Migration Manager Automation Guide

Version 10.4

Migration Manager
for Windows

Table of Contents

Introduction **6**

Purpose 6

Scope 6

Assumptions 6

Intended Audience 6

Using the Command-Line Interface **7**

Overview 7

Automating Personality Migrations 7

Using Unicode Characters in Batch Files 8

Application Command-Line Parameters **9**

Introduction 9

Basic Command-Line Parameters 9

AUTOBACKUP 9

AUTOEXTRACT 10

AUTOINJECT 10

CONFIG 11

DATASTORE 11

PERSONALITYPATH 12

HARDLINKS 12

EXCLUDEDISKS 13

PASSWORD 13

SOURCE 14

OVERWRITE 14

MOSTRECENT 15

MAPPINGFILE 15

User-Related Command-Line Parameters 16

ALLUSERS 16

DOMAIN 17

EXCLUDEDOMAIN 17

EXCLUDELOCAL 17

EXCLUDENOTLOGGEDIN 18

EXCLUDEUSER 18

INCLUDEUSER 19

INJECTTOLOGGEDINUSER 20

LOCALPROFILE 21

REDIRECTFOLDERS ... 21
ROAMINGPROFILES ... 22
Advanced Command-Line Parameters ... 23
DISPLAYERRORCODE ... 23
ELEVATEDCREDENTIALS ... 23
HIDESTATUS ... 24
IMPORT ... 25
NOCANCEL ... 25
PERSONALITYNAMING ... 25
THROTTLE ... 26
Automation Examples ... 27
Processing Logged On Users ... 28
Description ... 28
Process Examples ... 28
Extract.bat File Example ... 28
Inject.bat File Example ... 29
Processing Not-Logged On Users ... 30
Description ... 30
Process Examples ... 30
Extraction Example (Invoking the Extract.bat file) ... 30
Extract.bat File when user is not logged in ... 30
Injection Example (Invoking the Inject.bat file) ... 31
Inject.bat File Example when user is not logged in ... 31
Processing Multiple Users ... 32
Description ... 32
Process Examples ... 32
Extraction Example (Invoking the Extract.bat file) ... 32
Extract.bat File Example to Extract Multiple Users ... 32
Injection Example (Invoking the Inject.bat file) to Inject Multiple Users ... 33
Inject.bat File Example to Inject Multiple Users ... 33
Moving Users Between Domains ... 34
Description ... 34
Process Examples ... 34
Extraction Example (Invoking the Extract.bat file) ... 34
Extract.bat File Example for Moving Users between Domains ... 35
Injection Example (Invoking the Inject.bat file) ... 35

Inject.bat File Example for Moving Users between Domains 35

Using Passwords in Migrations 36

Description 36

Process Examples 36

Extraction Example (Invoking the Extract.bat file) 36

Extract.bat File Example USING A PASSWORD 36

Injection Example (Invoking the Inject.bat file) Using a Password 37

Inject.bat File Example Using a Password 37

Injection Mapping Files 38

Description 38

Mapping File Structure 38

Creating Mapping Files Using the Injection Mapping Tool 38

Creating a New Mapping File 39

Adding Source Computers to a Mapping File 39

Importing Source and Target Computers 40

Response Files 41

Description 41

Response File Example 41

Example 41

Offline Migrations 42

Introduction 42

Extracting Offline Users 42

Injecting Offline Users 42

Example Command-Line with Offline Users 42

Extraction 42

Injection 42

Using Hardlinks 43

Introduction 43

Extracting Hardlinks 43

Injecting Hardlinks 43

Example Command-Line 43

Extraction 43

Injection 44

Example Command-Line with SCCM/MDT 44

Extraction 44

Injection 44

Migration Manager Exit Codes **45**

Using Migration Manager With a Scheduler **50**

Copyright and Patent Information **52**

Introduction

Purpose

This document describes how Migration Manager can be used in an automated fashion without requiring any user intervention, something that's essential to be able to perform large-scale migrations.

Migration Manager provides a rich set of functionality through command-line parameters that allow you to perform both extractions and injections of user state which makes it possible to incorporate Migration Manager in Operating System Deployment scenarios.

It's possible to use this in MS-DOS-style batch files, NT-style .cmd files, PowerShell scripts or as part of a desktop management suite if you have that deployed in your environment. This document doesn't make any assumptions about your environment other than that you have at least one Windows domain.

This document explains the uses of the various command-line parameters and provides examples of batch files and network login scripts.

Scope

This document applies to functionality within Migration Manager. The batch files use standard MS-DOS commands and the login script examples use standard Windows NT login syntax.

Assumptions

This is a technical discussion and it is presumed that the reader is proficient with standard Windows and networking concepts. It is also assumed that the reader is familiar with and has a working knowledge of Migration Manager. For details on how to use Migration Manager, please see the Migration Manager User's Guide.

Intended Audience

This document is intended for administrative users of Migration Manager and anyone involved with the deployment of the software.

Using the Command-Line Interface

Overview

Migration Manager provides a rich set of command-line parameters that make it possible to fully automate both migrations and ongoing use of Migration Manager. Scenarios where this is useful include:

- Migrating users as part of machine deployment; it’s possible to extract the user state from the user’s current system before starting the OS deployment of the new system and then finish up by injecting the user state as the last step of the OS deployment
- Provide ongoing recovery services by doing an initial extraction and then regular backups of a user’s system. If something goes wrong with the system, it can be reimaged/reinstalled and the backed up user state restored

Automating the use of Migration Manager helps ensure an efficient and repeatable process that allows IT administrators to be more productive.

In a typical networked company environment, it’s most efficient to deploy Migration Manager on a shared server that hosts the application files and typically also the user state data extracted from the user systems (although this information can also be stored elsewhere). This approach is useful as Migration Manager then doesn’t have to be installed on each individual system where it will be used; the application can be run directly from the server.

Configuration settings and the information needed by Migration Manager is also stored centrally on this shared server.

In a highly distributed environment, it’s of course possible to have multiple shared installations of Migration Manager (e.g. one per branch office). Your network configuration will help determine what the best approach is for your environment.

In most cases, one or more scripts are created for each operation so that you don’t have to remember all of the command-line parameters every time you perform an operation with Migration Manager. These scripts can be simple batch files, PowerShell scripts or anything else that can run an application and pass command-line parameters to the application.

These scripts are also useful for integration into OS deployment solutions or desktop management tools from other software publishers.

Automating Personality Migrations

Using command-line parameters, Migration Manager can be set up to automatically extract, inject and backup the user state for the currently logged in user, a user that is not logged in to the computer, or multiple users.

The personality is extracted or backed up on the source PC and automatically injected on the target PC. The next section details all supported command-line switches followed by batch file examples that will assist you in the development of an automated migration process.

Note

To extract, inject or backup a personality for a user or users that are not currently logged in to the machine, the user that is performing the extraction or injection must have Local Administrator Rights. Migration Manager also requires UAC elevation on Windows if enabled.

Using Unicode Characters in Batch Files

Migration Manager is typically automated using batch files. If there is a need to use Unicode characters in your batch files, there are a few steps to follow in order for Windows to correctly process the batch files: The batch file must be saved using the Unicode UTF-8 encoding without a Byte Order Marker (BOM) The batch file must contain the code page directive to enable Unicode (chcp 65001)

Example Batch File

```
@echo off
chcp 65001
echo Extracting data...
start /w \\MyServer\MigrationManager\MigrationManager.EXE /autoextract /allusers /DATASTORE \\MyServer\MigrationManager\질겻쪉걝앐숱꼽
IF ERRORLEVEL 1 (echo Extraction failed) ELSE (echo Extraction succeeded)
```

Application Command-Line Parameters

Introduction

This chapter describes the command-line parameters supported by Migration Manager. Using these command-line parameters it's possible to fully automate Migration Manager. Do note, however, that an administrator will need to run Migration Manager at least once in order to define the configuration that should be used by Migration Manager.

You need at least one configuration file, but it's also possible to have multiple configuration files to accommodate different needs for different sets of users, see the `CONFIG` parameter for information on how to define which configuration file to use for an operation.

When running Migration Manager from the command-line, it's highly recommended that you use `start /w` to run the application since it ensures Windows will wait for Migration Manager to complete the operation before executing the next command.

Basic Command-Line Parameters

The basic command-line parameters are used to control basic Migration Manager operations and include:

- AutoBackup – perform user state backup
- AutoExtract – extract user state
- AutoInject – inject user state
- Config – specify the configuration file to use for an operation
- Datastore – specify where user state data is located
- PersonalityPath – specify an explicit path for where personality is stored
- HardLinks - store data locally with hardlinks (NTFS)
- Excludedisks – exclude disks when injecting data
- Password – specify a password for AES256 encryption during an operation
- Source – specify the name of the computer the data was extracted from, or MAC address when data was extracted from offline Windows
- Overwrite - will overwrite an existing personality in the datastore during extraction instead of the creating an additional personality if one already exists for the specified personality name (typically the source computer name)
- MostRecent - If more than one matching personality exists during injection, the most recent personality will be used instead of returning an exit code
- MappingFile – define the source computer for automated zero-touch migrations

AUTOBACKUP

Syntax: /AUTOBACKUP

Extraction use: Backs up changes made to user state after an initial extraction has been performed for the user in question (note that a full extraction must be performed for a user before a backup can be performed).

If the personality to backup isn't specified on the command-line, Migration Manager scans the user state data store location for an existing extraction for a computer with the same name where the backup is taking place.

If no matching user state can be found or if more than one match is found, Migration Manager exits with an appropriate exit code.

Note that you can only perform a backup on the same system where the original extraction took place. Backup is not supported from offline Windows systems.

Injection use: N/A.

Must be used with: N/A.
Cannot be used with: `AUTOEXTRACT`, `AUTOINJECT`.

Example: `START /w MigrationManager.EXE /autobackup`

AUTOEXTRACT

Syntax: `/AUTOEXTRACT`

Extraction use: The `/AUTOEXTRACT` command, if used without another supported extraction command switch will automatically perform a personality extraction of the user that is currently logged on to the computer.

Note that the default Migration Manager configuration will be used if a configuration file is not specified in the command-line (using the `CONFIG` command).

Administrators will have to configure Migration Manager with the desired settings, by selecting content and preferences within the Migration Manager User Interface and saving the configuration. See the "Migration Manager User's Guide" section on "Configuring Migration Manager" for details on creating and saving the configuration. To extract users other than the default currently logged in user, refer to User-Related Command-Line Parameters.

Injection use: N/A.

Must be used with: Can be used by itself, but typically at least the `CONFIG` switch is used as well.

Cannot be used with: `AUTOINJECT`, `AUTOBACKUP`, `SOURCE`.

Example: `START /w MigrationManager.EXE /autoextract`

AUTOINJECT

Syntax: `/AUTOINJECT`

Extraction use: N/A.

Injection use: If this command is used without another supported injection command, the switch will automatically perform a personality injection for the user that is currently logged on to the computer.

Migration Manager searches the default data store for personalities with a user name that matches the user name of the currently logged on user. If only one matching personality containing that username is found the personality for that user is injected.

If more than one matching personality is found, or no matching personalities are found, Migration Manager will terminate and return an exit code.

Injection to offline Windows is not currently supported.

Must be used with: Can be used by itself, but typically at least the CONFIG and SOURCE switches are used as well.

Cannot be used with: AUTOBACKUP, AUTOEXTRACT.

Example: `START /w MigrationManager.EXE /autoinject /source MYCOMPUTER /allusers`

CONFIG

Syntax: `/CONFIG <fully qualified path to configuration file>`

Extraction use: Specifies the configuration file to use when performing an automatic extraction or injection.

If the specified path to the configuration file is invalid Migration Manager will terminate and return an exit code.

Injection use: Loading a configuration file during injection does NOT specify what content or specific application/windows settings are to be injected. All items that are extracted and present in the personality will be injected.

Must be used with: Can be used by itself, but typically used with AUTOBACKUP, AUTOEXTRACT or AUTOINJECT.

Cannot be used with: N/A. **Example:** `START /w MigrationManager.EXE /autoextract /config "\\MyServer\MigrationManager\configuration.xml"`

DATASTORE

Syntax: `/DATASTORE <fully qualified path to data store>`

Extraction use: Specifies the location of where user state data from the extraction should be stored. This command overrides the data store information in the configuration file.

If the directory specified in the path doesn't exist it will be created. If the creation fails, Migration Manager will terminate and return an appropriate exit code.

Note: By design, Migration Manager does not extract any files from any folder below the specified data store location. Please take this into account if you place the data store on a local drive.

Injection use: Specifies the location where user state data can be found. This command overrides the data store information in the configuration file.

If the directory specified in the path doesn't exist, Migration Manager will terminate with an appropriate exit code.

Must be used with: AUTOBACKUP, AUTOEXTRACT or AUTOINJECT.

Cannot be used with: PERSONALITYPATH.

Example: `START /w MigrationManager.EXE /autoextract /datastore \\MyServer\MigrationManager\datastore`

PERSONALITYPATH

Syntax: `/PERSONALITYPATH <fully qualified path to personality location>`

Extraction use: Specifies the fully qualified path of the directory where the extracted user state data should be stored. Unlike the DATASTORE parameter which defines the path of a directory where a unique directory for the user state data should be created, this parameter defines the complete path for the user state data.

If the directory specified in the path doesn't exist it will be created. If the creation fails, Migration Manager will terminate and return an appropriate exit code.

If the specified directory already contains user state data, Migration Manager will terminate and return an appropriate exit code.

Injection use: Specifies the fully qualified path of the directory where user state data to inject is located.

If the directory specified in the path doesn't exist or doesn't contain user state data, Migration Manager will terminate with an appropriate exit code.

Must be used with: AUTOBACKUP, AUTOEXTRACT or AUTOINJECT.

Cannot be used with: DATASTORE, SOURCE.

Example: `START /w MigrationManager.EXE /autoextract /personalitypath \\MyServer\MigrationManager\datastore\%USERNAME%`

Note

This parameter is for advanced scenarios only and should only be used when you need complete control over the entire directory path of where user state data is located for a particular user or system.

HARDLINKS

Syntax: `/HARDLINKS`

Extraction use: Store data files as hardlinks on local NTFS volumes, for use during in-place operating system refreshes. It is recommended to be used with `PERSONALITYPATH`. Migration Manager does not protect the data store location during operating system reimaging.

Note

The specified location to store the personality and data file hardlinks must a local volume and be protected during an operating system reimage. If using SCCM or MDT, this can be done by setting the Task Sequence Variable `OSDStateStorePath`, and using this variable with the `PersonalityPath` command line.

Injection use: The personality storage type is determined automatically on injection.

Must be used with: AUTOEXTRACT.

Cannot be used with: AUTOBACKUP or PASSWORD.

Example: `START /w MigrationManager.EXE /autoextract /personalitypath C:\_Data /hardlinks`

```
START /w MigrationManager.EXE /autoextract /personalitypath
%OSDStateStorePath% /hardlinks
```

For more information see Using Hardlinks.

EXCLUDEDISKS

Syntax: `/EXCLUDEDISKS <drive letter>[;<drive letter>]`

Extraction use: N/A.

Injection use: Specifies drive letters that Migration Manager shouldn't inject data to. Files originally extracted from the designated drives will instead be placed in the directory `C:\MIGRATED_<drive letter>_DRIVE`.
In the example below, files originally extracted from the E drive would be placed in the directory `C:\MIGRATED_E_DRIVE` on injection.

Must be used with: AUTOINJECT.

Cannot be used with: AUTOBACKUP, AUTOEXTRACT.

Example: `START /w MigrationManager.EXE /autoinject /EXCLUDEDISKS D;E`

PASSWORD

Syntax: `/PASSWORD <password>`

Extraction use: Assigns a password with AES256 encryption to the extracted user state data during extraction. This password must be specified for any subsequent backup or injection.

The specified password must be 7 to 15 characters in length and is case sensitive.

Injection use: When used for injection and the password is either missing or incorrect Migration Manager will terminate and return an appropriate exit code.

Injections will only occur if the specified password matches the password defined at the time of the original extraction.

Must be used with: AUTOBACKUP, AUTOEXTRACT or AUTOINJECT.

Cannot be used with: HARDLINKS.

Example: `START /w MigrationManager.EXE /autoextract /PASSWORD password`

For more information see Using Passwords in Migrations.

SOURCE

Syntax: `/SOURCE <computer name | MAC address from offline Windows or :MACID for MAC address of current machine>`

Extraction use: N/A.

Injection use: Specifies the name of the computer associated with the extracted user state data. If the extracted user state is from an offline Windows system, the MAC address is used instead of the computer name.

This command is typically used in combination with the ALLUSERS command-line switch and only on Injection. When used in conjunction with the ALLUSERS switch, all the users associated with the personality that matches the specified computer name following the SOURCE command will automatically inject.

If there are no matching personalities or if there is more than one matching personality then Migration Manager will by default terminate and return an appropriate exit code. When there are multiple matching personalities, MOSTRECENT can be used to inject the most recent matching personality.

Note that the computer name is defined as just the unique computer name (i.e. MYCOMPUTER as opposed to a fully qualified DNS name like MYCOMPUTER.MYDOMAIN.LOCAL).

Must be used with: AUTOINJECT.

Cannot be used with: AUTOBACKUP, AUTOEXTRACT.

Example: `START /w MigrationManager.EXE /autoinject /SOURCE MYCOMPUTER /ALLUSERS`

OVERWRITE

Syntax: `/OVERWRITE`

Extraction use: Overwrites an existing personality folder in the datastore during extraction. The default personality folder name create by Migration Manager uses the source computername. If multiple extractions are performed from the same source computer, multiple folders will be created using that computername. Using /OVERWRITE will instead overwrite the existing computername folder.

Note

The personality will be overwritten regardless if the previous extraction included the same users.

Injection use: N/A.

Must be used with: AUTOEXTRACT.

Cannot be used with: AUTOBACKUP, AUTOINJECT.

Example: `START /w MigrationManager.EXE /autoextract /ALLUSERS /OVERWRITE`

MOSTRECENT

Syntax: `/MOSTRECENT`

Extraction use: N/A.

Injection use: Specifies injecting the most recent matching personality (as determined by `autoinject`, `includeuser`, and `source`) when multiple matching personalities exist. The default behavior without `mostrecent` is for Migration manager to terminate and return an exit code that multiple matching personalities exist.

Must be used with: AUTOINJECT.

Cannot be used with: AUTOBACKUP, AUTOEXTRACT.

Example:

```
START /w MigrationManager.EXE /autoinject /SOURCE MYCOMPUTER
/ALLUSERS /MOSTRECENT
```

MAPPINGFILE

Syntax: `/MAPPINGFILE <mapping file path>`

Extraction use: N/A.

Injection use: Specifies the path of a mapping file that defines the mappings between source and target computers to enable fully automatic, zero-touch, migrations.

This command is typically used in combination with the ALLUSERS command-line switch and only on Injection. When used in conjunction with the ALLUSERS switch, all the users associated with the personality that matches the source computer defined in the mapping file will automatically inject.

If there are no matching personalities or if there is more than one matching personality then Migration Manager will terminate and return an appropriate exit code.

Must be used with: AUTOINJECT.

Cannot be used with: AUTOBACKUP, AUTOEXTRACT, SOURCE.

Example: `START /w MigrationManager.EXE /autoinject /mappingfile mappings.m7map /ALLUSERS`

Note

See Injection Mapping Files for more information on how to create Mapping Files.

User-Related Command-Line Parameters

The user-related command-line parameters are used to define which users to include or exclude for an operation:

- AllUsers – include all users in the operation
- Domain – map users from one domain to another
- ExcludeDomain – exclude all users from a domain
- ExcludeLocal – exclude all local users
- ExcludeNotLoggedIn - exclude all users that have not logged in with specified number of days
- ExcludeUser – exclude a specific user
- IncludeUser – include a specific user
- InjectToLoggedInUser – inject user state to the currently logged on user
- LocalProfile – convert roaming profiles to local profiles
- RedirectFolders – control the root path used for folder redirection during injection
- RoamingProfiles – control the root path used for roaming profiles during injection

ALLUSERS

Syntax: `/ALLUSERS`

Extraction use: Extracts all existing user profiles on the computer.

It is strongly recommended that you exclude the local administrator account when using this command to avoid accidentally injecting that account on the target system.

Injection use: Injects all users in a specified personality. The personality can be specified using the SOURCE command.

Must be used with: AUTOEXTRACT or AUTOINJECT.

Cannot be used with: AUTOBACKUP.

Example: `START /w MigrationManager.EXE /autoextract /ALLUSERS /EXCLUDEUSER %COMPUTERNAME%\Administrator`

```
START /w MigrationManager.EXE /autoinject /SOURCE MYCOMPUTER /ALLUSERS
```

DOMAIN

Syntax:

```
/DOMAIN <source domain name>:<target domain name> [<source domain name>:<target domain name>]
```

Extraction use: N/A.

Injection use: Redirects users from a source domain to a different target domain.

This command is typically used in conjunction with the ALLUSERS when users are being moved from one domain to another.

Note: Domain names containing spaces must be enclosed in quotes.

Must be used with: AUTOINJECT.

Cannot be used with: AUTOBACKUP, AUTOEXTRACT, INCLUDEUSER.

Example:

```
START /w MigrationManager.EXE /autoinject /SOURCE MYCOMPUTER /ALLUSERS /DOMAIN "MYDOMAIN:SOME DOMAIN"
```

Note

Migration Manager does not create domain user accounts. When migrating users between domains using the /DOMAIN command the user's account must already exist in the target domain otherwise the injection will fail.

EXCLUDEDOMAIN

Syntax:

```
/EXCLUDEDOMAIN <domain name>
```

Extraction use: Prevents user profiles from the specified domain from being extracted.

Injection use: Prevents user state data belonging to users from the specified domain from being injected.

Must be used with: ALLUSERS and one of AUTOEXTRACT or AUTOINJECT.

Cannot be used with: AUTOBACKUP.

Example:

```
START /w MigrationManager.EXE /autoextract /allusers /EXCLUDEDOMAIN MYDOMAIN
```

```
START /w MigrationManager.EXE /autoinject /source MYCOMPUTER /allusers /EXCLUDEDOMAIN MYDOMAIN
```

EXCLUDELOCAL

Syntax:

```
/EXCLUDELOCAL
```

Extraction use: Excludes all local users from being extracted.

This command is most commonly used in conjunction with the /ALLUSERS command.

If by using this switch it results in no personalities being extracted, Migration Manager will terminate and return an exit code.

Injection use: Excludes local users from being injected.

This command is most commonly used in conjunction with the /ALLUSERS command.

If by using this switch it results in no personalities being injected, Migration Manager will terminate and return an exit code.

Must be used with: ALLUSERS and one of AUTOEXTRACT or AUTOINJECT.

Cannot be used with: AUTOBACKUP.

Example: `START /w MigrationManager.EXE /autoextract /ALLUSERS /EXCLUDELOCAL`

```
START /w MigrationManager.EXE /autoinject /SOURCE MYCOMPUTER /ALLUSERS
/EXCLUDELOCAL
```

EXCLUDENOTLOGGEDIN

Syntax: `/EXCLUDENOTLOGGEDIN <days>`

Extraction use: Excludes all users that have not logged in within the specified number of days from being extracted.

This command is most commonly used in conjunction with the /ALLUSERS command.

If by using this switch it results in no personalities being extracted, Migration Manager will terminate and return an exit code.

Injection use: N/A.

Must be used with: AUTOEXTRACT and one of ALLUSERS or INCLUDEUSER.

Cannot be used with: AUTOBACKUP, AUTOINJECT.

Example: `START /w MigrationManager.EXE /autoextract /ALLUSERS /EXCLUDENOTLOGGEDIN 90`

EXCLUDEUSER

Syntax: `/EXCLUDEUSER <domain name\user name> [<domain name>\<user name>]`

Extraction use: Allows you to exclude specified users from being extracted.

This command is most commonly used in conjunction with the ALLUSERS command.

If by using this switch it results in no personalities being extracted, Migration Manager will terminate and return an exit code.

Injection use: Allows you to exclude specified users from being injected.

This command is most commonly used in conjunction with the ALLUSERS command.

If by using this switch it results in no personalities being injected, Migration Manager will terminate and return an exit code.

Must be used with: ALLUSERS and one of AUTOEXTRACT or AUTOINJECT.

Cannot be used with: AUTOBACKUP.

Example:

```
START /w MigrationManager.EXE /autoextract /ALLUSERS /EXCLUDEUSER
MYDOMAIN\User1
```

```
START /w MigrationManager.EXE /autoinject /Source MYCOMPUTER /ALLUSERS
/EXCLUDEUSER MYDOMAIN\User1
```

INCLUDEUSER

Syntax:

```
/INCLUDEUSER <domain name>\<user name> [<domain name>\<user name>]
```

```
/INCLUDEUSER <domain name>\<user name>[:<target domain name>\<target user
name>]
<domain name>\<user name>[:<target domain name>\<target user name>]]
```

Extraction use: The /INCLUDEUSER command extracts the personalities for each user that is specified following the command.

In domain environments, user names must be specified with the domain name in the form <DOMAIN>\<USER>.

If there are no usernames that match the users specified in the command-line then Migration Manager will terminate and return the appropriate exit code.

If at least one user specified matches a username on the computer where the extraction operation is being performed, but one or more other specified users don't match any usernames on the computer, the extraction process will continue and extract the user state for the users that matched and the operation log that gets created following the operation displays the users that were not extracted.

Note: Usernames and Domain names with spaces must be contained in quotes when specified following the /INCLUDEUSER command.

Injection use: This parameter is used to specify which users should be injected.

In domain environments, user names must be specified with the domain name in the form <DOMAIN>\<USER>.
It's also possible to remap users using this command. The most common case for this is when users are being moved from one domain to another. To do this, specify the user names as <SOURCE DOMAIN>\<SOURCE USER>:<TARGET DOMAIN>\<TARGET USER>.

Migration Manager will only inject the matching users if all specified users exist within a single personality. Using the SOURCE command allows you to further limit the scope of possible personalities when comparing usernames.

If all users specified with INCLUDEUSER exists in more than one personality, Migration Manager will terminate and return the appropriate exit code.

Note: Usernames and Domain names with spaces must be contained in quotes when specified following the INCLUDEUSER command.

Must be used with: AUTOEXTRACT, AUTOINJECT.

Cannot be used with: ALLUSERS , AUTOBACKUP.

Example:
```
START /w MigrationManager.EXE /autoextract /INCLUDEUSER
MYDOMAIN\User1 MYDOMAIN\User2
```

```
START /w MigrationManager.EXE /autoextract /INCLUDEUSER "SOME DOMAIN\User A"
"SOME DOMAIN\User B"
```

```
START /w MigrationManager.EXE /autoinject /SOURCE MYCOMPUTER /INCLUDEUSER
MYDOMAIN\User1 MYDOMAIN\User2
```

```
START /w MigrationManager.EXE /autoinject /SOURCE computername /INCLUDEUSER
"MYDOMAIN\User1:SOME DOMAIN\User A"
"MYDOMAIN\User2:SOME DOMAIN\User B"
```

Note

Migration Manager does not create domain user accounts. When migrating a user between domains using the /INCLUDEUSER command the user’s account must already exist in the target domain otherwise the injection will fail.

INJECTTOLOGGEDINUSER

Syntax: /INJECTTOLOGGEDINUSER

Extraction use: N/A.

Injection use: Forces data to be injected to the user that’s interactively logged on to the computer regardless of which user the data was extracted for.

Note: There are very few scenarios where this command is required, in most scenarios the INCLUDEUSER command will work better and also doesn’t require that a user is interactively logged on to the computer.

Note: There must be only a single user in the user state data being injected.

Must be used with: AUTOINJECT.

Cannot be used with: AUTOBACKUP.

Example: `START /w MigrationManager.EXE /autoinject /source MYCOMPUTER /INJECTTOLOGGEDINUSER`

LOCALPROFILE

Syntax: `/LOCALPROFILE`

Extraction use: N/A.

Injection use: The `/LOCALPROFILE` command-line argument is used to specify that profiles will be local on the injection system. Use this argument if roaming profiles were used on the extraction system, but roaming profiles will not be used on the injection system.

Note: You will need to configure Active Directory to stop using roaming profiles after the extraction and before the injection.

Do not use this argument if roaming profiles were used on the extraction system, and roaming profiles will continue to be used on the injection system.

If the profile being injected was not a roaming profile, this parameter has no effect.

If folders were redirected on the extraction system, they will continue to be redirected on the injection system. To change the location of the redirected folders, see `/REDIRECTFOLDERS`.

Must be used with: `AUTOINJECT`.

Cannot be used with: `AUTOEXTRACT`, `AUTOBACKUP`.

Example: `START /w MigrationManager.EXE /autoinject /source MYCOMPUTER /LOCALPROFILE`

REDIRECTFOLDERS

Syntax: `/REDIRECTFOLDERS <UNC path for root of redirect folders>`
Extraction use: N/A.

Injection use: The `/REDIRECTFOLDERS` command-line argument is used to specify a remote path for redirected folders in three scenarios:

1. You are injecting to users whose user or domain names differ from the extracted users, and you want the injection users' folders to be redirected
2. You are injecting to the same user and domain names you extracted, and the extraction system was not using redirected folders but you want to start using folder redirection on the injection system
3. You are injecting to the same user and domain names you extracted, and the extraction system used a different path for redirected folders. Use this argument if you want the injection system to use a different path for redirected folders than the extraction system.

Note: In either case, you will still need to configure Active Directory to use the redirected folders at the new location you specify.

If you *are* using folder redirection on the extraction system and are injecting to the same user and domain names, and you want to use the same path for redirected folders on the injection system, *do not* use this argument. By default, the same path used for folder redirection on the extraction system will be used on the injection system.

If the specified path to the redirected folders is invalid, Migration Manager will terminate and return an appropriate error code.

Redirected folders will be created at the supplied path, if they do not already exist, in the form `\\MyServer\Users\<user name>\My Documents`, for example. The files extracted from shell folders on the extraction system will be injected at that path.

Must be used with: `AUTOINJECT`.

Cannot be used with: `AUTOBACKUP`, `AUTOEXTRACT`.

Example: `START /w MigrationManager.EXE /autoinject /allusers /REDIRECTFOLDERS \\MyServer\Users`

ROAMINGPROFILES

Syntax: `/ROAMINGPROFILES <UNC path for root of roaming profiles>`

Extraction use: N/A.

Injection use: The `/ROAMINGPROFILES` command-line argument is used to specify a remote path for roaming profiles when you are injecting to users whose roaming profiles' server share location differs from the extracted users.

If the extracted users are using roaming profiles and you are injecting to users whose profiles are located on the same server as the extracted users there is no need to use this parameter.

Note: You will need to configure Active Directory to use roaming profiles at the new location for the users you specify.

If the extracted users are not using roaming profiles this parameter has no effect.

Roaming profiles will be created at the supplied path, if they do not already exist, in the form `\\MyServer\Users\<user name>`, for example. The files extracted from roaming profile locations on the source system will be injected to this path. Active Directory needs to be configured to be consistent with this naming convention.

Note: A .V# suffix (such as .V2) is added to the root roaming profile folder for injections on Windows Vista and later.

Must be used with: `AUTOINJECT`.

Cannot be used with: `AUTOBACKUP`, `AUTOEXTRACT`.

Example: `START /w MigrationManager.EXE /autoinject /allusers /ROAMINGPROFILES \\MyServer\Users`

Advanced Command-Line Parameters

The advanced command-line parameters control behavior that aren't always used in the most common use cases but handle scenarios that come up from time to time:

- DisplayErrorCode – display any errors at the end of the operation
- ElevatedCredentials – Enables embedded Local Administrator passwords
- HideStatus – don't display the progress dialog during the operation
- Import – import file and/or registry rules before an extraction
- NoCancel – don't display the cancel button in the progress dialog
- PersonalityNaming - specify naming personality folder based on computername or macid
- Throttle - throttle network use during extraction

DISPLAYERRORCODE

Syntax: `/DISPLAYERRORCODE`

Extraction use: Causes a dialog describing any errors encountered during the extraction after the extraction completes.

If the extraction completes without errors, no dialog is displayed.

Note: This command should only be used if Migration Manager will be run when a user is interactively logged on to the computer. For fully automated scenarios, it's preferable to check the exit code from Migration Manager and if an error is indicated check the generated log file instead.

Injection use: Causes a dialog describing any errors encountered during the injection after the injection completes.

If the injection completes without errors, no dialog is displayed.

Note: This command should only be used if Migration Manager will be run when a user is interactively logged on to the computer. For fully automated scenarios, it's preferable to check the exit code from Migration Manager and if an error is indicated check the generated log file instead.

Must be used with: `AUTOBACKUP`, `AUTOEXTRACT` or `AUTOINJECT`.

Cannot be used with: N/A.

Example:

```
START /w MigrationManager.EXE /autoextract /allusers
/DISPLAYERRORCODE
```

ELEVATEDCREDENTIALS

Syntax:

```
MigrationManager.EXE /ELEVATEDCREDENTIALS <username> <domainname>
<password>
```

Note

This command works with `MigrationManager.EXE`, and **Not** with `SE.EXE`

Extraction use: Enables migration of users not logged in without giving users Local Administrator rights.

Injection use: Enables injection on systems without elevating other Local or domain users.

Must be used with: `MigrationManager.EXE` and can replace all `SE.EXE` command line usage.

Cannot be used with: `SE.EXE`

Example: `MigrationManager.EXE /ELEVATEDCREDENTIALS JOEADMIN CORPDOMAIN 1234567`

This creates the encrypted file “SE.dat” which contains the login credentials.

Migration technician runs Migration Manager `MigrationManager.exe /autoextract`

MigrationManager.exe will read the “SE.dat” file and launch SE.exe as the specified user with elevated credentials. The expectation is that the migration technician will interact solely via batch script.

This means that: If the SE.dat file is present, MigrationManager.exe requires that it be used with the `/AUTOEXTRACT`, `/AUTOINJECT` or `/AUTOBACKUP` options present. Otherwise, it will not proceed.

No error message will be displayed to the user in the case that MigrationManager.exe (itself, as opposed to SE.exe) encounters an error. In order to detect whether an error has occurred, and which error, the script will need to utilize `%ERRORLEVEL%`

Note: A side effect of running MigrationManager.exe this way is that the machine will have a password protected account created for the domain admin user specified.

Note

The file SE.dat is encrypted using Microsoft CryptoAPI and the RSA Encryption Algorithm with a SHA2 hash.

HIDESTATUS

Syntax: `/HIDESTATUS`

Extraction use: Hides the progress dialog during an extraction.

See also the related `NOCANCEL` command.

Injection use: Hides the progress dialog during an injection.

See also the related `NOCANCEL` command.

Must be used with: `AUTOBACKUP`, `AUTOEXTRACT` or `AUTOINJECT`.

Cannot be used with: N/A.

Example: `START /w MigrationManager.EXE /autoextract /allusers /HIDESTATUS`

IMPORT

Syntax: `/IMPORT <fully qualified path to rule file>`

Extraction use: This command imports a predefined list of file and/or registry rules via the AUTOEXTRACT command-line.

The XML file that contains the rules uses the same format as the rules that are created and exported using the Migration Manager rule export command.

Injection use: N/A.

Must be used with: AUTOEXTRACT.

Cannot be used with: AUTOBACKUP, AUTOINJECT.

Example: `START /w MigrationManager.EXE /autoextract /import \\MyServer\MigrationManager\rules.xml`

NOCANCEL

Syntax: /NOCANCEL

Extraction use: Hides the Cancel button in the progress dialog during an extraction. See also the related HIDESTATUS.

Injection use: N/A.

Must be used with: AUTOBACKUP, AUTOEXTRACT.

Cannot be used with: AUTOINJECT.

Example: `START /w MigrationManager.EXE /autoextract /allusers /NOCANCEL`

PERSONALITYNAMING

Syntax: `/PERSONALITYNAMING: <DEFAULT | MACID | COMPUTERNAME>`

Extraction use: Specifies the naming of the personality folder within the datastore. The default personality naming is computername when extracting from Windows, and MACID when extracting offline Windows using Windows PE.

This command overrides the personality naming information in the configuration file.

Injection use: N/A.

Must be used with: AUTOEXTRACT.

Cannot be used with: AUTOINJECT, AUTOBACKUP, PERSONALITYPATH.

Example: `START /w MigrationManager.EXE /autoextract /PersonalityNaming:MACID`

THROTTLE

Syntax: `/THROTTLE <kbps>`

Extraction use: Limits the data write speed to throttle network use to the specified kilobytes per second.

Injection use: N/A.

Must be used with: AUTOEXTRACT.

Cannot be used with: AUTOBACKUP, AUTOINJECT.

Example: `START /w MigrationManager.EXE /autoextract /allusers /Throttle 50`

Automation Examples

With a good understanding of how the command-line parameters are used to automate a migration, the next step is to incorporate those command-line switches into an automated script.

The following sections illustrate several automation use case examples:

- Processing Logged On Users
- Processing Not-Logged On Users
- Processing Multiple Users
- Moving Users Between Domains
- Using Passwords in Migrations

Each example there includes a fully functional extraction and injection batch file along with a table that describes the commands being used to perform the operation.

Note
To save any of the examples as MS-DOS batch files, open Notepad and copy then paste the text. Select Save, change the 'Save as type' to 'All files' then change 'untitled' to 'Extract.bat' and select Save.

Note
The batch file examples in this section do not contain exit codes. The full list of supported exit codes is available in Migration Manager Exit Codes. It is recommended that exit codes be included in each batch file that you develop.

Processing Logged On Users

Description

Extracting and injecting a currently logged user is a use case that most commonly comes up in smaller environments that don't have any kind of desktop management tool deployed. In this case there may not even be login scripts being used in which case it may be necessary to make the batch files accessible to the users in the form of a desktop shortcut (or a shortcut placed in the Startup folder for regular backups).

Note

If you are performing an extraction or injection of the currently logged in user's personality, the logged in user must have local administrator rights on the computer.

Many applications don't write their settings until the user exits the application (most of the Office applications operate this way for instance). For this reason it's highly recommended that users be instructed to exit all applications before performing a Migration Manager operation.

Process Examples

Migrating the user state for the currently logged on user is a very straightforward process. If you plan on using technicians to upgrade the systems or to deploy a new image to the machine, then the technician can execute the extraction and injection batch files on the user's computer while they are still logged on.

Once the technician begins the extraction or injection process on one machine, they can simply move to the next user's machine and use the same process. Using a manual process the technician can only perform one migration at a time. However, by automating the process they can perform several extractions and injections in the time it would take to perform a single migration manually.

The process can also be configured to have the users initiate the extraction and injection, but this is rarely very practical as local administrator rights are required to perform any operation with Migration Manager.

Extract.bat File Example

This Extract.bat file can be used for each of the processes mentioned above to extract the currently logged on user. This example assumes that Migration Manager was installed on the server "servername" and that the installation directory is shared as "Migration Manager".

```
@echo off
echo Starting extraction...
START /w \\MyServer\MigrationManager\MigrationManager.EXE /autoextract /config \\MyServer\MigrationManager\configuration.xml
IF ERRORLEVEL 1 (echo Extraction failed) ELSE (echo Extraction succeeded)
```

Line Number	Extract.bat File Definition
Line 1	Turns off the screen messages so the user does not see the commands in the batch file and is optional.
Line 2	Display a progress message so the user knows what's going on.
Line 3	Starts Migration Manager performing an extraction using the specified configuration file and waits for the extraction to complete.
Line 4	Performs a very simple check to see if the extraction succeeded or not (0 means success, anything greater than 0 means an error occurred).

Inject.bat File Example

This Inject.bat file can be used for each of the processes mentioned above to inject to the currently logged on user. This example assumes that Migration Manager was installed on the server "servername" and that the installation directory is shared as "Migration Manager".

```
1.   @echo off
2.   echo ...Injecting Personality
3.   START /w \\MyServer\MigrationManager\MigrationManager.EXE /autoinject
     /config \\MyServer\MigrationManager\configuration.xml
4.   IF ERRORLEVEL 1 (echo Injection failed) ELSE (echo Injection succeeded)
```

Line Number	Inject.bat File Definition
Line 1	Turns off the screen messages so the user does not see the commands in the batch file and is optional.
Line 2	Display a progress message so the user knows what's going on.
Line 3	Starts Migration Manager performing an injection using the specified configuration file and waits for the injection to complete.
Line 4	Performs a very simple check to see if the injection succeeded or not (0 means success, anything greater than 0 means an error occurred).

Processing Not-Logged On Users

Description

The most common use case for Migration Manager is to run it when there's no user logged on to the system. This not only ensures that the operation can be performed remotely, but also offers the best fidelity since no applications will be running and thus all application settings will have been stored properly before the operation starts.

Process Examples

Using environment variables and command-line switches a technician can log in to a given workstation and perform an automated extraction and injection of a specified user. The technician simply uses a parameter in the batch file that defines the user to process.

The username is specified when the batch file is invoked. The advantage of using this process is the user does not have to be present during the extraction or the injection, and the technician performing the migration does not have to obtain the username and password of the user that will be migrated.

Note

To extract or inject a personality for a user or users that are not currently logged in to the machine, the user that is performing the extraction or injection must have Local Administrator Rights. Migration Manager also requires UAC elevation on Windows if enabled.

Extraction Example (Invoking the Extract.bat file)

In this example, the Extract.bat file is located on the file share `\\MyServer\MigrationManager`. The technician can invoke the Extract.bat file from an elevated command-prompt by entering the path to where the Extract.bat file resides.

The user that needs to be extracted is specified after the batch file:

```
C:\> \\MyServer\MigrationManager\extract.bat mydomain\user1
```

Extract.bat File when user is not logged in

This example assumes that Migration Manager is available from `\\MyServer\MigrationManager`. In order to extract the correct user, the `/INCLUDEUSER` parameter is used.

To build this script, simply take the script from Extract.bat File Example, and replace line 3 with the following:

```
3.  START /w \\MyServer\MigrationManager\MigrationManager.EXE /autoextract
/IncludeUser %1
/config \\MyServer\MigrationManager\configuration.xml
```

Extract.bat File when user is not logged in

Line 3 - The command has been modified to specify the name of the user that should be extracted using the `/INCLUDEUSER` parameter. The actual user name must be specified when the batch file is executed.

Injection Example (Invoking the Inject.bat file)

In this example, the inject.bat file is located on the file share `\\MyServer\MigrationManager`. The technician can invoke the Inject.bat file from an elevated command-prompt by entering the path to where the inject.bat file resides.

The username of the user you want to inject is specified after the batch file:

```
C:\> \\MyServer\MigrationManager\inject.bat mydomain\user1
```

Inject.bat File Example when user is not logged in

This example assumes that Migration Manager is available from `\\MyServer\MigrationManager`. In order to extract the correct user, the /INCLUDEUSER parameter is used.

To build this script, simply take the script from Inject.bat File Example, and replace line 3 with the following:

```
3. START /w \\MyServer\MigrationManager\MigrationManager.EXE /autoinject
/IncludeUser %1
/config \\MyServer\MigrationManager\configuration.xml
```

Inject.bat File Definition (By Line)

Line 3 - Performs the automatic injection of the user's personality that was specified when the batch file was invoked. Following the `/IncludeUser`switch is a `%1`. This is the batch file parameter that represents the username specified following the `Inject.bat` file called from the `Start | Run` field. It is, again, important to add the `/w` parameter to the `start` command.

Processing Multiple Users

Description

Migration Manager can be used to process the user state for multiple users on a computer. This is useful when migrating a computer that is shared by several users.

In most cases many of the settings and files associated with a user are specific for that particular user. Migration Manager fully supports this use case.

Process Examples

Using environment variables and command-line switches a technician can log in to a given workstation and perform an automated extraction and injection of all the users that exist on the computer. For extraction, the technician can use the ALLUSERS parameter to extract all of the users on the computer.

On injection the batch file will combine the ALLUSERS switch and the SOURCE switch to specify and inject the extracted user state data. The SOURCE parameter will be followed by a batch file parameter that will represent the name of the computer where the extraction was performed.

The computer name is specified when the batch file is invoked. The advantage of using this process is the user does not have to be present during the extraction or the injection, and the technician performing the migration does not have to obtain the username and password for any of the users that have profiles on the computer.

Note

To extract or inject a personality containing multiple users, the user that is performing the extraction or injection must have Local Administrator Rights. Migration Manager also requires UAC elevation on Windows if enabled.

Extraction Example (Invoking the Extract.bat file)

This example assumes that Migration Manager is available from `\\MyServer\MigrationManager`. The technician can invoke the `Extract.bat` file from an elevated command-prompt by entering the path to where the `Extract.bat` file resides, or by simply double clicking on the `Extract.bat` file:

```
C:\> \\MyServer\MigrationManager\extract.bat
```

Extract.bat File Example to Extract Multiple Users

This example Extract.bat file performs an automated extraction for all users on the computer. To build this script, simply take the script from Extract.bat File Example, and replace line 3 with the following:

```
3. START /w \\MyServer\MigrationManager\MigrationManager.EXE /autoextract
/AllUsers
/config \\MyServer\MigrationManager\configuration.xml
```

Extract.bat File Definition (By Line)
Line 3 - Performs an extraction of all users on the computer where the script is run.

Injection Example (Invoking the Inject.bat file) to Inject Multiple Users

In this example, the inject.bat file is located on the file share `\\MyServer\MigrationManager`. The technician can invoke the `Inject.bat` file from an elevated command-prompt by entering the path to where the `Inject.bat` file resides. The name of the computer where the extraction was performed is specified after the batch file:

```
C:\> \\MyServer\MigrationManager\inject.bat mycomputer
```

Inject.bat File Example to Inject Multiple Users

This example assumes that Migration Manager is available from `\\MyServer\MigrationManager`. This example `Inject.bat` file performs an automated injection of all the users extracted from the specified computer.

To build this script, simply take the script from Inject.bat File Example, and replace line 3 with the following:

```
3. START /w \\MyServer\MigrationManager\MigrationManager.EXE /autoinject
/Source %1 /AllUsers
/config \\MyServer\MigrationManager\configuration.xml
```

Inject.bat File Definition (By Line)
Line 3 - Injects all of the users extracted from the specified computer.

Moving Users Between Domains

Description

The DOMAIN command allows you to take user state data extracted for a user in one domain and redirect that to a user with the same user name in a different domain. This is useful when users are being moved between domains as part of a migration.

Note

Migration Manager does not create domain user accounts. When migrating a user between domains the user's account must already exist in the target domain otherwise the injection will fail.

Process Examples

Using environment variables and command-line switches a technician can log in to a given workstation and perform an automated extraction and injection of all the users that exist on the computer. For extraction, the technician can use the ALLUSERS command-line switch to extract all of the users on the computer. On injection the batch file will combine the ALLUSERS switch and the SOURCE switch to specify the name of the computer the user state data was extracted from.

The Computer Name is specified when the batch file is invoked. In addition, the DOMAIN switch will be used to redirect the users in the specified personality to be created with association to the specified target domain.

The advantage of using this process is the user does not have to be present during the extraction or the injection, and the technician performing the migration does not have to obtain the user name and password for any of the users that have profiles on the computer.

Note

To extract or inject a personality containing multiple users, the user that is performing the extraction or injection must have Local Administrator Rights. Migration Manager also requires UAC elevation on Windows if enabled.

Extraction Example (Invoking the Extract.bat file)

This example assumes that Migration Manager is available from \\MyServer\MigrationManager. The technician can invoke the Extract.bat file from an elevated command-prompt by entering the path to where the Extract.bat file resides, or by simply double clicking on the Extract.bat file:

```
C:\> \\MyServer\MigrationManager\extract.bat
```

Extract.bat File Example for Moving Users between Domains

This example `Extract.bat` file performs an automated extraction for all users on the computer. To build this script, simply take the script from Extract.bat File Example, and replace line 3 with the following:

```
3. START /w \\MyServer\MigrationManager\MigrationManager.EXE /autoextract
/AllUsers
/config \\MyServer\MigrationManager\configuration.xml
```

Extract.bat File Definition (By Line)
Line 3 - Performs an extraction for all users on the computer.

Injection Example (Invoking the Inject.bat file)

In this example, the inject.bat file is located on the file share `\\MyServer\MigrationManager`. The technician can invoke the `Inject.bat` file from an elevated command-prompt by entering the path to where the `Inject.bat` file resides. The name of the computer where the extraction was performed is specified after the batch file:

```
C:\> \\MyServer\MigrationManager\inject.bat mycomputer
```

Inject.bat File Example for Moving Users between Domains

This example assumes that Migration Manager is available from `\\MyServer\MigrationManager`. This example `Inject.bat` file performs an automated injection of all the users extracted from the specified computer.

To build this script, simply take the script from Inject.bat File Example, and replace line 3 with the following:

```
3. START /w \\MyServer\MigrationManager\MigrationManager.EXE /autoinject
/Source %1 /AllUsers
/Domain OldDomain:NewDomain /config
\\MyServer\MigrationManager\configuration.xml
```

Inject.bat File Definition (By Line)
Line 3 - Injects the users extracted from the specified computer, mapping any user from the domain “OldDomain” to the domain “NewDomain”

Using Passwords in Migrations

Description

The PASSWORD parameter allows you to assign a password when extracting user state data to encrypt the data using AES256. This password then needs to be provided for any future operations with the extracted data, the data cannot be accessed without the password.

The password can both be entered and saved in the extraction and injection batch files you use, or for more security the password can be specified when either batch files are invoked with the use of simple batch file parameters.

Note

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

Process Examples

Using batch file parameters and command-line switches a technician can specify a password to be assigned when extracting the personality and then called when injecting the password protected personality. In these examples, the password is provided as a parameter to the batch files.

Note

To extract or inject a personality containing multiple users, the user that is performing the extraction or injection must have Local Administrator Rights. Migration Manager also requires UAC elevation if enabled.

Extraction Example (Invoking the Extract.bat file)

This example assumes that Migration Manager is available from `\\MyServer\MigrationManager`. The technician can invoke the `Extract.bat` file from an elevated command-prompt by entering the path to where the `Extract.bat` file resides, specifying the password that should be used as a parameter to the batch file:

```
C:\> \\MyServer\MigrationManager\extract.bat mypassword
```

Extract.bat File Example USING A PASSWORD

This example `Extract.bat` file performs an automated extraction for all users on the computer, assigning a password through a batch file parameter. To build this script, simply take the script from Extract.bat File Example, and replace line 3 with the following:

```
3.  START /w \\MyServer\MigrationManager\MigrationManager.EXE /autoextract
/AllUsers /PASSWORD %1
/config \\MyServer\MigrationManager\configuration.xml
```

Extract.bat File Definition (By Line)
Line 3 - Performs an extraction of all users from the computer, assigning the specified password to the extracted user state data.

Injection Example (Invoking the Inject.bat file) Using a Password

In this example, the `inject.bat` file is located on the file share `\\MyServer\MigrationManager`. The technician can invoke the `Inject.bat` file from an elevated command-prompt by entering the path to where the `Inject.bat` file resides. The name of the computer where the extraction was performed is specified after the batch file as is the password specified when the extraction was performed:

```
C:\> \\MyServer\MigrationManager\inject.bat mycomputer mypassword
```

Inject.bat File Example Using a Password

This example assumes that Migration Manager is available from `\\MyServer\MigrationManager`. This example `Inject.bat` file performs an automated injection of all the users extracted from the specified computer and using the provided password to get access to the user state data.

To build this script, simply take the script from Inject.bat File Example, and replace line 3 with the following:

```
3.  START /w \\MyServer\MigrationManager\MigrationManager.EXE /autoinject
/Source %1 /AllUsers /PASSWORD %2
/config \\MyServer\MigrationManager\configuration.xml
```

Inject.bat File Definition (By Line)
Line 3 - Injects the user state extracted from the specified computer using the provided password.

Injection Mapping Files

Description

Injection Mapping files are used to define which source computer contains the user state for a given target computer so that the injection can be fully automated without any administrator intervention required.

Mapping File Structure

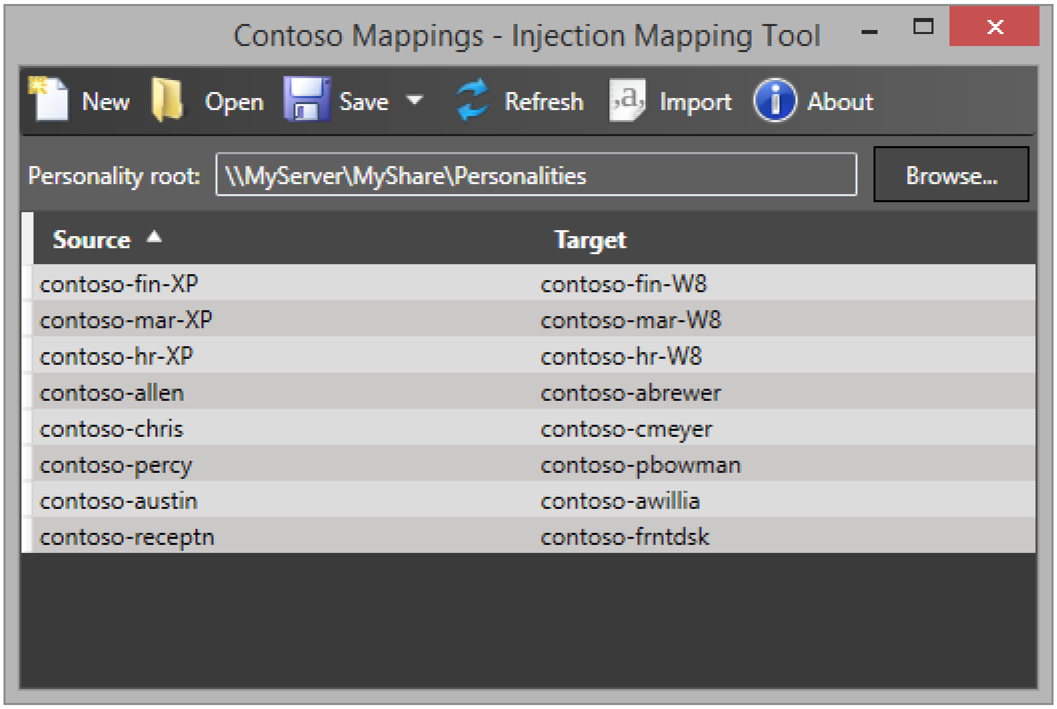
Mapping files are XML files with this structure:

```
<?xml version="1.0" encoding="utf-8"?>
<MappingFile xmlns:i="http://www.w3.org/2001/XMLSchema-instance"
xmlns="http://tranxition.com/schemas/mappingfile/2011/5">
 <Mappings>
 <ComputerMapping>
 <SourceComputer>CONTOSO-hr-XP</SourceComputer>
 <TargetComputer>CONTOSO-hr-W8</TargetComputer>
 </ComputerMapping>
 </Mappings>
 <PersonalityRoot>\\MyServer\MigrationManager\Personalities</PersonalityRoot>
</MappingFile>
```

Each source/target computer pairing is defined in a `<ComputerMapping>` element with each source and target computer only occurring once in the file.

Creating Mapping Files Using the Injection Mapping Tool

Mapping files can be created with any tool that can create XML files, but the easiest way to create them is to use the Injection Mapping Tool that is provided with Migration Manager:



Contoso Mappings - Injection Mapping Tool

Personality root: \\MyServer\MyShare\Personalities

Source ▲	Target
contoso-fin-XP	contoso-fin-W8
contoso-mar-XP	contoso-mar-W8
contoso-hr-XP	contoso-hr-W8
contoso-allen	contoso-abrewer
contoso-chris	contoso-cmeyer
contoso-percy	contoso-pbowman
contoso-austin	contoso-awillia
contoso-receptn	contoso-frntdsk

Creating a New Mapping File

To create a new Mapping File, follow these steps:

1. Start the Injection Mapping Tool
2. Click the Browse button to display the folder browser
3. Select the location where the personalities are located and click the OK button
4. The tool now reads all of the available personalities and populates the Source column with the names of the computers user state have been extracted from
5. Enter the corresponding target computer names in the Target column
6. Click the Save button to save the Mapping File

Note

The mapping file should contain just the base name of the computer, not the fully qualified DNS name.

Adding Source Computers to a Mapping File

Once a Mapping File has been created, additional source computers from subsequent extractions can be added to the file using these steps:

1. Start the Injection Mapping Tool
2. Click the Open button to display the Open Mapping File dialog and open the mapping file in question
3. Click the Refresh button to add all new source computers (i.e. source computers that aren’t already in the Mapping File) to the file.

4. Enter the target computer names for the new source computers
5. Click the Save button to save the Mapping File

Importing Source and Target Computers

If you already have the source and target computer information available from another source and can make that available as a CSV file, that file can be imported into the Mapping Tool.

The CSV file must have the following format:

```
<source computer>,<target computer>
```

With a single source/target computer pair on each line in the file.

A CSV file can be imported to create a new mapping file or imported into an existing mapping file using these steps:

1. Start the Injection Mapping Tool
2. If you want to import into an existing Mapping File, open the file
3. Click the Import button display the Import CSV File dialog
4. Select the CSV file to import and click the Open button to add all source systems from the CSV file that aren’t already in the Mapping File
5. Click the Save button to save the Mapping File

Response Files

Description

Since there are limits to command-line length in some environments and since the potential exists for complex command-lines to exceed those limits, Migration Manager supports command-line response files. A response file contains command-line arguments (switches) that are accessed indirectly.

Command line response file support reflects the long-standing Microsoft response file behavior. An at-sign (@) followed by a file specification will designate a response file to include in the logical command-line.

Response File Example

The response file `\\MyServer\MigrationManager\response.txt` contains:

```
/IncludeUser user1 /Config \\MyServer\MigrationManager\configuration.xml
```

The corresponding logical command-line processed by Migration Manager is:

```
Start /w \\MyServer\MigrationManager\MigrationManager.EXE /autoextract
/IncludeUser user1
/Config \\MyServer\MigrationManager\configuration.xml
```

Example

This example will extract the personality of the user that is specified in the response file.

```
@echo off
echo Extracting data...
start /w \\MyServer\MigrationManager\MigrationManager.EXE /autoextract
@\\MyServer\MigrationManager\response.txt
IF ERRORLEVEL 1 (echo Extraction failed) ELSE (echo Extraction succeeded)
```

Offline Migrations

Introduction

Migration Manager allows offline users to be extracted from a Windows PE environment.

Extracting Offline Users

When Migration Manager is installed to a network share and launched from Windows PE, it automatically connects to the offline image. When launching Migration Manager from PE, it is recommended that `MigrationManager.cmd` is used. This cmd script file will automatically determine the architecture of the Windows PE OS and launch the appropriate Migration Manager executable (32 or 64 bit). The architecture of Windows PE determines which architecture of Migration Manager to use, the offline Windows machine can be either architecture even if it does not match that of Windows PE. Extractions can then be done as they would if Migration Manager had been launched on the offline Windows machine itself.

Injecting Offline Users

Migration Manager does not currently support inject to offline systems. Inject offline users to Windows as normal. When using the `/Source` switch, the default for offline systems is to specify personalities using the MAC address instead of the computer name of the source computer. If injecting to the same system during a system refresh, `/Source:macid` can be used to specify the current machine's MAC address.

Note

The default personality naming behavior of using MACID for offline systems can be changed in Extraction Policies under `Edit | Preferences`, or by using `PERSONALITYNAMING`

Example Command-Line with Offline Users

Extraction

```
start /w MigrationManager.CMD /autoextract /allusers /excludelocal
```

Injection

```
start /w MigrationManager.EXE /autoinject /allusers /source 000a959d6816
```

```
start /w MigrationManager.EXE /autoinject /allusers /source:macid
```

Using Hardlinks

Introduction

Migration Manager allows storing data files as hardlinks locally on NTFS volumes. This for use with In-Place Operating System refreshes to reduce migration time and use less storage for the personality during migration. Instead of copying data to the personality data store, the data is Hardlinked to and remains in place.

Extracting Hardlinks

When Migration Manager extracts with hardlinking, data files on NTFS volumes are hardlinked to instead of being copied into a data store. If multiple ntfs volumes exist, the specified datastore will be created on each ntfs volume for hardlinking files on that volume. Non-ntfs volumes will store data on the primary ntfs volume.

Note

Files on non-ntfs volumes, as well as locked files on ntfs volumes cannot be hardlinked and are copied into the specified data store location instead of being hardlinked.

Injecting Hardlinks

During the injection, files are hardlinked to their destination location. Any files that are being injected to a different volume will be copied as ntfs does not support hardlinks to different volumes.

The file attribute `read-only` does not persist in a hardlink migration due to ntfs limitations.

Note

If using File Rules to redirect files from a single location to multiple locations, such as using a File Rule to redirect files from `C:\Data` to `%MyDocuments%`, all of the injected files will be hardlinked together. As a result, changes made to a file in one location will be reflected in that file in all locations.

Example Command-Line

Extraction

```
start /w MigrationManager.EXE /autoextract /allusers /personalitypath
C:\_data /hardlinks
```

WARNING

The specified data store location, in this example `C:\_data` must be protected during the operating system reimage process, as well as the same specified directory, for example `E:\_data`, on each ntfs volume if multiple ntfs volumes exist. Migration Manager does not provide protection of the directory during reimage and failure to protect the directory will result in complete data loss.

Injection

```
start /w MigrationManager.EXE /autoinject /allusers /personalitypath C:\_data
```

Note

The personality storage type is automatically determined on injection. Specifying `/hardlinks` with `/autoinject` is optional

Example Command-Line with SCCM/MDT

Note

Prior to the Task Sequence with the command line to run Migration Manager, a Task Sequence Variable must be set for `OSDStateStorePath`. This variable must then be used to specify the data storage location for Migration Manager as sccm protects this location during the operating system reimaging. Failure to use a location that is not being protected during os reimaging for data storage will result in complete data loss.

Extraction

```
start /w MigrationManager.EXE /autoextract /allusers /personalitypath
%OSDStateStorePath% /hardlinks
```

Injection

```
start /w MigrationManager.EXE /autoinject /allusers /personalitypath
%OSDStateStorePath%
```

Migration Manager Exit Codes

Exit codes are used during Migration Manager automation to provide the technician performing the automation more information that can assist in resolving issues concerning the operation of Migration Manager.

Exit Code	Description
0	The operation was successful
4	The User Interface does not work with saved elevated credentials - it must be used with one of the following: `/autoextract`, `/autoinject`, or `/autobackup`.
5	Elevated Credentials failed. The method for saving Elevated Credentials was updated in 10.4 and credentials saved with earlier versions of Migration Manager are not compatible. Recreate encrypted storage of credentials by running the `/ELEVATEDCREDENTIALS` command (see Migration Manager User's Guide for usage).
12	Process aborted
13	The user canceled the operation
246	Unable to create domain user
248	Unable to open response file
251	No personalities exist for specified user on `/AUTOINJECT` command switch or Not all of the requested users could be found in any personality
252	No user exists for `/AUTOEXTRACT` command switch
253	Invalid command-line option
254	Improper installation
255	Insufficient rights to execute Migration Manager
256	`/Password` not supported with this type of personality storage
257	More than one matching personality exists for specified `/SOURCE` on `/AUTOINJECT` command switch

258	/SOURCE and /DATASTORE cannot be used at the same time
259	Personality file not found
260	Insufficient rights to migrate users not currently logged on.
261	Invalid response file
263	Password is out of range must be between 7-15 letters, numbers, and/or underscores ("_")
264	/AUTOEXTRACT and /AUTOINJECT cannot be used at the same time
265	Invalid password
266	Import file not found
267	Import parameter not correct
268	No content items were selected for extraction
269	Error processing password
270	Multiple personalities exist for specified user(s) on injection
271	Configuration file not found
272	Invalid configuration file parameter
273	Template file is obsolete
275	Invalid data store entry
276	Configuration file is read-only
277	Cannot create default configuration file
279	Cannot save configuration file
280	Cannot write to data store
284	Migration Manager is already running on this computer

286	No personalities exist for specified /SOURCE on /AUTOINJECT command switch
287	Invalid /EXCLUDEUSER parameter
288	Invalid /INCLUDEUSER parameter
289	Extraction failed
290	Injection failed
291	Source file not found for hardlinking
292	Multiple redirections to the same user
293	Server disconnected
294	An obsolete personality was specified
295	Invalid /DOMAIN usage. Source domain and target domain must be separated by a ":" Only valid with the /AUTOINJECT switch.
296	Domain usage conflict. Cannot use /DOMAIN with /INCLUDEUSER switch if /INCLUDEUSER contains user redirection
297	Invalid Exclude Disk Parameter
298	Invalid Data Store
307	Personality already exists at data store location
312	The Migration Manager engine was unable to allocate memory to complete the operation
313	Insufficient disk space to complete the operation, or data files may be too large for the datastore file system (FAT32 does not support > 4GB)
314	A file write error caused the operation to fail
319	The operating system denied access to the specified file
321	Personality file is read-only
322	Spaces are not allowed in the upload directory

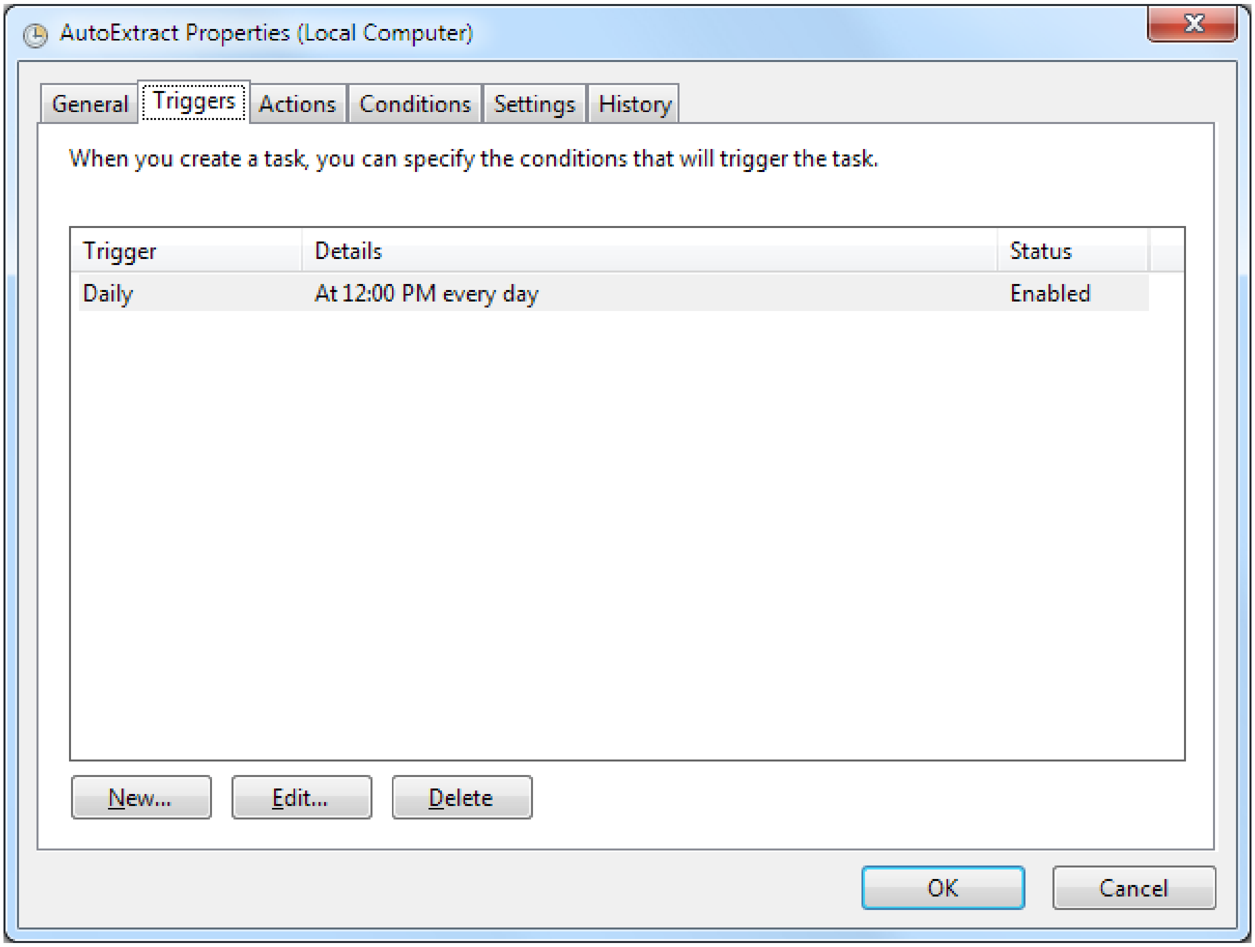
323	Insufficient file or directory permissions to access a personality file
324	Personality file is being used by another application
325	No personalities found.
326	Load user registry hive failed. If you are migrating users with roaming profiles, the cause is most likely that user account used to run Migration Manager doesn’t have access to the profile. Administrators should be granted access to the roaming profiles before they are created by enabling the group policy “Computer Configuration -> Policies -> Administrative Templates -> System/User Profiles -> Add the Administrators security group to roaming user profiles”
327	`/INJECTTOLOGGEDINUSER` can only be used with a single user.
328	File too large to migrate
330	The configuration file could not be read
332	The version of the specified personality is not compatible with the version of Migration Manager being used
333	The specified personality is corrupt and cannot be read
334	The extraction operation partially failed. This is almost always due to Migration Manager being denied access to a file during the extraction and is not uncommon to see for temporary files created during Windows update installations. The operation log contains information about the affected file(s).
335	The injection operation partially failed. This is almost always due to Migration Manager being denied access to a file when trying to write it to the target system. The operation log contains information about the affected file(s).
336	The rule file being imported is not a valid rule import/export file.
337	The evaluation license has expired.
338	All purchased license seats have been used.
339	The `/MAPPINGFILE` parameter must be used with the `/AUTOINJECT` parameter.
340	The `/MAPPINGFILE` parameter can’t be used with the `/SOURCE` parameter.
341	The mapping file specified either does not exist or can’t be read.

342	The mapping file specified does not contain a mapping for the computer where the injection is being performed.
343	The mapping file specified doesn’t contain valid mapping data.
344	The source computer name specified either through a mapping file using the /MAPPINGFILE parameter or through the /source parameter is not a valid computer name.
345	A local user could not be created because the default password defined in the Migration Manager configuration file doesn’t meet the password policy on the system.
346	An injection that requires a user profile to be written to a network location failed since the policy “Allow injections to network locations” policy is disabled.
347	64-bit executable only for running under Windows PE 64-bit. Use 32-bit executable for all other environments including 64-bit Windows.
348	The license used is invalid.
349	Unable to verify license.
350	Operation is not supported under Windows PE.
351	Unable to determine the MAC address.
352	/AUTOBACKUP use with /HARDLINKS is not supported.

Using Migration Manager With a Scheduler

Some Migration Manager license agreements allow for Migration Manager to be indefinitely used on the target PC. This means you can continue to use Migration Manager to perform regular backups of user data and settings. Using the standard scheduler that comes with Windows you can choose to have periodic extractions. For example the Windows scheduler will allow administrators to perform an extraction once every 4 weeks on Thursday at noon. You can also schedule tasks at logon, daily or monthly.

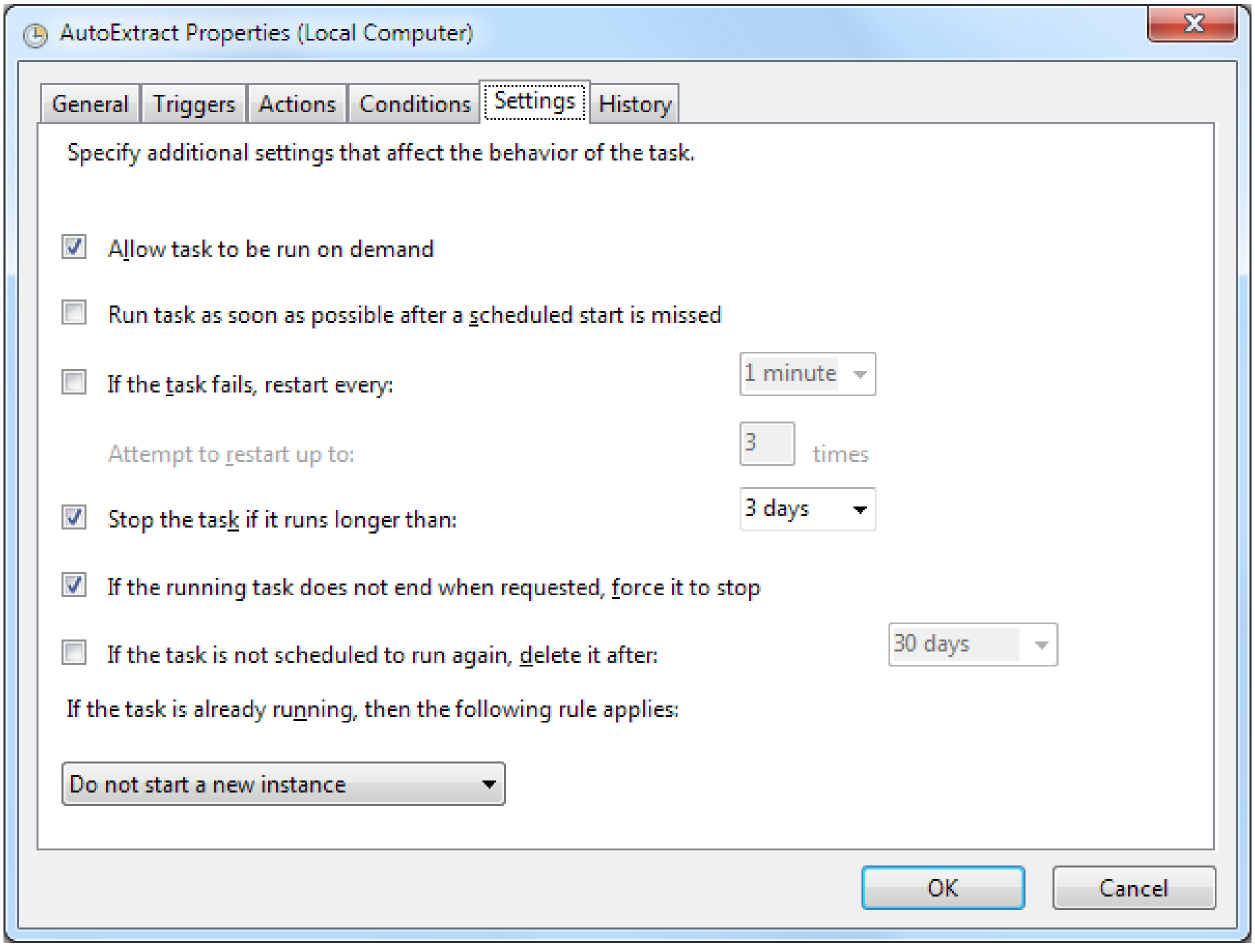
Here is a screen shot of a typical scheduled task that was created using the Windows 7 Task Scheduler:



When you create a task, you can specify the conditions that will trigger the task.

Trigger	Details	Status
Daily	At 12:00 PM every day	Enabled

There are also settings that can be modified to provide additional control over when scheduled tasks are executed. Below is an example of the settings available:



AutoExtract Properties (Local Computer)

Specify additional settings that affect the behavior of the task.

☑ Allow task to be run on demand

☐ Run task as soon as possible after a scheduled start is missed

☐ If the task fails, restart every: 1 minute

Attempt to restart up to: 3 times

☑ Stop the task if it runs longer than: 3 days

☑ If the running task does not end when requested, force it to stop

☐ If the task is not scheduled to run again, delete it after: 30 days

If the task is already running, then the following rule applies:

Do not start a new instance

Copyright and Patent Information

Tranxition Corporation
P.O. Box 42132
Portland, OR 97202
503-688-5046
www.tranxition.com