Quest

Quest® Migration Manager for Active Directory
8.14

Resource Processing Guide

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.

Attn: LEGAL Dept

4 Polaris Way

Aliso Viejo, CA 92656

Refer to our Web site (https://www.quest.com) for regional and international office information.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at https://www.quest.com/legal.

Trademarks

Quest, the Quest logo, and Join the Innovation are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit https://www.quest.com/legal/trademark-information.aspx. All other trademarks and registered trademarks are property of their respective owners.

Legend

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

IMPORTANT, **NOTE**, **TIP**, **MOBILE**, or **VIDEO**: An information icon indicates supporting information.

Migration Manager for Active Directory Resource Processing Guide
Updated - December 2017
Version - 8.14

Contents

Introduction to Resource Update

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. Production servers, such as Exchange server, SQL server, SharePoint server , Systems Management Server (SMS) and System Center Configuration Manager (SCCM).

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.

Resource Update Task	Description	Tool Used	Reference
Distributed resource update	Update ACLs for distributed resources, service accounts, user profiles, etc., including those residing on cluster servers	Resource Updating Manager	See the Delegating Resource Update topic.
Active Directory update	Update security descriptors for Active Directory objects in selected domains	Active Directory Processing Wizard	See the Active Directory Processing topic.
Exchange Server update	Update permissions set on Exchange 2000–2013 servers	Exchange Processing Wizard	See theExchange Server Processing topic.
Systems Management Server update	Update permissions on Systems Management Server and System Center Configuration Manager	SMS Processing Wizard	See the SMS Processing topic.
SQL Server update	Update permissions on SQL servers	SQL Processing Wizard	See the SQL Server Processing topic.
SharePoint permissions update	Reassign SharePoint permissions after your migration	SharePoint Permissions Processing Wizard	See theSharePoint Processing topic.

Distributed Resource Update

Distributed resource update is the most time-consuming and requires the most planning. It is performed in the Resource Updating Manager console.

The typical scenario for working with Resource Updating Manager is as follows:

1. Identify the computers to be processed and install resource processing agents on them.
2. Organize the computers into collections for scheduling purposes.
3. Schedule the processing and subsequent move operations for the collections.
4. After the computers have been moved to the target domain, decommission the resource processing agents installed on them.

For details about using Resource Updating Manager, see the Distributed Updates in Resource Updating Manager topic.

Resource Updating Manager can be used centrally on the Migration Manager Console computer. You can also package and use a standalone Resource Updating Manager console. This lets you delegate the task to other administrators. For details, see the Delegating Resource Update topic.

Production Server Update

Production server-related tasks that do not involve Resource Updating Manager 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, for that, refer the table in the Introduction to Resource Update topic. To create the task, in Migration Manager go to the **Resource Processing | Tasks** node and click the corresponding button in the right pane. For more detail, see the table in the Introduction to Resource Update topic.
- 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 in the Introduction to Resource Update topic) or from the command line by specifying this INI file. Refer to the Delegating Resource Update topic for more details.

For more details, see the related topics:

- Selecting Objects for Processing Explicitly
- Delegating Resource Update
- Resource Update Considerations
- Active Directory Processing
- Exchange Server Processing
- SMS Processing
- SQL Server Processing

- Cluster Server Migration
- Command-Line Resource Update
- SharePoint Processing

Distributed Updates in Resource Updating Manager

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 Services (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

The actual processing is done by Resource Updating Manager agents, which are deployed on the computers you need to process and controlled from the Resource Updating Manager console. To handle large, geographically dispersed networks, the agents 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.

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

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**. Alternatively, run the application directly from the **Start** menu.

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/AD LDS 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.

Before You Update Resources

Before you start processing resources in your network, you should complete the following tasks:

- Obtaining Administrative Rights over the Computers
- Deciding on the Use of Agents
- Pre-installing Resource Updating Manager Agents

IMPORTANT: For a successful resource update, trusts should be established between source and target domains.

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

CAUTION: 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/AD LDS 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.

NOTE: 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.

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

Deciding on the Use of Agents

In most situations, resources are updated by Resource Updating Manager agents that are installed locally on the computers you want to process. However, agents are not always required for successful resource update. Resource Updating Manager can perform the necessary operations remotely without agents if the network environment permits this.

The following table shows the differences between the two operation modes:

Comparison Criteria	With Agents	Without Agents
Resource updating and computer moving works over a firewall	Yes	No
Network traffic	Insignificant	High when many computers are processed at once
Additional software needs to be deployed on the local computers	Yes, the agent	No
NAS resources can be processed	No	Yes
Recommended for computers that are online only occasionally (for example, laptops)	Yes, with group policy or similar methods used for agent deployment	No

Agents are installed automatically in the following situations:

- As part of a computer discovery task (see Discovering Computers for details)
- When a task with the **Perform the task remotely (without agents)** option disabled starts running on a computer that has no agent

For details about other ways to install Resource Updating Manager agents, see the next section.

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. Also Resource Updating Manager Agents cannot be installed from Resource Updating Manager console to computers with a firewall turned on. To avoid these issues, you can deploy Resource Updating Manager Agents on the computers you want to update using Group Policy, SMS Server and similar tools, or manually.

NOTE: When you deploy Resource Updating Manager Agents via Group Policy, make sure that you have the **Full Control** permission over the shared folder where the agent setup is located.

If the NetBIOS protocol is not supported in your configuration, use the following registry keys to process the workstations:

- For RUM agents that are distributed via agent setup: **HKEY_LOCAL_MACHINE\SOFTWARE\Aelita\Migration Tools\CurrentVersion\Resource Updating Manager** (create this registry key if it does not exist)
  Create the **RemoteController** parameter in the **Resource Updating Manager** registry key on the computer where RUM console with RUM controller is installed and add the parameter value in one of the following formats: FQDN, IP address or NetBIOS name of the RUM Controller Service server.
- For RUM agents that are distributed via Resource Updating Manager console: **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\QsRUMController\Config**
  Create the **RemoteController** parameter in the **Config** registry key on the computer where RUM console with RUM controller is installed and add the parameter value in one of the following formats: FQDN, IP address or NetBIOS name of the RUM Controller Service server.

To create agent setup

1. Log on to the console with an account that has administrative rights over the computers. See the Obtaining Administrative Rights over the Computers topic 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.

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.

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
```

NOTE: 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
```

NOTE: 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 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 (some computers may be turned off, or behind the firewall, or you just deploy an agent to the host via Group Policy, Systems Management Server or manually).

NOTE: 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 the Processing Scope topic, and use drag-and-drop to reorganize computers.

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.

NOTE: 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 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.

CAUTION: There is a separate task queue for each instance of Resource Updating Manager. Your Resource Updating Manager console displays tasks created in other console instances, but cannot queue additional tasks after them.

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.

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 step, you can use the **Perform the task remotely (without agents)** option to specify whether you want to use Resource Updating Manager agents for this task. Selecting this option will make sure that agents are not used on the computers where they are installed; instead, the task will be performed directly from the computer where this instance of Resource Updating Manager is installed. If the option is cleared, agents will be used; they will be installed on computers that do not have them. If you use agents, you also have the option of running custom scripts locally on the computers before and after the task.
   On the same step, the Show processing progress for individual computers option lets you enable the display of basic task progress information next to each computer list entry. Note that enabling this option increases network traffic, so using it for a large number of computers may be undesirable.
6. On the next step you can specify when the task starts. You can start the task immediately by selecting the Start now option or select the Start at option to specify the date and time to start the operation.

   NOTE: If you are not using agents (the Perform the task remotely (without agents) option is selected on the Advanced Options step), the same step lets you specify the pending timeout for the task operation in case some computers are not accessible at the task start time (some computers may be turned off, or behind the firewall, or you just deploy an agent to the host via Group Policy, Systems Management Server or manually). If the task is not able to start before the deadline you set, then Resource Updating Manager will cancel this task and all subsequent queued tasks for the inaccessible computers.
7. On the Task Description step you can specify an optional task description.
8. Click **Finish** to start processing.

You can review and edit the schedule and other settings for any task that has not started. For that, right-click the task and select **Edit Properties**. In addition, you can run any task immediately, regardless of its schedule (see the Running Tasks Immediately topic.

For more details, see Configure Processing Settings.

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.

Specifying Objects for Processing

By default, Resource Updating Manager will perform the updates for accounts (also referred to as security principals or objects) that were migrated by Migration Manager for Active Directory.

However, you can manually define the accounts you want to update the resources for. You have two options how to do that:

- Manually select the accounts from the list of all migrated accounts
- Specify the external file that contains list of accounts

Selecting Accounts Manually

To manually select accounts to process resources for, right-click the collection or category node in the console management tree and click **Operate with Selected Accounts**. After that select the specific set of accounts to process.

Specifying Accounts from File

To specify an account matching file with accounts to process resources for, right-click the collection or category node in the console management tree and click **Operate with Accounts from File**. In the opened dialog box click **Browse** and select an account matching file.

The account matching file must contain a list of migration pairs in the following format, one pair per line:

```
SourceNetBIOSDomainName\SourceUserName,SourceUserSID,SourceUPN,SourceDomainDNSName,TargetNetBIOSDomainName\TargetUserName,TargetUserSID,TargetUPN,TargetDomainDNSName
```

The following is an example of possible account matching file:

```
SOURCE1\user1.name,S-1-5-21-sourceUser1SID,user1@source1.principal.name,source1.com,TARGET1\user1.name,S-1-5-21-targetUser1SID,user1@target1.principal.name,target1.com
SOURCE2\user2.name,S-1-5-21-sourceUser2SID,user2@source2.principal.name,source2.local,TARGET2\user2.name,S-1-5-21-targetUser2SID,user2@target2.principal.name,target2.local
```

NOTE: To select all accounts migrated by Migration Manager for Active Directory for updating resources for, you need to right-click the collection or category node in the console management tree and click **Update for All Migrated Accounts**. Note that current account selection will be lost.

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.

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

  NOTE: If two source users were merged to one target user, and if only one of them had permissions on some objects, then, after resource update and reverting the permissions, both users would have common permissions on these objects.

If you select the **Reassign local group membership, user rights, and object permissions to target users** option, the next step will be Account Matching. On this step, you have the following options:

- Use only the matching information from the project configuration
- Match accounts by analyzing the SID history in the target domain in addition to existing matches

If you select to match accounts by SID history data, the **Vmover.exe** utility will be used automatically for that. You only need to specify the target domain where to examine SID history data.

For access to the domain, the utility will use the credentials configured for the project (**Project | Manage Domain Credentials** in the main menu) or for the particular collection or category (the **Manage Domain Credentials** button in the toolbar when the collection or category is selected). Make sure that valid credentials are specified.

NOTES: If you use the Create Processing Task wizard for the purpose, SID history matching behaves as follows:

- After resource processing, the “clean up” and “revert” actions are possible only for those accounts that have been migrated by Migration Manager.
- The domain credentials must be specified before you run the Create Processing Task wizard.

If you need different behavior, consider using **Vmover.exe** manually, as described in SIDHistory Mapping.

Also note that the password for domain access is stored in plain text in the **ldapPsw** parameter of the configuration file for **Vmover.exe**. Because of this, it is recommended that you run the task remotely—that is, the **Perform the task remotely (without agents)** option is enabled on the Advanced Options step.

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**.

NOTE:

- 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**.

NOTE:

- Scheduled task accounts are replaced whether or not the Leave source accounts' permissions option was selected.
- For a successful scheduled task update, 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 re-assigned 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)

For the full lsit of processed IIS properties, see the *IIS* section of Vmover Processing Options.

NOTE: 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>

CAUTION: 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.

  NOTE: In this case only several types of objects will be processed, for example, shares. This option is needed for NAS 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 the related topics:

- Start Moving Computers
- Configure Move Computers to Domain Settings
- Moving Exchange Servers to Another Domain
- Moving Cluster Servers to Another Domain

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. On the Advanced Options step, you can use the **Perform the task remotely (without agents)** option to specify whether you want to use Resource Updating Manager agents for this task. Selecting this option will make sure that agents are not used on the computers where they are installed; instead, the task will be performed directly from the computer where this instance of Resource Updating Manager is installed. If the option is cleared, agents will be used; they will be installed on computers that do not have them. If you use agents, you also have the option of running custom scripts locally on the computers before and after the task.
7. On the next step you can specify when the task starts. You can start the task immediately by selecting the Start now option or select the Start at option to specify the date and time to start the operation.

   NOTE: If you are not using agents (the **Perform the task remotely (without agents)** option is selected on the Advanced Options step), the same step lets you specify the pending timeout for the task operation in case some computers are not accessible at the task start time (some computers may be turned off, or behind the firewall, or you just deploy an agent to the host via Group Policy, Systems Management Server or manually). If the task is not able to start before the deadline you set, then Resource Updating Manager will cancel this task and all subsequent queued tasks for the inaccessible computers.
8. On the Task Description step you can specify an optional task description.
9. Click **Finish** to start processing.

You can review and edit the schedule and other settings for any task that has not started. For that, right-click the task and select **Edit Properties**. In addition, you can run any task immediately, regardless of its schedule (see the Running Tasks Immediately topic).

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.

NOTES:

- 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 a computer account in the source Active Directory has child objects with the Windows BitLocker Drive Encryption recovery information, then identical objects will be created for the corresponding computer account in the target Active Directory.
- Resource Updating Manager cannot move domain controllers, cluster servers, non-Windows computers, and unknown computers between domains.
- 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.
- See the Moving Exchange Servers to Another Domain topic 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 and the target organizational unit (optional). 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 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.

NOTE: 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.

   NOTE: The above permissions are normally added with the first installation of an Exchange Server to the domain.
4. Follow the procedures in Microsoft KB article 297295.

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.

NOTE:

- Moving cluster server to another domain is not supported for Windows Server 2008 or higher.
- 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 file system 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.

NOTE: 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.

Renaming Computers

By default, when computers are migrated from the source to the target domain their names are not changed. However, you can choose to rename the computers in the target domain. For that, 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 rename task.
2. Select **Create Task | Rename** from the short-cut menu.
3. On the Old and New Names step, specify pairs of old and new computer names.
4. On the Computers Restart Options step, specify whether computers should be restarted automatically to complete the rename task. Also, you can specify the following options:
    - 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.
5. On the Advanced Options step, you can use the **Perform the task remotely (without agents)** option to specify whether you want to use Resource Updating Manager agents for this task. Selecting this option will make sure that agents are not used on the computers where they are installed; instead, the task will be performed directly from the computer where this instance of Resource Updating Manager is installed. If the option is cleared, agents will be used; they will be installed on computers that do not have them. If you use agents, you also have the option of running custom scripts locally on the computers before and after the task.
6. On the next step you can specify when the task starts. You can start the task immediately by selecting the **Start now** option or select the **Start at** option to specify the date and time to start the operation.

    NOTE: If you are not using agents (the Perform the task remotely (without agents) option is selected on the Advanced Options step), the same step lets you specify the pending timeout for the task operation in case some computers are not accessible at the task start time (some computers may be turned off, or behind the firewall, or you just deploy an agent to the host via Group Policy, Systems Management Server or manually). If the task is not able to start before the deadline you set, then Resource Updating Manager will cancel this task and all subsequent queued tasks for the inaccessible computers.
7. On the Task Description step, specify the task description for further reference and then click **Next**.
8. Click **Finish**.

You can review and edit the schedule and other settings for any task that has not started. For that, right-click the task and select **Edit Properties**. In addition, you can run any task immediately, regardless of its schedule (see the Running Tasks Immediately topic).

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. Specify when the task starts. You can start the task immediately by selecting the **Start now** option or select the **Start at** option to specify the date and time to start processing.
5. On the Task Description step, specify the task description for further reference and then click **Next**.
6. Click **Finish**.

You can review and edit the schedule and other settings for any task that has not started. For that, right-click the task and select **Edit Properties**. In addition, you can run any task immediately, regardless of its schedule (see the Running Tasks Immediately topic).

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.

   NOTE: 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 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 (some computers may be turned off, or behind the firewall, or you just deploy an agent to the host via Group Policy, Systems Management Server or manually).
6. On the Task Description step you can specify an optional task description.
7. Click **Finish**.

NOTE: 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 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 (some computers may be turned off, or behind the firewall, or you just deploy an agent to the host via Group Policy, Systems Management Server or manually).
5. Click **Finish**.

You can review and edit the schedule and other settings for any task that has not started. For that, right-click the task and select **Edit Properties**. In addition, you can run any task immediately, regardless of its schedule (see the Running Tasks Immediately topic).

Running Tasks Immediately

Assigning a schedule is one of the steps to create a Resource Updating Manager task. In some situations, you may need to run a task immediately instead of waiting for its scheduled time. For that, right-click the task and select **Start Now**.

Note that tasks are one-off operations. Using the **Start Now** command resets the task's current schedule so that the task starts straight away. Once the task has started, it cannot be rescheduled any more. If you want to repeat the task later, use a copy of it.

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.

NOTE:

- 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 or AD LDS 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(x86)%\Common Files\Aelita Shared\Migration Tools\Resource Updating** folder (on 64-bit Windows) or in the **%ProgramFiles%\Common Files\Aelita Shared\Migration Tools\Resource Updating** folder (on 32-bit Windows) on the console computer

NOTE: The **Discover computer information, Process computer resources, Move Computer to domain** and **Cleanup computer** actions create log files in the **%Program Files%\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 Profile Update topic first and then perform the additional actions described in the Roaming Profile Update topic.

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 (except for Windows 10 profiles; see details below).

IMPORTANT: Avoid performing revert of a local user profile while the target user is logged on. Otherwise, the target user will not be able to save current work and log out properly.

Specifics of Windows 10 Profile Update

Before updating local user profiles on a computer running Windows 10, consider the following specifics:

- A source user will no longer be able to sign in to the existing user profile after local user profile processing. A new profile will be created for the source user at first sign-in after processing.
- If during profile processing source user is signed in, a same profile will be used for both source and target users until the source user signs out. After that the profile will no longer be accessible for the source user.

CAUTION: Do not perform revert of a local user profile while the target user is logged on. Otherwise, the Start menu may not work for that local user profile. If this happens, you will not be able to fix the Start menu for the affected profile.

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.

NOTE: 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.

CAUTION: 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:

```
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:
http://www.microsoft.com/downloads/details.aspx?FamilyId=1B286E6D-8912-4E18-B570-42470E2F3582

Automating Distributed Resource Processing

Resource Updating Manager operation can be automated using Resource Updating Toolkit for PowerShell (PowerRUM). For information how to use it, see the *Resource Updating Toolkit for PowerShell Reference*.

Common Resource Update Workflows

This section describes common procedures that help update the resources on different types of production servers after an Active Directory migration. These suggestions will work across the different resource updating wizards:

- Exchange Processing Wizard
- Active Directory Processing Wizard
- SQL Processing Wizard
- SMS Processing Wizard
- SharePoint Permissions Processing Wizard

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**.

NOTE: 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. Click **Yes**.

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.
- Creating a setup package for a resource processing task.
- 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 in related topics.

Resource Update Using Task Setup Packages

If you need to delegate a resource processing task, you can create a setup package for the task. The setup package is a standard MSI installation file. There are two types of the setup packages:

- Containing the task configuration only—for administrators with Migration Manager installed on their workstations
- Containing the task configuration and executables needed to run this task—for administrators without Migration Manager installed

To create an MSI installation file, take the following steps:

1. Right-click the task in Migration Manager.
2. Click **Create Setup** on the shortcut menu.
3. Select the replica of the ADAM/AD LDS instance that contains your migration project.
4. Specify the output folder for the package.
5. Select the type of MSI installation package.
6. Click **Start**.

When you have successfully created the task setup package, locate the MSI file in the specified folder and send it to the delegated administrator.

The delegated administrator should then install the package and perform the resource processing as specified in the task configuration. He or she cannot change the configuration of the task. Note that the custom packages must be installed using an administrative account with elevated privileges.

Creating an INI File for Resource Update

You can create the INI files for the following resource updating tools:

- Exchange Processing Wizard
- SQL Processing Wizard

- SMS Processing Wizard
- Active Directory Processing Wizard

To create an INI file for a resource updating tool

1. In the Resource Updating Manager console, create a new collection or choose an existing one.
2. Right-click on the collection and choose **Create Task** | **Processing**. In the Create Processing Task wizard, specify the processing settings you need.
3. Click on the **Tasks** tab in the right pane.
4. Right-click on the task and select **Export Settings to File**.
5. Save the INI file in the desired location.

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 file system 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.

  > **CAUTION: Please consider that when resources are processed remotely, computers are handled in turns. In comparison with agent-based resource processing, remote processing takes significantly more time.**

- Expect about 10% (depending on the environment) of your workstations to require troubleshooting due to various reasons: they may be offline, the Server service may not be running, the domain administrators may be absent from the local Administrators group, and so on.

It is recommended that you create separate lists for end-user workstations and servers, and process the workstations first and the servers next.

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 or AD LDS for updating permissions. Active Directory Processing Wizard also allows you to process Microsoft Exchange directory permissions and clean up SIDHistory of the migrated objects.

When and Where to Use Active Directory Processing Wizard

Generally, if you want the new users to have the same level of access as the old users after Active Directory migration, you need to run Active Directory Processing Wizard (ADPW) in all domains where the old users had specifically configured access rights. This is as good as obligatory in most Active Directory migrations, at least for the initial transition period.

The following are examples of activities that you may need to perform in ADPW to restore users' resource access levels:

- Add target users to source groups
  This is the most common operation for ADPW.
- Update linked attributes other than group membership
  For that, ADPW modifies forward links so that back links are resolved as you expect. All linked attributes are supported.

NOTE: Commonly-used important linked attributes include:

- The **managedBy** attribute of groups
- Links (to users) that role-based administration in Exchange 2007 and later is based on

- Update permissions on objects such as OUs
- If an Exchange resource forest topology is set up in the environment, update Active Directory in the Exchange resource forest
  For details about handling Exchange resource forests, see the When and Where to Use Exchange Processing Wizard topic.

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 topic 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 topic 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 a specific set of steps, as described in the related topics.

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 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.

CAUTION:

- **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.

  CAUTION:

  - **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.

  CAUTION:

  - **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.

NOTE: 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.

> **CAUTION: 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 production 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 Administrative Roles.

  > **NOTE:** 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 in 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.

  > **CAUTION:**
  >
  > - **For successful Default schema permissions processing, the service account must be a member of the Schema Admins group.**
  > - **Enable this option if you are going to process Exchange mailbox permissions or Other Exchange permissions. This is necessary for correct processing of the SendAs and ReceiveAs permissions.**

- **Exchange mailbox permissions**. Select this check box to update the permissions both in Active Directory and in the Exchange mailbox database.

  > **CAUTION: The service account must have permissions to do the following:**
  >
  > - **Modify the msExchMailboxSecurityDescriptor attribute on mailbox-enabled objects that are processed.**
  > - **Read and modify items in the Exchange mailbox database.**
  >
  > **Grant these permissions using the Exchange System Manager Console or ADSI Edit snap-in. For details about assigning permissions in your particular Exchange environment, see the corresponding Exchange Environment Preparation document.**

- **Other Exchange permissions**. Select this check box to update the following:
  - Directory permissions for Exchange objects, such as organizations, servers, and containers
  - In domains with Exchange 2013 organizations, role-based access control settings

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.

> **CAUTION: 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.

> **CAUTION: 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 topic 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.

  > **CAUTION:**
  >
  > - **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.

  > **CAUTION:**
  >
  > - **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.

  > **CAUTION:**
  >
  > - **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.

> **NOTE:** 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.

> **CAUTION: 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 production 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.

  > **NOTE:** 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.

  > **CAUTION: 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 permissions both in Active Directory and in the Exchange mailbox database.

  > **CAUTION: The service account must have permissions to do the following:**
  >
  > - **Modify the msExchMailboxSecurityDescriptor attribute on mailbox-enabled objects that are processed.**
  > - **Read and modify items in the Exchange mailbox database.**
  >
  > **Grant these permissions using the Exchange System Manager Console or ADSI Edit snap-in. For details about assigning permissions in your particular Exchange environment, see the corresponding Exchange Environment Preparation document.**

- **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.

> **CAUTION: 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.

> **CAUTION: 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

> **CAUTION: 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.

> **NOTE:** 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.

NOTE: 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 topic 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.

When and Where to Use Exchange Processing Wizard

Exchange Processing Wizard (EPW) is a tool for updating permissions on Exchange mailboxes and public folders during Active Directory migrations to align the permissions with the new user configuration. EPW updates the following:

For mailboxes:

- Client permissions
- Mailbox contents

For public folders:

- Client permissions
- Administrative rights
- Public folder contents

There are a variety of situations where the use of EPW is necessary. In general, you need it whenever you want to give migrated user accounts the same level of access to mailboxes and public folders as they had before Active Directory migration.

This section describes three common scenarios for using EPW. Other real-life scenarios are similar, and some elements of the scenarios in this document can be reused in them.

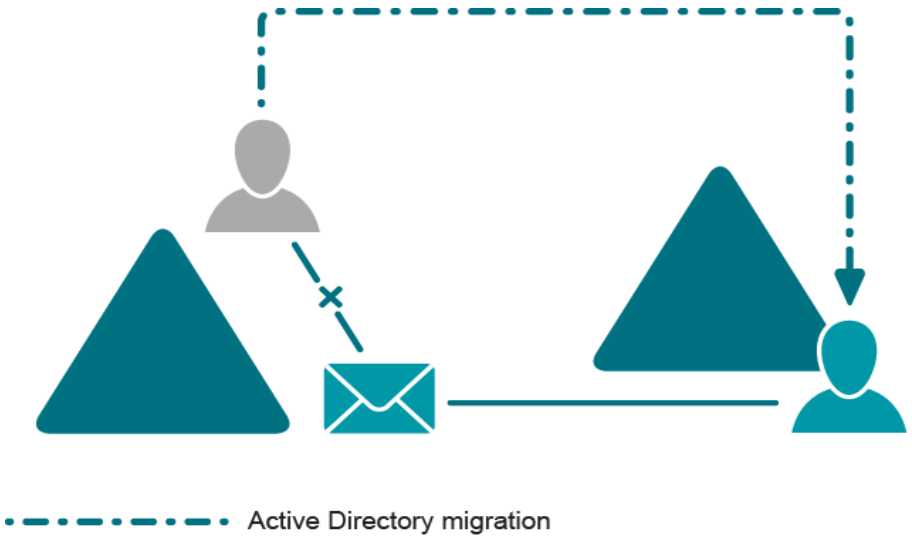
- Intra-Forest Domain Migration
- Inter-forest migration scenarios involving an Exchange resource forest (ERF):
  - Source Forest Becomes an ERF
  - Users Change Forest in an ERF Topology

NOTE:

- An Exchange resource forest is an Active Directory forest that hosts Exchange servers for users from another forest and is dedicated to Exchange operations.
- Often, EPW is not the only tool that you need to use to complete the configuration. You also need to run Active Directory Processing Wizard to update the **msExchangeSecurityDescriptor** attributes of the old users (in Active Directory and Exchange stores) so that it points to the new users. Generally, ADPW is always required if mailboxes and public folders have customized permissions.

Intra-Forest Domain Migration

The most common scenario for the use of EPW is during Active Directory migration from one domain to another within the same forest. User accounts are migrated with their Exchange-related properties intact.



Role of EPW

After the migration of user accounts is complete, the users in the target domain can still log in to their mailboxes, provided that the **Reconnect Exchange mailbox** option was used in the migration session. However, these users do not have any of the permissions that the source user accounts had (because the target users have different SIDs). In public folders, the permissions are also based on the old domain configuration.

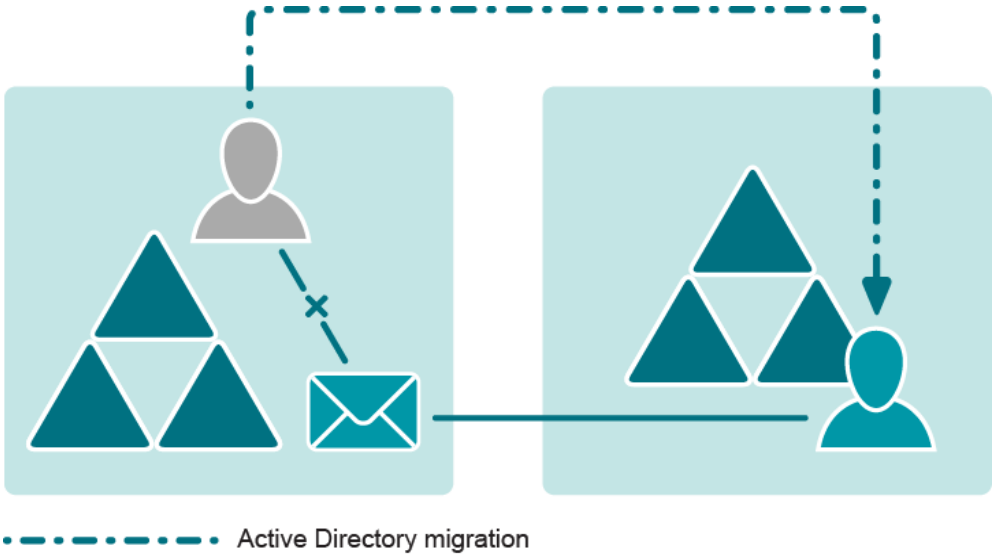
Run EPW against the Exchange server after the migration to make sure that:

- All delegation-related permissions on the mailboxes are re-aligned correctly to the new users.
- The new users have the same level of access to public folders that the old users did.

NOTE: You may need to use Active Directory Processing Wizard in the source domain after these steps.

Source Forest Becomes an ERF

A popular scenario involving EPW is creation of an Exchange resource forest (ERF) topology instead of a single forest. In this variation of the scenario, user accounts move to another newly-created or existing Active Directory forest, and the target users are supposed to become the new owners of the mailboxes. The source forest remains as an ERF, and the source users are disabled.



Role of EPW

After the migration of user accounts is complete, the users in the target forest have no access to the mailboxes in the ERF. Run EPW against the Exchange server after the migration to make sure that:

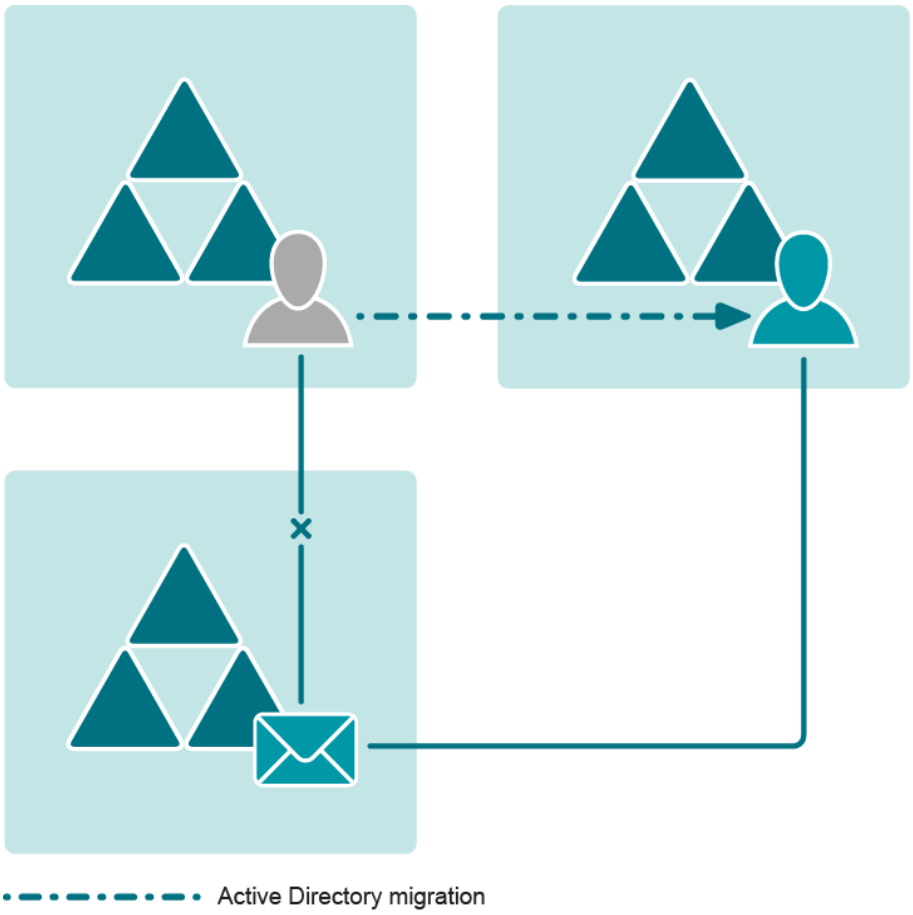
- The target forest user accounts become the new owners of the mailboxes.
- All delegation-related permissions on the mailboxes are re-aligned correctly to the new users.
- The new users have the same level of access to public folders that the old users did.

NOTE:

- You may need to use Active Directory Processing Wizard in the Exchange resource forest after these steps.
- ERF setup requires EPW only if the source forest becomes an ERF. Making the target forest an ERF involves the use of Migration Manager for Exchange, which automates the permission update work. As long as users' SIDs can be resolved during the Exchange migration, the permissions will be modified correctly for both source and target users.

Users Change Forest in an ERF Topology

A possible scenario is when users from one forest have mailboxes in another (ERF) forest and are moved to a third forest. The target users are supposed to become the new owners of the mailboxes in the ERF, and the old forest is supposed to be decommissioned.



Role of EPW

After the migration of user accounts is complete, the users in the target forest have no access to the mailboxes in the ERF. Run EPW against the Exchange server after the migration to make sure that:

- The target forest user accounts become the new owners of the mailboxes.
- All delegation-related permissions on the mailboxes are re-aligned correctly to the new users.
- The new users have the same level of access to public folders that the old users did.

NOTE: You may need to use Active Directory Processing Wizard in the Exchange resource forest after these steps.

Prerequisites (Exchange Server Processing)

- For a successful Exchange directory update, you must use an account with the 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.
- 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 topic 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 topic 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 in the related topics.

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.

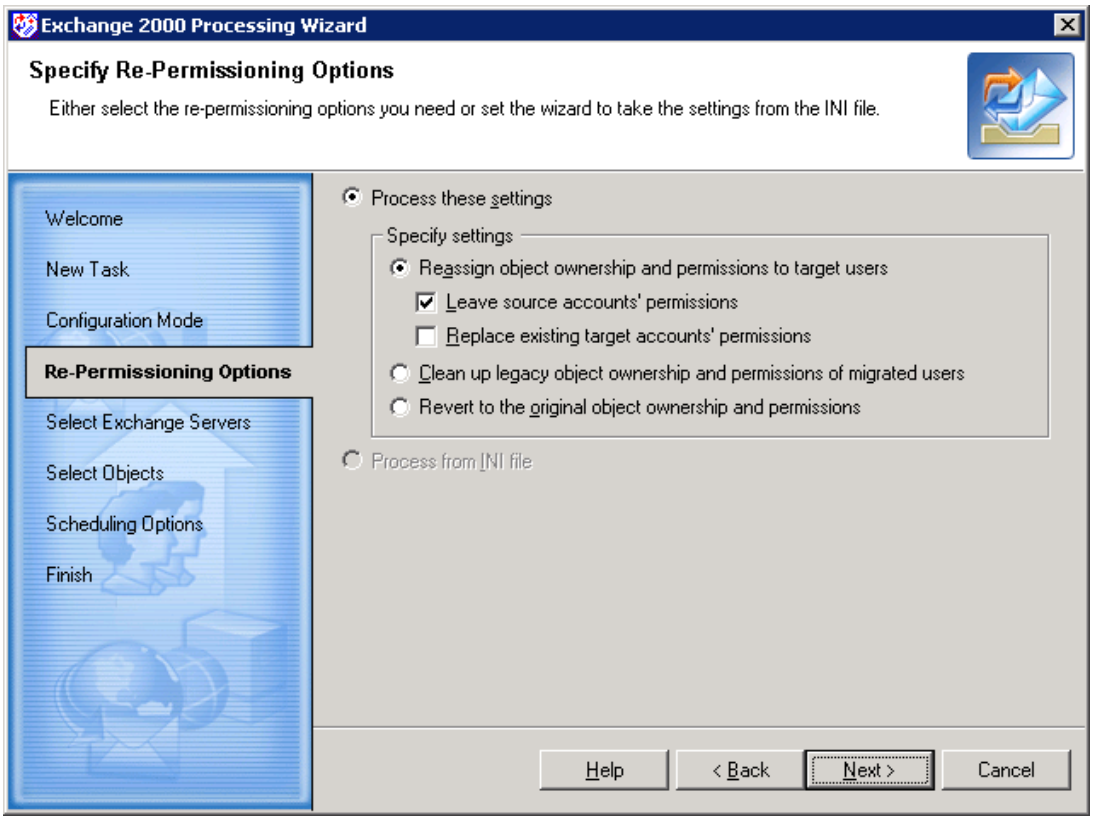
- **Delegate resource processing task**—Select this option if you want to create the task and delegate it to a trusted person who will run the task.
- **Configure resource processing task**—Select this option if you want to create, configure, and schedule the task.

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 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.
- **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.

  NOTE: 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 Delegating Resource Update topic for more details. Note that if no INI file exists, the option is disabled.

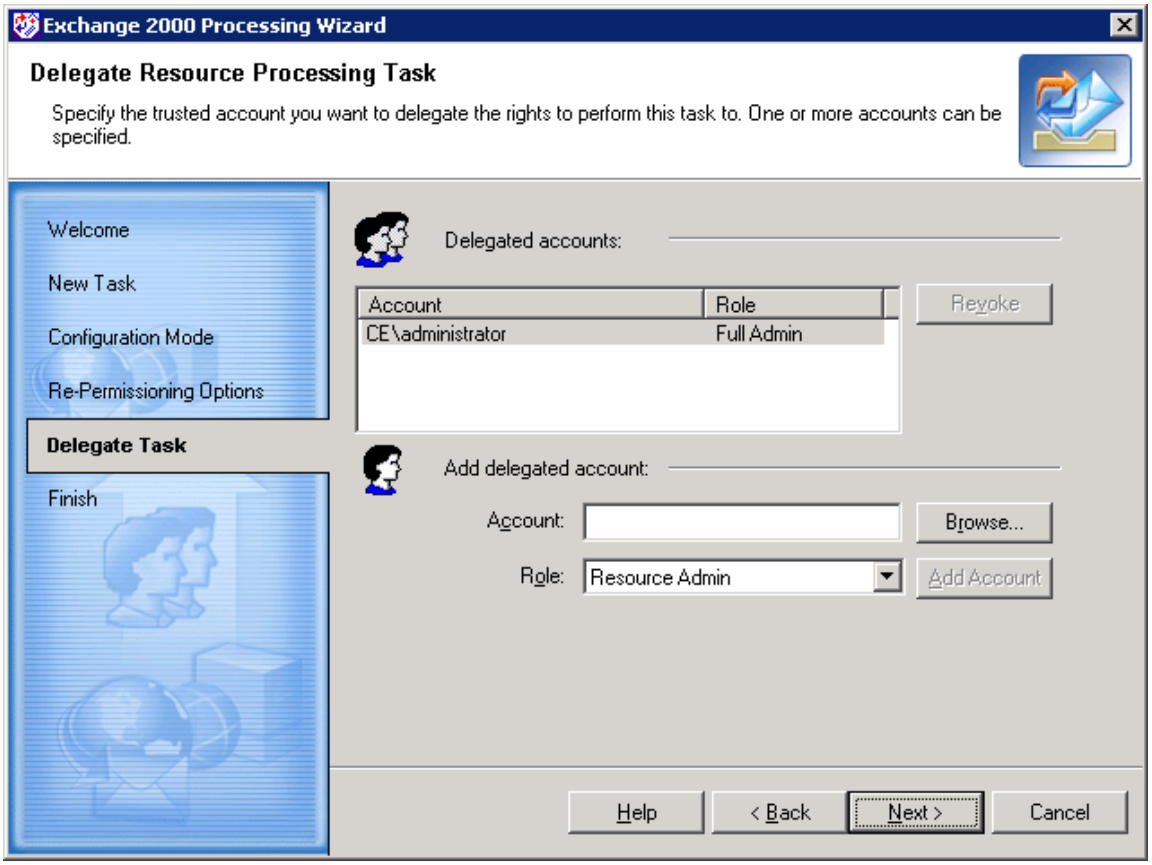
CAUTION: This option is enabled only when the wizard runs in stand-alone mode.

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.

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 *System Requirements and Access Rights* document.

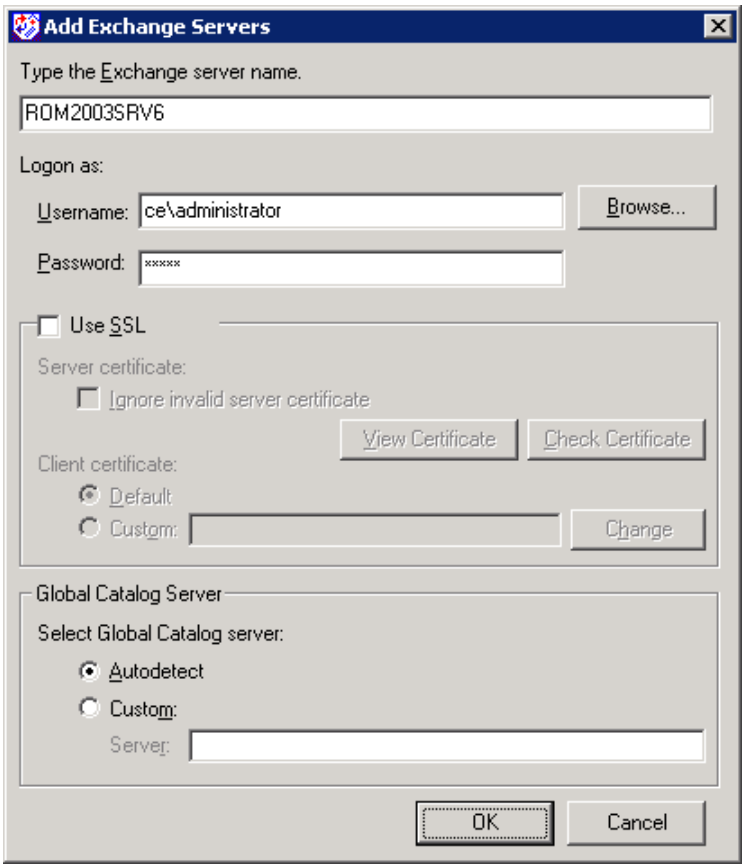
Click **Next** to proceed to the **Complete the Exchange Processing Wizard** step.

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.

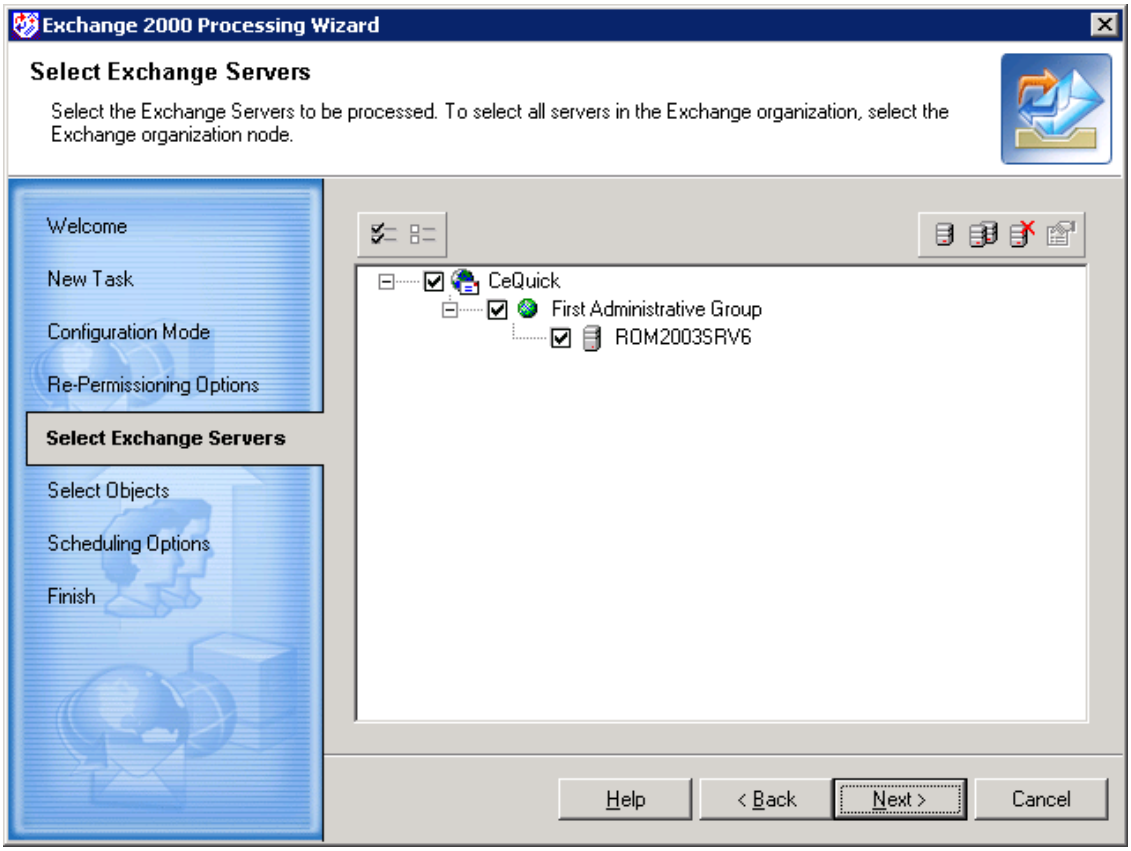
NOTE: If the account you specify does not have enough privileges to modify some of the Exchange objects, they will remain unchanged. No error or warning messages will be displayed—all messages will be written to the log file. See the Prerequisites section above for details.

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.

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

Specifying the Right Credentials for Public Folder Processing in Mixed Exchange Organizations

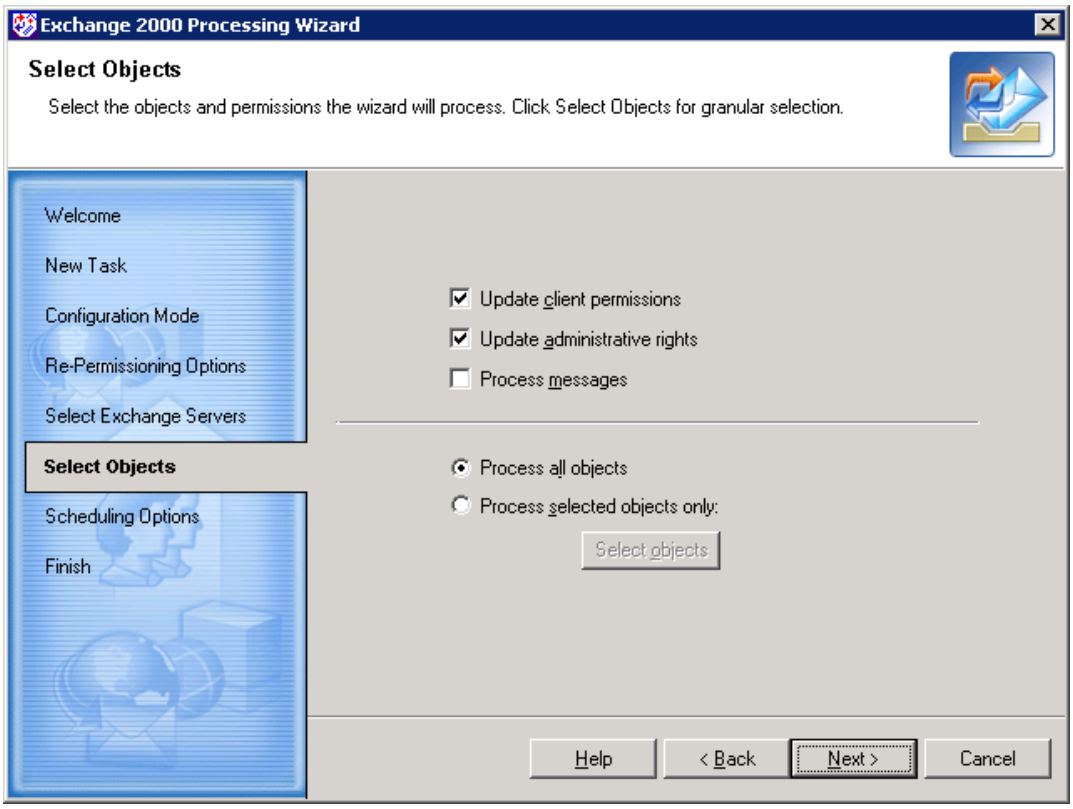
If you want to process public folders on an Exchange server in an organization that has a combination of Exchange 2003, Exchange 2007 and Exchange 2010 servers, then some additional requirements apply. The user you specify in the Add Exchange Servers dialog box must have the following:

1. The privileges listed for “Exchange update” in the *Accounts and Rights Required for Active Directory Migration Tasks* section of the *System Requirements and Access Rights* document.
2. A mailbox on the server you are adding.

If the server does not host the specified user's mailbox, you may encounter errors when trying to select public folders for processing.

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.

NOTE: For successful message processing, ensure the following:

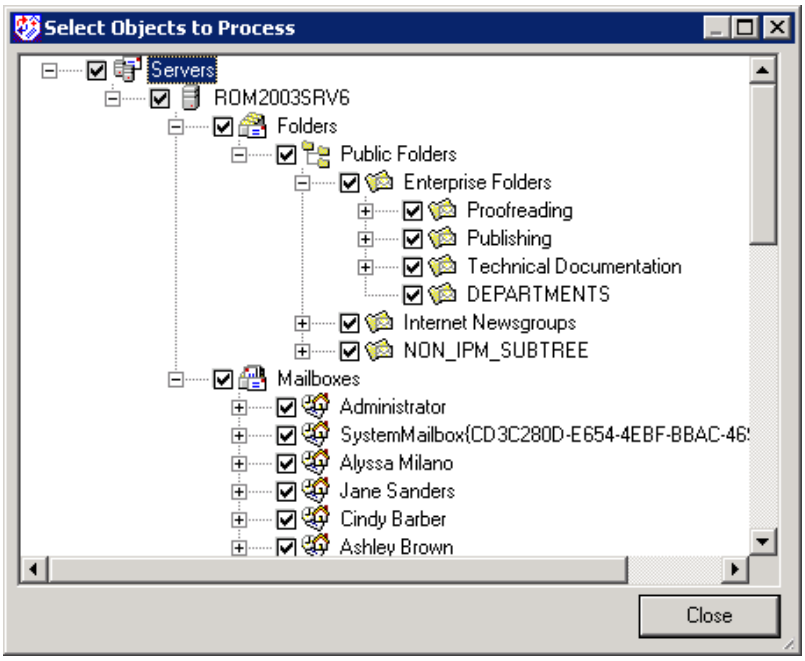
- The account under which the processing is performed must have the **Send As** and **Receive As** permissions on the processed store or server.
- The mailbox database has an associated public folder.

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.

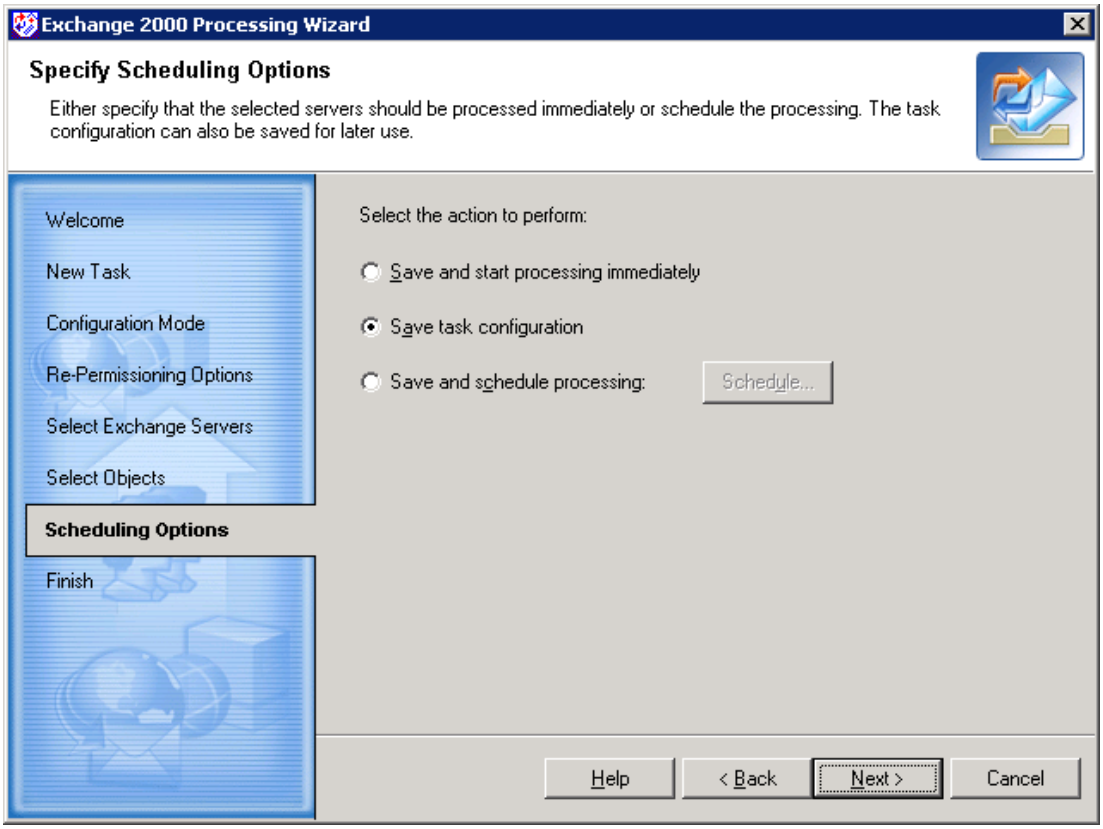


You can select individual mailboxes and public folders to process. If you select or clear an object, the objects below it will also be selected or cleared.

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.

NOTE: 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.

NOTE: 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.

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.

> **CAUTION: 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 topic 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

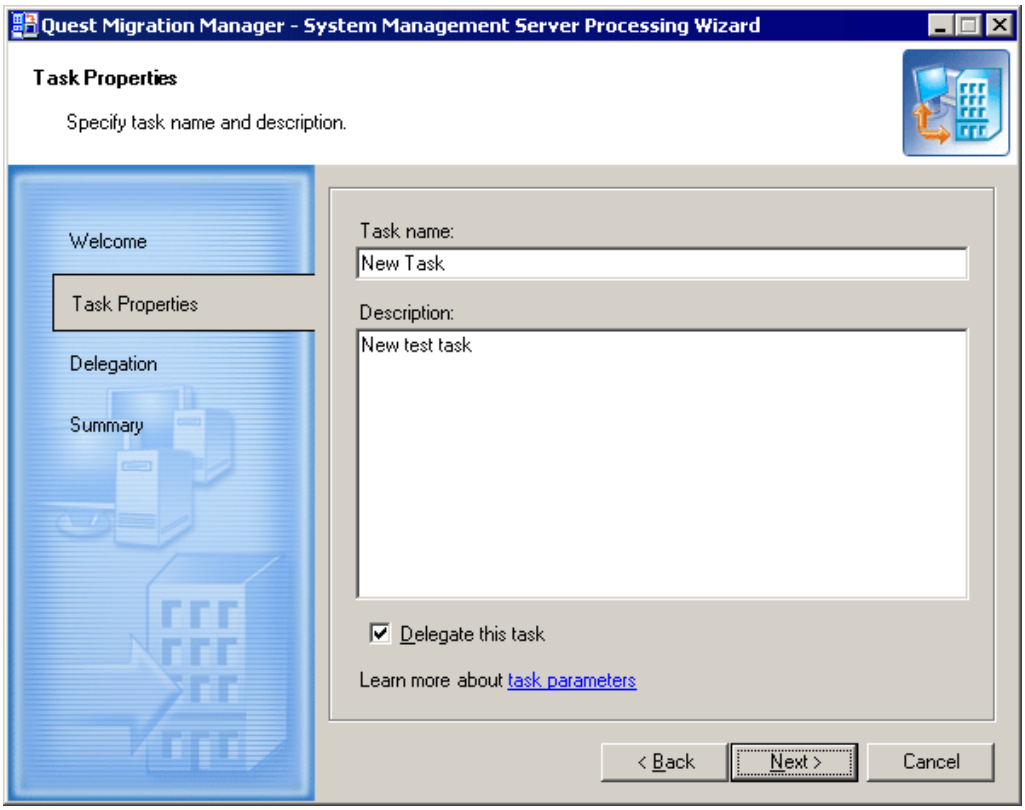
In this step, you can give the task a new name and add a descriptive comment.

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.

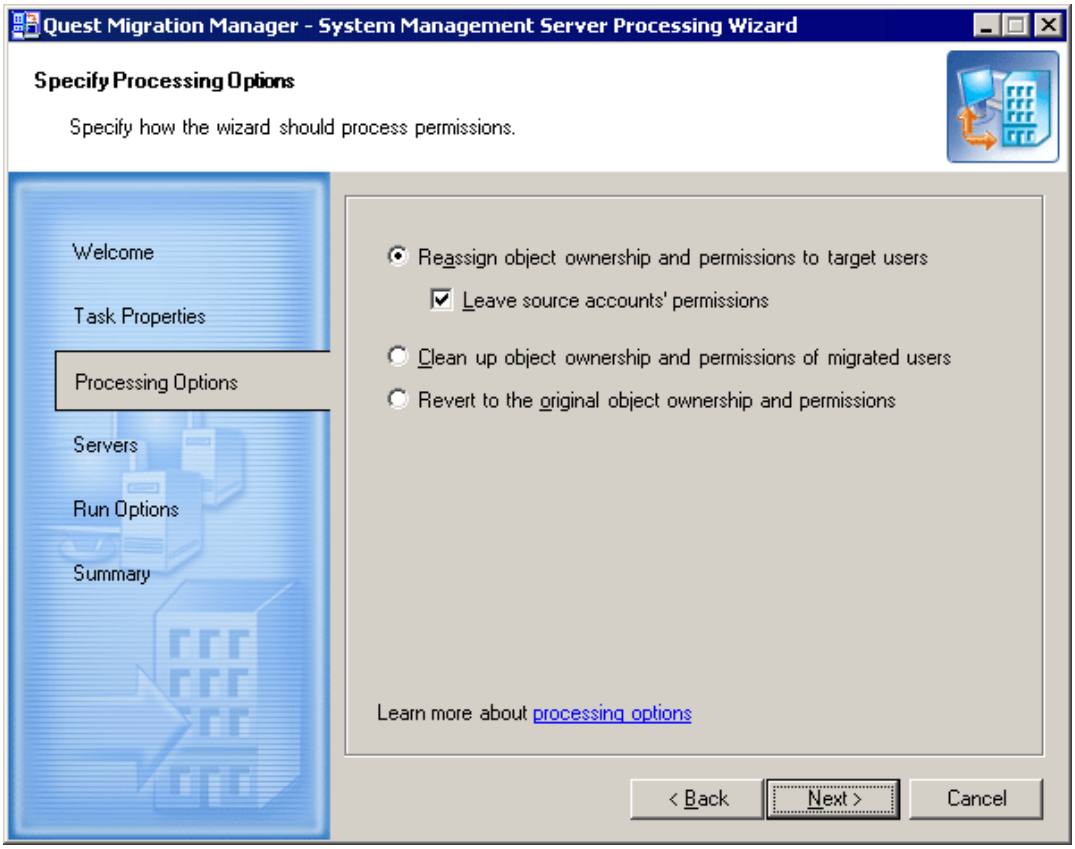


Depending on the mode you selected, the remaining steps offered by the wizard are different.

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.

  NOTE: 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 you undo re-permissioning, removing target users from the objects' Access Control Lists (ACL) and returning all rights to the source accounts.

  NOTE: 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).

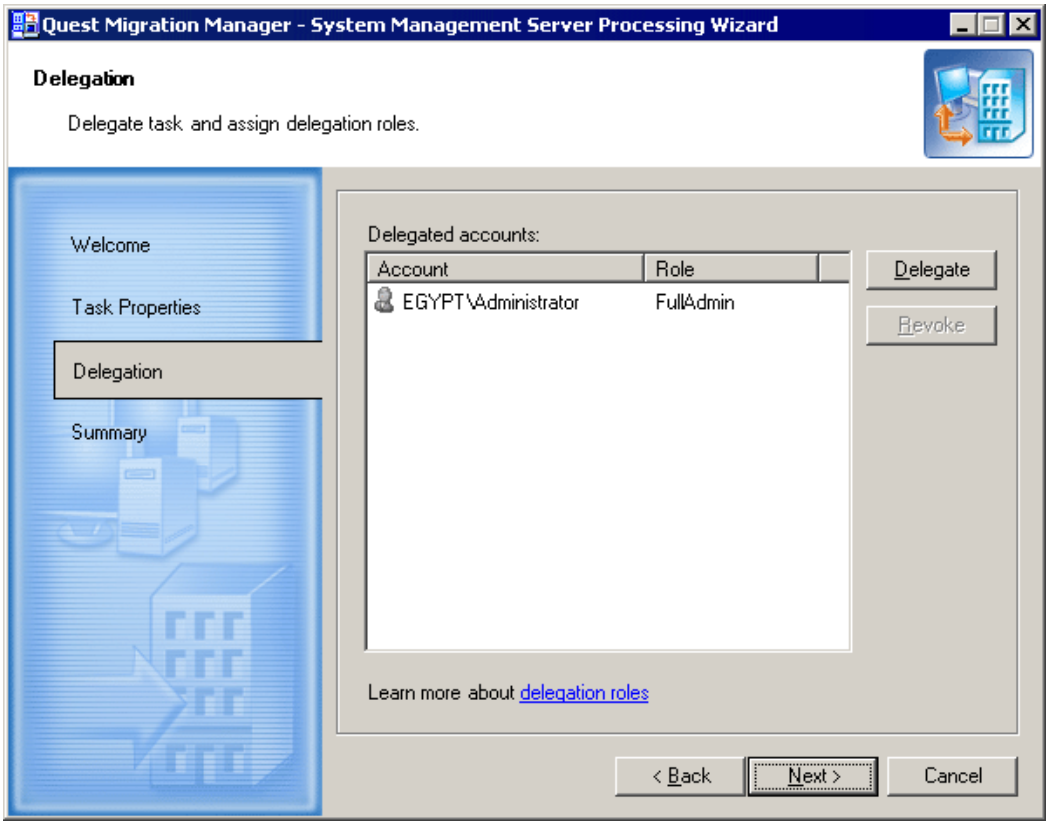
- **Process as specified in the exported INI settings file**—Select this option if you want to retrieve the processing options from the INI file. The INI settings file can be created in Migration Manager (**Tools | Export to | INI File**). See the Delegating Resource Update topic for more details. Note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

  NOTE: 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:

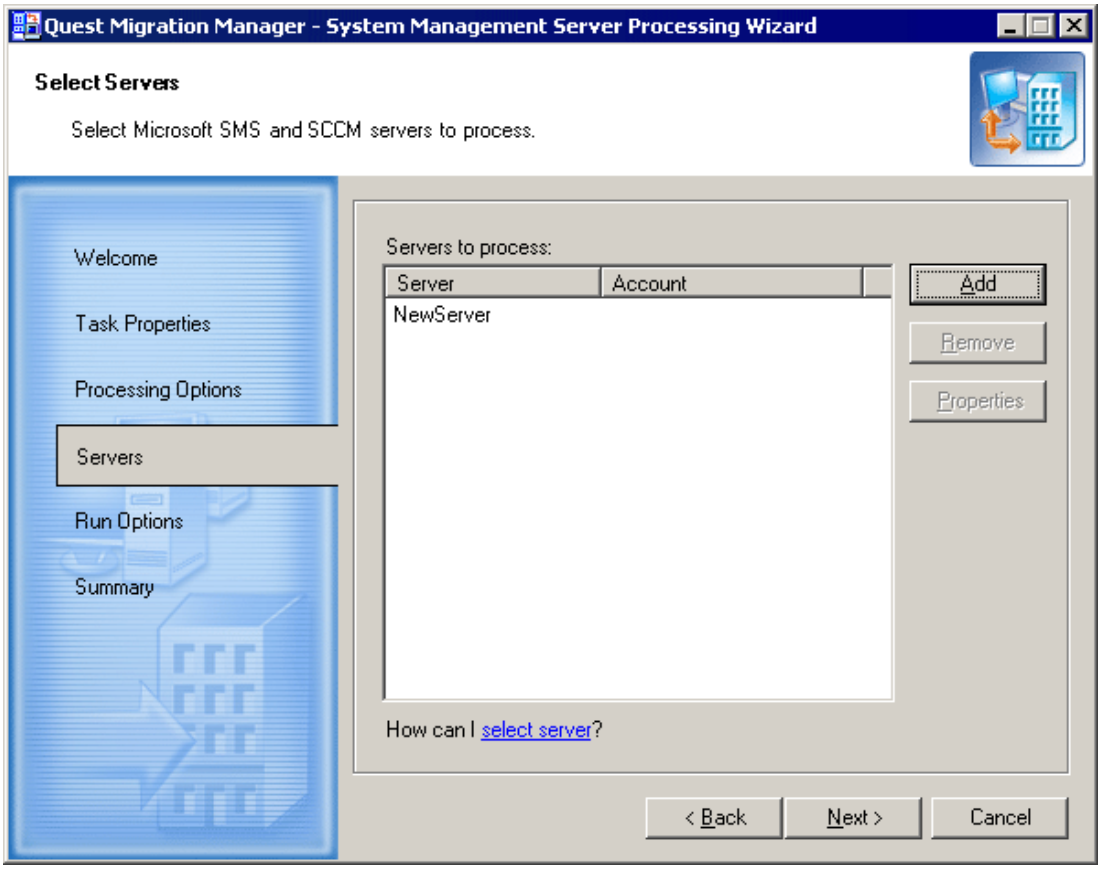
1. Click the **Delegate** button.
2. Specify account and the role you want to delegate. Click **OK**.

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**.

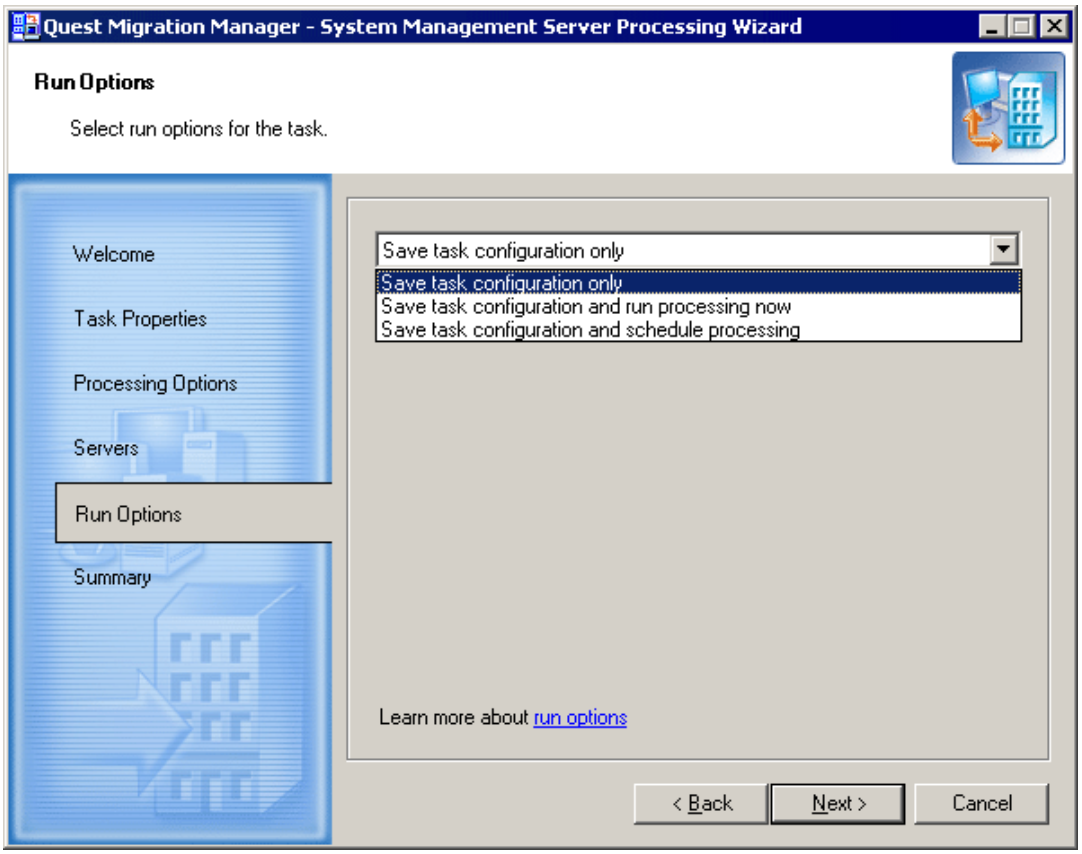


Use the **Remove** button to remove servers from the list. To change credentials, select the server in the list, click the **Properties** button, and specify the new credentials in the **SMS Server Properties** dialog box.

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.

NOTE: 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.

CAUTION: 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.

> **CAUTION: 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 wizard automatically detects the SQL Server version and performs the updates in accordance with the server's structure.

> **IMPORTANT:** For information on supported SQL Server versions, refer to *Processed Platforms – SQL Servers* topic of the *System Requirements and Access Rights* document.

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. 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.

> **NOTE:** 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 2012 SP1 and Microsoft SQL Server 2014

The following objects are updated on Microsoft SQL Server 2012 Service Pack 1 or Microsoft SQL Server 2014 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
- 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 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

Processing Details

NOTE: 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.

CAUTION: 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 (SQL Server Processing)

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 2000 and 2005 must be a member of the **sysadmin** role.

CAUTION: 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

CAUTION: 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.

NOTE: 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 topic for more details.

Regardless of the method you select, the SQL Processing Wizard will guide you through the updating process, as explained in the related topics.

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.

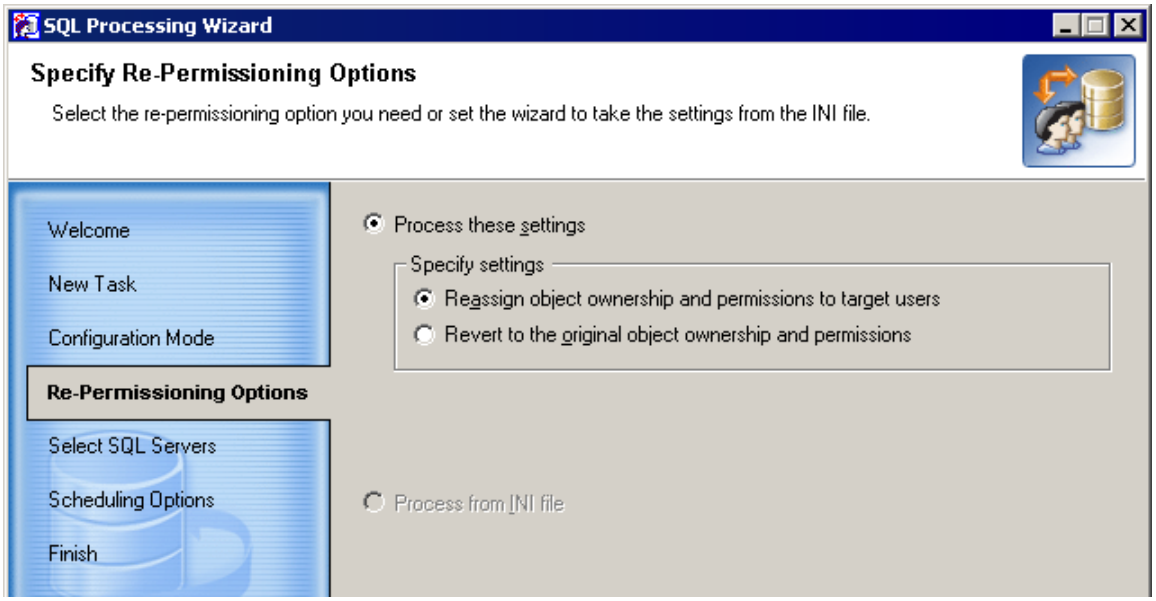
- **Delegate resource processing task**—Select this option if you want to create the task and delegate it to a trusted person who will run the task.
- **Configure resource processing task**—Select this option if you want to create, configure, and schedule the task.

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.

NOTE: 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.

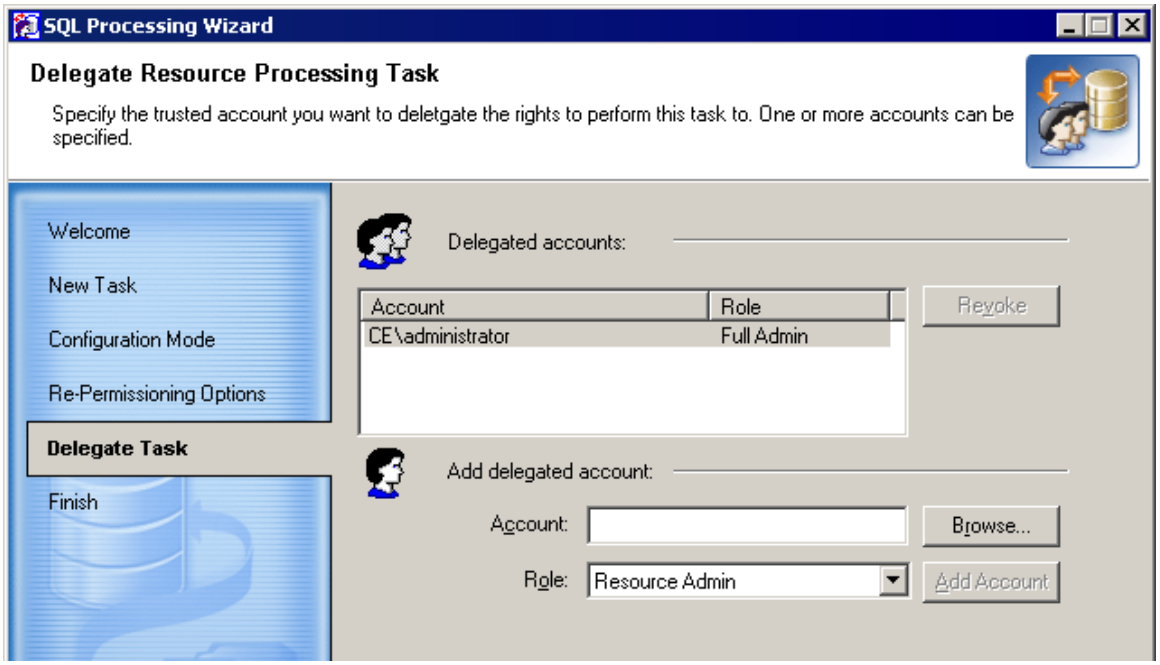
- **Process from INI file**—Select this option if you want to retrieve the processing options from an INI file. An INI settings file can be created in Migration Manager (**Tools | Export to | INI File**). See the Delegating Resource Update topic for more details. Note that if no INI file exists, the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

NOTE: 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.

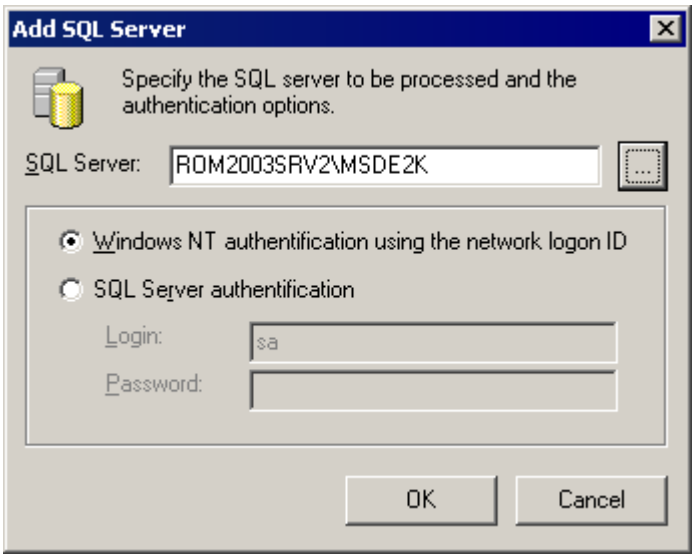


To delegate the rights to the trusted accounts, complete the following steps:

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.
4. Click **Next** to proceed to the **Complete the SQL Processing Wizard** step.

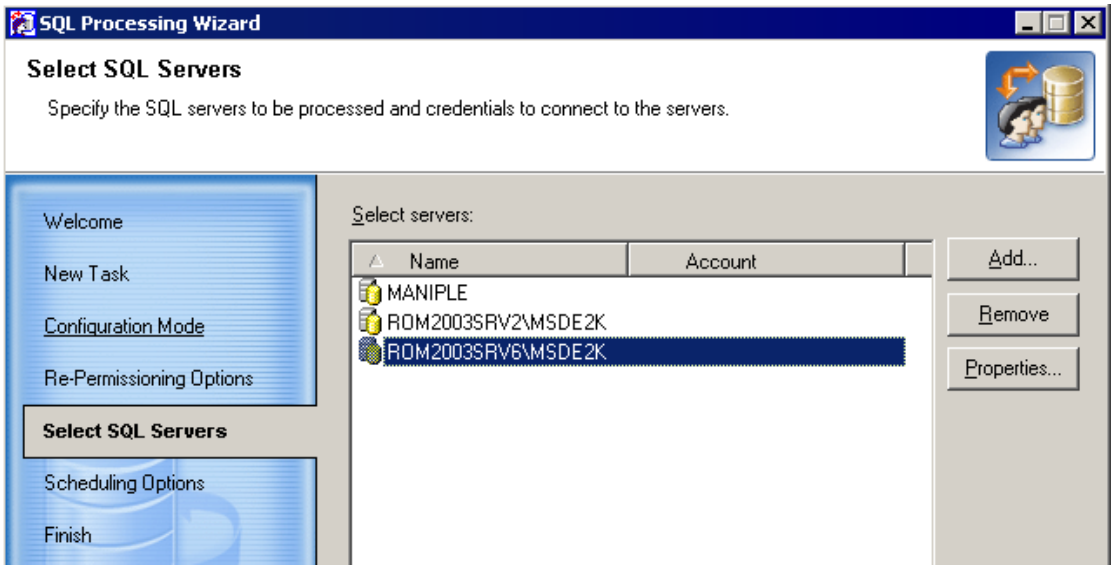
Step 5. Select SQL Server

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**.

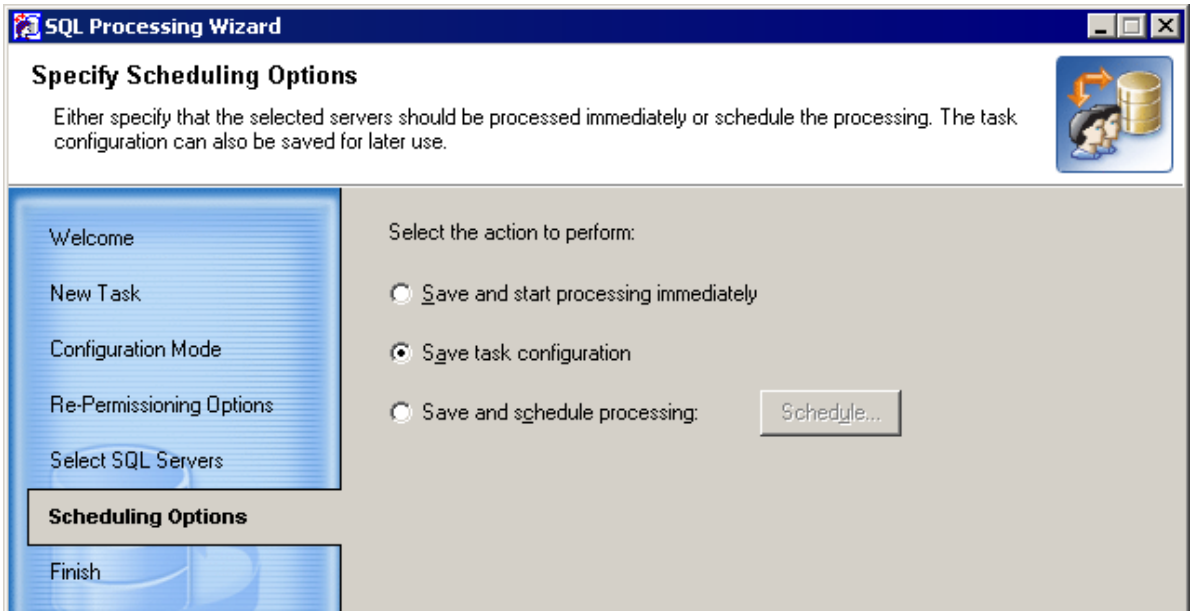
! **CAUTION: The login used to process the SQL Server must be a member of the sysadmin role.**



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.

> **CAUTION: 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 user**s 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.

! **CAUTION: 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 (Cluster Server Migration)

1. In the Resource Updating Manager console, add all cluster nodes to a new collection. Make sure you select only the actual nodes and not the virtual servers.
2. Right-click on the collection and choose **Create Task** | **Processing**. In the Create Processing Task wizard, specify the processing settings. This task will process all resources except the cluster shares, cluster database, and cluster printers.
3. Click on the **Tasks** tab in the right pane.
4. Right-click on the newly created task and select **Export Settings to File**.
5. Save the INI file in the desired location.
6. Open the INI file in Notepad and verify that the settings are accurate and the file contains the desired objects only.
7. 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`
8. 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.

   NOTE: 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.
9. Reboot the passive node. Verify that the **Cluster Service** account on this node is changed to the target account.
10. Restart the **Cluster Service** on the active node. Verify that the **Cluster Service** account on this node is changed to the target account.

    NOTE: During the restart of the service the resources will not be available.

11. After a successful start of the **Cluster Service** on the active node, start the cluster service on the passive node.
12. Move the resources to the passive node and reboot the active node.
13. After the node restarts move the resources back.

Option 2 (Cluster Server Migration)

Follow steps 1–8 above. Then, instead of taking steps 9–13, 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 knowledge article 13599 on the Quest Support site for more details.

NOTE: 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.

Command-Line Resource Update

The command-line tool **Vmover.exe**, located in the **%ProgramFiles(x86)%\Common Files\Aelita Shared\Migration Tools\Resource Updating\Agent** folder (on 64-bit Windows) or **%ProgramFiles%\Common Files\Aelita Shared\Migration Tools\Resource Updating\Agent** folder (on 32-bit Windows) 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.

NOTE: On 64-bit Windows, an additional native 64-bit version of Vmover.exe is located in the **%ProgramFiles(x86)%\Common Files\Aelita Shared\Migration Tools\Resource Updating\Agent\x64** folder.

Among the main applications of Vmover are the following tasks:

- Updating remote resources
- Processing roaming profiles
- Processing file system permissions on non-Windows systems with Common Internet File System (CIFS)

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.

Processed Rights and Resources

This section describes which resources or rights can be processed by Vmover.

Parameters that define processing options for Vmover are specified under the **[Options]** section of the Vmover INI file. For example of Vmover INI file, see the What do the parameters and data stored in the vmover.ini mean KB article.

TIP: For more details on using the Vmover, see the Command-Line Resource Update article.

The following table lists resources and rights that can be processed by Vmover on local and remote computers:

Parameter in Vmover INI	Processed rights/resources
`LocalGroups=Yes/No`	Local group membership
`UserPrivileges=Yes/No`	User rights
`Services=Yes/No`	Service accounts
`ScheduledTasks=Yes/No`	Scheduled tasks
`Profiles=Yes/No`	Local profiles
`RoamingProfiles=Yes/No`	Roaming profiles
`Registry=Yes/No`	Registry
`FileSystem=Yes/No`	File system

Parameter in Vmover INI	Processed rights/resources
`ProcessFileSystemOwner=Yes/No`	File ownership
`Shares=Yes/No`	Shares
`Printers=Yes/No`	Printers
`COMPlus=Yes/No`	COM+
`DCOM=Yes/No`	DCOM
`IIS=Yes/No`	IIS

Local group membership

Vmover adds target accounts to the local groups that contain the corresponding source accounts.

User rights

Vmover assigns target accounts exactly the same user rights as the corresponding source accounts have.

Service accounts

For each Windows service Vmover updates the account that the service uses to log on. For example, if a service runs under *SOURCE\User1* and *User1* is migrated to the target domain, the account will be changed to *TARGET\User1*.

NOTE:

- Account passwords are not updated in the service's properties. Therefore, if source and target passwords of a service account are not the same, the corresponding service may not start after resource update.
- If the service being processed at the moment is running under a source account while a user logs on under a new corresponding target account, duplicate profiles can be created.
- Source account is replaced with the corresponding target account in the service's properties whether or not the **Leave source accounts' permissions** option is turned on.

Scheduled tasks

Vmover processes scheduled task accounts and permissions. For example, if a task runs as *SOURCE\User1* and *User1* is migrated to the target domain, the task account will be changed to *TARGET\User1*.

Objects processed

For each scheduled task Vmover performs the following:

- Updates scheduled task account (account under which task runs)
- Duplicates entry for the updated scheduled task account in the **Credential Manager** if original account is presented there.
- Processes accounts specified in the task's triggers (if any)
- Updates the permissions for the task file

NOTE:

- If a scheduled task is running under a source account while a user logs in under a new corresponding target account, duplicate profiles can be created.
- Source scheduled task accounts are replaced with the corresponding target accounts in the task's properties whether or not the **Leave source accounts' permissions** option is turned on.

Local profiles

Vmover processes local profiles of source users.

Objects processed

For each local profile, Vmover performs the following steps:

1. Vmover creates a new user profile for the corresponding target user that is linked to the same local profile file as the source user.

   NOTE: The paths to user profile files are stored in the **ProfileImagePath** values of **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\ProfileList** sub-keys.

2. Vmover processes the registry hive from each local profile file (**ntuser.dat** or **ntuser.man**) and also registry hive from the **UsrClass.dat** file. For details on objects processed, see the Registry section.

Roaming profiles

Vmover updates roaming user profiles.

Objects processed

For each roaming profile found on a computer, Vmover performs the following steps:

1. Vmover processes the registry hive from the roaming user profile file (**ntuser.dat** or **ntuser.man**) and also registry hive from the **UsrClass.dat** file. For details on objects processed, see the Registry section.
2. Vmover processes permissions for **ntuser.dat** and **ntuser.man** files. For details on permissions processed, see the File system and File ownership sections.

Registry

Vmover processes permissions for all keys in the **HKEY_LOCAL_MACHINE** subtree of Windows Registry. If processed computer is not a Windows cluster, keys from the **HKEY_USERS** subtree are processed as well.

Objects processed

Vmover grants target account exactly the same permissions as the corresponding source account has. The following properties are updated:

- Discretionary Access Control List (DACL)
- System Access Control List (SACL)
- Owner
- Primary group

NOTE: Owner and primary group are replaced whether or not the **Leave source accounts' permissions** option is turned on.

File system

Vmover updates permissions for files and folders located on local hard disk drives with NTFS or ReFS format.

Objects processed

Vmover grants target account exactly the same permissions on files and folders as the corresponding source account has. The following properties are updated for files and folders:

- Discretionary Access Control List (DACL)
- System Access Control List (SACL)
- Primary group

NOTE:

- Files and folders on CD/DVD disks, USB flash drives, RAM disks, network drives and so on are not processed.
- The recycler, *$recycle.bin*, and System Volume Information folders are skipped during processing.
- The drives of Windows clusters are supported.
- Primary group is replaced whether or not the **Leave source accounts' permissions** option is turned on.

File ownership

The ownership of the files and folders in the file system is changed from the source account to the corresponding target account. For example, if a file owner is *SOURCE\User1* and *User1* is migrated to the target domain, the file owner will be changed to *TARGET\User1*.

The file owner is specified on the **Owner** tab of **Advanced Security Settings** dialog in the file or folder **Properties**.

NOTE: File ownership is replaced whether or not the **Leave source accounts' permissions** option is turned on.

Shares

Vmover updates share permissions.

NOTE: Local file system permissions for shares are not processed.

Printers

Vmover processes permissions for local printers and for network printer connections.

Objects processed

Vmover grants target account exactly the same permissions as the corresponding source account has.

The following properties are updated:

- Discretionary Access Control List (DACL)
- System Access Control List (SACL)
- Owner
- Primary group

NOTE:

- Owner and primary group are replaced whether or not the **Leave source accounts' permissions** option is turned on.
- Network printer connections permissions are processed only on computers running Windows Vista or later, and Windows Server 2008 or later.
- Network printer connections permissions are not processed for clusters.

COM+

Vmover processes settings for all COM+ application installed on a computer.

Objects Processed

For each installed COM+ application the following items are processed:

- Account under which the application runs
- Accounts assigned to roles

NOTE: Account under which the application runs is replaced in the application properties whether or not the **Leave source accounts' permissions** option is turned on.

DCOM

Vmover processes the DCOM security settings.

Objects Processed

The following computer-wide settings are processed:

- Launch and Activation Permissions (both Limits and Defaults)
- Access Permissions (both Limits and Defaults)

The following settings are processed for each DCOM application:

- Launch and Activation Permissions
- Access Permissions
- Configuration Permissions
- User account that is used to run the application

Corresponding registry entries processed by Vmover are

- **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Ole** registry values:
    1. DefaultAccessPermission
    2. DefaultLaunchPermission
    3. MachineAccessRestriction
    4. MachineLaunchRestriction
- For each sub-key in **HKEY_CLASSES_ROOT\AppId**:
    1. Key security (see Registry section for details)
    2. RunAs value
    3. AccessPermission value
    4. LaunchPermission value
    5. AccessPermissions value
    6. LaunchPermissions value

NOTE: User account (RunAs registry value) is replaced whether or not the **Leave source accounts' permissions** option is turned on.

IIS

Vmover processes IIS 6.0 metabase properties and IIS 7.x/8.x/10.0 settings.

Objects processed

IIS 6.0 metabase properties

The following IIS metabase properties are processed:

- AdminAcl
- AnonymousUserName
- WAMUserName
- UNCUserName
- All properties that are explicitly specified in the Vmover INI file under **[IIS Identifiers]** (see product documentation for details).

NOTE: All properties except AdminAcl are replaced whether or not the **Leave source accounts' permissions** option is turned on.

IIS 7 or higher settings

For IIS version 7.0 or higher the following settings are updated:

- Site or server settings:
    - ASP.NET– .Net Authorization Rules
    - ASP.NET–Providers (user name in connection strings)
    - ASP.NET–Session State (user name in connection strings)
    - ASP.NET–SMTP E-Mail

- FTP–FTP Authentication
    - Anonymous Authentication (user name)
    - Basic Authentication (domain)
- FTP–FTP Authorization Rules
- FTP-FTP User Isolation (IIS 8 and higher)
- IIS–Authentication
    - Anonymous Authentication (user name)
    - ASP.NET Impersonation (user name)
    - Basic Authentication (domain)
- IIS–Authorization Rules
- IIS–Logging–ODBC Logging
- IIS–WebDAV Authoring Rules
- Site Basic Settings (user name in Connect As)
- Site Advanced Settings (user name in Physical Path Credentials)

- Application pool settings:
    - Identity
    - Application Pools Default Identity
- Management
    - IIS Manager Permissions
    - Shared Configuration
    - Centralized Certificates

IMPORTANT: If **IIS Metabase Compatibility** component is installed for IIS 7 or higher, properties listed in the **IIS 6.0 metabase properties** above will be processed as well.

NOTE: All settings except rules (such as .Net Authorization Rules, etc.) are replaced whether or not the **Leave source accounts' permissions** option is turned on.

Command-Line Parameters

Vmover should be run using the following command-line syntax:

```
Vmover.exe /c [/ini=IniFile] [/roaming=UserDatPath] [/volume=Path]
```

[/system=Computer]

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.in_** (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.tx_**, and then **File.txt**.

NOTE: 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 Delegating Resource Update topic.

/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.

CAUTION: 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

CAUTION: 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: 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\Deimos
```

CAUTION: 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

NOTE: 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 SID history of the accounts in the target domain. This lets you use the tool even if the object migration was performed not by Migration Manager but by another tool capable of adding sIDHistory.

NOTE: 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:

Parameter	Description
SIDHistory=Yes/No	Set this parameter to **Yes** to enable SIDHistory mapping.

Parameter	Description
hostName=Host_Name	Specify the target domain controller to use for LDAP queries. This should be a Global Catalog server.
ldapUser=UserName	The username to be used for LDAPrequests.
ldapDomain=UserDomain	The name of the target domain.
ldapPsw=Password	The password for the ldapUser user account.

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.

NOTE: 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.

For more details, see the following topics:

- Installing the SharePoint Permissions Processing Wizard
- Required Permissions (SharePoint Processing)
- Processing SharePoint Permissions

Installing the SharePoint Permissions Processing Wizard

To install the wizard, take the following steps:

1. Open the **Console** subfolder in **<QMM Installation Folder>** (by default, **%ProgramFiles%\Quest Software\Migration Manager**).
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.

Required Permissions (SharePoint Processing)

Before you run the wizard, make sure your account has the following permissions:

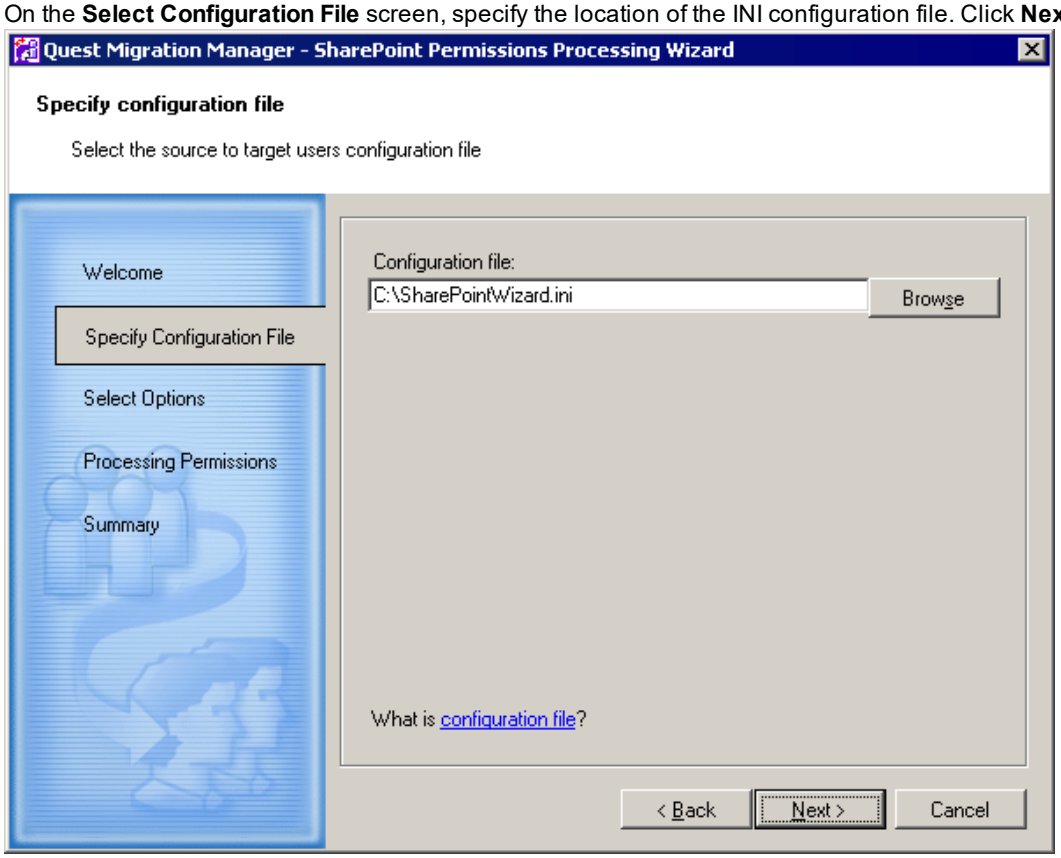
- Member of **Central Administrator** group for SharePoint server
- Member of the local **Administrators** group on the computer running the SharePoint Permissions Processing Wizard

Processing SharePoint Permissions

NOTE: 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**.
3. On the **Select Configuration File** screen, specify the location of the INI configuration file. Click **Next**.

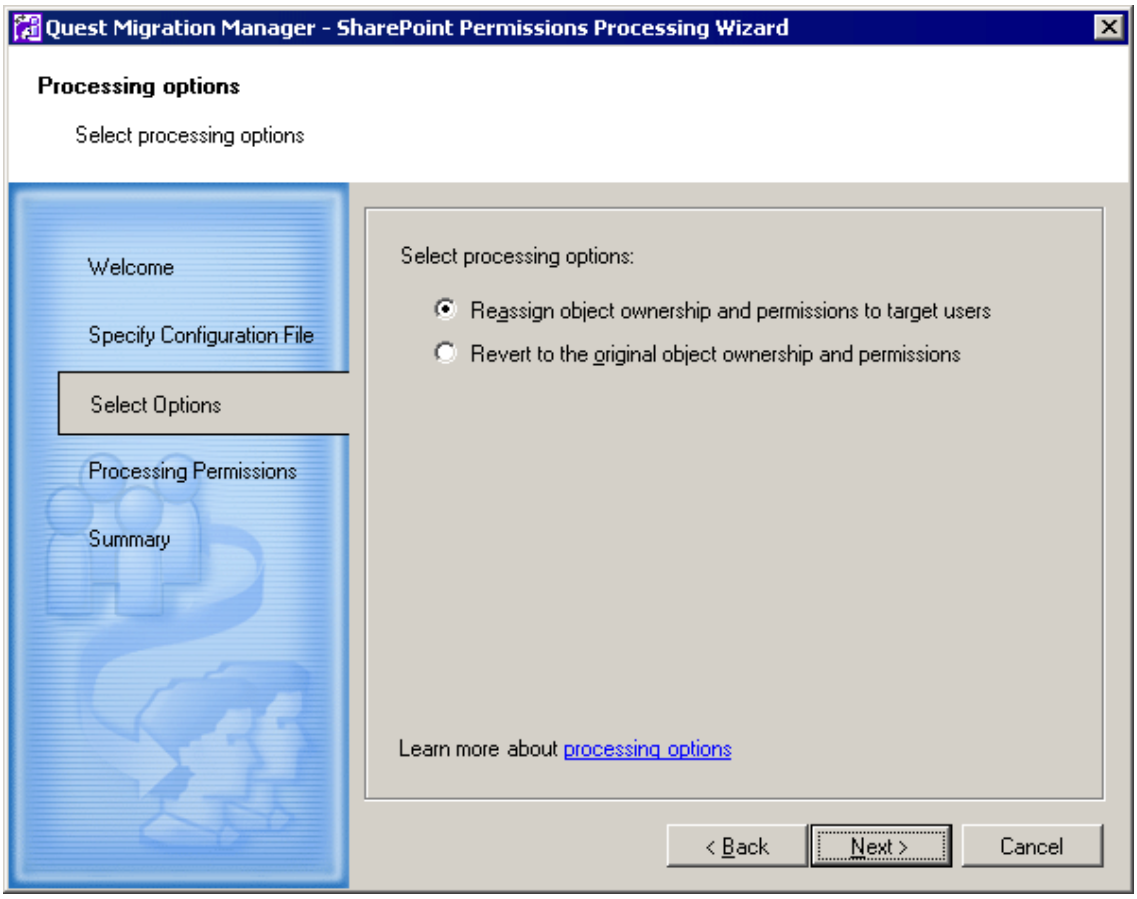


NOTE: To get the file, export INI file, as follows:

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 Name** list box.
3. Specify the INI file name and path in the **INI file** field, or leave the default.
4. Click **OK**. This will create INI file in the folder you specified in step 3.

4. 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.

NOTE: 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.



5. Click **Next** to start processing permissions.
6. 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.
7. Click **Finish** to exit the wizard.

About us

Quest provides software solutions for the rapidly-changing world of enterprise IT. We help simplify the challenges caused by data explosion, cloud expansion, hybrid datacenters, security threats, and regulatory requirements. We are a global provider to 130,000 companies across 100 countries, including 95% of the Fortune 500 and 90% of the Global 1000. Since 1987, we have built a portfolio of solutions that now includes database management, data protection, identity and access management, Microsoft platform management, and unified endpoint management. With Quest, organizations spend less time on IT administration and more time on business innovation. For more information, visit www.quest.com.

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at https://support.quest.com.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to-videos
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product