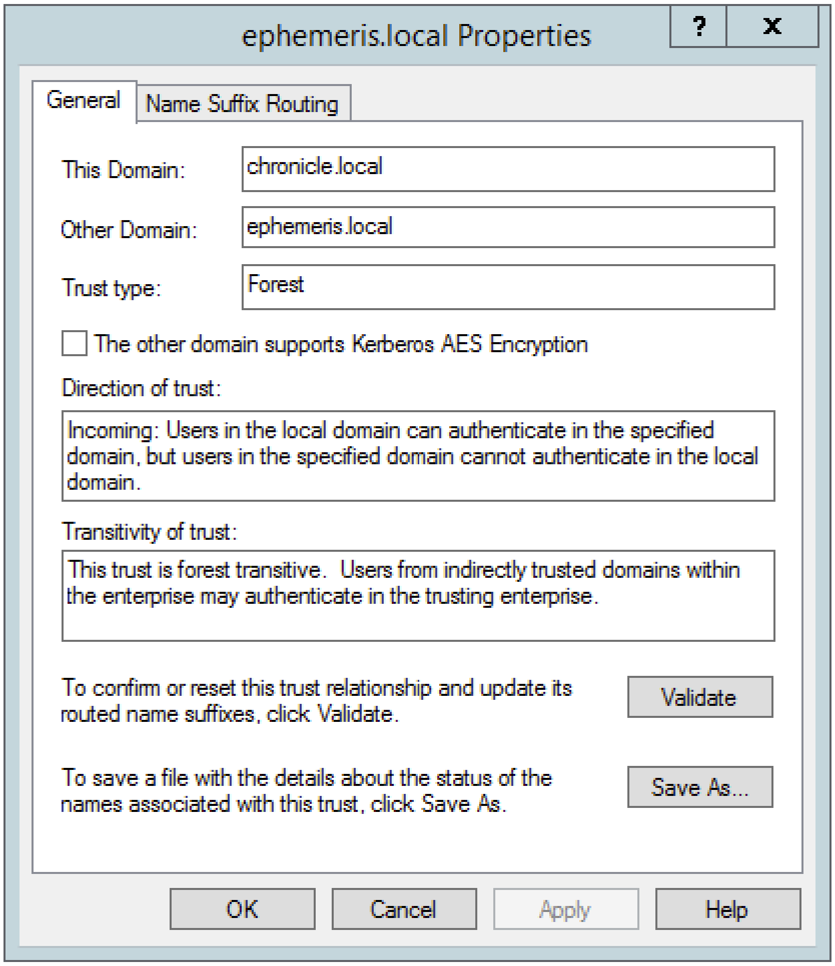
Domains trusted by this domain (outgoing trusts):

| Domain Name | Trust Type | Transitive |
|---|---|---|
| lambda.local | Forest | Yes |

Domains that trust this domain (incoming trusts):

| Domain Name | Trust Type | Transitive |
|---|---|---|
| ephemeris.local | Forest | Yes |
| lambda.local | Forest | Yes |

In the example above, `ephemeris.local` is supported.



This Domain: chronicle.local

Other Domain: ephemeris.local

Trust type: Forest

□ The other domain supports Kerberos AES Encryption

Direction of trust:

Incoming: Users in the local domain can authenticate in the specified domain, but users in the specified domain cannot authenticate in the local domain.

Transitivity of trust:

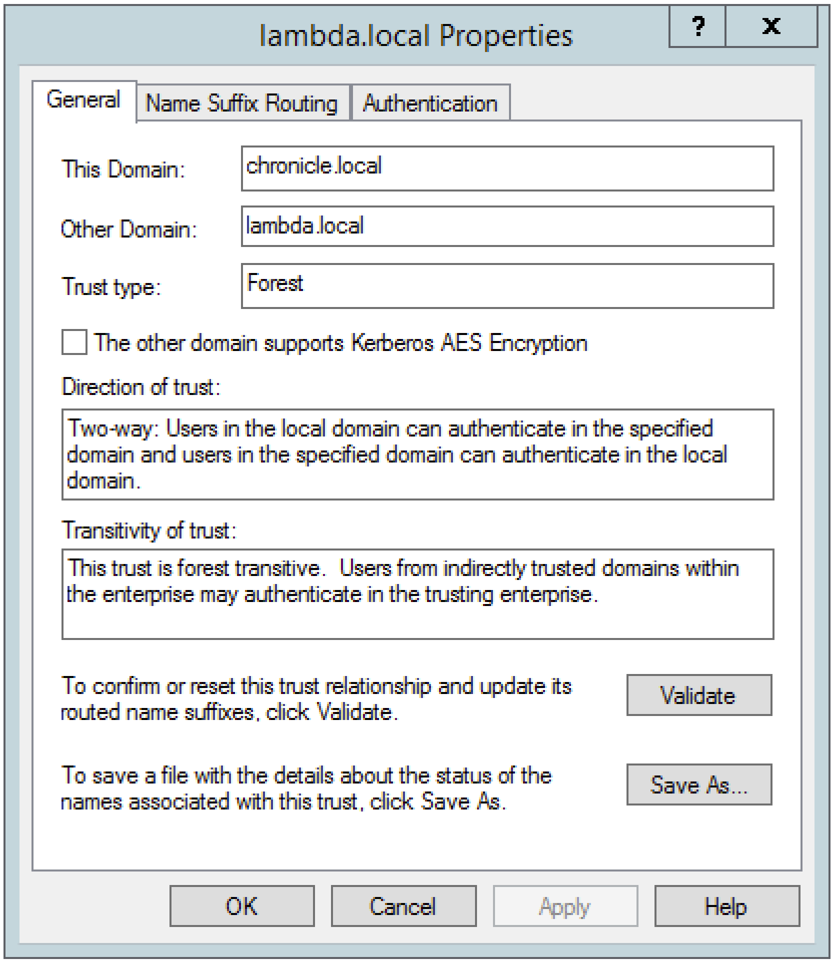
This trust is forest transitive. Users from indirectly trusted domains within the enterprise may authenticate in the trusting enterprise.

To confirm or reset this trust relationship and update its routed name suffixes, click Validate.

To save a file with the details about the status of the names associated with this trust, click Save As.

It is supported because it is a one-way incoming trust.

In the example below, `lambda.local` is not supported.



This Domain: chronicle.local

Other Domain: lambda.local

Trust type: Forest

□ The other domain supports Kerberos AES Encryption

Direction of trust:

Two-way: Users in the local domain can authenticate in the specified domain and users in the specified domain can authenticate in the local domain.

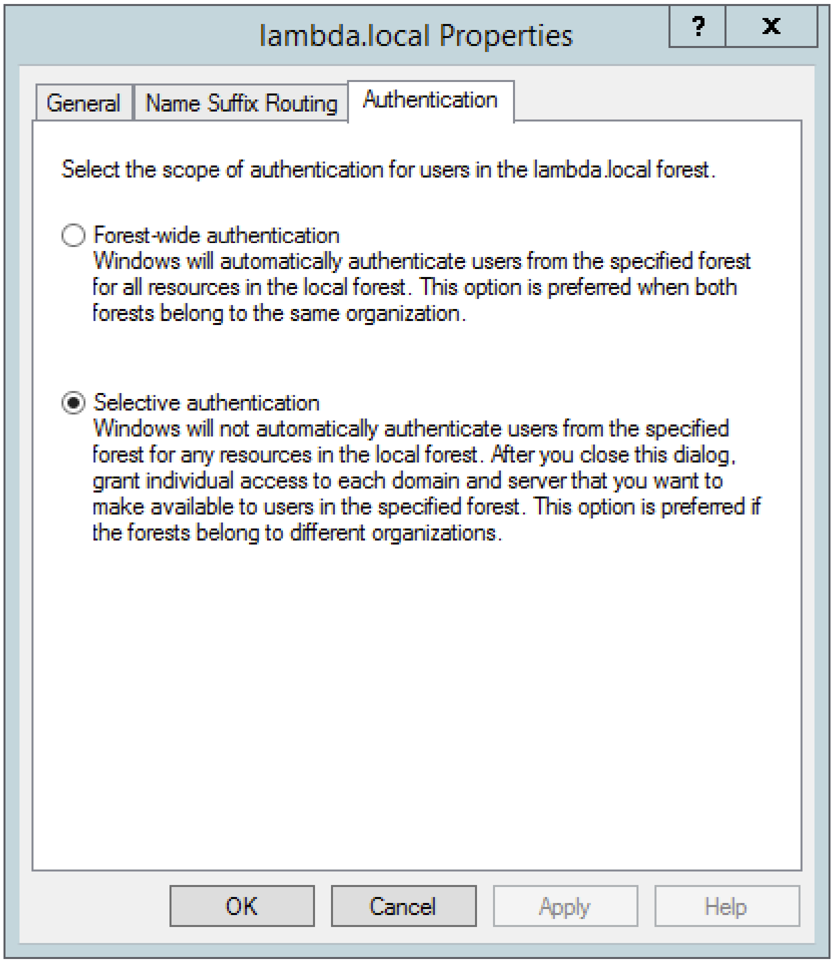
Transitivity of trust:

This trust is forest transitive. Users from indirectly trusted domains within the enterprise may authenticate in the trusting enterprise.

To confirm or reset this trust relationship and update its routed name suffixes, click Validate.

To save a file with the details about the status of the names associated with this trust, click Save As.

While it is a two-way transitive trust, it is configured for selective authentication.



Select the scope of authentication for users in the lambda.local forest.

○ Forest-wide authentication
Windows will automatically authenticate users from the specified forest for all resources in the local forest. This option is preferred when both forests belong to the same organization.

● Selective authentication
Windows will not automatically authenticate users from the specified forest for any resources in the local forest. After you close this dialog, grant individual access to each domain and server that you want to make available to users in the specified forest. This option is preferred if the forests belong to different organizations.

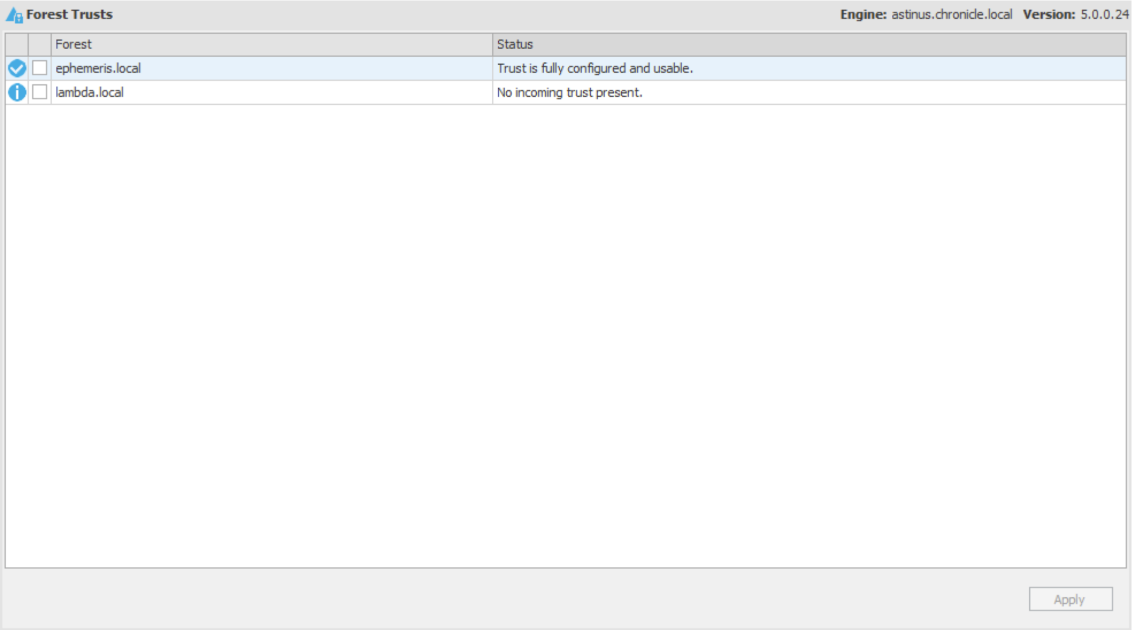
Selective authentication is an unsupported authentication scope.

## Example 2

1 In SMAdmin, click the **Home** tab.

2 Click **Forest Trusts**.

If you have configured forest trusts, they will appear in the list of Forest Trusts.



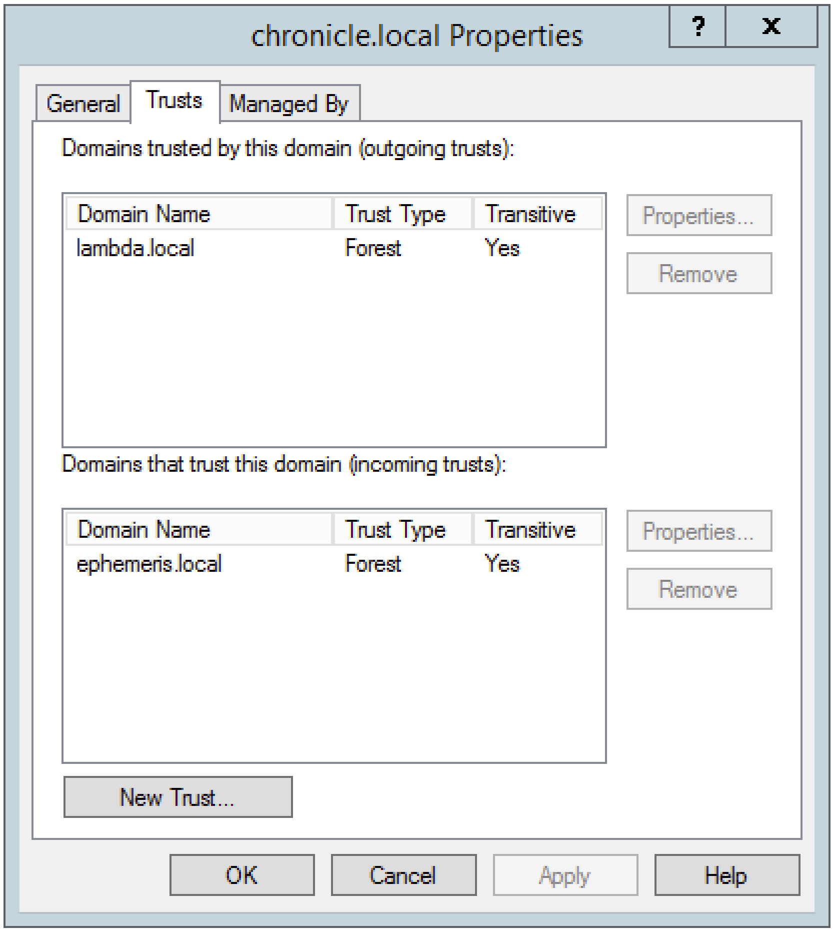
Forest Trusts

**Engine:** astinus.chronicle.local **Version:** 5.0.0.24

| | | Forest | Status |
|---|---|---|---|
| ✓ | □ | ephemeris.local | Trust is fully configured and usable. |
| ⓘ | □ | lambda.local | No incoming trust present. |

Supported forest trusts will have a check mark next to them. Unsupported forest trusts will be designated with an exclamation point. The **Status** column provides descriptive text as to why the forest trust is unsupported. If you select the check box to enable an unsupported forest trust, you will receive an error dialog indicating that the forest trust cannot be managed.

The properties for the chronicle.local forest are shown below.



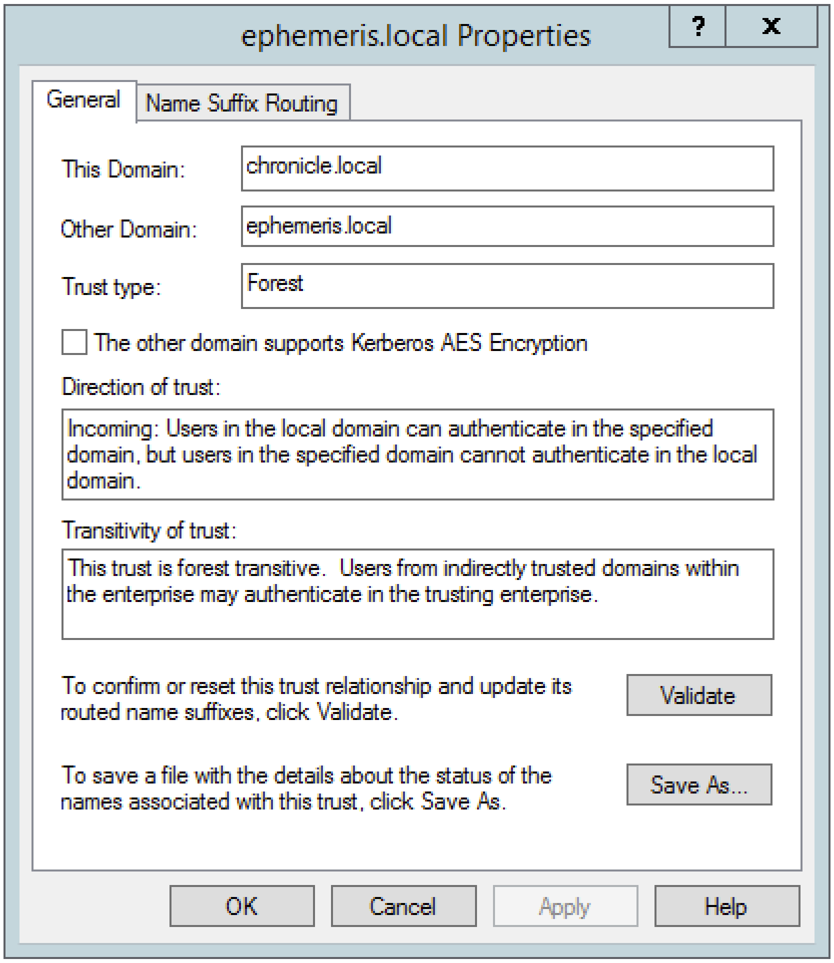
Domains trusted by this domain (outgoing trusts):

| Domain Name | Trust Type | Transitive |
|---|---|---|
| lambda.local | Forest | Yes |

Domains that trust this domain (incoming trusts):

| Domain Name | Trust Type | Transitive |
|---|---|---|
| ephemeris.local | Forest | Yes |

In the example above, `ephemeris.local` is supported.



ephemeris.local Properties

This Domain: chronicle.local

Other Domain: ephemeris.local

Trust type: Forest

□ The other domain supports Kerberos AES Encryption

Direction of trust:

Incoming: Users in the local domain can authenticate in the specified domain, but users in the specified domain cannot authenticate in the local domain.

Transitivity of trust:

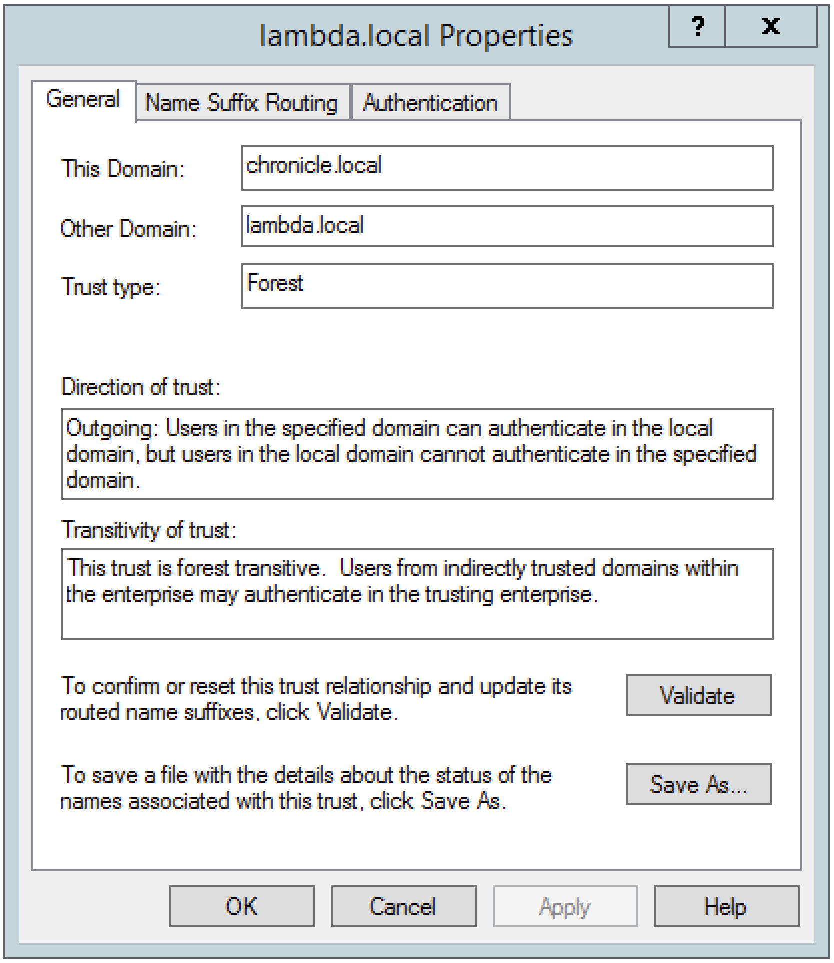
This trust is forest transitive. Users from indirectly trusted domains within the enterprise may authenticate in the trusting enterprise.

To confirm or reset this trust relationship and update its routed name suffixes, click Validate.

To save a file with the details about the status of the names associated with this trust, click Save As.

It is supported because it is a one-way incoming trust.

In the example below, `lambda.local` is not supported because it is configured as a one-way outgoing trust.



lambda.local Properties

This Domain: chronicle.local

Other Domain: lambda.local

Trust type: Forest

Direction of trust:

Outgoing: Users in the specified domain can authenticate in the local domain, but users in the local domain cannot authenticate in the specified domain.

Transitivity of trust:

This trust is forest transitive. Users from indirectly trusted domains within the enterprise may authenticate in the trusting enterprise.

To confirm or reset this trust relationship and update its routed name suffixes, click Validate.

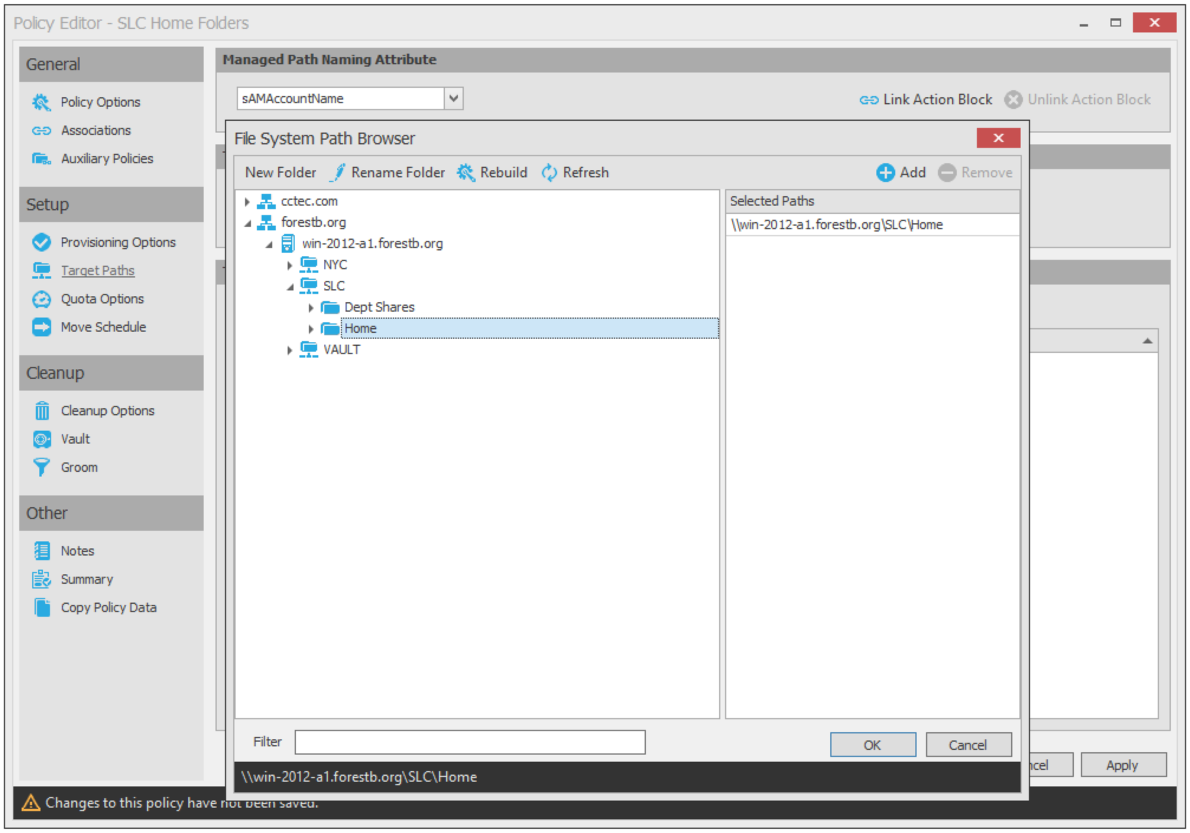
To save a file with the details about the status of the names associated with this trust, click Save As.

## Cross-Forest Data Management

After you have established a trust relationship, you can manage data in a secondary forest. The User and Group objects must reside in the primary forest, but these objects’ data can be managed in the secondary forest’s network file system.

For example, a User Home Folder policy assigned to User objects in Forest A can be set to a target path in Forest B. Similarly, data residing in the file system of Forest A can me moved, copied, or vaulted to Forest B through an operation.

*Figure 13-30 Target Path on a Secondary Forest*



Managed Path Naming Attribute

sAMAccountName

Selected Paths

\\win-2012-a1.forestb.org\SLC\Home

\\win-2012-a1.forestb.org\SLC\Home

Changes to this policy have not been saved.

## 13.1.15 Scope

Rather than burdening the Storage Manager 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 Chapter 4, "Configure the Event Monitor Scope," on page 27. For a complete discussion of the Scope feature, including Include and Exclude behaviors, see Appendix G, "Event Monitor Scope," on page 359.

## 13.1.16 Agents

Agents perform copying, moving, grooming, and vaulting through directives from the Engine. Storage Manager determines which Agent to use based on the target destination of the data or via proxy configuration.

For optimum performance, Agents should be installed on all servers with storage managed by Storage Manager. Agents run as a native 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 a 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 *Micro Focus Storage Manager 5.2 for Active Directory Installation Guide*.

## Deleting an Agent

Within SMAdmin, you can delete a deauthorized Agent. Only deauthorized Agents can be deleted. If you want to remove an Agent, you must deauthorize it first.

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

## Proxy Agents

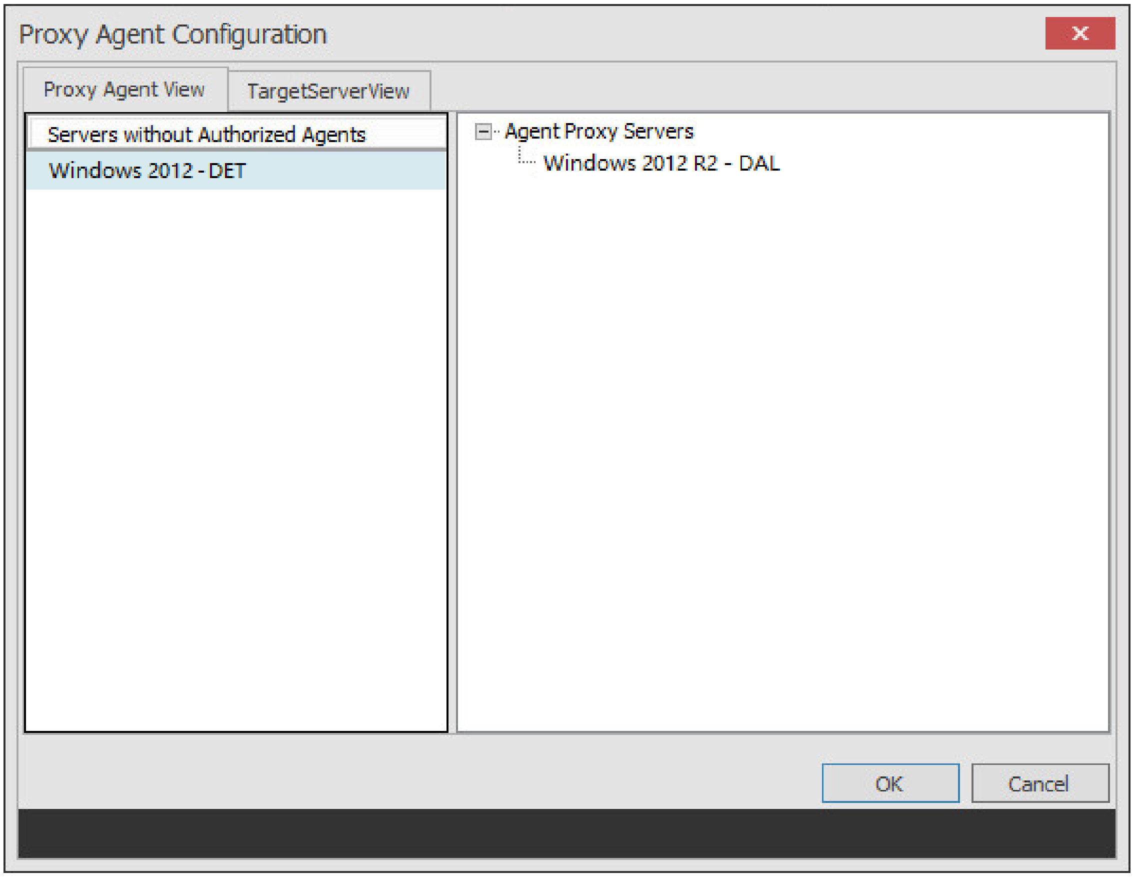
For storage resources that do not or cannot host an Agent, for example a NAS (Network Attached Storage) device, Storage Manager can utilize an Agent running on another server to perform the copying, moving, grooming, and vaulting on the server or NAS device. In this type of scenario, the Agent is serving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

A Proxy Agent can also be set up to reduce the workload on the Engine. For example, a Proxy Agent can be configured for a server on one side of a WAN environment to move data from one server to another on the same side of the WAN link. This keeps the data from crossing the WAN link only to cross back again.

### Configuring an Agent to be a Proxy Agent

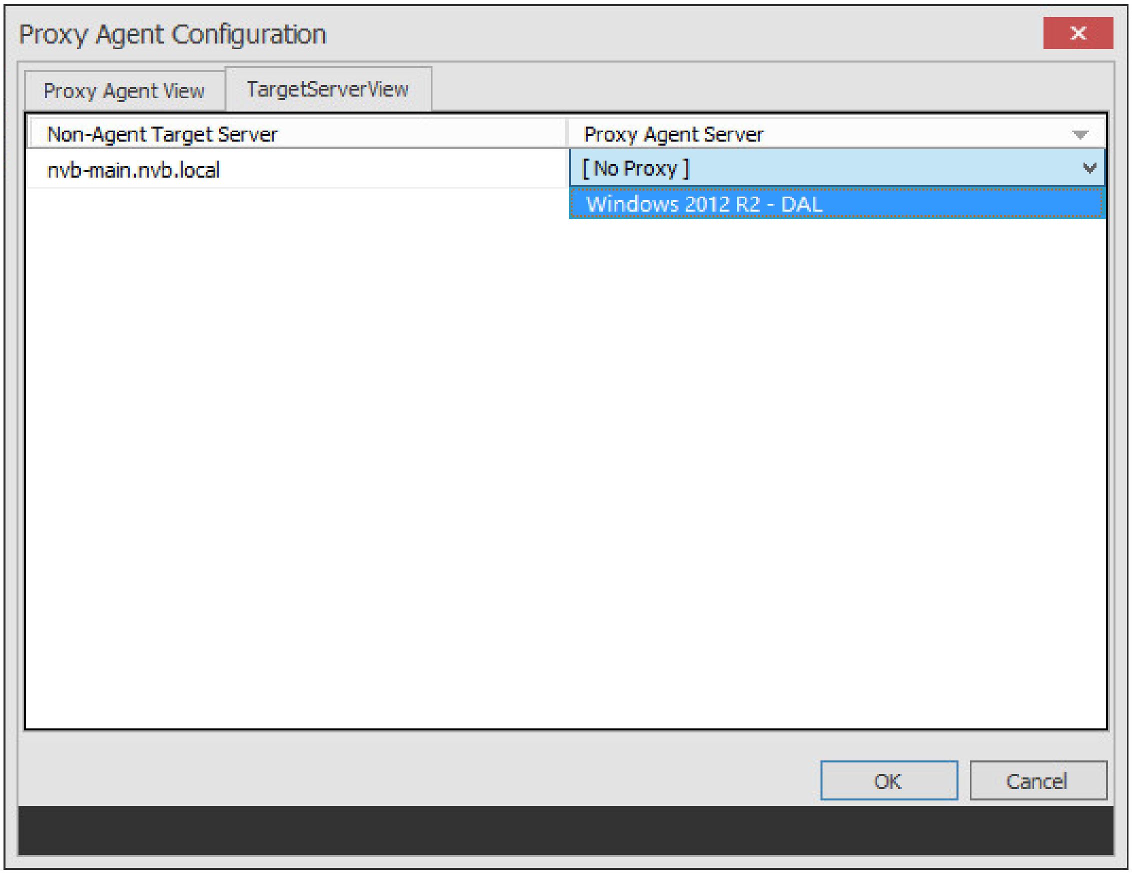
1. In SMAdmin, click the **Home** tab.
2. Click **Agents**.
3. Select the Agent you want to authorize to be a Proxy Agent and click **Proxy**.

   The left side of the Proxy Agent Configuration dialog box shows the list of servers without Agents installed. The right side shows the servers with Agents installed. In the example below, the Agent on Windows 2012 R2 - DAL could be set up to be the Proxy Agent for the Windows 2012 - DET server.



4 Click the **Target Server View** tab.

5 From the drop-down list, select the Agent server you want to serve as the Proxy Agent for the server on the left.



| Non-Agent Target Server | Proxy Agent Server |
|---|---|
| nvb-main.nvb.local | [ No Proxy ]<br>Windows 2012 R2 - DAL |

6 Click **OK** to save and close the proxy setting association.

## 13.1.17 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 native 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 in Authorizing the Event Monitor in the *Micro Focus Storage Manager 5.2 for Active Directory Installation Guide*.

### Deleting an Event Monitor

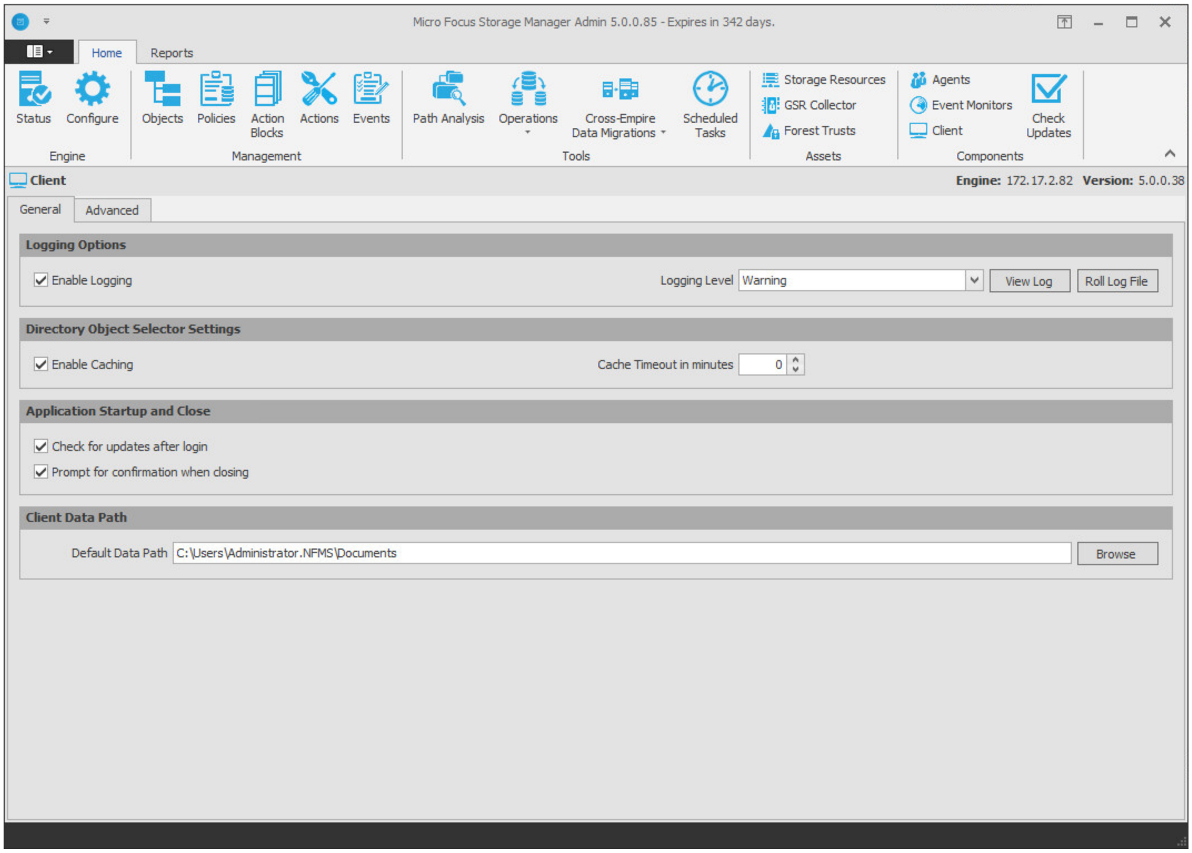
Within SMAdmin, you can delete a deauthorized Event Monitor. Only deauthorized Event Monitors can be deleted. If you want to remove an Event Monitor, you must deauthorize it first.

## 13.1.18 Client

This page lets you configure various settings within SMAdmin.

An overview of settings specific to the **General** tab follows the graphic.

*Figure 13-31 The General Tab of the Client Page*



Micro Focus Storage Manager Admin 5.0.0.85 - Expires in 342 days.

Client — Engine: 172.17.2.82 Version: 5.0.0.38

**Logging Options**

☑ Enable Logging — Logging Level: Warning

**Directory Object Selector Settings**

☑ Enable Caching — Cache Timeout in minutes: 0

**Application Startup and Close**

☑ Check for updates after login

☑ Prompt for confirmation when closing

**Client Data Path**

Default Data Path: C:\Users\Administrator.NFMS\Documents

**Enable Logging:** Selecting this check box enables logging the operations of SMAdmin and lets you specify the logging level and whether to roll the log or close the old log and start a new log.

**Logging Level:** This drop-down menu lets you select the classification of entry you want logged.

**View Log:** Clicking this button opens the log file.

**Roll Log File:** Clicking this button discontinues entries in the current log file and begins a new log file.

**Enable Caching:** Selecting this check box enables SMAdmin 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.

**Check for Updates after Login:** Selecting this check box allows SMAdmin to notify you of the availability of newer Micro Focus Storage Manager components.

**Check for Confirmation When Closing:** Selecting this check box prompts you with a confirmation of your choice when you close SMAdmin.

**Default Data Path:** This field specifies the location where all exported reports are stored. Fro example, if you were to export a Consistency Check report as a CSV or HTML file, it would be saved in this location.

**NOTE:** As stated on the Advanced tab page, the configuration settings on this page should be adjusted only under the direction of a Micro Focus Support representative during a support instance.

### 13.1.19 Check Updates

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

## 13.2 Reports Tab

The **Reports** tab provides the ability to generate and access various management reports, and Cross-Empire Data Management reports, Engine runtime reports, as well as view statistical information.

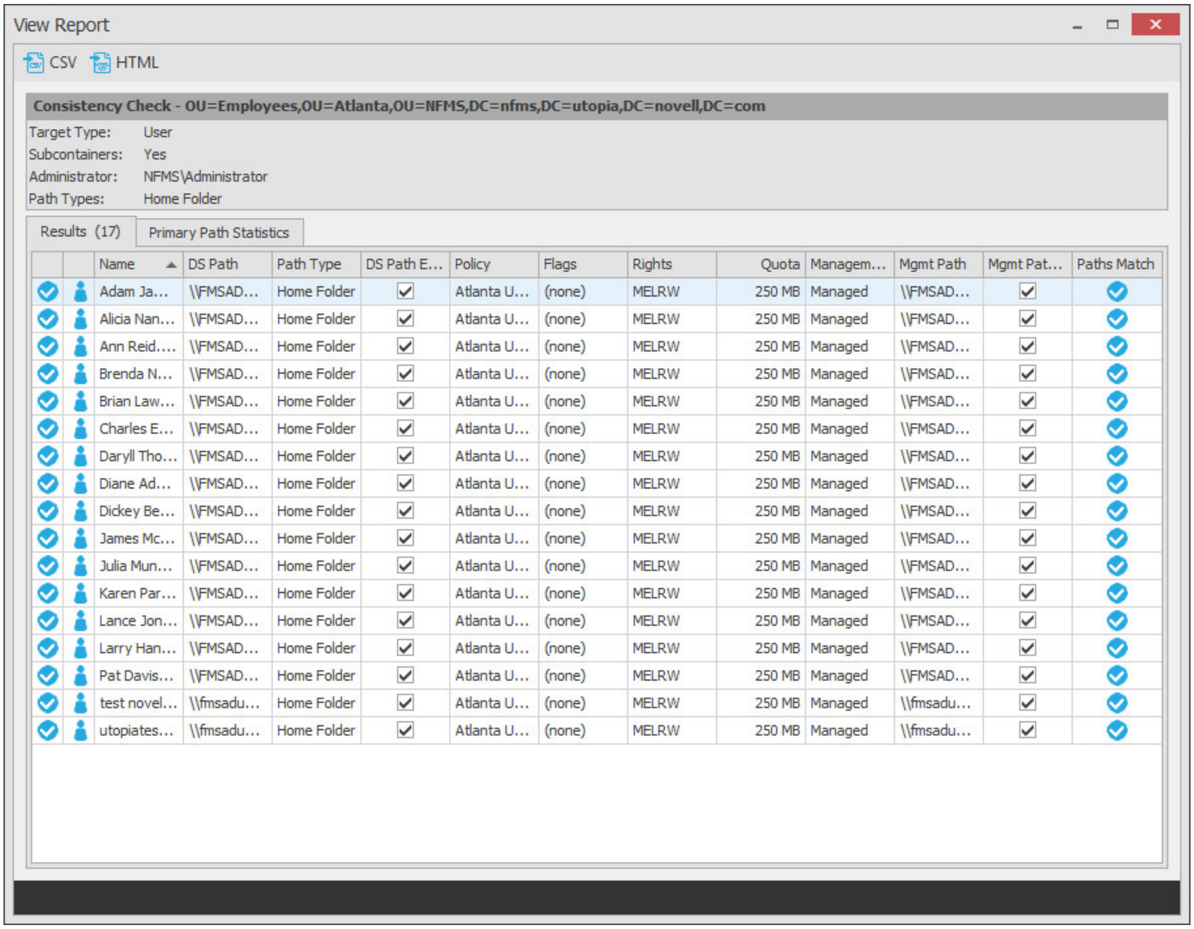
- Section 13.2.1, “Consistency Check,” on page 315
- Section 13.2.2, “Actions,” on page 317
- Section 13.2.3, “GSR Anomaly,” on page 318
- Section 13.2.4, “Completed Data Migration,” on page 324
- Section 13.2.5, “Preview Source Path,” on page 325
- Section 13.2.6, “Runtime Config,” on page 326
- Section 13.2.7, “Policy Paths,” on page 327
- Section 13.2.8, “Global,” on page 328
- Section 13.2.9, “Configuration,” on page 329
- Section 13.2.10, “Reports,” on page 329

### 13.2.1 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.

*Figure 13-32 Consistency Check Report*



**Consistency Check - OU=Employees,OU=Atlanta,OU=NFMS,DC=nfms,DC=utopia,DC=novell,DC=com**

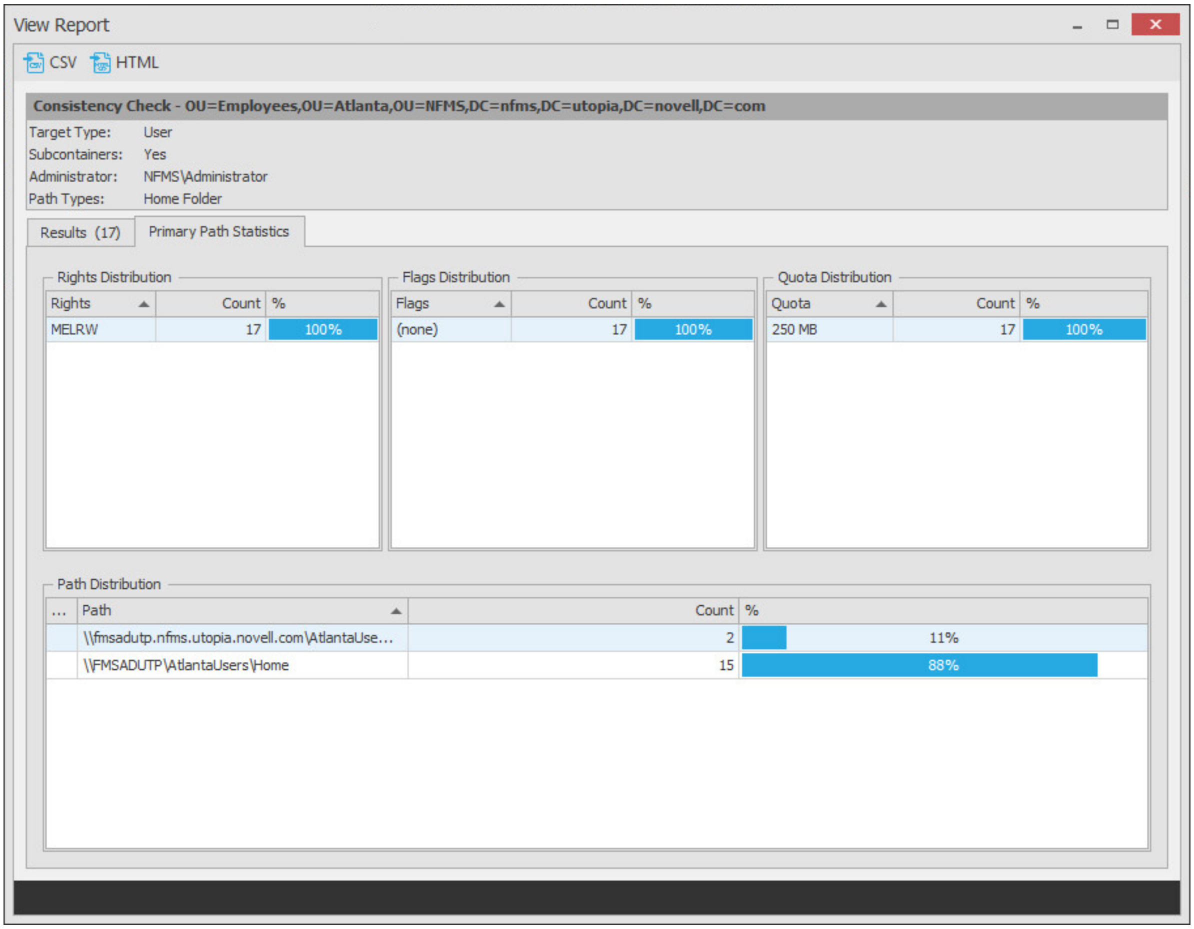
Target Type: User
Subcontainers: Yes
Administrator: NFMS\Administrator
Path Types: Home Folder

| | | Name | DS Path | Path Type | DS Path E... | Policy | Flags | Rights | Quota | Managem... | Mgmt Path | Mgmt Pat... | Paths Match |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ✓ | 👤 | Adam Ja... | \\FMSAD... | Home Folder | ☑ | Atlanta U... | (none) | MELRW | 250 MB | Managed | \\FMSAD... | ☑ | ✓ |
| ✓ | 👤 | Alicia Nan... | \\FMSAD... | Home Folder | ☑ | Atlanta U... | (none) | MELRW | 250 MB | Managed | \\FMSAD... | ☑ | ✓ |
| ✓ | 👤 | Ann Reid.... | \\FMSAD... | Home Folder | ☑ | Atlanta U... | (none) | MELRW | 250 MB | Managed | \\FMSAD... | ☑ | ✓ |
| ✓ | 👤 | Brenda N... | \\FMSAD... | Home Folder | ☑ | Atlanta U... | (none) | MELRW | 250 MB | Managed | \\FMSAD... | ☑ | ✓ |
| ✓ | 👤 | Brian Law... | \\FMSAD... | Home Folder | ☑ | Atlanta U... | (none) | MELRW | 250 MB | Managed | \\FMSAD... | ☑ | ✓ |
| ✓ | 👤 | Charles E... | \\FMSAD... | Home Folder | ☑ | Atlanta U... | (none) | MELRW | 250 MB | Managed | \\FMSAD... | ☑ | ✓ |
| ✓ | 👤 | Daryll Tho... | \\FMSAD... | Home Folder | ☑ | Atlanta U... | (none) | MELRW | 250 MB | Managed | \\FMSAD... | ☑ | ✓ |
| ✓ | 👤 | Diane Ad... | \\FMSAD... | Home Folder | ☑ | Atlanta U... | (none) | MELRW | 250 MB | Managed | \\FMSAD... | ☑ | ✓ |
| ✓ | 👤 | Dickey Be... | \\FMSAD... | Home Folder | ☑ | Atlanta U... | (none) | MELRW | 250 MB | Managed | \\FMSAD... | ☑ | ✓ |
| ✓ | 👤 | James Mc... | \\FMSAD... | Home Folder | ☑ | Atlanta U... | (none) | MELRW | 250 MB | Managed | \\FMSAD... | ☑ | ✓ |
| ✓ | 👤 | Julia Mun... | \\FMSAD... | Home Folder | ☑ | Atlanta U... | (none) | MELRW | 250 MB | Managed | \\FMSAD... | ☑ | ✓ |
| ✓ | 👤 | Karen Par... | \\FMSAD... | Home Folder | ☑ | Atlanta U... | (none) | MELRW | 250 MB | Managed | \\FMSAD... | ☑ | ✓ |
| ✓ | 👤 | Lance Jon... | \\FMSAD... | Home Folder | ☑ | Atlanta U... | (none) | MELRW | 250 MB | Managed | \\FMSAD... | ☑ | ✓ |
| ✓ | 👤 | Larry Han... | \\FMSAD... | Home Folder | ☑ | Atlanta U... | (none) | MELRW | 250 MB | Managed | \\FMSAD... | ☑ | ✓ |
| ✓ | 👤 | Pat Davis... | \\FMSAD... | Home Folder | ☑ | Atlanta U... | (none) | MELRW | 250 MB | Managed | \\FMSAD... | ☑ | ✓ |
| ✓ | 👤 | test novel... | \\fmsadu... | Home Folder | ☑ | Atlanta U... | (none) | MELRW | 250 MB | Managed | \\fmsadu... | ☑ | ✓ |
| ✓ | 👤 | utopiates... | \\fmsadu... | Home Folder | ☑ | Atlanta U... | (none) | MELRW | 250 MB | Managed | \\fmsadu... | ☑ | ✓ |

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

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

*Figure 13-33 Primary Statistics in a Consistency Check Report*



Consistency Check - OU=Employees,OU=Atlanta,OU=NFMS,DC=nfms,DC=utopia,DC=novell,DC=com

| | |
|---|---|
| Target Type: | User |
| Subcontainers: | Yes |
| Administrator: | NFMS\Administrator |
| Path Types: | Home Folder |

Rights Distribution

| Rights | Count | % |
|---|---|---|
| MELRW | 17 | 100% |

Flags Distribution

| Flags | Count | % |
|---|---|---|
| (none) | 17 | 100% |

Quota Distribution

| Quota | Count | % |
|---|---|---|
| 250 MB | 17 | 100% |

Path Distribution

| ... | Path | Count | % |
|---|---|---|---|
| | \\fmsadutp.nfms.utopia.novell.com\AtlantaUse... | 2 | 11% |
| | \\FMSADUTP\AtlantaUsers\Home | 15 | 88% |

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.

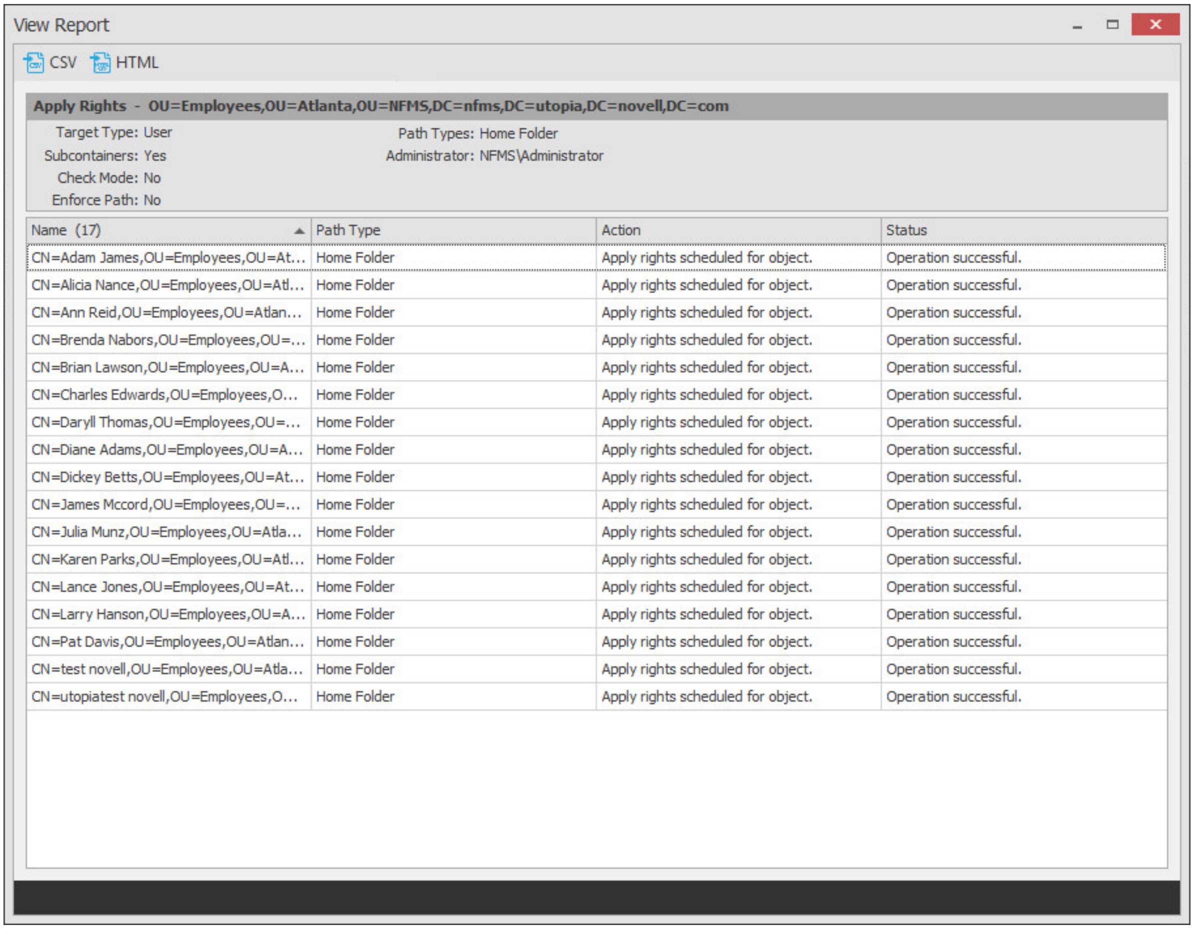
For more information on Consistency Check Reports, see Section 5.3, “Running Consistency Check Reports on Existing Storage,” on page 35 and Section 5.10, “Performing a Consistency Check,” on page 45.

## 13.2.2 Actions

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.

***Figure 13-34*** *Action Report*



**Apply Rights - OU=Employees,OU=Atlanta,OU=NFMS,DC=nfms,DC=utopia,DC=novell,DC=com**

Target Type: User
Subcontainers: Yes
Check Mode: No
Enforce Path: No
Path Types: Home Folder
Administrator: NFMS\Administrator

| Name (17) | Path Type | Action | Status |
|---|---|---|---|
| CN=Adam James,OU=Employees,OU=At… | Home Folder | Apply rights scheduled for object. | Operation successful. |
| CN=Alicia Nance,OU=Employees,OU=Atl… | Home Folder | Apply rights scheduled for object. | Operation successful. |
| CN=Ann Reid,OU=Employees,OU=Atlan… | Home Folder | Apply rights scheduled for object. | Operation successful. |
| CN=Brenda Nabors,OU=Employees,OU=… | Home Folder | Apply rights scheduled for object. | Operation successful. |
| CN=Brian Lawson,OU=Employees,OU=A… | Home Folder | Apply rights scheduled for object. | Operation successful. |
| CN=Charles Edwards,OU=Employees,O… | Home Folder | Apply rights scheduled for object. | Operation successful. |
| CN=Daryll Thomas,OU=Employees,OU=… | Home Folder | Apply rights scheduled for object. | Operation successful. |
| CN=Diane Adams,OU=Employees,OU=A… | Home Folder | Apply rights scheduled for object. | Operation successful. |
| CN=Dickey Betts,OU=Employees,OU=At… | Home Folder | Apply rights scheduled for object. | Operation successful. |
| CN=James Mccord,OU=Employees,OU=… | Home Folder | Apply rights scheduled for object. | Operation successful. |
| CN=Julia Munz,OU=Employees,OU=Atla… | Home Folder | Apply rights scheduled for object. | Operation successful. |
| CN=Karen Parks,OU=Employees,OU=Atl… | Home Folder | Apply rights scheduled for object. | Operation successful. |
| CN=Lance Jones,OU=Employees,OU=At… | Home Folder | Apply rights scheduled for object. | Operation successful. |
| CN=Larry Hanson,OU=Employees,OU=A… | Home Folder | Apply rights scheduled for object. | Operation successful. |
| CN=Pat Davis,OU=Employees,OU=Atlan… | Home Folder | Apply rights scheduled for object. | Operation successful. |
| CN=test novell,OU=Employees,OU=Atla… | Home Folder | Apply rights scheduled for object. | Operation successful. |
| CN=utopiatest novell,OU=Employees,O… | Home Folder | Apply rights scheduled for object. | Operation successful. |

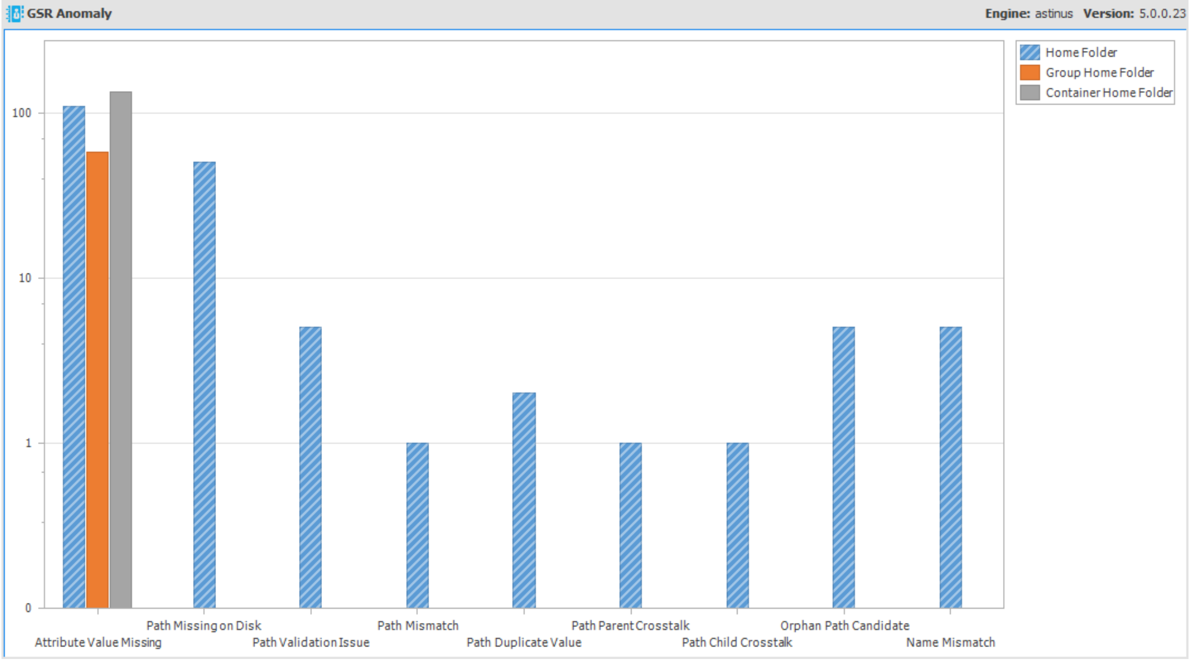
To export an Action report, double-click a report listing to access the View Report dialog box, and then in the upper-left corner of the dialog box, click either the **CSV** or **HTML** icons.

## 13.2.3 GSR Anomaly

- "Attribute Value Missing" on page 319
- "Path Missing on Disk" on page 320
- "Path Validation Issue" on page 321
- "Name Mismatch" on page 322
- "Path Duplicate Value" on page 322
- "Path Parent Crosstalk" on page 323
- "Path Child Crosstalk" on page 323
- "Orphan Path Candidate" on page 324

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 Storage Manager to bring storage under management by policy. Anomaly data will be produced for each object and path type specified in the GSR Collector configuration.

*Figure 13-35 GSR Anomaly Analysis*



To see further detail about a specific anomaly report, single-click on the column.

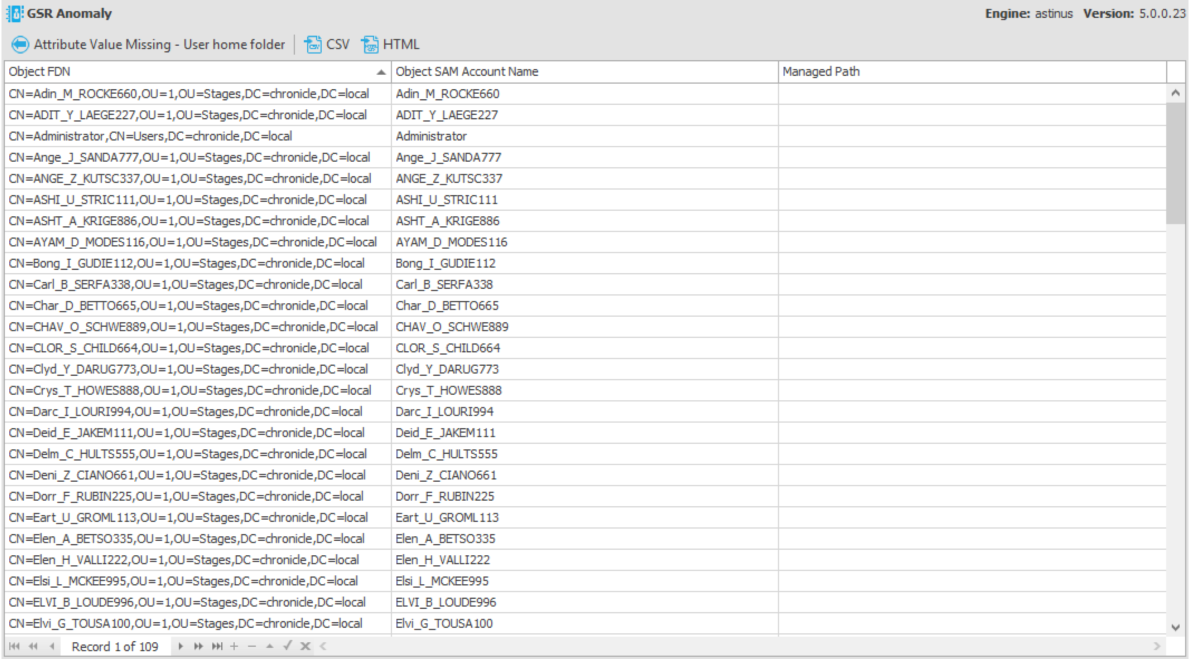
A detailed summary of each of the GSR Anomaly reports follows.

## 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.

Figure 13-36 on page 320 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 Storage Manager. 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.

***Figure 13-36*** *Attribute Value Missing*



GSR Anomaly
Engine: astinus Version: 5.0.0.23
Attribute Value Missing - User home folder
CSV
HTML

| Object FDN | Object SAM Account Name | Managed Path |
|---|---|---|
| CN=Adin_M_ROCKE660,OU=1,OU=Stages,DC=chronicle,DC=local | Adin_M_ROCKE660 | |
| CN=ADIT_Y_LAEGE227,OU=1,OU=Stages,DC=chronicle,DC=local | ADIT_Y_LAEGE227 | |
| CN=Administrator,CN=Users,DC=chronicle,DC=local | Administrator | |
| CN=Ange_J_SANDA777,OU=1,OU=Stages,DC=chronicle,DC=local | Ange_J_SANDA777 | |
| CN=ANGE_Z_KUTSC337,OU=1,OU=Stages,DC=chronicle,DC=local | ANGE_Z_KUTSC337 | |
| CN=ASHI_U_STRIC111,OU=1,OU=Stages,DC=chronicle,DC=local | ASHI_U_STRIC111 | |
| CN=ASHT_A_KRIGE886,OU=1,OU=Stages,DC=chronicle,DC=local | ASHT_A_KRIGE886 | |
| CN=AYAM_D_MODES116,OU=1,OU=Stages,DC=chronicle,DC=local | AYAM_D_MODES116 | |
| CN=Bong_I_GUDIE112,OU=1,OU=Stages,DC=chronicle,DC=local | Bong_I_GUDIE112 | |
| CN=Carl_B_SERFA338,OU=1,OU=Stages,DC=chronicle,DC=local | Carl_B_SERFA338 | |
| CN=Char_D_BETTO665,OU=1,OU=Stages,DC=chronicle,DC=local | Char_D_BETTO665 | |
| CN=CHAV_O_SCHWE889,OU=1,OU=Stages,DC=chronicle,DC=local | CHAV_O_SCHWE889 | |
| CN=CLOR_S_CHILD664,OU=1,OU=Stages,DC=chronicle,DC=local | CLOR_S_CHILD664 | |
| CN=Clyd_Y_DARUG773,OU=1,OU=Stages,DC=chronicle,DC=local | Clyd_Y_DARUG773 | |
| CN=Crys_T_HOWES888,OU=1,OU=Stages,DC=chronicle,DC=local | Crys_T_HOWES888 | |
| CN=Darc_I_LOURI994,OU=1,OU=Stages,DC=chronicle,DC=local | Darc_I_LOURI994 | |
| CN=Deid_E_JAKEM111,OU=1,OU=Stages,DC=chronicle,DC=local | Deid_E_JAKEM111 | |
| CN=Delm_C_HULTS555,OU=1,OU=Stages,DC=chronicle,DC=local | Delm_C_HULTS555 | |
| CN=Deni_Z_CIANO661,OU=1,OU=Stages,DC=chronicle,DC=local | Deni_Z_CIANO661 | |
| CN=Dorr_F_RUBIN225,OU=1,OU=Stages,DC=chronicle,DC=local | Dorr_F_RUBIN225 | |
| CN=Eart_U_GROML113,OU=1,OU=Stages,DC=chronicle,DC=local | Eart_U_GROML113 | |
| CN=Elen_A_BETSO335,OU=1,OU=Stages,DC=chronicle,DC=local | Elen_A_BETSO335 | |
| CN=Elen_H_VALLI222,OU=1,OU=Stages,DC=chronicle,DC=local | Elen_H_VALLI222 | |
| CN=Elsi_L_MCKEE995,OU=1,OU=Stages,DC=chronicle,DC=local | Elsi_L_MCKEE995 | |
| CN=ELVI_B_LOUDE996,OU=1,OU=Stages,DC=chronicle,DC=local | ELVI_B_LOUDE996 | |
| CN=Elvi_G_TOUSA100,OU=1,OU=Stages,DC=chronicle,DC=local | Elvi_G_TOUSA100 | |

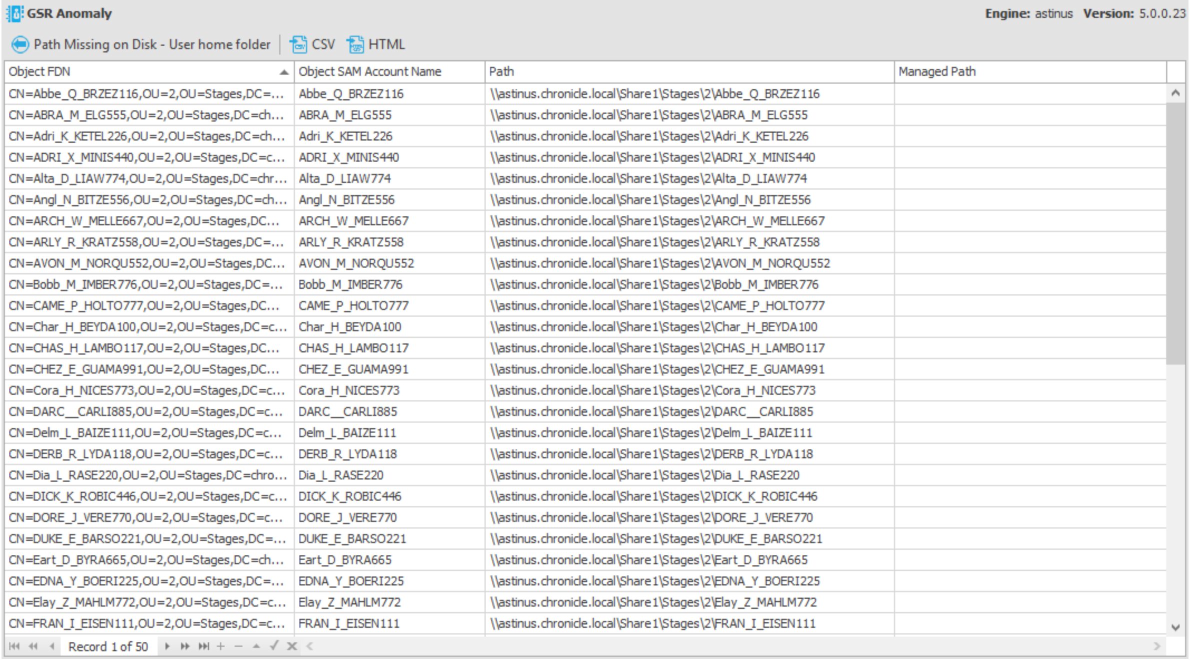
Record 1 of 109

## 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.

Figure 13-37 on page 321 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 Storage Manager. 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.

***Figure 13-37*** *Path Missing on Disk*


GSR Anomaly
Engine: astinus Version: 5.0.0.23
Path Missing on Disk - User home folder
CSV
HTML
Record 1 of 50

| Object FDN | Object SAM Account Name | Path | Managed Path |
|---|---|---|---|
| CN=Abbe_Q_BRZEZ116,OU=2,OU=Stages,DC=… | Abbe_Q_BRZEZ116 | \\astinus.chronicle.local\Share1\Stages\2\Abbe_Q_BRZEZ116 | |
| CN=ABRA_M_ELG555,OU=2,OU=Stages,DC=ch… | ABRA_M_ELG555 | \\astinus.chronicle.local\Share1\Stages\2\ABRA_M_ELG555 | |
| CN=Adri_K_KETEL226,OU=2,OU=Stages,DC=ch… | Adri_K_KETEL226 | \\astinus.chronicle.local\Share1\Stages\2\Adri_K_KETEL226 | |
| CN=ADRI_X_MINIS440,OU=2,OU=Stages,DC=c… | ADRI_X_MINIS440 | \\astinus.chronicle.local\Share1\Stages\2\ADRI_X_MINIS440 | |
| CN=Alta_D_LIAW774,OU=2,OU=Stages,DC=chr… | Alta_D_LIAW774 | \\astinus.chronicle.local\Share1\Stages\2\Alta_D_LIAW774 | |
| CN=Angl_N_BITZE556,OU=2,OU=Stages,DC=ch… | Angl_N_BITZE556 | \\astinus.chronicle.local\Share1\Stages\2\Angl_N_BITZE556 | |
| CN=ARCH_W_MELLE667,OU=2,OU=Stages,DC… | ARCH_W_MELLE667 | \\astinus.chronicle.local\Share1\Stages\2\ARCH_W_MELLE667 | |
| CN=ARLY_R_KRATZ558,OU=2,OU=Stages,DC=… | ARLY_R_KRATZ558 | \\astinus.chronicle.local\Share1\Stages\2\ARLY_R_KRATZ558 | |
| CN=AVON_M_NORQU552,OU=2,OU=Stages,DC… | AVON_M_NORQU552 | \\astinus.chronicle.local\Share1\Stages\2\AVON_M_NORQU552 | |
| CN=Bobb_M_IMBER776,OU=2,OU=Stages,DC=… | Bobb_M_IMBER776 | \\astinus.chronicle.local\Share1\Stages\2\Bobb_M_IMBER776 | |
| CN=CAME_P_HOLTO777,OU=2,OU=Stages,DC… | CAME_P_HOLTO777 | \\astinus.chronicle.local\Share1\Stages\2\CAME_P_HOLTO777 | |
| CN=Char_H_BEYDA100,OU=2,OU=Stages,DC=c… | Char_H_BEYDA100 | \\astinus.chronicle.local\Share1\Stages\2\Char_H_BEYDA100 | |
| CN=CHAS_H_LAMBO117,OU=2,OU=Stages,DC… | CHAS_H_LAMBO117 | \\astinus.chronicle.local\Share1\Stages\2\CHAS_H_LAMBO117 | |
| CN=CHEZ_E_GUAMA991,OU=2,OU=Stages,DC… | CHEZ_E_GUAMA991 | \\astinus.chronicle.local\Share1\Stages\2\CHEZ_E_GUAMA991 | |
| CN=Cora_H_NICES773,OU=2,OU=Stages,DC=c… | Cora_H_NICES773 | \\astinus.chronicle.local\Share1\Stages\2\Cora_H_NICES773 | |
| CN=DARC__CARLI885,OU=2,OU=Stages,DC=c… | DARC__CARLI885 | \\astinus.chronicle.local\Share1\Stages\2\DARC__CARLI885 | |
| CN=Delm_L_BAIZE111,OU=2,OU=Stages,DC=c… | Delm_L_BAIZE111 | \\astinus.chronicle.local\Share1\Stages\2\Delm_L_BAIZE111 | |
| CN=DERB_R_LYDA118,OU=2,OU=Stages,DC=c… | DERB_R_LYDA118 | \\astinus.chronicle.local\Share1\Stages\2\DERB_R_LYDA118 | |
| CN=Dia_L_RASE220,OU=2,OU=Stages,DC=chro… | Dia_L_RASE220 | \\astinus.chronicle.local\Share1\Stages\2\Dia_L_RASE220 | |
| CN=DICK_K_ROBIC446,OU=2,OU=Stages,DC=c… | DICK_K_ROBIC446 | \\astinus.chronicle.local\Share1\Stages\2\DICK_K_ROBIC446 | |
| CN=DORE_J_VERE770,OU=2,OU=Stages,DC=c… | DORE_J_VERE770 | \\astinus.chronicle.local\Share1\Stages\2\DORE_J_VERE770 | |
| CN=DUKE_E_BARSO221,OU=2,OU=Stages,DC=… | DUKE_E_BARSO221 | \\astinus.chronicle.local\Share1\Stages\2\DUKE_E_BARSO221 | |
| CN=Eart_D_BYRA665,OU=2,OU=Stages,DC=ch… | Eart_D_BYRA665 | \\astinus.chronicle.local\Share1\Stages\2\Eart_D_BYRA665 | |
| CN=EDNA_Y_BOERI225,OU=2,OU=Stages,DC=… | EDNA_Y_BOERI225 | \\astinus.chronicle.local\Share1\Stages\2\EDNA_Y_BOERI225 | |
| CN=Elay_Z_MAHLM772,OU=2,OU=Stages,DC=c… | Elay_Z_MAHLM772 | \\astinus.chronicle.local\Share1\Stages\2\Elay_Z_MAHLM772 | |
| CN=FRAN_I_EISEN111,OU=2,OU=Stages,DC=c… | FRAN_I_EISEN111 | \\astinus.chronicle.local\Share1\Stages\2\FRAN_I_EISEN111 | |

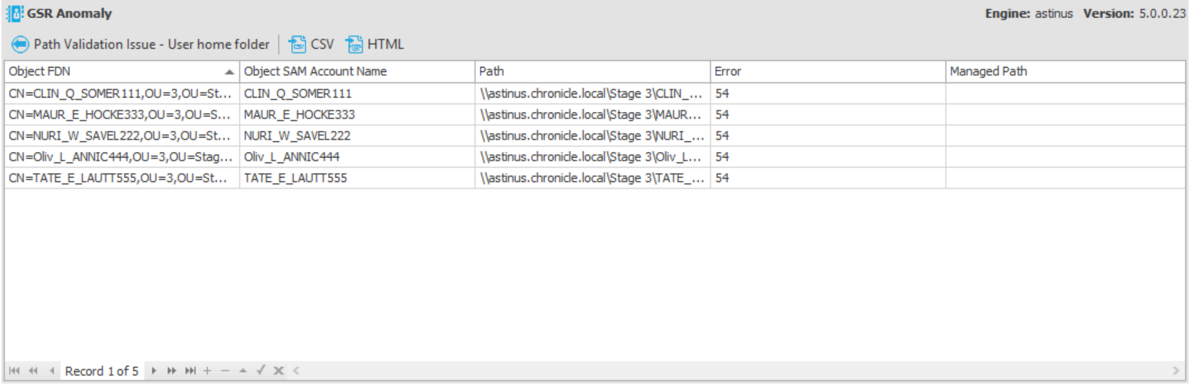
## Path Validation Issue

This Anomaly report indicates that there were errors when attempting to retrieve or verify the existence of the respective path attribute value (e.g. home folder).

Figure 13-38 on page 322 is an example of the Path Validation Issue 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 Storage Manager. These objects are reported because there was an error when trying to verify the existence of the path specified by their homeDirectory attribute. This report can be used to identify objects whose respective path attribute value no longer exists at the specified location or if the Engine has an issue communicating with the server or share on which the path is located. The symptoms can be:

- The share no longer exists.
- The server is down or no longer in commission.
- A permissions issue keeps Storage Manager from asking for the path.
- Some other connectivity issue exists.

*Figure 13-38* *Path Validation Issues*



**GSR Anomaly** **Engine:** astinus **Version:** 5.0.0.23

Path Validation Issue - User home folder | CSV | HTML

| Object FDN | Object SAM Account Name | Path | Error | Managed Path |
|---|---|---|---|---|
| CN=CLIN_Q_SOMER111,OU=3,OU=St... | CLIN_Q_SOMER111 | \\astinus.chronicle.local\Stage 3\CLIN_... | 54 | |
| CN=MAUR_E_HOCKE333,OU=3,OU=S... | MAUR_E_HOCKE333 | \\astinus.chronicle.local\Stage 3\MAUR... | 54 | |
| CN=NURI_W_SAVEL222,OU=3,OU=St... | NURI_W_SAVEL222 | \\astinus.chronicle.local\Stage 3\NURI_... | 54 | |
| CN=Oliv_L_ANNIC444,OU=3,OU=Stag... | Oliv_L_ANNIC444 | \\astinus.chronicle.local\Stage 3\Oliv_L... | 54 | |
| CN=TATE_E_LAUTT555,OU=3,OU=St... | TATE_E_LAUTT555 | \\astinus.chronicle.local\Stage 3\TATE_... | 54 | |

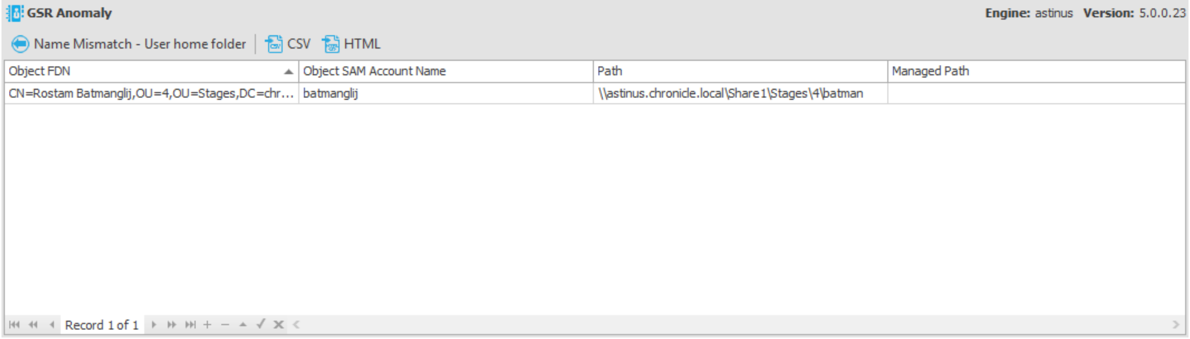
Record 1 of 5

## 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.

Figure 13-39 on page 322 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.

*Figure 13-39* *Name Mismatch*



**GSR Anomaly** **Engine:** astinus **Version:** 5.0.0.23

Name Mismatch - User home folder | CSV | HTML

| Object FDN | Object SAM Account Name | Path | Managed Path |
|---|---|---|---|
| CN=Rostam Batmanglij,OU=4,OU=Stages,DC=chr... | batmanglij | \\astinus.chronicle.local\Share1\Stages\4\batman | |

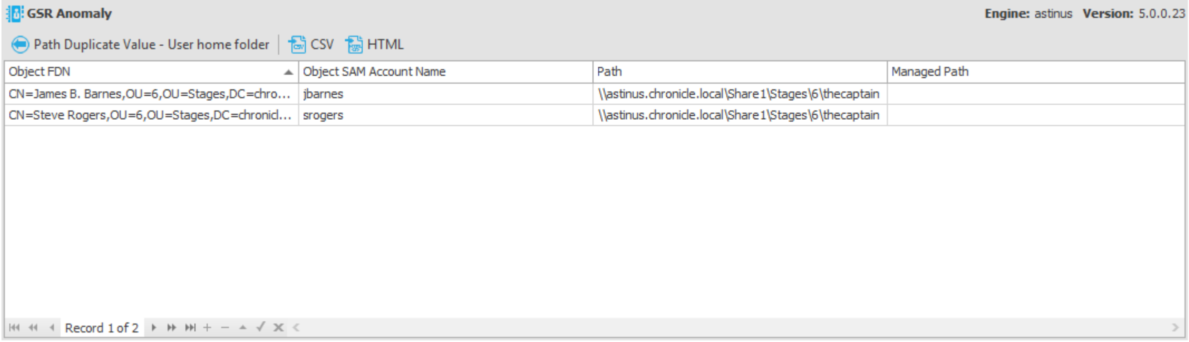
Record 1 of 1

## 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).

Figure 13-40 on page 323 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 Storage Manager. 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.

***Figure 13-40*** *Path Duplicate Value*


GSR Anomaly
Engine: astinus Version: 5.0.0.23
Path Duplicate Value - User home folder
CSV
HTML
Record 1 of 2

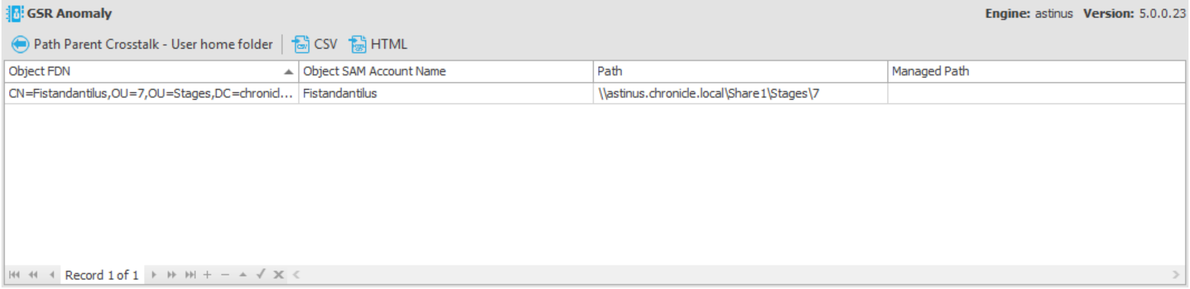
| Object FDN | Object SAM Account Name | Path | Managed Path |
|---|---|---|---|
| CN=James B. Barnes,OU=6,OU=Stages,DC=chro… | jbarnes | \\astinus.chronicle.local\Share1\Stages\6\thecaptain | |
| CN=Steve Rogers,OU=6,OU=Stages,DC=chronicl… | srogers | \\astinus.chronicle.local\Share1\Stages\6\thecaptain | |

## 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).

Figure 13-41 on page 323 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 Storage Manager. 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.

***Figure 13-41*** *Path Parent Crosstalk*


GSR Anomaly
Engine: astinus Version: 5.0.0.23
Path Parent Crosstalk - User home folder
CSV
HTML
Record 1 of 1

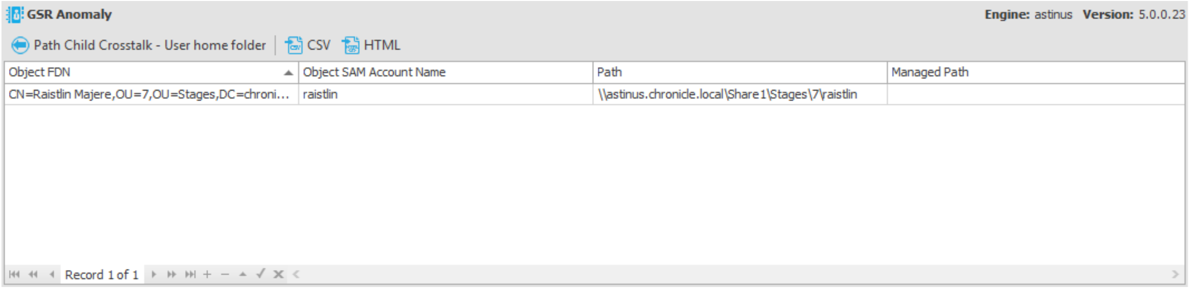
| Object FDN | Object SAM Account Name | Path | Managed Path |
|---|---|---|---|
| CN=Fistandantilus,OU=7,OU=Stages,DC=chronicl… | Fistandantilus | \\astinus.chronicle.local\Share1\Stages\7 | |

## 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).

Figure 13-42 on page 324 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 Storage Manager. 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.

*Figure 13-42 Path Child Crosstalk*


GSR Anomaly
Engine: astinus Version: 5.0.0.23
Path Child Crosstalk - User home folder
CSV
HTML
Record 1 of 1

| Object FDN | Object SAM Account Name | Path | Managed Path |
|---|---|---|---|
| CN=Raistlin Majere,OU=7,OU=Stages,DC=chroni… | raistlin | \\astinus.chronicle.local\Share1\Stages\7\raistlin | |

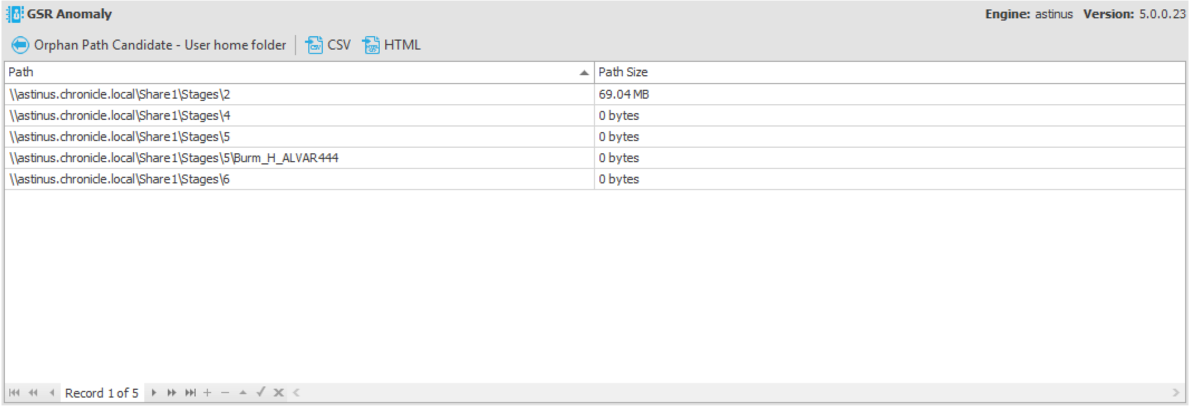
To see which object is a parent of this object's homeDirectory attribute value, see "Path Parent Crosstalk" on page 323.

## 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).

Figure 13-43 on page 324 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.

*Figure 13-43 Orphan Path Candidate*


GSR Anomaly
Engine: astinus Version: 5.0.0.23
Orphan Path Candidate - User home folder
CSV
HTML
Record 1 of 5

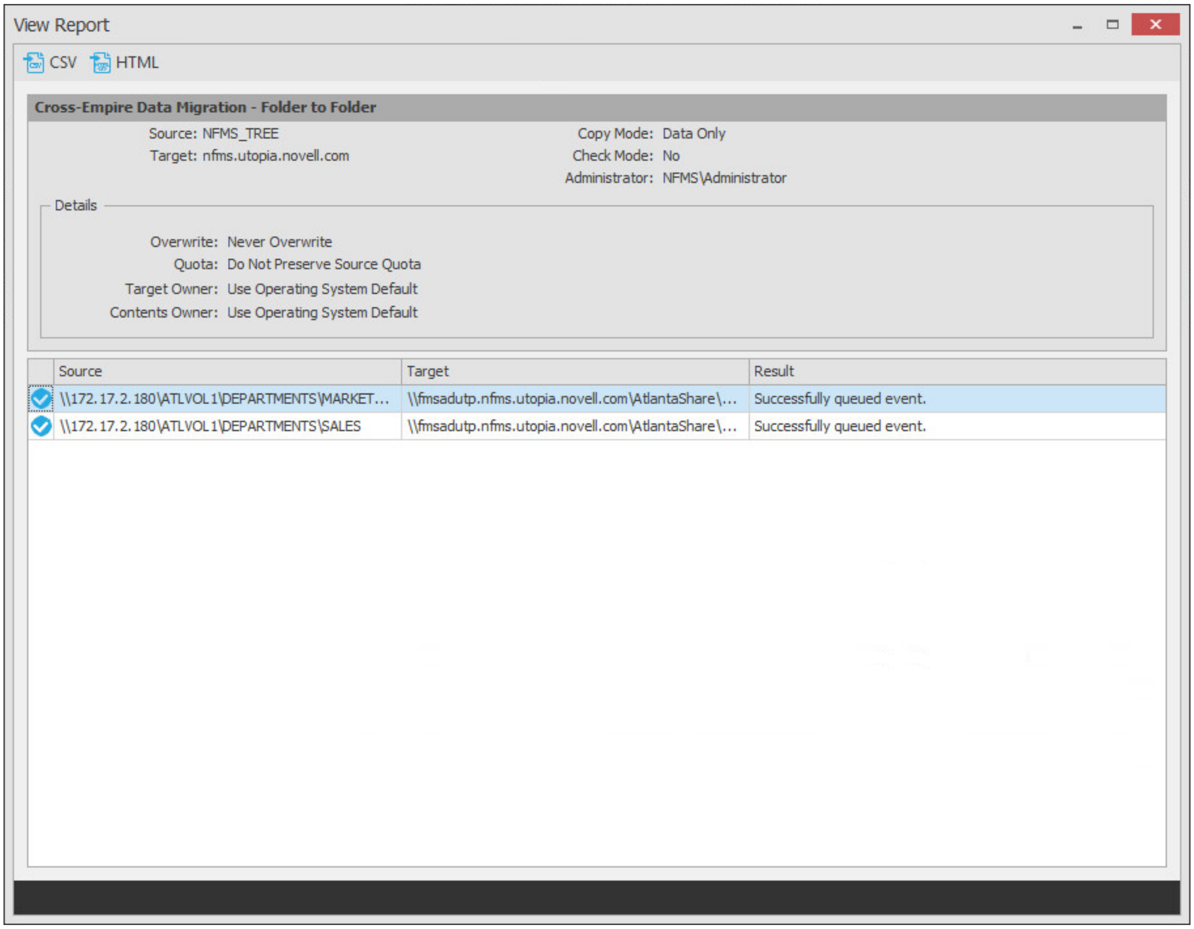
| Path | Path Size |
|---|---|
| \\astinus.chronicle.local\Share1\Stages\2 | 69.04 MB |
| \\astinus.chronicle.local\Share1\Stages\4 | 0 bytes |
| \\astinus.chronicle.local\Share1\Stages\5 | 0 bytes |
| \\astinus.chronicle.local\Share1\Stages\5\Burm_H_ALVAR444 | 0 bytes |
| \\astinus.chronicle.local\Share1\Stages\6 | 0 bytes |

# 13.2.4 Completed Data Migration

This page is used to access and export stored Completed Data Migration reports.

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

*Figure 13-44 Completed Data Migration Reports*



**Cross-Empire Data Migration - Folder to Folder**

Source: NFMS_TREE
Target: nfms.utopia.novell.com
Copy Mode: Data Only
Check Mode: No
Administrator: NFMS\Administrator

Details

Overwrite: Never Overwrite
Quota: Do Not Preserve Source Quota
Target Owner: Use Operating System Default
Contents Owner: Use Operating System Default

| | Source | Target | Result |
|---|---|---|---|
| ✓ | \\172.17.2.180\ATLVOL1\DEPARTMENTS\MARKET... | \\fmsadutp.nfms.utopia.novell.com\AtlantaShare\... | Successfully queued event. |
| ✓ | \\172.17.2.180\ATLVOL1\DEPARTMENTS\SALES | \\fmsadutp.nfms.utopia.novell.com\AtlantaShare\... | Successfully queued event. |

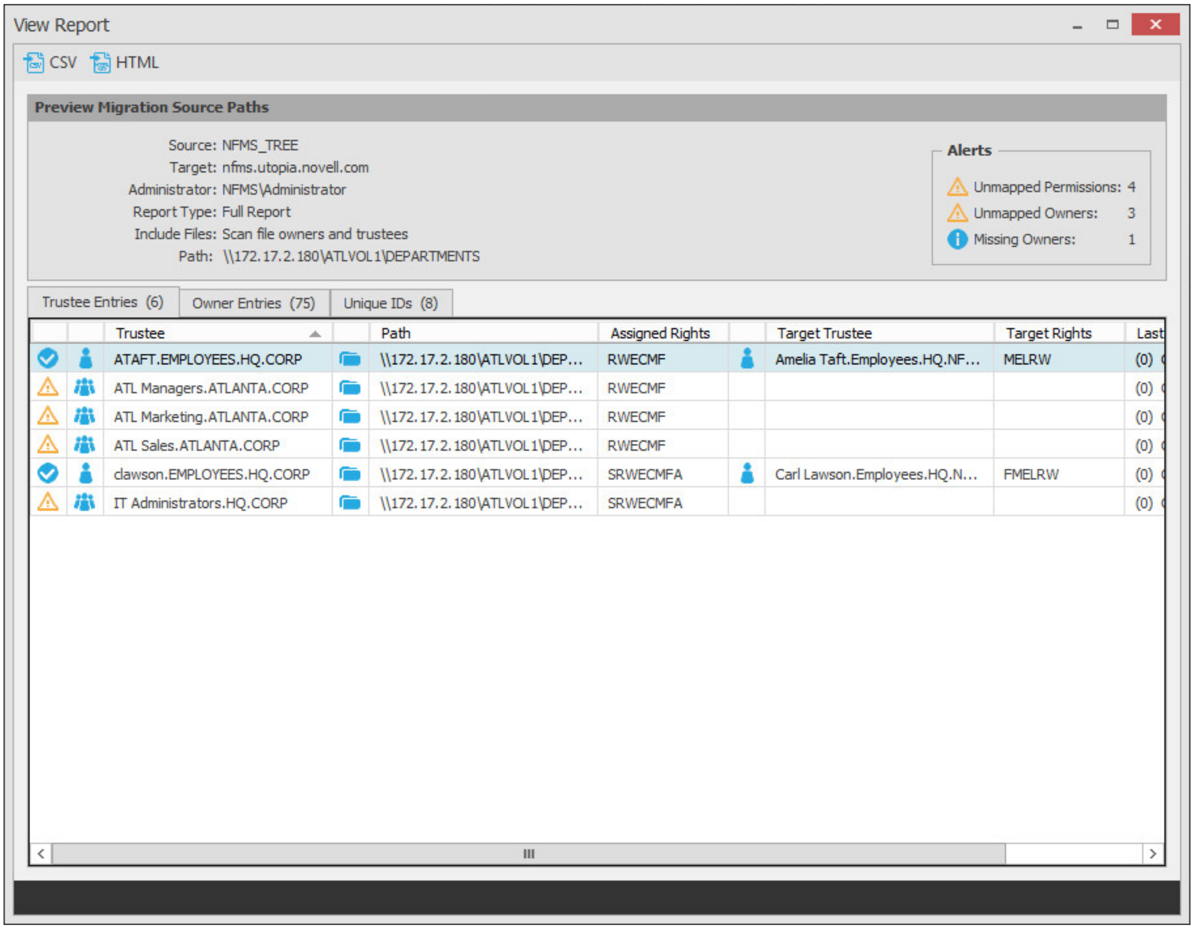
To export a Completed Cross-Empire Data Migration report, double-click a report listing to access the View Report dialog box, and then in the upper-left corner of the dialog box, click either the **CSV** or **HTML** icons.

## 13.2.5 Preview Source Path

This page is used to access and export stored Migration Preview reports. For more information of Migration Preview reports, see Section 10.5.7, “Generating a Migration Preview Report,” on page 145.

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

*Figure 13-45 Preview Source Path Report*



View Report

CSV HTML

**Preview Migration Source Paths**

Source: NFMS_TREE
Target: nfms.utopia.novell.com
Administrator: NFMS\Administrator
Report Type: Full Report
Include Files: Scan file owners and trustees
Path: \\172.17.2.180\ATLVOL1\DEPARTMENTS

**Alerts**

| | | |
|---|---|---|
| ⚠ | Unmapped Permissions: | 4 |
| ⚠ | Unmapped Owners: | 3 |
| ℹ | Missing Owners: | 1 |

Trustee Entries (6) | Owner Entries (75) | Unique IDs (8)

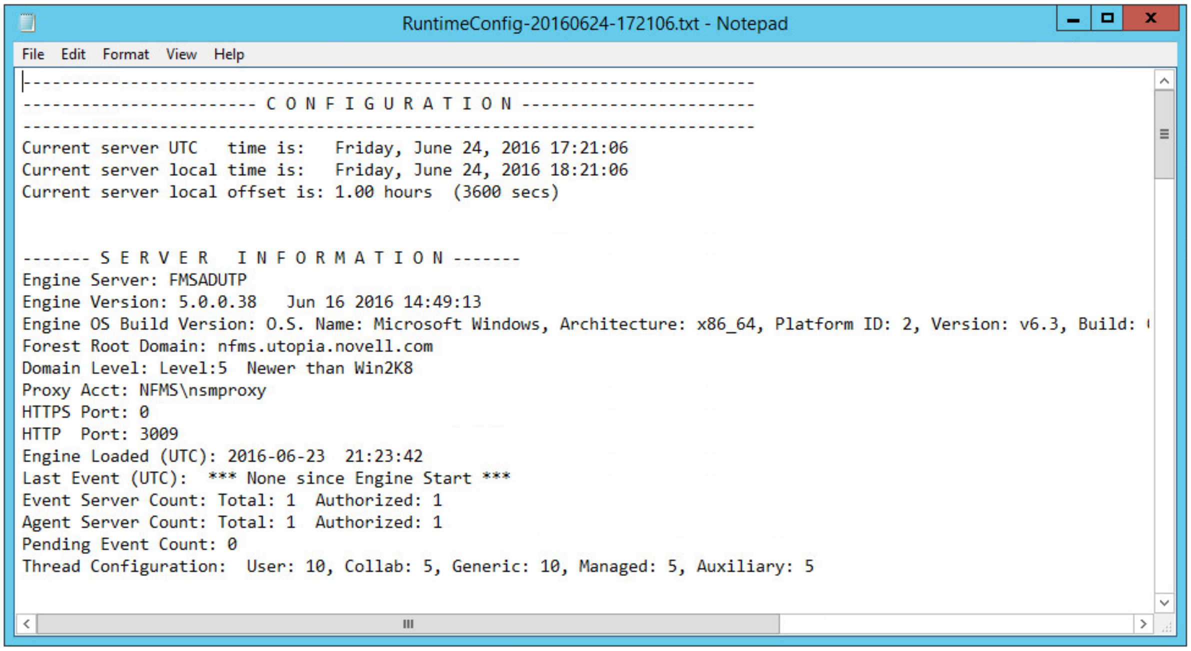
| | | Trustee | | Path | Assigned Rights | | Target Trustee | Target Rights | Last |
|---|---|---|---|---|---|---|---|---|---|
| ✓ | 👤 | ATAFT.EMPLOYEES.HQ.CORP | 📁 | \\172.17.2.180\ATLVOL1\DEP... | RWECMF | 👤 | Amelia Taft.Employees.HQ.NF... | MELRW | (0) |
| ⚠ | 👥 | ATL Managers.ATLANTA.CORP | 📁 | \\172.17.2.180\ATLVOL1\DEP... | RWECMF | | | | (0) |
| ⚠ | 👥 | ATL Marketing.ATLANTA.CORP | 📁 | \\172.17.2.180\ATLVOL1\DEP... | RWECMF | | | | (0) |
| ⚠ | 👥 | ATL Sales.ATLANTA.CORP | 📁 | \\172.17.2.180\ATLVOL1\DEP... | RWECMF | | | | (0) |
| ✓ | 👤 | clawson.EMPLOYEES.HQ.CORP | 📁 | \\172.17.2.180\ATLVOL1\DEP... | SRWECMFA | 👤 | Carl Lawson.Employees.HQ.N... | FMELRW | (0) |
| ⚠ | 👥 | IT Administrators.HQ.CORP | 📁 | \\172.17.2.180\ATLVOL1\DEP... | SRWECMFA | | | | (0) |

To export a Preview Source Path 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.

## 13.2.6 Runtime Config

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

*Figure 13-46 Sample Runtime Config Report*


RuntimeConfig-20160624-172106.txt - Notepad
File Edit Format View Help

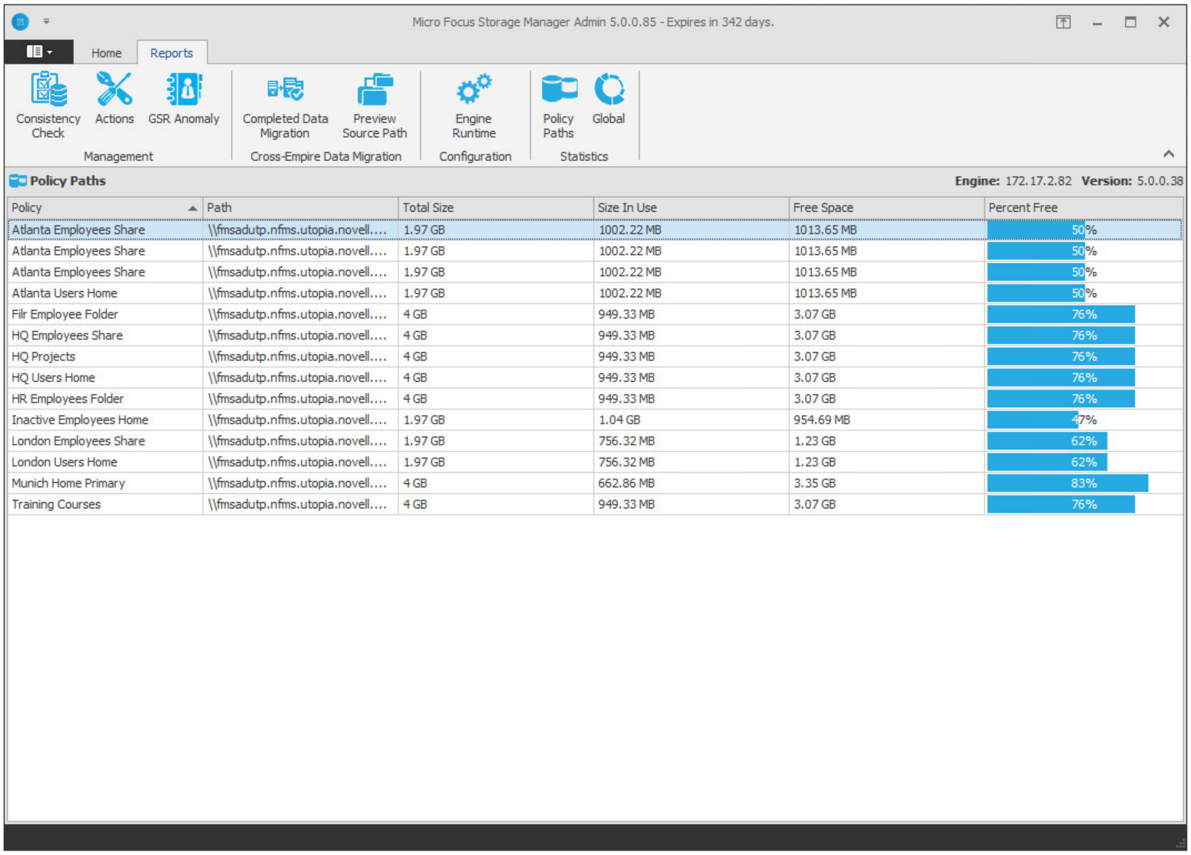
```
----------------------------------------------------------------------------
----------------------- C O N F I G U R A T I O N -----------------------
----------------------------------------------------------------------------
Current server UTC   time is:   Friday, June 24, 2016 17:21:06
Current server local time is:   Friday, June 24, 2016 18:21:06
Current server local offset is: 1.00 hours  (3600 secs)


------- S E R V E R   I N F O R M A T I O N -------
Engine Server: FMSADUTP
Engine Version: 5.0.0.38   Jun 16 2016 14:49:13
Engine OS Build Version: O.S. Name: Microsoft Windows, Architecture: x86_64, Platform ID: 2, Version: v6.3, Build: (
Forest Root Domain: nfms.utopia.novell.com
Domain Level: Level:5  Newer than Win2K8
Proxy Acct: NFMS\nsmproxy
HTTPS Port: 0
HTTP  Port: 3009
Engine Loaded (UTC): 2016-06-23  21:23:42
Last Event (UTC):  *** None since Engine Start ***
Event Server Count: Total: 1  Authorized: 1
Agent Server Count: Total: 1  Authorized: 1
Pending Event Count: 0
Thread Configuration:  User: 10, Collab: 5, Generic: 10, Managed: 5, Auxiliary: 5
```

## 13.2.7 Policy Paths

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

*Figure 13-47 Policy Paths Report*



**Engine:** 172.17.2.82 **Version:** 5.0.0.38

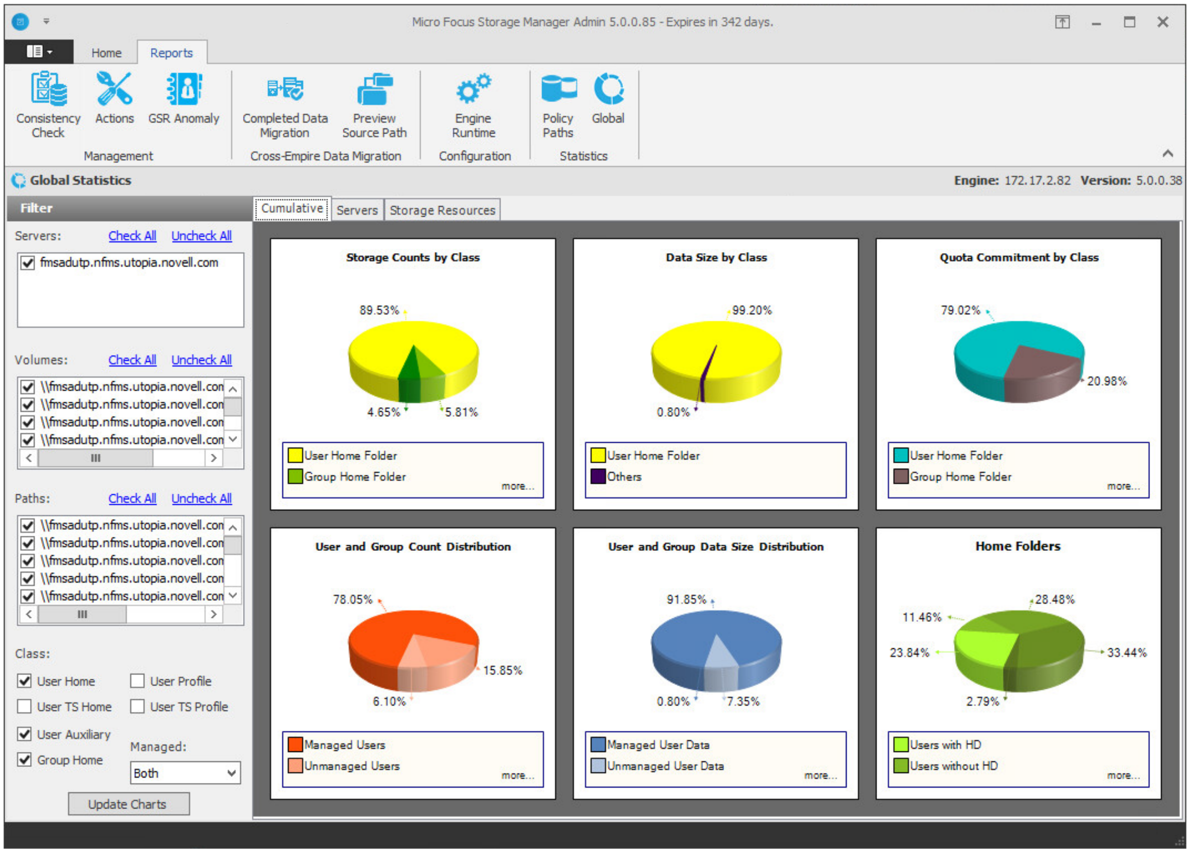
| Policy | Path | Total Size | Size In Use | Free Space | Percent Free |
|---|---|---|---|---|---|
| Atlanta Employees Share | \\fmsadutp.nfms.utopia.novell.... | 1.97 GB | 1002.22 MB | 1013.65 MB | 50% |
| Atlanta Employees Share | \\fmsadutp.nfms.utopia.novell.... | 1.97 GB | 1002.22 MB | 1013.65 MB | 50% |
| Atlanta Employees Share | \\fmsadutp.nfms.utopia.novell.... | 1.97 GB | 1002.22 MB | 1013.65 MB | 50% |
| Atlanta Users Home | \\fmsadutp.nfms.utopia.novell.... | 1.97 GB | 1002.22 MB | 1013.65 MB | 50% |
| Filr Employee Folder | \\fmsadutp.nfms.utopia.novell.... | 4 GB | 949.33 MB | 3.07 GB | 76% |
| HQ Employees Share | \\fmsadutp.nfms.utopia.novell.... | 4 GB | 949.33 MB | 3.07 GB | 76% |
| HQ Projects | \\fmsadutp.nfms.utopia.novell.... | 4 GB | 949.33 MB | 3.07 GB | 76% |
| HQ Users Home | \\fmsadutp.nfms.utopia.novell.... | 4 GB | 949.33 MB | 3.07 GB | 76% |
| HR Employees Folder | \\fmsadutp.nfms.utopia.novell.... | 4 GB | 949.33 MB | 3.07 GB | 76% |
| Inactive Employees Home | \\fmsadutp.nfms.utopia.novell.... | 1.97 GB | 1.04 GB | 954.69 MB | 47% |
| London Employees Share | \\fmsadutp.nfms.utopia.novell.... | 1.97 GB | 756.32 MB | 1.23 GB | 62% |
| London Users Home | \\fmsadutp.nfms.utopia.novell.... | 1.97 GB | 756.32 MB | 1.23 GB | 62% |
| Munich Home Primary | \\fmsadutp.nfms.utopia.novell.... | 4 GB | 662.86 MB | 3.35 GB | 83% |
| Training Courses | \\fmsadutp.nfms.utopia.novell.... | 4 GB | 949.33 MB | 3.07 GB | 76% |

## 13.2.8 Global

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

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

***Figure 13-48*** *Global Report*



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

## 13.2.9 Configuration

Use the Configuration page to establish the Work Log reporting database settings in SMAdmin.

Work Log reporting is an optional feature introduced in Storage Manager 5.2. The Work Log database is hosted on a CouchDB database deployed either on-site or in the cloud. Once the CouchDB database has been deployed, you specify the CouchDB host system parameters in the fields on this page.

For procedures on how to set these parameters, see Section 12.3, “Establishing the Work Log Database Settings in SMAdmin,” on page 233.

## 13.2.10 Reports

Use the Reports page to build Work Log Reports.

Work Log reporting is an optional feature introduced in Storage Manager 5.2. Work Log reports are built 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.

For an overview of each of the report types, along with procedures for building Work Log reports, see Section 12.4, “Building Work Log Reports,” on page 234.

# A SMAdmin and Database Communication

## A.1 Transition to Direct Database Access

Historically, SMAdmin has used XML-RPC to perform all interactions with the Engine. Beginning with the release of version 4.1, Storage Manager is slowly transitioning away from that model and moving towards directly accessing certain resources where direct access makes more sense. Direct access to the SQL Server database now takes place for the following:

- Events
- Event Properties
- Object History
- GSR Collector Data

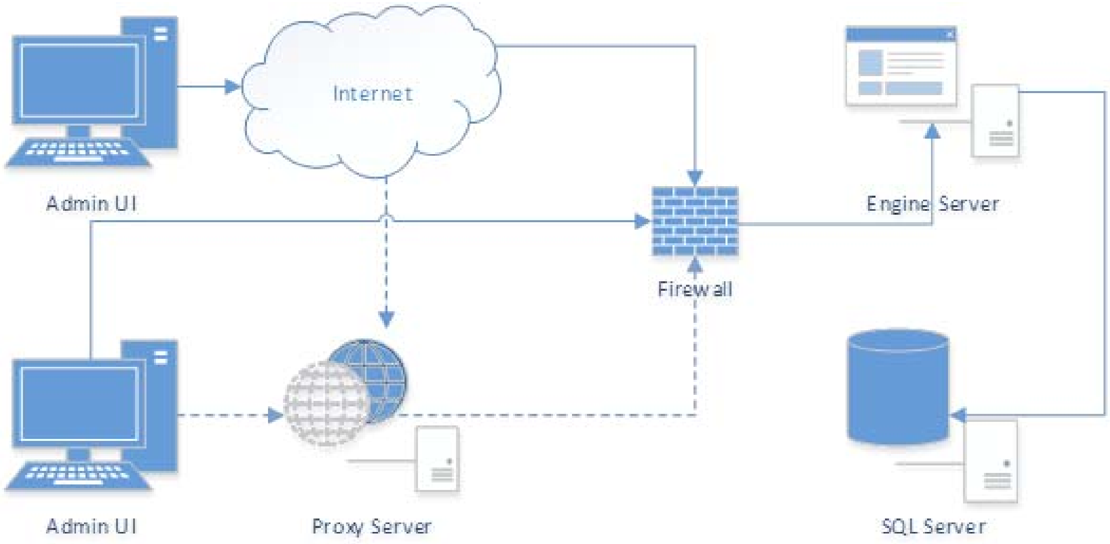
This change in behavior means that SMAdmin will no longer only be subject to firewall rules regarding the Engine's listening port (3009 is the default). Instead, greater consideration needs to be given to the environment and how SMAdmin will be used to access it. This also introduces a breaking change with interaction between SMAdmin and the Engine.

**NOTE:** SMAdmin can authenticate only to a matching version of the Engine. For example, SMAdmin 5.2 can only authenticate to a matching Storage Manager 5.2 Engine.

### A.1.1 Legacy Environment

In a legacy configuration, the SMAdmin would communicate with the Engine server host directly over a WAN, over the internet, and perhaps through a proxy. In all cases, communication would ultimately go through a firewall to the Engine server host.

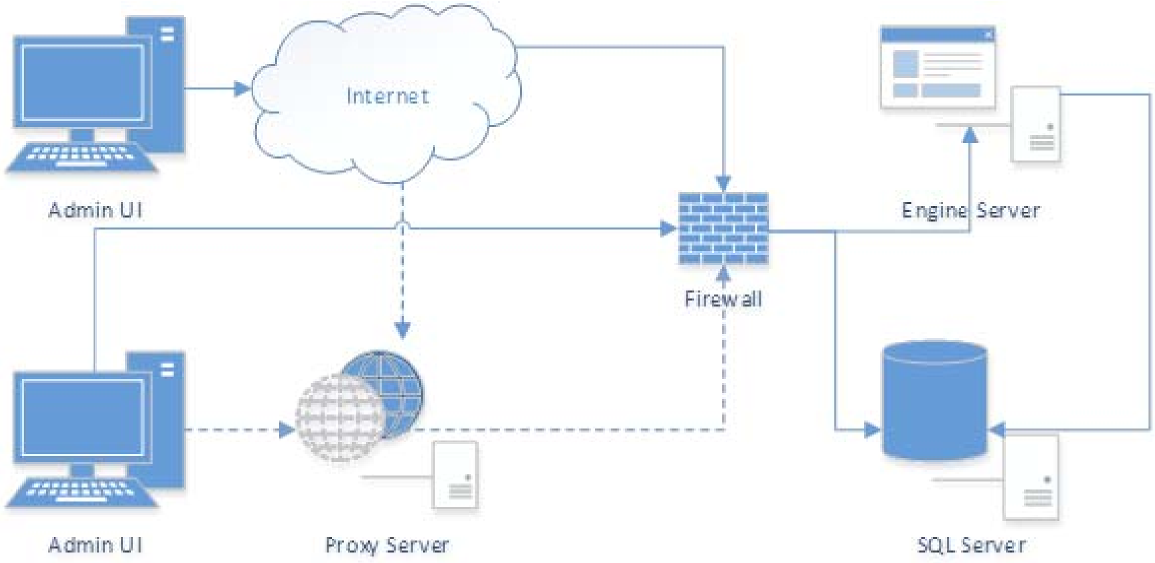
*Figure A-1 Legacy Environment*



## A.1.2 New Environment

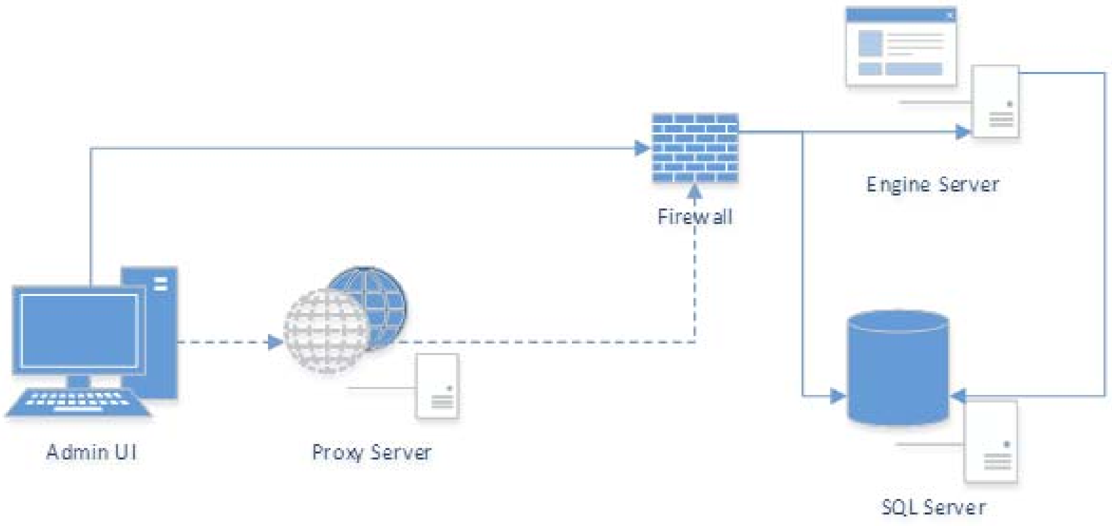
Given the new requirements of direct database access, SMAdmin will now need to have access to the SQL Server host through a proxy server or firewall, depending on the your requirements. If access to the SQL Server host is allowed over the internet, the following represents a likely scenario:

*Figure A-2 New Environment*



If access to the SQL Server host is restricted to the LAN/WAN, the following represents a likely scenario. In this case, it might be necessary for an administrator to connect through a VPN to access and manage the product. In most cases, it will no longer possible to manage the product outside of the corporate network.

*Figure A-3 New Environment Restricted to LAN/WAN*



## A.1.3 Database Host Address

In previous releases, the Database Host Address in the Engine's configuration was able to be set to the localhost address of 127.0.0.1. Now that SMAdmin is reliant upon direct access to the SQL Server database, this is no longer supported. A valid DNS FQDN or IP address is required.

This value needs to be updated and saved by using the Engine's Database Configuration Wizard. If the Database Host Address is set to 127.0.0.1, the Wizard will attempt to convert it to a DNS FQDN and correct this value automatically on an upgrade. During a new installation, the DNS FQDN of the local machine will be used by default.

# A.2 SMAdmin Database User Setup

SMAdmin uses a specific database user created during the Engine's Database Configuration Wizard. Because it is a product managed login, the administrator is not given the opportunity to change the name of the login or database user that are created. They are blindly managed by the Engine's Database Configuration Wizard.

The name of the login and database user created is `fsfui`. The login is created with `CHECK_EXPIRATION=OFF` to disable password expiration. However, enforcement of password policy still applies because `CHECK_POLICY=OFF` is not specified. Therefore, normal Windows password policy mechanisms still apply. For further details, see: https://msdn.microsoft.com/en-us/library/ms161959.aspx

To satisfy the default Windows password complexity, a random password with a minimum length of 20 characters will be generated. For example, a password will be produced that looks something like the following:

```
!#U)F^KV!ED?UWRJ0DN&
```

The login and database user are created in the Database Connection step of the Engine's Database Configuration Wizard. Each time the Database Configuration Wizard successfully moves beyond the Database Connection step, the login's password is set to a new value and `CHECK_EXPIRATION=OFF` is set.

If there's an existing login and database user by fsfui, Storage Manager will attempt to use it. The following properties on the login will cause the Wizard to return an error:

- Login type is not SQL Login
- Login is disabled
- Login is locked
- Login is expired

If the login's password is set to expire, a warning will be reported informing the administrator that they should consider disabling password expiration for the login.

The database user is added to the `db_datareader` database-level role of the target database. For further details, see: https://msdn.microsoft.com/en-us/library/ms189121.aspx.

## A.2.1 SMAdmin Database Access

SMAdmin performs database access once it has received the database credentials from the Engine after a user has successfully performed a logon. It will perform direct database queries for the following:

- Events
- Event Properties
- Object History
- GSR Collector Data

# B Security Specifications

This section provides details on configuring your Windows firewall to accommodate the components of Storage Manager for Active Directory. It also specifies the Local Security Authority (LSA) rights and privileges that must be set.

- Section B.1, “Windows Firewall Requirements,” on page 335
- Section B.2, “LSA Rights and Privileges,” on page 336
- Section B.3, “ProxyRights Group Permissions,” on page 337
- Section B.4, “Windows Clustering via Proxy Agents,” on page 337
- Section B.5, “Considerations for NAS Devices,” on page 338

## B.1 Windows Firewall Requirements

The Windows Firewall has different default configurations on Windows Server 2012 R2, Windows Server 2012, and Windows Server 2008 R2.

In most cases, the Storage Manager installation enables the following firewall settings. In the rare circumstances where it does not, you will have to establish these manually.

- The Engine must be permitted to make outbound connections.
- The Engine must be able to listen on ports 3008 and 3009. These are the default port choices that are presented during the installation and configuration. If you use different values, you must adjust the firewall port exceptions to match the port values.
- The Agent must be permitted to make outbound connections.
- The Agent must be able to listen on ports 3010 and 3011. These are the default port choices that are presented during the installation and configuration. If you use different values, you must adjust the firewall port exceptions to match the port values.
- The Event Monitor component must be permitted to make outbound connections.
- On each 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.`

On servers running Windows Server 2008, the firewall settings are applicable to each of three different categories of network interfaces that are identified based upon their IP address range (public IP addresses versus private IP addresses) and whether or not the computer is a member of a domain. Depending upon the specific environment where Storage Manager for Active Directory is installed, the firewall might need to have these exceptions enabled in one or more of the following categories:

- Domain
- Private
- Public

# B.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 Storage Manager for Active Directory to function properly.

| Right/Privilege | Applies to | Security Principal |
|---|---|---|
| "Access this computer from the network" [SeNetworkLogonRight] | All systems hosting folder shares that are to be managed by the product; all domain controllers in all managed domains; all systems on which the Engine, Agent or Event Monitor components are installed. | "ProxyRights" |
| "Create a token object" [SeCreateTokenPrivilege],<br>"Impersonate a client after authentication"<br>[SeImpersonatePrivilege],<br>"Act as part of the operating system"<br>[SeTcbPrivilege] | All systems on which the Engine, Agent or Event Monitor components are installed. | "ProxyRights" |
| "Back up files and directories"<br>[SeBackupPrivilege],<br>"Bypass traverse checking"<br>[SeChangeNotifyPrivilege],<br>"Manage auditing and security log"<br>[SeSecurityPrivilege],<br>"Restore files and directories"<br>[SeRestorePrivilege],<br>"Take ownership of files or other objects"<br>[SeTakeOwnershipPrivilege] | All systems hosting folder shares that are to be managed by the product; all domain controllers in all managed domains; all systems on which the Engine, Agent or Event Monitor components are installed. | "ProxyRights" |
| "Create symbolic links"<br>[SeCreateSymbolicLinkPrivilege]<br>Only on Vista / Win2K8 & newer. | All systems hosting folder shares that are to be managed by the product; all domain controllers in all managed domains; all systems on which the Engine, Agent or Event Monitor components are installed. | "ProxyRights" |
| "Log on as a batch job"<br>[SeBatchLogonRight] | The system on which the Engine component is installed. | The administrative user whose credentials are used to log in to the Setup Wizard during configuration of the Engine. By default, the built-in SMAdministrators group is granted this right on all domain controllers and member servers. |

| Right/Privilege | Applies to | Security Principal |
|---|---|---|
| "Log on as a batch job"<br>[SeBatchLogonRight] | The system on which the Engine component is installed. | "Admins", File / Storage Reporting Users |

As indicated in the table above, installing any of the product components grants the appropriate rights and privileges on the server on which the component is installed. However, in certain situations, the security changes that are configured automatically during the installation process are not sufficient to meet all of the security requirements needed to monitor events and manage storage across an entire domain or multiple domains.

## B.3 ProxyRights Group Permissions

By default, whenever any of the components of Storage Manager for Active Directory are installed on a computer in a domain, the SMProxyRights universal security group is granted membership in that domain's Administrators built-in security group. This grants the product all of the necessary permissions to read and write attribute values on objects in the domain. This also eliminates the need for the **Synchronize directory service data** privilege to be granted to the SMProxyRights group on each domain controller in the domain.

**IMPORTANT:** If your organization's security policies do not allow for SMProxyRights to be a member of each domain's Administrators built-in security group in each managed domain, then you need to explicitly grant permissions and extend rights in Active Directory to SMProxyRights at the domain level of every managed domain. Please contact Micro Focus technical support for assistance when configuring these detailed permissions.

By default, whenever any of the components of Storage Manager for Active Directory are installed on a member server in a domain, SMProxyRights is granted membership in the built-in Administrators group on the member server.

On other servers in the domain that are hosting user or collaborative storage managed by Storage Manager for Active Directory, you must also grant SMProxyRights group membership in the built-in Administrators group. This is necessary because there are many storage management actions performed that require membership in this group regardless of the LSA privileges that the user has been granted—in particular, managing file shares and directory quotas.

Additionally, the other servers in the domain that are not hosting components, but are hosting user or collaborative storage, must have the rights and privileges described in the table above, along with Full Control share permissions. The easiest way of granting these rights and privileges is through Group Policy objects in Active Directory.

As explained in “Setting Rights and Privileges on Managed Storage” and of the *Micro Focus Storage Manager 5.2 for Active Directory Installation Guide*, you must grant Full Control sharing and security privileges to the SMProxyRights group for each share that Storage Manager for Active Directory will manage.

## B.4 Windows Clustering via Proxy Agents

Storage Manager for Active Directory supports clustering of Windows Server 2003 and later 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 SMProxyRights 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 SMProxyRights group for all shares that will be managed by Storage Manager for Active Directory.

# B.5 Considerations for NAS Devices

Storage Manager for Active Directory can manage storage on Network Attached Storage (NAS) devices through a Proxy Agent. Integration information for reporting on specific NAS device types is found below.

## B.5.1 EMC Celerra

For an EMC Celerra NAS device, configuration is similar to configuring a server in the domain to be managed by a Proxy Agent.

1. Join the NAS device to a domain where Storage Manager for Active Directory can manage from.
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 that are required to access the storage.
4. Grant the LSA rights and privileges to the proxy rights group, except the rights and privileges that don't exist on the EMC Celerra NAS device.

## B.5.2 EMC Isilon and Other NAS Devices

Perform the following steps to integrate an EMC Isilon device. You can use these same steps to see if other NAS devices integrate with Storage Manager for Active Directory.

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.

# C Distributed File System (DFS)

This section provides procedures for configuring the DFS namespaces to work with Storage Manager.

## C.1 Prerequisites

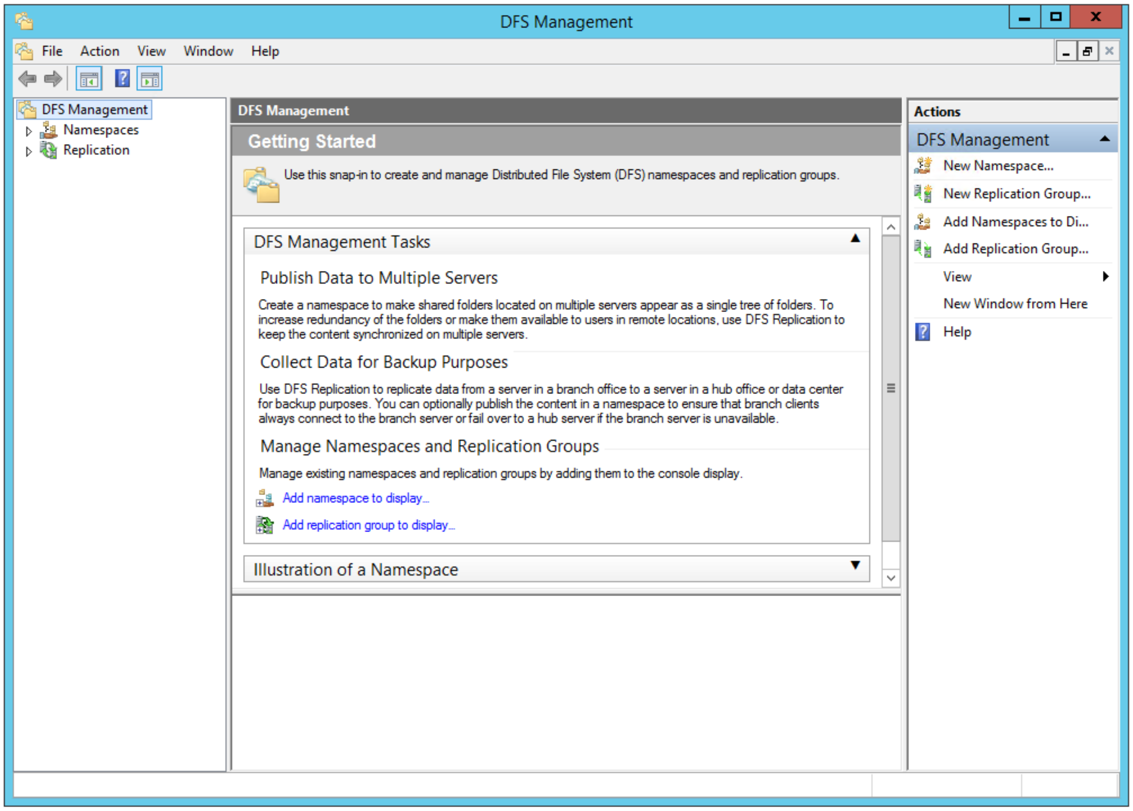
- Enable DFS Namespaces on an appropriate server in your domain.

## C.2 Creating DFS Namespace Permissions

The Storage Manager Proxy Rights Group (named SMProxyRights by default) requires Full Control in the CIFS permissions on the root share of the DFS namespace.

1 From Server Manager, click **Tools** > **DFS Management.**

2 Double-click **DFS Management**.



Use this snap-in to create and manage Distributed File System (DFS) namespaces and replication groups.

Publish Data to Multiple Servers

Create a namespace to make shared folders located on multiple servers appear as a single tree of folders. To increase redundancy of the folders or make them available to users in remote locations, use DFS Replication to keep the content synchronized on multiple servers.

Collect Data for Backup Purposes

Use DFS Replication to replicate data from a server in a branch office to a server in a hub office or data center for backup purposes. You can optionally publish the content in a namespace to ensure that branch clients always connect to the branch server or fail over to a hub server if the branch server is unavailable.

Manage Namespaces and Replication Groups

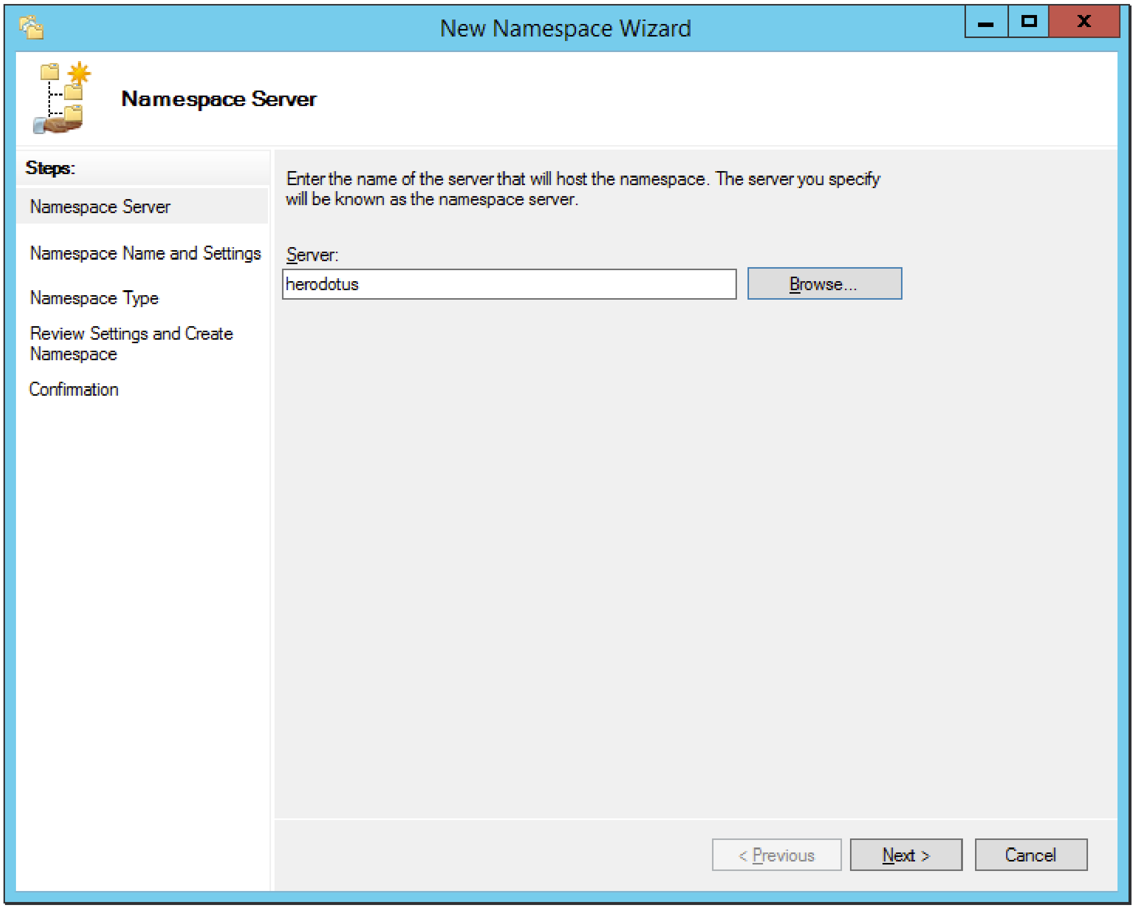
Manage existing namespaces and replication groups by adding them to the console display.

Add namespace to display...

Add replication group to display...

3 Right-click the **Namespaces** node and select **New Namespace.**

This launches the New Namespace Wizard.

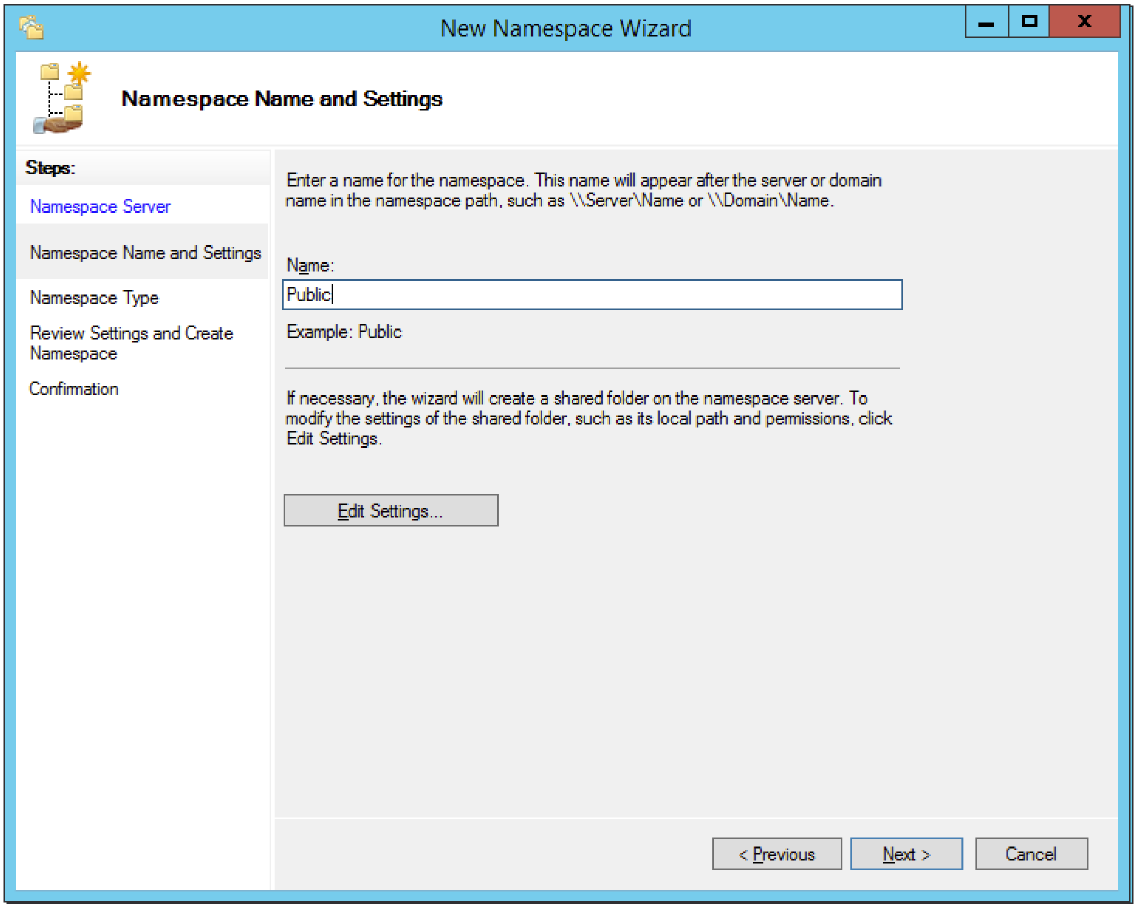


Enter the name of the server that will host the namespace. The server you specify will be known as the namespace server.

Server: herodotus

4 Use the **Browse** button to specify the server that will host the namespace.

5 Click **Next**.



**Namespace Name and Settings**

Steps:
Namespace Server
Namespace Name and Settings
Namespace Type
Review Settings and Create Namespace
Confirmation

Enter a name for the namespace. This name will appear after the server or domain name in the namespace path, such as \\Server\Name or \\Domain\Name.

Name: Public

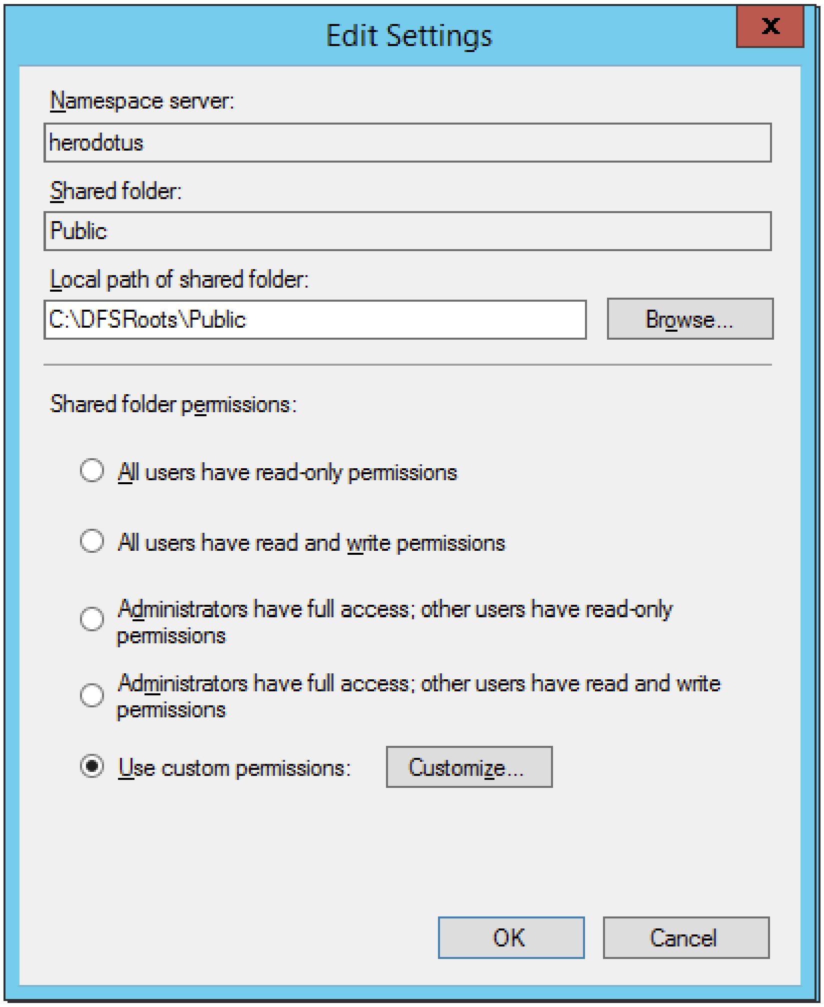
Example: Public

If necessary, the wizard will create a shared folder on the namespace server. To modify the settings of the shared folder, such as its local path and permissions, click Edit Settings.

6 In the **Name** field, specify the name of the namespace.

For example, HomeNamespace or Public.

7 Click **Edit Settings**.



Edit Settings

Namespace server:

herodotus

Shared folder:

Public

Local path of shared folder:

C:\DFSRoots\Public

Shared folder permissions:

○ All users have read-only permissions

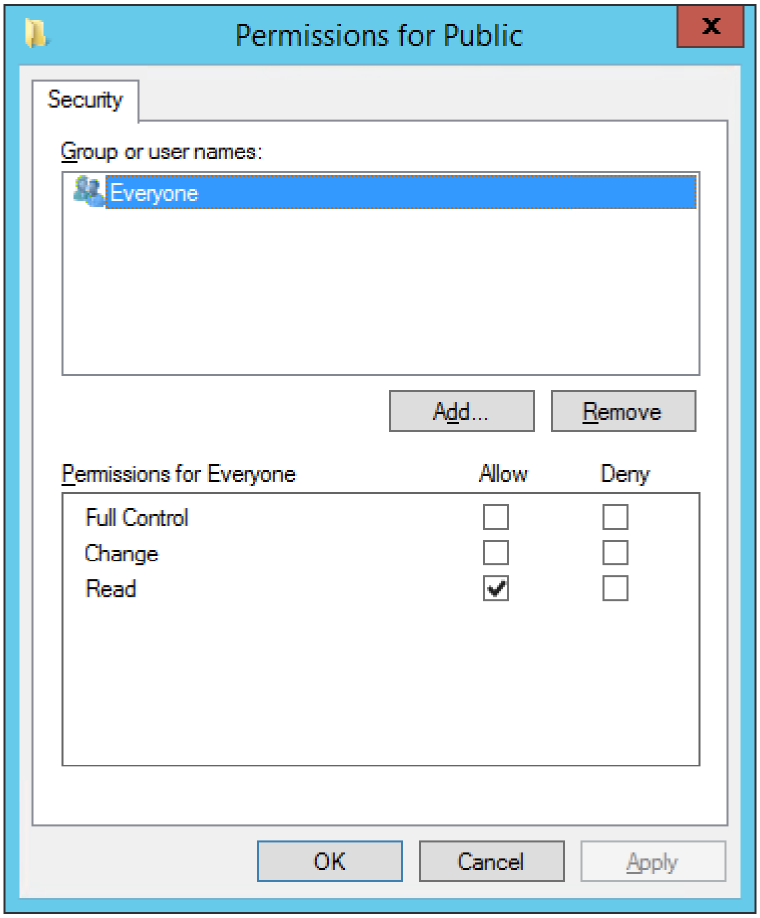
○ All users have read and write permissions

○ Administrators have full access; other users have read-only permissions

○ Administrators have full access; other users have read and write permissions

● Use custom permissions:

8 Select **Use custom permissions**, then click **Customize**.



Group or user names:

Everyone

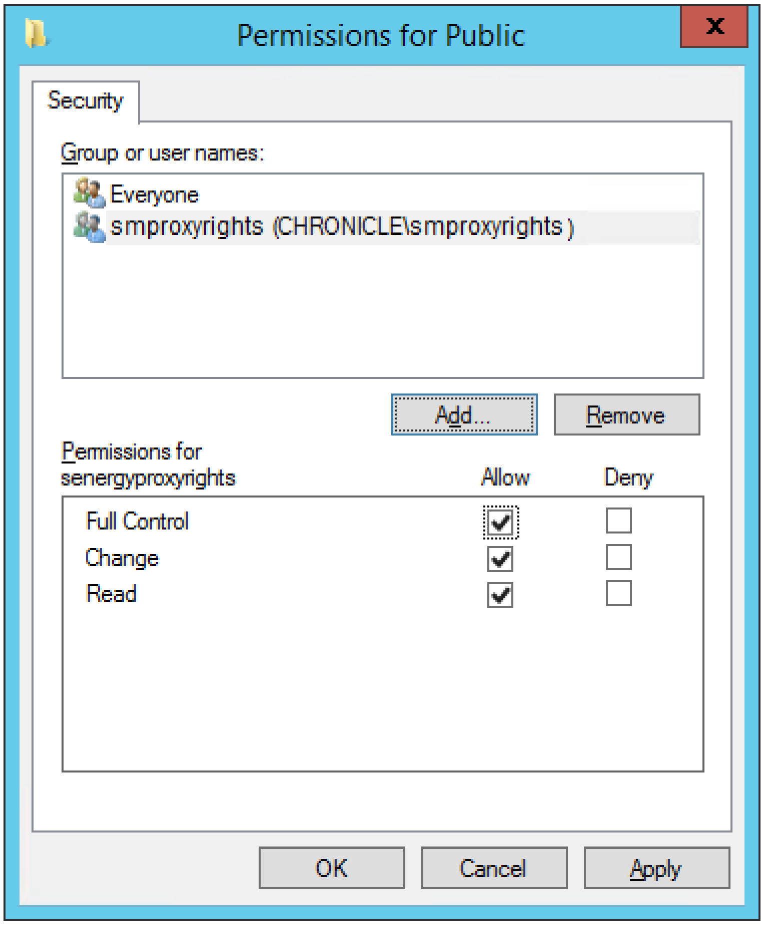
| Permissions for Everyone | Allow | Deny |
|---|---|---|
| Full Control | □ | □ |
| Change | □ | □ |
| Read | ☑ | □ |

9 Click **Add**.

10 In the **Enter the object names to select** field, type `sm` and click **Check Names**.

11 From the dialog box, select `smproxyrights` and click **OK**.

12 Click **OK** to close the Select Users Computers, Service Accounts, or Groups dialog box.



Group or user names:

- Everyone
- smproxyrights (CHRONICLE\smproxyrights )

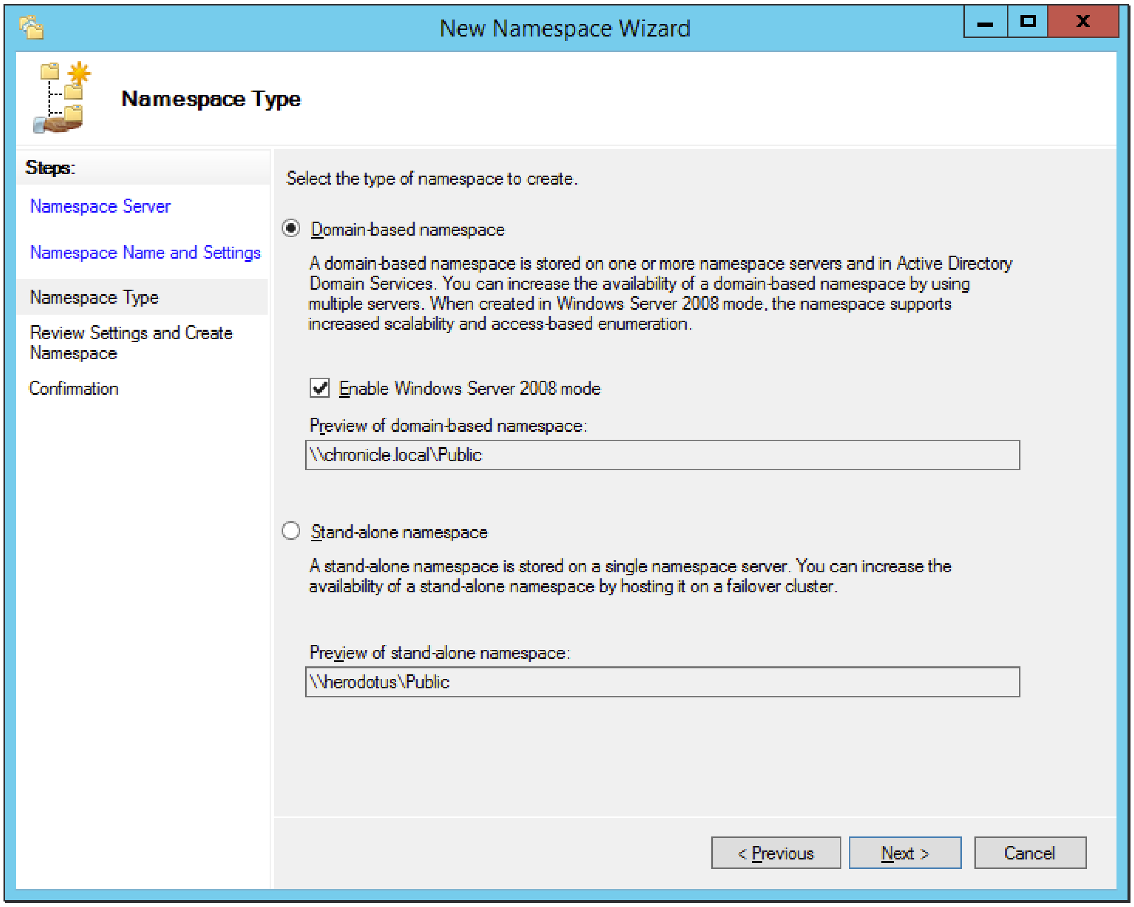
| Permissions for senergyproxyrights | Allow | Deny |
|---|---|---|
| Full Control | ☑ | □ |
| Change | ☑ | □ |
| Read | ☑ | □ |

**13** With `smproxyrights` selected, select the **Full Control** check box.

**14** Click **OK**.

**15** Click **OK** to close the Edit Settings dialog box.

**16** Click **Next**.



Namespace Type

Steps:
Namespace Server
Namespace Name and Settings
Namespace Type
Review Settings and Create Namespace
Confirmation

Select the type of namespace to create.

● Domain-based namespace

A domain-based namespace is stored on one or more namespace servers and in Active Directory Domain Services. You can increase the availability of a domain-based namespace by using multiple servers. When created in Windows Server 2008 mode, the namespace supports increased scalability and access-based enumeration.

☑ Enable Windows Server 2008 mode

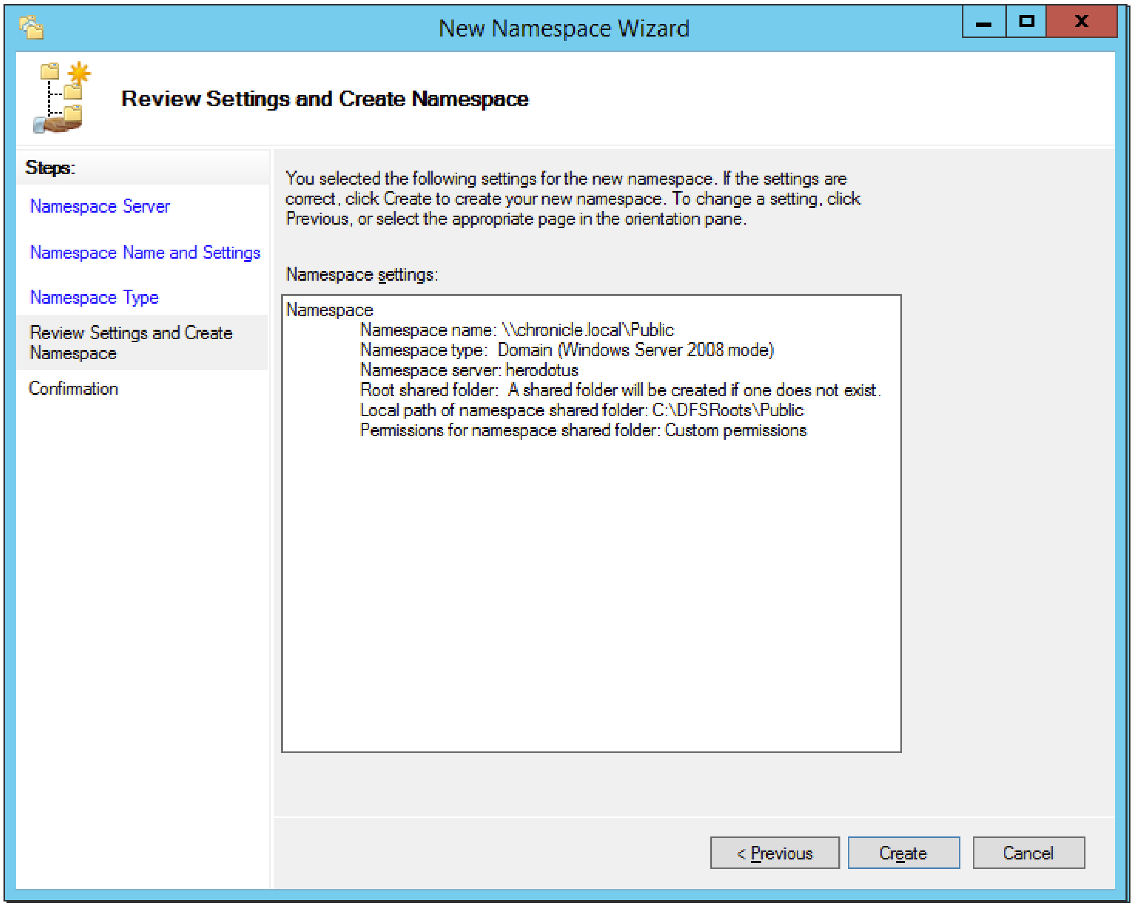
Preview of domain-based namespace: \\chronicle.local\Public

○ Stand-alone namespace

A stand-alone namespace is stored on a single namespace server. You can increase the availability of a stand-alone namespace by hosting it on a failover cluster.

Preview of stand-alone namespace: \\herodotus\Public

**17** Choose your preferred namespace option and click **Next**.


New Namespace Wizard
Review Settings and Create Namespace
Steps:
Namespace Server
Namespace Name and Settings
Namespace Type
Review Settings and Create Namespace
Confirmation
< Previous
Create
Cancel

You selected the following settings for the new namespace. If the settings are correct, click Create to create your new namespace. To change a setting, click Previous, or select the appropriate page in the orientation pane.

Namespace settings:

```
Namespace
        Namespace name: \\chronicle.local\Public
        Namespace type:  Domain (Windows Server 2008 mode)
        Namespace server: herodotus
        Root shared folder:  A shared folder will be created if one does not exist.
        Local path of namespace shared folder: C:\DFSRoots\Public
        Permissions for namespace shared folder: Custom permissions
```

18 Review the settings and click **Create**.

19 Click **Close** to close the wizard.

# C.3 Configuring DFS Folders

Storage Manager 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:

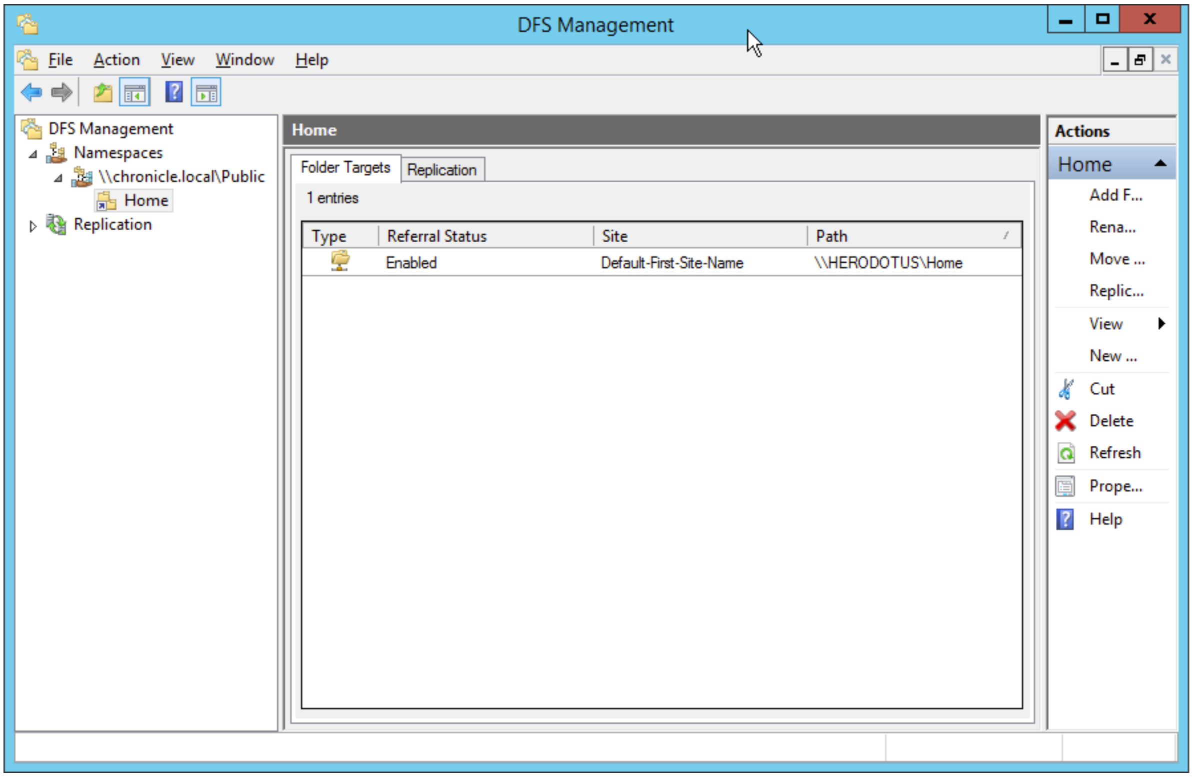
- Section C.3.1, “Providing Only One Target Per DFS Link,” on page 346
- Section C.3.2, “Disabling All but One Target Per DFS Link,” on page 347
- Section C.3.3, “Enabling Multiple Target Paths,” on page 348

## C.3.1 Providing Only One Target Per DFS Link

The simplest way to guarantee that Storage Manager 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.

***Figure C-1*** *One Target Path*



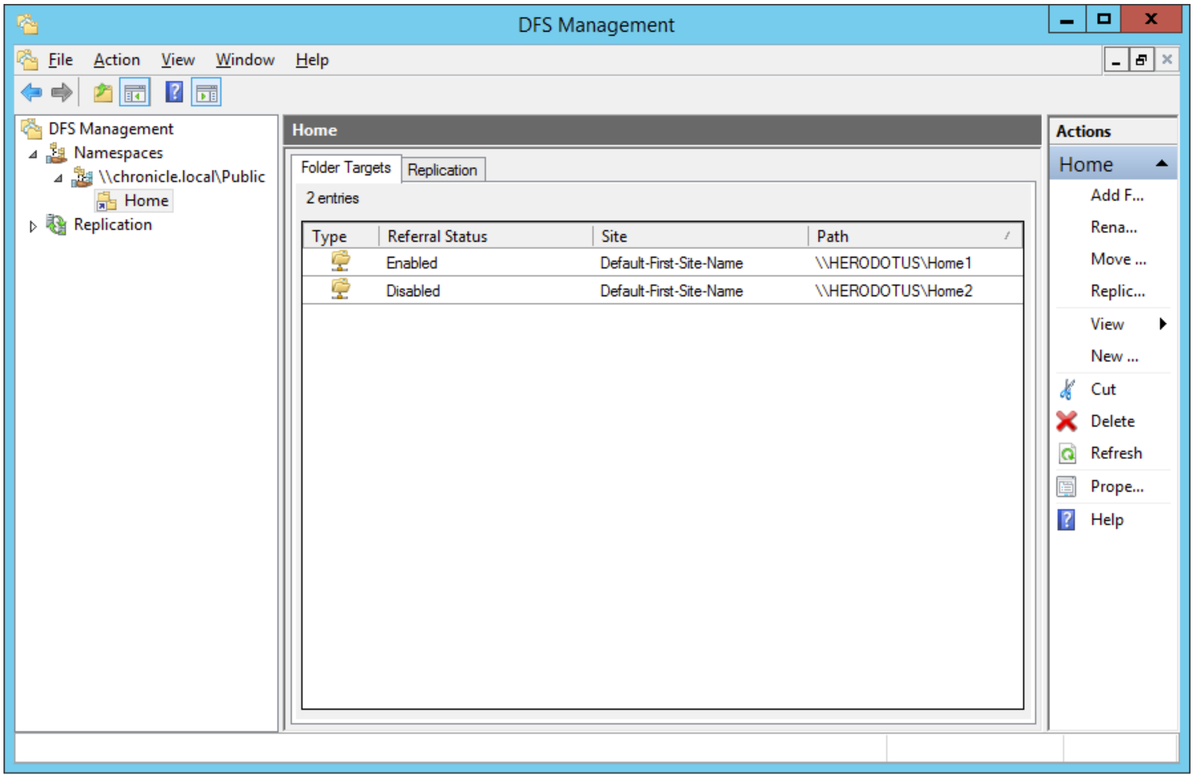
| Type | Referral Status | Site | Path |
|---|---|---|---|
| | Enabled | Default-First-Site-Name | \\HERODOTUS\Home |

## C.3.2 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, Storage Manager can successfully provision and manage storage through the DFS path.

In the following graphic, there are multiple target paths, but only one is enabled.

***Figure C-2** Multiple Target Paths with One Enabled*



| Type | Referral Status | Site | Path |
|---|---|---|---|
| | Enabled | Default-First-Site-Name | \\HERODOTUS\Home1 |
| | Disabled | Default-First-Site-Name | \\HERODOTUS\Home2 |

## C.3.3 Enabling Multiple Target Paths

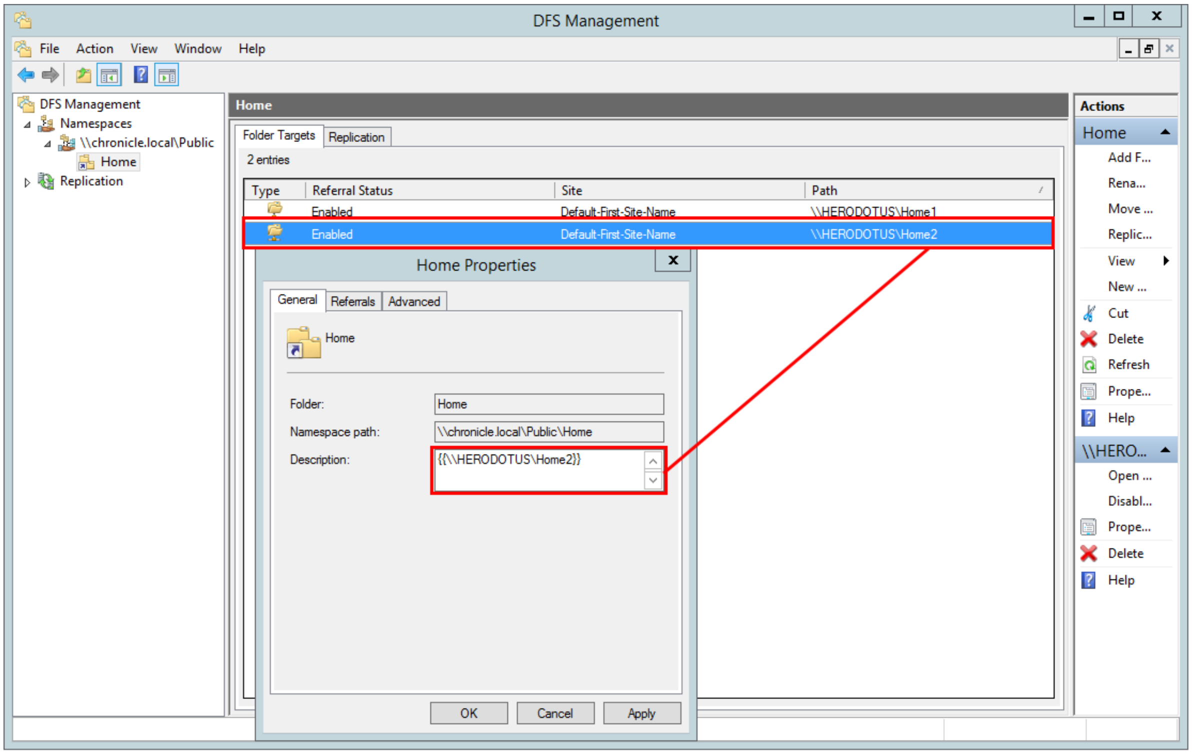
Storage Manager can parse the description field on a DFS folder to determine which of several enabled targets is the primary, unambiguous target. This allows Storage Manager to manage namespaces with multiple enabled targets in a DFS link.

To do this, the description for the DFS link must enclose the complete UNC path of the path Storage Manager 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 following graphic, there are two target paths enabled.

The Home Properties dialog box is accessed by double-clicking the listing in the DFS Management console.

*Figure C-3*   *Two Target Paths Enabled*



2 entries

| Type | Referral Status | Site | Path |
|---|---|---|---|
| | Enabled | Default-First-Site-Name | \\HERODOTUS\Home1 |
| | Enabled | Default-First-Site-Name | \\HERODOTUS\Home2 |

Folder: Home

Namespace path: \\chronicle.local\Public\Home

Description: {{\\HERODOTUS\Home2}}

# D Active Directory Schema Extensions

Micro Focus Storage Manager for Active Directory extends the Active Directory schema by adding new attributes and classes.

## D.1 Attributes

### D.1.1 ccx-FSFAuxiliaryStorage

A list of one or more paths pointing to managed auxiliary storage associated with this object

***Table D-1*** *ccx-FSFAuxiliaryStorage Specifications*

| 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.

***Table D-2*** *ccx-FSFManagedPath Specifications*

| Active Directory Attribute Property | Value |
|---|---|
| Name | ccx-FSFManagedPath |
| LDAP Display Name | ccx-FSFManagedPath |
| Admin Display Name | ccx-FSF-Managed-Path |
| 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

- Section D.2.1, “ccx-FSFManagedAttributes,” on page 352

### D.2.1 ccx-FSFManagedAttributes

An auxiliary class holding common attributes managed by Storage Manager for Active Directory.

***Table D-3*** *ccx-FSFManagedAttributes Specifications*

| Active Directory Class Property | Value |
|---|---|
| Name | ccx-FSF-Managed-Attributes |
| LDAP Display Name | ccx-FSF-Managed-Attributes |
| Admin Display Name | ccx-FSF-Managed-Attributes |
| Admin Description | Auxiliary class holding common attributes managed by Storage Manager |

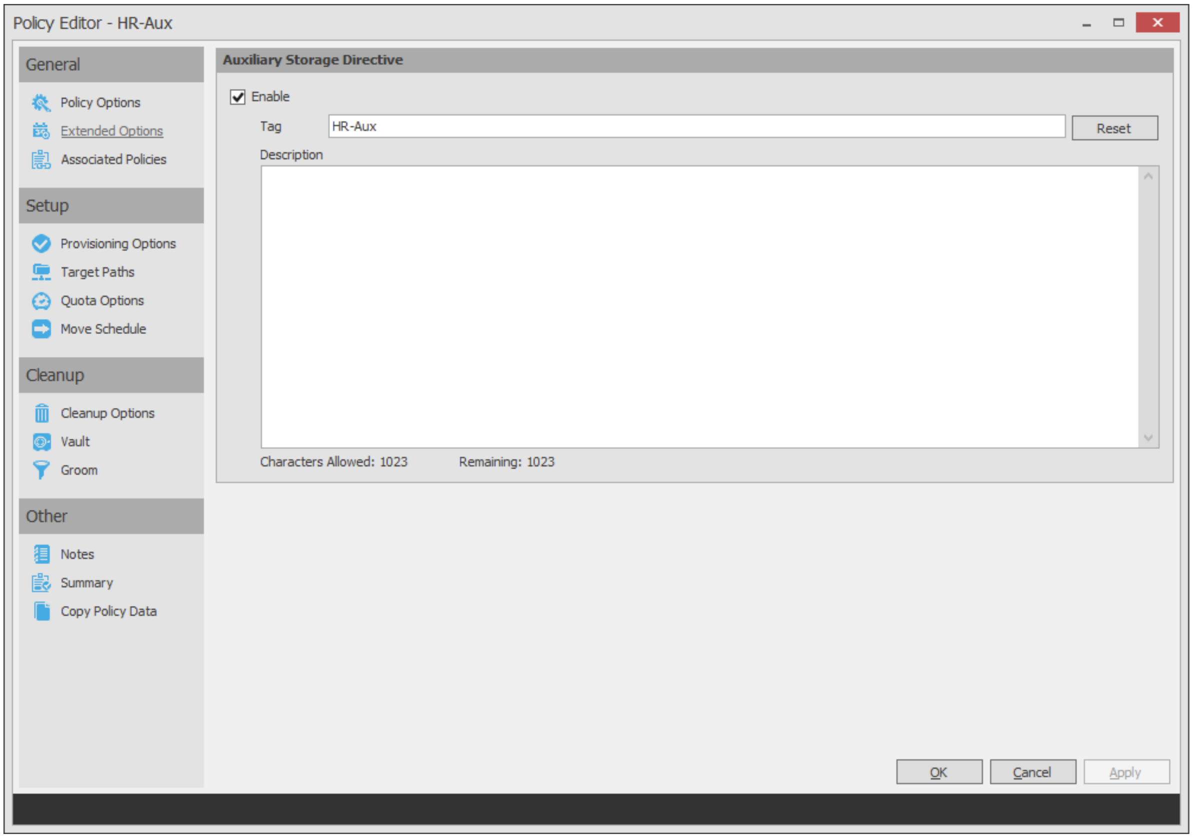
| Active Directory Class Property | Value |
|---|---|
| ASN.1 ID | 1.3.6.1.4.1.35052.1.1.2.1.1 |
| Schema ID GUID | c4bacb93-075e-11df-bcab-eee40b817f62 |
| Class Type | Auxiliary |
| Parent Class | top |
| Default Object Category | ccx-FSFManagedAttributes |
| Naming Attribute | - |
| Mandatory Attributes | - |
| Optional Attributes | ccx-FSFAuxiliaryStorage<br>ccx-FSFManagedPath |
| Possible Superiors | - |
| System Possible Superiors | - |
| System Flags | - |
| Default Security Descriptor | - |

# E AuxMap

The AuxMap utility lets you map drive letters to a user’s auxiliary storage folders through command line parameters in a Windows logon script. When the user logs in to Active Directory, AuxMap reads the auxiliary attribute associated with each auxiliary storage folder assigned to the user and then enables the drive mappings.

You must have the **Enable** check box checked, and an entry in the **Tag** field of the Extended Options of an auxiliary storage policy.

***Figure E-1*** *Extended Options Page of an Auxiliary Storage Policy*



Auxiliary Storage Directive

☑ Enable

Tag: HR-Aux

Description

Characters Allowed: 1023 Remaining: 1023

For more information, see “Enabling Auxiliary Storage Extended Options” on page 70.

At the root of the ISO, go to the applicable path to locate AuxMap:

- `\Utilities\AuxMap\win32\AuxMap.exe`
- `\Utilities\AuxMap\win64\AuxMap.exe`

Example Usage:

```
AuxMap --drive=<drive-letter> --storage=<storage-name>
```

```
AuxMap -d=<drive-letter> -s=<storage-name>
AuxMap --delete --drive=<drive-letter>
```

```
AuxMap --list-mappings
```

The following command line switches are supported:

***Table E-1*** *AuxMap Command Line Switches*

| | |
|---|---|
| `--help`<br>or<br>`-?` | Displays command line switch help information for AuxMap. |
| `--list-mappings`<br>or<br>`-lm` | Lists all currently mapped network drives. |
| `--drive=<drive-letter-or-path>`<br>or<br>`-d=<drive-letter-or-path>` | This must be a single uppercase letter in the range A through Z. The storage referred to in the storage parameter will be mapped to the chosen drive letter. |
| `--storage=<storage-name>`<br>or<br>`-s=<storage-name>` | This must be the name of an auxiliary storage area that has been provisioned for the user and is currently enabled and specified in the **Tag** field of the Extended Options page of an auxiliary storage policy. If the string in the **Tag** field contains a space, you must have quotes around the auxiliary storage area name. |
| `--delete` | Performs a map delete on the specified drive letter or path. Use with the `--drive` or `-d` switches. |
| `--debug` | If present, this causes AuxMap to produce more detailed diagnostic logging as it executes. |

# F Managed Path Naming Attribute Specifications

Storage Manager 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 Storage Manager. 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.

## F.1 Rules

### F.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” on page 261.

- 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.

### F.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\Share1\Users\123456789`
- Policy 1 Vault or Groom Path for user Keith whose `employeeNumber` attribute is “123456789”: `\\Server9\Vault\Users\123456789`

## F.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.

## F.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.

# G Event Monitor Scope

The Event Monitor scope identifies the portions of an AD environment that are relevant for event monitoring purposes. Setting the scope allows Storage Manager to generate actionable events only for the appropriate containers and groups. A scope is defined by explicit Include and/or Exclude lists. You can define a scope to encompass a multi-domain forest environment with subsets of scoped elements being individual AD domains and containers or group objects within them.

The Event Monitor scope does not affect the AD Forest Trust Filter or Storage Resources. These have separate configuration mechanisms that limit what portions of the AD environment they make use of. However, an AD Forest Trust Filter can affect the scope if the filter excludes entire AD forests that are otherwise included by the scope. The accessible portions of AD will be the intersection of the AD Forest Trust Filter and the scope. Or, to put it another way, every AD forest that is included by the AD Forest Trust Filter will, by default, have all of its AD domains also implicitly included in the absence of a scope that explicitly excludes any AD domains.

- Section G.1, “Include and Exclude,” on page 359
- Section G.2, “Event Monitoring,” on page 360
- Section G.3, “Non-Monitored Active Directory Containers,” on page 361
- Section G.4, “Operational Containers,” on page 362

## G.1 Include and Exclude

An Event Monitor scope is defined by the domain, container and group objects that are specified in its Include and Exclude lists. Presence in either one of the lists has different effects based upon the type of object chosen. By default, if there are no entries in either of these lists, the domain and all of its objects in which the product is installed are implicitly included. This is the default behavior of Storage Manager prior to the introduction of the scope feature.

Within an AD domain, there can be no ancestor/descendent relationship between areas of inclusion:

- After you explicitly exclude a container, its subordinate containers are by default implicitly excluded. You cannot include any of its subordinate containers by explicitly including them.
- If the scope is defined only by includes, the remainder of the AD domain is by default implicitly excluded, except for the explicitly included containers and their subordinate containers. You must explicitly include all portions of the AD domain that are of interest.
- If the scope is defined only by excludes, the remainder of the AD domain is by default implicitly included, except for the explicitly excluded containers and their subordinate containers.

- Section G.1.1, “Include,” on page 359
- Section G.1.2, “Exclude,” on page 360

### G.1.1 Include

The Include list provides a means for creating a white-list such that only specified objects are white-listed. Consequently, anything not contained within the Include list is implicitly excluded. This holds true for domains, containers, and groups.

### Containers

After a container has been added to the Include list, all other objects that are not subordinate to it that are not added to the Include list are implicitly excluded. Any explicit include of a container applies to that container and the entire sub tree that is subordinate to it. In the case of includes, subordinate containers at any depth under the included container may be explicitly excluded to “prune off” portions of the domain that should be ignored.

### Groups

After a group has been added to the Include list, all other groups in the same container as that group, which were not added to the Include list, are implicitly excluded. The members of a group are independently evaluated to determine if they are in scope or out of scope for event monitoring purposes. Any monitored change that occurs where the pairing of a group and a group member has either or both objects out of scope results in no change being reported for that particular pairing.

## G.1.2 Exclude

The Exclude list provides a means for creating a black-list such that the specified objects and their respective subordinate objects are excluded and everything else is implicitly included. This holds true for domains, containers, and groups.

### Containers

After a container has been added to the Exclude list, all other objects that are not subordinate to it that are not added to the Exclude list are implicitly included. Any explicit exclude of a container applies to the container and the entire sub tree that is subordinate to it. Explicit excludes of containers are “final”, in that no subordinate objects below and explicit exclude are allowed to be explicitly included.

### Groups

After a group has been added to the Exclude list, all other groups in the same container as that group, which were not added to the Exclude list, are implicitly included. The members of a group are independently evaluated to determine if they are in scope or out of scope for event monitoring purposes. Any monitored change that occurs where the pairing of a group and a group member has either or both objects out of scope results in no change being reported for that particular pairing.

# G.2 Event Monitoring

The content of the Event Monitor Partial Replica (PR) is not currently being limited by the explicitly set scope. However, the PR content is limited by the internal scope that the Event Monitor constructs and populates with explicit exclude filter elements for the `CN=Builtin,`*`<domain-ldap-fdn>`* container and for all of the “[Other] Well Known Objects” containers except the “Users”, “Computers” and “Domain Controllers” containers.

The suppression of Event Record Entry (ERE) creation is limited by the scope.

Given a constant scoping filter, the following behavior is expected as the Partial Replica is built and maintained over time:

- Objects that are within scope when created or deleted will have Partial Replica Entries (PREs) created and maintained for them, with appropriate Event Record Entries (EREs) being created and made available for use.
- If an object is created while out of scope and is then moved in scope, the Event Monitor will process the move as if it was a create for a new object.
- If an object is created while in scope and is then moved out of scope, the PRE will be updated and an ERE will be created for the object move, after which no other EREs will be created for the object for as long as it remains out of scope. Additionally, the PRE for the object will not be maintained while it is out of scope.
- If an object that was previously in scope and had a PRE create for it is deleted after it was moved out of scope, the PRE will be marked as being a stub that represents a tombstone, but no EREs will be generated related to the object being deleted.

When the scope changes (e.g. the portion that affects the content of the PR) after the PR has been created, then the following behavior can be expected as the PR is maintained over time:

- A partial rebuild or full rebuild of the partial replica will be initiated when the Event Monitor receives the updated scope and determines that it is different from the previous scope that it had been using. This rebuild happens only if the portions of the filter that affect the PR have changed; changes to the portions of the scope that affect only ERE filtering will go into effect immediately without triggering a PR rebuild.
- If an object was created when it was out of scope, and then the scope is altered so that the object is now in scope, then the next time that the object is modified, it will be handled as if it was just created.
- If an object was created when it was in scope, and then the scope is altered so that the object is now out of scope, then no further EREs will be generated for the object and its PRE will not be maintained, for as long as it remains out of scope. If the object is deleted while it is out of scope, the PRE will be marked as being a stub that represents a tombstone, but no EREs will be generated related to the object being deleted.

## G.3 Non-Monitored Active Directory Containers

As a means of avoiding the monitoring of non-applicable network events, the Event Monitor excludes the monitoring of the following Active Directory containers:

- Builtin
- Foreign Security Principals
- Managed Service Accounts
- Program Data
- System

## G.4 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.

Only a subset of object classes are permitted for container include/exclude elements, as follows:

- container
- groupPolicyContainer [exclude only]
- configuration [exclude only]
- builtinDomain [exclude only]
- organization
- organizationalUnit
- country
- locality
- msExchSystemObjectsContainer [exclude only]
- msDS-QuotaContainer [exclude only]

# H Glossary

**Action Block:** A feature of Storage Manager that allow the sharing of specific policy options between multiple policies. With the release of Storage Manager 5.0, you can create Action Blocks for policy-based vaulting, policy-based grooming, and non-policy-based grooming.

**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 Storage Manager policies from affecting members of organizational units, members of groups, or even individual users.

**Consistency check:** This Management Action notifies you of inconsistencies or potential problems pertaining to user and group storage being managed through Storage Manager. These potential problems might be missing storage quotas, inconsistent directory attributes, missing home directories, inconsistent file paths, and more.

**Container:** A synonym for organizational unit in the Micro Focus Storage Manager documentation.

**Collaborative storage:** A shared storage area where a group of people in an organization can collaborate by accessing files. Storage Manager lets you easily create collaborative storage areas through collaborative storage policies that you can assign to Group objects or to an organizational unit.

**Cross-Empire Data Migration:** Separately-purchased susbsystems of Storage Manager that allow for the movement of file system data, along with associated permissions, and metadata, between storage infrastructures on different platforms or different Active Directory forests. There is a Cross-Empire Data Migration offering from eDirectory to Active Directory, and another from Active Directory to Active Directory.

**Deferred delete event:** The scheduled deletion of a managed path, but has not yet taken place because the number of days in the Cleanup Storage parameter of the policy has not been met.

**Dynamic Template Processing:** Within Storage Manager, the process that creates personal folders in a collaborative storage folder.

**Effective policy:** A policy that is applied by default to a group, user, or subcontainer when no associated policy is specifically assigned.

**Enumeration operation:** The process of locating and displaying all objects.

**Identity map:** Within the Cross-Empire Data Migration subsystem, the mechanism that lets you make security and ownership associations between the source and the target.

**Managed Path:** A location that Storage Manager 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.

**Operation:** An action performed in Storage Manager that is not tied to a policy. At the present time, Storage Manager can perform Vault and Groom operations.

**Personal folder:** A user-specific folder in a collaborative storage area.

**Policy:** Rules and settings within Storage Manager that indicate what storage-specific actions to enact when an event in 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, Storage Manager uses this setting to determine which policies to apply. Storage Manager 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.

**SMAdmin:** The management interface for Storage Manager.

**Target Path:** The path to the network share where managed paths are hosted.

**Template: I**f 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 Storage Manager 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.

# Documentation Updates

This section contains information about documentation content changes that were made in this *Micro Focus Storage Manager 5.2 for Active Directory Administration Guide* after the initial release of Storage Manager 3.0 for Active Directory. The changes are listed according to the date they were published.

The documentation for this product is provided on the Web in two formats: HTML and PDF. The HTML and PDF documentation are both kept up-to-date with the changes listed in this section.

If you need to know whether a copy of the PDF documentation that you are using is the most recent, the PDF document includes a publication date on the title page.

The documentation was updated on the following dates:

## I.1 May 16, 2017

Updates were made to the following sections:

| Location | Update Description |
|---|---|
| Chapter 12, “Work Log Reports,” on page 229. | New section. |
| “Status” on page 245. | Updated section. |
| “Creating a Move Schedule Action Block” on page 263. | New section. |
| “Creating a Target Paths Action Block” on page 266. | New section. |
| Section 13.2.9, “Configuration,” on page 329. | New section. |
| Section 13.2.10, “Reports,” on page 329. | New section. |

## I.2 December 13, 2016

Updates were made to the following sections:

| Location | Update Description |
|---|---|
| Chapter 4, “Configure the Event Monitor Scope,” on page 27. | New section. |
| Section 6.5.4, “Setting Target Paths,” on page 54. | Updated section. |
| Section 8.9, “Creating a Multi-Principal Collaborative Storage Policy,” on page 107. | New section. |
| “Creating a Managed Path Naming Attribute Action Block” on page 261. | New section. |

| Location | Update Description |
|---|---|
| "Creating a Multi-Principal Suffix Mapping Action Block" on page 264. | New section. |
| "Cross-Forest Data Management" on page 309. | New section. |
| Section 13.1.15, "Scope," on page 310. | New section. |
| Appendix F, "Managed Path Naming Attribute Specifications," on page 357. | New section. |
| Appendix G, "Event Monitor Scope," on page 359. | New section. |

## I.3 July 19, 2016

Updates were made to the following sections:

| Location | Update Description |
|---|---|
| Section 5.2, "Viewing Anomaly Reports," on page 34. | Updated with information on new Anomaly reports. |
| Chapter 11, "Performing an Active Directory to Active Directory Cross-Empire Data Migration," on page 207. | New section. |
| "Properties" on page 251. | An extensive set of new information has been written about the GSR Collector and the **History** tab. |
| Section 13.1.5, "Action Blocks," on page 257. | New section. |
| Section 13.1.13, "GSR Collector," on page 283. | New content in section. |
| Section 13.1.14, "Forest Trusts," on page 290. | New section. |
| Section 13.2.3, "GSR Anomaly," on page 318. | An extensive set of new information has been added to this section. |
| Section 13.2.4, "Completed Data Migration," on page 324. | New section. |
| Appendix A, "SMAdmin and Database Communication," on page 331. | New section. |

## I.4 October 7, 2014

Updates were made to the following sections:

| Location | Update Description |
|---|---|
| Section 6.11.4, "Establishing Auxiliary Purpose Mappings," on page 73. | New section. |
| "Enforce Policy Path" on page 271. | Added new feature information. |
| Appendix C, "Distributed File System (DFS)," on page 339. | Updated procedures. |

## I.5 October 17, 2013

Updates were made to the following sections:

| Location | Update Description |
|---|---|
| "Apply Home Drive" on page 271. | New section. |
| "Apply Owner" on page 271. | New section. |

## I.6 September 26, 2013

Updates were made to the following sections:

| Location | Update Description |
|---|---|
| "Importing Identity Associations through Delimited Text" on page 134. | New section. |
| "Creating Object Associations" on page 138. | New section. |
| Section 10.5.5, "Saving a Local Instance of the Identity Map," on page 145. | New section. |
| Section 10.5.6, "Loading a Saved Identity Map," on page 145. | New section. |

## I.7 June 12, 2013

Updates were made to the following sections:

| Location | Update Description |
|---|---|
| Section 6.5.1, "Setting Policy Options," on page 51. | Updated the description of Bypassable Events. |
| Section 6.5.4, "Setting Target Paths," on page 54. | Updated the description of the Leveling Algorithm. |
| Section 13.1.7, "Events," on page 274. | Updated the description of the **Defer** field. |

## I.8 January 18, 2013

Updates were made to the following sections:

| Location | Update Description |
|---|---|
| Multiple locations throughout the manual. | Changed references of 3.0.*x* to 3.1. |
| "Folder to Folder" on page 128. | Discussion of new Cross-Empire Data Migration utilities. |
| Section 10.12, "Performing a Folder to Folder Migration," on page 180. | Presented a two-phased approach for folder to folder migration, including the use of the new utilities. |

| Location | Update Description |
|---|---|
| Appendix H, "Glossary," on page 363. | Added new glossary entries. |

## I.9 October 15, 2012

Updates were made to the following sections:

| Location | Update Description |
|---|---|
| "Folder to Folder" on page 128. | New paragraph about the **Skip Open Files** option. |
| Section 10.12, "Performing a Folder to Folder Migration," on page 180. | IMPORTANT information added about the **Skip Open Files** option. |
| Section 10.12.2, "Migrating to an Existing Target Folder," on page 181. | Inserted a new Step 2 on page 182. Expanded Step 14 on page 185 to include the **Advanced Namespace Handling** and **Open File Options**. |
| Section 10.12.6, "Creating a Target Folder in the Data Migration Wizard," on page 200. | Inserted a new Step 2 on page 200. Expanded Step 17 on page 203 to include **Advanced Namespace Handling** and **Open File Options**. |

## I.10 May 18, 2012

Updates were made in the following section:

| Location | Update Description |
|---|---|
| Appendix C, "Distributed File System (DFS)," on page 339. | New appendix. |

## I.11 February 2, 2012

Updates were made to the following sections:

| Location | Update Description |
|---|---|
| Throughout the manual. | Changed 3.0.2 to 3.0.*x*. |
| Section 6.5.5, "Setting Quota Options," on page 56 | Added a note about managing quota on NAS devices. |

## I.12 July 5, 2011

Updates were made to the following sections:

| Location | Update Description |
|---|---|
| Section 9.3, "Understanding Quota Manager Status Indicators," on page 122 | Added this section. |

## I.13 May 16, 2011

Updates were made to the following sections:

| Location | Update Description |
|---|---|
| "What's New" on page 11 | Description of identity mapping in the Cross-Empire Data Migration subsystem. |
| Chapter 7, "Managing Existing Collaborative Storage," on page 79 | Added this chapter. |
| Section 10.2, "Security and Ownership," on page 128 | Updated this section with new information on identity mapping. |
| Section 10.5, "Creating and Modifying an Identity Map," on page 133 | Added this section. |
| Appendix H, "Glossary," on page 363 | Added new glossary terms. |

## I.14 March 16, 2011

Updates were made to the following sections:

| Location | Update Description |
|---|---|
| Section 10.3.1, "Prerequisite Tasks," on page 130 | Added this section. |
| Section 10.10, "Performing a Group to Group Data Migration," on page 166 | Prefaced the procedures with an Important notice stating that the group folders to be migrated must be managed through group-based collaborative storage policies in eDirectory. |

## I.15 March 1, 2011

Updates were made to the following sections:

| Location | Update Description |
|---|---|
| Section 10.4, "Creating the Migration Proxy Account," on page 131 | Inserted information on the need for the Universal Password policy to support 32-character passwords, and provided a link to documentation on how to reconfigure the policy. |

## I.16 February 14, 2011

Updates were made to the following sections:

| Location | Update Description |
|---|---|
| Chapter 1, "What's New," on page 11 | Descriptions of features new to Novell Storage Manager 3.0.1. |

| Location | Update Description |
|---|---|
| Section 6.10, “Copying Policy Data,” on page 68 | Procedures for importing a policy. |
| Chapter 10, “Performing an eDirectory to Active Directory Cross-Empire Data Migration,” on page 125 | Procedures for using Data Migration. |