# CA Desktop Migration Manager

## Best Practices Guide

**12.9**

# CA Technologies Product References

This documentation set references to the following CA products:

- CA Advantage® Data Transport® (CA Data Transport)
- CA Asset Intelligence
- CA Asset Portfolio Management (CA APM)
- CA Business Intelligence
- CA Common Services™
- CA Desktop Migration Manager (CA DMM)
- CA Embedded Entitlements Manager (CA EEM)
- CA Mobile Device Management (CA MDM)
- CA Network and Systems Management (CA NSM)
- CA Patch Manager
- CA Process Automation
- CA Service Desk Manager
- CA WorldView™

# Contact CA Technologies

**Contact CA Support**

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

**Providing Feedback About Product Documentation**

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

# Contents

# Chapter 1: DMM Best Practices

CA DMM is a solution for migration, replacement, and recovery of operating system settings, application settings, and data files, collectively known as DNA.

The topics that follow help you determine the best method for creating a migration process in your unique enterprise environment. This guide contains information about planning and configuring an enterprise migration process. The guide addresses questions that are commonly asked to CA Technologies Technical Support.

**Accessing CA DMM**

Open CA DMM by selecting Start, Programs, CA, Desktop Migration Manager. From Start menu path, you can open any of the options.

**CA DMM Installation Path**

By default, CA DMM is installed in C:\Program Files\CA\Desktop Migration Manager. Throughout the documentation, this is termed as installation path.

## Planning the Migration Method

CA DMM supports two types of migrations. With either of these migration methods, CA DMM can be installed on the computer hard drive or it can be accessed from a central network location.

**Deferred Migrations**

Performing a deferred migration is considered best practice where one or more of the following situations exist:

- The source computer and the destination computer have the same hardware. The source computer is going to be 'wiped and reloaded' with a new operating system or applications.
- The DNA file can be created and saved to a storage device such as another computer, a server location (such as a file server, network appliance, or an Apache Web server), removable media for later retrieval.

**Real-Time Migrations**

Performing a real-time migration is considered best practice where one or more of the following situations exist:

- Two separate computers are involved and both exist on a common network.
- Two computers are involved and they can be connected directly to each other with a crossover cable.
- Two computers can have different hardware and operating systems.

  This method is the best solution when you are refreshing hardware and/or moving to a new operating system and/or applications.

# Requirements for Migrating Users with a Crossover Cable

When performing a real-time migration using a crossover cable, all of the user accounts, except local users, are orphan accounts. An orphan account is a user account that cannot be resolved at the time of migration. It becomes impossible to resolve orphan accounts because the systems are connected directly to each other and not to a network.

Therefore before you attempt the real-time migration using the crossover cable, create user profiles for all the users that you want to migrate on the destination computer. While the destination computer is connected to the network, create identical user profiles on the destination computer using standard Windows Administration Tools.

## Migrate Users Using a Crossover Cable

You can migrate NT domain and Active Directory user profiles during a crossover cable migration.

**Follow these steps:**

1. Create all the user profiles on the destination computer before you disconnect it from the network and before you begin the crossover cable migration.
2. Open DMM Options Editor from the Start menu.
3. Click the Open toolbar button, browse to the installation location of CA DMM, and then select DNAOptions.dox.

4. Click the User Profile branch.
5. Select Use existing profiles to resolve user destinations. (This option is not selected by default.)

   When you set this option, you can migrate orphan user profiles to match user profiles on the destination.

   When you do not set this option, you can perform a crossover cable migration (or any migration where resolution of the user account is not possible). Hence, CA DMM does not create the unresolved account, and the migration of those users fails.
6. Click Save and close DMM Options Editor.

## Considerations for Redirecting Using a Crossover Cable

You can also redirect users on the destination computer to different user names and NT domains or Active Directory accounts by explicitly naming each user that you want to redirect.

When the Check Use existing profiles to resolve user destinations option is checked in the DMM Options file, user migrations are processed differently than those for network migrations as follows:

- Wildcards resolve to the existing profile account paths only.
- No account or profile creation is attempted because only existing profiles are matched.
- Individual users that fail to match an existing profile are not migrated, and an error is recorded in the event log.

If you want to redirect source domain users to local users on the destination computer, redirect users to the local computer name in place of the domain name.

Additionally, in a crossover migration, most profile account paths display their domain as unknown because the migration process is unable to authenticate the domain or Active Directory. For this reason, specify ** as the destination path for best results.

# FIPS 140-2 Support

The Federal Information Processing Standard (FIPS) Publication 140-2, (FIPS PUB 140-2) is a U.S. government computer security standard used to accredit cryptographic modules. The standard is issued and maintained by the National Institute of Standards and Technology (NIST).

Computer products that use FIPS 140-2 accredited cryptographic modules in their FIPS-accredited mode can only use FIPS approved security functions such as AES (Advanced Encryption Standard), SHA-1 (Secure Hash Algorithm), and higher level protocols such as TLS v1.0 as explicitly allowed in the FIPS 140-2 standard and implementation guides.

Cryptography in Client Automation deals with the following aspects:

- Storage and verification of passwords
- Communication of all sensitive data between components of CA products, and between CA products and third-party products

FIPS 140-2 specifies the requirements for using cryptographic algorithms within a security system protecting sensitive but unclassified data.

Client Automation supports FIPS-compliant techniques for cryptography. Client Automation incorporates the RSA BSafe and Crypto-C ME v2.1 cryptographic libraries, which have been validated as meeting the FIPS 140-2 Security Requirements for Cryptographic Modules.

## Migration Methods and FIPS Compliance

CA DMM complies with FIPS 140-2 standards while performing real-time and deferred migrations.

**Real-time migration**

Protects the following using FIPS-compliant encryption:

- Data that is transferred between source and destination computers
- Password that is transferred from the destination computer to the source computer

**Deferred migration**

Provides an option to encrypt all the data captured in a DNA file using FIPS-compliant cryptography.You can configure this option when you create a DNA file.

## Supported FIPS Modes

CA DMM supports FIPS-compliant cryptography in two modes—FIPS-preferred and FIPS-only. You can select the FIPS mode while installing CA DMM. If you want to change the FIPS mode later, you need to reinstall CA DMM and select the required FIPS mode in the installer.

**FIPS-Only**

Specifies that only FIPS-compliant cryptography is allowed. This mode is not backward-compatible and you cannot access password-protected DNA files created using the previous releases of CA DMM.

**FIPS-Preferred**

Specifies that FIPS-compliant cryptography is preferred. This mode is backward-compatible and lets you access password-protected DNA files created using the previous releases of CA DMM. However, if you have a Client Automation installation on the computer, CA DMM will operate in the same FIPS mode as Client Automation. For example, if Client Automation is operating in the FIPS-only mode, CA DMM will also operate in the FIPS-only mode even though you have selected the FIPS-preferred mode. You can configure CA DMM to ignore the FIPS mode of Client Automation using a command line option. For more information, see the Reference Guide.

The default FIPS mode is FIPS-preferred and the mode of operation is decided at run-time based on the following table:

| CA DMM Installation | Client Automation is in FIPS-Only Mode | Client Automation is in FIPS-Preferred Mode |
|---|---|---|
| CA DMM is installed in FIPS-only mode or the /FO option is set through CLI | Runs in FIPS-only mode | Runs in FIPS-only mode |
| CA DMM is installed in FIPS-preferred mode or the /IFM option is set through CLI | Runs in FIPS-preferred mode | Runs in FIPS-preferred mode |
| CA DMM is installed in FIPS-preferred mode and did not receive the /IFM option through CLI. | Runs in the same FIPS mode as Client Automation that is FIPS-only mode | Runs in the same FIPS mode as Client Automation that is FIPS-preferred mode |

## Operating in FIPS-Only Mode

To help ensure that the entire organization is operating CA DMM in FIPS-only mode, you must install CA DMM in FIPS-only mode. If users are executing CA DMM from a shared location, you must do one of the following so that CA DMM always operates in FIPS-only mode:

- Provide the /FIPSONLY switch through the CLI in the options file along with the other relevant options. For more information about this switch, see the *Reference Guide*.
- Verify that Client Automation is installed in FIPS-only mode of operation on computers where CA DMM in installed.
- Verify that the Settings.xml file in the shared folder is from a FIPS-only installation.
- Select the FIPS-only mode of operation using the Options Editor. For more information, see the *Options Editor Help*.

## How to Switch to FIPS-Only Mode

You can switch from the FIPS-preferred mode to the FIPS-only mode if you want to use only FIPS-compliant cryptography. Perform one of the following steps to switch to FIPS-only mode:

- Provide the /FIPSONLY option through CLI
- Change the FIPS mode of your Client Automation installation to FIPS-only
- Reinstall CA DMM and select the FIPS-Only mode
- Change the Settings.xml file in the *install_path* of CA DMM to match the Settings.xml file of a FIPS-only installation.

**Note:** We recommend that you take a backup immediately after switching to the FIPS-only mode as you cannot open password-protected DNA files created using the previous releases of CA DMM.

## How to Switch to FIPS-Preferred Mode

You can switch from the FIPS-only mode to the FIPS-preferred mode if you want to open a password-protected DNA file created using the previous releases of CA DMM. Perform one of the following to switch to FIPS-preferred mode:

- Reinstall CA DMM and select the FIPS-Preferred mode
- Change the Settings.xml file in the *install_path* of CA DMM to match the Settings.xml file of a FIPS-preferred installation.

## Protect a DNA File Using FIPS-Compliant Encryption

Use FIPS-compliant encryption to protect the data in a DNA file. Encrypting the DNA file helps ensure that only an authorized person or program can open and apply the DNA file.

**To protect a DNA file using FIPS-compliant encryption**

1. Open CA DMM.

   The Select a DMM Task page appears.

2. Click Create.

   The Select Users for Migration page appears.

3. Follow the instructions in the wizard until you get the Store to DNA File page.

4. In the Store to DNA File page, click Advanced, and select Use FIPS compatible cryptography to encrypt data (safest).

   The Enter Key Path button is enabled

5. Click Enter Key Path and specify the location where you want to store the encryption key.

   The specified location is configured to store the encryption key. You need this key to open or apply the DNA file.

6. Click OK.

   The settings are saved.

7. Click Next.

   The Waiting to Process page appears.

8. Click Start Store.

   The migration process stores and encrypts the data using FIPS-compliant encryption. Once the migration is complete, the encrypted DNA file and the encryption key are available in the location you specified while creating the DNA file.

## Rights and Permissions

When performing migrations, it is best practice for the logged on user to have Administrator privileges. However, each migration process is unique, so be aware of the functions available only if the user has Administrator privileges.

To perform the following functions during a migration, you must use an administrative sign-on:

- Crossover cable migrations (two systems are connected directly to each other with a crossover cable)
- Migration of NTFS (file and folder) security settings
- Migration of group security
- Migration of multiple users, and when migrating one or more users to a new or different domain.

  In the case of migrating users to new or different domains, you must have domain administrator privileges. Users can be created on the new system when performing the operation with the correct access level.
- Migration of printers requires at least power user access.
- Migration of applications (the application itself is being migrated).
- Migration of user settings the end user cannot change manually, such as the Netscape user profile. (Non-administrative users do not have permission to change settings in the HKEY_LOCAL_MACHINE registry item.)
- Apply a self-extracting DNA file

**Note:** In DMM Options Editor, you must be signed on as an administrator or power user. However, you can edit a DMM options in XML format in an editor, such as notepad with these rights.

## Close All Applications and Services

The only application running during a migration should be CA DMM. Maximum performance is realized when more local resources are available to CA DMM. The most common applications to cause interference with a migration are those trying to control access, such as virus scanners.

Deployment tools, application wrappers, assessment tools, and other migration process applications or tools rarely cause conflicts when performing a migration.

# Open File Migration

CA DMM provides support for migrating open and locked files. The ability to migrate open and locked files eliminates the need to close the corresponding applications before starting the migration. As a result, no interruption in work takes place and you can continue working on the files even while performing the migration.

You can migrate open and locked files using deferred migration and real-time migration modes. In deferred migration mode, you back up open and locked files into a .dna file (or a self-extracting file). In real-time migration mode, you directly migrate open and locked files from a source computer to a destination computer.

**Note:** CA DMM supports migration of open and locked files on 32- and 64-bit Windows XP, Windows Vista, and Windows 7 operating systems.

## Considerations for Open File Migration

Make sure that you consider the following points while migrating open and locked files:

- While performing the migration, if a file is found to be open at the destination computer, the file is not considered for migration. For example, if a .ppt file is open at the destination computer, the .ppt file is not migrated.

  The event log contains information about all the files that have not been migrated because of being open at the destination computer. You do not receive any UI message in this context.
- If CA DMM fails to migrate open and locked files and logs the error in the event log, you can try the following steps to troubleshoot the error:
  - Check that the Volume Shadow Copy Service (VSS) and its dependencies are not disabled.
  - Review the troubleshooting article available at the Microsoft website http://support.microsoft.com/kb/940184.
- Backup of the FAT32 systems is possible only if you have at least one valid NTFS partition on the same disk.

# Dynamic Drive Exclusion

You are able to dynamically exclude drive types from a migration process. CA DMM migrates files and folders designated by filter processing and script processing, even if those files and folders reside on mapped network drives, removable drives, and so on.

The following examples illustrate how you might use dynamic drive exclusion:

- Suppose users store their main .pst files on a network drive that is mapped on their PC, and they may have additional .pst files saved locally. You want to move only the .pst files that are saved locally. Additionally, you do not want to migrate any files that are located on a network drive. Because .pst files are moved by the MS Outlook script, creating an exclude filter will not be sufficient. You must enter a drive exclusion.
- Suppose you create a migration process that saves the DNA file on a Flip2Disk, and do not want this drive included in any migration processing.
- Suppose you do not want UNC paths included in any migration processing.

To support this function, the following variables are supported in the Desktop DNA exclude.dnax file:

**%DNA_FIXED_DRIVES%**

Excludes all local drives from the migration.

**%DNA_REMOVABLE_DRIVES%**

Excludes all removable drives from the migration.

**%DNA_NETWORK_DRIVES%**

Excludes all network drives and network locations from the migration (mapped drives).

**%DNA_DDNA_DRIVE%**

Excludes the drive CA DMM is running from, this allows for removal flash RAM, Flip2Disk, and other items to be excluded from the migration process.

**%DNA_UNC_PATHS%**

Excludes the UNC paths from the migration.

**%DNA_DDNARUN_FOLDER%**

Excludes the path where CA DMM is running from the migration process.

You can include these special variables to support subdirectories and files.

Returning to the .pst example, to exclude any network drives where .pst files might be stored, include the following in the Desktop DNA exclude.dnax file:

```
%DNA_NETWORK_DRIVES%\Outlook\*.pst
```

To include any of these variables in the Desktop DNA exclude.dnax file, follow these steps:

1. Open Windows Explorer on the computer where CA DMM is installed, and navigate to the following file:

   *installation path*\Desktop DNA exclude.dnax

2. Right-click the Desktop DNA exclude.dnax file, and then select Open or Open With Notepad.

   Notepad opens.

3. Scroll down to the end of the file.

4. Enter the drive exclusion or exclusions you require.

5. Click File, Save.

6. Close Notepad.

   CA DMM will exclude any of the variables you include for all users you migrate.

## Filters: Preserve Directory Structure

When you migrate files using a filter, you can redirect the contents of the filter to a new location on the destination. If you redirect filters on the destination, use the following directions when creating the migration template in DMM Template Editor:

1. Click Filters, and define the criteria for the filter on the Name and Type, Date and Size, and Redirection tabs.

   The fields available for each tab appear as you click the tab.

2. Select the Redirect to This Folder check box on the Redirection tab, and then specify a new path to store the files migrated with this filter.

3. Select the Preserve Directory Structure check box if you want to preserve the directory structure of the files.

   The Preserve Directory Structure option migrates the files to the same path they were saved on the source computer. For example, the DNA file has a filter to save all *.hlp files from the source system. You redirect this filter to C:\Help on the destination. Depending on your selections, the following can result:

   - If you check the Preserve Directory Structure option, the files are saved as: *installation path*\DesktopDNA.hlp
   - If you clear the Preserve Directory Structure option, the files are saved as: C:\Help\DesktopDNA.hlp

   **Note:** If you clear the Preserve Directory Structure option, you should use the Overwrite option to control any situation where duplicate files might be encountered.

4. Click Create Filter.

## Filters: Overwrite

The Overwrite options determine when to overwrite duplicate files. There are two overwrite options available.

**Migration Overwrite**

Determines when to overwrite duplicate files when performing a migration where the DNA file **does not** contain revisions. The valid values are Always, Newer, or Never. The default for this option is Newer.

**Revision Overwrite**

Determines when to overwrite duplicate files when performing an apply from a DNA file containing revisions. The valid values are Always, Newer, or Never. The default for this option is Always.

When the Overwrite option is set to Newer, CA DMM checks the file version to determine which file is the newest file if duplicates are encountered. If duplicate versions of a file exist, CA DMM increments the files. For example, two files exist with the same version number Expenses.xls. Both files are saved and named Expenses01.xls and Expenses02.xls

When the Overwrite option is set to Always, CA DMM always applies the file contained in the DNA file.

## Filters: Include, Exclude, Omit, and Always Omit

You can create filters for data files and for document extensions associated with applications. CA DMM can process filters using wildcards, by data, by size, or location. You can define filters as Include, Exclude, or Omit filters. Exclude filters always take precedence over Include filters.

You can use environment or DMM variables when you create filter criteria or redirect a filter.

It is important to note the following about the include, exclude, and omit filter criteria:

- Include filters include the files matching the filter criteria defined.
- Exclude filters exclude the files matching the filter criteria from the migration wherever the file may have been selected, either through a filter or by selecting it directly on the Select Files and Folders page.
- Omit filters omit the defined criteria from the filter they are associated with.
- Always omit filters omit the defined directories from **all** filter processing.

## Create an Include Filter

You can create include filters to include the files matching the defined filter criteria. You can use the DMM Template Editor to create an include filter.

**To create an include**

1. Open DMM Template Editor from the Start menu.

   DMM Template Editor opens.

2. Click the Filters branch.

   The Filters page appears. Include is selected by default. You can define the criteria on any of the three tabs, Name and Type, Date and Size, or Locations. The filter you create includes all files that meet the defined criteria.

3. When you have defined the filter, click Create Filter.

   The filter is added to the list of filters for the migration.

## Create an Exclude Filter

Exclude filters exclude the files matching the filter criteria from the migration wherever the file may have been selected, either through a filter or by selecting it directly on the Select Files and Folders page. You can use DMM Template Editor to create an exclude filter.

**To create an exclude filter**

1. Open DMM Template Editor from the Start menu.

   DMM Template Editor opens.

2. Click the Filters branch.

   The Filters page opens.

3. Click the Exclude option button.

   You can define the criteria on any of the three tabs, Name and Type, Date and Size, or Locations. The filter you create excludes all files that meet the defined criteria from the migration processing.

   **Note:** Exclude filters exclude files matching the filter criteria from migration processing independently of where the file was selected for migration. For example, if you create a filter to exclude all .mp3 files from the migration, even if you explicitly select an .mp3 file on the Select Files and Folders page, no .mp3 files will be migrated.

4. Click Create Filter.

   The filter is added to the list of filters for the migration.

## Specify Omit Criteria

Omit filters omit the defined criteria from the filter they are associated with. Use DMM Template Editor to create an omit filter.

**To specify omit criteria**

1. Open DMM Template Editor from the Start menu.

   DMM Template Editor opens.

2. Click the Filters branch.

   The Filters page appears.

3. Click the Locations tab.

   The fields on the Locations tab appear.

4. Click Add in the Omit the Following Folders group box.

   The Omit Folder dialog appears.

5. Enter a path or use the Browse button in the Path to Omit field to specify the folder you want to omit from the filter search.

   **Note:** Clear the Omit all subfolders check box if you do not want to omit the subfolders of the specified folder from the filter search.

6. Click Create Filter.

   The filter you created matches the criteria defined and searches everywhere but in the omitted path. This omit criteria is specific only to the defined filter.

## Specify Always Omit Criteria

Always omit filters omit the defined directories from all filter processing. Use DMM Template Editor to create an always omit filter.

**To specify always omit criteria**

1. Open DMM Template Editor from the Start menu.

   DMM Template Editor opens.

2. Click the Filters branch.

   The Filters page appears.

3. Click Always Omit.

   The Always Omit Folders dialog appears.

4. Click Add.

   The Omit Folder dialog appears.

5. Enter a path or browse to the path of the folder you want to omit from the filter search in the Path to omit field.

   **Note:** Clear the Omit All Subfolders check box if you do not want to omit the subfolders of the specified folder from the filter search.

6. Click OK.

   The Omit path you have defined is added to the list of Always Omit Folders. You can view this list by clicking Always Omit.

   **Note:** You can add multiple paths to omit from the filter processing.

   Always Omit filters omit the defined paths from all filter processing.

## Create a Selective Apply Process with Templates

There can be situations where you may not want to apply everything saved in a DNA file. To automate a selective Apply using a template created specifically for the apply side of the migration, follow these steps:

1. Create a template to save the DNA file.

   The template should contain everything you want saved into the DNA file from the source computer.

2. Create a separate template for the destination.

   This is necessary because everything saved in a DNA file is selected to apply to the destination computer by default. You can create a unique destination template by opening the template you will use for the apply, and removing any selections you do not want applied to the destination from the Users, System, Applications, Files, and Filters branches of the tree located in the left pane of the DMM Template Editor.

3. To redirect any of the users, applications, or files to be applied from the DNA file, click the branch, and then click the Redirection tab to define the redirection in the left pane of the DMM Template Editor.

4. Save this template with a different name.

5. Open the DMM Options Editor from the Start menu.

   DMM Options Editor opens.

6. Click File, Open or click the File Open toolbar button. Browse to the folder where CA DMM is installed and select the DDNAOptions.dox file.

7. If you have not run DesktopDNA.exe, click File, New.

8. Click Advanced in the left pane of the DMM Options Editor.

   The advanced DMM Options appears in the right pane of the DMM Options Editor.

9. Locate the option: Open DNA file with No Items Selected. If this option is set to True, the DNA file is loaded with no items selected to migrate. This lets you open a template and apply only what is selected in the template (selective apply).

   This option is set to False by default.

10. Check Open DNA file with No Items Selected check box to change the setting to True.

11. Save the DDNAOptions.dox file with a different name.

12. When you run the destination migration (if you created a new DMM Options file instead of editing the existing DMM Options file), you must pass this new DMM Options file with the command line. The syntax is:

    ```
    "Path to the DesktopDNA.exe file" /O "Path and file name of the new DDNAOptions.dox file"
    ```

For more information on creating and using the DMM command line, see Command Line Interface.

# Merging or Selecting Multiple Templates

When creating templates for a large enterprise with diverse migration needs it is often easier to establish a master enterprise-wide template and separate templates for each business unit or department. The master template can be merged into one template or the two templates can be passed together on the command line. Both processes are additive. You need only decide which method best meets your migration needs. Directions for both methods are detailed following.

## Merge Templates

To merge the templates, follow these steps:

1. Create a template file containing only the items you know may need to be migrated for every business unit.

2. Save the template as follows if you are creating a master template from an existing template:

   - Click Options, Save Options.
   - In the Save Options dialog, clear everything except those items you want to save for a master template.

3. Save the template.

4. Create the Template file with the business unit or departmental details.

   This template should include any additional system or application settings and data that may be unique to the business units.

5. Click File, Merge before saving the comprehensive template file.

   A browse dialog lets you browse to the location of the master template. When you select the template to merge, it merges the master template with the business level selections you made.

6. Save this file to use for the business or department level migration.

### Select Multiple Templates

If you choose to pass two or more templates on the command line at the time of migration, follow these steps:

1. Determine if you will select the templates in the CA DMM user interface at the time of migration, or create a command line as part of an automated process.

   - If you choose to select the template in the CA DMM user interface at the time of migration, see the CA DMM help file, and from the table of contents select the following path:

     `CA Desktop Migration Manager \ Deferred Migration \ Create a DNA File \ Start Tab \ Open a Template File.`

   - If you choose to pass the two (or more) templates on the command line as part of an automated process, use the following step.

2. Use the template command line switch, /T many times as in the following example:

   ```
   /D "C:\MyDNAFile.dna" /T "C:\Template 1.dtf" /T "C:\Template 2.dtf" /T "C:\Template 3.dtf"
   ```

   In this example, if any of the templates contain conflicting information, Template 3 has precedence over Template 2, which has precedence over Template 1.

# Managing Recovery

DMM Always Current Scheduler provides the means to ensure that your enterprise DNA files are regularly stored so that if problems arise, such as unexpected hardware failure, users can recover their systems using a current version of their DNA file.

## Schedule a DMM Task

To schedule a DMM storage task, follow these steps:

1. Start DMM Always Current Scheduler from the Start menu.

   The DMM Always Current Scheduler opens.

2. Click Next and follow the tasks in the wizard.

The wizard asks you to do the following:

- Create a task and identify the DNA you want to store.
- Specify details about the task, including the name of the template, and the name of the user under which this task runs.

  **Note:** When specifying the name of the user under which the task runs, CA DMM uses values from the registry to provide the user name. Be sure that the information is correct (user name, including domain, and password) or the job will not run. Also, if you are required to change your password at regular intervals, you must change the password for the task. The scheduled task will fail to run until you change the password.

- Specify how often the task runs.
- When the task should run

3. Click Finish after you review the details about the task.

   The first time the task runs, it creates the specified DNA file. At the next scheduled run it creates a revision to the DNA file.

   When the task runs, it displays a dialog that lets you choose to reschedule the task or cancel it. If you choose to reschedule, DMM Always Current Scheduler opens and you can choose an alternate time. If you choose cancel, the task does not run until its next scheduled time.

**Note:** The DMM Always Current Scheduler creates an XML file (with the .dmx extension) that contains the settings. By default it stores the file in your My Documents directory. You can open this file using DMM Options Editor and make changes if you like.

## View Scheduled DMM Task

**Follow these steps:**

1. Open the Windows Scheduler from the Start menu.

   The Windows Scheduled Tasks dialog opens to display the DMM Scheduled Tasks.

2. Double-click a task to modify the schedule settings.

   Windows Scheduler opens; you can modify the scheduled task.

3. Click OK when you have completed the modifications.

   The changes to the scheduled task are saved.

## Apply DNA from Storage

**Follow these steps:**

1. Execute Apply DNA from Storage command from the Start menu.

   The CA DMM wizard opens displaying the DNA File Options page.

   **Edit**

   Select what settings are applied. You can proceed through the CA DMM wizard to select individual settings, files and folders, or filters to apply.

   **Destination**

   Opens the Destinations tab. You can apply everything that is stored in the DNA file. You can also define redirection for settings, files, and folders or filters, if you choose.

   **Revision**

   Select a different DMM revision. You can select a previous version of the DNA file and can select individual settings, files and folders, or filters to apply, allowing you to roll back to a specific point in time.

2. Follow the rest of the CA DMM wizard instructions to complete the application of the stored DNA.

**Note:** You can use the /RD parameter to apply a revision. For more information, on command-line parameters and examples, see the *Reference Guide*.

# Tips to Optimize Time and Resources

The topics that follow will help you to determine the best method for creating a migration process in your unique enterprise environment. Each topic has best practice suggestions to help you optimize performance of the migration process.

## Reduce Time of Multiple User Migrations

In some migration scenarios, you might increase the speed of your migration by changing the Detect scripts as every selected user option to false on the Advanced tab of the DMM Options file. This setting is true by default. CA DMM detects scripts for each user profile selected for migration unless you change this option to false.

Loading user profiles for all users selected for migration can be a time consuming process. On the source system, CA DMM must verify the accounts exist on the domain or Active Directory for use later in the migration process. Then each user profile selected for migration must also be loaded and detection for the scripts evaluated for each user in succession.

On the destination computer, CA DMM must verify each account exists, and if necessary, create any user accounts or profiles for the selected users. Then, CA DMM must detect application scripts for each user on the destination to resolve application destination paths. The application detection occurs when opening a DNA file on the destination or when opening the Application Destination page.

In contrast, when you are migrating only the current user, detection is much faster for the following reasons:

- Current user migrations are using the currently loaded user profile.
- The current user is already resolved, and there are no additional users to verify.
- The Detect function included in the scripts only needs to run once for each script for the one user profile. Additional user profiles are not loaded.

Because current user detection runs much faster, it can be substituted for multi-user detection in most cases because the majority of scripts Detect functions are based only on the local computer registry settings and do not vary from user to user. Additionally the majority of the scripts detect functions do not change the state of the computer during detection.

The exceptions to this rule that makes multi-user detection necessary for some scripts are:

- Some scripts (listed below) use current user settings and shortcuts to resolve application paths and detect system features. Each user must be loaded to resolve the shortcuts and application paths.
- Some scripts change the state of the computer to migrate settings from the source to the destination in real-time migrations.

The scripts that use multi-user detection to migrate settings are like:

- The Internet Explorer script exports user certificates for each user.
- The Dial Up system script migrates phonebook information in the registry for each user.
- The Printers system script migrates the printer setup and is dependent on user specific files on the source system.

If you are not migrating the settings for Internet Explorer, Dial Up system settings, or Printers for multiple users, or performing real time migrations, you can safely turn off the multi-user detection option, and increase the performance of CA DMM.

## Multi-User Detection Option

The following option was added to turn off the Detect scripts for every selected user option when performing migrations. This option should only be modified if you have evaluated your migration process with the information provided to ensure it will not impact your migration results.

| Name | Explanation | Comment | Valid Values | Dependency |
|---|---|---|---|---|
| Detect scripts as every selected user | Do you want to detect system and application scripts based on settings for all selected users or only on the currently selected user? | If false, detection for multiuser migration finishes faster on slow systems with the potential of not detecting some user-specific settings in rare cases. Use true to guarantee that all possible settings are displayed.<br>**Note:** Some older scripts might require multiuser detection to function properly. | 1 = True<br>0 = False<br>Default value is True. | None |

## Change Detect Scripts Setting

To change the default Detect Scripts settings using DMM Options Editor, follow these steps:

1. Open the DMM Options Editor from the Start menu as follows:

   Start, Programs, CA, Desktop Migration Manager, Migration Toolkit, DMM Options Editor

   DMM Options Editor opens.

2. Click the File Open toolbar button. Browse to the folder where CA DMM is installed and select the DDNAOptions.dox file.

   The DMM Options file opens in the DMM Options Editor.

3. Click the Advanced branch.

   The Advanced options appear in the right pane of the DMM Options Editor.

4. Scroll down to the Detect scripts as every selected user option, clear the check box.

   The Detect scripts as every selected user is not checked. Be sure you have evaluated the impact of changing this option.

5. Click the Save toolbar button.

   The change is saved.

6. Close the DMM Options Editor.

   The next time you run CA DMM, it will use this setting and not detect scripts as every selected user during the migration.

## Access CA DMM from a Local Drive

Networks are generally not as fast as hard drives and can also have bottlenecks or unpredictable traffic that will limit migration speed. Whether you are performing a real-time migration (streaming data over the network) or performing a deferred migration (creating a DNA file to a network location), you can achieve better performance by running the CA DMM application from an installed location on the local system hard drive.

## Script Directory Option

If you have created customized or proprietary scripts for your enterprise, you are able to install the custom scripts for a migration process, even if you are installing CA DMM locally.

There are two different ways to install custom scripts:

1. You are installing CA DMM directly (without using DMM Director)
2. You are installing CA DMM inside of a DMM Director process

### Install Custom Scripts Directly

To install custom scripts by installing CA DMM, follow these steps:

1. Locate the directory where the CA DMM install folder has been copied from the install CD. This folder is named DDNAInst.
2. Create two subfolders named System Scripts and Application Scripts in the DDNAInst directory.

3. Copy your custom system scripts into the System Scripts subfolder you created in the DDNAInst directory.
4. Copy your custom application scripts into the Application Scripts subfolder you created in the DDNAInst directory.

The next time you run the installer from the modified DDNAInst directory, the installer merges the custom scripts with the standard DMM scripts and installs them on the system. If you have any scripts with duplicate names, the installation process replaces any of the standard DMM scripts with the custom script that has the same name.

When you install CA DMM using the installer user interface, the Scripts component displays for selection in the Select Components page of the installer. The scripts are selected for installation by default. If you choose to do a custom installation, you can deselect the scripts from the installation. If you deselect installing the scripts from the Select Components page, only the scripts you added to the appropriate directories are installed. You may want to deselect the scripts if you want to install only the custom scripts you have defined.

## Install Custom Scripts Using DMM Director

To install custom scripts when using a DMM Director process, follow these steps:

1. Locate the directory where DMM Director created the DirectorMigration folder.
2. In the ddnarun directory, there are two subfolders named System Scripts and Application Scripts.
3. Copy your custom system scripts into the System Scripts folder located in the DirectorMigration\ddnarun\system scripts directory
4. Copy your custom application scripts into the Application Scripts folder located in the DirectorMigration\ddnarun\application scripts directory.

The next time you run a DMM Director process that specifies CA DMM will be installed locally before running the migration, the installer merges the scripts you placed in the two directories with the standard CA DMM scripts. If you have any scripts with duplicate names, the installation process replaces any of the standard DMM scripts with the custom script.

## Create and Apply files from the Local Drive

If there is enough free space on the source system's hard drive, you can create the DNA file on the hard drive. After the file has been created, copy or move it to any network location. This is usually faster than having CA DMM save the DNA file directly to the network location.

When Applying, if the destination system has a large amount of free space on the hard drive, copy the DNA file to the local drive. Run CA DMM from the local computer, and use the local copy of the DNA file.

## Turn Off Compression

The compression setting determines how CA DMM compresses the DNA files created. CA DMM uses standard PKZip file compression technology to compress the data in a DNA file. Not all files compress with equal success. Compressing an already compressed file takes more time and can actually be larger after the file is compressed.

The compression options are:

**None**

Select this option to prevent compressing a DNA file. This is also the best selection if you are performing a real-time migration and your network environment is capable of handling the increased traffic.

**Quickest**

Select this option to compress a DNA file in the quickest way without checking to ensure it will be the smallest size possible.

**Smallest**

Select this option to ensure the smallest possible DNA file size.

**Note:** Compressing and decompressing information takes time. If you have enough space on your hard drive, performance is optimized if you turn compression off before creating your DNA file.

If you are using the CA DMM user interface, follow these steps:

1. Click Options, Settings.

   The DMM Settings dialog appears.

2. Select None in the Compression group box, and click OK.

   The migrations you perform with this instance of CA DMM use the compression setting you defined.

If you are using an options file, follow these steps:

1. Open the DMM Options Editor from the Start menu.

   DMM Options Editor opens.

2. Click File, Open or click the File Open toolbar button. Browse to the folder where CA DMM is installed and select the DDNAOptions.dox file.

   **Note:** If you have not run DesktopDNA.exe, click File, New to create the file.

3. Click General in the left pane of the DMM Options Editor.

   All the General options appear in the right pane of the DMM Options Editor.

4. Locate the option: Compression.

   This option determines what compression level is used when creating a DNA file. The valid values are None, Quickest, and Smallest. CA DMM defaults to Quickest.

5. Change the setting to None.

6. Save the DDNAOptions.dox file.

   The compression setting is set to None.

## Turn Off Verification

The Verification option enables or disables whether the contents of the DNA file is verified against the original source files and registry items. If you have a reliable network, you can turn off the verification.

**Note**: The Verification option is set to off by default.

**Follow these steps:**

1. Open the DMM Options Editor from the Start menu.
2. Click File and then the File Open toolbar button.
3. Browse to the folder where CA DMM is installed and select the DDNAOptions.dox file.

   **Note:** If you have not run the DesktopDNA.exe, click File and then New to create the file.

4. Click Advanced in the left pane of the DMM Options Editor.

   All the Advanced options appear in the right pane of the DMM Options Editor.

5. Locate the Verify DNA file option.

**Note:** When you set verify DNA file option to True, it adds checksums to the DNA file, lets you perform a sure verification using the DMM Explorer. Also, execute a fast verification in CA DMM at the end of the deferred migration process.

This option is set to False by default.

If this option is already selected, clear the check box to turn off the Verify DNA file option.

6. Save the DDNAOptions.dox file.

   The verification setting is turned off.

## Create Undo Logs on the Local Drive

When performing migrations, undo logs can get large. The efficient method is to designate the local drive for the creation of the Undo file, provided space is available. After the migration and completion of the Undo file, it can be moved to a network location.

**Follow these steps:**

**CA DMM user interface**

1. Click Options, Logs
2. Change the path to save the undo file.
3. Click OK.

   The undo file is saved by default to the local My Documents folder.

**Options File**

1. Open the DMM Options Editor from the Start menu.
2. Click File and then the File Open toolbar button.
3. Browse to the folder where CA DMM is installed and select the DDNAOptions.dox file.

   **Note:** If you have not run the DesktopDNA.exe, click File and then New to create the file.
4. Expand the Logging node in the left pane of the DMM Options Editor.
5. Select the Undo Log subnode.

   The Undo Log options appear in the right pane of the DMM Options Editor.
6. Change the option Path to save Undo log.
7. Save the DDNAOptions.dox file.

   The path of the Undo log file is changed.

## Turn Off Undo Logs

To undo logs, can be large. If you have created a backup image of your systems before the migration, turn off the Undo Log option.

**Follow these steps:**

**CA DMM user interface**

1. Click Options, Logs.
2. Uncheck the Undo group check box to disable the creation of an undo file.
3. Click OK.

**Options File**

1. Open the DMM Options Editor from the Start menu.
2. Click File and then the File Open toolbar button.
3. Browse to the folder where CA DMM is installed and select the DDNAOptions.dox file.

   **Note:** If you have not run the DesktopDNA.exe, click File and then New to create the file.
4. Expand the Logging subnode in the left pane of the DMM Options Editor.
5. Select the Undo Log subnode.

   The Undo Log options appear in the right pane of the DMM Options Editor.
6. Uncheck the Create Undo Log option to turn off the creation of an Undo log file.
7. Save the DDNAOptions.dox file.

   Creation of the Undo log file is disabled.

## Turn Off Authenticate Domain User Profiles

You can turn off the Authenticate Domain User Profiles option to optimize the performance. If you disable this option, the domain user profiles that are selected for migration are not authenticated by their domain manager.

**Follow these steps:**

1. Open the DMM Options Editor from the Start menu.

2. Click File and then the File Open toolbar button.
3. Browse to the folder where CA DMM is installed and select the DDNAOptions.dox file.

   **Note:** If you have not run the DesktopDNA.exe, click File and then New to create the file.
4. Click Security Migration in the left pane of the DMM Options Editor.

   The Security Migration options appear in the right pane of the DMM Options Editor.
5. Locate the Authenticate Domain User Profiles option.

   **Note:**

   - The Authenticate Domain User Profiles option allows the domain server to authenticate the domain user profiles.
   - The valid values are Never, Always, and Never in crossover cable migration.
   - CA DMM defaults to Never in crossover cable migration.
6. Change the setting to Never.
7. Save the DDNAOptions.dox file.

   The domain server does not authenticate the domain user profiles.

## Turn Off Manifest Log

The manifest log file is an XML-based file that captures the detailed contents of a migration. The Manifest log option determines whether you want to create a manifest log when a DNA file is stored or applied. For performance enhancement, ensure that this option is disabled.

**Follow these steps:**

1. Open the DMM Options Editor from the Start menu.
2. Click File and then the File Open toolbar button.
3. Browse to the folder where CA DMM is installed and select the DDNAOptions.dox file.

   **Note:** If you have not run the DesktopDNA.exe, click File and then New to create the file.
4. Click Logging, Manifest Log in the left pane of the DMM Options Editor.

   The Manifest Log options appear in the right pane of the DMM Options Editor.

5. Locate the Create Manifest Log option.
6. Uncheck the Create Manifest Log option.
7. Save the DDNAOptions.dox file.

   Creation of the Manifest log file is disabled.

## Turn Off Debug Log

The Debug Log option allows you to specify whether you want to create a debug log when a DNA file is applied to a destination computer. However, to optimize the performance, ensure that this option is not selected.

**Follow these steps:**

**CA DMM user interface**

1. Click Options, Logs.
2. Click Advanced.
3. Ensure that the Debug log group check box is not selected which disables the creation of a debug log file.
4. Click OK.

**Options File**

1. Open the DMM Options Editor from the Start menu.
2. Click File and then the File Open toolbar button.
3. Browse to the folder where CA DMM is installed and select the DDNAOptions.dox file.

   **Note:** If you have not run the DesktopDNA.exe, click File and then New to create the file.
4. Click Logging, Debug Log in the left pane of the DMM Options Editor.

   All the Debug Log options appear in the right pane of the DMM Options Editor.
5. Uncheck the Create Debug Log option.
6. Save the DDNAOptions.dox file.

   Creation of the Debug log file is disabled.

# Turn Off Network Log

The Network Log option determines whether you want to create a network log when performing a real-time migration. However, to optimize the performance, ensure that this option is disabled.

**Follow these steps:**

**CA DMM user interface**

1. Click Options, Logs.
2. Click Advanced.
3. Ensure that the Network log group check box is not selected which disables the creation of a network log file.
4. Click OK.

**Options File**

1. Open the DMM Options Editor from the Start menu.
2. Click File and then the File Open toolbar button.
3. Browse to the folder where CA DMM is installed and select the DDNAOptions.dox file.

   **Note:** If you have not run the DesktopDNA.exe, click File and then New to create the file.
4. Click Logging, Network Log in the left pane of the DMM Options Editor.

   All the Network Log options appear in the right pane of the DMM Options Editor.
5. Uncheck the Create Network Log option.
6. Save the DDNAOptions.dox file.

   Creation of the network log file is disabled.

## Set Event Log Level

The Event Log level lets you specify the level of detail you want to capture in the event log. To optimize the performance, ensure that the log level is set to Error.

**Follow these steps:**

**CA DMM user interface**

1. Click Options, Logs.
2. Select Errors from the Level drop-down list available under the Event Log area.
3. Click OK.

**Options File**

1. Open the DMM Options Editor from the Start menu.
2. Click File, and then the File Open toolbar button.
3. Browse to the folder where CA DMM is installed and select the DDNAOptions.dox file.

   **Note:** If you have not run the DesktopDNA.exe, click File and then New to create the file.
4. Click Logging, Event Log in the left pane of the DMM Options Editor.

   All the Event Log options appear in the right pane of the DMM Options Editor.
5. Locate the Event log level option.

   The valid values are Error, Warning, and Information. CA DMM defaults to Error.
6. Check the Error option.
7. Save the DDNAOptions.dox file.

   The Event Log level is set to Error.

## Do Not Create Self-extracting Files

Creating the self-extracting DNA files takes longer time than creating the standard DNA files. If you do not need the self-extracting feature and concerned about performance, save DNA files in standard format.

# Turn Off Migrate Group Memberships

CA DMM migrates the group membership for users by default. If you do not need to migrate the group security, turn off this option in the DMM Options file.

**Follow these steps:**

1. Open the DMM Options Editor from the Start menu.
2. Click File, and then the File Open toolbar button.
3. Browse to the folder where CA DMM is installed and select the DDNAOptions.dox file.

   **Note:** If you have not run the DesktopDNA.exe, click File and then New to create the file.
4. Click Security Migration in the left pane of the DMM Options Editor.

   All the Security Migration options appear in the right pane of the DMM Options Editor.
5. Uncheck the Migrate group memberships option.
6. Save the DDNAOptions.dox file.

   Migration of the group membership is disabled.

# Index