Migration Manager User’s Guide
**Table of Contents**

1. **Introduction** ................................................................................................................................. 8  
   Overview ................................................................................................................................................ 8  
   What is User State? ................................................................................................................................. 8  
      Operating System Settings .................................................................................................................. 8  
      Application Settings ............................................................................................................................ 8  
      Documents and Data Files ................................................................................................................... 8  
      Custom Applications ........................................................................................................................... 8  
   How Does Migration Manager Work? .................................................................................................... 9  
      Core Engine ......................................................................................................................................... 9  
      User Interface ..................................................................................................................................... 9  
      Content ............................................................................................................................................... 9  
      Process ............................................................................................................................................... 9  
   Automating Migration Manager ............................................................................................................. 10  
   Flexible Application Support ............................................................................................................... 10  
   Using Imaging Software with Migration Manager ............................................................................... 10  
   ITSM Environments and Appliances .................................................................................................... 10  
   Moving Applications ............................................................................................................................. 10  

2. **Planning a Migration Project with Migration Manager** ................................................................. 11  
   Overview ............................................................................................................................................. 11  
   Project Considerations ......................................................................................................................... 11  
      Types of Computers and User Profiles ............................................................................................... 11  
      Number of Computers ....................................................................................................................... 11  
      Networked Environment ..................................................................................................................... 11  
      Operating System Deployment .......................................................................................................... 11  
      User State Data Storage .................................................................................................................... 11  
   Migration Manager Process Overview .................................................................................................. 12  
      Installing Migration Manager ............................................................................................................ 12  
      Choosing a Data Store Location ......................................................................................................... 12  
      Creating Configuration Files ............................................................................................................. 12  
      Extracting User State Data ................................................................................................................ 12  
      Injecting User State Data .................................................................................................................... 13  
   Migrating Computers in a Networked Environment .............................................................................. 13  
      Overview ............................................................................................................................................ 13  
      Source Systems .................................................................................................................................. 13  
      Target Systems ................................................................................................................................... 13  
      Process ............................................................................................................................................... 13
9. Restore Files ............................................................................................................................................... 52
   Overview................................................................................................................................................. 52
   Restoring Files .......................................................................................................................................... 52
      Specifying the Data Store Location ...................................................................................................... 52
      Selecting the User State Data to Restore Files From .......................................................................... 53
      Selecting Files to Restore .................................................................................................................... 54
      Redirecting Files .................................................................................................................................. 55
      Restoring a Particular Version of a File ................................................................................................. 56
10. File Rules ................................................................................................................................................ 57
    Overview................................................................................................................................................. 57
    How File Rules Work ............................................................................................................................... 57
       Include/Exclude Rules ........................................................................................................................... 57
       File Rule Criteria .................................................................................................................................. 58
       File Rule Evaluation Order .................................................................................................................... 58
       File Rule Path Tokens ........................................................................................................................... 59
       Using Wild Cards in File Rules ............................................................................................................. 62
       Moving Files on the Target System ........................................................................................................ 63
       Files that Match Multiple File Rules ..................................................................................................... 64
    Defining File Rules .................................................................................................................................. 65
       Adding New File Rules ............................................................................................................................ 66
       Editing File Rules ................................................................................................................................ 67
       Deleting File Rules ................................................................................................................................. 68
       Changing File Rule Evaluation Order ..................................................................................................... 68
    File Rule Editor ......................................................................................................................................... 69
       Include or Exclude ................................................................................................................................. 69
       Source Path .......................................................................................................................................... 69
       Date Criteria .......................................................................................................................................... 70
       Size Criteria .......................................................................................................................................... 71
       Remapping Files ................................................................................................................................... 71
11. Registry Rules .......................................................................................................................................... 73
    Overview................................................................................................................................................. 73
    How Registry Rules Work ......................................................................................................................... 73
       Scope ................................................................................................................................................... 73
       Path Translation ................................................................................................................................... 73
    Defining Registry Rules ............................................................................................................................ 74
       Adding a Registry Rule ............................................................................................................................ 74
       Deleting a Registry Rule ........................................................................................................................ 75
17. **Support Notes** .............................................................................................................................. 90
   Supported Operating Systems .................................................................................................................. 90
   Supported ITSM Environments and Appliances ......................................................................................... 90
   Supported Migration Paths ......................................................................................................................... 90
   Operating Systems ...................................................................................................................................... 90
   Microsoft Office .......................................................................................................................................... 91
   Supported Content ....................................................................................................................................... 91
   Microsoft Office .......................................................................................................................................... 91
   Other Supported Applications ..................................................................................................................... 92
   Windows Options ......................................................................................................................................... 92
   User Documents and Media Files ................................................................................................................ 93
   Windows Explorer ......................................................................................................................................... 93
   Control Panel Settings ................................................................................................................................. 93
   Microsoft Office Content Notes ................................................................................................................ 93
   Spelling and Grammar Settings ................................................................................................................... 93
   InfoPath ...................................................................................................................................................... 94
   Outlook ....................................................................................................................................................... 94

18. **Copyright and Patent Information** .................................................................................................. 95
1. Introduction

Overview
Migration Manager captures and transfers user state between PCs, Remote Desktop Services hosts, virtual images, or from offline Windows, translating the captured user state when needed to match operating system and application upgrades.

Migration is a painful, costly process for any organization. Migration Manager dramatically lowers the cost, reduces the labor and increases the success rate of any PC refresh or OS migration project. The tool ensures a smooth, repeatable process that can be used to migrate a single user’s system or automate migration for hundreds or thousands of PCs. Migration Manager not only moves data files, but eliminates time spent configuring settings on the new platform. Moreover, it increases user satisfaction and reduces support calls post-migration. Migration Manager also can be used to back up user state in order to restore settings and data when needed. The software proves invaluable in case of loss or damage of key employee PCs.

What is User State?
The user state represents everything that makes a computer personal and productive for a user. This includes operating system settings, application settings and the user’s data files stored locally on the computer.

Note
The Migration Manager user interface uses the term Personality instead of User State. The meaning is the same in both cases.

Operating System Settings
Operating system elements handled by Migration Manager include the user’s desktop background, Windows Explorer settings, task bar and start menu settings, control panel settings, dial-up networking, etc.

Application Settings
Migration Manager translates literally thousands of application settings from common applications such as Microsoft Office. This includes e-mail and web browser settings, cookies and favorites. The software can also be configured easily to support settings from any commercial or custom application.

Documents and Data Files
Migration Manager locates and moves documents and files to ensure no data is missed, including application data in directories not visible to the user. Migration Manager also finds documents not only in the user’s profile folders (like My Documents or My Pictures) but in any location on the computer.
Custom Applications
Migration Manager can be configured to support any application through its File and Registry Rule features (see Chapters 10 and 11 for more information).

How Does Migration Manager Work?
Migration Manager has 3 major components:

- Core Engine
- User Interface
- Content

Core Engine
The Core Engine in Migration Manager takes the defined configuration (see Chapter 5 for information on configuring Migration Manager) and the associated content (see below) and executes the migration.

User Interface
Primarily intended for administrators to use when configuring migrations, it can also be used to do interactive operations. The Migration Manager user interface makes it easy to configure exactly what should be done and when used for interactive operations eliminates the need for remembering command-line parameters to use. See Chapters 4 through 12 for more information on the user interface.

Content
Migration Manager content defines:

- Where application settings are stored.
- How application settings are stored.
- How application settings should be transformed when going from one version to another (e.g. going from Word 2003 to Word 2010).
- What file types to migrate.

The content that should be included in a migration is part of the configuration (see Chapter 6 for more information on configuring content)

Process
Chapter 2 covers recommended steps for performing migration projects using Migration Manager, but at a high level the sequence of events is this:

1. Install Migration Manager in a central location (see Chapter 3).
2. Create one or more configuration files using the user interface (see Chapter 5).
3. Run Migration Manager on each of the source systems from which user state data should be extracted (read). See the “Automating Migration Manager” guide for more information on how this can be automated.
4. Run Migration Manager on each of the target systems to which user state data should be injected (written to). Note that this process can also be automated.
Automating Migration Manager

Almost every aspect of Migration Manager can be scripted and automated through the use of the extensive command-line support provided by Migration Manager. Please see the separate “Automating Migration Manager” guide for a complete reference of the command-line features of Migration Manager.

It is also possible to use Migration Manager to migrate individual systems or a small number of systems. The process descriptions in Chapter 2 cover these scenarios.

Flexible Application Support

The Migration Manager Core Engine is very flexible and designed to keep pace with new versions of applications and operating systems. The engine also provides File and Registry Rule technology (see Chapters 10 and 11) which enable IT administrators to quickly and easily add support for any application.

Using Imaging Software with Migration Manager

Migration Manager and imaging software for operating system and application deployment work hand-in-hand as part of an overall deployment process. Imaging technology ensures that identically configured computers are deployed to users with the right version of the operating system, applications, required patches, etc.

Prior to imaging, Migration Manager extracts the user state from the source computer(s). After the imaging is complete, Migration Manager injects the previously-extracted user state into the freshly imaged computer.

ITSM Environments and Appliances

Migration Manager works in IT Service Management environments and on appliances, where offline users can easily be extracted. With a single install to a shared network location, Migration Manager can be run from 32-bit or 64-bit Windows PE environments.

Moving Applications

Migration Manager moves application settings and data associated with those applications, but does not move the applications themselves. There are many reasons for this, but some of the more important are:

- It’s easy to get into a state where you violate the licensing terms of the software by having it installed on 2 systems instead of the 1 licensed computer
- Many software vendors only support applications that have been installed by the appropriate installer, not installed by other means
- When migrating users, this typically happens as part of an overall operating system and application deployment with both the operating system and applications being upgraded to a more recent version rendering the idea of moving the applications moot
2. Planning a Migration Project with Migration Manager

Overview
This Chapter covers what to consider when planning a migration project with Migration Manager and recommended steps to make migrations as efficient and painless as possible.

Project Considerations
Examining the basic conditions and available resources helps determine the best approach to a project. Aspects to consider include:

Types of Computers and User Profiles
Migration Manager can migrate user state from both regular Windows desktops and from servers used for Terminal Services/Remote Desktop Services. Migration Manager also supports roaming profiles, profiles using folder redirection, and saving user state from offline Windows. Different types of profiles have different requirements.

Number of Computers
Determining the number of computers to be migrated informs whether to automate extraction and injection processes. Migration Manager can handle manual or automated migration up to thousands of systems.

Networked Environment
In a networked environment, a central server may be used to store user state data extracted during migration. Bandwidth limitations must also be taken into account. If no networked environment is available, external media storage will be required.

Operating System Deployment
Is the migration part of an overall OS deployment project in which deployment tools are used? Migration Manager can be integrated with common OS deployment solutions to automate user state extraction from the prior platform and injection (including any upgrade translation required) following OS and application installation by the deployment tool.

User State Data Storage
User state data can take up a considerable amount of space when user data files are included. Sufficient storage space must be provided. Storage space is particularly important if user data will be stored for some length of time (e.g. in gradual migration or user-state backup scenarios).
Migration Manager Process Overview

1. Install Migration Manager in a central location (see Chapter 3).
2. Create one or more configuration files using the user interface (see Chapter 5).
3. Run Migration Manager on each of the source systems where user state data should be extracted (read). See the “Automating Migration Manager” guide for more information on how this can be automated.
4. Run Migration Manager on each of the target systems where user state data should be injected (written) to. This can also be automated.

Installing Migration Manager

Migration Manager supports a single installation on a server from which Migration Manager is shared so it can be accessed and run from other systems. This is described in more detail in Chapter 3.

Choosing a Data Store Location

Bandwidth, storage space, duration of migration and availability of a network connection are all critical considerations in choosing a data store location. The size of a typical user’s data files, multiplied by the number of users being extracted, is a reasonable estimate for how much space is needed (although since Migration Manager compresses data, the space required will typically be less).

As mentioned earlier, the overall migration process determines how much storage space is required. In a large, automated migration project, large volumes of user data may be extracted, requiring more storage space. Additionally, it may be necessary to incrementally extract data from the source systems over a period of time as there may be too many systems to be able to do it in one single operation due to network bandwidth considerations. In this case, dedicated storage space will be required until the data can be injected to the target systems.

Alternatively, less storage space is needed if systems are migrated in small batches. Dedicated storage space will be required only briefly since the data is injected soon after extraction.

Creating Configuration Files

The complexity of the migration project determines how many configuration files are required. For a smaller project a single configuration file may cover all migration parameters. For a larger, more complex, project multiple configuration files may be required depending on the variety of applications, different types of users and so on.

Configuration options are described in Chapter 5 and the “Automating Migration Manager” guide explains how to specify configuration files in automation scenarios.

Extracting User State Data

Extracting user state data is performed on the previous or “source” PC. While extraction can be performed manually using Migration Manager’s user interface, the rich command-line capabilities in Migration Manager make it easy to integrate into any desktop management suite.

Chapter 6 describes the extraction user interface and the “Automating Migration Manager” guide provides a complete command-line reference.
Injecting User State Data

Injection is done after target systems have been prepared by installing the operating system and applications. Translations may also occur during the injection process in cases of OS and application upgrades.

Chapter 7 describes the injection user interface and the “Automating Migration Manager” explains how to automate injections.

Migrating Computers in a Networked Environment

Overview

The most common scenario for using Migration Manager is an environment with one or more Windows domains in which users are migrated from their old systems to new systems. Usually migration occurs in conjunction with an operating system upgrade, application upgrade, and/or PC replacement project.

Source Systems

Migration Manager fully supports both systems primarily used by a single user and systems shared by several users. The “Automating Migration Manager” guide describes how to include or exclude specific users or categories of users (e.g. local computer accounts).

Target Systems

The operating system and applications must be installed on target systems prior to user state injection. Injecting user state after installing applications is critical, as most installers wipe out settings found during installation and replace them with defaults.

Process

In order to make the migration process as efficient as possible, it’s possible to extract and inject multiple systems in parallel. Migration Manager is flexible enough to support either all extractions followed by all injections, or paired extraction and injection operations.
Migrating Users between Domains

Process

Migration between domains in a networked environment is typically done through command-line automation using the /DOMAIN or /INCLUDEUSER commands (described in the “Automating Migration Manager” guide). This can also be done in the user interface as described in Chapter 7.

Other than specifying the relevant /DOMAIN or /INCLUDEUSER domain, domain migration is no different from the general process for migrating users in a networked environment described above.

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Migration Manager does not create domain user accounts. If a user is being migrated from DomainA to DomainB (e.g. the user DomainA\hdowd is being migrated to DomainB\hdowd), the user’s account must already exist in the target domain or the injection will fail.</td>
</tr>
<tr>
<td>While the new account must exist, it is not necessary for the user to log on to DomainB prior to migration.</td>
</tr>
</tbody>
</table>

Migrating Stand-Alone Computers

Overview

To migrate individual computers in a stand-alone manner, install Migration Manager and store extracted data on removable storage (e.g. a USB flash drive, a USB hard drive, etc.).

If using a USB flash drive, the device must be large enough to hold extracted user state data. The size of the user’s data files is a reasonable estimate for how much space is needed (although since Migration Manager compresses data, the space required will typically be less).

Installation

The Migration Manager installation program does not display removable devices as possible destination devices. It is necessary to specify the drive letter of the removable device in the installation path.

Alternatively, if Migration Manager is installed on a computer, the installation directory (with all of the sub-directories) can be copied to the removable device.
Process

The following process applies when using a removable storage device:

1. Add the removable storage device to the source system.
2. Navigate to the directory where the Migration Manager files are located.
3. Launch MigrationManager.EXE
4. Select the users and applications that should be migrated (see Chapter 6 for more information).
5. Run the extraction.
6. Remove the device from the source system.
7. Add the device to the target system.
8. Navigate to the directory where the Migration Manager files are located.
9. Launch MigrationManager.EXE
10. Select the user state data that should be injected (see Chapter 7 for more information).
11. Run the injection.

Of course it’s also possible to create scripts to do the extraction and injection automatically. See the “Automating Migration Manager” guide for more information on using Migration Manager from the command-line.
Migrating Users with Roaming Profiles

Migration Manager supports migrating users configured to use Roaming Profiles. There are, however, some prerequisites for being able to migrate all user-related information. The best practices configuration steps provided by Microsoft for Roaming Profiles on Windows Server 2008 R2 are summarized below.

Note

The steps below grant System Administrators full access to all files stored on the Roaming Profiles share. This is necessary for Migration Manager to be able to extract files that belong to the users. If this doesn’t work for your environment you will not be able to use Migration Manager to migrate users configured with Roaming Profiles.

Profile Share Configuration

On the server that will be used to hold the Roaming Profiles:

1. Create the directory where the profiles will be stored (e.g. C:\Users)
2. Create a share for the directory and give it a name ending with a ‘$’ (e.g. Users$), this ensures that the share will be hidden from browsing.
3. Grant “Full Control” permissions on the share to these groups:
   - SYSTEM
   - Roaming Profiles (domain group)
   - Domain Admins (domain group)
   - Administrators (domain group)
4. Grant “Full Control” security permissions to the directory to these groups:
   - Domain Admins (domain group)
   - Administrators (domain group)
5. The security group that contains all Roaming Profile domain accounts needs special security permissions to the directory (set to apply to the directory only):
   - List folder/read data (Allow)
   - Create folders/write data (Allow)
6. Finally, the built-in security group “CREATOR OWNER” must be granted special security permissions to the directory (set to apply to subfolders and files only):
   - Full control (Allow)

Group Policy Configuration

In order for Migration Manager to work properly in a Roaming Profiles environment, the account running Migration Manager operations must have access to all profile resources. The best way to provide the access to Migration Manager in a Roaming Profiles environment is to have the Administrators security group have "Full Control" over Roaming Profiles. This means that the account that runs Migration Manager on target systems must be part of the built-in Administrators group on the
system that stores the Roaming Profiles or is part of a domain security group that is part of the Administrators security group.

### Note

The built-in Administrators security group must be used since Group Policy does not allow any other security group to be granted administrator access to Roaming Profiles.

1. Open the Group Policy Management Editor (gpedit.msc) to edit the Default Domain Policy (it’s recommended to edit this policy to ensure that the policy is enforced on all computers in the domain)
2. Navigate to Computer Configuration | Administrative Templates | System | User Profiles
3. Enable the “Add the Administrators security group to roaming user profiles” policy
4. Save and close the Group Policy Management Editor

### Note

If you plan on using Migration Manager right away you will need to force a Group Policy on all computers in the domain.
Migrating Users with Folder Redirection Enabled

Migration Manager supports migrating users configured to use Folder Redirection. There are, however, some prerequisites for being able to migrate all user-related information. The best practices configuration steps provided by Microsoft for Folder Redirection on Windows Server 2008 R2 are summarized below.

Profile Share Configuration

On the server that will be used to hold the redirected folders:

1. Create the directory where the users’ redirected folders will be stored (e.g. C:\Users)
2. Create a share for the directory and give it a name ending with a ‘$’ (e.g. Users$), this ensures that the share will be hidden from browsing.
3. Grant “Full Control” permissions on the share to these groups:
   - SYSTEM
   - The security group that contains all users configured to use Folder Redirection (e.g. Folder Redirection Users)
   - Domain Admins (domain group)
   - Administrators (domain group)
4. Grant “Full Control” security permissions to the directory to these groups:
   - SYSTEM
   - Domain Admins (domain group)
   - Administrators (domain group)
5. The security group that contains all Folder Redirection domain accounts needs special security permissions to the directory (set to apply to the directory only):
   - List folder/read data (Allow)
   - Create folders/write data (Allow)
6. Finally, the built-in security group “CREATOR OWNER” must be granted special security permissions to the directory (set to apply to subfolders and files only):
   - Full control (Allow)

Note

The user used to run Migration Manager during extraction/injection of users configured for Folder Redirection must be a member of the Domain Admins security group.
Migrating Users in a Remote Desktop Services Environment

Migration Manager supports migrating users to/from Remote Desktop Services (RDS) and Terminal Services (TS) environments. This section describes recommended configuration settings for Migration Manager to work effectively.

Recommended Host Server Configuration Settings

<table>
<thead>
<tr>
<th>General Setting</th>
<th>Recommended Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete temporary folders on exit</td>
<td>Yes</td>
</tr>
<tr>
<td>Use temporary folders per session</td>
<td>Yes</td>
</tr>
<tr>
<td>Restrict each user to a single session</td>
<td>Yes</td>
</tr>
<tr>
<td>User logon mode</td>
<td>Allow all connections</td>
</tr>
</tbody>
</table>

The licensing mode of the environment does not impact Migration Manager.

If a Connection Broker is configured for your environment, it’s important to ensure that all user profiles are synchronized among the fail over or farm servers; otherwise the extracted profile data may be incomplete or out of date.

Gateway Configuration

If a Gateway is configured for your environment, the Connection Authorization Policy must be configured to allow the administrator account used to run Migration Manager full access to the server.

The Resource Authorization Policy (RAP) must be configured to allow for the most permissive access to system resources for the administrative account used to run Migration Manager; preferably Migration Manager should be granted access to all resources. If this conflicts with your security policies it’s possible to configure a temporary RAP to allow for permissive access for Migration Manager operations and then revert back to more restrictive RAP when the operation is complete.

Migrating Users from an offline system

Overview

From Windows PE, Migration Manager can be launched from a network share. User states can be extracted from the offline Windows system. The boot drive and Windows PE system drive are automatically excluded. Currently, Migration Manager must be launched from Windows to inject user states.

Process

Install Migration Manager to a network share. Launching MigrationManager.cmd from Windows PE will ensure Migration Manager launches with the same architecture as the Windows PE OS (the offline Windows system can be the same or different architecture). Offline users can be extracted through the user interface or automated. The process can be automated using the same command lines used for migrating an online Windows system, by calling MigrationManager.cmd instead of MigrationManager.exe in the command line. To inject the user states, Migration Manager must be
launched from the target Windows machine, and the source offline personality by default is stored under the Windows PE MAC address instead of by computer name.
3. Installing Migration Manager

Overview
Migration Manager can be installed on a central server and run from that shared location when operations need to be performed on individual computers.

It should be noted that in a distributed environment with multiple offices, it's desirable to do a central installation of Migration Manager in each branch office to avoid sending data between sites. Your network layout will determine the best deployment strategy for your needs.

Deployment Model

![Diagram of Migration Manager central server deployment]

Installing Migration Manager

Preparing for the Installation
The Migration Manager installer (MigrationManager.msi) must be run on the computer where it is intended to be installed.

Before starting installation, create a file share for the directory where Migration Manager will be installed. This file share provides:
- Access to the Migration Manager binaries so that you can run Migration Manager on other computers by starting Migration Manager from this file share.
- A shared location to store configuration files (see Chapter 5 for more information on configuration files).
- A default location for storing user state data.
- A distribution point for the optional Migration Manager client.

As an example, if you’re planning on installing Migration Manager in the location C:\MigrationManager, you would use the following steps to create the file share:

1. Create the directory C:\MigrationManager.
2. Give the appropriate users read/write permissions to the directory (since user state data will be stored in C:\MigrationManager\Personalities by default, the user(s) who will be running Migration Manager must have read/write access).
3. Finally, share C:\MigrationManager, giving the appropriate users Change sharing permissions).

**Note**

If you will be using a service account to run Migration Manager operations, only the service account needs to be given access to the file share.

In the examples below, the name of the computer where Migration Manager is being installed is MyComputerName and the file share is named MigrationManager.

**Running the Installer**

1. Locate MigrationManager.msi to start the installer.
2. Click Next to view the license agreement.
3. Specify where Migration Manager should be installed by entering the UNC path of the share you created as part of preparing for the installation. You can also choose whether to create
a desktop shortcut for launching Migration Manager (a Start Menu group is created automatically).

4. Provide a valid license file when prompted.
5. Click the Install button to perform the installation and accept the UAC prompt that will be displayed afterwards.
6. Wait for the installation to complete.
7. After the installation has completed, review the release notes for any information that may not have made it into this documentation and then click Next to continue.
8. Click Finish to complete the installation.
9. To launch Migration Manager, double-click the desktop icon if you chose the option to create one in step 3; otherwise go to Start | All Programs | Migration Manager and click the Migration Manager icon there.
4. Migration Manager User Interface Overview

Overview

The Migration Manager user interface is most commonly used to configure Migration Manager for a subsequent migration operation executed from the command-line. It is, however, possible to perform all operations supported by Migration Manager through the user interface.

Migration Manager Operations

Migration Manager can perform four primary operations:

- Extract user state data
- Inject user state data
- Backup user state data
- Restore files from user state data

Extract User State Data

Extracting user state data is the process of capturing user settings and application data from a source system in preparation for later injecting it to a target system.

Inject User State Data

Injecting user state data is the process of writing previously extracted user settings and application data to a target system, translating the user state to match a newer version of Windows and/or applications when required.

Backup User State Data

Backing up user state data is the process of extracting only what has changed since the original extraction (or last backup) of a particular user state.

There are two major reasons for using the Backup feature in Migration Manager:

- Large enterprise migrations may require weeks to extract user state from all source PCs and deploy new platforms. As users continue to use their PCs, extracted user state becomes outdated. Once the target PCs and infrastructure are ready for injection, Migration Manager Backup can extract incremental changes from source PCs for a fast, lightweight process that ensures no valuable user data is left behind.
- Ongoing, regular user state backup ensures that if a user’s PC must be replaced or reimaged, a user’s files and settings can be quickly restored.

Restore Files from User State Data

The Restore Files feature of Migration Manager can be used to retrieve only a subset of the files captured as part of an extraction or backup. Restore Files allows users to browse or search and selectively restore files contained in the user data store.

This feature is the only feature of Migration Manager that can’t be performed through the command-line since it requires users to specify which files to restore.
Main Window

This is the window displayed when you first start Migration Manager:

![Main Window Diagram]

Each of the 4 main tasks that can be performed by Migration Manager has a specific view. You select the task to perform by clicking the corresponding task icon in the list on the left. The individual task views are described in their own Chapters later in this document.

Figure 2: The Migration Manager main window.
## Main Menu

### File

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open</td>
<td>Load a different configuration file (see Chapter 5).</td>
</tr>
<tr>
<td>Save</td>
<td>Save the current configuration file.</td>
</tr>
<tr>
<td>Save as</td>
<td>Save the current configuration file with a different name.</td>
</tr>
<tr>
<td>Select data store location</td>
<td>Specify the location user state data should be stored to or loaded from.</td>
</tr>
<tr>
<td>Exit</td>
<td>Exit Migration Manager</td>
</tr>
</tbody>
</table>

### Edit

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preferences</td>
<td>Displays the preferences dialog used to configure Migration Manager (see Chapter 5)</td>
</tr>
<tr>
<td>File Rules</td>
<td>Add, edit or delete File Rules (see Chapter 10)</td>
</tr>
<tr>
<td>Registry Rules</td>
<td>Add, edit or delete Registry Rules (see Chapter 11)</td>
</tr>
<tr>
<td>Export File and Registry Rules</td>
<td>Export File and Registry Rules so they can be reused in other projects (see Chapter 12).</td>
</tr>
<tr>
<td>Import File and Registry Rules</td>
<td>Import previously exported File and Registry Rules (see Chapter 12).</td>
</tr>
<tr>
<td>Delete Personalities</td>
<td>Delete existing user state data (see Chapter 16).</td>
</tr>
</tbody>
</table>

### View

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Toolbar</td>
<td>Toggle the visibility of the toolbar in the main window.</td>
</tr>
<tr>
<td>Content Help Text Pane</td>
<td>Toggle the visibility of the content help text in the extract and inject task views.</td>
</tr>
<tr>
<td>Status Bar</td>
<td>Toggle the visibility of the status bar in the main window.</td>
</tr>
<tr>
<td>Extract Personality</td>
<td>Display the Extract User State task view (see Chapter 6).</td>
</tr>
<tr>
<td>Inject Personality</td>
<td>Display the Inject User State task view (see Chapter 7).</td>
</tr>
<tr>
<td>Backup Personality Changes</td>
<td>Display the Backup User State task view (see Chapter 8).</td>
</tr>
<tr>
<td>Restore Files from Personality</td>
<td>Display the Restore Files task view (see Chapter 9).</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>Last Operation Log</td>
<td>Display the most recent Operation Log, if any (see Chapter 15).</td>
</tr>
<tr>
<td>Personality Logs</td>
<td>Display the folder where the Operation Logs are stored.</td>
</tr>
<tr>
<td>Session Log</td>
<td>Display the current session log (see Chapter 15).</td>
</tr>
<tr>
<td>All Session Logs</td>
<td>Display the folder containing all session logs on this computer.</td>
</tr>
</tbody>
</table>

**Help**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Migration Manager Help</td>
<td>Displays the Migration Manager help file.</td>
</tr>
<tr>
<td>Tranxition</td>
<td>Opens a browser window displaying the Tranxition website.</td>
</tr>
<tr>
<td>Package Log Files for Support</td>
<td>Displays a dialog that makes it easy to capture the log files needed when opening a support case (see Chapter 15).</td>
</tr>
<tr>
<td>About Migration Manager</td>
<td>Displays version information about your copy of Migration Manager.</td>
</tr>
</tbody>
</table>

**Toolbar**

The toolbar provides quick access to items also available in the main menu:
5. Configuring Migration Manager

Overview

Before Migration Manager can be used to migrate users, it must be configured. The settings that control the behavior of Migration Manager are stored in a single XML configuration file which makes it possible to create different configuration files for different migration scenarios.

The configuration files are useful since they allow an administrator to pre-define behavior and what should be migrated ahead of time so that Migration Manager later can be automated to perform those actions for a large number of users on a large number of systems.

Migration Manager Settings

There are 3 major types of settings for Migration Manager:

- The location of the user state data (i.e. where user state data should be written to and read from).
- The behavior of Migration Manager, defined using the Preferences dialog.
- The content to process in the migration (applies to extractions only).

This Chapter describes all 3 types of settings.

Data Store Location

The data store location controls where Migration Manager reads and writes user data from/to. This setting is stored in the configuration file, but can also be overridden from the command-line for automation purposes (see the “Automating Migration Manager” guide for details on the command-line capabilities of Migration Manager).

In the user interface this setting can be changed both from the File menu and in each of the task views.

Note

Do not set the data store path to be the root of a drive (e.g. C:\). In Windows 7 and later, most users (including administrative users) do not have permissions to create files in the root of a drive, which causes a problem when Migration Manager attempts to create a file in the data store to validate that it can write to the data store.

The recommended approach is to use a sub-directory for the data store (e.g. C:\Personalities). This also reduces the number of directories Migration Manager needs to examine when searching for personalities in the data store.

HTTP Support

Migration Manager supports using a WebDAV store for user state data. With the exception of restoring files from user state data (see Chapter 9), this feature is not available from the user interface and can only be used with command-line automation as described in the “Automate Migration Manager” guide.
Preferences Dialog

The preferences dialog lets you define settings that control the behavior of Migration Manager during both extraction and injection. It also controls logging and HTTP settings.

Extraction Policies

![Extraction policies in the preferences dialog.](image)

<table>
<thead>
<tr>
<th>Policy</th>
<th>Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exclude the user’s temporary directory</td>
<td>Causes Migration Manager to skip any files located in the user’s temporary files directory.</td>
</tr>
<tr>
<td>Exclude the user’s temporary Internet directory</td>
<td>Causes Migration Manager to skip any files located in the user’s temporary Internet files directory.</td>
</tr>
<tr>
<td>Exclude the Program Files directory</td>
<td>Causes Migration Manager to skip any files located in the Program Files directory (both the 32- and 64-bit directory on 64-bit systems).</td>
</tr>
<tr>
<td>Exclude the Windows directory</td>
<td>Causes Migration Manager to skip any files located in the Windows directory.</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Exclude files from user profiles not being</td>
<td>Causes Migration Manager to auto-generate exclude file rules that exclude</td>
</tr>
<tr>
<td>extracted</td>
<td>the profile directories of those users not being extracted.</td>
</tr>
<tr>
<td>Extract files from profile folders located</td>
<td>When enabled, files located in profile folders located on a network share</td>
</tr>
<tr>
<td>on network shares</td>
<td>(e.g. a user’s My Documents folder that has been redirected using Folder</td>
</tr>
<tr>
<td></td>
<td>Redirection) to be included in the extraction. If disabled, these files are</td>
</tr>
<tr>
<td></td>
<td>not extracted.</td>
</tr>
<tr>
<td></td>
<td>See Chapter 2 for more information about Roaming Profiles and Folder</td>
</tr>
<tr>
<td></td>
<td>Redirection considerations.</td>
</tr>
<tr>
<td>Disable compression</td>
<td>Disable the file compression used when storing files that are part of the</td>
</tr>
<tr>
<td></td>
<td>extracted user state data.</td>
</tr>
<tr>
<td></td>
<td>Using compression helps reduce the amount of disk space required to store</td>
</tr>
<tr>
<td></td>
<td>the user state data and it’s recommended that this policy be left disabled</td>
</tr>
<tr>
<td></td>
<td>(which is the default).</td>
</tr>
<tr>
<td>Require password protection</td>
<td>When this policy is enabled, any extraction performed through the user</td>
</tr>
<tr>
<td></td>
<td>interface will prompt for a password that should be used to protect the</td>
</tr>
<tr>
<td></td>
<td>extracted user state data.</td>
</tr>
<tr>
<td></td>
<td>For extractions performed through the command-line you need to use the</td>
</tr>
<tr>
<td></td>
<td>/PASSWORD parameter. See the Migration Manager Automation Guide for more</td>
</tr>
<tr>
<td></td>
<td>details.</td>
</tr>
<tr>
<td>Personality Naming</td>
<td>By default, personality folders use the extraction Computer Name when</td>
</tr>
<tr>
<td></td>
<td>extracting from Windows, and MACID when extracting offline Windows using</td>
</tr>
<tr>
<td></td>
<td>Windows PE.</td>
</tr>
<tr>
<td></td>
<td>The command line /PERSONALITYPATH, or /NAME can be used to override this</td>
</tr>
<tr>
<td></td>
<td>setting.</td>
</tr>
<tr>
<td>Exclude MAC Address for Wireless Networks</td>
<td>Excludes MAC Address for wireless networks when personality naming is</td>
</tr>
<tr>
<td></td>
<td>MACID.</td>
</tr>
</tbody>
</table>
Note

The policies to exclude the user’s temporary files and temporary Internet files directories along with the Program Files and Windows directories are on by default and it’s recommended to leave them on unless there is a distinct need to extract files from these locations.

Note

The extraction policies impact the behavior of file rules as the policies are prioritized over file rules. Specifically the path tokens %WINDOWS%, %SYSTEM%, %SYSTEM64%, %PROGRAMFILES32% and %PROGRAMFILES64% are impacted (see page 59 for more information about path tokens). As an example, if the “Exclude the Windows directory” policy is enabled (which is the default), a file rule using the %WINDOWS% path token will not be evaluated.

The policy ‘Extract files from profile folders located on network shares’ also impacts user-specific path tokens such as %USERDOCUMENTS% if these folders have been redirected to a network location using Roaming Profiles or Folder Redirection.
## Injection Policies

![Preferences dialog](image)

**Figure 4: Injection policies in the preferences dialog.**

<table>
<thead>
<tr>
<th>Policy</th>
<th>Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transport broken shortcuts</td>
<td>By default, Migration Manager validates that a shortcut being injected points to a valid file and if that’s not the case places the shortcut in the directory C:\Broken Links instead. Enabling this policy turns off this validation and all shortcuts are injected regardless of whether they have a valid target or not.</td>
</tr>
<tr>
<td>Skip shortcut validation for non-logged in users</td>
<td>Disables shortcut validation when injecting user state for users that are not logged on interactively on the system.</td>
</tr>
<tr>
<td>Created accounts get local Administrator rights</td>
<td>When migrating local user accounts (i.e. not domain accounts) that don’t already exist on the target system, this policy enabled adds the</td>
</tr>
</tbody>
</table>
created local user to the local Administrators group.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transport administrative rights</td>
<td>If enabled, this policy causes migrated users to be added to the local Administrators group if they were members of that group on the source system.</td>
</tr>
<tr>
<td>Prevent injections to the following disks</td>
<td>This policy makes it possible to prevent Migration Manager from injecting data to local drives with the specified drive letters.</td>
</tr>
<tr>
<td>Allow injections to network locations</td>
<td>If enabled, this policy makes it possible to define File Rules that redirect files to a network location.</td>
</tr>
<tr>
<td>“Restore Files” ignores file replacement rules</td>
<td>If enabled, the Restore Files function will always overwrite existing files regardless of the defined File Replacement Rules.</td>
</tr>
<tr>
<td>Default password for local users created during injection</td>
<td>If local user accounts (i.e. not domain accounts) are created as part of an injection, this policy defines the password that should be used for those accounts.</td>
</tr>
</tbody>
</table>

**Note**

When the “Prevent injections to the following disks” policy is enabled, any files that were located on those disks on the source system will be placed in a directory named `C:\Migrated_<drive letter>_Drive` instead.

It’s not possible to prevent injection to the C drive.

**Note**

When allowing File Rules to redirect files to a network location it’s very important to make sure that the redirection path includes a user-specific component as you otherwise run the risk of files with the same names being overwritten.

The `%USERNAME%` File Rule token is useful for this purpose (e.g. a redirection path of `\server\users\%USERNAME%`).

Also note that if this policy isn’t enabled, files located in profile folders that have been redirected to a network location through the use of Roaming Profiles or Folder Redirection will not be injected.
Note

If password policies have been defined on the target system or the domain in a domain environment, the default password entered in the preferences dialog must match those password policies otherwise injections that need to create local user accounts will fail.

File Replacement Rules

![Preferences dialog showing file replacement rules]

**Figure 5: File replacement rules in the preferences dialog.**

<table>
<thead>
<tr>
<th>Rule</th>
<th>Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>Always replace</td>
<td>Migration Manager will always overwrite existing files on the target system with the files being injected.</td>
</tr>
<tr>
<td>Replace if newer</td>
<td>Migration Manager will only overwrite existing files on the target system if the file being injected has a more recent “last modified” date/time than the existing file.</td>
</tr>
<tr>
<td>Never replace</td>
<td>Migration Manager will never overwrite existing files on the target system.</td>
</tr>
</tbody>
</table>
Log File

Migration Manager uses two log files:

- An Operation Log that includes information about a particular operation (i.e. an extraction, injection, backup or file restore)
- A session log file that includes information about everything happening in Migration Manager while it’s running.

See Chapter 15 for more information about the log files.

The preferences dialog allows you to control the amount of information logged to both the operation and session log files.

**Note**

Migration Manager only displays the Operation Log file for operations performed through the user interface. Operations performed through the command-line never display the Operation Log (although the Operation Log file, of course, is created and stored in the usual location).
HTTP Options

Migration Manager supports the use of WebDAV to store user state data when performing extraction, injection or backup operations through the command-line. If the WebDAV server requires authentication (recommended), Migration Manager supports Digest authentication and the authentication information must be entered here to be saved in the log file.

If HTTPS is being used and a self-signed or otherwise untrusted SSL certificate is used Migration Manager can be configured to not verify the certificate and enable operations against the server.

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>The default is for Migration Manager to verify SSL certificates. If an untrusted SSL certificate is used by the server, operations will fail unless Migration Manager is configured to not verify the certificate (or the certificate is added as a trusted certificate).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>If HTTP authentication fails, Migration Manager will exit with error code 331 to indicate that the error is specifically due to a HTTP authentication error.</td>
</tr>
</tbody>
</table>
Content Selection

The final set of data stored in the configuration file determines what application settings and data files are extracted. This selection is done in the Extract User State task view. For a full description, see Chapter 6.

With this information stored in the configuration file it’s possible to select different content for different users or user groups and create unique configuration files in order to make the extraction process more efficient and to limit the amount of data that is extracted.

Using Passwords for User State Data

When the “Require password protection” policy (see Extraction Policies on page 30) is enabled, Migration Manager will prompt for a password to protect the extracted user data:

Passwords are case-sensitive, must be between 7 to 15 characters in length and may only contain characters, digits and underscores.

Note

Migration Manager only prompts for a password during an extraction performed through the user interface. If you are performing a command-line extraction, the /PASSWORD command must be used to protect the user state data. See the Migration Manager Automation Guide for more information.

Personalities that are password protected are displayed in the personality drop down menu with a lock icon:
When injecting or restoring files from user state data, Migration Manager will ask for the password before allowing the operation to proceed:

![Password dialog]

**Note**

Migration Manager prompts for a password only for operations performed through the user interface. If the operation is performed through the command-line, the `/PASSWORD` command must be used; otherwise the operation will fail. See the Migration Manager Automation Guide for more information.

**Configuration Files**

Since all of the settings that impact Migration Manager operations are stored in the configuration file, it’s often useful to create different configuration files for different migration scenarios. These different configuration files can then be used either interactively (use File | Open in the Migration Manager menu to open a different configuration file than the currently active one) or from the command-line for automation purposes (see the “Automating Migration Manager” guide for more details on that).

**Default Behavior**

A default configuration file is installed by the main Migration Manager installer, but if Migration Manager can’t find a configuration file for any reason, a default configuration file is created. The default configuration file is always created on the local system (as opposed to the file share where Migration Manager is located) in the local program data directory (`C:\ProgramData` on Windows Vista and later).
6. Extract User State

Overview
There are two situations in which to use the Migration Manager “Extract Personality” user interface:

Automated Extractions
Selecting content for extraction to be saved to a configuration file. There’s no need to select users as this is done when using the command-line features of Migration Manager (see the “Automating Migration Manager” guide for more information).

Interactive Extractions
Configuring extractions, including selecting both content and users, as well as executing the process.

Configuring Extractions

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local administration rights are required in order to run Migration Manager. This is enforced using UAC on Windows Vista and later. See ELEVATEDCREDENTIALS in Automating Migration Manager to save credentials securely if the process must be run by a user without administrator rights.</td>
</tr>
</tbody>
</table>

Specifying the Data Store Location
If the data store location needs to be changed from the current setting, click the Browse button at the top of the extraction task view:

This displays a standard Windows folder browser dialog to select a new location for storing the user state data:
Selecting Users to Extract

When performing an interactive extraction, select the users to extract on the “User(s) to Extract” tab. The extraction task view displays the name of all users who have logged on to the system where Migration Manager is being used:

![Extract Personality](image)

**Figure 6: The users to extract task view.**

**Note**

Extracting the user who’s currently logged in is not recommended as Windows and many applications don’t save settings until the application is exited. This means Migration Manager may not be able to access current settings for the extraction.
For best results, exit all other applications prior to performing an extraction for the currently logged on user.

Selecting Content to Extract

Selecting the content to extract is done on the “Select for Extraction” tab:

![Figure 7: The select for extraction task view.](image)

Available content is organized into 3 groups:

- Applications – Settings and data for common applications such as Office 2010.
- Data Transport – File and Registry Rules (see Chapters 10 and 11).
- Windows Options – Settings for the operating system.

Check the box for each piece of content to extract. Expand the content tree for highly granular options.

**Note**

Selecting all available content can increase the time required to perform extractions and may include more data than required.

It’s recommended to limit selected content to applications that are in use and are deployed on the source systems.

Once the appropriate content has been selected, either click the Save button in the toolbar or use File | Save to save the content selection to the configuration file.
Performing an Interactive Extraction

For an interactive extraction, once users and content have been selected, click the Extract button to initiate the extraction. A progress dialog is displayed during the extraction, the dialog also provides information on the result of the extraction on completion:

![Progress dialog](image)

Click ‘Show Log’ to display the Operation Log for the extraction.

![Operation Log](image)

The Operation Log file contains information about what was included in the extraction and may be used for troubleshooting purposes or as an audit log of what was performed. See Chapter 15 for more detail on the Operation Log file.

Performing a Command-Line Extraction

The command used to perform an extraction from the command-line is `/AUTOEXTRACT`. Please see the “Automating Migration Manager” guide for more details.

Performing an Extraction within ITSM Environments and Appliances

Migration Manager can capture offline user states when launched from Windows PE. This can be an automated extraction or an interactive extraction. To run Migration Manager from either 32 or 64 bit Windows PE, launch MigrationManager.cmd instead of MigrationManager.exe. This removes any
requirement for WOW64 to be installed, and automatically launches Migration Manager with the matching architecture. The architecture of the offline Windows environment does not have to match that of Windows PE.

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Migration Manager does not currently restore to offline Windows machines. Simply run Migration Manager from the online target Windows machine.</td>
</tr>
</tbody>
</table>
7. **Inject User State**

**Overview**

Unlike extractions (see Chapter 6), very little needs to be configured for an injection apart from the injection policies described in Chapter 5.

To perform automated injections from the command-line, see the “Automating Migration Manager” guide for information on how to do this.

**Performing an Interactive Injection**

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local administration rights are required in order to run Migration Manager. This is enforced using UAC on Windows Vista and later.</td>
</tr>
</tbody>
</table>

**Specifying the Data Store Location**

If the data store location needs to be changed from the current setting, click the Browse button at the top of the injection task view:

![Inject Personality](image)

This displays a standard Windows folder browser dialog to select the new location from which to read the user state data:
Selecting the User State to Inject

Right below the data store location is a drop-down list containing the available user state data from the current data store location:

The information provided in the drop-down list includes:

- The date/time the user state was extracted (or last backed up if a backup has been performed).
- The name of the computer from which the user state was extracted.
- Whether the user state data is password protected, indicated by the use of a padlock icon.

Selecting Users to Inject

Once the user state data has been selected and loaded, the included users are displayed. If multiple users were extracted, it’s possible to deselect users that shouldn’t be injected on the target system:

The top half of this display shows the users that were extracted. The lower half shows the target users for the injection.

Note

Injecting to the currently logged on user is not recommended as the injected settings may not take effect properly.

For best results, reboot the target system after completing an injection to the logged on user.

By default, the target user is always the same as the source user (e.g. if the user MYDOMAIN\HDOWD was extracted, the target user is also MYDOMAIN\HDOWD). It is, however, possible to change the target user.
Changing the target user is useful particularly when moving users between domains. Use the command-line capabilities of Migration Manager to do this on a large scale, see the “Automating Migration Manager” guide for more details.

To choose a different target user, expand the nodes “Existing Users” or “Network Users” in the target user view and select the desired target user.

**Selecting What Content to Inject**

By default, Migration Manager injects all content that was extracted from the source system. Extracted content can be excluded from injection as needed by unchecking content in the “Select for Injection” task view:
Performing the Injection

Once the selections have been made, click the Inject button to start the injection. A progress dialog displays the progress and result of the operation:

![Injection Progress]

Click “Show Log” to display the Operation Log file for the injection (see Chapter 15 for more information).

Performing a Command-Line Injection

The command used to perform an extraction from the command-line is /AUTOINJECT. Please see the “Automating Migration Manager” guide for more details.

Performing an Injection within ITSM Environments and Appliances

To inject a personality of an offline Windows system, Migration Manager must be run from the target online Windows system. By default, the source computer will appear with the MAC address instead of computer name.

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Migration Manager does not currently restore to offline Windows machines.</td>
</tr>
</tbody>
</table>
8. Backup User State

Overview

Backing up the user state makes it possible to capture changes made to the user state since an initial extraction (or a previous backup, whichever is more recent). This includes changes to application settings as well as new and modified data files.

Backups are typically performed using command-line automation, but can also be performed interactively via the user interface.

Preconditions

- In order to perform a backup on a given system, an extraction must have been performed first.
- A backup can only be performed on the same system as the original extraction.

Limitations

Migration Manager is not intended to be a full-featured backup solution. Limitations include:

- Files deleted from the source system are still present in the Migration Manager user state backup and can be restored at a later date.
- Files renamed on the source system are treated as unique files in subsequent backups. Both the original and renamed file become part of the user state backup.
- Migration Manager does not perform differential backups. When a file is changed the entire new version of the file is backed up with the user state.
- Backup is not supported from offline Windows environments.

Note

Migration Manager only does incremental backups for file-based data. Application settings stored in the Registry is processed as a complete extraction every time a backup is performed.

Since the amount of data stored in the Registry is small compared to the file data, this has only a minimal impact on the size of the user state data.

Backups and Password Protection

User state data that is password protected does not require the password to be provided in order to perform a backup. The reason for this is that no access is given to the actual data in the user state data and that a backup only can be performed on the system where the data was originally extracted.
Performing an Interactive Backup

Specifying the Data Store Location

If the data store location needs to be changed from the current setting, click the Browse button at the top of the backup task view:

This displays a standard Windows folder browser dialog to select the new location from which to read the user state data:

Select the User State Data to Backup

Right below the data store location is a drop-down list containing the available user state data from the current data store location:

The information provided in the drop-down list includes:

- The date/time the user state was extracted (or last backed up if a backup has been performed).
- The name of the computer from which the user state was extracted.
- Whether the user state data is password protected, indicated by the use of a padlock icon.

Note

Only user state data extracted from the system where Migration Manager is running is listed.
Performing the Backup

Once the user state data has been selected, the users and settings that were extracted are displayed for informational purposes only. Click the Backup Changes button to start the backup. A progress dialog displays the progress and result of the operation:

Click “Show Log” to display the Operation Log file detailing what was included in the backup.

Performing a Command-Line Backup

The command used to perform an extraction from the command-line is /AUTOBACKUP. Please see the “Automating Migration Manager” guide for more details.
9. Restore Files

Overview

Restore Files makes it possible to restore individual files from extracted or backed up user state data. This is useful when files are needed from user state data but a full injection isn’t desirable.

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unlike extractions, injections and backup, Restore Files cannot be performed through the command-line. Restore files is not supported to offline Windows environments.</td>
</tr>
</tbody>
</table>

Restoring Files

Specifying the Data Store Location

Unlike the Extract, Inject and Backup task views, the Restore Files task view supports both file share-based and HTTP-based user state data stores:

![Restore Files](image)

This displays a standard Windows folder browser dialog to select the new location from which to read the user state data:
To use an HTTP(S)-based data store, click the HTTP button instead. This displays a dialog for entering the URL of the data store:

![HTTP Options dialog](image)

The functionality of Restore Files is the same regardless of the data store type.

**Selecting the User State Data to Restore Files From**

Right below the data store location is a drop-down list containing the available user state data from the current data store location:

![User state data list](image)

The information provided in the drop-down list includes:

- The date/time the user state was extracted (or last backed up if a backup has been performed).
- The name of the computer from which the user state was extracted.
- Whether the user state data is password protected, indicated by the use of a padlock icon.
Selecting Files to Restore

Once the user state data has been selected, the files contained in it are displayed in the user interface:

Expand the file tree on the left to see the files available in the different folders. Mark a file for restoration by checking the checkbox in front of the file name in the list to the right.

It’s also possible to search for files contained in the user state data by using the Search tab in the Restore Files task view:

Enter a search term in the search field and click the “Start Search” button to display the matching files in the list to the right. Select files by checking the corresponding boxes.
Note

When searching for files based on name, you need to either specify the exact file name (e.g. Q1 Report.docx) or use the wildcard character (e.g. Q1*, Q1 report.* or *report*). When searching for files based on file type you also use the wildcard character (e.g. *.docx).

File names are not case-sensitive

To restore the selected files, click the “Restore Files” button. A progress dialog shows the progress of the operation followed by a message stating the result of the operation. After the message has been dismissed, the Operation Log file is displayed with information about which files were restored to what locations.

Redirecting Files

When restoring files, it’s possible to redirect them to a different location than the location from which they were originally extracted. Redirection may be global for all files using the “Restore to” field available in the Restore Files task view:

Click the “Restore to” radio button and then click the “…” button to select the desired location.

Following global redirection, Migration Manager preserves the directory hierarchy as shown in this example:

Original location: C:\Project Data\Reports\Q1 Progress Report.docx
Redirection path: C:\Users\hdowd\Documents\Restored Files
Restore path: C:\Users\hdowd\Documents\Restored Files\C\Project Data\Reports\Restored Files\C\Project Q1 Progress Report.docx

Alternatively, it’s possible to redirect individual files. Double-click the desired file to display this dialog:

Specify the directory the file should be restored to using the “…” button in the dialog.
The effect of an individual file redirection is illustrated in the example below:

Original location: C:\Project Data\Reports\Q1 Progress Report.docx

Redirection path: C:\Users\hdowd\Documents\Restored Files

Restore path: C:\Users\hdowd\Documents\Restored Files\Q1 Progress Report.docx

Restoring a Particular Version of a File

When doing user state data backups, a new version is captured of each file that has changed since the last backup or the original extraction.

To restore a particular version of a file, double-click the desired file to display the File Properties dialog:

The drop-down list in this dialog contains an entry for each captured version of the file. Each version listed includes:

- A version number, starting with 0 for the most recent version, -1 for the next oldest and so on.
- The date the version was last modified.
- The date the version was extracted.

Select the version that to restored and click OK to save the selection.
10. File Rules

Overview

File Rules provide administrators with an easy mechanism for specifying files and/or directories that should be included or excluded in a migration based on several possible criteria:

- Location
- File type
- Date last modified
- Size

File Rules can also be used to remap files from a source location (e.g. C:\Project Files to <My Documents>\Project Files).

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>File rules override the selection of what should be extracted. For instance, if you select that all PowerPoint files should be extracted by selecting Applications</td>
</tr>
</tbody>
</table>

See Chapter 13 for an example of how to use File and Registry Rules to migrate settings for an application.

How File Rules Work

Every file that Migration Manager finds during an extraction is evaluated against the defined File Rules with the order of the rules being significant. File Rules override the selections made in the content tree (see Chapter 4) and can be used to limit the scope of the data extracted.

Include/Exclude Rules

A File Rule can define which files to include or exclude in an extraction.

An include rule is used to include files of a specific type or from a specific location (e.g. include all *.abc files in the user’s My Documents folder).

An exclude rule is usually used together with an include rule to limit the scope of the include rule. For example, to include all files from the C:\Project Data directory except for any *.wav files, define an include rule to include all files from C:\Project Data followed by an exclude rule for any *.wav files in the same directory.

Exclude rules can also be used by themselves. For example, to exclude all *.mp3 files from the user’s My Documents folder to avoid extracting large amounts of music files.

The order of rule definitions is important, see page 58 for more detail.
File Rule Criteria

File Rules can evaluate files based on the following criteria:

- Location (e.g. the user’s My Documents folder)
- File type (e.g. *.mp3)
- Last modified date (before or after a specific date)
- File size (greater or smaller than a specific size)

Note

It’s possible to specify multiple file types in a single file rule by separating each file extension by a ; - e.g. *.mp3;*.wav;*.wma.

It’s not necessary to use all possible criteria in a rule, but at a minimum a Source Path must be defined for inclusion or exclusion.

Note

When defining the Source Path for the rule, define if the rule applies to any subdirectories by checking or unchecking the Include Subdirectories check box.

File Rule Evaluation Order

The order in which File Rules are defined is important as this impacts the effect of the defined rules. See page 68 for information how to change the order of File Rules).

When two (or more) mutually exclusive rules match a file, the first defined rule takes precedence.

Note

If content has been selected (e.g. *.docx files) in the “Select for Extraction” tab, this functions as an implicit include File Rule that can be overridden by an explicit exclude rule. You can, for instance, select *.docx files in the content tree and define an exclude rule for *.docx files larger than 50 MB. The result is only *.docx files smaller than 50 MB are included in the extraction.

As an example to illustrate this, assume that the following 2 rules are defined (in this order):

1. Include all *.xlsx files in C:\Project Data
2. Exclude all files from C:\Project Data

With this order, all *.xlsx from C:\Project Data will be included in the extraction, but all other files in C:\Project Data will be excluded.

If the order of the rules is reversed to:

1. Exclude all files from C:\Project Data
2. Include all *.xlsx files in C:\Project Data

This will have the effect of the exclude rule taking precedence and no files from C:\Project Data will be included at all.
## File Rule Path Tokens

Paths frequently change when moving between different versions of Windows (e.g. the use of `C:\Documents and Settings` in Windows XP vs. `C:\Users` in Windows Vista and later). To support path changes, Migration Manager supports the use of tokens when defining file rules:

<table>
<thead>
<tr>
<th>Token</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
</table>
| %DESKTOP%               | The Desktop “directory”            | [XP] `C:\Documents and Settings\hdowd\Desktop`  
                           | [W8] `C:\Users\hdowd\Desktop`                 |
| %USERDESKTOP%           | The Desktop “directory”            | [XP] `C:\Documents and Settings\hdowd\Desktop`  
                           | [W8] `C:\Users\hdowd\Desktop`                 |
| %USERNAME%              | The user name of the user that is selected for extraction. | `Hdowd`                                      |
| %MYDOCUMENTS%           | The default document storage folder | [XP] `C:\Documents and Settings\hdowd\My Documents`  
                           | [W8] `C:\Users\hdowd\Documents`                |
| %USERDOCUMENTS%         | The default document storage folder | [XP] `C:\Documents and Settings\hdowd\My Documents`  
                           | [W8] `C:\Users\hdowd\Documents`                |
| %MYMUSIC%               | The default music storage folder   | [XP] `C:\Documents and Settings\hdowd\My Documents\My Music`  
                           | [W8] `C:\Users\hdowd\Music`                    |
| %USERMUSIC%             | The default music storage folder   | [XP] `C:\Documents and Settings\hdowd\My Documents\My Music`  
                           | [W8] `C:\Users\hdowd\Music`                    |
| %MyPICTURES%            | The default pictures storage folder | [XP] `C:\Documents and Settings\hdowd\My Documents\My Pictures`  
                           | [W8] `C:\Users\hdowd\Pictures`                 |
| %USERPICTURES%          | The default pictures storage folder | [XP] `C:\Documents and Settings\hdowd\My Documents\My Pictures`  
                           | [W8] `C:\Users\hdowd\Pictures`                 |
| %MYVIDEOS%              | The default videos storage folder  | [XP] `n/a`                                      
                           | [W8] `C:\Users\hdowd\Videos`                   |
| %USERVIDEOS%            | The default videos storage folder  | [XP] `n/a`                                      
<pre><code>                       | [W8] `C:\Users\hdowd\Videos`                   |
</code></pre>
<p>| %WINDOWS%               | The Windows directory              | <code>C:\Windows</code>                                  |</p>
<table>
<thead>
<tr>
<th>Environment Variable</th>
<th>Description</th>
<th>Path on 32-bit Systems</th>
<th>Path on 64-bit Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>%SYSTEM%</td>
<td>The 32-bit System32 directory</td>
<td>C:\Windows\System32</td>
<td>C:\Windows\SysWOW64</td>
</tr>
<tr>
<td>%SYSTEM64%</td>
<td>The 64-bit System32 directory</td>
<td>Note: Only valid on 64-bit systems.</td>
<td>C:\Windows\System32</td>
</tr>
<tr>
<td>%PROGRAMFILES32%</td>
<td>The 32-bit Program Files Directory</td>
<td></td>
<td>C:\Program Files [on 32-bit systems]</td>
</tr>
<tr>
<td>%PROGRAMFILES64%</td>
<td>The 64-bit Program Files Directory</td>
<td>Note: Only valid on 64-bit systems.</td>
<td>C:\Program Files</td>
</tr>
<tr>
<td>%FIXEDDISKS%</td>
<td>All local fixed drives (can only be used in the source path of a file rule)</td>
<td></td>
<td>n/a</td>
</tr>
<tr>
<td>%HOMEDRIVE%</td>
<td>Redirect files to a user's local or network home drive (used only in the Destination Path of a file rule)</td>
<td></td>
<td>n/a</td>
</tr>
<tr>
<td>%USERPROFILE%</td>
<td>The user's profile folder</td>
<td>[XP] C:\Documents and Settings\hdowd</td>
<td>[W8] C:\Users\hdowd</td>
</tr>
<tr>
<td>%SYSTEMTEMPLATES%</td>
<td>The folder where shared templates are stored</td>
<td>[XP] C:\Documents and Settings\All Users\Templates</td>
<td>[W8] C:\ProgramData\Microsoft\Windows\Temp lates</td>
</tr>
<tr>
<td>%USERROAMINGAPPDATA%</td>
<td>The file system directory that serves as a common repository for application-specific data.</td>
<td>[XP] C:\Documents and Settings\hdowd\Application Data</td>
<td>[W8] C:\Users\hdowd\AppData\Roaming</td>
</tr>
<tr>
<td>%USERRECENTFILES%</td>
<td>The file system directory that contains shortcuts to the user's most recently used documents.</td>
<td>[XP] C:\Documents and Settings\hdowd\Recent</td>
<td>[W8] C:\Users\hdowd\AppData\Roaming\Micros oft\Windows\Recent</td>
</tr>
<tr>
<td>%SYSTEMALLUSERS%</td>
<td>The root directory for the profile folders that are shared by all users.</td>
<td>[XP] C:\Documents and Settings\All Users</td>
<td>[W8] C:\Users\Public</td>
</tr>
<tr>
<td>Environment Variable</td>
<td>Description</td>
<td>Example Path (XP)</td>
<td>Example Path (W8)</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------</td>
<td>-------------------------------------------------------</td>
</tr>
<tr>
<td>%USERLOCALAPPDATA%</td>
<td>The file system directory that serves as a data repository for local (nonroaming) applications</td>
<td>C:\Documents and Settings\hdowd\Local Settings\Application Data</td>
<td>C:\Users\hdowd\AppData\Local</td>
</tr>
<tr>
<td>%SYSTEMDESKTOP%</td>
<td>The file system directory that contains files and folders that appear on the desktop for all users</td>
<td>C:\Documents and Settings\All Users\Desktop</td>
<td>C:\Users\Public\Desktop</td>
</tr>
<tr>
<td>%USERTEMPLATES%</td>
<td>The file system directory that serves as a common repository for document templates</td>
<td>C:\Documents and Settings\hdowd\Templates</td>
<td>C:\Users\hdowd\AppData\Roaming\Microsoft\Windows\Templates</td>
</tr>
<tr>
<td>%USERPROGRAMS%</td>
<td>The file system directory that contains the user's program groups</td>
<td>C:\Documents and Settings\hdowd\Start Menu\Programs</td>
<td>C:\Users\hdowd\AppData\Roaming\Microsoft\Windows\Start Menu\Programs</td>
</tr>
<tr>
<td>%USERCOOKIES%</td>
<td>The file system directory that serves as a common repository for Internet cookies</td>
<td>C:\Documents and Settings\hdowd\Cookies</td>
<td>C:\Users\hdowd\AppData\Roaming\Microsoft\Windows\Cookies</td>
</tr>
<tr>
<td>%SYSTEMAPPDATA%</td>
<td>The file system directory that contains application data for all users</td>
<td>C:\Documents and Settings\All Users\Application Data</td>
<td>C:\ProgramData</td>
</tr>
<tr>
<td>%USERHISTORY%</td>
<td>The file system directory that serves as a common repository for Internet history items</td>
<td>C:\Documents and Settings\hdowd\Local Settings\History</td>
<td>C:\Users\hdowd\AppData\Local\Microsoft\Windows\History</td>
</tr>
<tr>
<td>%USERFAVORITES%</td>
<td>The file system directory that serves as a common repository for the user's favorite items</td>
<td>C:\Documents and Settings\hdowd\Favorites</td>
<td>C:\Users\hdowd\Favorites</td>
</tr>
<tr>
<td>%USERSTARTMENU%</td>
<td>The file system directory that contains Start menu items</td>
<td>C:\Documents and Settings\hdowd\Start Menu</td>
<td>C:\Users\hdowd\AppData\Roaming\Microsoft\Windows\Start Menu</td>
</tr>
</tbody>
</table>
%USERCONTACTS%  The file system directory that contains the user’s contacts (only on Windows Vista and later)  

[W8] C:\Users\hdowd\Contacts

%USERSEARCHES%  The file system directory that contains the user’s saved searches (only on Windows Vista and later)

[W8] C:\Users\hdowd\Searches

For instance, to define a rule to exclude all *.mp3 files in the user’s profile folder, the location can be defined as %USERPROFILE%\*.mp3.

Using tokens as opposed to hard-coding paths make File Rules more robust and reusable for different versions of Windows (see Importing and Exporting Rules on page 76 for more information about reusing rules).

**Note**

The 64-bit path tokens (%SYSTEM64% and %PROGRAMFILES64%) are only valid on 64-bit systems. On 32-bit systems these path tokens don't have a valid value and instead expand into an empty string that will not match any files when the tokens are used in file rules.

### Using Wild Cards in File Rules

File Rules support the use of the following wild card characters:

- ? – matches a single character/digit
- * – matches any number of characters/digits

**Examples:**

<table>
<thead>
<tr>
<th>File or Folder Specification</th>
<th>Include Subdirectories</th>
<th>Matches</th>
</tr>
</thead>
<tbody>
<tr>
<td>C: \Readme.*</td>
<td>Yes</td>
<td>Readme.doc, Readme.rtf, Readme.txt, etc. anywhere on the C: drive (since subdirectories are included).</td>
</tr>
<tr>
<td>C: \Read*.doc</td>
<td>Yes</td>
<td>Readme.doc, Readthis.doc, etc. anywhere on the C: drive.</td>
</tr>
<tr>
<td>C: \Readme.??</td>
<td>Yes</td>
<td>Readme.doc, Readme.wri, Readme.txt, etc. anywhere on the C: drive. Will not include the files Readme.html, Readme.jpeg, etc.</td>
</tr>
<tr>
<td>C: \Read??.txt</td>
<td>Yes</td>
<td>Readme.txt anywhere on the C: drive. Will not find Readthis. txt.</td>
</tr>
</tbody>
</table>

Migration Manager User’s Guide  Page 62
Moving Files on the Target System

The final major feature of File Rules is the ability to move files when they are injected to the target system. For example, this feature can move user files located outside the user’s profile folder on the source system into the user’s profile folder on the target system.

A file rule could be defined as:

<table>
<thead>
<tr>
<th>Include</th>
<th>Source Path</th>
<th>Include Subdirectories</th>
<th>Destination Path</th>
<th>Preserve Subdirectories</th>
</tr>
</thead>
<tbody>
<tr>
<td>INCLUDE</td>
<td>C:*.doc;<em>.dot;</em>.docx;*.dotx</td>
<td>Yes</td>
<td>%MYDOCUMENTS%\Word Documents</td>
<td>No</td>
</tr>
</tbody>
</table>

The result of this rule would be to move all *.doc, *.dot, *.docx and *.dotx files found outside of the user’s My Documents folder and place them in a directory named Word Documents in the user’s My Documents folder on the target system (assuming the user’s My Documents folder is located at C:\Documents and Settings\hdowd\My Documents on the source system and C:\Users\hdowd\Documents on the target system):

<table>
<thead>
<tr>
<th>Source System</th>
<th>Target System</th>
</tr>
</thead>
<tbody>
<tr>
<td>C:\Project Data\Project Overview.doc</td>
<td>C:\Users\hdowd\Documents\Word Documents\Project Overview.doc</td>
</tr>
<tr>
<td>C:\Project Data\Reports\Q1 2001 Progress.docx</td>
<td>C:\Users\hdowd\Documents\Word Documents\Q1 2001 Progress.docx</td>
</tr>
<tr>
<td>C:\Documents and Settings\hdowd\My Documents\Progress Report.docx</td>
<td>C:\Users\hdowd\Documents\Progress Report.docx</td>
</tr>
</tbody>
</table>

**Note**

Files that are already located in the user’s profile folder (e.g. the 3rd file in the example above) are **not** moved by the rule, but are instead placed in the appropriate profile folder location.
Below, the definition of the rule is changed to preserve the subdirectory structure:

<table>
<thead>
<tr>
<th>Include/Exclude</th>
<th>Source Path</th>
<th>Include Subdirectories</th>
<th>Destination Path</th>
<th>Preserve Subdirectories</th>
</tr>
</thead>
<tbody>
<tr>
<td>INCLUDE</td>
<td>C:*.doc;*.dot; <em>.docx;</em>.dotx</td>
<td>Yes</td>
<td>%MYDOCUMENTS%\Word Documents</td>
<td>Yes</td>
</tr>
</tbody>
</table>

The result is that the files are placed like this on the target system:

<table>
<thead>
<tr>
<th>Source System</th>
<th>Target System</th>
</tr>
</thead>
<tbody>
<tr>
<td>C:\Project Data\Project Overview.doc</td>
<td>C:\Users\hdowd\Documents\Word Documents\Project Data\Project Overview.doc</td>
</tr>
<tr>
<td>C:\Project Data\Reports\Q1 2001 Progress.docx</td>
<td>C:\Users\hdowd\Documents\Word Documents\Project Data\Reports\Q1 2001 Progress.docx</td>
</tr>
<tr>
<td>C:\Documents and Settings\hdowd\My Documents\Progress Report.docx</td>
<td>C:\Users\hdowd\Documents\Progress Report.docx</td>
</tr>
</tbody>
</table>

Note how the directory structure relative to the source location (C:\ in this particular case) is preserved when the files are moved according to the rule.

**Files that Match Multiple File Rules**

If a file is impacted by multiple File Rules, only the first rule (in order of evaluation) is used for the file and the file is only migrated once.
Defining File Rules

File Rules are defined through the Migration Manager user interface by going to Edit | File Rules or by clicking the File Rules button in the toolbar:

Figure 8: The File Rules toolbar button

The main File Rules dialog displays the currently defined File Rules:

There are 4 different operations that can be performed in this dialog:

- Add a new File Rule
- Edit an existing File Rule
- Delete a File Rule
- Change the priority of a File Rule
Adding New File Rules

The steps below describe how to add a file rule to include all *.wpd and *.wpt files from anywhere on the user’s system:

- Click the “Add Rule” button in the File Rules dialog
- Enter the definition for the rule in the File Rule dialog:
  - Click OK to add the new rule to the list of rules
  - Click OK again to save the list of File Rules
Editing File Rules

Follow these steps to modify the rule created in the previous section so that it only includes files that have been modified since June 15, 2011 and that are smaller than 100 MB:

- Select the rule in the File Rules dialog and click the Edit Rule button
- Check the “Limit by date” checkbox and enter 6/15/2011 in the date field
- Check the “Limit by file size” check box, enter 100 as the size and select MB as the size unit in the drop-down
Click OK to save the changes and return to the File Rules dialog.

Deleting File Rules

To delete an existing File Rule, follow these steps:

- Select the rule in the File Rules dialog and click the Delete Rule button.
- Click OK in the File Rules dialog to save the change to the File Rules.

Changing File Rule Evaluation Order

As discussed in File Rule Evaluation Order on page 58, the order in which File Rules are defined determines the effect the rules have on what files get extracted. To change the order of the rules, follow these steps:

- Select the rule that should be moved in the File Rules dialog.
- Click the “up” button to move the selected rule up in the order of evaluation and the “down” button to move it down in the order of evaluation.
**File Rule Editor**

This section describes the individual fields in the File Rule editor.

**Include or Exclude**

The first selection in the dialog is to determine if the rule includes or excludes files:

![File Rule Editor](image)

**Source Path**

This field defines the location to which the rule applies. See How File Rules Work on page 57 for more information on how locations and file types can be defined.

![File Rule Editor](image)

The “Include Subdirectories” check box determines whether the rule applies to any subdirectories below the Source Path. For instance, specifying a location like C:\*. doc without including subdirectories will only match *. doc files in the root of the C drive. When subdirectories are included, the rule matches *. doc files anywhere on the C drive.
Multiple file types can be specified by separating each file type with a semicolon (‘;’) like this: *doc;*.docx;*.dot;*.dotx.

When using the “Browse…” button to select a source folder, Migration Manager will offer to use the path token that best matches the selected folder (if any). Using path tokens make file rules more generically useful for different users and operating systems. See page 59 for more information about path tokens.

Date Criteria
A File Rule can limit extraction by the last modified date of a file.

The options for the date comparison are *On or before* the specified date or *On or after* the specified date.
Size Criteria

A File Rule can use the size of the file to evaluate the rule. Note that the size unit can be defined in KB, MB or GB.

Similar to the date comparison, the options are Less than or equal to or Greater than or equal to.

Remapping Files

As mentioned in Moving Files on the Target System on page 63, File Rules can move files when they are injected on the target system:

To enable this, check the “Remap destination” checkbox and specify the desired destination path and optionally choose to preserve the original subdirectory structure.
<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>The token <code>%FIXEDDISKS%</code> cannot be used in the destination path field. All other tokens described on page 59 can be used.</td>
</tr>
</tbody>
</table>
11. Registry Rules

Overview

Registry Rules provide administrators with an easy mechanism for specifying registry information to include in a migration. Registry Rules are most commonly used to support applications that store their settings in the registry.

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Caution should be exercised when using Registry Rules to migrate user settings. A good working understanding of the Windows Registry is required. Indiscriminately migrating registry data can result in an unstable environment on the target system.</td>
</tr>
<tr>
<td>Minimize the scope of Registry Rules to reduce the possibility of problems when injecting data extracted by the defined rules.</td>
</tr>
</tbody>
</table>

See Chapter 13 for an example using File and Registry Rules to migrate application settings.

How Registry Rules Work

Registry Rules are far simpler than File Rules (described in Chapter 10) as there are no conditions associated with these rules. As long as a registry key or value is defined and exists on the source system, the corresponding data will be included in the migration.

Scope

Each defined rule has a scope:

<table>
<thead>
<tr>
<th>Scope Type</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Branch</td>
<td>Migrates the registry key, all values and sub-keys below the key.</td>
</tr>
<tr>
<td>Key</td>
<td>Migrates the key and the values defined for that key, but no sub-keys</td>
</tr>
<tr>
<td>Value</td>
<td>Migrates the specific registry value only</td>
</tr>
</tbody>
</table>

Path Translation

To ensure that migrated registry data is correct on the target system, string-based registry values that correspond to a file path that Migration Manager is translating as part of the migration are also path translated.

For example, the file path `C:\Documents and Settings\hdao\My Documents\Project Data\Overview.rtf` stored in a registry value would be translated to `C:\Users\hdao\Documents\Project Data\Overview.rtf` in a typical Windows XP to Windows 7 migration.

This translation is performed automatically and is very useful for registry values that contain paths to configuration files, document locations or most recently used files.
Defining Registry Rules

Registry Rules are defined through the Migration Manager user interface by going to Edit | Registry Rules or by clicking the Registry Rules button in the toolbar:

![The registry rules toolbar button.](image)

Adding a Registry Rule

The easiest way to add a registry key or value to the list of rules is to expand the registry tree on the left and then drag-and-drop the key or value to the list:

![Registry Rules](image)

If you can’t find the registry key or value in the tree, you can type its path in the Key field (and optionally the name of the value in the Value field).
You can change the scope of the rule by clicking in the Type column:

![Image of Registry Rules dialog box with a note about changing the scope of the rule.]

**Note**

If you define a registry rule for a registry key and set the type to “Value” only the default value for the registry key is migrated, none of the other values or sub-keys are included.

**Deleting a Registry Rule**

Select the rule that should be deleted in the list and click the “Delete rule” button:

![Image of Registry Rules dialog box with the option to delete a rule.]
12. Importing and Exporting Rules

Overview

Migration Manager supports exporting and importing defined File and Registry Rules. A library of rules thus can be created and combined as needed depending on the particular needs of a migration.

Exporting Rules

File and Registry rules (see Chapters 10 and 11 for more information on how to create File and Registry rules) can be exported by clicking Edit | Export File and Registry Rules from the Migration Manager main menu.

This presents a standard Save File dialog where the location and name of the rule file can be specified.

Importing Rules

Importing rules is similar to exporting rules, click Edit | Import File and Registry Rules from the Migration Manager main menu.

This displays a dialog where the name of the rule file to import can be specified:

Select “Append to existing file and registry rules” to add imported rules to the current set of rules (if any). Otherwise, select “Replace existing file and registry rules” to replace current rules.
13. Using File and Registry Rules to Migrate Applications

Overview

Migration Manager can be configured to migrate settings and data for any application beyond the list explicitly supported in the “Select for Extraction” screen.

Configuring migration requires research to identify desired settings and files associated with an application. This Chapter illustrates how to conduct discovery of registry settings and files to be migrated for WordPad and set these up in the Edit | File Rules and Edit | Registry Rules features of Migration Manager.

Researching Required Rules

Determining File Types to Migrate

To find all file types that can be opened with WordPad, follow these steps:

1. Launch WordPad and click File | Open.
2. Click the dropdown “All WordPad Documents” and discover the supported file extensions: *.rtf, *.docx, *.odt, and *.txt.
3. Record this information for use in configuring File Rules.

Determining Registry Values to Migrate

To migrate new settings, determine the registry keys the application is using for these. Microsoft provides a tool called Process Monitor that can help with this. Process Monitor is free and can be downloaded from http://technet.microsoft.com/en-us/sysinternals/bb896645.aspx.

Follow these steps to determine what registry values WordPad uses:

1. Launch Process Monitor.
2. Launch the application, in this case WordPad.
4. In the first drop down, select Process Name.
5. In the third drop down, select the application’s .exe (wordpad.exe in this case).
6. Click Add, then OK.
7. Switch back to the application and change the settings that are relevant for this example, so that those changes are captured by Process Monitor. For this example the Measurement units setting and the recently used files need to be monitored. Change the Measurement units from Inches to Points. Open and close a few files to change this list of recently used files.

9. Switch to Process Monitor to see the activity from WordPad.
10. Since the setting Measurement units was changed, search the Process Monitor window for “unit” and look for operations that modify the registry (e.g. RegSetValue or RegCreateKey), in this case one entry is found:
HKCU\Software\Microsoft\Windows\CurrentVersion\Applets\Wordpad\Options
\Units

11. To find the Recently used files settings, search the Process Monitor window for “recent” and look for a key with several values that store the filenames that opened and closed in step 7:
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Applets\Wordpad\Recent File List

Defining the Required Rules

File Rules Required for WordPad

Start by adding the File Rules required to migrate the file types supported by WordPad:

1. In the Migration Manager menu bar, click Edit | File Rules.
2. Return to the list of file extensions collected determined through the research described on page 77.
3. Click Add Rule and add a rule that matches the supported file types.
Note

%%FIXEDDISKS%% is one of several tokens supported by File Rules and in this case ensures that files will be included from all local drives on the source system (e.g. C: and E:).

See the description of the supported tokens on page 59 for more information.

4. Next, add the required Registry Rules by clicking Edit | Registry Rules in the main Migration Manager window.
5. Use the registry tree to find the registry keys and values identified in the research on page 77:

![Registry Rules Window]

6. Finally, click File | Save to save the new rules to the configuration file (note that you can also export these rules as described in Chapter 12)
To use the new rules in an extraction, make sure that File and Registry Rules are selected in the “Select for Extraction” screen:

<table>
<thead>
<tr>
<th>User(s) to Extract</th>
<th>Select for Extraction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applications</td>
<td></td>
</tr>
<tr>
<td>Adobe Acrobat</td>
<td></td>
</tr>
<tr>
<td>Google Chrome</td>
<td></td>
</tr>
<tr>
<td>Lotus Notes</td>
<td></td>
</tr>
<tr>
<td>Microsoft Internet Explorer</td>
<td></td>
</tr>
<tr>
<td>Microsoft Office</td>
<td></td>
</tr>
<tr>
<td>Mozilla Firefox</td>
<td></td>
</tr>
<tr>
<td>QuickBooks</td>
<td></td>
</tr>
<tr>
<td>Data Transport</td>
<td>File Rules</td>
</tr>
<tr>
<td></td>
<td>Registry Rules</td>
</tr>
<tr>
<td>Media Files</td>
<td></td>
</tr>
<tr>
<td>iTunes Files</td>
<td></td>
</tr>
<tr>
<td>Windows Media Player Files</td>
<td></td>
</tr>
<tr>
<td>Windows Options</td>
<td>Control Panel</td>
</tr>
</tbody>
</table>
14. HTTP Support

Overview

By default Migration Manager uses a file share-based data store to store user state data. In some scenarios, use of a file share isn’t practical (such as when executing Migration Manager through a client-side agent running as Local System). In these cases the HTTP support in Migration Manager enables the use of a WebDAV-based data store.

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Migration Manager does not currently support HTTP operations from offline Windows machines.</td>
</tr>
</tbody>
</table>

SSL

Migration Manager supports both HTTP and HTTPS. Using HTTP requires no special configuration. HTTPS requires the use of an SSL certificate which is typically generated by a certificate server.

If a certificate server is not available, a self-signed certificate can be used as long as Migration Manager is configured appropriately. See HTTP Options on page 37 for more information on configuring Migration Manager to work with self-signed or untrusted SSL certificates.

Generating a Self-Signed Certificate Using IIS7

Follow the steps in this article to generate a self-signed certificate using the IIS7 Management Console: http://technet.microsoft.com/en-us/library/cc972767(WS.10).aspx

Authentication

Some common web servers (e.g. IIS6 and Apache 2.2) allow anonymous users to add, update and download files using WebDAV. Others, most notably IIS7 don’t allow anonymous WebDAV access which means that authentication must be configured.

Digest Authentication

Migration Manager supports digest authentication for the scenarios where HTTP authentication is required. Instructions for how to configure Migration Manager for digest authentication can be found on page 37.

Configuring IIS7 for Use with Migration Manager

Several configuration steps are required to use Migration Manager with IIS7 together. Much of this information can be found on the IIS Learning Center site.
Useful Links

- IIS7 WebDAV module: [http://www.iis.net/download/WebDAV](http://www.iis.net/download/WebDAV)

Configuration Notes

It’s recommended that you configure the connection time-out for the site hosting the data store to be at least 10 minutes as you may otherwise experience time-out errors while uploading files during an extraction.

This setting can be accessed by selecting the site node in the IIS Manager, clicking “Advanced Settings” and then changing the “Connection Time-Out (seconds)” value located in Advanced Settings | Behavior | Connection Limits.

Using the HTTP Support

The HTTP support in Migration Manager is available for all 4 main operations in Migration Manager. For extractions, injections and backup HTTP support is only available for command-line operations. See the “Automating Migration Manager” guide for information on the /HTTP command-line parameter.

When restoring files, HTTP support is available through the user interface. See Chapter 9 for more information.
15. Log Files

Overview
Migration Manager generates two types of log files:

- An Operation Log file generated for each operation (extraction, injection, backup and file restore) performed by Migration Manager.
- A session log file containing detailed information on the actions performed by Migration Manager while it’s running.

Log Levels
Migration Manager can be configured to use various log levels to determine the amount of information written to the log files. This is set in the Preferences dialog (see Chapter 5).

Operation Log File
The Operation Log file is stored with the related user state data for ease of access.

Naming Conventions
An Operation Log file is named using this pattern:
<computer name>_<month>_day_<year>_hour_<minute>_second_<am/pm>_operation.log

The operations are named as follows:
- Ext Extraction
- Inj Injection
- Bak Backup
- Res Restore

For instance, an extraction performed on a computer with the name MAINWIN7 on August 11, 2010 at 1:52PM would be named MAINWIN7_8_11_2010_1_52_00_PM_Ext.log.
Log File Contents

The contents of the log file depend on the operation performed, but typically the following sections are included:

<table>
<thead>
<tr>
<th>Section</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>Header</td>
<td>The command-line used for Migration Manager and the version of Migration Manager used.</td>
</tr>
<tr>
<td>User information</td>
<td>The name of the user account used to run Migration Manager and the users whose user state data were included.</td>
</tr>
<tr>
<td>Time</td>
<td>The time the operation started, completed and the time it took the operation to complete.</td>
</tr>
<tr>
<td>Operating System</td>
<td>The version of the operating system used.</td>
</tr>
<tr>
<td>Local Fixed Drives</td>
<td>The list of local drives on the system.</td>
</tr>
<tr>
<td>Configuration</td>
<td>The fully qualified path of the configuration file.</td>
</tr>
<tr>
<td>Data Store</td>
<td>The location of the data store used for the user state data.</td>
</tr>
<tr>
<td>Log Level</td>
<td>The log level used for the log file.</td>
</tr>
<tr>
<td>Content</td>
<td>The content selected for the operation.</td>
</tr>
<tr>
<td>Policies</td>
<td>The policies active for the operation.</td>
</tr>
<tr>
<td>File Rules</td>
<td>The file rules active for the operation.</td>
</tr>
<tr>
<td>File Section</td>
<td>All files and directories included in the operation.</td>
</tr>
<tr>
<td>Log Detail</td>
<td>The detailed logging information for each user involved in the operation.</td>
</tr>
<tr>
<td>Content Version</td>
<td>The version information for all binaries used by Migration Manager.</td>
</tr>
<tr>
<td>Installed Applications</td>
<td>The applications installed on the system.</td>
</tr>
</tbody>
</table>

The last entry in the Operation Log file has the format:

Engine Result: <exit code>

A result of 0 means success. This can be used by tools such as Microsoft System Center Operation Manager to determine the status of all Migration Manager operations.
Session Log File

The session log file is primarily intended for troubleshooting purposes. Provide this file, along with applicable Operation Log files, if you need to contact Tranxition Support.

Location

Unlike the Operation Log files, the session log files are stored locally on each system on which Migration Manager is run. The log files are stored in the standard “local program data” Windows directory (typically C:\ProgramData on Windows Vista and later) in the Tranxition\MigrationManager directory.

Session log files are named using this format:
SE-<year>-<month>-<date>-<hour>-<minute>.log

For instance, for a Migration Manager session started at 8:30am on Monday, August 16 2010, the Session Log file would be named SE-2010-08-16-08-30.log

Contents

The contents of the session log file are time-stamped entries with the format:

[<time stamp>] <log level> <thread id> <message>

Different messages in the log file have different log levels. A “lower” log level (e.g. Error) logs fewer messages. A “higher” log level (e.g. Trace) causes many more messages to be logged.

Sending Log Files to Support

If you ever need to contact Support, it’s almost certain that the relevant Session and Operation log files will be requested as this greatly speeds up resolving the issue. To make this easier, there is a feature in Migration Manager that assists with this task. In the Migration Manager main window, click Help | Package Log Files for Support to display the packaging dialog:
Note

You must do this on the computer where the issue manifests itself in order for Migration Manager to collect the right log files.

Package Options

By default both Operation and Session log files are collected and this is almost always the right thing to do. You can also choose to either collect the log files for a set number of days (the 3 past days by default) or collect all log files.

Finally you can also choose a location for the package. The default is to place the package (which is a regular Zip file) on your desktop to make it easy to find when e-mailing it to support.
16. Migration Manager Maintenance

Overview
Migration Manager does not need a lot of ongoing maintenance, but this Chapter describes some areas that may need attention on a regular basis.

Deleting User State Data

File Share-Based Data Stores
While it’s possible to directly delete user state data directories stored on the file share, Migration Manager provides a user interface for deleting existing user state data based on the name of the system the information was extracted for, when it was extracted and so on.

Go to Edit | Delete Personalities in the Migration Manager main menu which displays this dialog:

Select the user state data that should be deleted (use CTRL+click to select multiple items) and click the Delete button.

HTTP-Based Data Stores
Migration Manager does not provide a user interface for deleting user state data stored on a WebDAV server.

The alternate approach is to instead go to the URL used for Migration Manager using a WebDAV client and delete the files. Each file associated with a particular set of user state data is prefixed with the unique name specified when the original extraction was performed (see the “Automating Migration Manager” guide for more information) which can be used to identify the files to delete.
Deleting Session Log Files

As described in Chapter 15, Migration Manager creates a session log file every time it is run regardless of whether a migration operation is performed. If Migration Manager is run frequently on a system it may be necessary to clean up old session log files on a regular basis.
17. Support Notes

Supported Operating Systems

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Minimum</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows XP (SP3)</td>
<td>Pentium CPU, 128 MB RAM</td>
<td>Pentium CPU, 256 MB RAM</td>
</tr>
<tr>
<td>Windows XP x64</td>
<td>x64 capable CPU, 512 MB RAM</td>
<td>x64 capable CPU, 1GB RAM</td>
</tr>
<tr>
<td>Windows Vista</td>
<td>1 GHz x86 or x64 CPU, 1GB RAM</td>
<td>1 GHz x86 or x64 CPU, 2GB RAM</td>
</tr>
<tr>
<td>Windows 7</td>
<td>1 GHz x86 CPU, 1GB RAM</td>
<td>1 GHz x86 CPU, 2GB RAM</td>
</tr>
<tr>
<td>Windows 7 x64</td>
<td>1 GHz x64 CPU, 2GB RAM</td>
<td>1 GHz x64 CPU, 4GB RAM</td>
</tr>
<tr>
<td>Windows 8</td>
<td>1 GHz x86 CPU, 1GB RAM</td>
<td>1 GHz x86 CPU, 2GB RAM</td>
</tr>
<tr>
<td>Windows 8 x64</td>
<td>1 GHz x64 CPU, 2GB RAM</td>
<td>1 GHz x64 CPU, 4GB RAM</td>
</tr>
<tr>
<td>Windows 10</td>
<td>1 GHz x64 CPU, 1GB RAM</td>
<td>1 GHz x64 CPU, 2GB RAM</td>
</tr>
</tbody>
</table>

Supported ITSM Environments and Appliances

Migration Manager can extract offline user states when run from the following Windows PE versions. Please note Windows PE 32 and 64 bit versions are supported and do not need to match the offline Windows architecture. The offline Windows system may be any Operating System supported by Migration Manager. Injection to offline Windows systems is not currently supported.

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows PE</td>
<td>5, 10</td>
</tr>
</tbody>
</table>

Supported Migration Paths

Operating Systems

You can migrate user state data between the following combinations of Operating Systems. Please note that for all versions both x86 and x64 are supported.

<table>
<thead>
<tr>
<th>Target Source</th>
<th>Windows XP</th>
<th>Windows Vista</th>
<th>Windows 7</th>
<th>Windows 8</th>
<th>Windows 10</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows XP</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Windows Vista</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Windows 7</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Windows 8</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Windows 10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>
## Supported Content

Migration Manager provides rich content that migrates settings between different application versions as well as between the same version on different systems. Migration Manager can also be customized to support other applications (see Chapter 13).

### Microsoft Office

<table>
<thead>
<tr>
<th>Application</th>
<th>Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Groove/Sharepoint Workspace</td>
<td>2007, 2010</td>
</tr>
</tbody>
</table>

### Note

See page 93 for more information on the Microsoft Office content provided in Migration Manager.
Other Supported Applications

<table>
<thead>
<tr>
<th>Application</th>
<th>Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adobe Acrobat</td>
<td>7.x, 8.x, 9.x, 10.x, 11.x, DC</td>
</tr>
<tr>
<td>Adobe Acrobat Reader</td>
<td>7.x, 8.x, 9.x, 10.x, 11.x, DC</td>
</tr>
<tr>
<td>Lotus Notes</td>
<td>7.x, 8.x</td>
</tr>
<tr>
<td>Internet Explorer</td>
<td>6.x, 7.x, 8.x, 9.x, 10.x, 11.x</td>
</tr>
<tr>
<td>Firefox</td>
<td>3.x, 4.x, version 5 and later</td>
</tr>
<tr>
<td>Google Chrome</td>
<td>Version 13.x and later (Given the frequent release schedule and automatic required updates that Google has adopted in Chrome, testing has been performed using the versions of Google Chrome available when this version of Migration Manager was released.)</td>
</tr>
</tbody>
</table>

Windows Options

Persistent settings and files are preserved for:

- Control Panel
- Desktop Shortcuts
- Network Connections (VPN and similar)
- Windows Explorer
- Local Printer Logging
- Mapped Network Drives
- Network and Shared Printer Connections
- Taskbar and Quick Launch Bar

Note

Migration Manager supports the Taskbar and Quick Launch Bar in Windows XP and Windows Vista. When migrating to Windows 7 or later from XP or Vista, the Quick Launch Bar will not be enabled in the new operating system.

Migration Manager will migrate pinned Start Menu items in Windows 7 and will migrate pinned Taskbar items in Windows 7 and later. It will only validate the shortcuts for the pinned Taskbar items and remove broken links for the current logged-in user.

Note

For printers, Migration Manager does not migrate any printer drivers. These need to be installed separately.
User Documents and Media Files

Content is provided to explicitly migrate files located in the following user profile folders:

- Contacts
- Desktop
- My Documents
- My Pictures
- My Music
- My Videos

**Note**

Migration Manager will place files in the correct location regardless of the actual name and locations of profile folders on the source and target systems.

Windows Explorer

The following user-specific features are preserved:

- Favorites
- Folder Options
- Libraries
- Searches

Control Panel Settings

Persistent settings and files are preserved for:

- Accessibility Options
- Display
- Internet Options
- Keyboard
- Mouse Settings
- Power Management
- Regional Settings
- Time Zones

**Note**

Migration Manager does not migrate hardware-dependent settings. This is by design to eliminate the risk of incorrect settings being set on the target system.

Microsoft Office Content Notes

Spelling and Grammar Settings

In Office 2003, each application has individual settings for spelling and grammar while Office 2007 and newer have shared settings for all applications. When migrating from Office 2003, Migration Manager uses the Word 2003 spelling and grammar settings as the settings to migrate.
InfoPath

When migrating InfoPath, all .xml files located on the source system will be included. Many applications install XML files for purposes completely unrelated to InfoPath and it may be necessary to use File Rules to exclude XML files from specific locations on the source system.

Outlook

Services on the target system must be the same as the services on the source system. For example, if the source machine has Outlook set to Corporate Workgroup, then Outlook on the target machine must also be set to Corporate Workgroup.

If .pst files are selected for migration, but the Outlook Mail Clients and Associated Files content is not exclusively .pst files, the migrated files will be included but will not be made active in the Outlook configuration on the target system.

When migrating Outlook profiles with IMAP accounts, a message stating “IMAP Search Folders based on criteria of message size, recipient, or sender do not work on messages already downloaded. To fix this, remove your IMAP email account, and then add it again.” may be displayed when Outlook is launched. This message can be ignored.
18. Copyright and Patent Information


All Rights Reserved.

Protected by US Patent 8,775,788 and European Patents 1173809.

The information in this document is subject to change without notice and should not be construed as a commitment by Tranxition Corporation. Tranxition Corporation assumes no responsibility for any errors that might appear in this document.

The software described in this document is furnished under a license and may be used or copied only in accordance with the terms of such license. No responsibility is assumed for the use or reliability of software or equipment that is not supplied by Tranxition Corporation or its affiliated companies.

Restricted Rights: Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013. The Tranxition logo is a trademark of Tranxition Corporation. Microsoft Windows XP, Windows Vista, Windows 7, Windows 8, Windows 10, and Windows PE are registered trademarks of Microsoft Corporation. All other trademarks and registered trademarks are the property of their respective holders.

Tranxition Corporation
516 Se Morrison Street
Suite 242
Portland, OR 97206
503-688-5046
www.tranxition.com