Quest®
Migration Manager  8.7
for Active Directory

User Guide
# CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>About This Guide</strong></td>
<td>3</td>
</tr>
<tr>
<td>Overview</td>
<td>3</td>
</tr>
<tr>
<td>Conventions</td>
<td>3</td>
</tr>
<tr>
<td><strong>Active Directory Migration</strong></td>
<td>4</td>
</tr>
<tr>
<td>Introduction</td>
<td>4</td>
</tr>
<tr>
<td>Prerequisites</td>
<td>4</td>
</tr>
<tr>
<td>About Migration Manager</td>
<td>4</td>
</tr>
<tr>
<td>Initial Configuration of Migration Project</td>
<td>5</td>
</tr>
<tr>
<td>Managing the Migration Project</td>
<td>6</td>
</tr>
<tr>
<td>Delegating Migration Tasks</td>
<td>6</td>
</tr>
<tr>
<td><strong>Pre-migration Activities</strong></td>
<td>9</td>
</tr>
<tr>
<td>Trust Migration</td>
<td>9</td>
</tr>
<tr>
<td>Site Migration</td>
<td>12</td>
</tr>
<tr>
<td>Domain Pairs</td>
<td>15</td>
</tr>
<tr>
<td>Creating a Domain Pair</td>
<td>15</td>
</tr>
<tr>
<td>Configuring a Domain Pair</td>
<td>16</td>
</tr>
<tr>
<td><strong>Account Migration</strong></td>
<td>22</td>
</tr>
<tr>
<td>Migration Session</td>
<td>22</td>
</tr>
<tr>
<td>Considerations</td>
<td>22</td>
</tr>
<tr>
<td>Creating a Migration Session</td>
<td>23</td>
</tr>
<tr>
<td>Viewing Migration Session Details</td>
<td>34</td>
</tr>
<tr>
<td>Using a Completed Session as a Template</td>
<td>34</td>
</tr>
<tr>
<td>Configuring User and Group Renaming</td>
<td>34</td>
</tr>
<tr>
<td>Delegating Account Migration</td>
<td>36</td>
</tr>
<tr>
<td>Undo Account Migration</td>
<td>39</td>
</tr>
<tr>
<td><strong>Directory Synchronization</strong></td>
<td>42</td>
</tr>
<tr>
<td>Considerations</td>
<td>42</td>
</tr>
<tr>
<td>Directory Synchronization Agent</td>
<td>43</td>
</tr>
<tr>
<td>Agent Manager</td>
<td>43</td>
</tr>
<tr>
<td>Configuring the Synchronization Job</td>
<td>46</td>
</tr>
<tr>
<td>Starting and Stopping Directory Synchronization</td>
<td>54</td>
</tr>
<tr>
<td>Viewing Directory Synchronization Statistics</td>
<td>56</td>
</tr>
<tr>
<td><strong>Resource Update</strong></td>
<td>58</td>
</tr>
<tr>
<td>Overview</td>
<td>58</td>
</tr>
<tr>
<td>Resource Update Scenarios</td>
<td>59</td>
</tr>
<tr>
<td>Selecting Objects for Processing Explicitly</td>
<td>60</td>
</tr>
<tr>
<td>Resource Update Considerations</td>
<td>60</td>
</tr>
<tr>
<td>Resource Updating Manager</td>
<td>61</td>
</tr>
<tr>
<td>Overview</td>
<td>61</td>
</tr>
<tr>
<td>Starting Resource Updating Manager</td>
<td>62</td>
</tr>
<tr>
<td>Before You Update Resources</td>
<td>62</td>
</tr>
<tr>
<td>Specifying the Processing Scope</td>
<td>64</td>
</tr>
<tr>
<td>Discovering Computers</td>
<td>66</td>
</tr>
<tr>
<td>Sorting Computers</td>
<td>67</td>
</tr>
</tbody>
</table>
Processing Resources ........................................................................................................ 67
Moving Computers to Another Domain ........................................................................... 71
Task Scripting .................................................................................................................. 74
Post-Processing Operations ............................................................................................ 74
Processing Algorithm ...................................................................................................... 75
Managing Categories ....................................................................................................... 76
Viewing Log Files ............................................................................................................ 76
Interrupting the Process ................................................................................................. 77
User Profile Update ........................................................................................................ 77
Active Directory Processing ............................................................................................ 80
Exchange Server Processing ........................................................................................... 90
Exchange 5.5 Server Processing .................................................................................... 99
SMS Processing ............................................................................................................ 108
SQL Server Processing ................................................................................................. 115
Cluster Server Migration ................................................................................................. 125
Delegating Resource Update ......................................................................................... 127
Command-Line Resource Update ................................................................................... 128
SharePoint Processing .................................................................................................... 133
Rolling Back Migration Changes ................................................................................... 136
  Directory Migration Rollback ...................................................................................... 136
  Resource Update Rollback ........................................................................................... 136
About Quest Software, Inc. ............................................................................................ 137
  Contacting Quest Software ......................................................................................... 137
  Contacting Quest Support .......................................................................................... 137
Third Party Contributions ............................................................................................... 138
  Boost 1.0 License Agreement ...................................................................................... 138
  ZLib 1.1.4 License Agreement ..................................................................................... 138
About This Guide

Overview

This document has been prepared to assist you in becoming familiar with Quest Migration Manager for Active Directory. It contains the information required to configure and use the product for Active Directory migration. It is intended for network administrators, consultants, analysts, and any other IT professionals using the product.

Conventions

In order to help you get the most out of this guide, we have used specific formatting conventions. These conventions apply to procedures, icons, keystrokes and cross-references.

<table>
<thead>
<tr>
<th>ELEMENT</th>
<th>CONVENTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select</td>
<td>This word refers to actions such as choosing or highlighting various interface elements, such as files and radio buttons.</td>
</tr>
<tr>
<td><strong>Bolded text</strong></td>
<td>Interface elements that appear in Quest products, such as menus and commands.</td>
</tr>
<tr>
<td><em>Italic text</em></td>
<td>Used for comments.</td>
</tr>
<tr>
<td><strong>Bold Italic text</strong></td>
<td>Introduces a series of procedures.</td>
</tr>
<tr>
<td><strong>Blue text</strong></td>
<td>Indicates a cross-reference. When viewed in Adobe® Acrobat®, this format can be used as a hyperlink.</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Used to highlight additional information pertinent to the process being described.</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Used to provide Best Practice information. A best practice details the recommended course of action for the best result.</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Used to highlight processes that should be performed with care.</td>
</tr>
<tr>
<td>+</td>
<td>A plus sign between two keystrokes means that you must press them at the same time.</td>
</tr>
<tr>
<td></td>
<td>A pipe sign between elements means that you must select the elements in that particular sequence.</td>
</tr>
</tbody>
</table>
Active Directory Migration

Introduction

Prerequisites

We assume that you are familiar with Migration Manager concepts described in the Migration Manager Installation Guide, and that you have already installed the product, following the instructions provided in that guide. It is also recommended that you read the release notes for the current version of Migration Manager. The release notes contain information about specific product behavior, limitations, known issues, and workarounds that may be useful for planning and performing your migration.

About Migration Manager for Active Directory

Quest® Migration Manager™ for Active Directory is an efficient, flexible, and comprehensive solution for restructuring your Active Directory. The restructuring is performed by migrating objects between forests or domains. Migration involves moving Active Directory objects (users, groups, and resources) from a source domain to a target domain.

Depending on the environment and the goals of the migration, the migration scenario may vary. The Migration Manager Tips and Tricks document contains common migration scenarios and considerations for choosing the one that best fits your requirements.

While the migration is underway (and some large-scale migrations can last for years), the source and target domains must coexist and stay in synch. Migration Manager eases the administrative burden during this period by providing synchronization capabilities, such as synchronization of account properties, group membership, and passwords: administrators simply make necessary changes in one environment and those changes are automatically replicated to the other environment.

Migration Manager also allows delegation of migration task to other people. Delegated administrators are able to migrate and process only the resources you specify.

This guide describes the entire migration process, including pre-migration activities, the migration itself, directory synchronization, resource processing, and delegation.
Initial Configuration of Migration Project

The **Open Project Wizard** is the central place for configuring the migration project and all its components: the ADAM database, the SQL/MSDE database (for Exchange migrations only), and Statistics Portal.

The wizard can be used to start a new project, connect to an existing project, or change any settings of the current project.

In most cases you need just one Migration Manager project for your whole migration, no matter how many domains you have. Normally, you would use a separate project only for lab testing before you start migration in the production environment.

We assume that you became familiar with the **Open Project Wizard** while carrying out the procedures described in the *Opening a Migration Project* section of the *Migration Manager Installation Guide*. Refer to that document for a full description of the wizard steps.

To briefly review, the Open Project Wizard steps are as follows:

1. On the **Configure ADAM/ADLDS Project** step, you specify the server where ADAM is installed, specify the port number used by ADAM (the default is 389; it might be different if ADAM is installed on a domain controller or this is not the first ADAM instance on the server), and select a project to connect to (you can choose to create a new one).

2. Next, on the **Set Auxiliary Account** step, you supply the user name and password that program components will use to access the ADAM database.

3. The **Configure SQL/MSDE Database** step is displayed if you installed Migration Manager for Exchange. On that step, you configure the database that will be used to store information related to your Exchange migration.

4. On the **Configure Statistics Portal** step, you can optionally specify the portal's URL and connection settings.

5. On the final step, review the settings and finish the wizard. For detailed description, refer to the *Opening a Migration Project* chapter of the *Migration Manager Installation Guide*.

We recommend that you avoid managing the **Properties** setting of the same objects within the same migration project from several Migration Manager Console computers simultaneously.

Note also that having several parallel **Remote Desktop** connections to the same console computer is not supported.
Managing the Migration Project

Migration of simple environments where accounts and resources are centralized in one major location can be accomplished from that location using a single Migration Manager console.

However, this method is not appropriate when you need to migrate a large distributed environment where accounts and resources reside in different geographic locations (sites), particularly if the sites are connected by slow links that limit the amount of data that can be transferred effectively. In this case, the migration must be performed in each site locally.

Migration Manager provides for effective project implementation and management when migrating large distributed environments.

If a number of administrators from multiple locations are going to perform migration, it is recommended to have local ADAM installations in each major location with a replica of the project partition. To avoid excessive traffic over slow links, administrators should work with the nearest ADAM server that contains a replica of the project.

In this case, you will need to delegate responsibility for migration tasks, as explained in the next section.

Delegating Migration Tasks

Migration Manager allows administrators to delegate specific tasks to trusted persons responsible for particular stages of migration. For example, you can delegate the rights to manage the migration within a specified pair of domains to the administrators of those domains, or you can delegate the rights to process a specific server to the server administrator.

The trusted person will have the appropriate access to the objects that he or she is granted rights to only and will not have the opportunity to perform any actions with other objects.
The delegation is performed by assigning a role that defines a level of permissions to a person within a migration project. Only accounts that have **Full Admin** role over an object can delegate the rights over that object to another account.

The roles that can be assigned to a trusted person within a migration project are listed in the table below:

<table>
<thead>
<tr>
<th>TREE NODE OBJECT</th>
<th>AVAILABLE ROLES</th>
</tr>
</thead>
</table>
| Migration project| **Full Admin**—Can create and configure any objects (domain pairs, directory synchronization jobs, migration sessions, delegated migrations, resource processing tasks, etc.) and perform any task within the project.  
**Reader**—Can view objects within the project and their settings, except domain pairs and Exchange stores in the synchronization settings, but cannot perform any migration tasks or change the configuration. |
| Directory migration| **Domain Pair Creator**—Can create domain pairs. This person automatically gets the Full Admin role over the domain pairs he or she creates and therefore is able to change settings of the domain pairs later. |
| Domain pair| **Full Admin**—Can change any settings on a domain pair (such as credentials used to connect to each domain), and can also configure the directory synchronization between the domains, create and run migration sessions, and delegate the migration to other trusted persons.  
**Reader**—Cannot view or change settings of the domain pair, and cannot perform any migration tasks. |
| Delegated migration| **Migration Admin**—Can run migration sessions within the delegated migration job. This person can migrate objects from and to only those containers specified in the delegated migration job. He or she cannot see the credentials used to connect to the source and target domain or change the object processing custom add-in or the migration agent, but can see which custom add-in and agent are used. |
| Tasks| **Task Creator**—Can create resource processing tasks. This person is automatically assigned Full Admin role to the tasks he or she creates and therefore can change the task settings later and run the task. |
| Resource processing task| **Resource Admin**—Can run the resource processing task and change its settings. However, this person cannot change the re-permissioning options or perform undo or cleanup. |

Only a domain pair’s **Full Admins** are granted access to the domain pair’s sub-nodes (synchronization, migration, and other manually created delegated migration jobs) and migration sessions.
To delegate the rights to perform a migration task:

1. In Migration Manager, right-click the tree node object and select Delegate on the shortcut menu.
2. Specify the account to which you want to delegate the task.
3. Select the level of permissions for that account from the Role list.
4. Click Add Account. This will add the account to the Delegated accounts list.
5. Click OK.

To revoke permissions, complete the following steps:

1. In Migration Manager, right-click the tree node object and select Delegate on the shortcut menu.
2. In the Delegated accounts list, select the account you want to revoke the rights from and click Revoke.
3. Click OK.

Refer to the Delegating Account Migration section of this guide for more details about delegating account migration tasks.

Refer to the Delegating Resource Update section of this guide for more information about delegating resource processing tasks.
Pre-migration Activities

Before you start directory migration, analyze the existing directory. This includes identifying required hardware and software upgrades, possible naming conflicts in the case of directory merges, and for an inter-forest migration, comparing and unifying the source and target forest schemas. You can use Quest Reporter to obtain detailed information about the existing Active Directory configuration, hardware and software inventory, etc.

You can optionally set up the target Active Directory forest, administrative accounts, and organizational units before migration. For more information about environment preparation, refer to the Quest Migration Manager Installation Guide.

Migration Manager allows you to copy trusts that the source domain currently has with other domains to the target domain. Refer to the Trust Migration section below for more details.

Migration Manager also lets you preserve the physical entities of the source forest after the user accounts have been migrated. You can migrate sites, subnets, site links, and site link bridges between the Active Directory forests with help of the Site Migration Wizard. Refer to the Site Migration section below for more details.

Trust Migration

So that users can continue using the resources they need after their accounts have been migrated, the target domain must have the same trust relationships as the source domain. The Trust Migration Wizard allows you to verify trust relationships in the source domain and establish those trusts in the target domain.

To start the wizard, right-click the Trust Migration node in the Migration Manager Console management tree and select the Trust Migration command from the shortcut menu.
Step 1. Select Domains

Select the source and target domains for copying trust relationships. The source domain is the domain whose trust relationships will serve as a model for the target domain.

If you don't have administrative rights in the source and target domains, either add an account to the domain local Administrators group or run the net use \DC_NAME\c$ /u:D_NAME\administrator "password" command. For example:

net use \sourceDC\c$ /u:source\administrator "password"

Select the **Verify existing trusts** check box to test all existing trust relationships in the source and target domains to verify that they are functioning.

Step 2. Analyzing Trusts

As soon as you click **Next**, the wizard will start collecting information about trust relationships for the source and target domains. This operation can take some time.

When the wizard finishes inspecting the source domain, it will display all trust relationships found, except those established between the source and target domains.

Step 3. Analyzing the Source Domain Trusts

Wait while the wizard retrieves information about the trust relationships established for the source domain.
Step 4. Select Trusts

An arrow from a domain (that is, pointing right) designates a trusting domain. An arrow to a domain (that is, pointing left) denotes a trusted domain.

If in Step 1 you chose to verify trusts, the wizard also shows the trust status. A dashed arrow indicates a broken (non-functional) trust. An arrow with a question mark indicates a trust whose state could not be determined. Point to a trust icon to see its status.

Select each trust to be copied from the source domain to the target domain by selecting the check box next to the domain name. By default, all functional trusts, except those already present on the target, are selected.

Click Process to make the wizard establish the selected trusts in the target domain. Trusts in the source domain are not affected by the operation.

If you click Cancel during processing or an error occurs, further trust migration stops. However, trust relationships already established remain intact.

Step 5. Applying Trusts

The wizard is now trying to apply the selected trust relationships to the target domain. Wait until it completes.

Step 6. Complete the Wizard

The wizard displays the log file showing the results of the attempt to copy the trust relationships. You can save or print the log file, if required.
Site Migration

If you want to preserve the physical entities of the source forest after the user accounts have been migrated, you can migrate sites, subnets, site links, and site link bridges between the Active Directory forests. To do that, start the Site Migration Wizard by right-clicking the Site Migration node in the Migration Manager console management tree and selecting Site Migration from the shortcut menu. Complete the wizard as follows:

**Step 1. Select Source Domain Controller**

Select or browse to the domain controller of the domain belonging to the forest that is to be the source of migration. Specify the account under which the site migration should be performed. You can use the current account under which the Migration Manager console is running. Please note that the account you specify must have access to the objects of the forest that is the source of migration.

**Step 2. Select Target Domain Controller**

Select or browse to the domain controller of the domain belonging to the forest which is to be the target of site migration. Specify the account under which the site migration to the target forest should be performed. You can use the current account under which the Migration Manager console is running. Please note that the account needs to have access to the objects of the forest that is the target of migration.
Step 3. Select Objects to Migrate

Select the objects that should be migrated to the selected target forest. If you select an object, all its sub-objects are automatically selected. Clear the appropriate check boxes if you do not need the sub-objects to be migrated.

Step 4. Processing Options

This step allows you to set the configuration of the target forest.

Select the Mirror source forest site configuration option if you want the target forest site configuration to be an exact copy of the source site configuration.

If you select the Mirror source forest site configuration option, all target objects (sites, subnets, etc.) that do not exist in the source forest site configuration will be deleted.

If you want to merge the source and target forest objects, select the Merge the source and target forests site configurations option.

To assign domain controllers to Active Directory sites according to their IP addresses, select the corresponding check box. This will make the wizard use the IP addresses for assigning target domain controllers to Active Directory sites.
Step 5. Handle Duplicate Object Names

If you selected to merge source and target forest objects, conflicts may arise if source and target objects have identical names. This step allows you to specify rules for automatic conflict resolution during site migration. For each object type, select the action to be performed if a conflict arises.

Merge—Merge objects with similar names.

Replace—Replace the target object with the source object that has a similar name.

Skip—Skip source object migration in cases of conflict, leaving the target object with a similar name intact.

Step 6. Migrate Sites and Subnets

The wizard is now ready to migrate the selected objects. Click Next to continue.

Step 7. Migrating Selected Objects

Wait while the wizard performs the migration. This may take considerable time.

Step 8. Select License Servers

After the site migration is complete, you should select the license server for each target site using the Active Directory Sites and Services snap-in.
Domain Pairs

All migration activities are performed between source and target domain pairs. You should configure the pairs of source and target domains that will be involved in the migration and directory synchronization processes. The subsequent sections discuss how to create and configure the domain pairs.

Creating a Domain Pair

This section explains how to create a new domain pair in the migration project.

Before you create a domain pair, at least one Directory Synchronization Agent should be installed in your environment. Refer to the Directory Synchronization Agent section for more details.

To create a domain pair, right-click the Directory Migration node and select New Source and Target Domain Pair from the shortcut menu. This will start the New Domain Pair Wizard, which will guide you through the process:

Step 1. Select Source Domain

Specify or browse to the domain controller of the domain that you want to make a source of information for the migration.

Specify the credentials for accessing the domain controller.

- The account you specify on this page will be used by the Directory Synchronization Agent for accessing the source domain objects and to perform directory migration. Therefore, the account must have domain administrator rights in the source domain.
- If Exchange migration is planned as part of the migration project, some group membership restrictions apply to the account.

These specifics are detailed in the Accounts Used by the Directory Synchronization Agent section of the System Requirements and Access Rights document.
Step 2. Select Target Domain

Specify or browse to the domain controller of the domain that you want to make a target of migration.

Specify the credentials for accessing the domain controller.

- The account you specify on this page will be used by the Directory Synchronization Agent for accessing the target domain objects and to perform directory migration. Therefore, the account must have domain administrator rights in the target domain.
- If Exchange migration is planned as part of the migration project, some group membership restrictions apply to the account.

These specifics are detailed in the Accounts Used by the Directory Synchronization Agent section of the System Requirements and Access Rights document.

Step 3. Complete the New Domain Pair Wizard

The wizard displays the names of the source and target domains and the accounts you specified for connecting to domains.

As soon as a domain pair is created, it will be displayed in the Migration Manager console management tree as a node having two sub-nodes, Migration and Synchronization.

Configuring a Domain Pair

After you have created a domain pair, you can specify configuration parameters for the domain pair. To do this, right-click the domain pair and select Properties. The parameters you can specify are described below.

Modifying the parameters described below requires full directory resynchronization. You must stop the synchronization job for the domain pair and then restart it using the Start and Re-sync option.
**Skip Objects**

This step allows you to specify the categories of objects that will be skipped during processing for all migration and synchronization tasks. You can select to skip the following types of objects:

- Active Directory default objects (objects present in Active Directory by default, such as built-in accounts and accounts like Domain Admins and Domain Users)
- Disabled accounts
- Expired accounts

If you select to skip any of these objects, you will not see them and therefore will not be able to select them when you browse the source or target domain of the domain pair.

**Specify Conflict Resolution Rules**

You can specify the attributes that are to be unique within the given scope (forest, domain, or container) on source and target, and the action to be performed if these attributes are not unique (i.e., two or more objects exist with the same value for a specified attribute). This is done by setting conflict resolution rules.

The conflict resolution rules you specify affect both migration and synchronization.

Click **Add** to set a new rule for automatic conflict resolution and make the appropriate settings in the **New Conflict Resolution Rule** dialog box, described below.
Click **Edit** to edit an existing conflict resolution rule.

Click **Remove** to remove the selected conflict resolution rule from the list.

The rule consists of the following settings:

- **Source domain**—Specifies that the current conflict resolution rule will be applied on source.
- **Target domain**—Specifies that the current conflict resolution rule will be applied on target.
- **By attribute**—Select the attribute that you want to resolve the conflicts by.
- **Queue for manual resolution**—If this option is selected, conflicts in the selected attribute will not be resolved automatically but instead will be queued for later manual resolution. If directory synchronization is established between the domains in a domain pair, you will see objects that were queued for manual conflict resolution in the **Conflicts queue** of the directory synchronization job for the domain pair. Refer to the **Directory Synchronization** section for more details. In the case of migration, you can see the conflicting objects by inspecting the migration log. Refer to the **Viewing Migration Session Details** section for more details.
- **Add prefix**—If this option is selected, the specified prefix will be added to the attribute value if the attribute is not unique within the specified scope.
- **Add suffix**—If this option is selected, the specified suffix will be added to the attribute value if the attribute is not unique within the specified scope.
- **Forest**—Specifies that conflicts should be resolved within the whole forest.
- **Domain**—Specifies that conflicts should be resolved within the whole domain.
- **Container**—Specifies that conflicts should be resolved within each container.
Configure Object Matching

This step allows you to specify attributes for object matching during migration and synchronization.

The Directory Synchronization Agent will match the source and target objects according to the attributes selected for object matching. If the agent cannot find a matching object in the target directory, a new object is created in this directory and its attributes are populated with the values of the corresponding source object.

Object matching rules you specify affect both migration and synchronization.

The Match target objects by dialog box displays the fixed list of attributes that can be used to match source and target objects. These attributes are:

- **Account name**—If the account names of the source and target object are the same, the objects will be matched.
- **E-mail**—For mail-enabled objects, if a source and target object have the same primary SMTP address, the objects will be matched.
- **SIDHistory**—If the SIDHistory attribute of an object from one directory contains the security identifier (SID) of an object from another, the objects will be matched.

Select the attributes you want to use for matching the source and target objects. Matching will be performed in top-down priority. To change the attribute priority, use the up and down arrow buttons.

When two objects are matched, the information about matching is written to the service attribute specified to store the matching information. See the Service Attributes section for more details.
Service Attributes

The service attributes are used by the agent to store its internal information. Click Service Attributes on the Match target objects by dialog box to specify the attributes for each of the source and target object classes.

Object class—Specifies the object class for which you want to specify service attributes. In most cases you can use the default attributes.

Auxiliary—Specifies the attribute for storing information about conflict resolution and other service information. The attributes selected by default to store the auxiliary information for different object classes are listed below.

If Exchange is deployed in the forest, the following attributes are used:

<table>
<thead>
<tr>
<th>OBJECT CLASS</th>
<th>AUXILIARY ATTRIBUTE</th>
</tr>
</thead>
<tbody>
<tr>
<td>contact</td>
<td>extensionAttribute14</td>
</tr>
<tr>
<td>container</td>
<td>adminDescription</td>
</tr>
<tr>
<td>group</td>
<td>extensionAttribute14</td>
</tr>
<tr>
<td>inetOrgPerson</td>
<td>extensionAttribute14</td>
</tr>
<tr>
<td>organizationalUnit</td>
<td>adminDescription</td>
</tr>
<tr>
<td>printQueue</td>
<td>adminDescription</td>
</tr>
<tr>
<td>user</td>
<td>extensionAttribute14</td>
</tr>
<tr>
<td>volume</td>
<td>adminDescription</td>
</tr>
</tbody>
</table>

If there is no Exchange in the forest, then by default the adminDescription attribute is used to store auxiliary information for all object classes.

Matching—When two objects are matched, the Global Unique Identifier (GUID) of the corresponding object is written to the service attribute selected to store information about matching. The attributes selected by default to store the matching information for different object classes are listed below.
If Exchange is deployed in the forest, the following attributes are used:

<table>
<thead>
<tr>
<th>OBJECT CLASS</th>
<th>MATCHING ATTRIBUTE</th>
</tr>
</thead>
<tbody>
<tr>
<td>contact</td>
<td>extensionAttribute15</td>
</tr>
<tr>
<td>container</td>
<td>adminDisplayName</td>
</tr>
<tr>
<td>group</td>
<td>extensionAttribute15</td>
</tr>
<tr>
<td>inetOrgPerson</td>
<td>extensionAttribute15</td>
</tr>
<tr>
<td>organizationalUnit</td>
<td>adminDisplayName</td>
</tr>
<tr>
<td>printQueue</td>
<td>adminDisplayName</td>
</tr>
<tr>
<td>user</td>
<td>extensionAttribute15</td>
</tr>
<tr>
<td>volume</td>
<td>adminDisplayName</td>
</tr>
</tbody>
</table>

If there is no Exchange in the forest, then by default the `adminDisplayName` attribute is used to store matching information for all object classes.

The service attributes must meet the following criteria:
- The attributes configured as service attributes should not be used for other settings.
- Only **Unicode String** attributes should be used as service attributes.
- If you have multiple target domains in your environment make sure that the **Matching** attributes you select are replicated to Global Catalog.
- Matching attributes should be indexed in Active Directory.
Account Migration

Before you start your migration activities, be sure to install at least one Directory Synchronization Agent in your environment. You should also create in the migration project the pairs of source and target domains that will be involved in the migration and directory synchronization processes. Refer to the Directory Synchronization Agent and Creating a Domain Pair sections of this document for more details.

As soon as a domain pair is created, it will be displayed in the Migration Manager console management tree as a node having two sub-nodes, Migration and Synchronization.

The Synchronization node shows the template created for the directory synchronization job. The job can be further configured and started to perform object synchronization between the two domains. For more information about directory synchronization, refer to the Directory Synchronization section.

Migration Session

Using the Migration node, you can create migration sessions. Each migration session is basically a group of accounts to be migrated from the source domain to the target domain. The Migration Wizard will help you migrate the selected objects within the source-target domain pair along with the objects’ properties and security settings. Also, during migration you can change, in bulk, any of the attributes of the accounts being migrated by simply importing a tab-separated list with the new values. As soon as the selected objects have been migrated to the target domain, the session is considered to be complete.

The history and configuration of the session is stored in the database and can be viewed when necessary.

Considerations

When splitting up domain migration into sessions you should consider the way that linked attributes (such as group membership) get resolved:

- Linked attributes always get resolved in the scope of the session. For example, if you migrate a group and its members within the same session, the membership will get migrated.
- Linked attributes are also resolved for previously migrated objects. For example, if you first migrate users and then migrate a group, the group will be migrated with its membership.
• Backlinks (such as "member of") are not updated across sessions. For example, if you first migrate a group and then in other sessions migrate its members, the newly migrated accounts will not get added to the target group. If you have to migrate a group before its members, you can restore the membership by either re-migrating the group or doing full re-synchronization.

• Links to objects with well-known SIDs (for example, S-1-5-DomainPart-123) are not resolved by design, while links to built-in objects (whose SID does not contain DomainPart) are resolved as intended.

See the Migration Manager Tips and Tricks document for additional considerations and recommendations for setting up migration sessions.

Creating a Migration Session

To create a new migration session, right-click the Migration node under the appropriate domain pair and select New Session from the shortcut menu. This will start the Migration Wizard.

Step 1. New Migration Session

Specify a name for the migration session and optionally provide a comment for it.
Step 2. Select Source Objects

This step allows you to select objects for migration. The list of objects contains the objects currently selected for migration.

Click **Select** to add to or modify the selection. In the **Browse Source Domain** window, select the containers and/or individual objects you want to migrate.
When you select or clear a container, all its sub-objects are displayed in the right-hand pane and are automatically selected or cleared. If you want to select or clear individual objects, perform the selection in the list of objects in the right-hand pane.

To select or deselect containers, right-click the container and click Select or Deselect. Depending on your selection, the checkboxes will be marked as follows:

- A blue check mark indicates that the container and all objects and sub-containers within the container will be migrated.
- A white check mark indicates that the container will be created on the target and some objects and sub-containers within the container will be migrated as well.
- A grey check box without any check mark indicates that the container will not be created on the target but some objects or sub-containers within the container will be migrated.

Clicking the Select by group membership button offers you two options:

- **Select groups for selected objects**—Select the groups in which the selected objects are members. You can also specify the scope (global, local, or universal) and type (security or distribution) of groups for which to perform the select operation.

  ![Select by Group Membership](image)

- **Select objects within selected groups**—Select objects that are members of the selected groups. You can also specify the object class (users, contacts, or groups) for which to perform the select operation.

  ![Select by Group Membership](image)
After the selection is made, click **OK** to save it and close the window.

To remove an object from the list of selected objects, select the object and click **Remove**.

You can also export the current selection to an external text file for later use. The external list of objects is usually used for mass object renaming and populating target object attributes with different values.

To create an export file, click **Export**. In the **Export Selection to File** window, select the attributes you want to export for the selected users. This creates a tab-delimited list: the first column is the source object's DN, and the remaining columns are the selected attributes. The administrator can later modify the attribute values in this file and import it back by clicking **Import**. The modified attribute values will be applied to the target objects during migration.

One common use for such import files is to make Migration Manager rename user accounts and groups as part of the migration. For details about how to edit the import files in this scenario, see the **Configuring User and Group Renaming** section below.
Step 3. Select Target Container

This step allows you to select the container where migrated objects will be created. Click **Browse** to select the container where the migrated objects should be placed during migration.

You also can specify whether the OU hierarchy will be migrated and whether the accounts should be merged with the existing target accounts.

In the **OU hierarchy migration** section, choose one of the following:

- **Migrate selected objects with their OUs to the selected target OU**—If this option is selected, all selected objects and containers will be created on the target.
- **Migrate objects without OUs as a flat list**—If this option is selected, only selected objects (not containers) will be created on the target in the specified target OU.

In the **When merging with existing accounts on target** section, choose one of the following:

- **Merge and move the objects to the new OU**—If this option is selected, matched objects will be merged and moved to the specified target OU.
- **Merge and leave the account where it was before the migration**—If this option is selected, matched objects will be merged and left in the original target OU (not moved to the specified target OU).
- **Never merge: skip accounts that match any accounts on target**—If this option is selected, matched objects will be skipped from migration.
**Step 4. Set Security Settings**

This step allows you to specify the security settings for the migration.

Security Descriptor migration rule—Select the way security descriptors of the matched source and target objects will be handled.

All objects in Active Directory are securable objects. Each securable object has a security descriptor (SD) that identifies the object’s owner and can also contain the following access control lists:

- A discretionary access control list (DACL) that identifies the users and groups allowed or denied access to the object
- A system access control list (SACL) that controls how the system audits attempts to access the object

An ACL contains a list of access control entries (ACEs). Each ACE in an ACL identifies a trustee (a user account or group account) by its SID and specifies the access rights allowed, denied, or audited for that trustee.

You have the opportunity to **Merge**, **Replace**, or **Skip** the security descriptors:

- **Merge**—The security descriptor entries of the source object will be added to the security descriptor of the target object.
- **Skip**—The security descriptor of the target object will be left intact.
- **Replace**—All entries of the target object’s security descriptor will be deleted. The entries of the source object’s security descriptor will be copied to the target object’s security descriptor.
The DACL and SACL security descriptor entries of the source objects are assigned to the newly-created target objects during migration.

Regardless of the option you select to migrate security descriptors (Merge, Skip, or Replace) for each newly created target object, the default security descriptor defined for that object class will also be applied.

Only ACEs explicitly added to the source security descriptor are migrated.

The inheritance flag (the Allow inheritable permissions from parent to propagate to this object option on the Security tab of the object Properties) is migrated as well. That is, if the inheritance flag is set for the source object, it will be set for the corresponding target object; if the inheritance flag is not set for the source object, it will be cleared from the corresponding target object.

During migration, the ACEs of the source security descriptor referencing the source objects (source SIDs) are not translated to the target objects (target SIDs). To translate or clean up the source objects’ SIDs migrated to the target object’s security descriptor, use the Active Directory Processing Wizard.

Add SIDHistory—Select this checkbox if you want to allow the target accounts to access the source domain resources using the SIDHistory mechanism during the coexistence period.

To make users access the resources in the source domains by SIDHistory, trusts must be established between the source and target domains.

You should turn off SID filtering for each source domain to be migrated. You should also disable SID filtering if source accounts were previously migrated and contain SIDs from other domains in their SID history.

By default, SID filtering is turned on.

When you migrate accounts and groups, target group membership is automatically updated for the target users. In other words, the target group will have target user accounts as members corresponding to the source user accounts (members of the source group) migrated by that time. If you also want to add source accounts (the members of the source groups) to the corresponding target groups, select the Add source members to the corresponding target groups check box.

The User Principal Name handling section allows you specify how the User Principal Name (UPN) will be formed for each target user:

- **Copy**—If this option is selected, UPNs of source users will be assigned to the target users. This option is available only if the source and target domains belong to different forests.
- **Switch**—If this option is selected, the UPN is switched from the source user to the target user. This option is available only if the source and target domains belong to the same forest.
- **Skip**—If this option is selected, the target user UPN will be left intact.
- **Set the domain suffix of the UPNs to**—This option allows you to set the domain suffix of the UPNs of the target users to the value you specify.
The **Password handling** option allows you to also specify how user passwords will be handled:

- **Copy account password**—Passwords will be copied from the source to the target accounts.
- **Skip account password**—Passwords will not be copied for merged objects. The newly-created target accounts will get blank passwords.
- **Set password to username with**—Sets the target user password to its username with the specified prefix and/or suffix. To set the prefix or suffix, click **Configure**.
- **Set password to**—Sets the target user password to the specified value. To specify the common password value, click **Configure**.
- **Set random password**—Sets the password to a random value generated by some criteria. The passwords are stored in ADAM. You can select to generate strong or custom passwords. For custom passwords, you can set the range for the password length and the allowed characters.

To configure the complexity of the random password, click **Configure** and use the **Random length between** and **Allow characters** controls:

Selecting **Strong password** will disable the **Random length between** and **Allow characters** controls and make the generated passwords comply with the password requirements specified in Microsoft Knowledge Base article Q161990. According to the article, passwords must satisfy the following requirements:

- Passwords must be at least six (6) characters long. You can set the password length limit by editing the **Random length between** boxes.
- Passwords must contain characters from at least three (3) of the following four (4) classes:
  - English uppercase letters (A, B, C, ... Z)
  - English lowercase letters (a, b, c, ... z)
  - Westernized Arabic numerals (0, 1, 2, ... 9)
  - Non-alphanumeric or ‘special characters’, such as punctuation symbols
- Passwords may not contain a user name or any part of a full name.
**Step 5. Specify Object Processing Options**

Specify whether the target objects should be enabled after the migration session is completed. This setting makes sense if the users start using their target accounts immediately after the migration is completed. You may also want to disable source accounts after migration has been completed. Use the **Enable target accounts** and **Disable source accounts** options.

For intra-forest migrations, you can select to reconnect the source Exchange mailboxes to the target users so that users logged on to the target environment can use their source mailboxes until the Exchange migration is performed. Selecting the **Reconnect Exchange mailbox** check box will reconnect the source user mailboxes to the corresponding target users.

If you are planning to use a custom add-in to process the selected objects after they have been retrieved from the source domain and before they are copied to the target domain, select the **Use custom add-in** checkbox and browse for the `.xml` custom add-in file.

### Attributes to Skip

If you want to skip particular attributes, click the **Attributes to Skip** button. Then select the check boxes next to the attributes you do not want to migrate to the target domain.

Use the **Save Settings** button if you want to use the same settings when you create another migration session. Click **Load Settings** to apply a set of attribute skipping options you saved earlier.
Select the **Show advanced attributes** check box to choose from the complete list of attributes you can skip.

The Directory Synchronization Agent service attributes used by Migration Manager should never be skipped. Otherwise, Migration Manager will not be able to migrate and synchronize objects.

**Step 6. Select Migration Agent**

This step allows you to select the migration agent to perform the migration.

If you have only one agent installed in your environment, you will not be presented with this step.
Step 7. Summary

The wizard allows you to view the settings you made for the session. You can click Back to modify the settings if needed.

Select the Test mode check box if you want to run the migration in test mode, which does not apply any changes to the real target environment. Running a migration session in test mode allows you to check how the settings you made for the session will be applied to the target directory and decide whether these settings suit your needs. You can review the results by clicking View log after the migration is completed.

You can click Back and clear the Test mode check box to perform the actual migration only if you did not close the Migration Wizard dialog after the migration completed. You cannot clear the Test mode check box when you open the properties of the already-completed session. However, you can use this session as a template when you create a new session to perform the account migration. Refer to the Viewing Migration Session Details section for more details.

Step 8. Migrating Active Directory Objects

The wizard now migrates the selected objects to the target domain. All the activity takes place in the target domain only. The wizard displays the target domain directory update progress. Please wait while the wizard completes.
**Step 9. Complete the Wizard**

The migration session has been completed. The completed session configuration is now stored in the project database. Click the View log button to see if any errors or conflicts occurred during migration.

You can view the completed session configuration and use it later as a template for other migration sessions. For more information about migration session details, refer to the Viewing Migration Session Details section.

All changes made to the target environment during a migration session can be rolled back. For more information about undoing a migration, refer to the Undo Account Migration section below.

**Viewing Migration Session Details**

To view the migration session details, select the Migration node in the Migration Manager console management tree. The list of completed sessions is displayed in the right-hand pane. Right-click the session whose details you want to view and select Properties from the shortcut menu.

You can view the log of a completed session to see the results of migration by selecting the Summary tab and clicking View log.

**Using a Completed Session as a Template**

You can use a completed session as a template to create a new session with the same or similar configuration settings or similar objects to be migrated. For example, you might want to select a session that was previously run in test mode and perform the actual migration of objects using the settings specified in that session.

To use a completed session as a template, select the Migration node in the Migration Manager console management tree. The list of completed sessions will be displayed in the right-hand pane. Right-click the session you want to use as a template and select New Session from the shortcut menu. This will start the Migration Wizard. All the settings you made for the completed session, including objects selected for migration, are preserved and you do not need to specify these settings again.

**Configuring User and Group Renaming**

You have the option of renaming users and groups as part of the migration. This includes merging multiple source users or groups into a single target user or group.

Renaming of objects is performed using a specially formatted plain-text file, which should be imported on the Select Objects in Source Domain step of the Migration Wizard (see the Creating a Migration Session procedure).

All entries in the file should be tab-separated. The header is mandatory and should contain at least these two entries (note that the white space is a tab character):

```
SAMAccountName    SAMAccountName
```
One object per line should be specified. Here is a sample import file:

<table>
<thead>
<tr>
<th>SAMAccountName</th>
<th>SAMAccountName</th>
<th>name</th>
</tr>
</thead>
<tbody>
<tr>
<td>sourceuser01</td>
<td>targetuser01</td>
<td>sourceuser01</td>
</tr>
<tr>
<td>sourceuser02</td>
<td>targetuser02</td>
<td>sourceuser02</td>
</tr>
<tr>
<td>sourceuser03</td>
<td>targetuser03</td>
<td>sourceuser03</td>
</tr>
<tr>
<td>sourceuser04</td>
<td>targetuser04</td>
<td>sourceuser04</td>
</tr>
</tbody>
</table>

- If you are using this file to create a new user account and there is already a target domain user with the same name as the source user, the file above will not work. It is absolutely necessary to add at least the name attribute; then the file should look like this:

<table>
<thead>
<tr>
<th>SAMAccountName</th>
<th>SAMAccountName</th>
<th>name</th>
</tr>
</thead>
<tbody>
<tr>
<td>sourceuser01</td>
<td>targetuser01</td>
<td>targetuser01</td>
</tr>
</tbody>
</table>

- If object names contain spaces, there is no need to use quotation marks (spaces are not treated as delimiters). For example, to rename the Executive Users group to Target Executive Users, use this syntax:

<table>
<thead>
<tr>
<th>SAMAccountName</th>
<th>SAMAccountName</th>
<th>name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Users</td>
<td>Target Executive Users</td>
<td>Target Executive Users</td>
</tr>
</tbody>
</table>

The same file format can be used to populate other target attributes; here is a syntax sample:

<table>
<thead>
<tr>
<th>SAMAccountName</th>
<th>SAMAccountName</th>
<th>name</th>
<th>displayname</th>
<th>userprincipalname</th>
</tr>
</thead>
<tbody>
<tr>
<td>sourceuser1</td>
<td>targetuser1</td>
<td>targetuser1</td>
<td>Target</td>
<td><a href="mailto:targetuser1@dom.com">targetuser1@dom.com</a></td>
</tr>
<tr>
<td>sourceuser2</td>
<td>targetuser2</td>
<td>targetuser2</td>
<td>Target</td>
<td><a href="mailto:targetuser2@dom.com">targetuser2@dom.com</a></td>
</tr>
<tr>
<td>sourceuser3</td>
<td>targetuser3</td>
<td>targetuser3</td>
<td>Target</td>
<td><a href="mailto:targetuser3@dom.com">targetuser3@dom.com</a></td>
</tr>
</tbody>
</table>

The same import file can be used for merging with existing objects. When using such a file, you can merge two completely different accounts, for example Peter M. from the source domain can be merged with James T. from the target domain. The same applies to groups. In rare cases, the same approach is used to merge a built-in group with another (regular) group. When merging users or groups using sAMAccountName<tab>sAMAccountName, make sure that matching by sAMAccountName is enabled in the domain pair properties; otherwise DSA will attempt to create a new user with the same sAMAccountName and post a conflict instead of doing a merge.

The CN attribute cannot be changed using the CN as syntax. In order to modify the CN value, the Name attribute must be used. This will change the CN name on target.

Finally, note the following specifics:

- The maximum user or group name in the file is 64 characters. If this number is exceeded, you will receive an error message during the migration. Here is a sample log entry of the error:

```
LDAP error 0x13. Constraint Violation (00002082: AtrErr: DSID-03050B04, #1:0: 00002082: DSID-03050B04, problem 1005 (CONSTRAINT_ATT_TYPE, data 0, Att 3 (cn):len 130)).
```
• Import files work only for migration and are not applicable to synchronization.
• If synchronization is turned on and the attributes being changed during migration are not excluded, synchronization will overwrite the changes.
• When you migrate accounts using an import file, they will always be migrated as a flat list to the location you specify during the migration session no matter what is specified by the migration session settings. If you want to retain the source domain's OU structure for the listed objects, one possible option is to migrate the objects normally first, then rename them later using the import file and a merging migration session. When performing this, make sure the **Merge and leave the account where it was before the migration** option is selected.
• There are two ways to exclude attributes:
  • Excluding attributes when configuring the source and target domain pair will exclude them from all subsequent migrations and synchronization for the pair of domains.
  • Excluding attributes via a configuration script, on the corresponding tab of the configuration properties (Configure Synchronization), will exclude them from synchronization only.

**Delegating Account Migration**

If you want to re-assign the directory migration task to some other person without revealing key credentials (like administrative accounts and passwords to access source and target domains), you can delegate migration to that person and even limit the scope of the delegated migration to certain organizational units (OUs) belonging to the source and target domains.

The results and status information on the delegated migrations will be added to the project, so no matter how many delegated administrators are involved, you can keep track of the overall project.

Since the delegated administrators get access to only the tasks to which you grant them access, you can be sure that they do not interfere with other tasks.

A person to whom the migration task is delegated is called a **Migration Admin**. This person will be able to create migration sessions using the Migration Wizard. However, the objects available for migration will be limited to the scope you specified when you delegated the task. The Migration Admin to whom the task was delegated will not be able to select the agent to perform migration or the custom add-in to process the objects being migrated.

To delegate a migration task, right-click the domain pair node and select **New Delegated Migration** from the shortcut menu. The **New Delegated Migration Wizard** will help you delegate a part of migration to another person.
**Step 1. New Delegated Migration**

Specify a name for the delegated migration and enter comments.

**Step 2. Restrict Source Migration Scope**

This step allows you to select the OUs from which the objects can be migrated within the delegated migration scope.

**Step 3. Restrict Target Migration Scope**

This step allows you to select the OUs to which the objects can be migrated within the delegated migration scope.
**Step 4. Select Migration Agent**

A person to whom the migration task is delegated will be able neither to install the Directory Synchronization Agent nor to select the agent’s instance for performing migration. Therefore, in this step you should select the instance of the Directory Synchronization Agent which will perform the delegated migration.

If you have only one agent installed in your environment, you will not be presented with this step.

**Step 5. Specify the Object Processing Custom Add-in File**

A person to whom the migration task is delegated will not be able to select a custom add-in file for processing objects being migrated. Therefore, on this step you should select the custom add-in file if the migrated objects should be processed with the script before copying to the target server. Select the **Use custom add-in** checkbox and browse for the .xml custom add-in file.
**Step 6. Delegate the Migration**

This step allows you to assign the Migration Admin role to the account you select. The Migration Admin will be able to create migration sessions and make migration settings within the scope you just selected.

![Delegate the Migration](image)

**Step 7. Complete the Wizard**

The wizard displays the delegation settings you made.

**Undo Account Migration**

You can roll back the changes made to the target directory by each migration session independently.

All the changes made to the target domain by the session will be rolled back exactly to the state before the session started. The following example illustrates this behavior:

1. Suppose that during migration session 1, you migrated a number of objects from the source domain and specified to merge them with the existing target objects and move them to organizational unit A on the target.

2. Then during migration session 2, you re-migrated the same set of objects and specified to merge them with the existing objects in the target and move them to target organizational unit B.

3. If you undo migration session 2, the target objects that were merged with the source objects will be moved back to organizational unit A, not to their original location as it was before migration session 1.
In other words, when you undo a session, only changes made by that session are rolled back. Another example of such behavior is the following:

1. Assume a user object was migrated to the target three times in three different sessions. In the last session the Reconnect Exchange mailbox option was selected to reconnect the Exchange mailbox from the source to the target user account.

2. If you undo the first or second session for the migrated user, the mailbox will not be reconnected back to the source account.

Account passwords changed during a migration session cannot be rolled back.

To undo the results of a migration session, select the Migration node in the migration project tree, right-click the session displayed in the right-hand pane and select Undo from the shortcut menu. The Undo Wizard will start.

**Step 1. Select Objects to Revert the Changes for**

This step allows you to select the objects for which the migration should be undone.

To select the objects, you can either click **Select all** or select particular objects by selecting the check boxes next to those objects. Click **Set filter** to specify the object classes for which you want to undo changes. All object classes are selected by default.
Step 2. Reverting Migration Changes

The wizard now removes the migrated objects you selected from the target domain and reverts changes made during the migration session. Wait while the wizard completes.

If the source object was merged with the existing target object during migration, the target object will not be deleted from the target directory during the undo. All changes made to the target object during the merge operation (including moving to another organizational unit and changing attribute values) will be rolled back to the state the object had before the migration and merge.

If errors occurred during the rollback process, you can view more detailed information by clicking View log and inspecting the log file for the failed objects.
Directory Synchronization

Before you start your migration, you should create the domain pairs that will be involved in the migration or synchronization process. Refer to the Creating a Domain Pair section for more details.

If only Active Directory objects are being migrated from one forest to another, then directory synchronization is recommended but not required. If inter-org Exchange messaging system migration is performed, then directory synchronization is mandatory.

Since large migration projects can last for a long time, there is a period when the source and target environments have to coexist and be kept in sync. Migration Manager not only allows you to migrate accounts, but also to continuously synchronize these accounts and groups.

Considerations

- If your migration scenario includes Microsoft Exchange messaging system migration, it is recommended that you set the directory synchronization to create and synchronize objects for which no match can be found in the target directory. This allows you to maintain a unified global address list (GAL) for source and target Exchange organizations, which is important for Exchange migration. See the Migration Manager for Exchange User Guide for more details.

- If you want to use Migration Manager to implement Exchange Resource Forest, configure the Directory Synchronization Agent to create disabled and mailbox-enabled accounts in the target domain. In this case, the Directory Synchronization Agent will automatically add the Associated External Account (msExchMasterAccountSID) attribute to the target accounts. This will let users who still log on to the source domain access mailboxes in the target domain.

- Ongoing synchronization brings over the changes detected in the directory after its last run.

Full re-synchronization deletes the last state information and resynchronizes the directories. It overwrites single-valued attributes and merges multi-valued attributes. For example, if a group has member User1 on the source and the corresponding group has User2 on the target, after you re-sync from source to target the target group will have both User1 and User2.
Directory Synchronization Agent

Both migration and directory synchronization tasks are handled by the synchronization engine called the Directory Synchronization Agent (DSA).

The Directory Synchronization Agent can be installed on any computer in the network running Windows XP or Windows 2003. Please refer to the System Requirements and Access Rights document for details. It can reside locally on the administrator’s workstation or can be installed on multiple computers in the network.

Agent Manager

Agent Manager allows you to install and uninstall the Directory Synchronization Agents in your network and specify configuration parameters for them. You can also see which computers already have agents installed and the migration and synchronization jobs processed by each agent.

To start Agent Manager, in the Migration Manager console, select the Agent Manager command from the Tools menu.

Installing the Directory Synchronization Agent

To install the agent, in Agent Manager select Action | Install, or click the Install button on the toolbar. In the Install Agent dialog, type the name of the server to which you want to install the agent, and click OK.
If you specify a remote server, a remote desktop connection is started and installation is performed in a terminal session. During agent installation, you are prompted for the ADAM instance and the project the agent will work with.

Terminal Services must be running on the remote server to which you want to install the agent. Trust relationships must also be established between the domains where the console machine and the remote server are members.

If for some reason you cannot install remotely, you can install the DSA by running the agent setup package (.msi) locally on that server. The agent setup package is located by default in the \Program Files\Quest Software\Migration Manager\Common\BIN\DeployDistr folder on the console and is also accessible through automatically created share \<ConsoleComputer>\DSASetup\ share.

On the specified server the Quest Directory Synchronization Agent Installation Wizard will start. Complete the wizard to install the DSA.

To uninstall a selected agent, select Uninstall from the Action menu or click the Uninstall button on the toolbar. You also can uninstall an agent by selecting the Uninstall option from the agent’s shortcut menu. Note that if you remove the last agent in a project, you cannot perform any migration activity until a new agent is installed.

**Configuring the Directory Synchronization Agent**

For each Directory Synchronization Agent, you can set a number of parameters. To configure the agent, in Agent Manager, right-click the agent and select Properties.

The Preferences tab of the agent Properties dialog box displays the list of domains that take part in the current project and allows you to specify the preferred domain controllers and Global Catalog servers for each. To decrease possible delays and network traffic during migration and synchronization, for each Directory Synchronization Agent specify the domain controller and Global Catalog server located in the same site as the agent.

Click Edit on the selected domain in the list on the Preferences tab to specify the preferred DC and Global Catalog server for the domain.
Click **Clear** to remove the preferred DC and Global Catalog server settings for the selected domain.

You can also specify the time periods when the agent is allowed to perform its synchronization jobs. To do this, in the agent **Properties** dialog box, click the **Synchronization Schedule** tab.

![Synchronization Schedule Dialog Box](image)

The synchronization schedule you specify does not affect account migration. Migration jobs are processed by the Directory Synchronization Agent regardless of whether the agent is allowed to process synchronization jobs or not.

For example, you may want to prohibit the agent from processing synchronization jobs during normal business hours. To specify the allowed and not allowed hours, select the area in the schedule map and select either the **Synchronization allowed** or the **Synchronization not allowed** option.

The directory synchronization jobs are processed by the agent in sessions. After each session completes, the agent is in an idle state for a time. The default sleep interval is 15 minutes. You can adjust this interval using the **Sleep duration between synchronization sessions** control.

If an agent is running a session and the time period when the agent is not allowed to process directory synchronization jobs begins, the agent will stop processing the current session and enter an idle state until such time as it is permitted to work again. At that time, the agent will continue processing the session from the point where it stopped.

You can set the preferred DC and Global Catalog server, synchronization schedule, and sleep interval for each Directory Synchronization Agent independently.
Configuring the Synchronization Job

The default synchronization job is set for a domain pair as soon as the domain pair is registered in Migration Manager. However, this job is not assigned to any Directory Synchronization Agent, and has only default settings that should be modified to suit your needs.

To configure the synchronization job, right-click the Synchronization node under the appropriate domain pair and select Properties from the shortcut menu.

A DSA cannot synchronize groups with more than 5000 members. Even if you are using Microsoft Windows Server 2003 Forest mode, as recommended by Microsoft, use primary group membership to ensure correct synchronization of large groups.

**Step 1. Select Synchronization Agent**

Select the synchronization agent that will process the synchronization job between the domains in the domain pair. You can select any agent that is installed. If you want to use an agent that is not yet installed, you must first install it using the Agent Manager. Refer to the Directory Synchronization Agent section for details.
Step 2. Select Source Objects to Synchronize

This step allows you to select the source containers for which objects should be synchronized with the corresponding target objects.

The OU hierarchy and the movement of objects between OUs are not synchronized. Both of these operations can be performed during migration sessions.

Select the containers in the displayed source directory tree:

- A blue check mark indicates that all objects from the selected container and all subcontainers will be synchronized.
- A white check mark indicates that only explicitly selected containers will be synchronized.
- A grey check box without any check mark indicates that the container will not be synchronized but some of its sub-containers are selected for synchronization.

Set Filter—This button allows you to filter the specific objects to be synchronized from among all objects from the selected containers. For example, you might want to synchronize only users and groups and not synchronize computers, contacts, and all other objects.

- Object Class—On this tab, you can select from the list the object classes that you want to be synchronized.
- Exclude List—This tab allows you to explicitly select individual objects to be excluded from synchronization. Click Select, and then browse for and select the objects you want to exclude. You can also import objects to be excluded from a plain-text file by clicking Import. In the text file, specify object sAMAccountnames or distinguishedNames, one per line.
Advanced—You can specify a custom LDAP filter expression here. Type the LDAP query in the window and click OK.

Do not create objects on target (only merge them)—If this option is selected, no new objects will be created on target during synchronization. Only objects that already exist on target will be synchronized.

Create objects in—You can select whether the agent should create the objects on the target and select the container where the objects should be created. If this option is selected, all the new objects that do not exist on target will be created in the specified container. Click Browse to select the container from the target directory tree.

If you select the Create objects in option, then for each source object for which the Directory Synchronization Agent cannot find a match in the target domain, it will create a new object in the OU you specify.

If Exchange options are also configured in the directory synchronization job, the Directory Synchronization Agent will mailbox-enable target accounts if their corresponding source accounts are mailbox-enabled.

However, if a conflict by e-mail addresses (the proxyAddresses attribute) arises when creating a mailbox for the newly-created target account, the agent will behave as follows:

- If the conflict is not critical (for example, some e-mail addresses cannot be applied for the target account), the account will be created in the target domain and mailbox-enabled normally. However, it will not have the conflicting addresses in its proxy address list.
- If the conflict is critical (for example, the agent cannot apply the target address for mail-enabled objects), the account will still be created in the target domain. It will be mail-disabled and will be added to the failed queue.

Disable target accounts—By default the agent creates the target accounts as disabled accounts. If you want the state of the target account to be copied from the source account, clear this check box.
Step 3. Set Security Settings

This step allows you to specify the security settings for the synchronization.

Security Descriptor migration rule—If two objects, source and target, are matched during synchronization by any matching criteria, you can select the way security descriptors of these objects will be handled.

For more information about objects matching criteria, refer to the Configuring a Domain Pair section.

If the accounts are merged during synchronization, you have the opportunity to Merge, Replace, or Skip the security descriptors:

- **Merge**—The security descriptor entries of the source objects will be added to the security descriptors of the target objects.
- **Skip**—The security descriptors of the target objects will be left intact.
- **Replace**—The entries of the target object security descriptor will be replaced with those of the source objects.

Add SIDHistory—Select this checkbox if you want to allow the target accounts to access the source domain resources using SIDHistory mechanism during the coexistence period.

To make users access the resources in the source domains by SIDHistory, trusts must be established between the source and target domains.

The User Principal Name handling section allows you specify how User Principal Names (UPNs) will be processed:

- **Synchronize**—If this option is selected, source User Principal Names will be assigned to the target users.
- **Skip**—If this option is selected, the target user UPN will be left intact.
- **Set the domain suffix of the UPNs to**—Allows you to set the domain suffix of the UPNs of the target users to the value you specify.

**Synchronize passwords**—Select this checkbox if you want to synchronize passwords for the accounts.

If one-way directory synchronization is established, the source account’s password will be applied to the target account only if it is newer than the one of the target account. No passwords will be applied from target to source accounts even if the target accounts’ passwords are newer.

In the case of two-way directory synchronization, the newer password values are synchronized to the opposite directory (that is, passwords are synchronized in both directions).

These rules apply to both initial and delta synchronization.

**Step 4. Select Target Objects to Synchronize**

This step allows you to select the target directory objects that should be synchronized with the corresponding source objects. You can also select whether the agent should create the objects on the source and select the container where the objects should be created.

**Do not create objects on source (only merge them)**—If this option is selected, no new objects will be created on source during synchronization. Only the objects that already exist on source will be synchronized.

**Create objects in**—You can select whether the agent should create the objects on the source and select the container where the objects should be created. If this option is selected, all the new objects that do not exist on target will be created in the specified container. Click **Browse** to select the container from the source directory tree.
**Step 5. Specify Advanced Options**

If you are planning to use a custom add-in to process the selected objects after they have been retrieved from the source domain and before they are synchronized to the target domain, select the **Use custom add-in** check box and browse for the `.xml` custom add-in file.

If you want object deletions to be synchronized as well, select the **Synchronize object deletions** check box. If an object in the source domain was deleted, the Directory Synchronization Agent will delete it from the target domain.

- If an object is deleted on a Windows 2000 Server domain controller in the source domain, it is not deleted from the target domain regardless of scope settings; a message like the following is written to the DSA log:

  For safety reasons deletion of following objects will not be synchronized, being propagated by DC running Windows 2000 Server.

- Deletion of the matched objects in the target organization is not synchronized from target to source even if the "Synchronize object deletions" option is enabled in the synchronization properties. As a result, the source objects are not affected if the matched target objects are removed. To change the default behavior, refer to instructions in the Quest KB article [https://support.quest.com/SUPPORT/index?page=solution&id=SOL21332](https://support.quest.com/SUPPORT/index?page=solution&id=SOL21332).
Attributes to Skip

Select the check boxes next to the attributes you do not want to synchronize.

Use the **Save Settings** button if you want to use the same settings when you create another migration session. Click **Load Settings** to apply a set of attribute skipping options you saved earlier.

**Direction**—Click this button to specify the type of synchronization during which the attribute should be skipped:

- **Two-way Sync**—Select this option to skip the attribute from being applied on either side.
- **Source-to-Target Sync**—Select this option if you do not want to apply the attribute on target.
- **Target-to-Source**—Select this option if you do not want to apply the attribute on source.

Select the **Show advanced attributes** check box to choose from the complete list of attributes you can skip.

The Directory Synchronization Agent service attributes used by Migration Manager should never be skipped. Otherwise, Migration Manager will not be able to migrate and synchronize objects.
**Step 6. Specify Exchange Options**

If Exchange migration is planned for after directory migration, you may want to specify some options required for further Exchange messaging system synchronization. To do so, select the **Apply Exchange** options check box.

- This step is displayed only when Exchange Server is installed in both the source and target forests.
- If Exchange object browsing does not work on this page, make sure that the Directory Synchronization Agent account is configured correctly, as detailed in the **Accounts Used by the Directory Synchronization Agent** section of the **System Requirements and Access Rights** document.

The Directory Synchronization Agent can create a mailbox for the accounts being synchronized if they do not have mailboxes yet. You can select the Exchange servers and mailbox stores where the mailboxes will be created.

**Target mailbox store**—Specify the mailbox store to mailbox-enable the target account if the source account is mailbox-enabled.

**Source mailbox store**—Specify the mailbox store to mailbox-enable the source account if the target account is mailbox-enabled.

For uninterrupted user collaboration during the migration, users in each source and target Exchange organization should see other users’ mailboxes in their Global Address Lists. That is why two mailboxes, source and target, exist for each user. However, all mail sent to the user should arrive to the mailbox he or she is currently using, no matter which mailbox it was sent to. To achieve this, mail should be automatically forwarded to the currently-used mailbox from the other mailbox.

Direct forwarding to a recipient in another Exchange organization can be done by using the target address property of the mailbox.
For mail redirection purposes, the Directory Synchronization Agent adds the secondary SMTP address to the proxy addresses list of the mailbox-enabled object (attribute: proxyAddresses). You can specify the SMTP address templates to create the secondary SMTP addresses that will be applied to the source and target mailbox-enabled objects.

You should analyze your environment for SMTP namespaces and for redirection implement SMTP address templates that are NOT being used.

To forward mail to a recipient in another Exchange organization, the Directory Synchronization Agent populates the target address property (the targetAddress attribute) of either the source or target mailbox, depending on which mailbox is currently being used, with the additional SMTP address created for redirection.

**Target SMTP address template**—Specify the SMTP address template for the target accounts so that the target users receive their mail during the synchronization.

**Source SMTP address template**—Specify the SMTP address template for the source accounts so that the source users receive their mail during the synchronization.

If contacts with the same SMTP or X500 address as the synchronized objects already exist in the opposite directory, Migration Manager can merge SMTP and X500 addresses and membership for these objects and delete the corresponding contacts. To use this functionality, select the **Merge objects with corresponding contacts** check box.

**Starting and Stopping Directory Synchronization**

After you have configured the directory synchronization job for a pair of domains, you can start this job. To start directory synchronization between a pair of domains, complete the following steps:

1. In Migration Manager console, expand the domain pair node in the left-hand pane.
2. Right-click the **Synchronization** node and select **Start and Re-sync** in the shortcut menu. The **Job status** on the **Synchronization Statistics** screen is displayed as **Starting**.
3. Wait until the **Last operation progress** parameter for the **Start operation** reaches 100% on the **Agent Statistics** screen in the right-hand pane.
Use the **Synchronization Statistics** and **Agent Statistics** screens to track the synchronization job status and progress. For more information about viewing the directory synchronization statistics, refer to the **Viewing Directory Synchronization Statistics** section.

The first time you start a synchronization job, the first Directory Synchronization Agent session starts and full resynchronization takes place. The job status on the **Synchronization Statistics** screen is displayed as **Initial synchronization**. All objects in source domain and also objects in target domain if two-way synchronization is performed, are enumerated during the initial sync, but only the objects from the specified source and target scopes are synchronized. After the first synchronization session is completed, only delta changes are synchronized during the subsequent sessions.

**To stop directory synchronization between a pair of domains, complete the following steps:**

1. In Migration Manager console, expand the domain pair node in the left-hand pane.
2. Right-click the **Synchronization** node and select **Stop** in the shortcut menu. The **Job status** on the **Synchronization Statistics** screen is displayed as **Stopping**.
3. Wait until the **Last operation progress** parameter for the **Stop operation** reaches 100% on the **Agent Statistics** screen in the right-hand pane.

The following changes to the synchronization job require full directory resynchronization:

- Changing the source scope (adding containers to the synchronization scope or removing them)
- Changing the target scope (adding containers to the synchronization scope or removing them)
• Changing Security options
• Changing Advanced options
• Changing Exchange options

The following changes made to the domain pair configuration also result in full directory re-synchronization:

• Changing the service attributes
• Applying conflict resolution rules

**Viewing Directory Synchronization Statistics**

When you select the Synchronization node under the domain pair in the migration project tree, you can see synchronization state, progress, and statistics for the selected pair of domains on the screen in the right-hand pane.

**Synchronization Statistics**

The following information is provided on the Synchronization Statistics screen:

**Job status:**

• **Initial synchronization**—Indicates that initial synchronization (full re-sync) is going on. Either this is the first synchronization session for the Directory Synchronization Agent or synchronization was re-started with Start and Re-sync option.

• **Delta synchronization**—Indicates that the initial synchronization is completed and only delta changes are synchronized.

• **Sleeping**—Indicates that the Directory Synchronization Agent is in an idle state, either because it is in a sleep interval between synchronization sessions or due to its schedule restrictions. Refer to the Configuring the Directory Synchronization Agent section for more details.

**Job direction:**

• **Source to target**—Indicates that synchronization job is configured to synchronize objects from source to target only (only the source scope is set).

• **Target to source**—Indicates that synchronization job is configured to synchronize objects from target to source only (only the target scope is set).

• **Two-way**—Indicates that both source and target objects will be synchronized (both source and target scopes are set).

**Synchronized objects**—Displays the number of object pairs that were matched and synchronized.

**Source objects per minute**—Shows the approximate speed of the source-to-target synchronization process

**Target objects per minute**—Shows the approximate speed of the target-to-source synchronization process
Directory errors—Shows the number of errors that occurred during synchronization, such as connection errors, invalid credentials errors, and server unavailability errors. Click View next to the counter to see the list of errors.

The Directory errors queue is not dynamic and errors put in this queue are not removed from the queue even after they are resolved.

You also can view the queues of conflicts found during synchronization, failed objects, and unresolved objects. Click the corresponding View link for detailed information.

Conflicts—This queue contains the object-matching conflicts.

Failed objects—This queue contains issues that occurred to the synchronized objects and their attributes, such as if an object could not be created due to insufficient rights.

Unresolved objects—All unresolved linked attributes, such as unresolved membership, are put in this queue.

The Conflicts, Failed objects and Unresolved objects queues are dynamic, so if, for example, a conflict is resolved, it is thrown out of the queue.

Agent Statistics

Name—The name of the server running the agent.

Last operation—The last operation description the agent was instructed to perform (such as start or stop).

Last operation progress—The last operation’s progress (in percent).

Last operation error code—If the last operation completed successfully, this field is blank. If the operation failed, the error code is displayed.
Resource Update

Overview

In Active Directory, permissions are assigned to users via Access Control Lists (ACLs). The list contains references to security identifiers (SIDs) of the accounts to which the rights are granted.

To ensure that resources will still be available to users when they start using their target accounts and when you have cleaned up SIDHistory, permissions granted to source accounts to access the resources must be re-assigned to the target accounts. This means that ACLs of all the resources in the network need to be processed to refer to the new SIDs.

Service accounts and accounts used to run scheduled tasks must also be changed to the corresponding target accounts to ensure that services and scheduled tasks will run correctly after the source accounts are disabled. This is done during the resource update phase.

The resources can be divided in two groups:

1. Distributed resources, such as end-user workstations, file and print servers, servers running IIS, scheduled tasks, and other services and applications
2. BackOffice servers, such as Exchange, SQL, and SMS

To make the migration transparent to users, Migration Manager for Active Directory uses a set of tools to provide automated resource processing to reflect the domain reconfiguration. These tools are described in the table below.

<table>
<thead>
<tr>
<th>RESOURCE UPDATE TASK</th>
<th>DESCRIPTION</th>
<th>TOOL USED</th>
<th>REFERENCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distributed resource update</td>
<td>Update ACLs for distributed resources, service accounts, user profiles, etc., including those residing on cluster servers</td>
<td>Resource Updating Manager</td>
<td>See the Resource Updating Manager section.</td>
</tr>
<tr>
<td>Active Directory update</td>
<td>Update security descriptors for Active Directory objects in selected domains</td>
<td>Active Directory Processing Wizard</td>
<td>See the Active Directory Processing section.</td>
</tr>
</tbody>
</table>
### Resource Update Scenarios

Resource update can be performed in two ways:

- Centrally, from the Migration Manager console. You need to create and start a resource processing task of the desired type, as listed in the table above. To create the task, in Migration Manager go to the **Resource Processing Tasks** node and click the corresponding button in the right pane. See the sections listed in the table for more details.

- Locally, by delegating resource processing tasks to other persons, for example, to site administrators who are responsible for the resources in their location and already have the appropriate permissions to update them. There are two ways to delegate resource processing tasks:
  
a) Create a setup package for a resource processing task and send it to the person who will update resources. That person installs the package and runs the task.

b) Create a self-contained export INI file with the resource processing settings. Resource processing is later performed in stand-alone mode from the resource updating tool (see the table above) or from the command line by specifying this INI file. Refer to the **Delegating Resource Update** section for more details.

<table>
<thead>
<tr>
<th>RESOURCE UPDATE TASK</th>
<th>DESCRIPTION</th>
<th>TOOL USED</th>
<th>REFERENCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Systems Management Server update</td>
<td>Update Systems Management Server permissions</td>
<td>SMS Processing Wizard</td>
<td>See the SMS Processing section.</td>
</tr>
<tr>
<td>SQL Server update</td>
<td>Update permissions on SQL servers</td>
<td>SQL Processing Wizard</td>
<td>See the SQL Server Processing section.</td>
</tr>
<tr>
<td>SharePoint permissions update</td>
<td>Reassign SharePoint permissions after your migration</td>
<td>SharePoint Permissions Processing Wizard</td>
<td>See the SharePoint Processing section.</td>
</tr>
</tbody>
</table>
Selecting Objects for Processing Explicitly

By default, a resource processing task processes the resources for all objects migrated by the time the task is created. However, you can manually select objects you want to update the resources for. This is done by creating a custom map for the resource processing task.

To create a custom map

1. Select the resource processing task under the Tasks node.
2. Click Select Objects to Process Resources in the right pane.
3. In the dialog that appears, select the objects you want to update the resources for.
4. Click OK.

A custom map is applied only to the task for which it was created. If no custom map is defined for a task, the resources processed by that task will be updated for all migrated objects.

To delete a custom map

1. Select the resource processing task under the Tasks node.
2. Click Delete Custom Map in the right pane.
3. Click Yes.

Resource Update Considerations

Here are the factors to keep in mind when doing resource updates:

- The more objects a computer has (in most cases, this means the more files and folders), the longer it takes to process. Thus, it takes much longer to process a file server than a workstation. You may want to perform server processing during non-business hours to ensure that no users are affected by a possible server slowdown.
- Updating NTFS permissions requires a lot of disk access (I/O) operations and can slow the server for a period of time.
- Each computer in a set is processed by its own agent. Thus, all the computers are processed in parallel and it takes about as much time to process a dozen workstations as a thousand.
  
  Please consider that when resources are processed remotely, computers are handled in turns. As compared with resources processing using the agent, remote processing takes significantly more time.

- Expect about 10% (depending on the environment) of your workstations to require troubleshooting because either they are offline, the Server service is not running, the domain administrators were removed from the local Administrators group, or there is some other problem.

It is recommended that you create separate lists for end-user workstations and servers and process workstations first and then servers.
Resource Updating Manager

Overview

Resource update is among the most challenging tasks of a migration. While directory data is usually centralized, the resources (servers and end-user workstations) may be spread over domains, sites, buildings, offices, and countries. Resource Updating Manager is the main tool that lets you automate the update of various resources in your network.

After performing a directory migration, Resource Updating Manager is used to update resources so that the new users have the same permissions in the target domain as the corresponding users have in the source domain.

Resource Updating Manager facilitates resource update by automating the following tasks:

- Processing of all the selected computers in parallel
- Updating permissions, ownership information, and auditing on registries, shares, folders, and printers
- Updating local group membership
- Updating user rights and privileges
- Updating local user profiles
- Updating roaming user profiles
- Updating services and scheduled tasks
- Updating Internet Information Server (IIS) permissions
- Updating DCOM and COM+ objects’ permissions
- Restoring to a previous state with advanced undo and cleanup
- Moving computer accounts to the target domain without rebooting them and changing the last logged-in domain to the target domain
- Processing published resources when moving computers to the target domain

To handle large, geographically dispersed networks, Resource Updating Manager can be distributed using Group Policy or SMS.

One of the main features of Resource Updating Manager is parallel processing during resource migration: the actual resource processing is performed locally on each migrated computer. Because all the selected computers are updated simultaneously, 1000 resource servers can be updated in the same time required to update 10 servers.

Legacy Components under the COM+ node are processed by Resource Updating Manager only if you select the DCOM option before starting resource processing.
Starting Resource Updating Manager

To start Resource Updating Manager, in Migration Manager console management tree expand the Resource Processing node and click Tasks. In the right pane of the Migration Manager console click Resource Updating Manager.

Before You Update Resources

Before you start processing resources in your network, you should complete the tasks described below.

Obtaining Administrative Rights over the Computers

For a successful resource updating you must have administrative rights over the computers involved in the process.

Resource Updating Manager uses two service accounts when performing resource updating tasks. These accounts are:

- **Migration Manager RUM Controller service** account, used to:
  - Run the Migration Manager RUM Controller Service on the console computer
  - Access a computer to install or uninstall the Resource Updating Agent, if no other account is explicitly specified for domain

- **Migration Manager RUM Agent service** account used to run the Migration Manager RUM Agent service on the computers to be processed

  Migration Manager RUM Agent cannot work with multiple instances of Resource Updating Manager console or Migration Manager RUM Controller service.

Migration Manager RUM Controller Service Account

By default, the Migration Manager RUM Controller Service uses the auxiliary account. You can change the Migration Manager RUM Controller Service account using the Tools | Manage Controller Credentials option in the Resource Updating Manager console menu.

The Migration Manager RUM Controller service account must have the following permissions:

- Member of the local **Administrators** group on the computer running the Resource Updating Manager
- Full Admin access rights on ADAM database. Right-click the migration project node in the Migration Manager console management tree and select Delegate from the shortcut menu to assign these rights to the Migration Manager RUM Controller service account.

  By default, the Domain Admins group of the domain the computer is a member of a computer's local **Administrators** group. You will get administrative access to the computer if the account you are using is a member of the source Domain Admins group.
Migration Manager RUM Agent Service Account

To specify the Migration Manager RUM Agent service account for Migration Manager RUM agents installed using the Resource Updating Manager console, use the Tools | Manage Domains Credentials option in the console menu.

The Migration Manager RUM Agent service account must be a member of the local Administrators group on the computers running the Migration Manager RUM Agent.

If the Migration Manager RUM Agent service account is not specified, the Local System account (default) will be used.

Pre-installing Resource Updating Manager Agents

Usually, Resource Updating Manager Agents are installed to the computers you want to process directly from Resource Updating Manager console. If many computers are involved, this may cause excessive network traffic and slow down resource processing process. To avoid this, you can deploy Resource Updating Manager Agents on the computers you want to update using Group Policy, SMS Server and similar tools, or manually.

To create agent setup

1. Either log on to the console with an account that has administrative rights over the computers, or establish an administrative connection to the computers using the net use command. See the Obtaining Administrative Rights over the Computers section for more details.
2. In the Resource Updating Manager console toolbar, click Tools | Create Agent Setup.
3. Specify credentials for the Migration Manager RUM Agent service account and folder path to save setup files.

The setup package consists of the *.msi file (which provides the setup engine) and the Windows folder with the actual package contents. Both of these parts must be available together for successful agent deployment.

After the Resource Updating Manager Agents were successfully deployed to the computers using agent's setup, these computers appear in the right pane of the Resource Updating Manager console. If they were never added to the groups (either from Active Directory or from Network), they stay under the Unconfigured category.

If You Used Aelita Domain Migration Wizard or Aelita Enterprise Migration Manager 5.x/6.x Agents

If Aelita Domain Migration Wizard or Aelita Enterprise Migration Manager 5.x/6.x agents were used to update resources on some computers and were not removed, they will not be overwritten by Resource Updating Manager Agents. You should remove the old agents first (using either Domain Migration Wizard or Enterprise Migration Manager 5.x/6.x) and then install Resource Updating Manager Agents. Domain Migration Wizard 5.x/6.x can use Enterprise Migration Manager agents as well.
Specifying the Processing Scope

Before you start resource processing, the processing scope should be determined. You should create collections and include the computers you want to process. A collection contains computers and defines processing settings for them.

By default, you can work only with those collections that were created in the Resource Updating Manager console on the current computer. To gain access to collections created from other instances, disable the View | Show only collections created from this computer option in the main menu.

Creating Collections

To create a collection, in the left pane of the Resource Updating Manager console, right-click the Collections node and select Create Collection. Specify the collection name and an optional description, then add the computers you want using the Included Computers dialog box. The created collection node will appear under the Collections node in the console management tree.

Adding Computers to a Collection

To add computers to a collection, right-click the collection node and use the options in the Add Computers sub-menu.

To add computers from Active Directory

1. Right-click the collection node and select Add Computers | From Active Directory.
2. In the Add Computers from Active Directory dialog box click Browse.
3. In the Select Location dialog box that appears expand the tree, browse to the container where computers you want to process are located, and then click OK. The list of computers located in the selected container will be displayed in the Computers list.
4. Select the check boxes next to the names of computers you want to add to the processing scope or click Select All.
5. Click OK to close the dialog box.

To add computers from the network

1. Right-click the collection node and select Add Computers | From Computer Browser.
2. In the Add Computers from Computer Browser dialog box select the domain from the Domain drop-down list. The list of computers located in the specified domain will be displayed in the Computers list.
3. Select the check boxes next to the names of the computers you want to add to the processing scope or click Select All.
4. Click OK to close the dialog box.

Please consider the following:

- If a computer is offline, you cannot add it to a collection.
- Resource Updating Manager may not discover computers with an enabled firewall. Pay attention to computers running Microsoft Windows Vista and later, because the firewall is enabled by default on such computers.
To add computers from a file

1. Right-click the collection node and select Add Computers | From Text File. You are prompted to add computers listed in an import file prepared in advance.
2. In the file selection dialog box, select the import file and click Open.

The import file is a text file with two tab-separated columns. Every line should contain a computer you want to process, in one of the following formats:

- NetBIOS name with an optional domain NetBIOS name in the second column
- FQDN
- IP address

You can write your comments in the file after the * character.

Example:

*This is a comment
\\ComputerName1 NetBIOSDomainName
\\ComputerName2
ComputerName3 NetBIOSDomainName
ComputerName4
computername5.domainname.corp
12.34.56.78

Import files exported from Resource Updating Manager console in Migration Manager version 8.3 and earlier are also supported.

To add a specific computer

1. Right-click the collection node and select Add Computers | Single Computer option.
2. Specify the name of the computer you want to add and the domain that the computer is a member of.

To add computers from an existing migration project

1. Right-click the collection node and select Add Computers | From Migration Project. You are prompted to specify computers included in a migration project.
2. In the Add Computers from Project dialog box select the check boxes next to the migration scopes that you need.
3. Click OK to load all the computers in the selected scopes.

After computers are added to the collection, they appear in the right pane of the Resource Updating Manager console.
Specifying Preferred Master Browser

Resource Updating Manager cannot perform the Add Computers from Network and Add Computers from File operations (excluding cases when domain name is specified for all computers in the import file) if the information about domains in the network is not complete on the Computer Browser servers.

You can set a Preferred Master Browser or the domain in which it is located to use the specified Preferred Master Browser later for enumerating domains in the network.

Take the following steps:

1. Run Registry Editor and browse the HKEY_LOCAL_MACHINE\SOFTWARE\Aelita\Migration Tools\CurrentVersion\Resource Updating Manager registry key (or the HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Aelita\Migration Tools\CurrentVersion\Resource Updating Manager registry key on a computer running a 64-bit version of Microsoft Windows). If this key is absent from the registry, create it.

2. Create a new PreferredMasterBrowser string value in the key. Specify either the NetBIOS name of Preferred Master Browser or NetBIOS name of the domain in which Preferred Master Browser is located, as follows:

   DomainName
   
   or

   \\PreferredMasterBrowserName

   When specifying a domain name, do not add two backslashes before it. However, you must type two backslashes (\) before the name of Preferred Master Browser. Any time you edit the registry, you must restart Resource Updating Manager console.

Removing Computers from a Collection

To remove a computer from a collection, right-click the computer in the right pane of the Resource Updating Manager console and select Remove.

Discovering Computers

Before starting to process computer resources, Resource Updating Manager discovers the computers included into the processing scope and collects various statistical information, including the following:

- Operating system installed
- Operating system architecture

Also, Resource Updating Manager provides information about computer status and task results.
To view computer information, right-click a computer and select View History. The following information is displayed:

- List of performed tasks
- Task operation date and time
- Computer status
- Error description (if any)
- Resource Updating Manager Agent status
- Last operation date and time

To view the information about a specific task, go to the Task tab in the right pane in the Resource Updating Manager console, then right-click the task and select View Results.

Importantly, Resource Updating Manager agents are installed on the computers as part of the discovery process.

**Discovering Specific Computers or Collections**

To start discovery of a particular computer or collection, right-click it and select Create Task | Discovery.

In the Task Schedule dialog box you can specify when the task starts. You can start the task immediately by selecting the Start task now option or select the Start task at option to specify the date and time to start processing. On the same step, you can specify the pending timeout for the task operation in case some computers are not accessible at the task start time.

To decrease network traffic it is recommended that you discover and process your resources during off-peak hours.

**Sorting Computers**

This step is not required, but before you start resource processing you may want to revise your collections, depending on the statistics collected during computer discovery.

Create new collections if necessary, as described in the Specifying Processing Scope section, and use drag-and-drop to reorganize computers.

One useful technique is to sort computers by the results of the most recent task. For example, you can select only the computers for which the latest task failed, and retry the operation for them.

**Processing Resources**

After migrating the Active Directory data of the selected users and groups, you must update resources in Resource Updating Manager for the new users and groups so that they have the same permissions as the corresponding users and groups in the source domain.

For a successful resource update you must have administrative rights over the computers involved in the process. See Obtaining Administrative Rights over the Computers for details.
In Resource Updating Manager, updates usually involve the followings steps:

1. Process the security settings.
2. Move the computer to the target domain.
3. Remove the old security settings.

This is done by applying tasks to computer collections. Tasks can be either scheduled or queued directly one after another. If you want to run an uninterrupted series of tasks on a collection, create these tasks for it in the order you want them to run, and use the **Start task now** option as the schedule for each task. Alternatively, schedule these tasks in the correct order with very short intervals between them. This will queue the tasks individually for each computer in the collection.

Note that a queued task will wait for the preceding task to end, but if one of the tasks fails, then subsequent queued tasks will be cancelled.

For details about processing, move and cleanup tasks, see the following sections.

**Start Processing**

Follow these steps to process the resources in Resource Updating Manager:

1. In the Resource Updating Manager console management tree right-click the node of the collection you want to process.
2. Select **Create Task | Processing** in the shortcut menu. The Create Processing Task wizard starts.
3. On the Task Action step, select the action you want to perform.
4. On the Handling Rights and Resources step, select the types of rights and resources to process.
5. On the Advanced Options page, configure advanced options for the task.
6. In the Task Schedule dialog box you can specify when the task starts. You can start the task immediately by selecting the **Start task now** option or select the **Start task at** option to specify the date and time to start processing. On the same step, you can specify the pending timeout for the task operation in case some computers are not accessible at the task start time.
7. On the Task Description step you can specify an optional task description.
8. Click **Finish** to start processing.

For more details, see **Configure Processing Settings**.

Resource Updating Manager will perform the updates for security principals that were migrated when Resource Updating Manager was started.

However, you can manually define the objects you want to update the resources for. To define a custom selection of security principals, right-click the collection node in the console management tree and click **Select Custom Map**.

While the resource update is in progress, you can safely quit Resource Updating Manager, because the tasks are performed on the remote computers. As soon as all the agents have finished performing the specified tasks, Resource Updating Manager will collect the logs from the processed computers.
Configure Processing Settings

You can configure the following using the Create Processing Task wizard:

**Task Action**

On the Task Action step, select the action you want to perform:

- **Reassign local group membership, user rights, and object permissions to target users**
  This will update resources to conform to the domain reconfiguration.
  
  The Leave source accounts' permissions check box allows you to add newly created users and groups from the target domain to object DACLs and SACLs, rather than replace the entries with the current source account SIDs.

- **Clean up legacy local group membership, user rights, and permissions of migrated users**
  Remove references to the original source accounts after migration. See the Resource Cleanup section for details.

- **Revert to the original local group membership, user rights, and object permissions**
  Select this option to undo the update.

Handling Rights and Resources

On the Handling Rights and Resources step, select what accounts should be updated:

- **Local Group Membership**
  Adds target accounts to the local groups that contained the corresponding source accounts. If the Leave source accounts' permissions check box is not selected, the source accounts will be removed from the groups.

- **User Rights**
  Grants target accounts the user rights which belonged to the corresponding source accounts. If the Leave source accounts' permissions check box is not selected, the source accounts will be denied the rights they had.

- **Service Accounts**
  The Service Accounts check box allows you to update service accounts and permissions affected by the migration. For example, if a service runs as SOURCE\User1 and User1 is moved to the target domain, the service account credentials will be changed to those of TARGET\User1.

  - Service accounts are replaced whether or not the Leave source accounts' permissions option was selected.
  - If the processing service is running under a source account while a user logs in under a new corresponding target account, duplicate profiles can be created.
• Scheduled Tasks

The Scheduled Tasks check box allows you to update scheduled task accounts and permissions affected by the migration. For example, if a task runs as SOURCE\User1 and User1 is moved to the target domain, the task account credentials will be changed to those of TARGET\User1.

- Scheduled task accounts are replaced whether or not the Leave source accounts' permissions option was selected.
- For a successful scheduled task update, trusts should exist between source and target domains and the account should have the Read and Write permissions on the scheduled task file.
- If the scheduled task is running under a source account while a user logs in under a new corresponding target account, duplicate profiles can be created.

Then select the check boxes next to the objects whose permissions should be reassigned to target users. Permissions on the following objects can be updated:

- Registry
- Local profiles
- Roaming profiles
- Shares
- Printers
- File system
- IIS
- DCOM
- COM+
- File ownership

If you select the IIS check box, Resource Updating Manager will update the permissions of the Internet Information Services (IIS) if it is installed on the selected computers. The following IIS properties are processed by default:

- Microsoft Windows discretionary access control list (DACL) (the AdminACL property)
- Name of the registered local user that is used for anonymous users (the AnonymousUserName property)

To process any other IIS properties, you need to use the Vmover utility in manual mode. First, prepare the configuration file, Vmover.ini. The properties you need should be included in the [IIS Identifiers] section of the file as follows:

[IIS Identifiers]
UNCUserName=yes;1

The number at the end of the string specifies the property type:

- 0—security descriptor
- 1—user name
- 2—domain name

If the property type is not specified, the property will be skipped during processing.

Next, run Vmover remotely on the IIS servers you need to process using the edited configuration file, as follows:

`Vmover.exe /c /system=<IIS_server_name> /ini=<updated_INI_file>`
After processing printers, if some of them were processed via the registry (this can be verified by scanning the log file), the spooler should be restarted.

**Advanced Options**

On the Advanced Options step, you can configure additional options for the task:

- Select the **Process resources remotely (without agents)** check box to force Resource Processing Manager to process only remote resources.

  In this case only several types of objects will be processed, for example, shares. This option is needed for NetApp processing.

- Whether any script should be run on the processed machines before or after processing. Click **Browse** to specify the script file (the following file types are supported: *.vbs, *.js, *.bat, *.cmd, *.ps1).

  Note: Resource Updating Manager agent is a 32-bit application. So, when Resource Updating Manager agent runs scripts on a processed computer running a 64-bit operating system, all scripts will be launched in 32-bit mode.

**Moving Computers to Another Domain**

Once you have completed the migration of users and collections, you can choose to move the source computers to another target domain. Actions that must be performed in these cases are described in this section.

**Start Moving Computers**

Follow these steps to move computers to another domain in Resource Updating Manager:

1. In the Resource Updating Manager console management tree right-click the computer you want to move.
2. Select **Create Task | Move** in the shortcut menu.
3. On the Move Options step, specify where and how to move computers. For more details, see *Configure Move Computers to Domain Settings*.
4. On the Grant Local Administrator Privileges step, select the accounts that will be added to the local **Administrators** group on the computers you are going to move.
5. On the next step, specify when the computer will be restarted to complete the move operation. For more details, see *Configure Move Computers to Domain Settings*.
6. In the Task Schedule dialog you can specify when the task starts. You can start the task immediately by selecting the **Start task now** option or select the **Start task at** option to specify the date and time to start processing. On the same step, you can specify the pending timeout for the task operation in case some computers are not accessible at the task start time.
7. On the Task Description step you can specify an optional task description.
8. Click **Finish** to start processing.
If there are any shared folders or printers published in Active Directory on the computer being moved to the target domain, they should first be migrated to the target domain along with the computer account they are pointing to using Migration Manager. This will allow Resource Updating Manager to automatically update the resources that reside in the source and target domains after moving the computer to point to the target computer account.

- If there are only printers located under the computer account, there is no need to migrate them before moving the computer to the target domain. In this case, computer account will be created automatically, the spooler will be restarted and printers will be created pointing to the new account.
- If you click Cancel during a computer move or stop the service, further processing will be stopped. In this case and in the case when processing is stopped due to an error, computers that have not been moved by that moment will be left intact.
- Resource Updating Manager cannot move domain controllers, cluster servers, non-Windows computers, and unknown computers between domains.
- See the Moving Exchange Server to Another Domain section for information on how to move Exchange Servers.
- For information on how to move SMS servers to another domain, see the Moving SMS Servers Between Domains technical paper by Microsoft.

**Configure Move Computers to Domain Settings**

On the Move Options page, select the target domain from the list. In addition, you have the following options:

- **Change last logged-in domain to the target domain**
  If you want the last logged-in domain in the drop-down list in the logon window to be changed to the target domain after moving the computer, select this check box.

- **Preserve computer account in source domain**
  To ensure that valid accounts are available for logon in case of problems, select this check box. This option will cause the source accounts to be kept, but disabled.

If you do not use the Resource Updating Manager console when moving computers with the Resource Updating agent installed between domains, please consider the following:

- The Migration Manager RUM Agent service account must be a member of the local Administrators group on the computers running the Migration Manager RUM Agent both in the source and target domains.
- The Migration Manager RUM Agent service account must have the Logon As Service right in target domain

On the Computer Restart Options page, the following additional settings are available:

- The message to show to the currently logged-on user when the computer is about to restart.
- The delay between the message and the actual restart (that is, how much time users have for saving their work).
• Whether to forcibly close applications with unsaved data during restart.

If you select not to restart the computers after they join a different domain, you will need to tell the users to restart manually.

**Moving Exchange Servers to Another Domain**

If the target domain has never had an Exchange Server installed in it, you must take the following steps before you move the server. If the target domain already has (or has ever had) an Exchange Server installed, skip these steps.

1. If you haven't already done so, run **DomainPrep** in the target domain. This will create the necessary groups for Exchange, including Exchange Enterprise Servers and Exchange Domain Servers.
2. Use ADSIEdit and browse to Domain.com/Configuration/Services/Microsoft Exchange. Right-click Microsoft Exchange and add the target domain's Exchange Domain Servers group to this container with Read permissions. Make sure that this permission is applied to this object and all child objects.
3. Browse to the Org container and add the target domain's Exchange Domain Server group with the Create all child objects and Administer information store rights. Again, make sure that this is applied to this object and all child objects.

   The above permissions are normally added with the first installation of an Exchange Server to the domain.
4. Follow the procedures in the Microsoft Q297295 article.

**Moving Cluster Servers to Another Domain**

To move a cluster server where all nodes are member servers of some domain to a different domain, select all the nodes and move them simultaneously. After a couple of minutes all nodes and the virtual server will appear in the new domain.

   Always move all cluster nodes to the new domain simultaneously. Do not move a virtual server to the new domain.

Resource Updating Manager can process NTFS permissions, shares, local groups, privileges, registry, cluster shares, cluster database (registry), and cluster printers. Here is the procedure:

1. Select all of the nodes in Resource Updating Manager.
2. Specify the processing settings and process the nodes as regular computers. This will process all resources except the cluster shares, cluster database, and cluster printers.
3. Create the INI file and specify the required options.
4. Use Vmover with command line options, as follows:

   Vmover.exe /c /system=<Cluster Name> /ini=<Vmover.ini path>
This will process the cluster shares, cluster database, and cluster printers.

Vmover will not process a computer if it cannot verify whether it is a cluster server or a virtual cluster server. If the cluster node alias is specified as a computer name, Vmover cannot verify it is a cluster. In all other cases the cluster will be uniquely verified.

**Task Scripting**

You can create a custom task and run it using the Create Scripting Task wizard. To run the task, perform the following:

1. In the Resource Updating Manager console management tree right-click the node of the collection or category where you want to run the custom task.
2. Select **Create Task | Scripting** from the short-cut menu.
3. On the Task Scripting step, specify the script to execute on the selected workstations. Click **Browse** to specify the script file (the following file types are supported: *.vbs, *.js, *.bat, *.cmd, *.ps1).
4. In the Task Schedule dialog box you can specify when the task starts. You can start the task immediately by selecting the **Start task now** option or select the **Start task at** option to specify the date and time to start processing. On the same step, you can specify the pending timeout for the task operation in case some computers are not accessible at the task start time.
5. On the Task Description step, specify the task description for further reference and then click **Next**.
6. Click **Finish**.

**Post-Processing Operations**

After successful resource processing, you can remove any references to the source accounts and then disable or delete the source accounts. Also, you can remove the Resource Updating Manager agent from the processed computers.

**Resource Cleanup**

Once your users have started to log on under their new accounts in the target domain and are not experiencing any problems with access to resources, you may want to remove unnecessary references to the original source accounts in collections, user rights, and object security descriptors. Take the following steps:

1. In the Resource Updating Manager console management tree right-click the node of the collection or category you want to process.
2. Select the **Create Task | Processing** option in the shortcut menu.
3. On the Task Action step, select the **Clean up legacy local group membership, user rights, and permissions of migrated users** option.
4. Select the required items and settings to process in the Handling Rights and Resources dialog box.

The Leave Source accounts’ permissions check box will have no effect on this operation.
5. In the Task Schedule dialog box you can specify when the task starts. You can start the task immediately by selecting the Start task now option or select the Start task at option to specify the date and time to start processing. On the same step, you can specify the pending timeout for the task operation if some computers are not accessible at the task start time.

6. On the Task Description step you can specify an optional task description.

7. Click Finish.

After the cleanup, users from the source domain will lose their access rights. If cleanup is done before running Resource Updating Manager with the Reassign local group membership, user rights, and object permissions to target users option selected, there will be no way to get these permissions back, nor will there be a way to reassign permissions to target users.

**Computer Cleanup**

Follow these steps to remove the Resource Updating Manager agent from the processed computers:

1. In the Resource Updating Manager console management tree right-click the node of the collection or category you want to clean up.

2. Select Create Task | Cleanup in the shortcut menu.

3. On the Task Description step, specify the task description for further reference, and then click Next.

4. In the Task Schedule dialog box you can specify when the task starts. You can start the task immediately by selecting the Start task now option or select the Start task at option to specify the date and time to start processing. On the same step, you can specify the pending timeout for the task operation if some computers are not accessible at the task start time.

5. Click Finish.

**Processing Algorithm**

Objects are processed according to the following algorithm:

- If a source user account is the current owner, ownership is transferred to the target user account.
- If there is no reference to the source user account in the Access Control List, then permissions and auditing are left unchanged. If Source\User1 or Source\Group1 is found in the corresponding ACL, then:
  a) All entries of Target\User1 are removed.
  b) The ACE is cloned and assigned to Target\User1 or Target\Group1.

If you choose to process local profiles, user profiles will be shared between source and target user. No copying of profiles ever occurs.

The processing of Access Control Lists is comprehensive: not only permissions, but also ownership and auditing are processed, which ensures the completeness of the update. A relevant example would be Mac volumes that use ownership to control client access. These volumes are handled correctly by Resource Updating Manager.
Another notable Resource Updating Manager feature is that it will traverse and process all child directories and files, regardless of the ownership and permissions of the parent directory.

Managing Categories

The Categories node of the Resource Updating Manager console management tree contains several pre-installed categories which might help you to sort computers and find a particular computer among the processed resources. After a computer was added to any collection under the collections node, discovered, processed (successfully or not), it immediately appears under the corresponding category.

- Categories do not contain any processing settings.
- Since a category may contain computers from different collections with different Processing Options configured, the last operations will be repeated in the following order:
  - All Discover computer information actions
  - All Process computer resources actions
  - All Move computers to domain actions
  - All Cleanup computer actions

However, actions of the same type will stay unsorted.

Creating Categories

To create your own category, right-click the Categories node and select the Create Category option. In the Create Category dialog box provide the name and optional description for new category and configure query settings and node properties.

When creating a category, you actually create an LDAP filter for the ADAM database.

Viewing Log Files

The Migration Manager RUM Controller service stores all information about its functions in its log file. The log file is called RUMController.log and stored in the %ProgramFiles%\Common Files\Aelita Shared\Migration Tools\Resource Updating folder on the console computer.

The Discover computer information, Process computer resources, Move Computer to domain and Cleanup computer actions create log files in the %ProgramFiles%\Common Files\Aelita Shared\Migration Tools\Resource Updating\Logs\[computer_name] folder. Use the View Logs option to view these logs.

The Migration Manager RUM Agent service also stores all information about its activity in its log file. This log file is called RUMAgent.log and stored in the %WINDOWS%\Quest Resource Updating Agent folder on the computer where the agent is installed.

As soon as all the agents have finished performing the specified tasks, Resource Updating Manager will collect the logs from the computers. To view the collected logs right-click the computer in the right pane of the Resource Updating Manager console and select View Logs.
Interrupting the Process

To interrupt all tasks for a specific collection or category, right-click the collection or category node in the Resource Updating Manager console and select Cancel Tasks.

Resource Updating Manager behaves as follows in situations where processing is interrupted:

- If you click Cancel Task during a permission update, the computers being processed at that moment will be processed to the end and objects on these computers will have new (target) permissions. Computers for which processing has not started will not be processed, and objects on these computers will keep their old permissions. If you want to completely restore the system state, run Resource Updating Manager to perform the Revert to the original local group membership, user rights, and object permissions action.
- If you click Cancel while reverting changes, the computers being processed at that moment will be processed to the end and objects on these computers will have source permissions. Computers for which processing has not started will not be processed, and objects on these computers will keep their target permissions. If you want to restore the system state, run Resource Updating Manager to perform the Reassign local group membership, user rights, and object permissions to target users action.
- If you click Cancel Task during permission cleanup, the computers being processed at that moment will be processed to the end and permissions of the objects on these computers will be cleaned up. Computers for which processing has not started will not be processed, and objects on these computers will be left intact.
- If multiple tasks are associated with a specific computer and one of the tasks fails, then all subsequent tasks will be cancelled for that computer, and a corresponding error message will be displayed.

User Profile Update

To ensure zero user impact and zero help desk involvement when user accounts are migrated, the target user accounts must have the same profiles as the corresponding source accounts.

For this to occur, two tasks need to be accomplished:

- The target accounts must gain access to the source profiles (both to the corresponding files and registry keys).
- The target accounts’ settings must be pointed to the same profiles that the source accounts used.

Migration Manager manages these tasks for both local and roaming profiles, and ensures that at every migration phase, users have access to their personal profiles and settings.
**User Profile Basics**

A user profile consists of two parts: the key in system registry and the folder on a hard disk which contains user-specific data and desktop settings.

A user profile can be either local or roaming:

- If user data is stored on a local hard disk, the user profile is local.
- If user data is stored centrally on a server, the user profile is roaming.

When migrating accounts from one Active Directory domain to another, you can use the **Add SIDHistory** option to specify that the new accounts should automatically gain all privileges of the source accounts, so no resource update is required for users to start using their new accounts. When the coexistence period is over, you can process all resources, granting the target accounts explicit access, and then clean up SIDHistory and remove the source accounts.

However, adding SIDHistory does not cause the target accounts to use the source profiles. This task requires registry changes, which can be accomplished by using Resource Updating Manager or Resource Kit utilities.

**How User Profiles Work**

When a user logs on to a workstation the first time, a local profile is created on that workstation in the **Documents and Settings** folder.

When a user connects to a server with Terminal Services Client the first time, a local profile is created on that server in the **Documents and Settings** folder as well.

If a user is configured to use a roaming profile (that is, the settings in either the **Profile** or **Terminal Services Profile** tab in the user account properties contain valid paths to centrally stored profiles), the user data stored in the central profile folder is copied to the local profile folder on the workstation (if the user is logged on locally) or server (if the user is connected to the server with Terminal Services Client). All changes made to the profile during a session are saved in the local profile folder and uploaded into the central profile folder at the end of the session.

When a user logs on to a workstation, the following logic determines which user profile is used:

- If a profile path is specified on the **Profile** tab, then that profile is loaded.
- If no profile path is specified on **Profile** tab, then the local profile is loaded.

When a user initiates a new terminal session to a server, the following logic determines which user profile is used:

- If a profile path is specified on the **Terminal Services Profile** tab, then that profile is loaded, whether or not a profile is specified on **Profile** tab.
- If no profile path is specified on the **Terminal Services Profile** tab but a profile path is specified on **Profile** tab, then that profile is loaded.
- If no profile path is specified on either the **Terminal Services Profile** tab or the **Profile** tab, then the local profile is loaded.
If a computer has both local and roaming profiles, you should perform all actions described in the *Local Profiles Update* section below first and then perform the additional actions described in the *Roaming Profiles Update* section.

**Local Profile Update**

Local profiles are updated when you start processing from Resource Updating Manager with the **Local Profiles** and **File System** check boxes selected on the **Permissions Management** tab of the **Processing Options** dialog box. This will process registry keys and folder permissions for local profiles.

After the processing is complete, the same profile is shared for the source and target user.

**Roaming Profile Update**

Roaming profiles stored on a computer are updated when you start processing from Resource Updating Manager with the **Roaming Profiles**, **File System** and **File Ownership** check boxes selected on the **Permissions Management** tab of the **Processing Options** dialog box. This will process registry keys and folder permissions for roaming profiles.

When Migration Manager creates target accounts, it copies the roaming profiles’ paths, so the new accounts will have the same profiles as the old accounts.

If your migration procedure includes moving roaming profiles to another server, profile paths specified on the **Profile** and **Terminal Services Profile** tabs in the user account properties need to be updated as well.

If source account is using roaming profile, then before you start processing roaming profiles using Resource Updating Manager, you must log off from this profile. Otherwise, after the roaming profile update completes, the target account will fail to log on to this profile.

**Enabling the “Cross-Forest User Policy and Roaming User Profiles” Policy**

If the server where roaming user profiles are stored is running Windows 2000 SP4 or higher, you should enable the **Allow Cross-Forest User Policy** and **Roaming User Profiles** policy to allow users from trusted domains to use roaming profiles on that server. You can configure this policy either locally on the server or by using a domain or organizational unit-based Group Policy object (GPO). To do this locally on a server:

1. Log on to the computer as a user with administrator rights.
2. Click **Start**, click **Run**, type `gpedit.msc`, and then click **OK**.
3. Double-click **Computer Configuration**, double-click **Administrative Templates**, double-click **System**, and then click **Group Policy**.
4. In the right pane, double-click **Allow Cross-Forest User Policy** and **Roaming User Profiles**.
5. Click **Enabled**, click **Apply**, and then click **OK**.
6. Quit the Group Policy tool.
7. Allow sufficient time for the computer policy to be automatically updated, or update it yourself by running the following command in the command line:

```plaintext
secedit /refreshpolicy machine_policy
```

In Windows 2003, use the `gpupdate` command.

For more details on user policies, refer to Microsoft Knowledge Base article 823862 at http://support.microsoft.com/default.aspx?scid=kb;en-us;823862.

**Preventing Profile Duplication**

The target user accounts must use the same profiles as the corresponding source accounts. However, in some cases a duplicate profile can be created for the target user after processing. This section explains why duplicate profiles are created and describes how to prevent the duplication of profiles after processing.

If a service or scheduled task is running under the source account on a computer, this service or scheduled task maintains access to the source user profile. If the profile is already processed but the computer is not restarted, then after a user logs off and logs again with the new target account, the source user profile is still loaded by the source user account, instead of by the target account. In this case, temporary profile is created for the target user.

The User Profile Hive Cleanup Service (UPHClean) by Microsoft is intended to help troubleshoot issues with profiles being locked by any service during processing. For more information about the UPHClean, refer to Microsoft Knowledge Base article 837115, "Troubleshooting profile unload issues," at http://support.microsoft.com/default.aspx?scid=kb;en-us;837115 and to the UPHClean readme file at http://download.microsoft.com/download/a/8/7/a87b3d05-cd04-4743-a23b-b16645e075ac/readme.txt.

To download UPHClean, use the following link:


**Active Directory Processing**

Access to Active Directory objects is regulated with security descriptors (SDs) and group membership. After migration, the SDs and group membership of all objects must be modified so that the access that was granted to the source accounts is given to the target accounts as well.

**Active Directory Processing Wizard** allows you to update group membership, linked attributes, and Active Directory permissions to conform to the Active Directory reconfiguration after migration. Active Directory Processing Wizard uses mappings between the migrated source and target accounts stored in ADAM for updating permissions. Also Active Directory Processing Wizard allows you to process Microsoft Exchange directory permissions and cleans up SIDHistory of the migrated objects.
Starting Active Directory Processing

You can perform Active Directory processing in several ways. Select the one that best suits your situation.

- Create an Active Directory processing task and run it from Migration Manager. To create an Active Directory processing task, go to the Resource Processing | Tasks node and click the Active Directory Processing button in the right pane.

- Create an Active Directory processing task and then create a setup package for the task, delegate rights to perform this task to another person, and send the package to that person. The delegated administrator then will install the package and perform the Active Directory processing as specified in the task configuration. Refer to the Delegating Resource Update section for more details.

- Export the INI file with the appropriate settings for Active Directory processing, and then create and configure an Active Directory processing task to run in stand-alone mode using this INI file. Refer to the Delegating Resource Update section for more details.

Regardless of the method you select, Active Directory Processing Wizard will guide you through the updating process. You can use Active Directory Processing Wizard in any of the three modes:

- Standalone
- Console integration
- Delegation

Each mode has specific set of steps, as described in the corresponding sections below.

Using Standalone Mode

Step 1. Specify Mapping File

In this step you are prompted to specify location of the INI mapping file. The mapping file is used to establish matching between source and target accounts.

To get the file, export the INI file, as follows:

1. From the Tools menu in Migration Manager Console, select Export to | INI file. The Export INI File dialog box will appear.
2. Select Active Directory Processing Wizard in the Wizard’s Name list box.
3. Specify the INI file name and path in the INI file field or leave the default.
4. Select the desired re-permissioning options.
5. Click OK. This will create an INI file in the folder you specified in step 3.
Step 2. Set Processing Options

Select the way Active Directory will be processed.

- **Reassign group membership and permissions to target users**
  Select this option to save group membership and grant the permissions of the source accounts to the new (target) user accounts.
  - Target account permissions will be merged with the source account's permissions.
  - If you click **Cancel** during permissions update, further re-permissioning will be stopped. Objects that are already processed by that moment will have new (target) permissions. Objects that are not yet processed will keep old permissions. If you want to completely restore the Active Directory state, run the wizard with the **Revert to the original group membership and permissions** option.

- Select the **Leave source users' group membership and permissions** check box to allow access for both the source and the target user accounts. This way you will be able to make the migration smoother, granting both accounts the same privileges for the transition period.

- **Clean up group membership and permissions of migrated users**
  Select this option if you want to remove permissions granted for source accounts from the objects' Access Control Lists (ACLs), thus disabling the rights for the legacy accounts. Normally, this should be done as soon as the transition period is over.
  - The wizard revokes the rights for only source accounts that are already migrated to target.
  - If you click **Cancel** during the cleanup process, further processing will be stopped. Permissions of the objects that are already processed by that moment will be cleaned up. Objects that are not yet processed will be left intact.

- **Revert to the original group membership and permissions**
  This option lets you undo re-permissioning, which removes target accounts from the Access Control Lists and returns all rights to the source accounts.
  - If two source users were merged to one target user during migration, and if only one of the source users had permissions on some objects, then after the SD update and reverting of permissions back, both users will have permissions on these objects (that is, the users will have common permissions).
  - If you click **Cancel** while changes are being reverted back, further re-permissioning will be stopped. Objects that are already processed by that moment will have source permissions. Objects that are not yet processed will keep target permissions. If you want to restore the Active Directory state, run the wizard with the **Reassign group membership and permissions to target users** option.

- **Clean up objects' SIDHistory**
  Select this option to clean up SIDHistory attributes of Active Directory objects.
  - Only SIDs of the source objects migrated within the current migration project and selected for processing will be cleaned up from the SIDHistory attributes of the target objects. The SIDs of other objects (that is, objects either not selected for processing or migrated in a separate project) will be left intact.
Changes have probably been made to permissions, service accounts, group membership, etc. on resources since resource processing was last executed. We recommend you update distributed resources and BackOffice servers one more time before you clean up SIDHistory to make sure that all permissions, service accounts, and group membership are up to date.

**Step 3. Select Objects to Process**

Specify the objects to process. You can process one or more of the following objects:

- **Group membership** (group links). Select this check box to update the group membership (the member linked attribute) for the groups from the selected scope. If, for example, *SourceUser* is a member of a source group and this user is migrated to *TargetUser*, updating group membership using Active Directory Processing Wizard will ensure that *TargetUser* becomes a member of this group.
  
  You should also select this check box, if you want to process Exchange 2007 Administrative Roles.

  Group membership for the target migrated groups will not be processed; these groups will be skipped.

- **Linked attributes** (other links except group links). Select this check box to update the linked attributes (the linked attributes other than member) for the objects from the selected scope. The forward links (links to other objects in the directory) will be processed.

- **Active Directory permissions** (including processing the Default Security of Active Directory Schema Classes). Select this check box to update the permissions and ownership for the objects from the selected containers.
  
  Select the **Default schema permissions** check box to update the Default Security of Active Directory Schema Classes.

  For successful **Default schema permissions** processing, the service account must be a member of the **Schema Admins** group.

- **Exchange mailbox permissions**. Select this check box to update the Exchange mailbox directory permissions.

  The service account must have the following permissions:

  - To modify the `msExchMailboxSecurityDescriptor` attribute on processed mailbox-enabled objects.
  
  - To Read/Write permissions on Exchange mailbox store.

  Grant these permissions using Exchange System Manager Console or ADSI Edit snap-in.

- **Other Exchange permissions**. Select this check box to update directory permissions for Exchange objects, such as organizations, servers, and containers.

  To update the Public Folders directory permissions, select the **Permissions** check box and in the expanded processing scope tree select the check box next to the **Microsoft Exchange System Objects** container.

  For successful processing of the directory permissions for Exchange objects, the service account must be granted **Exchange Full Administrator** rights using Exchange System Manager Console.
Step 4. Select Domains

In this step, add the domains in which you want to process the objects. For each domain you add, specify the credentials that the wizard will use to access the domain and update objects. You can either use the credentials of the user currently logged on or specify different credentials.

For successful Active Directory processing, the specified account must have Administrative rights.

To change the specified credentials for the domain server, select the server and click the Properties button.

To set the processing scope for the selected domain server, take the following steps:

1. Click the Scope button.
2. In the Select Processing Scope dialog box, browse the domain hierarchy tree and clear check boxes next to the names of containers you want to exclude from processing.

To set the preferred GC and/or DC, take the following steps:

1. Click the Options button.
2. In the Specify Options dialog box, type the names of preferred Global Catalog and DC into the corresponding text boxes.

Step 5. Complete the Wizard

In the Progress step, you should wait while the wizard performs all requested operations. The following information is available:

- Processing progress bar
- State of processing for the particular server
- The name of container processed at the moment
- Number of errors

In the Summary step, you may review results and statistics of group membership and permissions processing. If any errors occurred during processing, they are indicated in the Summary. Error descriptions are available in the log file.

Click Finish to close the wizard.

Using Console Integration Mode

Step 1. Set Task Properties

In this step you are prompted to specify a task name and description.

To switch the wizard to Delegation mode, select the Delegate this task check box. Please refer to the Using Delegation Mode section below in this guide for details.
Step 2. Set Processing Options

Select the way Active Directory will be processed.

- **Reassign group membership and permissions to target users**
  Select this option to save group membership and grant the permissions of the source accounts to the new (target) user accounts.
  - Target account permissions will be merged with the source account's permissions.
  - If you click Cancel during permissions update, further re-permissioning will be stopped. Objects that are already processed by that moment will have new (target) permissions. Objects that are not yet processed will keep old permissions. If you want to completely restore the Active Directory state, run the wizard with the **Revert to the original group membership and permissions** option.
  - Select the **Leave source users' group membership and permissions** check box to allow access for both the source and the target user accounts. This way you will be able to make the migration smoother, granting both accounts the same privileges for the transition period.

- **Clean up group membership and permissions of migrated users**
  Select this option if you want to remove permissions granted for source accounts from the objects’ **Access Control Lists** (ACLs), thus disabling the rights for the legacy accounts. Normally, this should be done as soon as the transition period is over.
  - The wizard revokes the rights for only source accounts that are already migrated to target.
  - If you click Cancel during cleanup of permissions, further processing will be stopped. Permissions of the objects that are already processed by that moment will be cleaned up. Objects that are not yet processed will be left intact.

- **Revert to the original group membership and permissions**
  This option lets you undo re-permissioning, which removes target accounts from the Access Control Lists and returns all rights to the source accounts.
  - If two source users were merged to one target user during migration, and if only one of the source users had permissions on some objects, then after the SD update and reverting of permissions back, both users will have permissions on these objects (that is, the users will have common permissions).
  - If you click Cancel while changes are being reverted back, further re-permissioning will be stopped. Objects that are already processed by that moment will have source permissions. Objects that are not yet processed will keep target permissions. If you want to restore the Active Directory state, run the wizard with the **Reassign group membership and permissions to target users** option.

- **Clean up objects' SIDHistory**
  Select this option to clean up SIDHistory attributes of Active Directory objects.
  - Only SIDs of the source objects migrated within the current migration project and selected for processing will be cleaned up from the SIDHistory attributes of the target objects. The SIDs of other objects (that is, objects either not selected for processing or migrated in a separate project) will be left intact.
  - Changes have probably been made to permissions, service accounts, group membership, etc. on resources since resource processing was last executed. We recommend you update distributed resources and BackOffice servers one more time before you clean up SIDHistory to make sure that all permissions, service accounts, and group membership are up to date.
Step 3. Select Objects to Process

Specify the objects to process. You can process one or more of the following objects:

- **Group membership** (group links). Select this check box to update the group membership (the *member* linked attribute) for the groups from the selected scope. If, for example, *SourceUser* is a member of a source group and this user is migrated to *TargetUser*, updating group membership using Active Directory Processing Wizard will ensure that *TargetUser* becomes a member of this group. You should also select this check box if you want to process Exchange 2007 Administrative Roles.

  Group membership for the target migrated groups will not be processed; these groups will be skipped.

- **Linked attributes** (other links except group links). Select this check box to update the linked attributes (the linked attributes other than *member*) for the objects from the selected scope. The forward links (links to other objects in the directory) will be processed.

- **Active Directory permissions** (including processing the Default Security of Active Directory Schema Classes). Select this check box to update the permissions and ownership for the objects from the selected containers. Select the **Default permissions** check box to update the **Default Security** of Active Directory Schema Classes.

  For successful Default permissions processing, the service account must be a member of the **Schema Admins** group.

- **Exchange mailbox permissions**. Select this check box to update the Exchange mailbox directory permissions.

  The service account must have the following permissions:
  
  - To modify the *msExchMailboxSecurityDescriptor* attribute on processed mailbox-enabled objects.
  - To Read/Write permissions on Exchange mailbox store.

  Grant these permissions using Exchange System Manager Console or ADSI Edit snap-in.

- **Other Exchange permissions**. Select this check box to update directory permissions for Exchange objects, such as organizations, servers, and containers. To update the public folders' directory permissions, select the **Permissions** check box and in the expanded processing scope tree, select the check box next to the **Microsoft Exchange System Objects** container.

  For successful processing of the directory permissions for Exchange objects, the service account must be granted with **Exchange Full Administrator** rights using Exchange System Manager Console.
Step 4. Select Domains

In this step, add the domains in which you want to process the objects. For each domain you add, specify the credentials that the wizard will use to access the domain and update objects. You can either use the credentials of the user currently logged on or specify different credentials.

For successful Active Directory processing, the specified account must have Administrative rights.

To change the specified credentials for the domain server, select the server and click the Properties button.

To set the processing scope for the selected domain server, take the following steps:
1. Click the Scope button.
2. In the Select Processing Scope dialog box, browse the domain hierarchy tree, and clear check boxes next to the names of containers you want to exclude from processing.

To set the preferred GC and/or DC, take the following steps:
1. Click the Options button.
2. In the Specify Options dialog box, type the names of preferred Global Catalog and DC into the corresponding text boxes.

Step 5. Schedule Processing

This step allows you to specify whether the task should be started immediately or should be scheduled.

- **Save task configuration only.** Select to save the task configuration. You can start the task any time later by right-clicking it in Migration Manager console and selecting Start on the shortcut menu.
- **Save task configuration and run processing now.** Select to start the task immediately after you finish the wizard.
- **Schedule processing.** Allows you to specify the time when the task should be started. You can schedule the task to be performed, for example, during the night. You can Add New Schedule, Remove or Edit the existing schedule and specify the account under which the task should be performed.

Step 6. Complete the Wizard

In the Progress step, you should wait while the wizard performs all requested operations. The following information is available:

- Processing progress bar
- State of processing for the particular server
- The name of container processed at the moment
- Number of errors
In the **Summary** step, you may review results and statistics of group membership and permissions processing. If any errors occurred during processing, they are indicated in the **Summary**. Error descriptions are available in the log file.

Click **Finish** to close the wizard.

**Using Delegation Mode**

**Step 1. Set Task Properties**

To switch the wizard to the **Delegation** mode, the **Delegate this task** check box must be selected.

In this step you are prompted to specify a task name and description.

**Step 2. Configure Delegation Options**

In this step you can specify the account of the trusted person you want to delegate the task to. You can specify one or more accounts and assign them the appropriate rights to perform the task.

**To delegate the rights to the trusted accounts, complete the following steps:**

1. Click the **Delegate** button.
2. Specify the account and the role you want to delegate. Click **OK**

The following option is available:

- **Revoke.** Click to remove the selected account from the list and deprive it of the rights to process Active Directory. Note that you cannot remove accounts if their permissions are inherited.

**Step 3. Complete the Wizard**

After you create the list of delegates, click **Next** and then **Finish** to apply your changes and close the wizard.

**Running Active Directory Update**

To start an Active Directory processing task from Migration Manager, select the task in the project tree, right-click the task, and select the **Start** command from the shortcut menu.

To view the task execution progress, select the task object in the project tree and switch to the **Information** tab in the right-hand pane.
Stopping a Task

If for some reason you want to interrupt Active Directory processing, click the *Cancel* button in the wizard that starts after you run the task.

If you stop processing by clicking the *Cancel* button, or the task execution is stopped due to an error, the task acts as follows:

- If you stop the task during permissions update, further re-permissioning will be stopped. Objects already processed by that moment will have new (target) permissions. Objects not yet processed will keep old permissions. If you want to completely restore the system state, reconfigure and run the task with the *Revert to the original group membership, linked attributes, and object permissions* option.

- If you stop the task while reverting changes, further re-permissioning will be stopped. Objects already processed by that moment will have source permissions. Objects not yet processed will keep target permissions. If you want to restore the system state, reconfigure and run the task with the *Reassign group membership, linked attributes, and object permissions to target users* option.

- If you stop the task while cleaning up permissions, further processing will be stopped. Permissions of the objects already processed by that moment will be cleaned up. Objects not yet processed will be left intact.

Log File

The Active Directory processing task log is stored in the `QsActiveDirectoryProcessingWizard_<timestamp>.log` file in the `%temp%` folder.

Active Directory Processing Wizard does not store information about its own activities under the *History* node in the Migration Manager console management tree. All data is stored in the appropriate log file.

After the Migration Manager console is upgraded, activities history is not available for the Active Directory processing tasks, completed before upgrade.

Reconfiguring a Task

To reconfigure the task, right-click the task object and select *Properties*. The Active Directory Processing Wizard will start and let you specify different options for the task. Refer to the steps above for more information on the available options.
Exchange Server Processing

When user accounts are migrated, the messaging system must be updated to comply with the changes. Exchange Processing Wizard updates Exchange permissions to grant the migrated accounts in the target domain the permissions assigned to the source accounts. For example, Exchange Processing Wizard updates client and administrative permissions on mailboxes, public folders, and all other Exchange objects. Client permissions get automatically granted to the target users when they log into their old mailbox.

Exchange Processing Wizard cannot update administrative permissions on some system folders.

Exchange directory permissions are processed by the Active Directory processing task. See the Active Directory Processing section for details.

In case of intra-forest migration, after the Exchange Server update, the target accounts have all the source accounts’ rights but the mailboxes still continue to belong to the source accounts. The mailboxes need to be reassigned to the target accounts before the source accounts are decommissioned.

To update mailbox owners for Exchange Server, you should use the Reconnect Exchange mailbox option in the migration session. Refer to the Migration Session section for more details.

Prerequisites

- For a successful Exchange directory update, you must use an account with Full Exchange Administrator role for the Exchange organization.
- For a successful Exchange Server update, Integrated Windows authentication must be enabled on Exchange virtual servers and folders.
- No additional trust relationships are required for successful processing if the Exchange Server resides in the same forest as the target domain.
- An Exchange 2000 Server update requires Exchange 2000 Server Service Pack 1 or later. It is recommended to use the latest Exchange 2000 Server service pack (currently this is Service Pack 3).

Starting Exchange Update

You can perform Exchange update in several ways. Select the one that best suits your situation.

- Create an Exchange Processing task and run it from Migration Manager. To create an Exchange Processing task, go to the Resource Processing Tasks node, and click the Exchange Processing button in the right pane.
- Create an Exchange processing task, create a setup package for the task, delegate rights to perform this task to another person, and send the package to that person. The delegated administrator will then install the package and perform the Exchange processing as specified in the task configuration. Refer to the Delegating Resource Update section for more details.
• Export the INI file with the appropriate settings for Exchange processing, and then create and configure an Exchange Processing task to run in stand-alone mode using this INI file. Refer to the *Delegating Resource Update* section for more details.

Regardless of the method you select, Exchange Processing Wizard will guide you through the updating process. Complete the steps given by Exchange Processing Wizard, as described below.

**Step 1. New Exchange Processing Task**

Specify a name for the task and add a descriptive comment.

**Step 2. Select Configuration Mode**

Next, select whether you want to delegate this task to a trusted person or whether you want to configure and schedule the task.

- **Delegate resource processing task**—Select this option if you want to create the task and delegate it to a trusted person who will run the task.
- **Configure resource processing task**—Select this option if you want to create, configure, and schedule the task.

Depending on the mode you selected, the remaining steps offered by the wizard are different.

**Step 3. Specify Re-Permissioning Options**

This step is displayed regardless of the configuration mode you selected in the previous step.

This step lets you specify the options for the processing of Exchange objects.
• **Reassign object ownership and permissions to target users**—Select this option to re-assign permissions and ownership set to the Exchange 2000 objects to the new (target) user accounts.

  a) **Leave source accounts’ permissions**—Select this check box to allow access for both the source and target user accounts (recommended). This will make the update smoother by granting both accounts the same privileges for the coexistence period.

  b) **Replace existing target accounts’ permissions**—If permissions for the target user are already set (that is, the object Security Descriptor contains the target user’s SID), you can grant the source account’s permissions to the existing target account by selecting this check box. In this case, the target account’s permissions will be overwritten. Leaving this check box cleared will keep the target account’s permissions intact, and the target user will have permissions different from those of the source user. If this option is left cleared when updating Exchange, the target user’s permissions are merged with the source user’s permissions.

• **Clean up legacy object ownership and permissions of migrated users**—Select this option if you want to remove permissions granted for source accounts from the objects’ Access Control Lists (ACLs), thus disabling the rights for the legacy accounts. Normally, this should be done as soon as the coexistence period is over.

• **Revert to the original object ownership and permissions**—Select this option to undo re-permissioning, which removes target users from the objects’ Access Control Lists (ACL) and returns all rights to the source accounts.

  If two source users were merged to one target user during migration, and if only one of the source users had permissions on some objects, then after Exchange update and reverting permissions back, both users will have permissions on these objects (that is, the users will have common permissions).

**Process from INI file**—Select this option if you want to retrieve the processing options from an INI file. The INI settings file can be created in Migration Manager (Tools | Export to | INI File). See the Creating an INI File for Resource Update section for more details. Note that if no INI file exists, the option is disabled.

This option is enabled only when the wizard runs in stand-alone mode.

The wizard cannot update permissions on a mailbox that has never been used. The Exchange store does not actually create the mailbox until the first time the user opens it, at which time Exchange creates the security descriptor in the store. Before processing a newly-created mailbox, activate it by logging on to it. Otherwise, the wizard will not process the mailbox permissions.

SIDS that are not resolved in the domain where Exchange Server is installed cannot be added to the client permissions security descriptor.

To safeguard security, Exchange Processing Wizard does not process a security descriptor if at least one SID cannot be resolved. If this occurs, correct the SID resolution problem and re-run the wizard for objects that were not processed the first time.
Step 4. Delegate Resource Processing Task

This step appears only if Delegate resource processing task mode was selected in Step 2. If you selected the Configure resource processing task option, proceed to step 5.

This step lets you specify one or more trusted accounts and delegate the rights to perform the task to those accounts.

To delegate the rights to a trusted account, complete the following steps:

1. Click the Browse button.
2. In the Select User or Group dialog box, select a user or group you want to delegate the rights to and click OK.
3. Click the Add Account button. The account will be added to the list of delegated accounts and will automatically be assigned the rights assigned to the Resource Admin role. For more information about the available roles and the rights possessed by each role, refer to the Delegating Migration Tasks section.

Click Next to proceed to the Complete the Exchange Processing Wizard step.

Step 5. Select Exchange Servers

In this step, add at least one Exchange server for each organization you want to update.

First Use

When you run the Exchange Processing Wizard for the first time, it automatically displays the Add Exchange Servers dialog box before letting you select the Exchange objects to be processed, as shown below:
Specify the Exchange server name and the credentials to be used for connecting to the server.

If the account you specify does not have enough privileges to modify some of the Exchange objects, they will remain unchanged. No error or warning messages will be displayed—all messages will be written to the log file. See the Prerequisites section above for details.

Select the Use SSL check box in the Add Exchange Servers dialog box if you want to connect to the server using a secure connection. Note that to use a secure connection, the Web server installed on the computer running Exchange Server must be configured to support SSL. For the server to be successfully processed via the secured connection, the security certificate must be issued by a trusted company, the security certificate date must be valid, and the security certificate must have a valid name matching the specified Exchange server name. See the Web server and Exchange Server documentation for details.

In this step, you also select the Global Catalog server (GC). The GC stores information about all mailboxes in the organization and is used for mailbox enumeration. If you select the Autodetect option, the nearest GC is used. To select a specific catalog server, select the Custom option and specify the server name. This is recommended if the organization contains a large number of mailboxes, because it allows you to specify a GC that serves fewer queries and is less likely to become overloaded.
Subsequent Uses

If you are not running the wizard for the first time, it displays the Exchange organizations added previously. The wizard displays the object tree with all servers you have added. The name of a tree consists of the organization name, followed by the site name and the processing server name.

To add new Exchange organizations and servers for processing, use the **Add Exchange server** and **Add all servers from Exchange organization** buttons on the toolbar.

To change the credentials and connection settings for an Exchange server in the list, right-click the server object and select **Properties**. This will open the **Add Exchange Servers** dialog box.

Select the servers to be processed by selecting the check boxes. When you select a check box, all nodes at the lower levels will be selected. To select all servers in the Exchange organization, simply select the organization node. To exclude some servers of the organization from processing, clear their check boxes.

- You must select at least one check box at the lowest level. If no server is selected, you cannot proceed.
Step 6. Select Objects

This step lets you specify the objects for processing.

You can choose whether to update client permissions, administrative permissions, permissions on messages, or any combination. You can also specify whether to make these changes on all Exchange objects or only on the objects you specify.

For successful message processing, ensure the following:

- The account under which the processing is performed must have the Send As and Receive As permissions on the processed store or server.
- The mailbox database has an associated public folder.

It is recommended to create a backup of the mailbox and public stores before processing messages.

Selecting Objects for Processing

To select objects for processing explicitly, select the Process selected objects only and then click the Select objects button. The Select Objects to Process window will be displayed, showing the Exchange directory hierarchy.

The wizard shows the servers you have specified for processing and the organizations to which these servers belong. These objects are selected and unavailable because you have already selected them on the previous step. The lower levels present the organization hierarchy for each server in the organization. You can select or clear only the objects at the lower levels.
You can select individual mailboxes and public folders to process. If you select or clear an object, the objects below it will also be selected or cleared.

After you select the objects, click **Close**.

**Step 7. Specify Scheduling Options**

This step allows you to specify whether the task should be started immediately or scheduled.
• **Save and start processing immediately**—Select this option to start the task immediately after you finish the wizard. To view the task execution progress, select the task object in the project tree and switch to the **Information** tab in the right-hand pane.

• **Save task configuration**—Select this option to save the task configuration. You can start the task any time later by right-clicking it in Migration Manager and selecting **Start** from the shortcut menu.

• **Save and schedule processing**—Select this option if you want to specify the time when the task should be started. You can schedule the task to be performed, for example, during the night. Click the **Schedule** button to specify the time.

**Step 8. Complete the Exchange Processing Wizard**

In this step, the wizard displays all the settings you made in the previous steps. You can print these settings for later review by clicking the **Print** button and then selecting the printer. You can also save the settings in a text file by clicking the **Save As** button and specifying the filename.

Click **Finish** to complete the Exchange Processing Wizard. The new Exchange processing task will appear under the **Tasks** container in the Migration Project tree.

**Running Exchange Update**

To start an Exchange processing task from Migration Manager, select the task in the project tree, right-click the task, and select the **Start** command from the shortcut menu.

To view the task execution progress, select the task object in the project tree and switch to the **Information** tab in the right-hand pane.

**Stopping a Task**

If for some reason you want to interrupt Exchange processing, right-click the task and select the **Stop** command on the shortcut menu.

If an object was moved during Exchange server processing or after it was selected in the **Select Objects to Process** window in the Exchange Processing Wizard, it may not be processed.

If you stop processing by selecting the **Stop** command, or the task execution is stopped due to an error, the task acts as follows:

• If you stop the task during permissions update, further re-permissioning will be stopped. Objects already processed by that moment will have new (target) permissions. Objects not yet processed will keep old permissions. If you want to completely restore the Exchange directory state, run the wizard with the **Revert to the original object ownership and permissions** option.

• If you stop the task while reverting changes, further re-permissioning will be stopped. Objects already processed by that moment will have source permissions. Objects not yet processed will keep target permissions. If you want to restore the Exchange directory state, run the wizard with the **Reassign object ownership and permissions to target users** option.
If you stop the task during cleanup of permissions, further processing will be stopped. Permissions of the objects already processed by that moment will be cleaned up. Objects not yet processed will be left intact.

When processing public folders that are replicated on several servers using Exchange Processing Wizard, do not process another server until replication is finished (by default, replication occurs every 15 minutes). Otherwise, replication conflicts can arise.

Log File

The Exchange Processing Wizard log is stored in the following locations:

- If the wizard runs in console integration or delegation mode, the %temp% folder; the log file name is E2KPW.log
- If the wizard runs in standalone mode, the %Program Files%\Common Files\Aelita Shared\Migration Tools folder; the log file name is e2k<some_number>.tmp

Reconfiguring a Task

To reconfigure the task, right-click the task object and select Properties. The Exchange Processing Wizard will start and let you specify different options for the task. Refer to the descriptions of the steps above for more information on the available options.

Exchange 5.5 Server Processing

Exchange 5.5 Processing Wizard updates Exchange permissions to grant the migrated accounts in the target domain the permissions assigned to the source accounts. For example, Exchange 5.5 Processing Wizard updates permissions on public folders, and handles administrative and directory permissions on mailboxes and all other Exchange 5.5 objects. Client permissions get automatically granted to the target users when they log into their old mailbox.

Prerequisites

- For a successful Exchange Server 5.5 directory update, you must have the Modify Admin Attributes and Modify Permissions privileges assigned to you (Permissions Admin and Service Account Admin roles possess these privileges) for the organizations, sites, site configurations, and all servers involved in the update process.
- A trust relationship between the domain in which the Exchange Server 5.5 resides and the target domain is required for successful processing. The Exchange domain must trust the target domain to authenticate users.
Starting Exchange 5.5 Update

You can perform Exchange 5.5 update in several ways. Select the one that best suits your situation.

- Create an Exchange 5.5 processing task and run it from Migration Manager. To create an Exchange 5.5 processing task, go to the Resource Processing | Tasks node and click the Exchange 5.5 Processing button in the right pane.
- Create an Exchange 5.5 processing task, create a setup package for the task, delegate rights to perform this task to another person, and send the package to that person. The delegated administrator will then install the package and perform the Exchange 5.5 processing as specified in the task configuration. Refer to the Delegating Resource Update section for more details.
- Export the INI file with the appropriate settings for Exchange 5.5 processing, then create and configure an Exchange 5.5 processing task to run in stand-alone mode using this INI file. Refer to the Delegating Resource Update section for more details.

Regardless of the method you select, Exchange 5.5 Processing Wizard will guide you through the updating process. Complete the steps given by Exchange 5.5 Processing Wizard as described below.

Step 1. New Exchange 5.5 Processing Task

Specify a name for the task and add a descriptive comment.

Step 2. Select Configuration Mode

Select whether you want to delegate this task to a trusted person or whether you want to configure and schedule the task.

- Delegate resource processing task—Select this option if you want to create the task and delegate it to a trusted person who will run the task.
- Configure resource processing task—Select this option if you want to create, configure it and schedule the task.

Depending on the mode you selected, the steps offered by the wizard are different.

Step 3. Specify Re-Permissioning Options

This step is displayed regardless of the configuration mode you selected in the previous step.

This step lets you specify the options for Exchange 5.5 object processing.
• **Reassign object ownership and permissions to target users**—Select this option to re-assign permissions and ownership set to the Exchange 5.5 objects to the new (target) user accounts.

  a) **Leave source accounts’ permissions**—Select this check box to allow access for both the source and target user accounts (recommended). This will make the update smoother, granting both accounts the same privileges for the coexistence period.

  b) **Replace existing target accounts’ permissions**—If permissions for the target user are already set (that is, the object Security Descriptor contains the target user’s SID), you can grant the source account’s permissions to the existing target account by selecting this check box. In this case, the target account’s permissions will be overwritten. Leaving this check box cleared will keep the target account’s permissions intact, and the target user will have permissions different from those of the source user. If this option is left cleared when updating Exchange 5.5, the target user’s permissions are merged with the source user’s permissions.

• **Clean up legacy object ownership and permissions of migrated users**—Select this option if you want to remove permissions granted for source accounts from the objects’ **Access Control Lists** (ACLs), thus disabling the rights for the legacy accounts. Normally, this should be done as soon as the coexistence period is over.

• **Revert to the original object ownership and permissions**—Select this option to undo re-permissioning, removing target users from the objects’ Access Control Lists (ACL) and returning all rights to the source accounts.

If two source users were merged to one target user during migration, and if only one of the source users had permissions on some objects, then, after Exchange update and reverting permissions back, both users would have permissions on these objects (that is, users would have common permissions).
- **Process as specified in the exported INI settings file**—Select this option if you want to retrieve the processing options from an INI file. The INI settings file can be created in Migration Manager (Tools | Export to | INI File). See the Creating an INI File for Resource Update section for more details. Note that if no INI file exists, the option is disabled.

  This option is enabled only when the wizard is run in stand-alone mode.

### Step 4. Delegate Resource Processing Task

This step appears only the Delegate resource processing task mode was selected in Step 2. If you selected the Configure resource processing task option, proceed to step 5.

This step lets you specify one or more trusted accounts and delegate the rights to perform this task to these accounts.

To delegate the rights to the trusted accounts, complete the following steps:

1. Click the **Browse** button.
2. In the **Select User or Group** dialog box, select the user or group you want to delegate the rights to and click **OK**.
3. Click the **Add Account** button. The account will be added to the list of delegated accounts and automatically assigned the **Resource Admin** rights. For more information about the delegation roles and rights possessed by each role refer to the **Delegating Migration Tasks** section.

Click **Next** to proceed to the **Complete the Exchange 5.5 Processing Wizard** step.
Step 5. Select Exchange Servers

In this step, add at least one Exchange 5.5 server for each organization you want to update.

When you run the Exchange 5.5 Processing Wizard for the first time, it automatically displays the Add Exchange Servers dialog box before letting you select the Exchange objects to be processed.

If the account you specify does not have enough privileges to modify some of the Exchange objects, they will remain unchanged. No error or warning messages will be displayed—all messages will be written to the log file. See the Prerequisites section above for details.

If the port used by an Exchange 5.5 server for the LDAP protocol is not 389, explicitly supply the port number (for example EXCHANGE:7775).

If you are not running the wizard for the first time, it displays the Exchange organizations added previously. The wizard displays the object tree with all servers you have added. The name of a tree consists of the organization name, followed by the site name and the processing server name.

To add new Exchange organizations and servers for processing, use the Add Exchange server and Add all servers from Exchange organization buttons on the toolbar.

After adding the specified servers, you may want to add all servers from Exchange organization for the Exchange organization to which the added server belongs. To do this, use the Add all servers from Exchange organization button on the toolbar.
Select the servers to be processed by selecting the check boxes. When you select a check box, all nodes at the lower levels will be selected. Thus, to select all servers in the Exchange organization, select the organization node. To exclude some servers of the organization from processing, clear their check boxes.

You must select at least one check box at the lowest level. If no server is selected, you cannot proceed.

To change credentials and connection settings for the Exchange servers you have already added, right-click the server object and select **Properties**. This will open the **Server Properties** dialog box.

**Step 6. Select Objects**

This step lets you specify the objects for processing.
You can choose either to update client and administrative permissions on all Exchange objects of the types you select, or to update permissions on only the objects you select.

To select objects for processing explicitly, select the **Process selected objects only** option and then click the **Select objects** button. The **Select Objects to Process** window will be displayed, showing the Exchange directory hierarchy.

The wizard shows the servers you have specified for processing and organizations to which these servers belong. These objects are selected and unavailable because you have already selected them on the previous step. The lower levels present the organization hierarchy for each server in organization. You can select or clear only the objects of the lower levels.

![Select Objects to Process window](image)

You can select individual recipient containers and other Exchange objects to process. If you select or clear an object, the objects below it will also be selected or cleared.

The wizards show only the objects whose permissions and ownership can be changed and the containers of such objects. For example, it does not show the Exchange 5.5 schema attributes.

**Mailboxes**, **Distribution Lists**, **Custom Recipients**, and **Public Folders** nodes cannot be expanded in Exchange 5.5 Processing Wizard. When such nodes are selected, all Exchange directory objects of the corresponding type are processed.

If an object’s properties Admin-Display-Name, CN, and Display-Name are not set, the object is displayed in the Exchange 5.5 object list as ‘???’.

After you select the objects, click **Close**. Click **Next** to proceed with the next step.
Step 7. Specify Scheduling Options

This step allows you to specify whether the task should be started immediately or scheduled.

- **Save and start processing immediately**—If this option is selected, the task will be started immediately after you finish the wizard. To view the task execution progress, select the task object in the project tree and switch to the Information tab in the right-hand pane.
- **Save task configuration**—Select this option to save the task configuration. You can start the task any time later by right-clicking it in Migration Manager and selecting Start from the shortcut menu.
- **Save and schedule processing**—Select this option if you want to specify the time when the task should be started. You can schedule the task to be performed, for example, during the night. Click the Schedule button to specify the time.

Step 8. Complete the Exchange 5.5 Processing Wizard

In this step, the wizard displays all the settings you made in the previous steps. You can print these settings for later review by clicking the Print button and then selecting the printer. You can also save the settings in a text file by clicking the Save As button and specifying the filename.

Click Finish to complete the Exchange 5.5 Processing Wizard. The new Exchange 5.5 processing task will appear under the Tasks container in the Migration Project tree.
Running Exchange 5.5 Update

To start an Exchange 5.5 processing task from Migration Manager, select the task in the project tree, right-click the task and select the Start command from the shortcut menu.

To view the task execution progress, select the task object in the project tree and switch to the Information tab in the right-hand pane.

Stopping a Task

If for some reason you want to interrupt Exchange 5.5 processing, right-click the task and select the Stop command from the shortcut menu.

If an object was moved during Exchange 5.5 server processing or after it was selected in the Select Objects to Process window in Exchange 5.5 Processing Wizard, it may not be processed.

If you stop processing by selecting the Stop command, or the task execution is stopped due to an error, the task acts as follows:

- If you stop the task during permissions update, further re-permissioning will be stopped. Objects already processed by that moment will have new (target) permissions. Objects not yet processed will keep old permissions. If you want to completely restore the Exchange directory state, run the wizard with the Revert to the original object ownership and permissions option.

- If you stop the task while reverting changes, further re-permissioning will be stopped. Objects already processed by that moment will have source permissions. Objects not yet processed will keep target permissions. If you want to restore the Exchange directory state, run the wizard with the Reassign object ownership and permissions to target users option.

- If you stop the task during cleanup of permissions, further processing will be stopped. Permissions of the objects already processed by that moment will be cleaned up. Objects not yet processed will be left intact.

When processing public folders that are replicated on several servers using Exchange 5.5 Processing Wizard, do not process another server until replication is finished (by default, replication occurs every 15 minutes). Otherwise, replication conflicts can arise.

Log File

The Exchange 5.5 Processing Wizard log is stored in the E55PW.log file in the %ProgramFiles%\Common Files\Aelita Shared\Migration Tools folder.

Reconfiguring a Task

To reconfigure the task, right-click the task object and select Properties. The Exchange 5.5 Processing Wizard will start and let you specify different options for the task. Refer to the descriptions of the steps above for more information on the available options.
SMS Processing

SMS Processing Wizard is a tool for updating Microsoft Systems Management Server 2003 and Microsoft System Center Configuration Manager 2007 permissions for the selected objects to reflect the domain migration changes after a domain reconfiguration with Migration Wizard.

For a successful SMS update, you need local Administrator permissions on the SMS server you are going to process and the SQL server hosting SMS Server database.

Starting SMS Update

You can perform SMS update in several ways. Select the one that best suits your situation.

- Create an SMS processing task and run it from Migration Manager. To create an SMS processing task, go to the Resource Processing | Tasks node and click the SMS Processing button in the right pane.
- Create an SMS processing task and then create a setup package for the task, delegate rights to perform this task to another person, and send the package to that person. The delegated administrator then will install the package and perform the SMS processing as specified in the task configuration. Refer to the Delegating Resource Update section for more details.
- Export the INI file with the appropriate settings for SMS processing, and then create and configure an SMS processing task to run in stand-alone mode using this INI file. Refer to the Delegating Resource Update section for more details.

Regardless of the method you select, the SMS Processing Wizard will guide you through the update process, as follows:

Step 1. New SMS Processing Task

In this step, you can give the task a new name and add a descriptive comment.

Step 2. Select Configuration Mode

In this step, select whether you want to delegate this task to a trusted person or configure and schedule the task.

If you want to proceed with configuring the task, specify task name and description.
To delegate the task, select the **Delegate this task** check box.

Depending on the mode you selected, the remaining steps offered by the wizard are different.

**Step 3. Specify Re-Permissioning Options**

This step is displayed regardless of the configuration mode you selected in the previous step.

This step lets you specify the options for SMS object processing.
• **Reassign object ownership and permissions to target users**—Select this option to re-assign permissions and ownership set to the SMS objects to the new (target) user accounts. Select the **Leave source accounts’ permissions** check box to allow access for both the source and target user accounts (recommended). This will make the update smoother by granting both accounts the same privileges for the coexistence period.

If the User A and User B have been merged to User C during the account migration session, the target user will get the permissions of both user A and user B.

If the target account already possesses SMS permissions, these permissions will be replaced by the source account’s permissions.

• **Clean up object ownership and permissions of migrated users**—Select this option if you want to remove permissions granted for source accounts from the objects’ Access Control Lists (ACLs), thus, disabling the rights for the legacy accounts. Normally, this should be done as soon as the coexistence period is over.

• **Revert to the original object ownership and permissions**—Select this option to undo re-permissioning, removing target users from the objects’ Access Control Lists (ACL) and returning all rights to the source accounts.

If two source users were merged to one target user during migration, and if only one of the source users had permissions on some objects, then, after SMS update and reverting permissions back, both users would have permissions on these objects (that is, users would have common permissions).

• **Process as specified in the exported INI settings file**—Select this option if you want to retrieve the processing options from the INI file. The INI settings file can be created in Migration Manager (**Tools | Export to | INI File**). See the **Creating an INI File for Resource Update** section for more details. Note that if no INI file exists, the option is disabled.

This option is enabled only when the wizard is run in stand-alone mode.
**Step 4. Delegate Resource Processing Task**

This step appears only the Delegate resource processing task mode was selected in Step 2. If you have selected the Configure resource processing task option, proceed to step 5.

This step lets you specify one or more trusted accounts and delegate the rights to perform this task to these accounts.

To delegate the rights to the trusted accounts, complete the following steps:

1. Click the Delegate button.
2. Specify account and the role you want to delegate. Click OK.

Click Next to proceed to the Complete the SMS Processing Wizard step.
Step 5. Select SMS Servers

Use the Add button to add SMS servers to be processed by this task. In the Add SMS Server dialog box that appears, either type the server name in the text box or use the Browse button to select the server from the list.

You can either use the credentials of the currently logged-in user to connect to the server or specify different credentials. In the latter case, either type the username and the password in the text boxes or use the Browse button to select the user. Click OK.

Use the Remove button to remove servers from the list. To change credentials, select the server in the list, click the Properties button, and specify the new credentials in the SMS Server Properties dialog box.

Click Next to proceed with the next step.
Step 6. Specify Scheduling Options

This step allows you to specify whether the task should be started immediately or scheduled.

- **Save task configuration only**—Select this option to save the task configuration. You can start the task any time later by right-clicking it in Migration Manager and selecting Start from the shortcut menu.

- **Save task configuration and run processing now**—If this option is selected, the task will be started immediately after you finish the wizard. To view the task execution progress, select the task object in the project tree and switch to the Information tab in the right-hand pane.

- **Save task configuration and schedule processing**—Select this option if you want to specify the time when the task should be started. You can schedule the task to be performed, for example, during the night. Click the Schedule button to specify the time.

Step 7. Complete the SMS Processing Wizard

In this step, the wizard displays all the settings you made in the previous steps. You can print these settings for later review by clicking the Print button and then selecting the printer. You can also save the settings in a text file by clicking the Save As button and specifying the filename.

Click Finish to complete the SMS Processing Wizard. The new SMS processing task will appear under the Tasks container in the Migration Project tree.
Running SMS Update

To start an SMS processing task from Migration Manager, select the task in the project tree, right-click the task and select the Start command from the shortcut menu.

To view the task execution progress, select the task object in the project tree and switch to the Information tab in the right-hand pane.

Stopping a Task

If for some reason you want to interrupt SMS processing, right-click the task and select the Stop command from the shortcut menu.

If you stop processing by selecting the Stop command, or the task execution is stopped due to an error, the task acts as follows:

- If you stop the task during permissions update, further re-permissioning will be stopped. Objects already processed by that moment will have new (target) permissions. Objects not yet processed will keep old permissions. If you want to completely restore the SMS state, run the wizard with the Revert to the original object ownership and permissions option.
- If you stop the task while reverting changes, further re-permissioning will be stopped. Objects already processed by that moment will have source permissions. Objects not yet processed will keep target permissions. If you want to restore the SMS state, run the wizard with the Reassign object ownership and permissions to target users option.
- If you stop the task during cleanup of permissions, further processing will be stopped. Permissions of the objects already processed by that moment will be cleaned up. Objects not yet processed will be left intact.

Log File

The QsSmsProcessingWizard_<Timestamp>.log file is stored in the %TEMP% folder.

SMS Processing Wizard does not store information about its own activities under the History node in the Migration Manager console management tree. All data is stored in the appropriate log file.

Reconfiguring a Task

To reconfigure the task, right-click the task object and select Properties. The SMS Processing Wizard will start and let you specify different options for the task. Refer to the steps above for more information on the available options.

If some members of the local groups BUILTIN\Administrators and SMSAdmins on the source were processed by the SMS Processing Wizard, you should process these groups on the source domain controller with Resource Updating Manager to make these accounts members of the corresponding groups.
SQL Server Processing

The SQL Processing Wizard allows you to update your Microsoft SQL servers to reflect the domain migration changes that were made using Migration Manager. The SQL update should be performed after Migration Manager has been used to migrate accounts to the new domain.

SQL processing wizard does not process an SQL server if one or more of its databases is in Offline, Read Only, or Single User mode. Such behavior is merely a precaution to prevent inconsistencies in permissions.

The SQL Processing Wizard retrieves the object migration information from the migration project and replaces the old accounts it locates on the processed SQL server (the source logins) with the corresponding new accounts (the target logins).

The following SQL Server versions are supported:

- Microsoft SQL Server 2000
- Microsoft SQL Server Desktop Engine (MSDE)
- Microsoft SQL Server 2005
- Microsoft SQL Server 2008
- Microsoft SQL Server 2008 Express

SQL processing wizard does not process aliases on Microsoft SQL Server 2008 and Microsoft SQL Server 2008 Express.

The wizard automatically detects the SQL Server version and performs the updates in accordance with the server’s structure.

The wizard has the ability to merge logins. That is, if a target login name or security identifier (SID) is already used on the SQL server, or several source logins have the same target login, then the resulting target login will have its own privileges and the privileges of all the source logins as well.

The wizard cannot split database users; that is, a source database user can be migrated only to one target database user. For SQL Server 7.0 or above, once a source database user has been migrated, the SQL Processing Wizard cannot then migrate that source database user to another target database user because the source database user is already absent—it has been migrated to the first target database user.

If you decide to roll back a migration, the SQL Processing Wizard can also be used to revert the changes to the SQL server.

If accounts are merged during the update process, the wizard will not be able to separate them during the rollback. In this case, it is recommended that you restore the server from a backup if required.
SQL Objects Processed

SQL Processing Wizard replaces all occurrences of the selected migrated accounts with the corresponding target accounts.

Microsoft SQL Server 2008 and Microsoft SQL Server 2008 Express

The following objects are updated on Microsoft SQL Server 2008 servers:

- Security Logins
- Database Users
- Object Owners
- Object Permissions
- Database Owners
- Replication Publications:
  - Login Names in Publication Access Lists
  - FTP Logins for Snapshot Locations
  - Destination Owners
- Database Maintenance Plan Owners
- Legacy Database Maintenance Plan Owners
- Job Owners for SQL Server Agents
- Legacy Data Transformation Services:
  - Local Package Owners
  - Meta Data Services Package Owners
  - Meta Data Authors
- Statement Permissions
- Role Owners
- Endpoints Owners:
  - Database Mirroring Owners
  - Service Broker Owners
  - SOAP Owners
  - TSQL Owners
- Schema Owners
- Keys Owners (symmetric, asymmetric)
- Certificates Owners
- Service Broker:
  - Message Types Owners
  - Contracts Owners
  - Services Owners
  - Routes Owners
  - Remote Service Binding Owners
- Full Text Catalog Owners
- Assemblies Owners
Microsoft SQL Server 2005

The following objects are updated on Microsoft SQL Server 2005 servers:

- Security Logins
- Database Users
- Object Owners
- Object Permissions
- Database Owners
- Replication Publications:
  - Login Names in Publication Access Lists
  - FTP Logins for Snapshot Locations
  - Destination Owners
- Database Maintenance Plan Owners
- Legacy Database Maintenance Plan Owners
- Job Owners for SQL Server Agents
- Legacy Data Transformation Services:
  - Local Package Owners
  - Meta Data Services Package Owners
  - Meta Data Authors
- Aliases
- Statement Permissions
- Role Owners
- Endpoints Owners:
  - Database Mirroring Owners
  - Service Broker Owners
  - SOAP Owners
  - TSQL Owners
- Schema Owners
- Keys Owners (symmetric, asymmetric)
- Certificates Owners
- Service Broker:
  - Message Types Owners
  - Contracts Owners
  - Services Owners
  - Routes Owners
  - Remote Service Binding Owners
- Full Text Catalog Owners
- Assemblies Owners
Microsoft SQL Server 2000

The following objects are updated on Microsoft SQL Server 2000 servers:

- Security Logins
- Database Users
- Object Owners
- User-Defined Data Types
- User-Defined Functions
- Database Owners
- Replication Publications:
  - Login Names in Publication Access Lists
  - FTP Logins for Snapshot Locations
  - Destination Owners
- Database Maintenance Plan Owners
- Job Owners for SQL Server Agents and Accounts Under which the Job is Started
- Data Transformation Services:
  - Local Package Owners
  - Meta Data Services Package Owners
  - Meta Data Authors
- Linked Servers:
  - Local Logins
  - Remote Users
  - Default Remote Logins
- Remote Servers:
  - Remote Logins for login mapping
- Aliases
- Statement Permissions
- Object Permissions
- Role Owners

Microsoft SQL Server 7.0

SQL Processing Wizard updates the following objects on Microsoft SQL Server 7.0 servers:

- Security Logins
- Database Users
- Object Owners
- User-Defined Data Types
- Database Owners
- Replication Publications:
  - Login Names in Publication Access Lists
  - FTP Logins for Snapshot Delivery
  - Destination Owners
- Database Maintenance Plan Owners
• Job Owners for SQL Server Agents and Accounts Under which the Job is Started
• Data Transformation Services:
  • Local Package Owners
  • Repository Package Owners
  • Metadata Authors
• Linked Servers:
  • Local Logins
  • Remote Users
  • Default Remote Logins
• Remote Servers:
  • Remote Logins for login mapping
• Aliases
• Statement Permissions
• Object Permissions
• Role Owners

Processing Details

The target account always is preferred over the source account during the update. For instance, SQL Server does not allow you to merge aliases, so if the logins are merged and the target login already has an alias, it is left intact, and the source login’s alias is not used.

If accounts are merged during the update process and if at least one of these accounts had a deny attribute, the target account will also have a deny attribute.

The SQL Server Agent Proxy Account’s password is not updated during processing. For SQL Server to function correctly, you should set the password for the Agent Proxy Account after processing.

Also, the wizard changes ownership for database objects such as tables, views, stored procedures, extended stored procedures, rules, defaults, user data types, and user-defined functions, and it processes statement permissions and object permissions of the database user.

If any of the source accounts are renamed after the migration but before the SQL Server update, some SQL objects might have old names, but they will preserve their privileges to certain actions. Renaming the migrated accounts before processing the SQL server is not recommended.
Pre-requisites

The following requirements must be met for a successful SQL server update:

- The names of all the databases to be processed must conform to the standard Microsoft SQL naming requirements. For details, see the Microsoft SQL Server Books online article, *Rules for Regular Identifiers*.
- Processing errors will appear if the database to be processed is either of the following:
  - In Single User mode and there is already a connection to the database
  - In Read-only mode
- To preserve the consistency of the SQL server, the wizard will not update the server if any of the databases on the server are in Suspend or Offline mode.

The login used to process SQL Server versions 7.0, 2000, and 2005 must be a member of the `sysadmin` role.

In the case of the error message ‘Operation failed. Failed to migrate User1 to User2’, it is recommended that you increase the key value `[HKEY_LOCAL_MACHINE\SOFTWARE\Aelita\Enterprise Migration Manager\Current Version\SQL Processing Wizard]\LongCommandTimeout`.

Starting SQL Update

It is recommended that you run Resource Updating Manager before using SQL Processing Wizard. Otherwise, the wizard will not be able to update rights granted via membership in local groups.

It is recommended that you create a backup of the SQL server before starting SQL Processing Wizard.

You can perform SQL processing in several ways. Select the one that best suits your situation:

- Create the SQL Processing task and run it from Migration Manager. To create an SQL processing task, go to the Resource Processing | Tasks node and click the `SQL Processing` button in the right pane.
- Create a setup package for the SQL Processing task, delegate rights to perform this task to another person, and send this package to that person. The delegated administrator will then install the package and perform the SQL processing as specified in the task configuration.
- Export an INI file with the appropriate settings for SQL processing, and then create and configure an SQL processing task to run in stand-alone mode using this INI file. Refer to the Delegating Resource Update section for more details.

Regardless of the method you select, the SQL Processing Wizard will guide you through the updating process, as explained below.
Step 1. New SQL Processing Task

Specify a name for the task and add a descriptive comment.

Step 2. Select Configuration Mode

Select whether you want to delegate this task to a trusted person or whether you want to configure and schedule the task.

- **Delegate resource processing task**—Select this option if you want to create the task and delegate it to a trusted person who will run the task.
- **Configure resource processing task**—Select this option if you want to create, configure, and schedule the task.

Depending on the mode you selected, the steps offered by the wizard are different.

Step 3. Specify Re-Permissioning Options

This step is displayed regardless of the configuration mode you selected in the previous step.

This step lets you specify the options for processing SQL objects.

- **Reassign object ownership and permissions to target users**—Select this option to re-assign the permissions and ownership set to the SQL objects to the new (target) user accounts.
- **Revert to the original object ownership and permissions**—Select this option to undo re-permissioning, which removes target users from the objects’ Access Control Lists (ACL) and returns all rights to the source accounts.

If you choose the **Revert to the original object ownership and permissions** option, the following two situations are possible:

- If user A was migrated to user B, selecting this option will revert the changes made by SQL Processing Wizard.
- If user A and user B were merged to user C, permissions for the source users cannot be separated. In this case, selecting this option will revert permissions to only one of the source users.
• **Process from INI file**—Select this option if you want to retrieve the processing options from an INI file. An INI settings file can be created in Migration Manager (Tools | Export to | INI File). See the *Creating an INI File for Resource Update* section for more details. Note that if no INI file exists, the option is disabled.

This option is enabled only when the wizard is run in stand-alone mode.

**Step 4. Delegate Resource Processing Task**

This step appears only the **Delegate resource processing task** mode was selected in Step 2. If you have selected the **Configure resource processing task** option, proceed to step 5.

This step lets you specify one or more trusted accounts and delegate the rights to perform the task to these accounts.

To delegate the rights to the trusted accounts, complete the following steps:

1. Click the **Browse** button.
2. In the **Select User or Group** dialog box, select the user or group you want to delegate the rights to and click **OK**.
3. Click the **Add Account** button. The account will be added to the list of delegated accounts and automatically assigned the rights associated with the **Resource Admin** role. For more information about the available roles and the rights possessed by each, refer to the **Delegating Migration Tasks** section.

Click **Next** to proceed to the **Complete the SQL Processing Wizard** step.
Step 5. Select SQL Server

Use the Add button to add the SQL servers to be processed by this task. The Add SQL Server dialog box will appear. In this dialog box, either type the server name in the text box or use the Browse button to select the server from the list.

You can select either Windows integrated authentication or SQL Server authentication. If SQL Server authentication is selected, enter the login ID and the password, and then click OK.

The login used to process the SQL Server must be a member of the sysadmin role.

Use the Remove button to remove servers from the list. To change the credentials for a server, select the server in the list and click the Properties... button. Specify the new credentials in the SQL Server Properties dialog box.
Step 6. Specify Scheduling Options

This step allows you to specify whether the task should be started immediately or scheduled.

- **Save and start processing immediately**—Select this option to start the task immediately after you finish the wizard. To view the task execution progress, select the task object in the project tree and switch to the Information tab in the right-hand pane.

- **Save task configuration**—Select this option to save the task configuration. You can start the task any time later by right-clicking it in Migration Manager and selecting Start from the shortcut menu.

- **Save and schedule processing**—Select this option if you want to specify the time when the task should be started. You can schedule the task to be performed, for example, during the night. Click the Schedule... button to specify the time.

Step 7. Complete the SQL Processing Wizard

In this step, the wizard displays all the settings you made in the previous steps. You can print these settings for later review by clicking the Print button and then selecting the printer. You can also save the settings in a text file by clicking the Save As button and specifying the filename.

Click Finish to complete the SQL Processing Wizard. The new SQL processing task will appear under the Tasks container in the Migration Project tree.

Running SQL Update

To start an SQL processing task from Migration Manager, select the task in the project tree, right-click the task, and select the Start command from the shortcut menu.

If the SQL server agent is not running while the SQL server is being updated, a warning message will be displayed. If this message appears in the case of a running agent, then some tasks may not work properly. Restarting the SQL server agent is recommended.
To view the task execution progress, select the task object in the project tree and switch to the Information tab in the right-hand pane.

**Stopping a Task**

If for some reason you want to interrupt SQL processing, right-click the task and select the Stop command from the shortcut menu.

If you stop processing by selecting the Stop command, or the task execution is stopped due to an error, the task acts as follows:

- If you stop the task during permissions update, further re-permissioning will be stopped. Objects already processed by that moment will have new (target) permissions. Objects not yet processed will keep old permissions. If you want to completely restore the SQL state, run the wizard with the Revert to the original object ownership and permissions option.

- If you stop the task while reverting changes, further re-permissioning will be stopped. Objects already processed by that moment will have source permissions. Objects not yet processed will keep target permissions. If you want to restore the SQL state, run the wizard with the Reassign object ownership and permissions to target users option.

- If you stop the task during cleanup of permissions, further processing will be stopped. Permissions of the objects already processed by that moment will be cleaned up. Objects not yet processed will be left intact.

**Log File**

The SQL Processing Wizard log is stored in the SQLWiz.log file.

**Reconfiguring a Task**

To reconfigure the task, right-click the task object and select Properties. The SQL Processing Wizard will start and let you specify different options for the task. Refer to the steps above for more information on the options.

If you access SQL Server as a member of the local group (for example, BUILTIN\Administrators), you should process the local groups on the source domain controller with Resource Updating Manager to make the newly-created accounts members of these groups. In that case, the local groups must be excluded from processing by the SQL Processing Wizard.

**Cluster Server Migration**

Migration Manager is capable of re-permissioning a Microsoft cluster. However, it requires a more involved procedure than what is required by non-clustered servers. This section describes the detailed steps for a successful cluster migration.

Note that cluster resources are processed only if they belong to the same group as Network Name.
The procedure involves the three major steps:

1. Processing physical nodes with Resource Updating Manager
2. Processing virtual servers with Vmover.exe (remotely)
3. Joining physical nodes to the target domain

There are two variations on the steps that can be taken:

**Option 1**

1. Select all nodes in Resource Updating Manager. Make sure you select only the actual nodes and not the virtual servers.
2. Specify the processing settings and process the nodes as typical computers. This will process all resources except the cluster shares, cluster database, and cluster printers.
3. From the Tools menu in Quest Migration Manager, select Export to | INI file. The Export INI File dialog box will appear.
4. Select Resource Updating in the Wizard’s Name list box.
5. Specify a name and path for the INI file in the INI file field or leave the default.
6. Specify the required options for processing.
7. Click OK. This will create an INI file in the folder you specified.
8. Run the following command remotely from the console machine against each virtual server, and run it run from the location where the Vmover.exe file and the Vmover.ini files reside:

   `Vmover.exe /c /system=<Virtual_Server_Name> /ini=Vmover.ini`

9. Using Resource Updating Manager, move the nodes to the target domain (without rebooting). After a couple of minutes all nodes and the virtual server will appear in the target domain.

   Always move all cluster nodes to the new domain simultaneously. Do not move a virtual server to the new domain.

   The Cluster Service account is not changed when a cluster server is moved to another domain.

10. Reboot the passive node. Verify that the Cluster Service account on this node is changed to the target account.
11. Restart the Cluster Service on the active node. Verify that the Cluster Service account on this node is changed to the target account.

   During the restart of the service the resources will not be available.

12. After a successful start of the Cluster Service on the active node, start the cluster service on the passive node.
13. Move the resources to the passive node and reboot the active node.
14. After the node restarts move the resources back.
**Option 2**

Follow steps 1–9 above. Then, instead of taking steps 10–14, reboot both nodes at the same time.

Whether you choose Option 1 or Option 2, the resources will be unavailable for a period of time, because the cluster service cannot run using two accounts (source and target). Both of the nodes should be running using the same account (either source or target), as Microsoft documentation states:

> "The Cluster service on all nodes must be stopped and restarted during this procedure (changing the account under which the Cluster service runs). The Cluster service must use the same account and password at all times on all nodes within the cluster."

Refer to the following articles for more details:

**For Windows 2000:**


**For Windows 2003:**


Please pay attention when specifying the name of a cluster. Use the virtual cluster name, not the name of a node; otherwise, Vmover cannot verify that the computer is part of a cluster and will not process it.

**Delegating Resource Update**

In a distributed migration project management model, Migration Manager can greatly facilitate resource update at a site or in resource domains where you cannot get administrative access to computers. Decentralizing resource update is also useful if computers to be updated are located across a slow WAN connection and therefore sending multiple agents, no matter how small, would consume too much of the available bandwidth.

In these scenarios, you can delegate the resource updating tasks to the remote site or to other domain administrators who have the required level of access and are located within an area of good connectivity to the computers to be updated.

Resource update can be delegated by either of the following methods:

- Creating a setup package for a preconfigured Resource Updating Manager console.
- Exporting an INI file and performing resource update using this file by running the updating tools in stand-alone mode or running resource update from the command line.

These techniques are described in more detail below.
Resource Update Using Preconfigured Resource Updating Manager

In some highly distributed environments, the geographically dispersed administrators in charge of post-migration resource processing can benefit from having a dedicated resource updating console detached from the rest of the migration tools. For such purposes, Resource Updating Manager can package itself into a setup file, which can be sent to any administrator who needs it. The resulting setup file automatically contains all of the relevant configuration for the ongoing migration project, such as the ADAM database connection settings.

To create a dedicated, preconfigured Resource Updating Manager setup file, select Tools | Create Resource Updating Manager setup.

Next, grant resource updating privileges to the user or users that you expect to use the preconfigured console. For that, right-click the Resource Updating node and select Delegate. You will be prompted to specify the account to give the privileges to. Note that a user will not be able to use the console unless they have been granted the privileges in this way.

Creating an INI File for Resource Update

You can create the INI files for the following resource updating tools:

- Resource Updating Manager
- Exchange 5.5 Processing Wizard
- Exchange Processing Wizard
- SQL Processing Wizard
- SMS Processing Wizard
- Active Directory Processing Wizard

To create an INI file for a resource updating tool

1. From Tools menu in Quest Migration Manager, select Export to | INI file. The Export INI File dialog box will appear.
2. Select resource updating wizard’s name in the Wizard’s Name list box.
3. Specify the INI file name and path in the INI file field or leave the default.
4. Select the desired re-permissioning options.
5. Click OK. This will create the INI file in the folder you specified in step 3.

Command-Line Resource Update

The command-line tool Vmover.exe, located in the \%ProgramFiles\%\Common Files\Aelita Shared\Migration Tools folder by default, can be used to update resources without installing an agent. The update can be performed directly from the command-line interface or via a logon script.

Among the main applications of Vmover are the following tasks:

- Updating remote resources
- Processing roaming profiles
- Processing file system permissions on NT-compatible non-NT systems
Vmover can be used to process resources on a computer running NT 3.51 or later (NT 4 SP4 or later if SIDHistory mapping is used).

To perform the updates, Vmover retrieves the source-target account pairs from the INI file or target accounts’ SIDHistory. The INI file also contains the required parameters. Some parameters can be set from the command line.

**Command-Line Parameters**

Vmover should be run using the following command-line syntax:

```
```

**Explanation**

/c — Mandatory parameter for command-line usage.

/ini — Optional parameter. Name of the INI file that contains the parameters for the update.

By default, the Vmover utility searches its folder for the *Vmover.ini* (compressed) file, and, if the file is not found, then for the *Vmover.ini* (uncompressed) file.

You can use Vmover’s /ini parameter to specify an alternative INI file name and location. In this case Vmover will also first search for the file’s compressed version. For example, if you specify *File.txt*, Vmover will first attempt to locate *File.txt*, and then *File.txt*.

Thus, if you specify an uncompressed INI file to be created, but there is a compressed file with the same name in Vmover’s folder, Vmover will use the compressed file instead of the specified one.

For more information on creating INI files for processing resources, refer to the *Creating an INI File for Resource Update* section.

/roaming — Processes roaming profiles. If the /roaming parameter is specified, Vmover will process only profile on which the parameter’s value indicates. Recursive bypass through the subfolders with profiles will not be performed.

If you specify the /volume or /roaming parameter, Vmover will not update other resource types in the INI file (such as group membership or user rights).

/volume — Processes file system permissions in the specified location

If you specify the /volume or /roaming parameter, Vmover will not update other resource types in the INI file (such as group membership or user rights).

/system — Specifies the computer name. By default, the local computer is updated.

/log — Specifies the location of the log file by means of overriding the LogFile key in the INI file.
/exclude—Sets exclude masks. Use the | symbol as a divider and the * symbol as a wildcard. During processing Vmover skips files and directories if their names match one of the specified exclude masks.

/excludepath—Sets exclude paths. Use the | symbol as a divider. During processing Vmover skips directories if their names match one of the specified exclude paths. This parameter should specify network paths, not local file system paths.

/recursion—Sets the recursion level. Vmover processes file system to the depth specified in this parameter, starting either from the path given in the /volume parameter (if specified) or from the root drive path.

/affinity—Sets the CPU affinity mask in a view of a bit mask that indicates what processors are eligible to be selected for work. The value of 1 means that only first processor will be used, the value of 2 means that only second processor will be used, the value of 3 allows to use only first and second processors and so on. If the mask specifies the number of processor, that exceeds the real number of processors in the system, Vmover will exit with an error displayed.

/priority—Sets the priority for Vmover.exe for the resource updating process, allowing you to avoid overloading the client computers when resource processing is running during working hours. The following priority values are used:

- A value of -2 means Low priority.
- A value of -1 means Below Normal priority.
- A value of 0 means Normal priority.
- A value of 1 means Above Normal priority.
- A value of 2 means High priority.
- A value of 3 means Realtime priority.

Note: The priority values Below Normal and Above Normal are unavailable on client computers running Microsoft Windows NT4.

To study examples of using of these parameters, run Vmover.exe with parameter /?.

To perform recursive bypass through the subfolders with profiles, create the INI file with the Roaming profiles option enabled and run Vmover from the command line without the /roaming parameter. For example:

Vmover.exe /c [/INI=IniFile] [/system=Computer]

Remote Update

By default, Vmover applies the changes specified in the INI file on the local computer. To make Vmover update a remote computer, use the /system command-line parameter or add the /System=TargetComputerName key to the INI file. The following example shows how to use the /system command-line parameter:

Vmover /c /system=Mars

When Vmover is updating a remote computer, it locates all the system shares of the computer (such as c$ and d$) and updates all the files and folders located in the shares.
To update a specific share of the computer, use the `/volume` command-line parameter. In this case, no other shares will be affected. The following example shows how to use the `/volume` parameter:

```
Vmover /c /volume=\Mars\Demos
```

If you use the `/volume` parameter, Vmover will not process any other options in the INI file (such as group membership or user rights). Only file system permissions of the specified share will be processed.

For a successful remote update, the account under which Vmover is started must be administrative and have the following privileges on the remote and local computers (granted explicitly or by establishing a `net use` connection):

- Restore files and directories
- Backup files and directories
- Take ownership of files and other objects
- Manage auditing and security log
- Bypass traverse checking

For successful IIS permissions processing on the remote computer, IIS must also be installed on the computer on which Vmover is running and the account under which Vmover is started must be a local administrator on the computer being processed.

**SIDHistory Mapping**

By default, Vmover’s INI file contains source-target account pairs migrated by the moment when the file was generated.

Alternatively, Vmover can automatically locate and append to the INI file the pairs by analyzing the SIDHistory of the accounts in the target domain. This lets you use the tool even if the object migration was performed not by Quest Migration Manager but by another tool capable of adding SIDHistory.

If Vmover was already run with the same INI file, it will locate and append to the INI file the information about the newly migrated accounts.

To use SIDHistory mapping, the following parameters need to be added to the `[options]` section:

<table>
<thead>
<tr>
<th>PARAMETER</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIDHistory=Yes/No</td>
<td>Set this parameter to <strong>Yes</strong> to enable SIDHistory mapping.</td>
</tr>
<tr>
<td>hostName=Host_Name:Port_Number</td>
<td>Specify the target domain controller and the port number to be used for LDAP queries.</td>
</tr>
<tr>
<td>ldapUser=UserName</td>
<td>The username to be used for LDAP requests.</td>
</tr>
<tr>
<td>ldapDomain=UserDomain</td>
<td>The name of the target domain.</td>
</tr>
<tr>
<td>ldapPsw=Password</td>
<td>The password for the ldapUser user account.</td>
</tr>
</tbody>
</table>
The source domains are specified in a separate section [SourceDomains]. Each line of the section should contain a source domain name and its SID, separated by a semicolon character (;).

The following is an example of an INI file with SIDHistory mapping:

```
[dmw4]
[Options]
FileSystem=No
Shares=Yes
LocalGroups=No
UserPrivileges=No
Printers=No
Registry=No
Profiles=No
InstallProfilesAgent=Yes
Services=No
ScheduledTasks=No
Clone=Yes
CleanUp=No
Undo=No
AutoRemove=No
MaxErrors=10
LogMask=-1
LogFile=Vmover.log
StateFile=Vmover.txt
Version=400
MaxCriticalErrors=10
MaxRegUsage=95
ProcessRegGroupOwner=No
UpdateStateSec=1
SetArchiveBit=No
sidHistory=Yes
hostName=pdc-target2000:389
ldapUser=administrator
ldapDomain=target2000
ldapPsw='adminpswd'
[SourceDomains]
TRUST;S-1-5-21-750286249-1451910610-2033415169
```

If SIDHistory mapping is used but the source-target pairs are also listed, both the SIDHistory pairs and the explicitly set pairs are used.

💡 For troubleshooting purposes, you can enable extended logging. To do this, set the `LogMask` parameter value to 255 (default value is 15). Note that enabling extended logging may lead to the generation of huge log files.
SharePoint Processing

To reassign Microsoft SharePoint permissions after your migration, use the SharePoint Permissions Processing wizard. The wizard will grant SharePoint permissions of the source users to the matching target users.

Installing the Wizard

To install the wizard, take the following steps:

1. Open the QMM\InstallationFolder\Console directory.
2. Copy either the SharePointProcessing.msi file or the SharePointProcessingX64.msi file to the SharePoint server you want to process, depending on the operation system installed in your environment. Separate MSI files are provided for x86 and x64 operating systems.
3. Run the MSI file on the SharePoint server and complete the installation wizard.

System Requirements

The SharePoint Permissions Processing wizard requires Microsoft .NET Framework 2.0.

Required Permissions

Before you run the wizard, make sure your account has the following permissions:

- Member of Central Administrator group for SharePoint server
- Member of the local Administrators group on the computer running the SharePoint Permissions Processing

Processing SharePoint Permissions

To update SharePoint farm environment you need to start the wizard once, on any front-end SharePoint server.

To reassign Microsoft SharePoint permissions, take the following steps:

1. Click Start | All Programs | Quest Software | SharePoint Processing Wizard to run the wizard.
2. On the Welcome screen, click Next.

On the Select Configuration File screen, specify the location of the INI configuration file. Click Next.
To get the file, export INI file, as follows:

1. From Tools menu in Migration Manager Console, select Export to | INI file. The Export INI File dialog box will appear.
2. Select any wizard in the Wizard’s Name list box.
3. Specify the INI file name and path in the INI file field, or leave the default. Click OK. This will create INI file in the folder you specified in step 3.

3. On the Select Processing Options screen, select either of the following options:
   a) Reassign source accounts' permissions to target users—This option allows you to change the permissions of the source accounts on the selected server to the new (target) user accounts, select the first option.
   b) Revert to the original accounts' permissions—This option lets you undo re-permissioning. It removes target users from the access lists and returns all rights to the source accounts.

If you click Cancel while reverting back the changes, further re-permissioning will be stopped. Objects that are already processed by that moment will have source permissions. Objects that are not yet processed will keep target permissions. If you want to restore the SharePoint state, run the wizard with the Reassign source accounts' permissions to target users option.
4. Click **Next** to start processing permissions.

5. On the **Summary** screen, you may review results and statistics of permission processing.
   If any errors occurred during processing, they are indicated in the **Summary**.
   Error descriptions are available in the log file.

6. Click **Finish** to exit the wizard.
Rolling Back Migration Changes

Directory Migration Rollback

Finished migration sessions can be rolled back. Once you have completed a session, you may want to undo changes you made to Active Directory.

To restore the original domain state, take the following steps:

1. Right-click on the session name in the Quest Migration Manager and select the **Undo** item on the shortcut menu.
2. Complete the Undo Wizard’s steps.

Refer to the *Undo Account Migration* section for more details.

Resource Update Rollback

All Migration Manager resource updating tools (Resource Updating Manager, Active Directory Processing Wizard, Exchange 5.5 Processing Wizard, Exchange Processing Wizard, SMS Processing Wizard, and SQL Processing Wizard) can roll back the changes they have previously made. All you need to do is start the tool, choose the **Revert processing** option, and complete the steps of the wizard.
About Quest Software, Inc.

Quest simplifies and reduces the cost of managing IT for more than 100,000 customers worldwide. Our innovative solutions make solving the toughest IT management problems easier, enabling customers to save time and money across physical, virtual and cloud environments. For more information about Quest go to www.quest.com.

Contacting Quest Software

Email info@quest.com
Mail Quest Software, Inc.
World Headquarters
5 Polaris Way
Aliso Viejo, CA 92656
USA
Web site www.quest.com

Refer to our Web site for regional and international office information.

Contacting Quest Support

Quest Support is available to customers who have a trial version of a Quest product or who have purchased a Quest product and have a valid maintenance contract. Quest Support provides unlimited 24x7 access to SupportLink, our self-service portal. Visit SupportLink at http://support.quest.com/

From SupportLink, you can do the following:

- Retrieve thousands of solutions from our online Knowledgebase
- Download the latest releases and service packs
- Create, update and review Support cases

View the Global Support Guide for a detailed explanation of support programs, online services, contact information, policies and procedures.

The guide is available at: http://support.quest.com.
Quest Migration Manager for Active Directory contains some third party components (listed below). Copies of their licenses may be found at http://www.quest.com/legal/third-party-licenses.aspx.

### COMPONENT LICENSE OR ACKNOWLEDGEMENT

<table>
<thead>
<tr>
<th>COMPONENT</th>
<th>LICENSE OR ACKNOWLEDGEMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boost 1.34.1</td>
<td>Boost 1.0</td>
</tr>
<tr>
<td>TinyXml 2.2.1</td>
<td>This product contains portions of the PAWN scripting software (formerly known as SMALL).</td>
</tr>
<tr>
<td>ZLib 1.1.4</td>
<td>Copyright (C) 1995-2005 Jean-loup Gailly and Mark Adler</td>
</tr>
</tbody>
</table>

A copy of the source code for these component may be available at http://rc.quest.com, if necessary to fulfill attribution requirements.

### Boost 1.0 License Agreement

Boost Software License - Version 1.0 - August 17th, 2003

Permission is hereby granted, free of charge, to any person or organization obtaining a copy of the software and accompanying documentation covered by this license (the "Software") to use, reproduce, display, distribute, execute, and transmit the Software, and to prepare derivative works of the Software, and to permit third-parties to whom the Software is furnished to do so, all subject to the following:

The copyright notices in the Software and this entire statement, including the above license grant, this restriction and the following disclaimer, must be included in all copies of the Software, in whole or in part, and all derivative works of the Software, unless such copies or derivative works are solely in the form of machine-executable object code generated by a source language processor.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NONINFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE FOR ANY DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

### ZLib 1.1.4 License Agreement

/* zlib.h -- interface of the 'zlib' general purpose compression library
 version 1.2.3, July 18th, 2005

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly jloup@gzip.org
Mark Adler madler@alumni.caltech.edu