Sys-Manage

User Manual

CopyRight2

Copyright © 2012 by Sys-Manage. All rights reserved.

This publication is protected by Copyright and written permission should be obtained from the publisher prior any prohibited reproduction, storage in retrieval system, or transmission in any form or by any means, electronic, mechanical, photocopying, recording, or likewise.

Sys-Manage Informatica SL
Phone: +1 (408) 345-5199
Phone: +1 (360) 227-5673
Phone: +44 (0) 8455273028
Phone: +49-(0)69-99999-3099
Phone: +34-810 10 15 34
Mail: Support@Sys-Manage.com
Web: http://www.Sys-Manage.com
YouTube: www.YouTube.com/SysManage
Facebook: www.facebook.com/pages/Sys-Manage/153504204665791
Bluesky: https://bsky.app/profile/sys-manage.bsky.social
Mastodon: https://techhub.social/@SysManage
Reddit: https://www.reddit.com/r/CopyRight2/

Use of trademarks: Microsoft, Windows, Windows NT, XP, Windows Vista, Windows 7, Windows 8, Windows 10, Windows 11 and the Windows logo are ® trademarks of Microsoft Corporation in the United States, other countries, or both. All other company, product, or service names may be trademarks of others and are the property of their respective owners.

ABSTRACT **9**

REQUIREMENTS **10**

USAGE SCENARIOS **12**

FILE SERVER MIGRATIONS 12
Different File Server Migration Approaches Using CopyRight2 ..... *13*
Maintain Original Server Names *15*
Microsoft Cluster Services as Source or Destination File Server *16*
Network Attached Storage as Source and/or Destination Server *17*
LOCAL USER AND GROUP ACCOUNT MIGRATION 17
DOMAIN USER, GROUP, CONTACT, OU AND CONTAINER MIGRATION 17
MIGRATION OF COMPUTER ACCOUNTS AND USER PROFILES 17
BACKUP OF FILE SERVERS, LOCAL ACCOUNT DATABASES AND ACTIVE DIRECTORIES 17
INTRODUCTION OF A CENTRALIZED DFS NAMESPACE 18

INSTALLATION / UPDATING / BACKUP **19**

DOWNLOADING 19
CODE SIGNING 19
INSTALLATION 20
BACKING UP JOBS, LOG FILES AND LICENSE ACTIVATIONS 23

LICENSING **24**

VIRTUAL MACHINES 24
CLUSTERS 24
STORAGE SOLUTIONS 24
CHANGING THE LICENSE FILE LOCATION 24
INSTALLING THE LICENSE KEY 25

USING COPYRIGHT2'S GUI **30**

TOOLBAR 31
Action Commands *31*
Job Commands *31*
Clipboard Commands *31*
Help Commands *32*
View Commands *32*
OPTIONS 33
General Settings *33*
Advanced Options *35*
OS Types, Roles and Domain Controllers *38*
Computer and Profile Migration *39*
Configuring the Computer Connection Point *40*
RPC Service *42*
Extended Logging *44*
ADDING OR EDITING A DATA MIGRATION JOB 45
Name and Description *45*
Source and Destination *46*
Inclusions and Exclusions *52*
File Attributes and Time *53*

ACL and Owner Permissions *55*
User and Group Filter *59*
User and Group Options *61*
User Environment *63*
Active Directory Options *65*
File Shares *67*
Advanced Options *69*
Real Time Synchronization *72*
Scripting *73*
Boot Environment *75*
Compare File System *77*
Error Processing *79*
ADDING OR EDITING A SECURITY AND ATTRIBUTES JOB 82
Source and Destination *82*
File Attributes and Time *83*
ACL and Owner Permissions *84*
File Shares *86*
User Environment Migration *87*
ADDING OR EDITING A USER AND GROUP MIGRATION JOB 89
Source and Destination *90*
User and Group Migration *91*
Filter *92*
Settings *94*
User Environment Migration *96*
Active Directory Options *97*
Active Directory Attribute In- and Exclusion List *99*
Advanced *101*
Scripting *103*
ADDING OR EDITING A DFS COPY JOB 105
Source and Destination *105*
Shares and Settings *108*
ADDING OR EDITING A COMPUTER AND PROFILE MIGRATION JOB 109
Source and Destination *110*
Computer Migration *112*
Settings *113*
Profile Filter *115*
Active Directory Options *117*
Active Directory Attribute In- and Exclusion List *119*
Domain Trust *121*
File System *123*
Advanced Settings *124*
Entra *127*
Scripting *129*
RUNNING A JOB INTERACTIVELY 131
SCHEDULING A JOB FOR BACKGROUND EXECUTION 132
VIEWING A JOB'S LOG FILE 134
COPYING AND PASTING A JOB DEFINITION 134

INFRASTRUCTURE REPORTING 135

ADDING OR EDITING A COMPUTER SCAN JOB 137
Computers *137*
Settings *138*

File Services *139*
Software *141*
Security (SAM) *142*
ADDING OR EDITING A LDAP SCAN JOB 143
Settings *143*
OUs, Users, Groups, Contacts, Computers and Built-In Accounts *145*
ADDING OR EDITING A SCAN IMPORT JOB 146
Jobs *146*
USING PRE-DEFINED REPORTING SERVICES REPORTS 147

ROLLOUT PLANNING 149

COPYRIGHT2 INSTALLATION 150
AGENT FOLDER PREPARATION 150
CSV IMPORT WIZARD 150
Select CSV File *151*
Select Rows *152*
Remote Agent *153*
Job Scheduling *154*
Select Copy Job to Deploy *155*
Assign CSV Fields *157*
Import Summary *158*
Import Progress *159*
Import Result *160*
ADDING OR EDITING A ROLLOUT PLANNING JOB 161
Name and Description *161*
Source and Destination *162*
Jobs to Deploy *163*
Time Schedule *164*
EXPORT DATA TO CSV FILE 165
DEPLOYMENT 166
CONNECTING TO REMOTE SERVER 166
RUN A JOB 167
DEACTIVATE A JOB 168
REACTIVATE A JOB 168

ADD-ONS 169

PASSWORD MIGRATION ADD-ON 169

IIS FTP/HTTP MIGRATION ADD-ON 169

MIGRATE IIS FTP/HTTP SITE CONFIGURATION DURING DATA MIGRATION 169
IIS FTP Filter *169*
IIS HTTP *172*
MIGRATE IIS FTP/HTTP SITE CONFIGURATION WITHOUT DATA MIGRATION 174
Source and Destination *174*
Sites *175*
FTP Filter *176*
HTTP Filter *177*
Search and Replace *178*

DFS REPLICATION (DFSR) ADD-ON 180

DFS REPLICATION 180

AZURE ADD-ON 182

REPLACING REFERENCES TO THE EVERYONE GROUP 182
AZURE APP REGISTRATION 183
MIGRATE FILE SHARES TO AZURE STORAGE ACCOUNTS DURING DATA MIGRATION 186
Adding File Shares to the Job 186
Azure Options 187
MIGRATE FILE SHARES TO AZURE STORAGE ACCOUNTS WITHOUT DATA MIGRATION 189
Source and Destination 189
Azure Options 190

POWERSHELL INTEGRATION ADD-ON 191

USING ACTIVESCRIPT 194

GLOBAL VARIABLES 194
TRANSFORMATION OF ATTRIBUTES 195
Accessing Local Account's Attributes 195
Terminal Server, Citrix and Remote Access Server (RAS) Attributes 196
LOGGING AND WSCRIPT FUNCTIONS 196

CREATING A MAPPING DEFINITION FILE TO REASSIGN PERMISSIONS 197

MAPPING FILE FORMAT 198
Source and Destination Account Format 198
Reacling 199
AddAcling 199
DeAcling 199
MAPPING FILE ADVANCED OPTIONS 199
Domain Mapping (Negative List) 201
Domain Mapping (Positive List) 201
Rename samAccountName of Target Account 201
AddAcling 202
Creating a Mapping File based on NTFS and/or Share Permissions 202

USING THE WINDOWS EXPLORER EXTENSION 204

COPYING WITH THE WINDOWS EXPLORER EXTENSION 204
REASSIGNING PERMISSIONS (REACLING) 207
ENABLE BACKUP / RESTORE PRIVILEGE FOR WINDOWS EXPLORER 207

USING A DFS SERVER TO MAINTAIN THE EXISTING UNC NAMESPACE 208

NON CLUSTERED DFS SERVER 208
CLUSTERED DFS SERVER 210

USING SID-HISTORY FOR ACTIVE DIRECTORY MIGRATIONS 212

INTER-FOREST SID-HISTORY MIGRATION REQUIREMENTS 212
Trust, Special Local Group & Auditing 212
Advanced Auditing 213
Source Domain Controller 213
Security Context Requirements 213
Naming Resolution 214
USING SID-HISTORY IN USER AND GROUP COPY JOB 215
Inter-forest SID-History Migration (Different Forests) 215
Intra-forest Domain sidHistory Migration (Same Forest) 216

DISABLING SID FILTERING FOR INTER-FOREST DOMAIN MIGRATIONS 217
SID-HISTORY CLEAN-UP AFTER MIGRATION 218

COMPUTER AND USER PROFILE MIGRATION 219

USING THE GRAPHICAL USER INTERFACE 219
Configuring the Computer Connection Point and Other Options 219
Migrating from a Synology Directory Server Domain 220
Creating a PPKG File with Microsoft Windows Configuration Designer 221
Configuring Authentication for Microsoft Entra Device Migrations 225
Running the Job 230
Tracking Execution Results 231
Performing an Undo to Reverse Changes 233
USING THE COMMAND LINE INTERFACE 234
Command Line Parameters 234
Remote Execution (Push Method) 235
Logging 235
VPN Users / CopyRight2 Cached Credential Update Add-On 235
Required Files if Using Remote Deployment Software 236
Examples 237

USING COPYRIGHT2'S COMMAND LINE INTERFACE (CLI) 240

ADVANCED PARAMETERS 241
SHARE AND NTFS PERMISSION MODIFICATIONS 242
USER AND GROUP MIGRATION AND REACLING 243
MIGRATING USER AND GROUP ACCOUNTS WITHOUT COPYING FILES OR SHARES 244
REMOTE EXECUTION 245
TEXT FILE INVENTORY 246
DFS UPDATE 247

OFFLINE MIGRATIONS OF DISCONNECTED SYSTEMS 248

EXPORT AND IMPORT OF USERS, GROUPS, GROUP MEMBERS AND FILE SHARES 248
EXPORT AND IMPORT OF FILES, FOLDERS AND NTFS PERMISSIONS 250
USING WINRAR FOR AN OFFLINE MIGRATION 251
Export Users, Local Groups, Local Group Memberships, Shares and Share Permissions 251
Exporting Data into a RAR File 251
Unpacking RAR File to Temporary Folder 253
Importing Users, Local Groups, Shares, Share Permissions and Data 253
IMPORTING SAMBA (LINUX) PASSWORD HASHES 254
SAMPLES 255

DOMAIN.INI FILE 257

NAS MIGRATIONS 258

AUDITING NO SUPPORTED 258
COMPRESSION NOT SUPPORTED 259
ADMINISTRATIVE OVERRIDE / BACKUP OPERATORS 260
ACCESS DENIED ERRORS 260
SYNOLOGY NAS AS SOURCE 261
SYNOLOGY NAS AS TARGET 262
MIGRATION OF PASSWORD HASHES FROM OR TO SYNOLOGY NAS SYSTEMS 263

SUPPORT FOR VERITAS ENTERPRISE VAULT 264

METHOD 1: SKIP OFFLINE FILES (PLACEHOLDERS) – PREFERRED METHOD....264
METHOD 2: MIGRATE PLACEHOLDERS WITH COPYRIGHT2 & RECALL THEM WITH FSAUTILITY....265

TROUBLESHOOTING....266

ERROR MESSAGE DURING INSTALLATION....266
NAME RESOLUTION PROBLEMS IF SPECIFYING SERVERS BY IP ADDRESS....266
LOCKED FILES CAUSE ERRORS DURING FILE COPY....267
WHILE MOVING A SHARE SERVER INTERNALLY AN ERROR INDICATES SHARE IS ALREADY EXISTING....267
ERROR 266 PASSWORD POLICY PROBLEM WHILE SYNCHRONIZING A USER ACCOUNT....267
THE SYSTEM FREEZES WHEN USING THE GUI OF COPYRIGHT2 ON A VMWARE GUEST....267
A BLUE SCREEN OCCURS DURING FILE COPY....267
DFS COPY JOB FEATURE IS NOT SHOWING UP....267
ERROR 84 OR 77 WHEN COPYING DATA BETWEEN SERVERS BECAUSE OF VIRUS PROTECTION....268
NETWORK PROBLEMS CAUSING WINDOWS ERROR 59 OR 64....268
AUTHENTICATION PROBLEM MIGRATING FROM OR TO WINDOWS WORKSTATIONS....269
ERROR 89 IF COPYING TO A SYSTEM THAT DOES NOT SUPPORT FILE LEVEL COMPRESSION....269
ERROR 3500 (WIN32ERR=87) DURING PASSWORD MIGRATION....269
FIREWALL CONFIGURATION....270
SOURCE OR TARGET NAS ROLE SHOWS UP AS WORKGROUP MODE INSTEAD OF DOMAIN MEMBER....271
SLOW PERFORMANCE DUE TO ANTI-VIRUS REAL-TIME SCAN ON SOURCE AND/OR TARGET....273
UNEXPLAINABLE ERRORS DUE TO ANTI-VIRUS REAL-TIME SCAN....273
ADMINISTRATORS PROMPTED WITH „YOU DON'T CURRENTLY HAVE PERMISSION TO ACCESS THIS FOLDER" 274
CANNOT FIND COMPUTER OR NAS SYSTEM WHEN SELECTING SOURCE FOLDER....276
ERROR 296 DURING SIDHISTORY MIGRATION....276
PRODUCT UNINSTALLATION FROM SETTINGS -> APPS & FEATURES FAILS IF UAC IS DISABLED....277

CONTACTING SUPPORT....278

CONTACT INFORMATION....278

Abstract

CopyRight2 lets you easily migrate network shares, files, folders, permissions, groups and user accounts (including passwords) from source to destination computers.

It is a comprehensive solution that will support you in your planning stages up to the actual migration phase.

You can use CopyRight to perform…

- ...file server migrations and consolidations within the same or across domain boundaries.
- …local user and group migrations (including user passwords).
- …Active Directory migrations (including user passwords).
- …backups of file servers and local or domain account databases.
- …the introduction of DFS (Distributed File Services).
- …migrations of IIS FTP/HTTP sites including settings.
- …migrations to Azure storage accounts.

You can copy files with CopyRight2 that are “normally” not accessible, in the same way it is done by Windows backup features, allowing you to backup all your files, even locked files or files where permissions would deny access.

Use the intuitive graphical user interface to create a copy job with a few mouse clicks and simply select the source files and destination folders.

Any jobs created with the graphical user interface can be run unattended and at a chosen date and time or interval. You can optionally configure CopyRight2 to send emails upon success and/or failure of copy jobs scheduled for background execution.

Beside of the graphical user interface it is integrated with Windows® Explorer and offers an additional command line interface very similar to the built-in Xcopy command.

Requirements

CopyRight2 has the following hardware requirements:

- At least 4GB of RAM
- At least 1 CPU with 2 cores (or hyper-threading)
- At least 256MB of available disk space

CopyRight2 supports the following versions of Windows:

- Microsoft Windows® NT 3.51
- Microsoft Windows® NT 4.0
- Microsoft Windows® 2000
- Microsoft Windows® 2003 / Windows® 2003 R2
- Microsoft Windows® 2008 / Windows® 2008 R2
- Microsoft Windows® 2012 / Windows® 2012 R2
- Microsoft Windows® 2016
- Microsoft Windows® 2019
- Microsoft Windows® 2022
- Microsoft Windows® 2025
- Microsoft Windows® XP
- Microsoft Windows® Vista
- Microsoft Windows® 7
- Microsoft Windows® 8.0 / 8.1
- Microsoft Windows® 10
- Microsoft Windows® 11
- Windows® Cluster Services

CopyRight2 supports the following Network Attached Storage Solutions:

- Netapp® ONTAP7, ONTAP8, ONTAP9 (clustered & stand-alone)
- EMC® Celerra, VNX and Isilon
- Hitachi® HDI & HNAS
- Synology®
- NetGear ReadyNAS®
- Nutanix®
- Nasuni®
- Many others...

CopyRight2's IIS FTP/HTTP Site Migration Add-On supports the following IIS versions:

- IIS 5.0 (only as source)
- IIS 6.0 (only as source)
- IIS 7.0 (only as source)
- IIS 7.5
- IIS 8.0
- IIS 8.5

- IIS 10 Build 1607 and newer (1709, 1809, …)

CopyRight2's Azure Migration Add-On supports the following Cloud Platforms:

- Azure Storage Account

For a successful operation the following Windows security privileges are required at a minimum, which are granted to members of the Administrators group by default:

- Copying files and folders (in case of files or folders not accessible to the security context being used, where for example administrators have been locked out)
  - Backup files and directories (at source)
  - Take ownership of files and directories (at source)
  - Restore files and directories (at destination)
  - Note: Most network attached storage solutions require membership in the local group "Backup Operators" on the storage system instead of granted privileges (at source / at destination)

- Copying file shares
  - Member of "Administrators", "Power Users", "Print Operator" or "Server Operator" (at source)
  - Member of "Administrators" or "Server Operators" (at destination)

- Migration of Active Directory Users and Groups
  - Member of "Enterprise Admins", "Domain Admins" or "Local Administrators" (at source domain).
  - Member of "Enterprise Admins", "Domain Admins" or "Local Administrators" or delegated "Create, delete and manage users/groups" permissions for the target OU (at destination domain).

It is recommended that you specify computers using their computer names and that DNS or NetBIOS name resolution will provide addresses for those names. Specifying IP addresses can potentially create problems. In case of problems with name resolution you can always create a LMHOSTS file to map computer names to network addresses (See chapter Troubleshooting / Name Resolution Problems if Specifying Servers by IP Address). This problem affects network drives connected to hosts using IP addresses as well. The most reliable solution is to create a LMHOSTS file.

Usage Scenarios

File Server Migrations

CopyRight2 can be used within a wide range of migration scenarios. You can use it to migrate data…

a) from one server to another domain internally,

b) from one server to another across domains or

c) server internally (e.g. relocating a network share from one hard drive to another hard drive while preserving permissions or applying changes to local NTFS and share security).

It will automatically detect security identifiers (SIDs) of groups and users that would not be resolvable at the destination computer and, depending on settings, create any missing accounts.

Destination / Source	Member Server (Same Domain)	Domain Controller (Same Domain)	Member Server (Foreign Domain)	Domain Controller (Foreign Domain)	Workgroup
Member Server	Requires copying local groups and local users.	Requires copying local groups and local users.	Requires copying global groups, global users, local groups and local users.	Requires copying global groups, global users, local groups and local users.	Requires copying global groups, global users, local groups and local users.
Domain Controller	Requires copying local groups and local users in pre W2K AD mode. In native mode local groups are domain local and can be used on member servers without copying.	**Note:** Not necessary to migrate any accounts.	Requires copying global groups, global users, local groups and local users.	Requires copying global groups, global users, local groups and local users.	Requires copying global groups, global users, local groups and local users.
Workgroup	Requires copying global groups, global users, local groups and local users.	Requires copying global groups, global users, local groups and local users.	Requires copying global groups, global users, local groups and local users.	Requires copying global groups, global users, local groups and local users.	Requires copying global groups, global users, local groups and local users.

Different File Server Migration Approaches Using CopyRight2

Copy All Data Using a Single Copy Job in Single Pass

This is the simplest approach to use CopyRight2. This method uses a single copy job and requires that the maintenance window available for the migration provides sufficient time to complete the execution of the copy process. First you create a copy job to copy all the required files and folders. Optionally you can also enable the migration of network shares, happening at the end of the copy job's execution for any file share located at or below the specified source path(s). It is also recommended to enable the corresponding user and group migration settings to prevent the copy job from having to interrupt during execution to ask how to handle user or group accounts requiring migration.

After the job completed successfully you can stop sharing the migrated folders at the source. In case you want to replace the entire source server you could shut it down now. Next you could rename the destination server into the original server's name or add its name as an additional NetBIOS name at this point in time. This will ensure that clients can still access any data using the existing UNC paths.

Please note that any files locked by users or running applications on the source computer, will stop the copy process with an error message. Please make sure that users are not working during the execution of the copy job. The copy job should succeed without any errors. You can review a copy job's error log file by selecting the corresponding copy job and then clicking on the "View Log File" button in CopyRight2's toolbar.

Use Differential Copies to Reduce Downtime with Multiple Passes

In case copying the complete data takes more time than time is available to complete the migration in a given maintenance window or if you simply want to complete the cutover step as quickly as possible, you can use CopyRight2's differential copy function to minimize downtime. A differential copy will skip any existing files and additionally delete any files at the destination that have been deleted (or renamed) on the source side, since the copy job executed the last time. It is similar to a "robocopy /MIR" command. Any subsequent executions of the copy job will run much faster and only copy the differences.

In this case, you do split the copy job into two steps. The first step is used to pre-copy as much data as possible. We recommend to use the "Ignore errors resulting from locked files" option to skip any files locked by users during the pre-copy phase. Alternatively, you could also use the "Use Volume Shadow Copy" option instead to include locked files by using Windows built-in snapshot functionality.

When the time has come to replace the source server (or some of its shares), you do ensure that the last run of the differential copy job is being executed without the "Ignore locked files" and without the "Use Volume Shadow Copy" option, to make sure that all the data is included.

Once the final copy job has completed successfully you could change the destination server's name into the original source servers name at this point in time. This will ensure that clients can still access any data using the existing UNC paths.

Pre-Copy Job Settings

Option	Tab	Description	Setting
Copy modified files only. If enabled, any files not modified at the source will be skipped	Source and Destination	Skip files that exist at the destination already.	**Checked**
Sync. source with destination. Additionally causes the deletion of files deleted at source	Source and Destination	Delete files on the destination that were once copied but have been deleted (or renamed) at the source in the meantime.	**Checked**
Ignore errors resulting from locked files	Error Processing	Skip files in use without error.	**Checked** (to skip locked files during pre-copy phase)

Final Copy Job Settings

Option	Tab	Description	Setting
Copy modified files only. If enabled, any files not modified at the source will be skipped	Source and Destination	Skip files that exist at the destination already.	**Checked**
Sync. source with destination. Additionally causes the deletion of files deleted at source	Source and Destination	Delete files that were once copied to the destination but have been deleted at the source in the meantime.	**Checked**
Ignore errors resulting from locked files	Error Processing	Skip files in use without error	**Unchecked** (to fail if any file is locked)

Maintain Original Server Names

There are multiple approaches to maintain the original NetBIOS and DNS name of your source servers after the migration. If not maintaining the original server names, you may have to apply changes to logon scripts, GPOs, persistently stored network connections and shortcuts. The two latter ones are stored in the user profiles and if not using roaming (server based) profiles those reside on each workstation. Additionally, server names could be referenced by applications, for example if hyperlinks were used in Office documents or if Office macros reference them.

If you carry over the source server's name, for whatever reason, CopyRight2 can update server based profiles if migrating the folders where the profiles are stored and enabling the corresponding settings (see chapter "User Environment" in "Adding or Editing a Data Migration Job" and "Adding or Editing a Security and Attributes Job"). To update the workstation profiles, we recommend 3rd party tools, such as ForenSit's "User Profile Wizard".

Switch Source and Target Computer Names

Using this method, requires to simply switch the computer names of source and target, once the migration has been completed and all data was copied over to the target. Please contact Sys-Manage support to switch the licenses on our licensing server as well after you have performed the rename, otherwise the program will refuse to work with a license validation error.

Configure Target Server for Multiple NetBIOS Names

You can define multiple NetBIOS names on the target server by setting the registry value "HKLM\System\CurrentControlSet\Services\LanmanServer\Parameters\OptionalNames" to a REG_MULTI_SZ value containing one or more NetBIOS names that you want the server service to respond to. Please make sure that you have either turned off the old server or renamed it before you make this change, otherwise a duplicate NetBIOS name error will occur. After making the change, it is required to restart the server service.

Define an Additional CNAME in DNS

You can simply define an additional CNAME, in case you do not rely on NetBIOS, and let it resolve to the new target server's IP address.

Use DFS to further minimize Downtime

CopyRight2 can further minimize the downtime by utilizing a DFS Server (either running on a regular Windows server or running in a cluster). This approach requires some more steps but will allow you to migrate share by share while retaining the original UNC paths.

In a first step you create a copy of your source computer's shares within DFS by using a "DFS Copy Job". This will create DFS shares on your DFS server pointing to the original source server name modified by a prefix or a suffix for example (e.g. by appending "–RT" for retired). After this step has completed successfully you will have to rename the original source server to this new name.

Next you will add the original source server's name as an additional name to the destination server. This step differs depending on whether you run DFS on a clustered server (for higher availability) or on a standalone server. We describe this process in detail in a separate chapter.

After these steps have been completed the clients should be able to access any of their data using the existing UNC paths. The DFS server will redirect them automatically to the retired server's shares. Please note that at this point in time no data has been copied actually.

After these required steps have been completed you can start a share-by-share migration. Please make sure that you check the option "Update DFS Server" within your copy job settings to let CopyRight2 update each successfully migrated share on the DFS Server to point to the shares new location. The share can still be accessed using its original UNC path after the migration completed.

You can find more details about how to use DFS in this scenario in the chapter "Using a DFS Server to Maintain the Existing UNC Namespace".

Additional Copy Job Settings

Option	Tab	Description	Setting
Update DFS (Distributed File System) after share was migrated to new location	Shares	Will update the specified DFS server's links pointing to source share(s) to point to the new share(s) location instead.	Checked

Microsoft Cluster Services as Source or Destination File Server

CopyRight2 is fully compatible with Microsoft Cluster Services. Please check our support matrix below:

Source \ Destination	Windows 2000 Cluster	Windows 2003 Cluster	Non Cluster (Windows or NAS)	Windows 2008 (or newer) Cluster
Windows 2000 Cluster	Not supported	Not supported	Supported	Supported
Windows 2003 Cluster	Not supported	Not supported	Supported	Supported
Windows 2008 (or newer) Cluster	Not supported	Not supported	Supported	Supported
Non Cluster (Windows or NAS)	Not supported	Not supported	Supported	Supported

To specify a Windows 2008 (or newer) cluster as the source or destination of a copy job or reacling job please use the file server resource's fully qualified DNS name or its NetBIOS name.

If the source is a clustered Windows file server, you can select the file shares offered by the file server resource shown below the node of the computer object when selecting files and folders to copy. You can optionally change the UNC path to use an administrative share pointing to the corresponding clustered volume. For example instead of

“\\SrcClusteredFileServer\Data$”, you could specify “\\SrcClusteredFileServer\e$\data”, if that is the folder providing the “Data$” share.

If targeting a Windows cluster, please make sure that the specified destination share’s volume belongs to the file server resource. If your cluster’s file server resource is called \\DstClusteredFileserver and the destination is the q: drive which belongs to this file server, you would specify “\\DstClusteredFileserver\q$\...” as the target path of your copy job.

Network Attached Storage as Source and/or Destination Server

CopyRight2 is compatible with the majority of network attached storage solutions available on the market. In case of unexpected access denied error messages, please try to enable the “NAS Compatibility Mode” located within the “ACL and Owner Permissions” tab. This enables some workarounds for known compatibility issues regarding backing up and restoring files and other compatibility issues that some network attached solutions may have.

Local User and Group Account Migration

CopyRight2 can be used to migrate local user and group accounts (including passwords). This is for example useful during the migration of FTP servers or other applications that require user authentication. The migration can be scripted optionally to apply custom transformations to migrated objects using VBScript and other ActiveScript languages.

Domain User, Group, Contact, OU and Container Migration

CopyRight2 can be used to migrate domain users (including passwords), groups, contacts, OUs and containers between different Active Directory domains. It supports the migration of either all or specific Active Directory attributes (include/exclude list), optionally the migration of object permissions and can be scripted to apply custom transformations to migrated objects using VBScript and other ActiveScript languages.

Migration of Computer Accounts and User Profiles

CopyRight2 provides the ability to remotely migrate computer accounts between domains and/or migrate local user profiles stored on those computers.

Backup of File Servers, Local Account Databases and Active Directories

CopyRight2 can be used to backup data including permissions. It is possible to backup to locally connected storage or directly onto a remote computer. Backups can be scheduled for automatic background execution and provide a

mechanism to report about success or failure via email. It is also possible to backup local users and groups or Active Directories using a “User and Group” type of copy job to either remote systems or into text files.

Introduction of a Centralized DFS Namespace

CopyRight2 can be used to introduce centralized file share access using DFS as well. You can use a “DFS Copy Job” to create DFS links of a specified source server within a specified DFS namespace that CopyRight2 will automatically create.

You could for example move all the file shares located on file server \\Server01 to a DFS namespace named “Accounting” located on the DFS server \\Corp. This would allow users to access the shares using the alternative name \\Corp\Accouting [\Share Name]. Once all users are using the new name, you can easily change the storage server being used by updating the DFS link to point to another location (or let CopyRight2 do it automatically after a share has been migrated).

Installation / Updating / Backup

Downloading

You can download the most current version of CopyRight2 from our web site located at http://www.Sys-Manage.com.

Code Signing

All our downloadable MSI installer files are code signed using Windows Authenticode, so you can verify the authenticity and integrity of the download. All executables (EXE and DLL) files released by Sys-Manage are code signed as well.

You can validate code signing using Windows explorer by displaying the properties of the file and then selecting the "Digital Signatures" tab. Next pick the signature from the list below and click on the "Details" button. You should see "This digital signature is OK".

If the validation should fail, please make sure the system has the latest updates and root certificate updates installed. Try validation of the file on another system, preferably running a newer OS version. If validation fails there as well, try downloading the file again. If this does not resolve the issue, please contact Sys-Manage support (support@sys-manage.com).

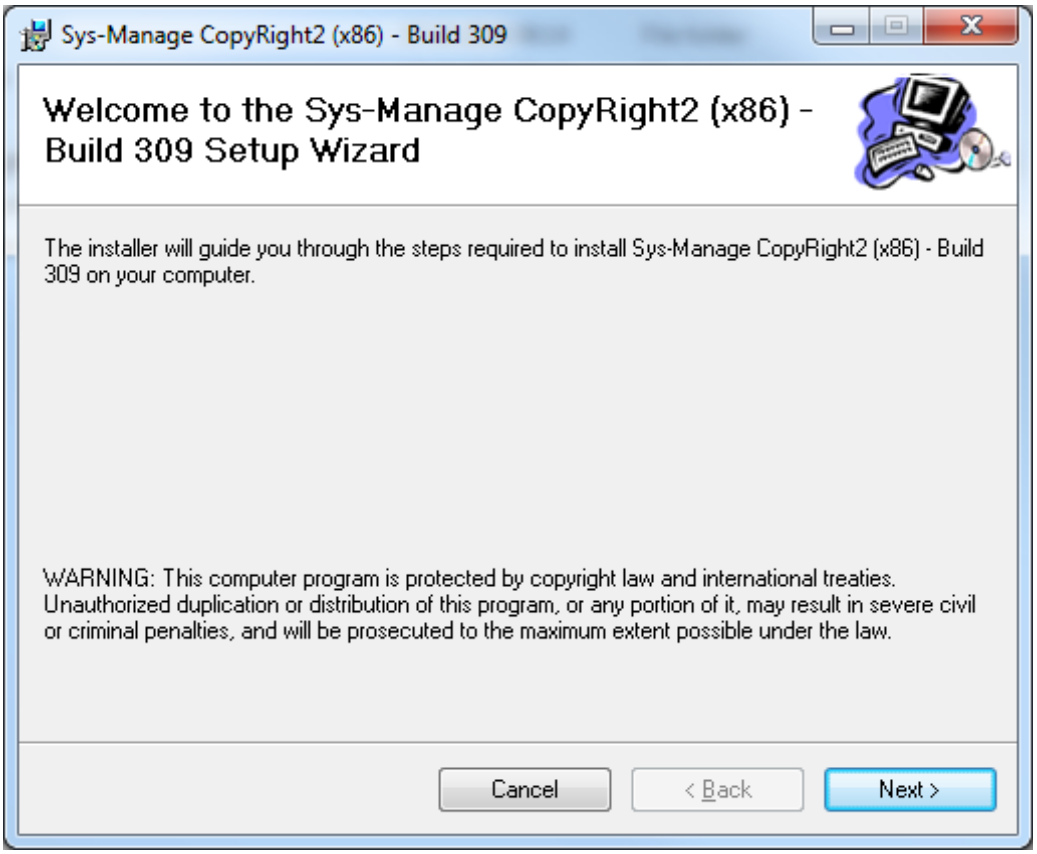
Installation

It is sufficient if you install the software either on the source or the target computer. In case of a migration between two storage systems, please install the software on a 3rd computer running Microsoft Windows.

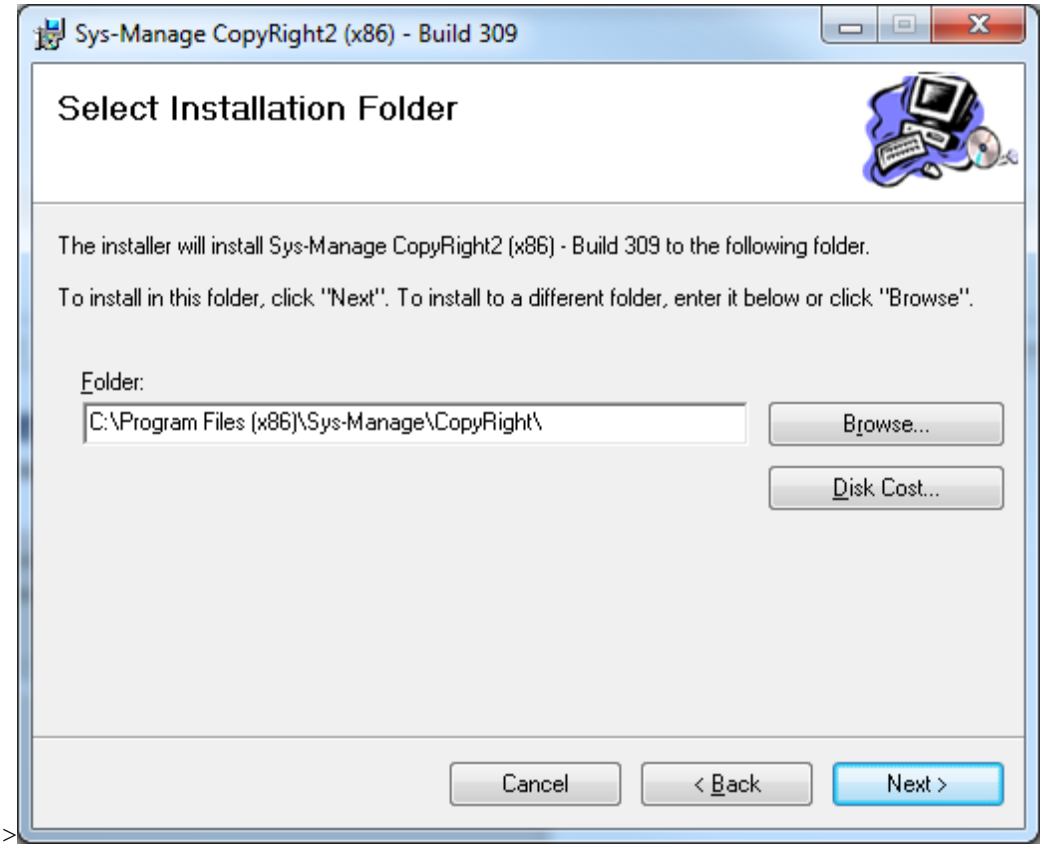
Note: Please note that you can update CopyRight2 by running the installer of a newer build version. The installer will preserve your existing jobs, log files and your license activation files. To update add-ons, such as the password migration add-on, please uninstall it first using "Add / Remove Programs" from the control panel and then install the updated version of the add-on.

After you have downloaded the MSI file double click on it to launch the installation.

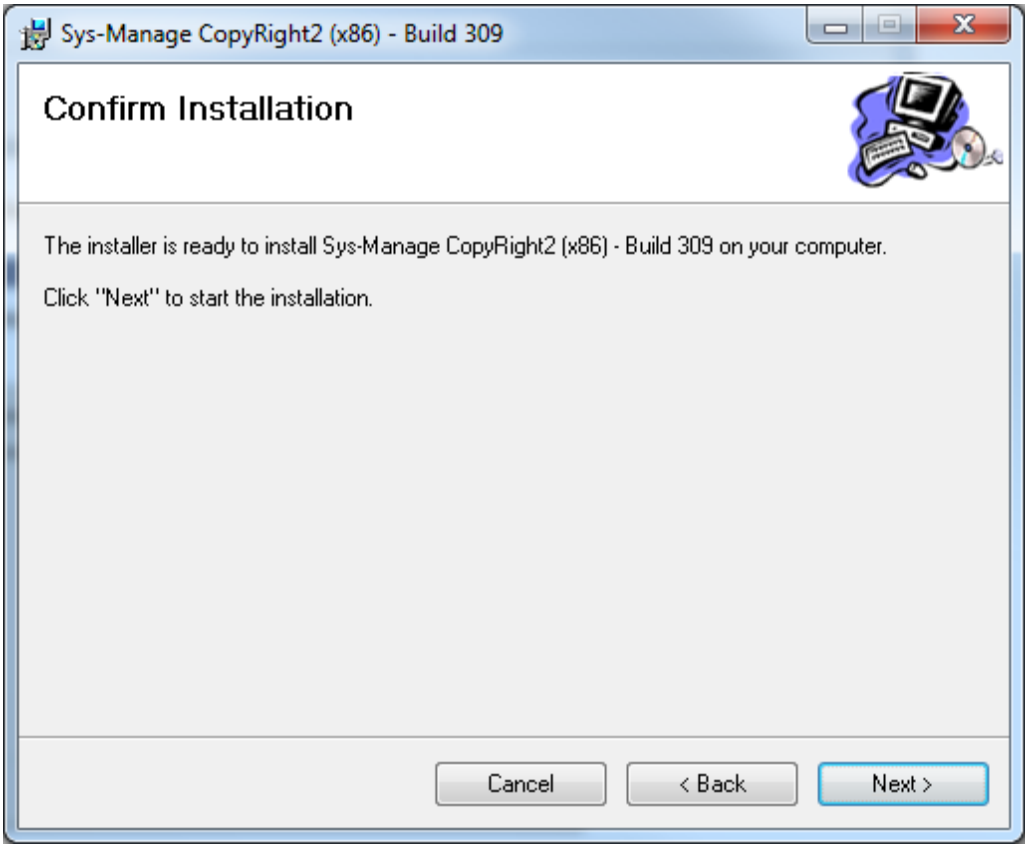
1. The CopyRight2 installation wizard appears. Please click on “Next” to continue the installations process.



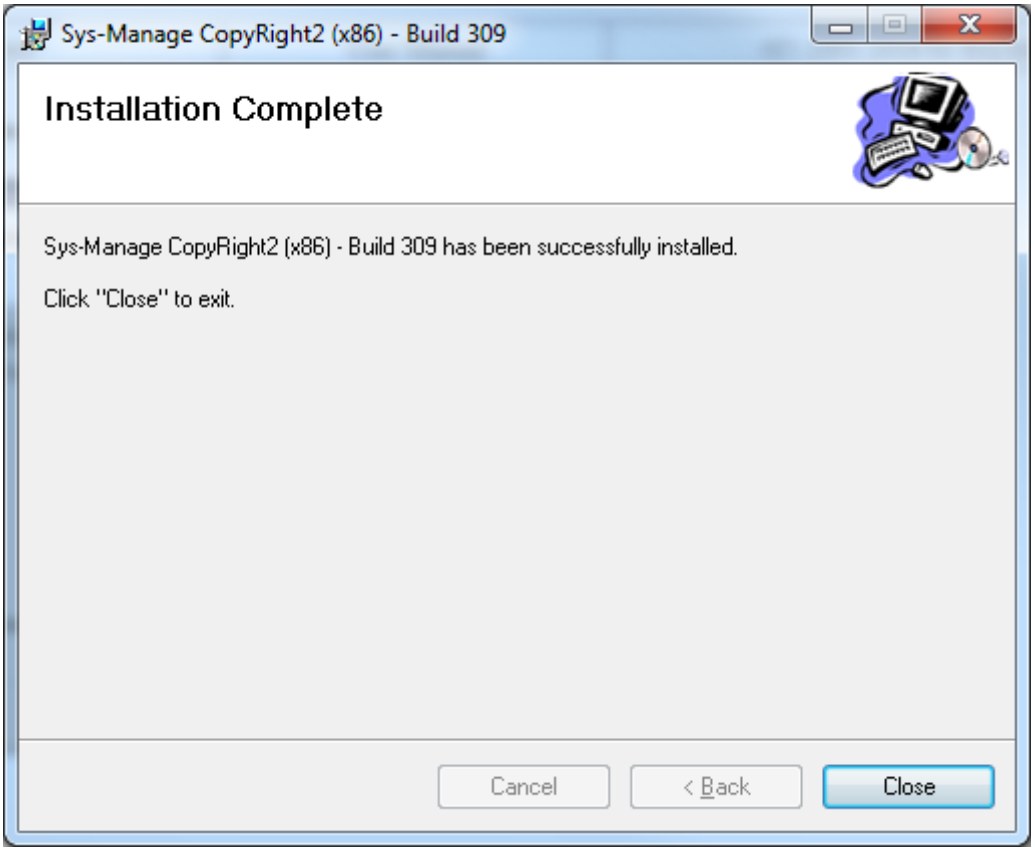
2. In the following wizard page you can enter an optional installation folder. Click on “Next” to continue.



3. Confirm the installation by clicking on “Next”.



4. After the installation is completed click on “Close” to finish the installation process.



Backing up Jobs, Log Files and License Activations

To back up your CopyRight2 installation, you can save the *.JOB, *.LOG and *.LIC files located in the program’s installation folder.

Additionally you can save the registry key “HKEY_LOCAL_MACHINE\SOFTWARE\Sys-Manage\CopyRight” with Regedit.exe to save any custom settings made.

Licensing

Please note that CopyRight2 is licensed per computer participating in the migration. The licenses are locked to specific machines and are not transferable. That means you will need a separate license for each source and each destination server. You can re-use the licenses currently assigned to destination servers, when they become source servers of a future migration again.

It is usually sufficient to install the product on either the source OR the target system. Please make sure to activate the licenses for the source AND target systems on the computer where you run the software at. An exception to that are so-called offline migrations, where source and target are on disjoint networks, requiring an installation on both and a license activation on each system.

Virtual Machines

In case of virtualized server environments, each guest operating system counts as a single source or destination server. If you have one physical machine, running 10 virtual servers, as a destination and 10 other physical source servers, you would need 20 licenses.

Clusters

Windows clustered file server resources require a single license, just like a non-clustered file server or NAS system would need. During activation, please ensure that you are activating the license for the file server resource name and not the cluster name or the cluster node name.

Storage Solutions

Each instance (NetBIOS/DNS name) that is reference by a copy job, needs a separate license.

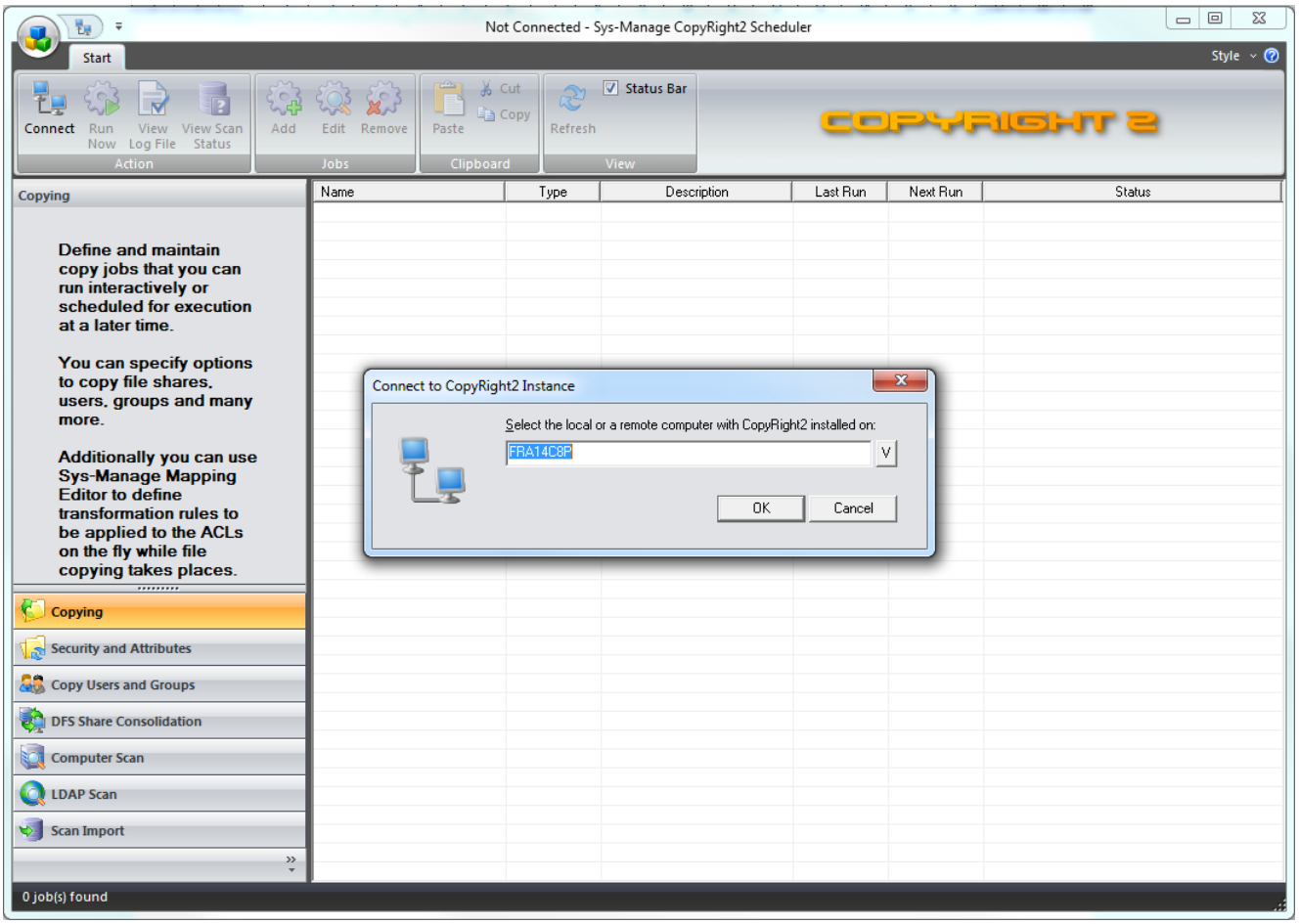
Changing the License File Location

CopyRight2 stores the license activation data in the local CopyRight2 installation folder by default. The location of this folder can be redirected to a network location to share the license activations between multiple computers on the network. To redirect it to another location please set the registry value “KeyServerPath” of type REG_SZ, located in registry key “HKLM\ Software\Sys-Manage\CopyRight” accordingly. You could for example create a network share Cr2License$ on a computer called \\Server01 and then set the registry value to “\\Server01\Cr2License$”. Please make sure that the file share and NTFS permissions provide sufficient access for the user account used to run the CopyRight2 software. It will at least require read permissions. Activating new licenses additionally requires permissions to allow the creation of new files and write permissions to existing files.

Installing the License Key

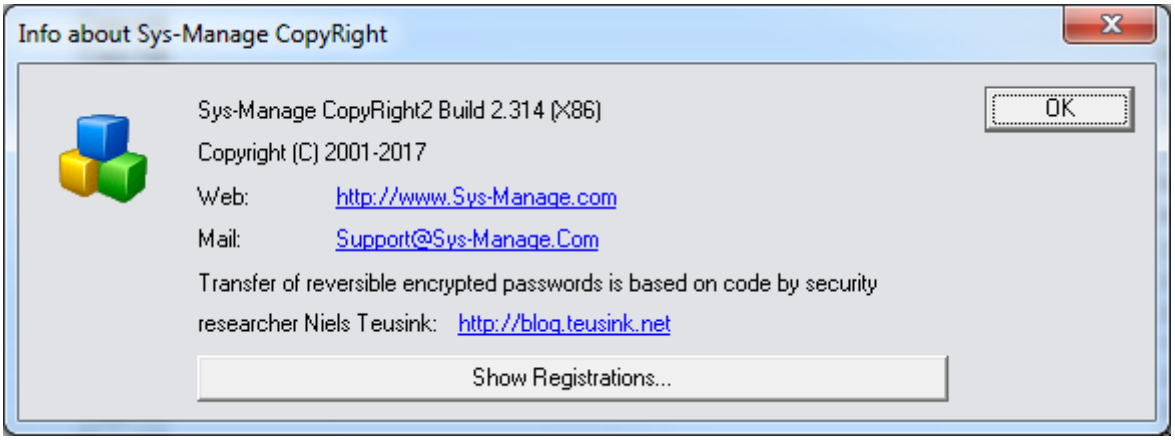
Please follow the next steps to activate computers for using the CopyRight2 software.

1. To install the license key file that you have obtained by ordering CopyRight2 start an instance of CopyRight2's graphical surface from the Start menu by clicking on Start -> Programs -> Sys-Manage CopyRight -> CopyRight2. A dialog shows up asking for a remote computer to connect with. Please click on "Cancel".

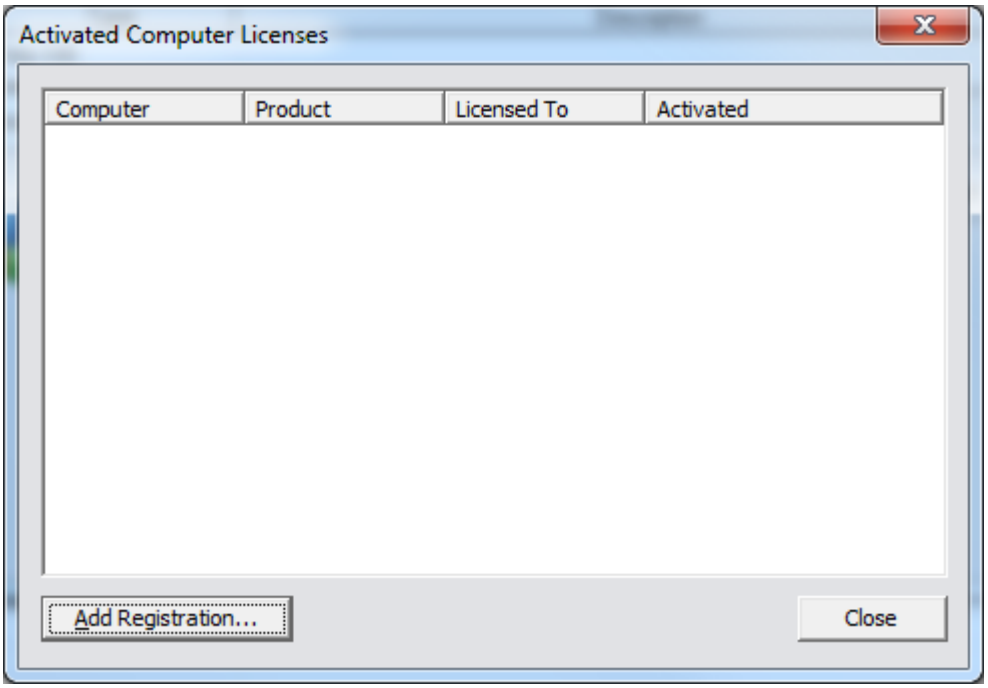


2. Click on the blue question mark symbol located in the upper right corner of the application window to open up the about box.

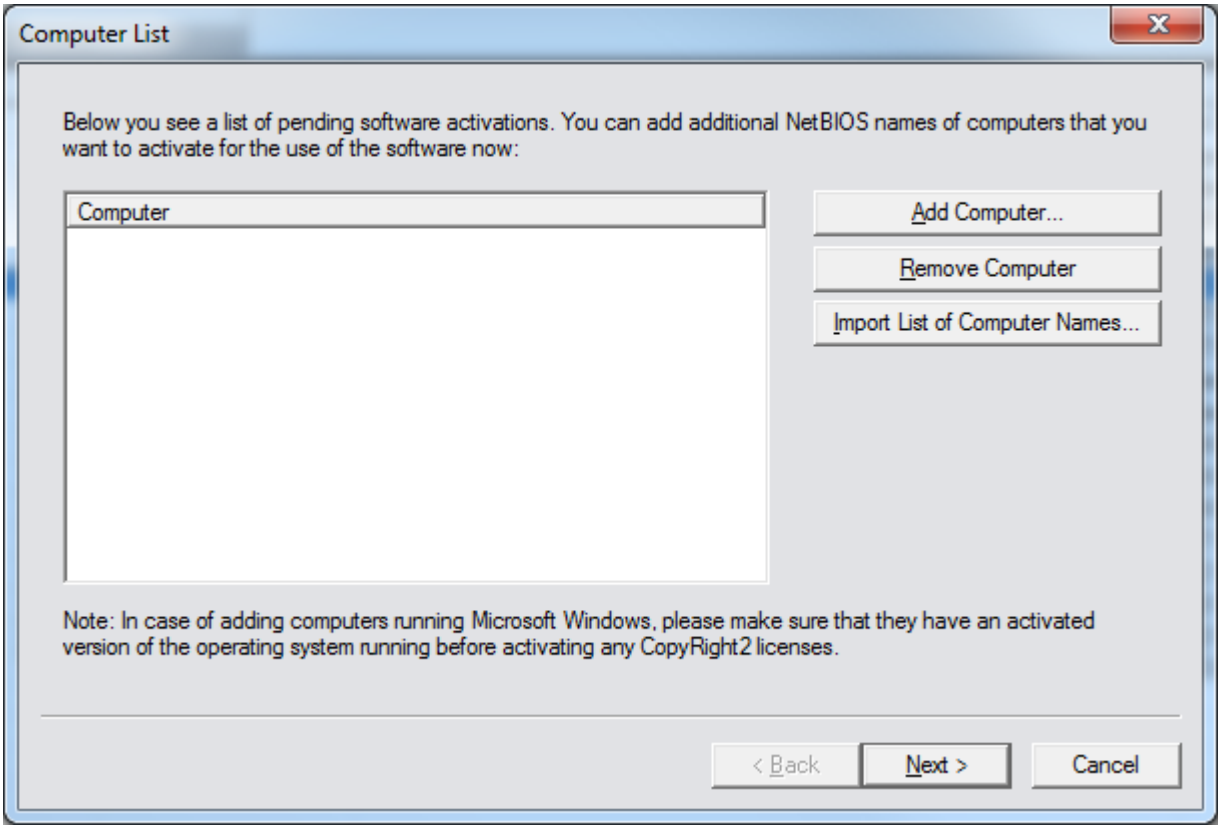
3. Click on the “Show Registrations…” button.



4. You will see a list of existing activations. Click on “Add Registration…” to activate one or more computers.

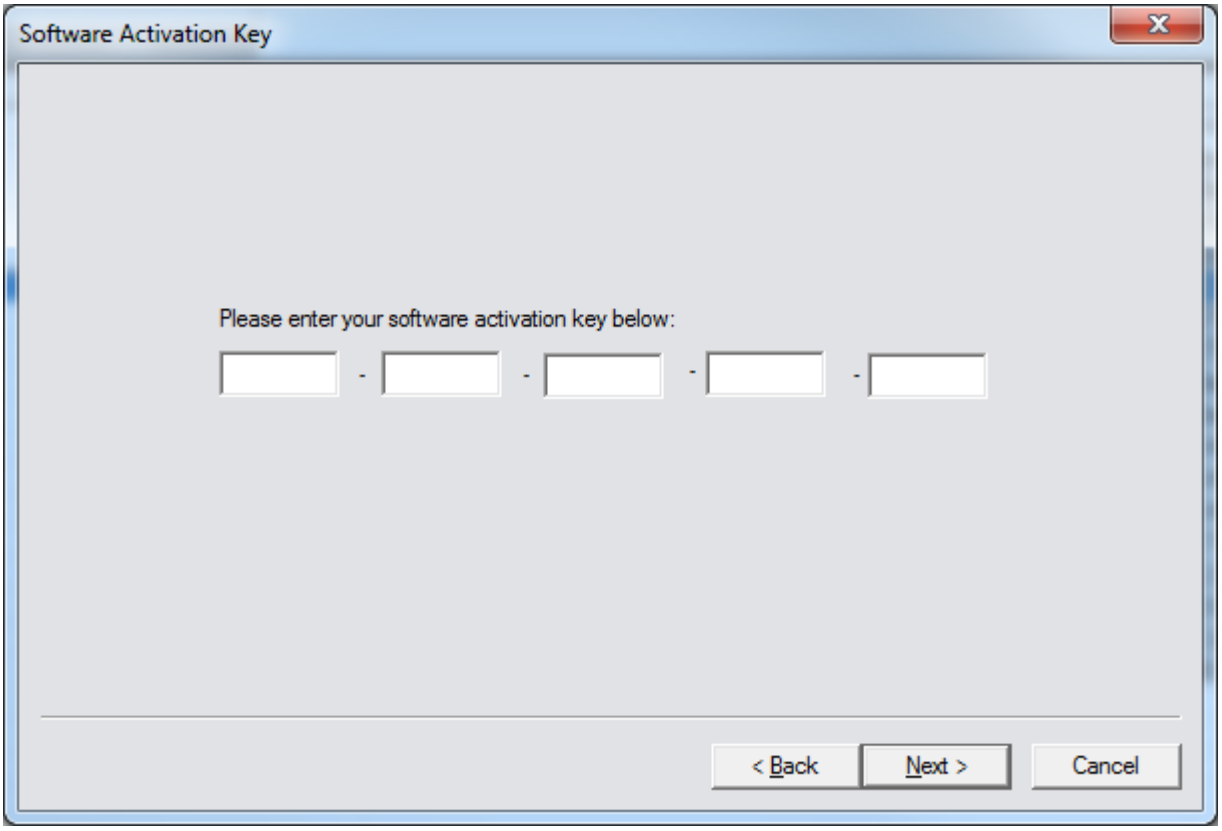


5. During the next step you can define the computers you want to activate CopyRight2 for. You can click on “Add computer…” to add a computer to the list, “Remove Computer” to remove a computer or on “Import List of Computer Names…” to import a text file containing computer names (one computer name per row). Activate the source AND the target systems that are referenced by copy jobs to run on this system using the exact name used in the job (NetBIOS or DNS FQDN):

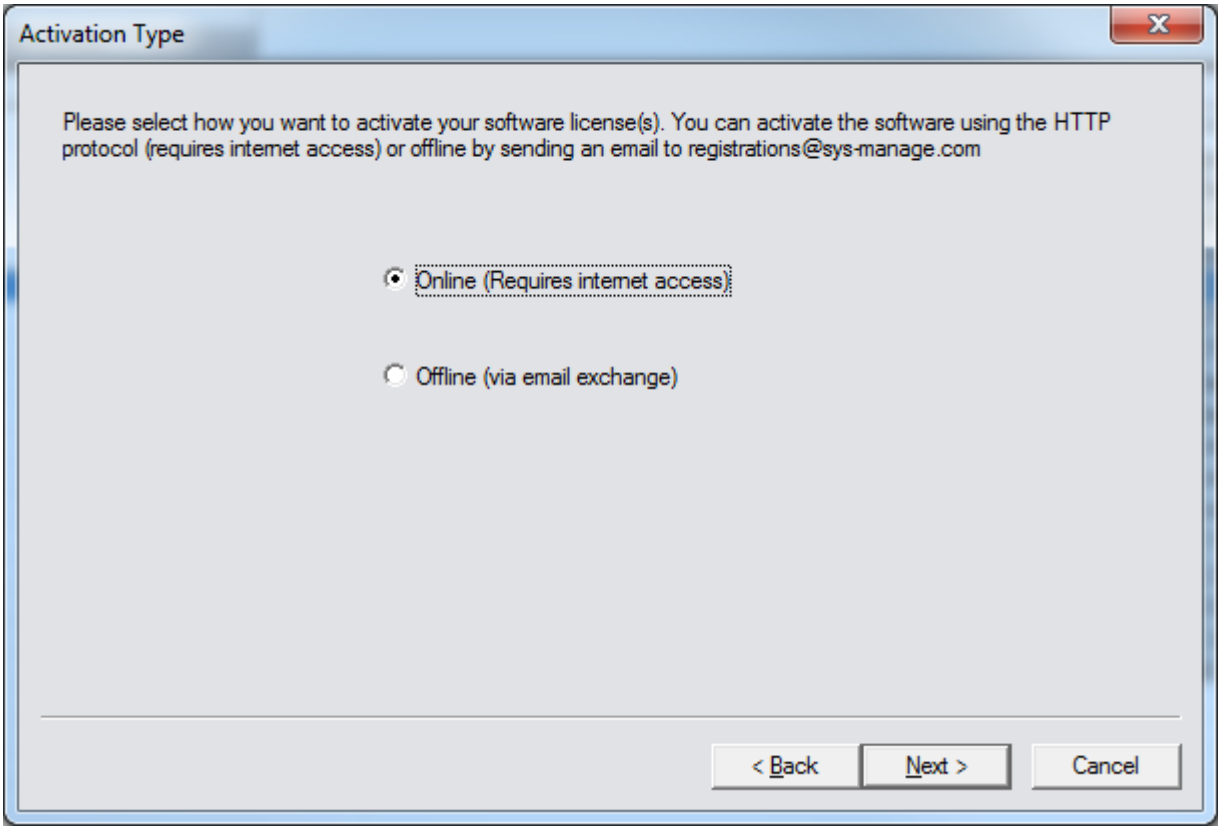


Note: An exception to this are so-called offline migrations, where source and target are on disjoint networks, requiring an installation on both and a license activation on each system.

6. Enter the software activation key or copy & paste it into the first field.



7. Either select online activation, requiring an internet connection or offline activation, requiring an email exchange:

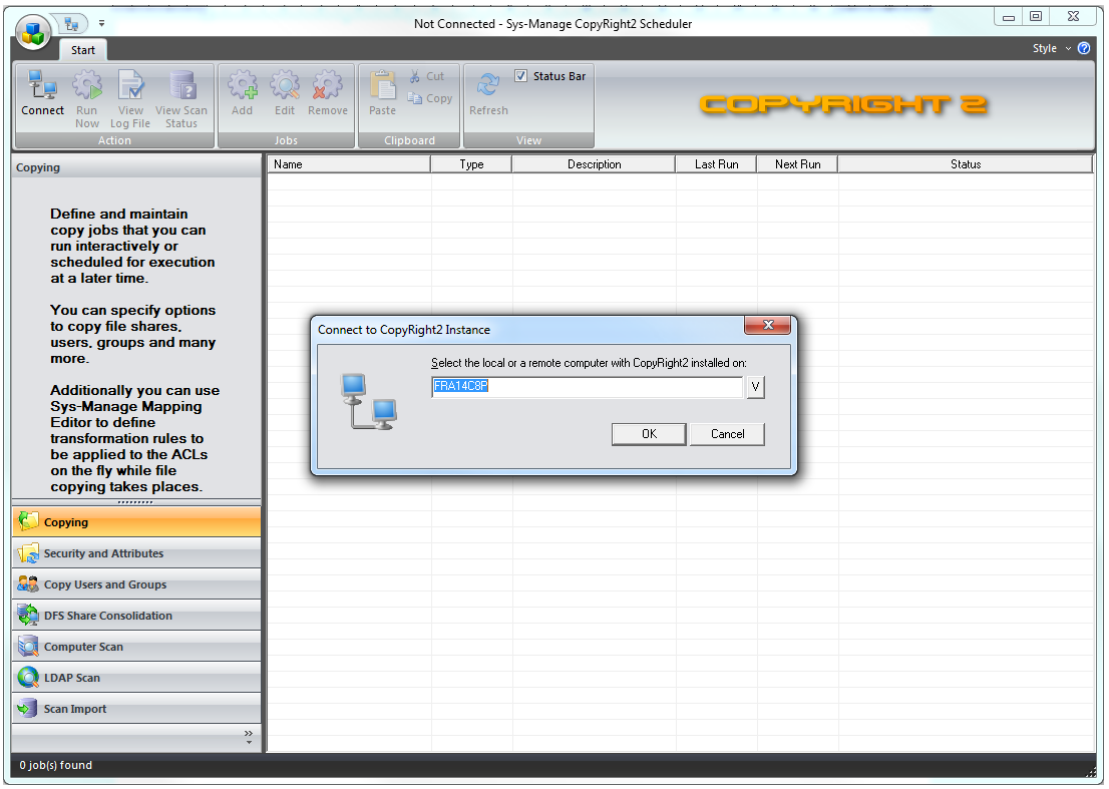


Follow the on-screen instructions to complete the activation.

Using CopyRight2's GUI

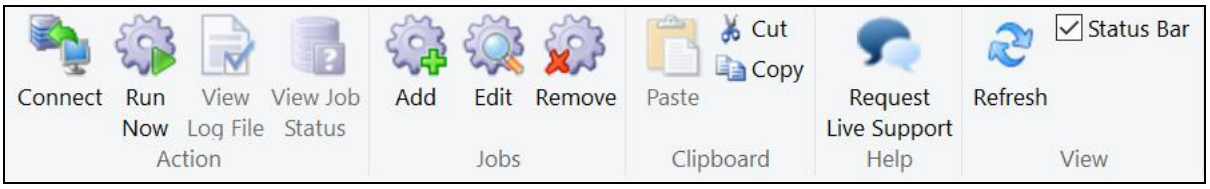
To start CopyRight2 go to the start menu group "Sys-Manage CopyRight" and click on the "CopyRight2" shortcut. You might be prompted for UAC elevation in case you use Windows Vista, Windows 2008 or newer operating systems. Please confirm the elevation in this case.

Next connect to the computer that you want to run or schedule jobs on by either entering the computer's name or selecting it from the drop down control. You can connect to the local computer or to a remote computer that has CopyRight2 installed on. Then click on "OK" to confirm.



On the left side of the window you can see a filter that shows you the type of jobs available with a short description. The list beside the job type filter shows you the defined jobs of that specific kind. On top of the application you see the toolbar containing the commands to control the application. The status bar on the bottom area of the application window shows status information.

Toolbar



The toolbar contains all the commands required to use CopyRight2.

Action Commands

Command	Description
Connect	Use this command to connect to the local computer or to a remote computer that has CopyRight2 installed on.
Run Now	Run the currently selected job.
View Log File	This command shows the currently selected job's log file. If the command is disabled, there is no log file available.
View Job Status	This command is used by "Computer and Profile Migration" and "Computer Scan" jobs and shows the status of the job's execution on remote systems.

Job Commands

Command	Description
Add	Adds a new job to the list.
Edit	Edit the currently selected job.
Remove	Delete the currently selected job.

Clipboard Commands

Command	Description
Cut	Cut out the currently selected job onto the clipboard
Copy	Copy the currently selected job onto the clipboard
Paste	Paste the job located on the clipboard

Help Commands

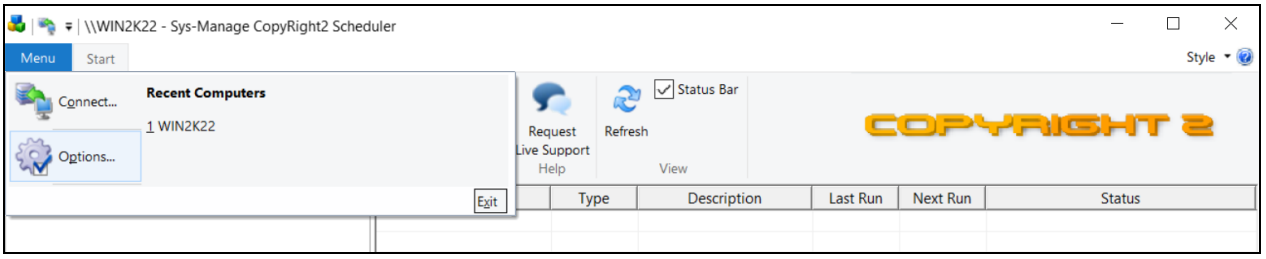
Command	Description
Request Live Support	Connect to Sys-Manage's support chat (requires internet access)

View Commands

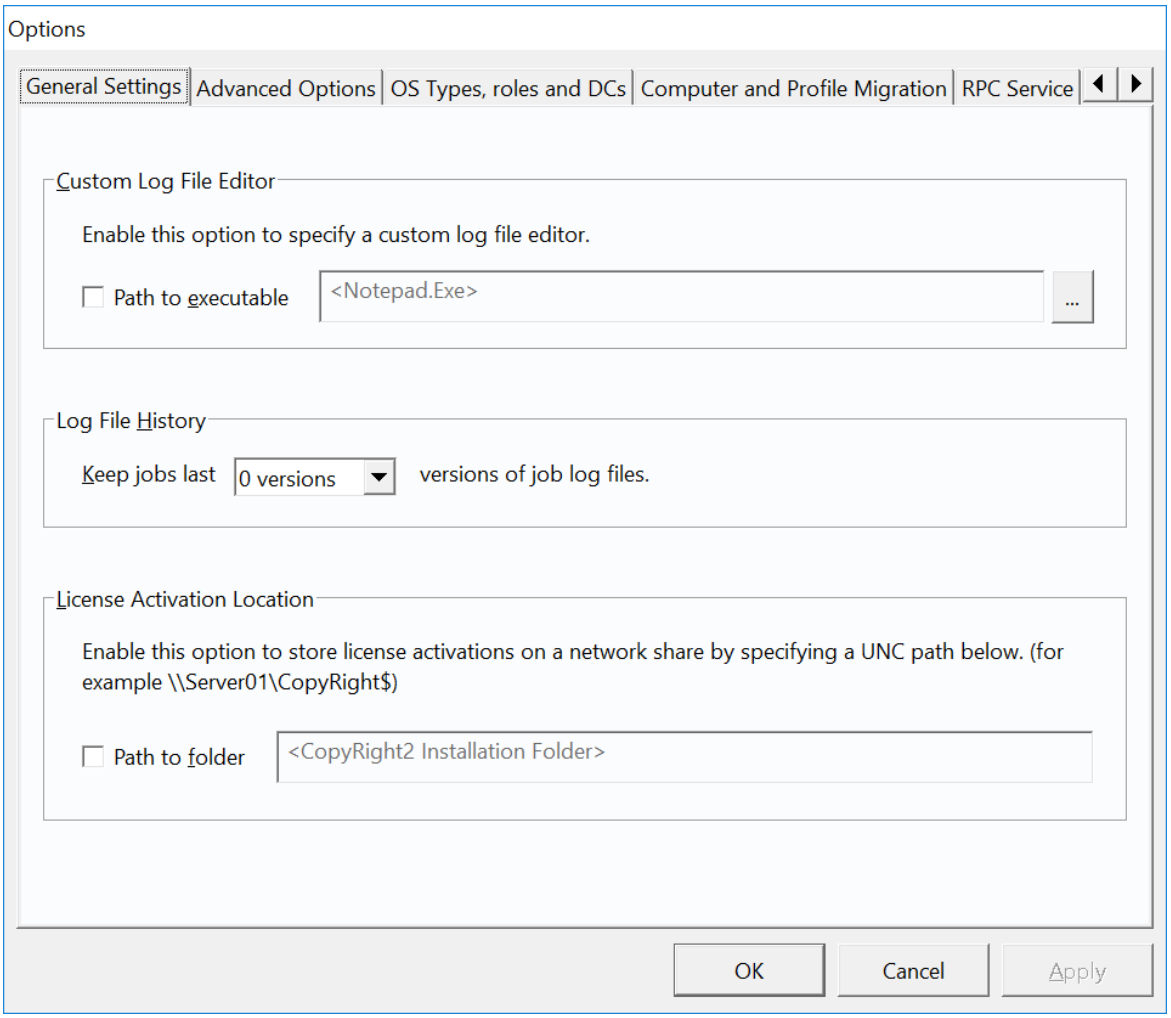
Command	Description
Refresh	Refresh the list of jobs shown currently.
Status Bar	Enable and disable the status bar.

Options

To display or change options, please click on the Menu button to the left and then select the “Options…” command to display the “Options Dialog”.



General Settings



Custom Log File Editor

In the “Custom Log File Editor” you can enable/disable a custom editor used to display log files after clicking on the “View Log File” button. If enabled, you can specify the path to a different editor, for example WordPad, or 3rd party tools such as Notepad++, Ultra Edit or others.

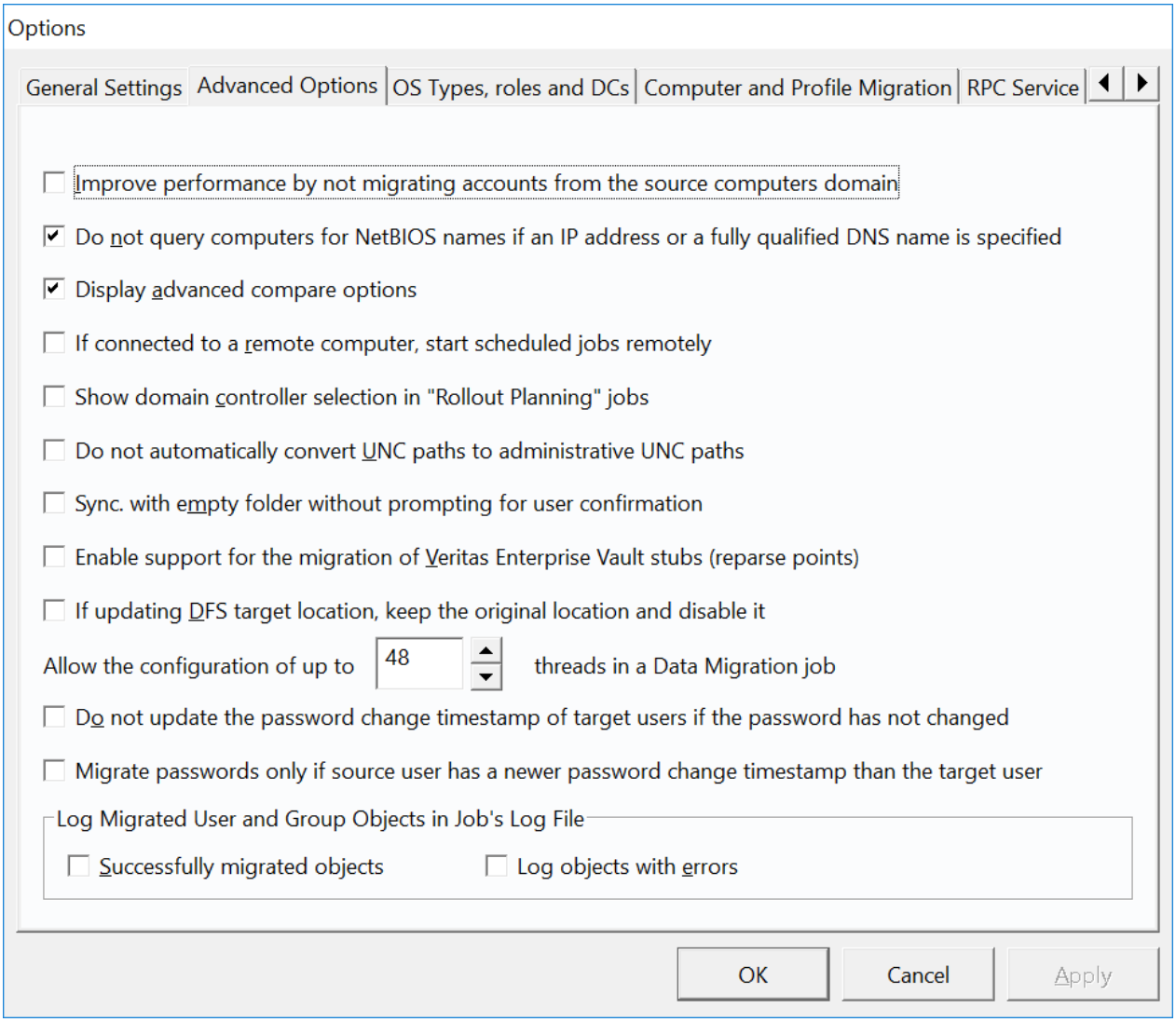
Log File History

The log file history option, allows you to configure the program to keep a history of log files instead of overwriting them, every time you are running the same job. It will keep the specified number of log files before deleting the oldest ones. By default, the program does not preserve the log file history. If using log file history, appending to the log file should be disabled in your jobs error processing page.

License Activation Location

You can define a custom location for storing license activations. By default, license activations get stored locally in the CopyRight2 installation folder. You could specify a UNC path here, to store license activations in that alternative location instead. This will allow to share license activations between multiple installations of the program. This change can also be made in the registry, please read the chapter” Changing the License File Location” for more information.

Advanced Options



Improve performance by not migrating accounts from the source computers domain

If source and target computers are in different domains, but you know for sure that accounts from the source computers domain should not be migrated and are valid on the target computer, through a trust relationship, you can enable this option to skip certain checks performed during the migration of NTFS or share permissions, to speed up the copy performance.

Do not query source computer for computer name if an IP address is specified

If you specify IP addresses as source or target of your copy job, which is not recommended but may work, enable this option to prevent CopyRight2 from using the NetBIOS name that the specified IP address serves for licensing purposes. If enabled, the IP address will be used instead of the NetBIOS name.

Display advanced compare options

If enabled, the advanced compare options will be shown in the “Compare File System” page of a data migration job (see chapter “Compare File System”).

If connected to a remote computer, start scheduled jobs remotely

If connecting to a remote instance, where CopyRight2 is installed, using the GUI, the program will by default execute the copy job locally on the computer where you run the GUI. If this option is enabled and you have scheduled a copy job for background execution on the remote computer, the copy job will instead run in the background of the remote computer.

Show domain controller selection

If enabled a “Rollout Planning” job will display the additional fields to define a domain controller for each source and each target server to control which domain controller CopyRight2 uses to query for information. This is useful if the AD site & services structure is not setup correctly to redirect the lookup queries to the desired domain controllers.

Do not automatically convert UNC paths to administrative UNC paths

By default, CopyRight2 automatically converts specified UNC paths, for example “\\SERVER\MyData$” into an administrative UNC path, for example “\\SERVER\C$\MyData” to access the source data in order to bypass share level permissions eventually restricting access. You can turn off that behavior by enabling this option.

Sync. with empty folder without prompting for user confirmation

By default, CopyRight2 will prompt with a warning if you attempt to synchronize an empty source folder with a destination folder containing data. You can turn off that behavior by enabling this option.

Enable support for the migration of Veritas Enterprise Vault stubs

If this option is enabled, CopyRight2 will migrate Veritas Enterprise Vault file stubs (reparse point). Please read the chapter “Support for Veritas Enterprise Vault” for more information.

If updating DFS target location, keep the original location and disable it

If this option is enabled and a “Data Migration” job has DFS update enabled, CopyRight2 will add the new location for DFS entries and disable the existing location instead of updating the DFS entry with the new location.

Allow the Configuration of up to 99 Threads in a Data Migration Job

Using this option, you can increase the maximum number of configurable threads of Data Migration jobs.

Do not Update the Password Change Timestamp

The default behavior for password migrations is to update the password change timestamp regardless, each time the job is executed. If the option is checked, the timestamp will only be updated if the password about to be set is different from the target account's current one.

Migrate Passwords Only if Source User has a Newer Password Change Timestamp Than the Target User

By default, the NT password hash gets migrated from source to target any time the job is executed. If this option is enabled, the NT hash will only be migrated if the password change timestamp of the source user object is newer than the timestamp of the target user.

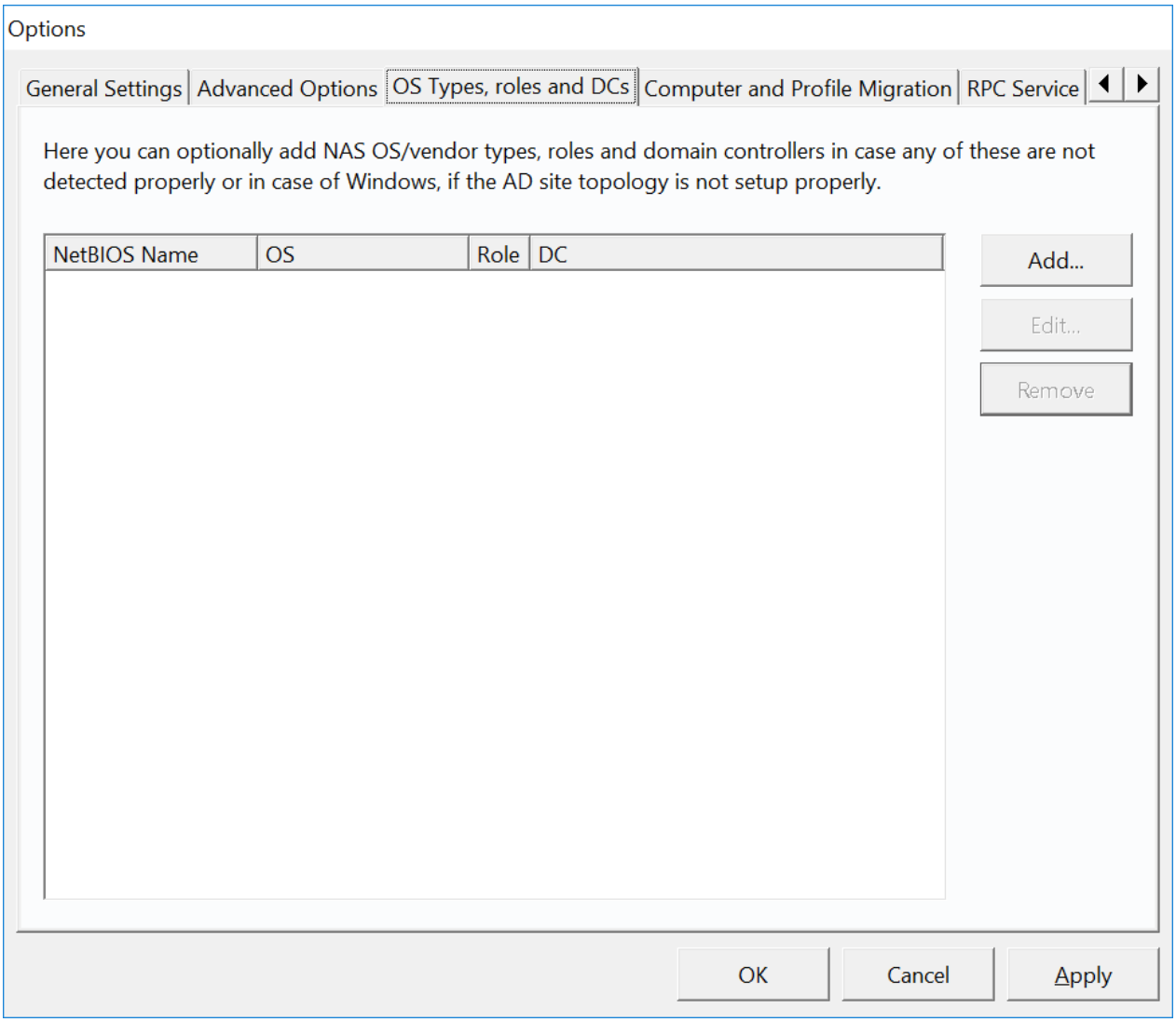
Log Migrated User and Group Objects in Job's Log File

If enabled, additional information about successful and/or failed migrated user and group objects, will be logged at the end of the job's log file.

OS Types, Roles and Domain Controllers

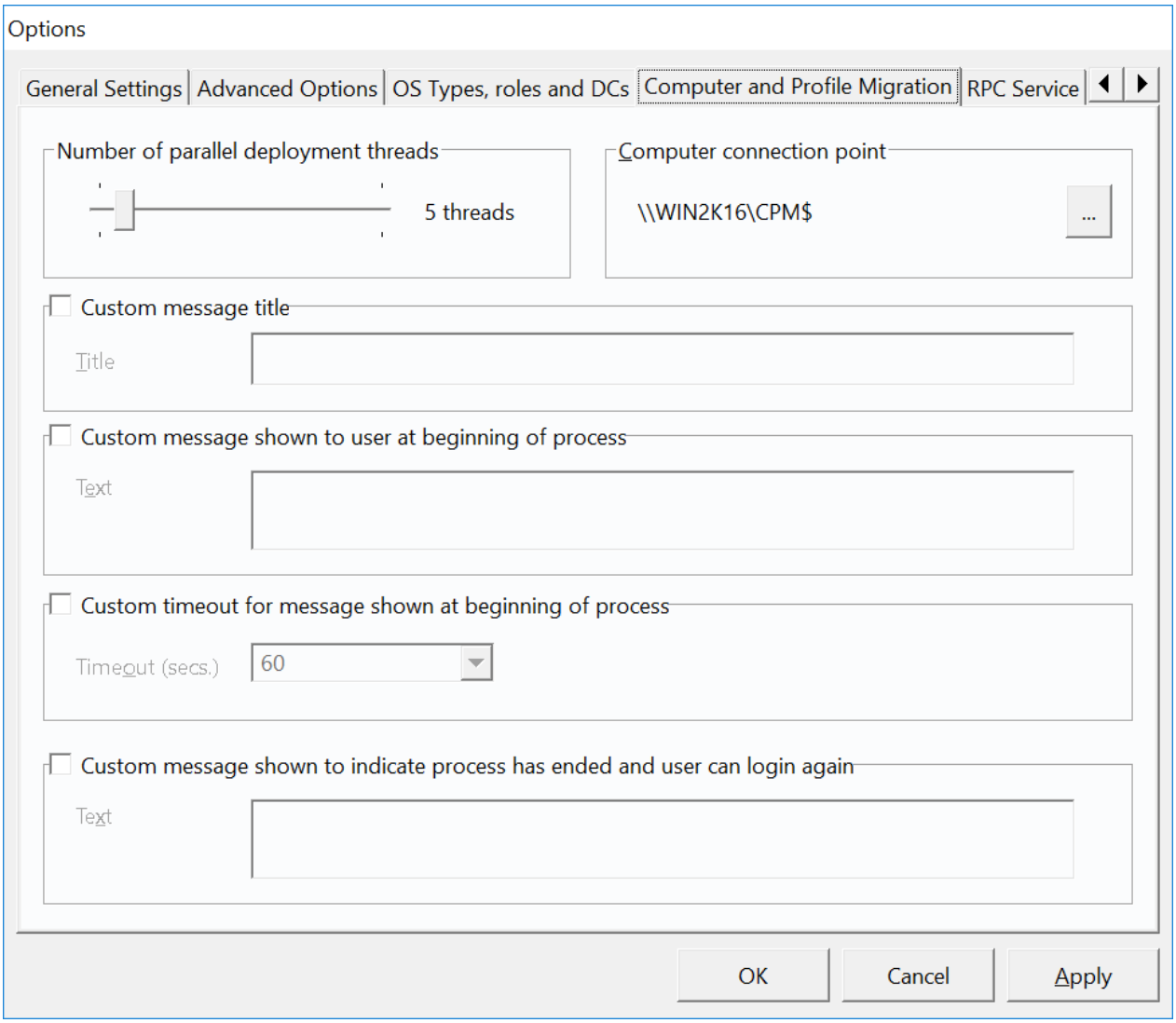
Here can optionally define OS types, roles and which domain controller to use for a specific system. Many NAS systems are, for example not properly detected as domain members. If you should find the role or the domain not properly detected in a copy job's log file, you can override the detection here. This is also useful in case of Windows systems, where the AD site topology is not properly defined, causing the program to use a domain controller that is not on the same site as your source or target system and you cannot (easily) change the topology because of corporate policies.

If your source or target is a Synology, Hitachi HDI NAS or an Azure storage account, you can define those OS types here. If your NAS is of another vendor, you can simply define it as "Auto detect".



Computer and Profile Migration

In the Computer and Profile Migration tab, you can configure settings relating to Computer and Profile Migration jobs.



Number of parallel deployment threads

You can configure the number of computers the job should get deployed to in parallel. The default setting is 5.

Computer connection point

Before a Computer and Profile Migration job can be run, you have to configure the computer connection point. The remote computers will connect to it to deliver their status and log file. To configure it you can press on the "…" button.

Custom message title

This is the window title to be used for messages shown to the user in front of the remote computer.

Custom message and timeout shown to user at beginning of process

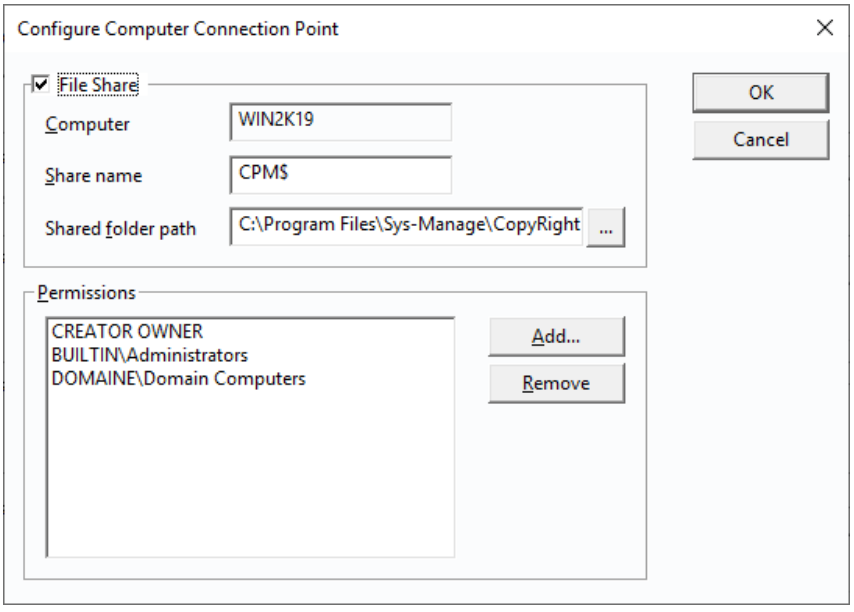
Those options allow you to configure the message shown at the beginning of the process along with a timeout value. After the defined timeout has been reached the message will be automatically closed and the process will continue.

Custom message shown to inditcate process has ended and user can login again

This option allows you to configure the message shown at the end of the process to inform the user that a login is now possible again. Please note that this message will only be shown if the job is migrating user profiles without changing the computer's domain, in which case no reboot is required and a logoff of currently working users is sufficient.

Configuring the Computer Connection Point

You can either turn on or off the computer connection point. Please note that the actual creation or deletion of the computer connection point will occur after clicking on OK or Apply of the Options dialog!



File Share

In the file share group box you can configure the computer the computer connection point will be configured on, the share name (default is CPM$) and the folder location (default is below "<CopyRight2 installation folder>\Data\Computer and Profile Migration").

Permissions

The default permissions will grant access to the Domain Computers group of the source domain. You could grant permissions to additional users that should administer the process or additional Domain Computers from other domains (in case the computers are already migrated to a target domain and you only want to perform the profile migration). You could remove the Domain Computers group from permissions and use a custom group that you make the computers to migrate a member of.

Note: Please note that the Computer Connection Point will be created on the local computer if you have not connected the GUI to an instance of CopyRight2 installed on a remote computer. If you should have connected to a remote computer having CopyRight2 installed, the Computer Connection Point will be created on that computer!

RPC Service

In the RPC Service tab, you can install and uninstall the RPC service and configure the service's context.

This service currently performs two functions:

a) It is used to perform domain join operations in case the target domain does not trust the source domain.

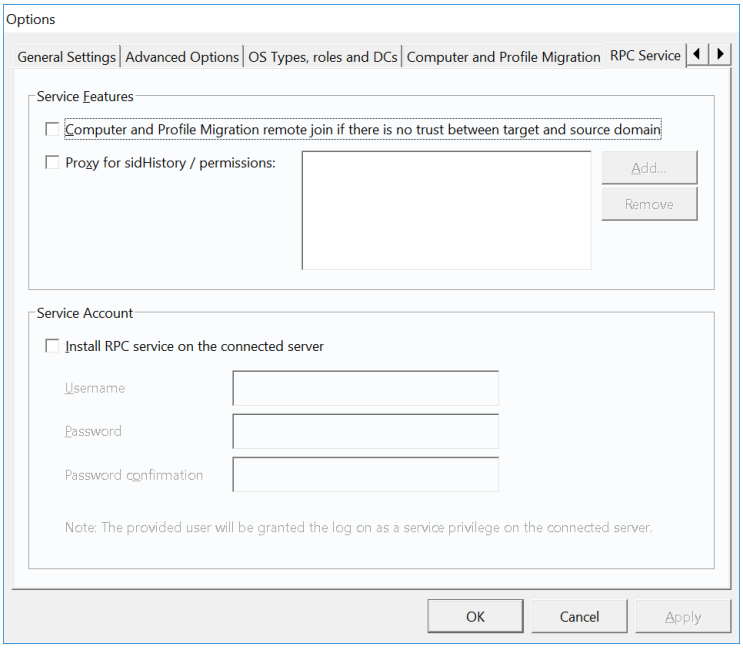
b) It is used to proxy the functionality to add to the sidHistory attribute for example for delegated admins that do not possess the "Migrate SID-History" permission in the target domain. It also solves the issue, where you have disabled delegation in the target domain for security reasons, forcing you to run the call that adds to sidHistory on the domain controller to let it use impersonation (RPC Service -> Source-DC) only instead of delegation (CopyRight2 GUI -> Target-DC -> Source-DC).

You can enable each of those two features. For the sidHistory proxy functionality, you can define a list of accounts you grant permissions to, to add to the sidHistory field if the calling account has full control access over the target AD object.

Once the dialog gets closed with OK or if Apply is clicked the service will be configured accordingly (installed and started or stopped and remove).

You can use a regular Domain user account or a managed service account.

For the remote join functionality, the account needs to be a member of the local Administrators group on the remote computers to migrate. For the sidHistory proxy, this accounts need to be at least a delegated admin having the "Migrate SID-History" permission in the target domain.



Note: You can optionally define an allow-list of target AD objects specified by samAccountName that can be used in addition to the full control check on the target AD object or instead of that check. To enable this functionality you

can modify the registry value HKLM\System\CurrentControlSet\Service\CopyRightRPCSvc\Parameters\Options which contains a DWORD.

The define Options value uses the following bitmask:

Value (hexadecimal)	**Meaning**
0x1	Enable sidHistory Proxy interface
0x2	Enable remote join interface
0x1000	Enable allow list check
0x2000	Disable AD target object full control check

For example, if you want to enable the sidHistory proxy interface and the additional allow list check of the target object's samAccountName, you would set the Options value to a REG_DWORD of 0x1001. A caller would then not only have to be on the list of accounts you granted access to, to call the proxy, but additionally the targeted object's samAccountName would additionally have to be in the allow list to let it succeed without being denied.

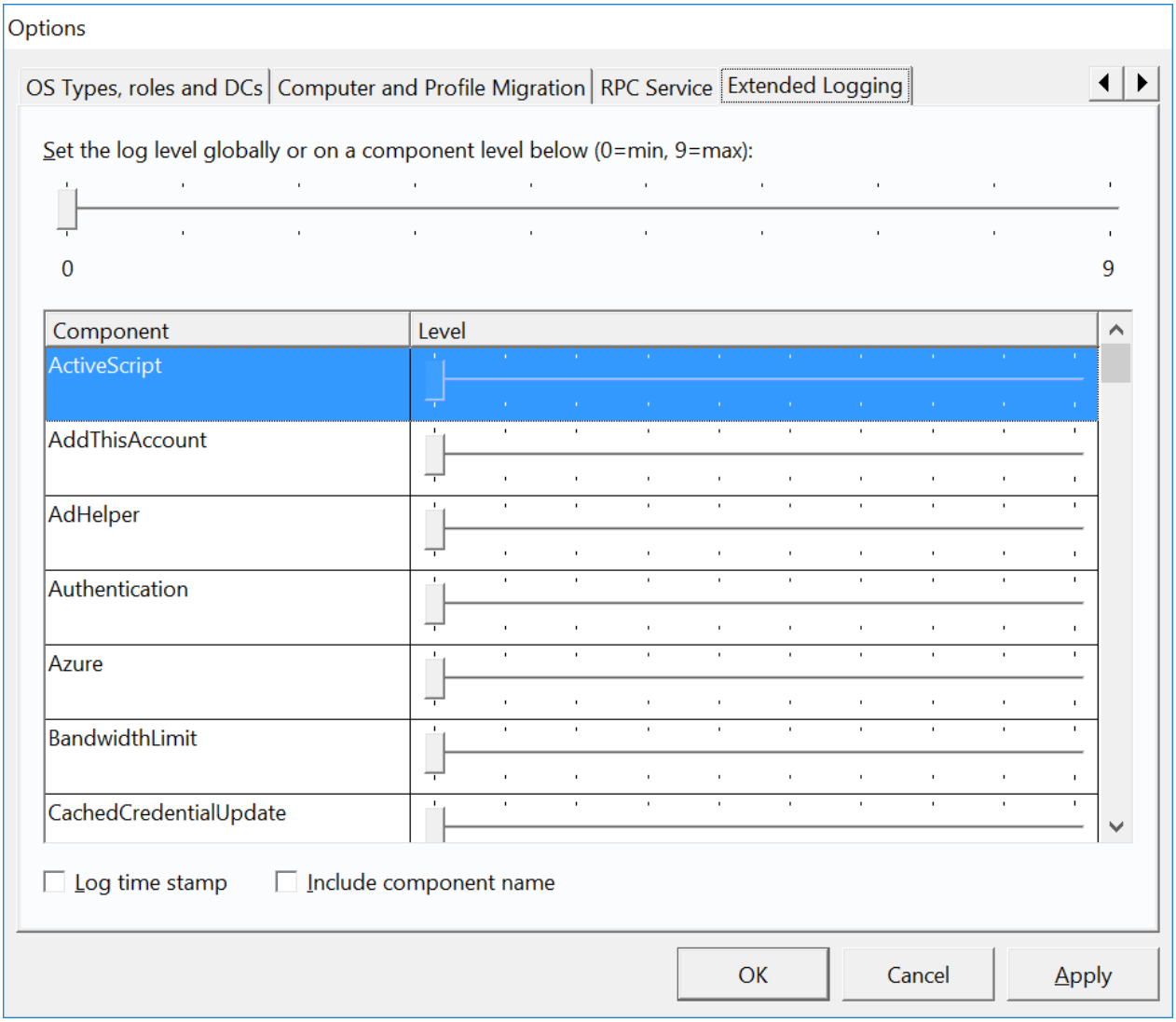
You could set the Options value to 0x3001 to enable the proxy and the allow list and at the same time turn off the access check validating that the caller has full control access over the target object. In that configuration a caller can add additional SIDs to any sidHistory attribute of any object in the target domain, as long as that object's samAccountName is in the list.

If the allow list option is enabled, the service will load that list from a file called sidHistory.txt which needs to be created in the CopyRight2 installation folder on the system where you have the RPC service installed.

Extended Logging

The extended logging dialog allows to set the logging level for all or for specific components to a level between 0 (minimum) and 9 (maximum).

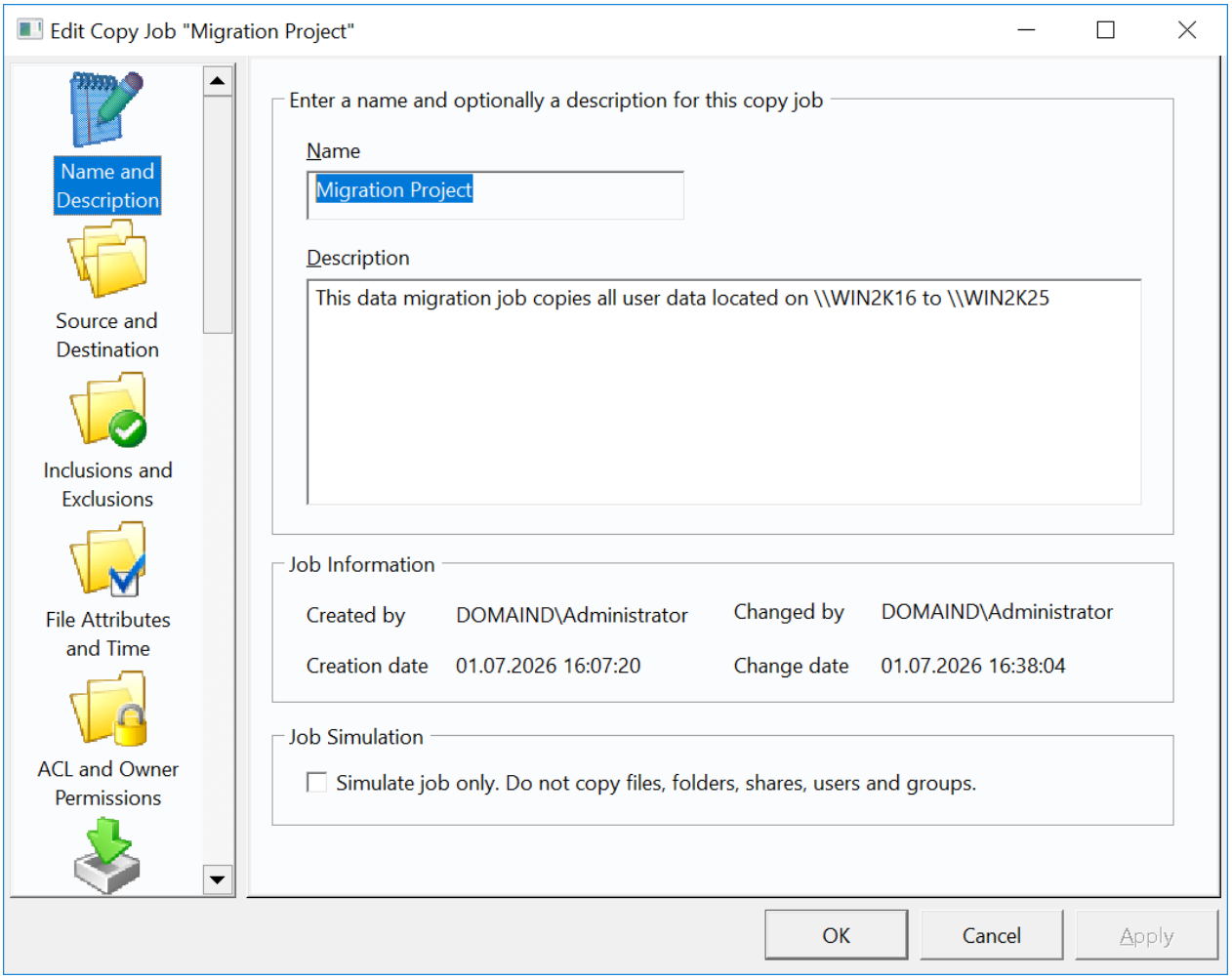
You can use the slider on top, if you want to enable logging for all components. Sys-Manage support may request an extended log file in case of troubleshooting.



Adding or Editing a Data Migration Job

Name and Description

Within this tab you can specify a job's name and description and if you want this copy job to actually write to the destination or if you want this to be a simulation only.



Job Name and Description

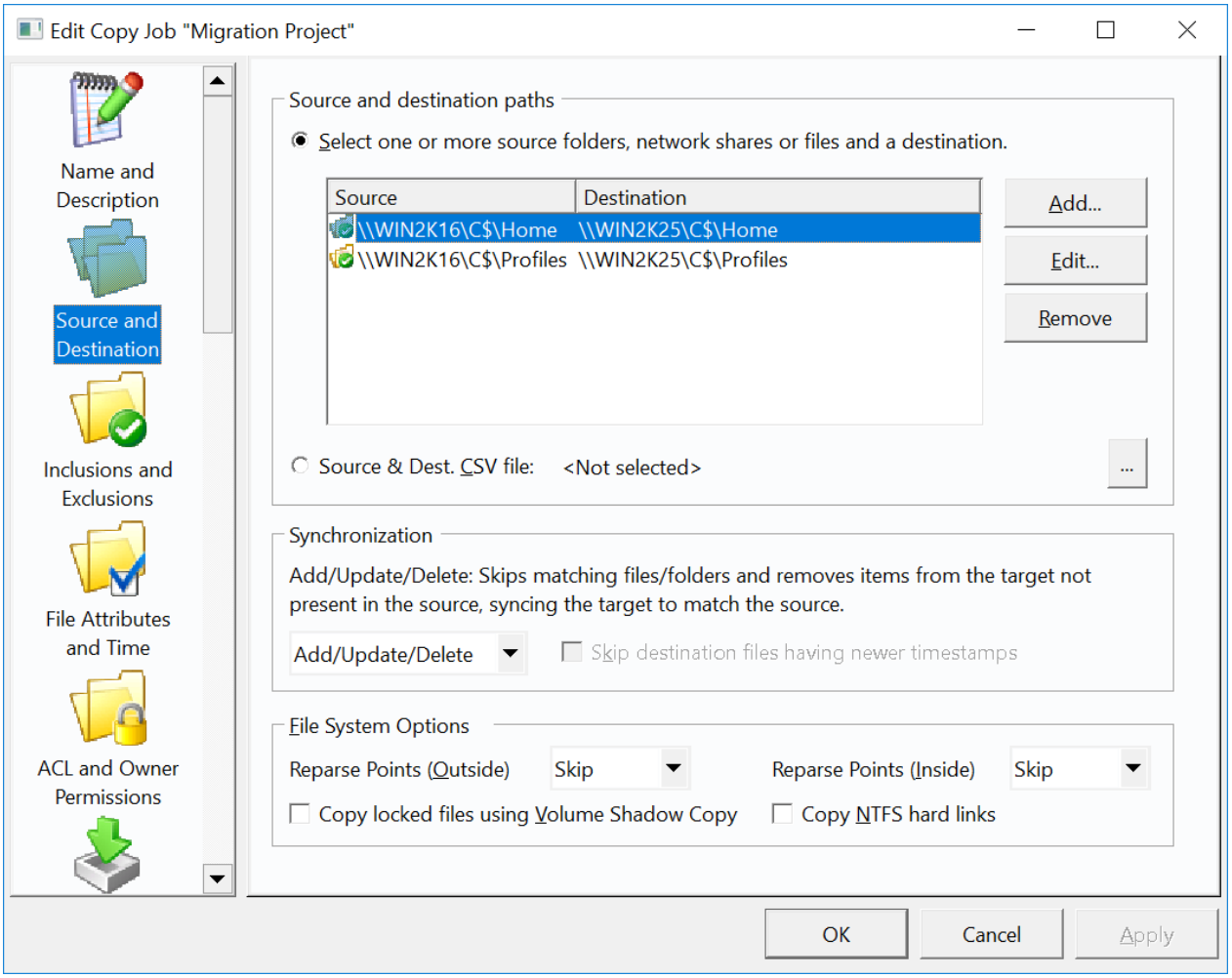
In the "Name and Description" tab of any job's definition you will see that each job has a unique name. You can optionally use the description field to describe the purpose of this job. Below the name and description, you will find information like who created this job, when this job was created initially, who changed the job most recently and when it was last changed.

Copy Job Simulation Mode

To test the copy job settings, you can enable the “Simulate job only” option. If this option is enabled, CopyRight2 does not copy any data, permissions, user or group accounts to the destination but tries if it can access any source files and write at the specified destination.

Source and Destination

Within this tab you specify a copy job’s source and destination folders and how to copy the data. You can choose to copy the data any time the job runs completely or to copy only modified files since the job ran the last time.



Source(s) and Destination Paths

Within this section you can add / edit / remove shares, folders or files to the list of copy operations that this job should perform. You can alternatively specify a comma separated file containing the source in the first column and the destination in the second column.

Synchronization

Those settings allow you to control how CopyRight2 copies data from the source to the destination.

There are 4 possible combination of settings:

Option	Skip Dest. Files Having Newer Timestamps	Description
Full Copy	Not checked	This default option, will copy all files & folders from source to destination regardless of timestamps. During a subsequent run, it will copy all the data again. If you want to improve the speed of subsequent runs, you would have to select one of the other options instead.
Add/Update	Not checked	This option will copy any new files and folders and additionally those having a different timestamp on the destination. This will improve performance for subsequent runs. It will not remove files on the destination that do not exist on the source anymore, for example files or folders that were renamed or deleted since the last run completed. So in case of a migration, you will end up with more data on the destination than on the source. This option is helpful if you are copying data to an archive for example. If you run the copy job and there is a file “a.txt” on the source and after the copy job completes, you would rename “a.txt” into “b.txt” and then run the job again, the destination would have two files “a.txt” and “b.txt”.
Add/Update	Checked	This option will copy any new files and folders and skip files having the same or an older timestamp on the source. This will improve performance for subsequent runs. It will not remove files on the destination that do not exist on the source anymore, for example files or folders that were renamed or deleted since the last run completed. So in case of a migration, you will end up with more data on the destination than on the source, because those deleted or renamed files will not be removed from the destination. If you run the copy job and there is a file “a.txt” on the source and after the copy job completes, you would rename “a.txt” into “b.txt” and then run the job again, the destination would have two files “a.txt” and “b.txt”. This combination is sometimes used during a pilot phase, where some users are already working on the target.
Add/Update/Delete	Not checked	This option will copy any new files and folders and additionally those having a different timestamp on the destination, effectively making the destination identical to the source. It will remove files on the destination that do not exist on the source anymore, for example files and folders that were renamed or deleted since the last run completed. This is the recommended setting for migrations.

Previous builds of CopyRight2 (<471) had 2 checkboxes instead of a combo box. In the table below you can see how the old options match with the new option:

New Option	Skip Identical Files	Sync. Source With Destination
Full Copy	Not checked	Not checked
Add/Update	Checked	Not checked
Add/Update/Delete	Checked	Checked

By default, CopyRight2 copies all the files from source to destination. If you want CopyRight2 to copy only files that do not exist at the destination yet, select the "Add/Update" or "Add/Update/Delete" options. This will speed up the copy process by skipping any identical files.

If you selected "Add/Update" you can additionally enable the "Skip destination files with newer timestamps" option to skip newer files at the destination as well. If this option is not enabled, CopyRight2 will overwrite any file changed at the destination with the original source file. This is not possible if selecting "Add/Update/Delete" because that would not make sense.

If you additionally want to purge any files existing at the destination that do not exist at the source, select the "Add/Update/Delete" option. If you run the migration in multiple phases, with a pre-copy, while users are still working and a final copy. This will cause CopyRight2 to delete any files at the destination that have been deleted in the meantime at the source since the copy job ran the last time. This option would be comparable to the Robocopy /MIR option.

CopyRight2 uses a file's modification time and the file size to determine whether a file should be copied or not.

Note: Please be careful when using the "Add/Update/Delete" option. If you specify a wrong source path or the wrong destination path, it will make the destination identical to the source. By default, it will warn you, if you attempt to synchronize an empty folder with a folder that contains data. You can optionally disable this warning prompt in "Options" if you have a requirement to synchronize a source folder sometimes having data and sometimes not, for example for automation purposes.

Reparse Points (Inside and Outside)

This option controls how CopyRight2 treats reparse points (a.k.a. junction or mounting points) and symbolic links. You can separately define this setting for inside (within the specified source paths) and outside (outside of copy job's specified source paths). The default setting is to skip them and continue with the next file or folder.

You can either skip them, copy them to the other system, translate (and copy) or follow them.

If the copy option is selected the reparse point will be created on the destination in identical form.

If translate is selected, reparse point will be copied and translated. For example, if "c:\data" containing a reparse point pointing to "c:\data\folder1" is copied to "d:\data" it will become "d:\data\folder1".

If the follow option is selected, CopyRight2 will follow the reparse point and copy any data as if the reparse point was a regular file or directory.

Mounting points are resolved at the file system level and can point to other volumes or even directories located on remote computers (requires corresponding Windows configuration!). Symbolic links on the other hand are resolved

on the client.

Note: The Windows volume deduplication feature introduced with Windows 2012 internally uses reparse points to deduplicate files that exist multiple times with identical content. If copying from such a volume, please make sure to select the follow option, otherwise deduplicated files will be missing on the destination after copying.

Copy NTFS Hard Links

This option controls how CopyRight2 treats NTFS hard links. If enabled CopyRight2 will migrate hard links from the source to the destination. Hard links are for example used by Windows to implement deduplication of the WinSXS folder located below the Windows folder.

Copy Locked Files Using “Volume Shadow Copy”

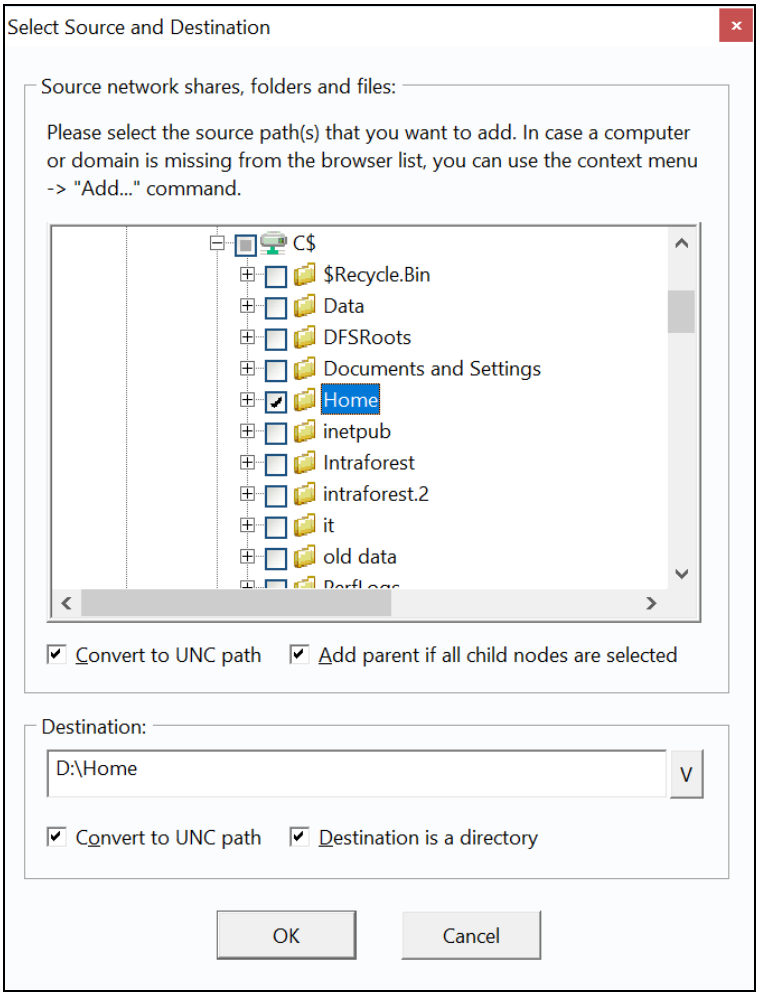
If this option is enabled, CopyRight2 will create a volume shadow copy of the source automatically to circumvent errors resulting from locked files. Please note that this option only works with Windows 2003 and newer operating systems. If used without block transfer mode (see Advanced Options) it only supports local files and folders as the source for the copy operation, pushing the data to the destination. If used in conjunction with block transfer mode you can either push or pull the data without this restriction.

Adding Files, Folders and Shares

After clicking on the “Add” button you can choose multiple file(s), folder(s) and share(s), even from multiple source servers and specify a single target. Clicking on OK will create the corresponding source and destination pairs within the list of shares, files and folders.

You can select a local path from the node below “This computer” in case the path is a local path. If the path is for a remote system, you can select it from below the corresponding computer account below the “Active Directory” node (shows only if you authenticated to Active Directory) or from below Network Neighbourhood -> Microsoft Windows Network.

What you see below Microsoft Windows Network is based on the Windows browser and it may not always show the computer you are looking for in some configuration cases. If a domain or workgroup does not show up, you can select “Microsoft Windows Network”, then open up the context menu (right mouse button click) to add it using the “Add missing domain/workgroup…”. Likewise, if a computer you are looking for should be missing, you can select a workgroup or domain below “Microsoft Windows Network” and then use the context menu and “Add missing computer…” to add it. This only needs to be done once and will then be stored for future use. You can remove manually added workgroups, domains and computers the same way using the context menu.



If the “Add parent if all child nodes are selected” option is selected, it will add one source/destination pair, if all child nodes of the parent are selected. This option is enabled by default. In case of a server consolidation case or if migrating from multiple source folders into a single destination folder, you may want to disable it.

For example, if you have the following structure on the source:
C:\HOME
C:\HOME\USER1
C:\HOME\USER2

If the “Add parent if all child nodes are selected” option is enabled and the two user folders are checked, the program would add a single source/destination for the C:\HOME folder, because all child nodes are selected.

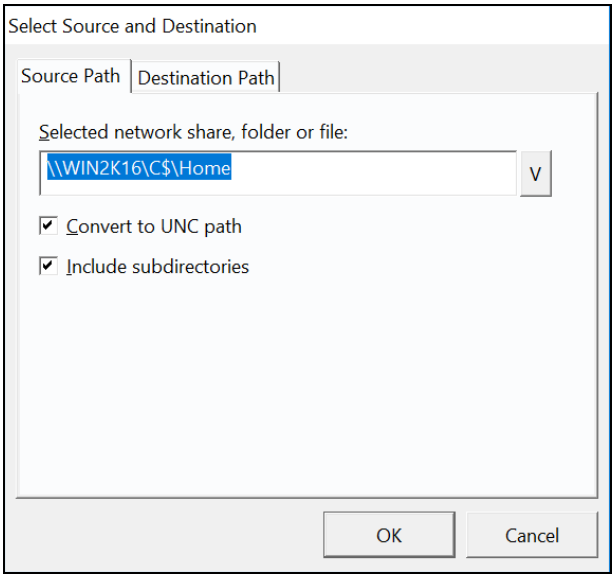
If the “Add parent if all child nodes are selected” option is not enabled and the “USER1” and “USER2” folders are checked, it will add two source/destination pairs instead, one for each folder containing data.

This is important if you want to use the “Add/Update/Delete” synchronization option, if you want to consolidate data from a different source, for example another “HOME” folder located on a different source drive or a different system.

If using the “Add/Update/Delete” synchronization option and having two source/destination pairs, one for the “C:\DATA” source and the other one for “E:\DATA” source, the first one would copy all data of the “C:\DATA” folder and the second one would make the destination identical to “E:\DATA”, effectively deleting anything on the destination that was previously copied from “C:\DATA”. In this case you should uncheck the “Add parent if all child nodes are selected” option and add a source/destination pair for each individual sub folder, for example “C:\DATA\USER01”, “C:\DATA\USER02” and “E:\DATA\USER03” and so on, to copy the data into the same destination folder.

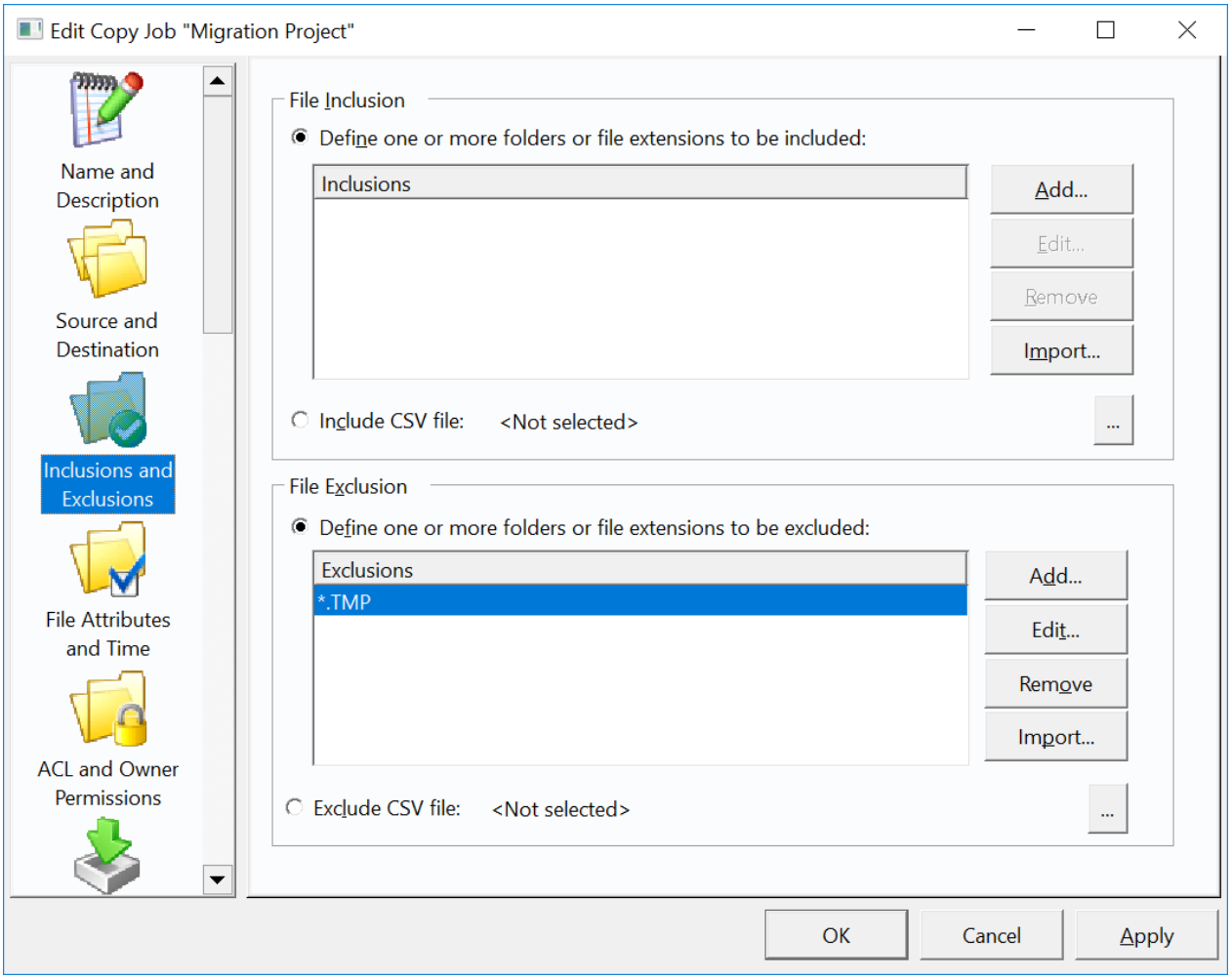
Edit Files, Folders or Shares

After clicking the edit button you can modify an existing source & destination pair’s source and destination path.



Inclusions and Exclusions

Within this tab you can optionally specify a filter defining which files or folders you want to copy (inclusion) and which files or folders you want to skip (exclusion). If the inclusion list is empty, as it is by default, all files and folders will be copied. You can use the wildcard character "*" and the placeholder "?" in your filter expression. For example "*.PST", "?:\MyFolders*" or "*\XYZ.TXT" are all valid expressions that could be used in an in- or an exclude filter. You can use the "Add", "Edit" and "Remove" buttons to modify each list. The "Import…" button allows the static import of a text file containing the file in- or exclusions. You can also specify the path to a text file if you want to process the content dynamically at runtime of the copy job.



File Inclusion

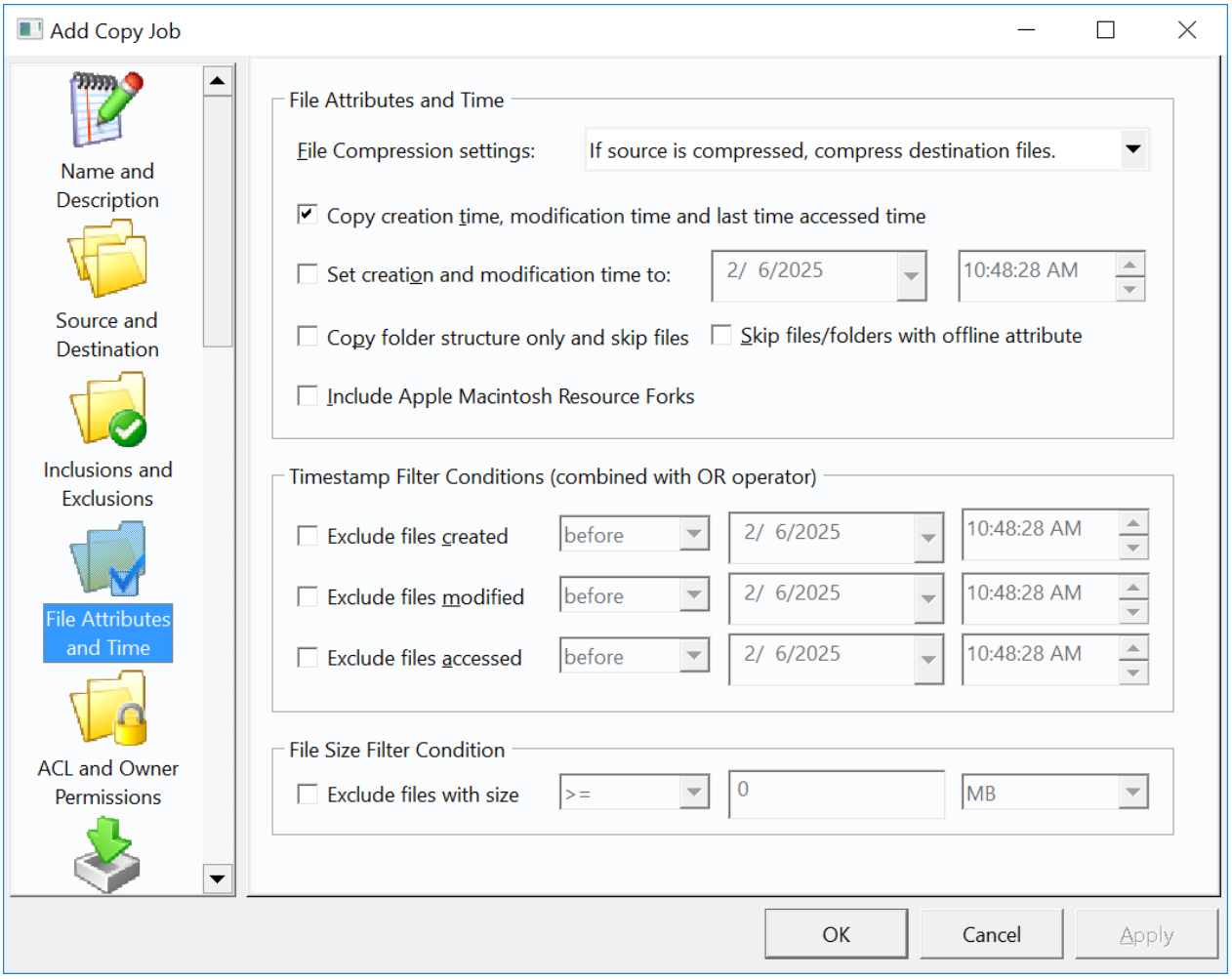
Within this list you can define the files and folders that you want to include in your copy job.

File Exclusion

Within this list you can optionally define the files and folders that you want to skip.

File Attributes and Time

Within this tab you can specify a copy job's properties regarding the treatment of file attributes and a filter to exclude files from the copy operation.



File Compression Settings

You can specify how CopyRight2 should treat the compression file attribute. You can either keep compressed files compressed, never compress files at the destination or compress all files at the destination.

Note: Compression is only supported on NTFS volumes. There is a Windows limit regarding the cluster size. Compression is only supported up to a cluster size of 4096 bytes. Because the maximum NTFS volume size is 2^32-1

clusters, this in turn means that the maximum volume size is 16TB. If you go beyond that limit, it is impossible to use compression. In this case select the “Never Compress” option to remove the compression attribute of all source files.

Set Creation and Modification Time

You can enable the “Set Creation and Modification Time to” option if you want all the files at the destination to have a specific timestamp.

Copy Creation Time, Modification Time and Last Time Accessed Time

This option is enabled by default and causes CopyRight2 to copy any files and folders creation, modification and last accessed time. If you disable this option, the timestamp used will be the point in time when the file or folder was created at the destination.

Copy Folder Structure Only and Skip Files

If you enable this option, CopyRight2 will only copy the folder structure from source to destination skipping any files.

Skip Files/Folders with Offline Attribute

If this option is enabled, any files having the offline attribute set, will be skipped during a data copy. This can be helpful if you want to migrate archived files or folders using a different method. If the option is not selected, the archiving software will restore the file content from the archive before it gets copied to the target by CopyRight2. Restoring the file from the archive takes additional time and disk space. Please read the chapter “Support for Veritas Enterprise Vault” for additional information about support for Veritas Enterprise Vault.

Include Apple Macintosh Resource Forks

Apple Macintosh resource forks can occur if there are Macintosh computers storing data onto the file server(s) to be migrated. It is some special information embedded within a file as a separate stream of data. You can enable this option, if you want to migrate any existing Macintosh resource forks.

Timestamp Filter Conditions

You can optionally define filters to exclude files that have been created, modified or accessed before a specified point in time.

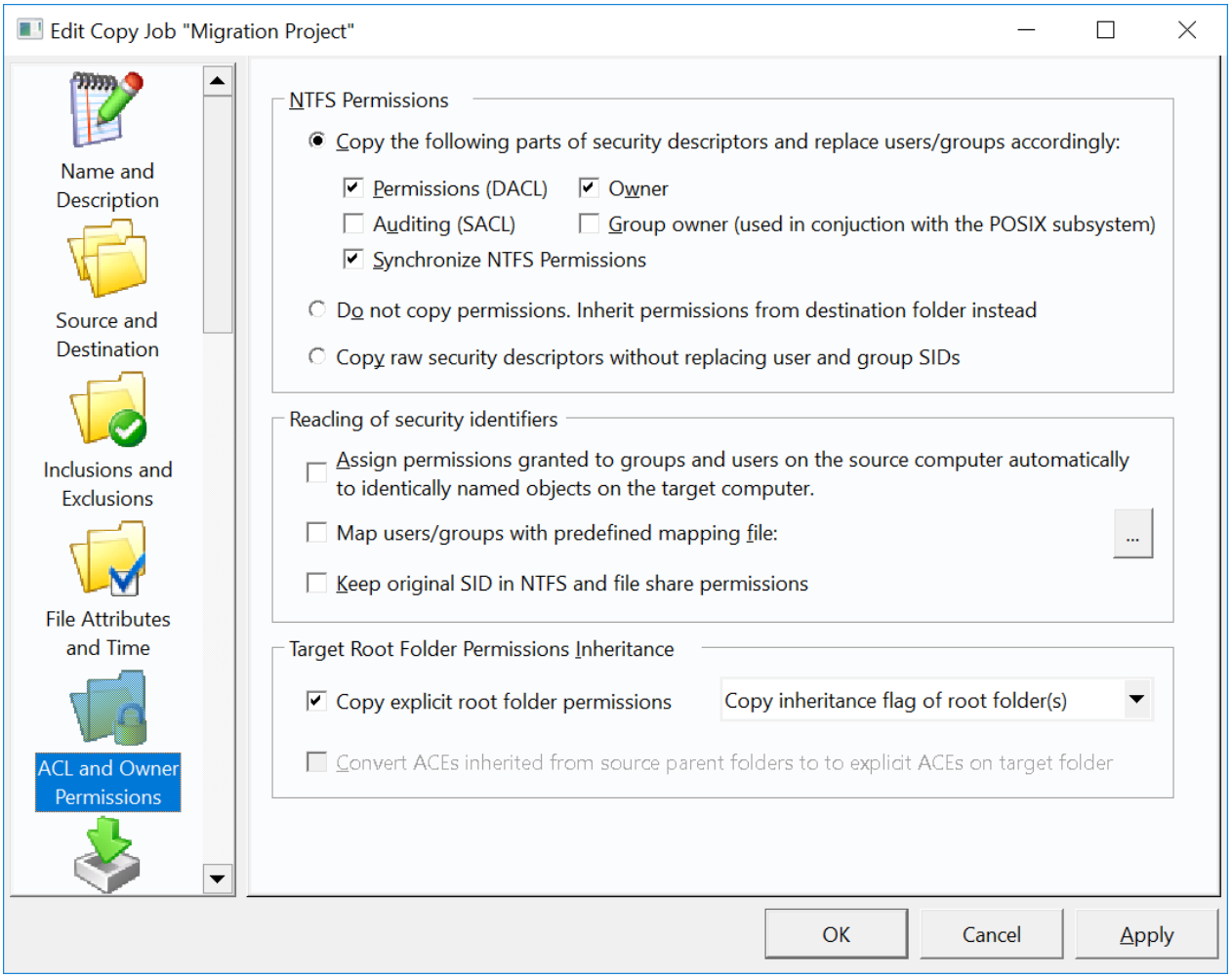
Please note that it is possible to define multiple conditions that will be logically OR’d. That means if you for example check “Any files created before” and “Any files modified before”, CopyRight2 will exclude all files that were either created or modified before the specified date (outdated files).

File Size Filter Condition

You can optionally define a file size filter condition to skip files based on their file size. As operator you can select either “>=” (larger or equal than), “<” (smaller than) or “=” (equal to).

ACL and Owner Permissions

Within this tab you specify how CopyRight2 should treat NTFS Permissions and Ownership. Additionally, you can enable the use of a mapping file that defines which user and group accounts of the source relate to which user and group accounts of the destination.



NTFS Permissions

You can either copy the NTFS permissions from source to destination, inherit the existing permissions from the destination folder or to copy permissions without applying any changes. If you choose to copy permissions, you can

select which parts of the ACL (Access Control List) you want to copy. You can copy the actual permissions (DACL), the owner, the auditing information (SACL) and the group owner that can be copied. The group owner is usually not used unless you have used the Windows POSIX sub system. It stores a SID of a user or group similar to the regular owner field. Actually the group owner is not even visible within Windows Explorer. The “Copy permissions without migrating users and groups” copies the raw security descriptor as it is defined on the source computer, without applying any changes to the SIDs used in permissions.

The “Synchronize NTFS permissions” is useful to minimize the runtime of copy jobs. It allows you to control how CopyRight2 treats NTFS permissions of files where the data was not changed since the last run. In its checked default setting it will migrate all NTFS permissions, even for files where the data was not changed since the last run. If the option is not checked, CopyRight2 will only migrate NTFS permissions for files that are new or where the data was changed since the last run, speeding up the process. This allows scenarios where you for example do a pre-copy with the option checked. Then you define a frozen zone, beginning with the start of your last pre-copy, where NTFS permissions should not be changed any more on the source, allowing you to run the final copy with the “Synchronize NTFS permissions” option unchecked to decrease the time spent during the final stage.

Reacling of Security Identifiers

In case you have local groups and/or local users defined on a member server, you can let CopyRight2 automatically use identically named users and groups that already exist at the destination server. This applies to global groups as well, in case of a migration crossing domain boundaries. To do so enable the option “Assign security identifiers of groups and users on the source computer automatically to identically named groups and users on the destination computer”.

You can define a so-called mapping file with the “User and Group Assignment” tool from the CopyRight2 start menu group, to define the relationship between accounts in the source and the destination environment. After creating the mapping file, you can enable the “Map Security Identifiers with a Predefined Mapping Table” option and then select the mapping file. You can read more about creating mapping files in the chapter “Creating a Mapping Definition File to Reassign Permissions”.

Keep original SID in NTFS and file share permissions

Use this option if you want to keep the original SID within permissions of the file system (NTFS) and file shares. If enabling this option CopyRight2 will add the identical permission (for example READ, EXECUTE, FULL ACCESS) for each user or group encountered, allowing the “old” user and group objects, that were migrated to ActiveDirectory using SID-History the same access they had before. This usually requires an additional cleanup job, that should be run after all user and group objects were migrated to ActiveDirectory, using a “Security and Attributes” type of job cleanup the file system and file share permissions at a later time (see defining a “Security and Attributes” job).

Target Root Folder Permissions Inheritance

The “Copy explicit permissions of root folder(s)” and “Convert ACEs inherited from source parent folders to explicit ACEs on target folder” options control if permissions of the specified source root folder(s), shall get copied to the target and how. It does not affect any folders (or files) below that level. Any files and subfolders below the specified source/destination folder inherit those permissions as well, if they have inheritance enabled.

Copy explicit permissions of root folder(s)	Inheritance	Convert ACEs inherited from source parent folders to explicit ACEs on target folder.	Description
Checked	Copy Inheritance	NA	This is the default setting. The program will copy the inheritance flag of the specified source folder(s). If a specified source folder has inheritance enabled, it will get enabled on the destination as well and it will inherit from the destination folder’s parent(s). Any files and subfolders below the destination folder inherit those permissions as well, if they have inheritance enabled.
Checked	Enable Inheritance	NA	The program will enable inheritance for the specified destination folder(s) regardless if the corresponding source folder had inheritance enabled or not. The destination folder will then inherit from its parent. Any files and subfolders below the destination folder inherit those permissions as well, if they have inheritance enabled.
Checked	Disable Inheritance	Checked	The program will migrate the effective permissions of the root of the specified source folder(s). If the source folder inherits permissions from its parent folders, those inherited entries will get converted to explicit entries for the corresponding destination root folder. Any files and subfolders below the destination folder inherit those permissions as well, if they have inheritance enabled.
Checked	Disable Inheritance	Not checked	The program will migrate the explicit permissions (not inherited) of the root of the specified source folder(s). Any inherited permissions from the source folders parents, are removed on the specified destination folder. Any files and subfolders below the destination folder inherit those permissions as well, if they have inheritance enabled.
Not checked	NA	Not checked	The program will not migrate permissions of the source root folder. Instead it will create the target folder if it does not exist and let it inherit from the targets parent folder. If the target folder already exists, the program will not make changes to the permissions. This allows you to define custom permissions for the target root level. Any child folders or files, below the target’s root will properly inherit those permissions as long as they have

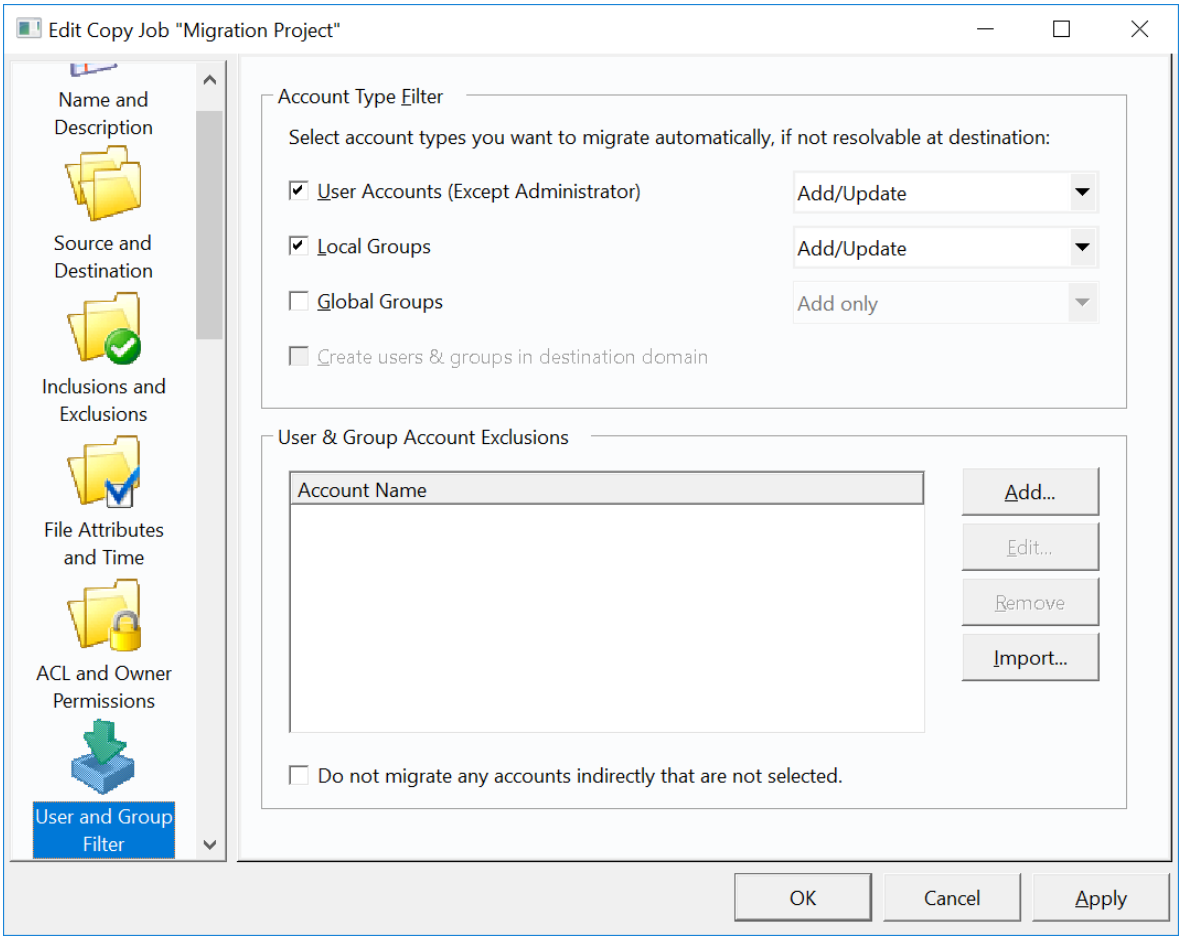
			inheritance enabled.

User and Group Filter

The user and group filter page controls how CopyRight2 should treat user and group accounts that are used in NTFS or share permissions on the source computer and that do not yet exist on the destination computer. You can enable the automatic migration of specific object types to prevent a copy job from asking for confirmation each time an object is discovered in permissions that requires a migration.

Additionally, you can specify how existing objects should be treated, by either selecting “Add only”, “Add/Update” or in case of user accounts “Add/Update/Remove”. The default setting of “Add only” will only migrate accounts, that do not already exist at the destination computer. If an account already exists, it will not be updated with account information from the source in this case. The “Add/Update” option will migrate non-existent accounts and additionally synchronize the information of existing accounts. Please note that this includes any account information except group members and user memberships which can be controlled by separate options (see “User and Group Migration”). The “Add/Update/Remove” option additionally deletes any objects that were created during previous executions of a copy job, that were either deleted or renamed in the meantime on the source system (lonely users).

NOTE: This account type filter replaces the “Sync. Users and Groups copied” option that previous builds of CopyRight2 had and allows a more granular control over how each object type should be treated. Having “Sync. Users and Groups copied” checked in older builds of CopyRight2 is equivalent to having “Add/Update” selected for each enabled account filter.



Account Type Filter for User Accounts, Local Groups and Global Groups

You can select which objects (users, local groups, global groups) you want to be transferred automatically from the source to the destination system in case they do not exist at the destination. This can be the case for example if you transfer data from a member server (that can have local users and local groups) or if transferring data cross-domain boundaries (users and global groups).

If enabled CopyRight2 will automatically copy the object to the destination server and replace its occurrences within any migrated NTFS or file share permissions on the destination system automatically.

Create Users and Groups in Destination Domain

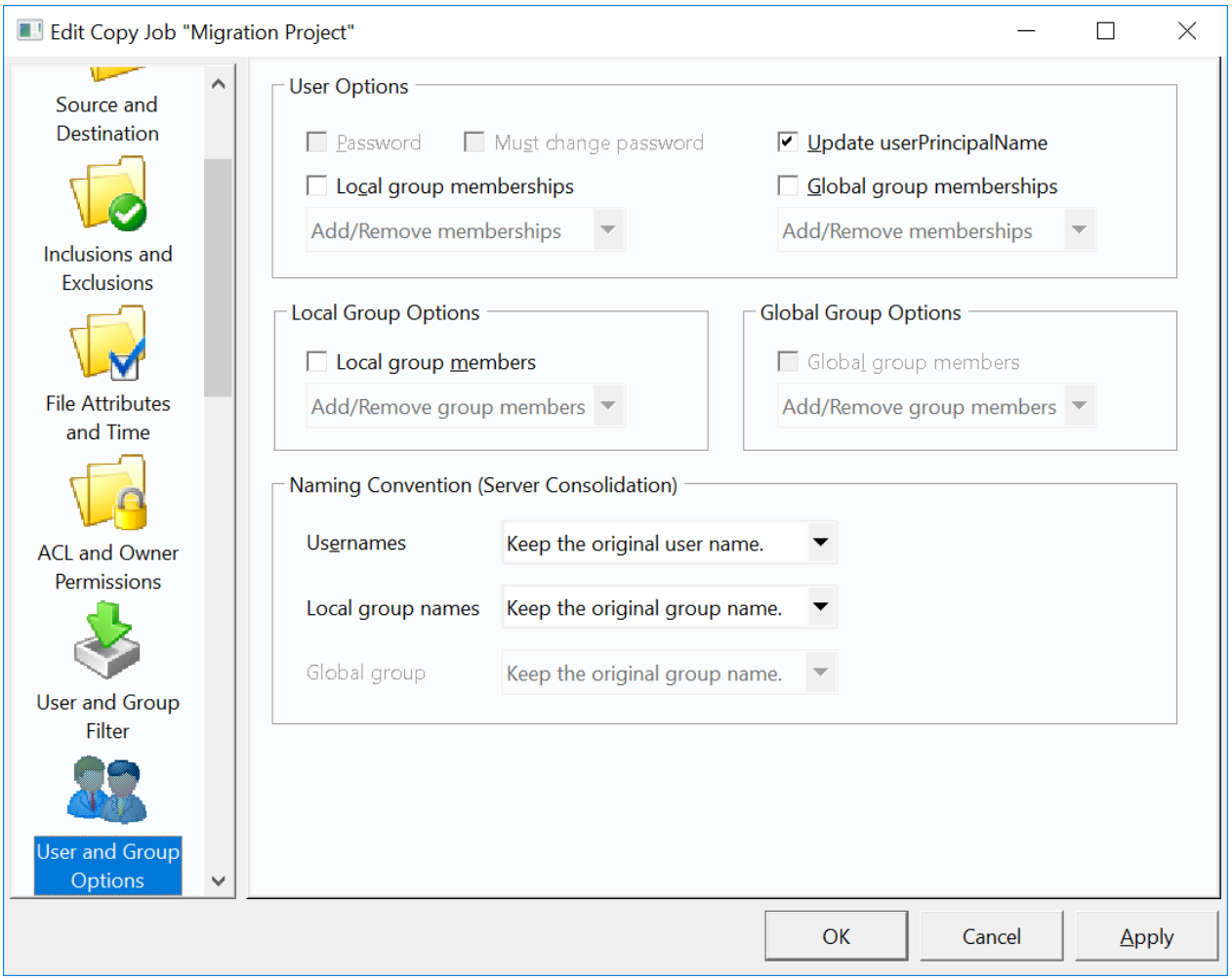
If this option is enabled any migrated local users and local groups are created in the destination server's domain instead of being created locally on the destination member server. If this option is not enabled, local users or groups will remain local objects on the destination server instead.

User & Group Account Exclusions

This list allows the exclusion of specific user or group accounts by specifying their samAccountName. Any excluded accounts will not be migrated during the copy job's execution.

User and Group Options

Within this tab you specify how CopyRight2 migrates user and group account information.



Migrate User Passwords / Must Change Password

If you have installed the separately available “PwdSync Addon for CopyRight2” you can copy the user’s password hashes (a.k.a. NT-Hash) as well. Please note that this option is disabled if you have not installed the add on. Additionally, you can enable the “Must change password” option to force the user to change the password during first logon.

Update userPrincipalNames

Enable this option to update each user’s userPrincipalName attribute in Active Directory by replacing the source domain name with the target domain name, while preserving the portion before the “@” sign.

For example: john.smith@source.com → john.smith@target.com

Local and Global Group Memberships

The options “Local group memberships” and “Global group memberships” control if CopyRight2 shall copy user’s memberships in groups as well. If enabled, CopyRight2 will attempt to add the destination account to the same groups the source account is a member of. If any groups are missing and the account type filter for groups is enabled as well, CopyRight2 will automatically create the groups at the destination as well. You can select either “Add only” or “Add / Remove memberships” to control if the program should add group memberships to destination accounts only or additionally remove the destination account from any groups that the source account is not a member of.

Local Group Members and Global Group Members

The options “Local Group Members” and “Global Group Members” do copy all user accounts that are a member of the encountered groups as well, even though these accounts themselves are not used directly within permissions of files, folders or shares being copied. You can either select “Add group members only” or “Add/remove group members” to control if the program should add members to destination groups only or additionally remove any group members of the destination group that are not a member of the source group.

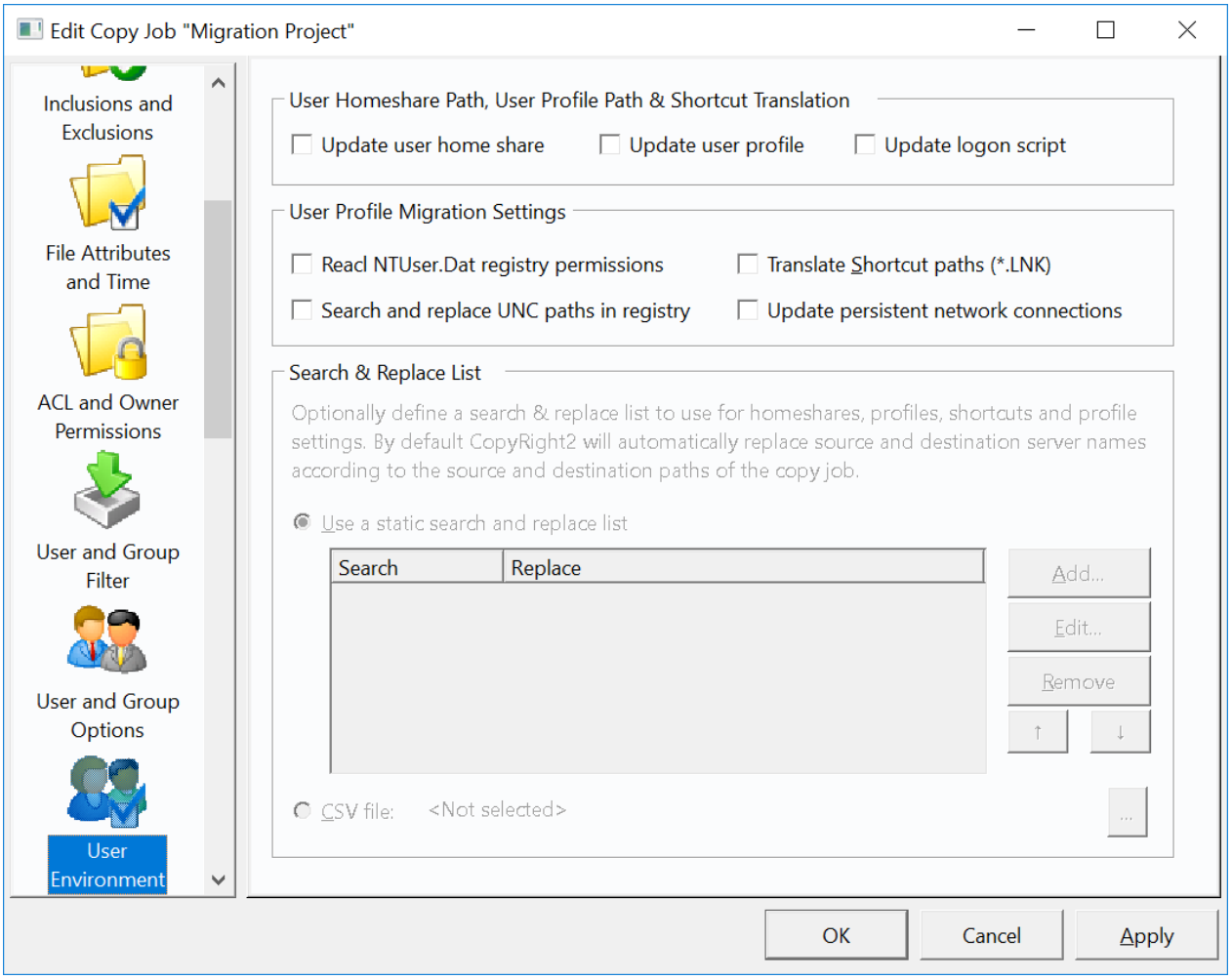
Naming Convention (Server Consolidation)

You can optionally define a prefix or suffix to be applied to the samAcountName of migrated users and groups, useful during server consolidations. For example, if you define a prefix “S1_” for local groups, a local group with a samAccountName of “Grp01” will become “S1_Grp01” on the target.

User Environment

Within this tab you specify if CopyRight2 should update home share and profile paths of local or domain users, how it should treat LNK shortcuts and if it should automatically migrate Windows user profiles (NTUser.Dat and NTUser.Man) on-the-fly while copying. By default, CopyRight2 will use the defined source and destination paths of the copy job to translate source to destination paths. You can additionally define a static search and replace list containing server names (server01 -> server02) or folder paths in case of local user accounts (for example c:\home -> x:\homeshares) or use a comma separated CSV file that is loaded dynamically at run-time.

These features work for local account migrations, for example between member servers or for the migration of domain accounts between domains.



Update User Homeshare & User Profile Path

If enabled CopyRight2 will automatically replace the user home share path or profile path in local or domain user settings. You can define a static search and replace list using the “Add…”, “Edit…” and “Remove” buttons or alternatively select a comma separated CSV file containing the search and replacement server names.

Translate Shortcut Path

If enabled CopyRight2 will automatically translate paths used in Windows shortcut files (.LNK) from source to destination.

Reacl NTUser.Dat registry permissions

If enabled CopyRight2 will automatically reacl Windows user profiles on-the-fly while copying, replacing user (or group) accounts in permission with the corresponding accounts of the destination. It will process regular and mandatory user profiles.

Search and Replace UNC paths in registry

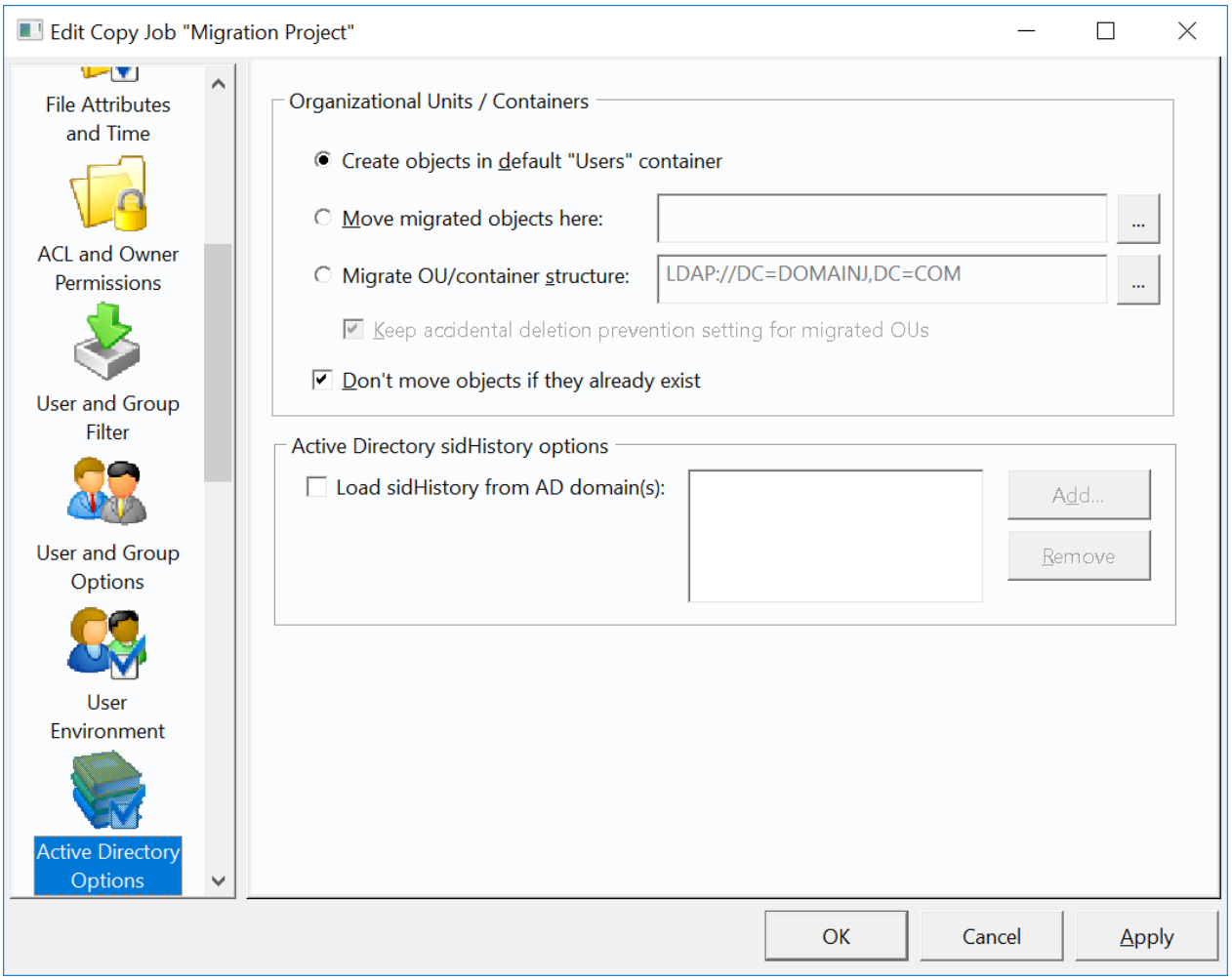
If this option is enabled CopyRight2 will translate references within user profiles, from source path to destination path, for example to take care of recently opened document lists contained in the user profile.

Update persistent network connections

If this option is enabled CopyRight2 will translate persisent network connections within user profiles, from source path to destination path, to take care of connected user profiles contained in the user profile.

Active Directory Options

Within the tab you can set options regarding the migration of Active Directory domain objects, for example to control where objects should be created in the destination domain.



Create Objects in Default "Users" Container

The default option will migrate any corresponding users and groups into the "Users" container. This includes domain users and groups requiring migration but also local accounts getting migrated to the domain because the "Create Users and Groups in Destination Domain" option is checked.

Move migrated Objects Here

This option will move any migrated objects into the specified OU or container. This includes domain users and groups requiring migration but also local accounts getting migrated to the domain because the "Create Users and Groups in Destination Domain" option is checked.

Migrate OU & Container Structure

This option migrates the source's OU and container structure to the specified location of the destination's Active Directory tree. By default, it uses the destination domains root as a target, causing any OU or container to get created at the same level of the directory tree.

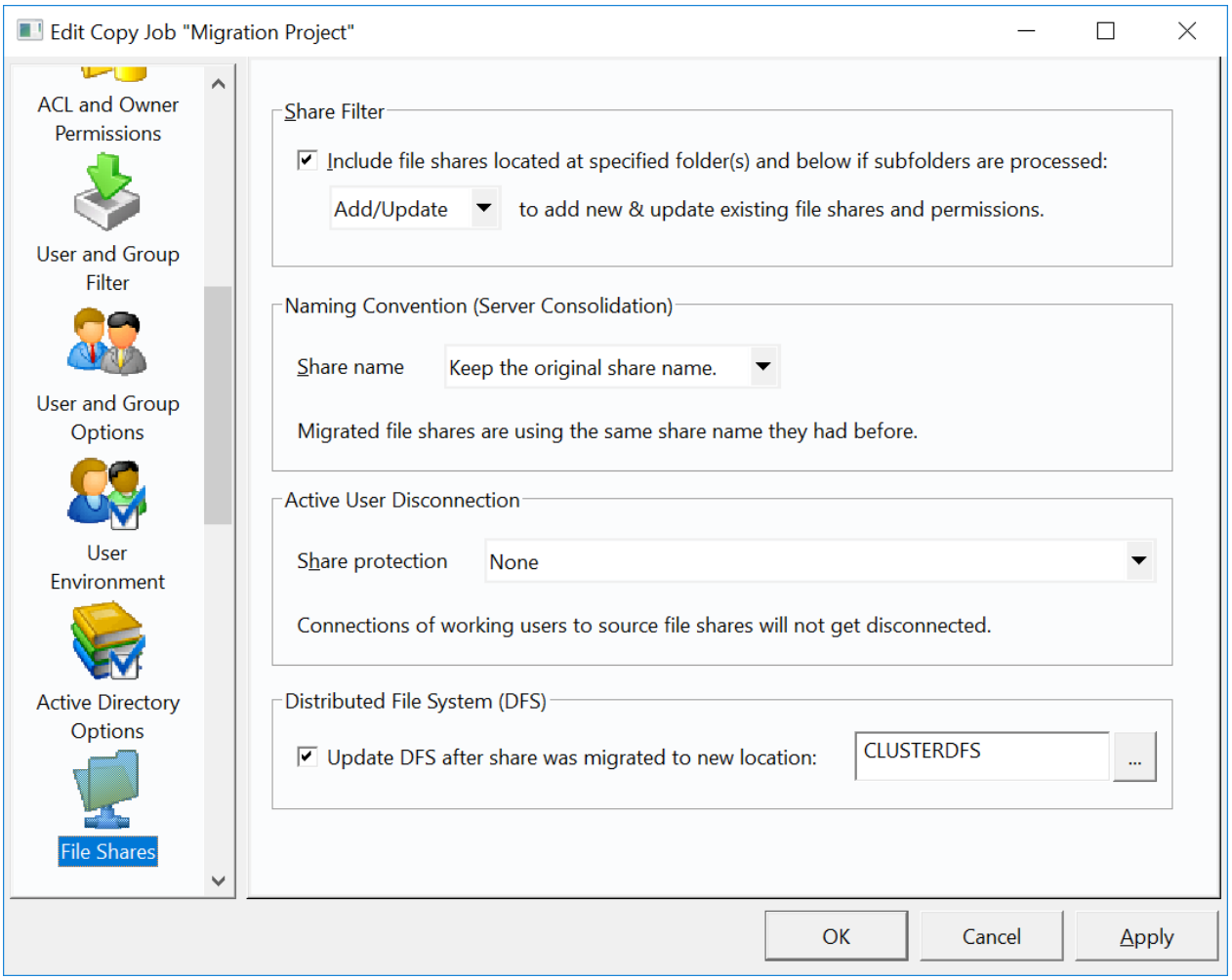
Load sidHistory from AD domain(s)

Use this option to specify one or more Active Directory domains that contain users or groups having the sidHistory attribute populated with their original SIDs. You can either specify a domain controllers NetBIOS name (for example DC9999) or a fully qualified DNS name of the domains (for example domain1.mycorp.com). If activated the job will use Active Directory to determine the existing mapping between old account SIDs and new account SIDs during job execution.

If you use this option CopyRight2 will query the specified domains for any user or group object that has the sidHistory attribute populated with one or more old SIDs and map them to the objects new SID to clean up the file systems NTFS and file share permissions by replacing the old SID(s) with the new corresponding SID.

File Shares

Within this tab you specify if CopyRight2 should copy file shares from the source to the destination computer.



Include File Shares

If you want CopyRight2 to automatically copy any file share existing within the copy job's source folders, then enable the "Include File Shares" option. Once enabled you can define the filter to either "Add only" file shares that do not yet exist on the target or "Add/Update" to create shares that do not yet exist and additionally update existing file shares locations, settings and permissions.

If you want to define a copy job that updates file shares on the target every time it runs, for example in a scenario with a pre-copy and a final-copy phase, please set this option to "Add/Update" to update the share location, settings and permissions every time the job is executed.

Note: Please set this option to "Add/Update" if you are copying a file share server internally, for example if moving a

share from one hard drive to another, because the file share is technically already existing as well in this case and has to become synchronized. Otherwise the share locations will not get updated accordingly.

Naming Convention (Server Consolidation)

You can optionally define a prefix or suffix to be applied to the name of migrated file shares, useful during server consolidations. For example, if you define a prefix “S1_”, a file share with a name of “Share01” will become “S1_Share01” on the target system.

Share Protection

If any users are locking files at the source, a copy job might fail. To prevent this from happening you can specify the following options, intended for the final copy, running before the cut-over takes place:

Option	Description
None	No special processing.
Disconnect Active Users	Disconnect any users connected to a share that is being migrated.
Disconnect Active Users & Deny Any Source Share Access	Disconnect any users connected to a share that is being migrated and additionally deny access to the source file share (otherwise users could potentially reconnect). This is achieved by adding an “Everyone:No Access” ace to the share level permissions of the share. **Note:** To undo those changes and rollback to the original source server, this permission would have to get removed for each file share on the source server!
Disconnect Active Users & Deny Source Server Access	Disconnect any users connected to a share that is being migrated and additionally remove “Access this computer from the network” privilege for anyone except the “Administrators” group when the copy job starts its execution.

If you want to define a copy job for the pre-copy phase, where users are still working, you may enable the option to “Skip errors resulting from locked files” or the “Use Shadow Copy Option” instead.

CopyRight2 will take these additional steps as soon as a folder is processed that is being shared. In case you use the option to deny source share access, CopyRight2 will remove the protection (from the share now residing at the destination) automatically after the share has been copied to the destination.

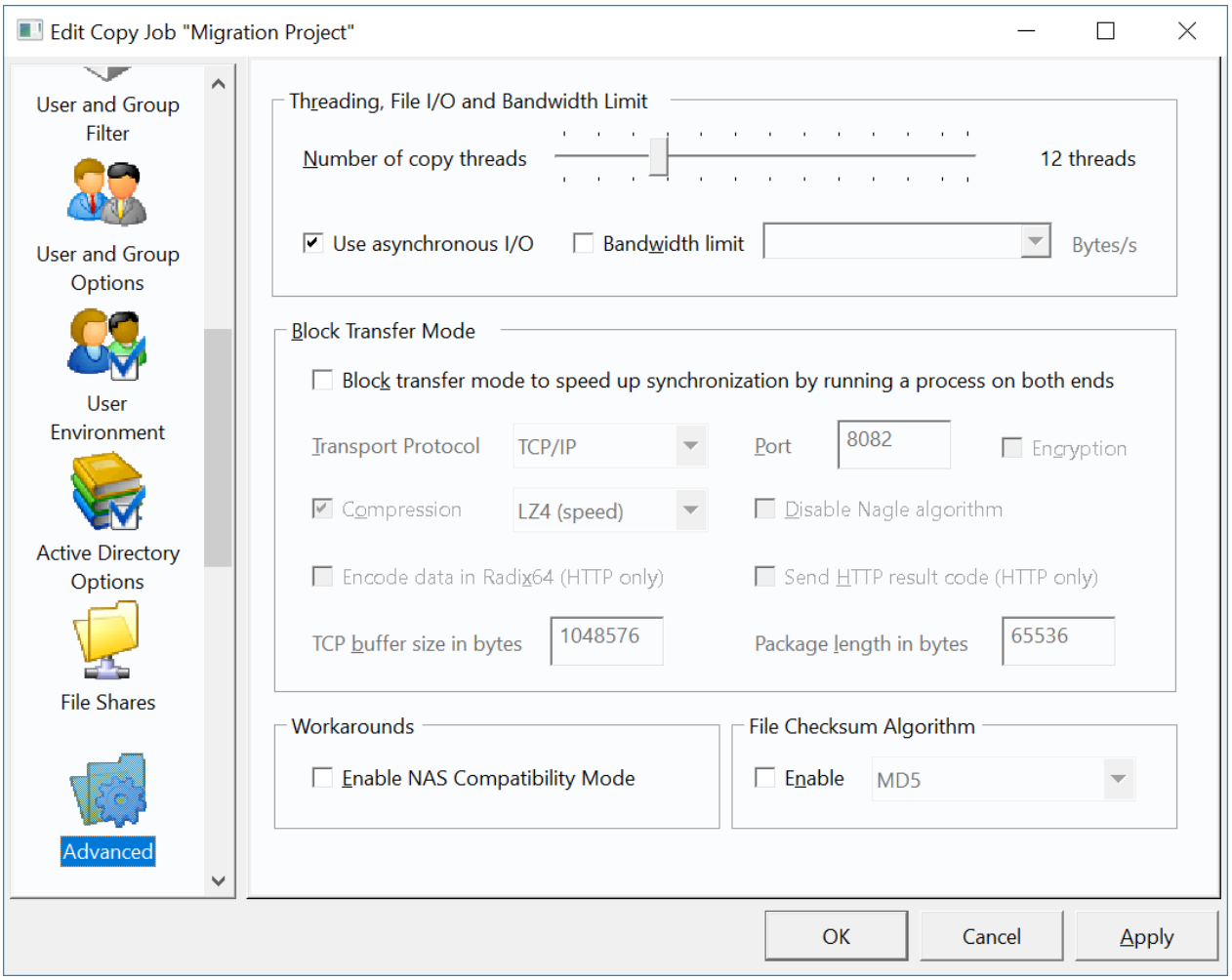
Please note that the original source share will still be locked to prevent users from making changes to those files!

Update DFS (Distributed File System) after share was migrated to new location

If the share(s) you are migrating do exist as links within a DFS server, you can update these to point to the share’s new location automatically after the share was migrated successfully. You can create such links by using a “DFS Copy Job”.

Advanced Options

Within this page you can specify advanced copy options.



Number of Copy Threads

With this option you can customize the number of concurrent threads that are used to copy files. The default setting is 12 threads meaning that there are 12 files copied concurrently.

Use asynchronous I/O

With this option you can enable or disable the use of asynchronous I/O when copying large files. Asynchronous I/O eliminates double buffering by the operation system and increases the transfer speed of large files. It reduces memory overhead caused by double buffering and lets the data use a more direct path between the disk driver and the CopyRight2 application.

Bandwidth Limit

You can use this option to specify a guaranteed bandwidth limit in bytes per second. CopyRight2 will automatically adjust its transfer speed to the specified limit during runtime.

Block Transfer Mode

Use this option to enable block transfer mode for your copy operation. This option is currently only supported if you run CopyRight2 on either the source or the destination AND if both, the source and the destination run Microsoft Windows. This mode will not use Microsoft's SMB protocol which can be inefficient if used across low bandwidth and low latency connections. It requires the installation of a service on the remote peer which will happen automatically. Both peers will exchange a file list and only modified files will be transferred. If there is already some data existent at the destination for a specific modified file, the sender will utilize that data and only transfer the modified blocks of the file.

Transport Protocol

The block transfer mode currently supports TCP/IP (default) and the HTTP protocol to transport data.

Port

Use this option to specify which TCP port is used for the data transfer. The default Port is 8082. Please make sure that you open up this port on your firewall for both peers (sender and receiver). Otherwise a communication between the two will not be possible.

Encryption

Use this option to enable data encryption for the data transfer. If enabled, all traffic will be encrypted by a combination of the RSA/AES-256 algorithms. If enabled, you will be prompted to confirm the remote peers fingerprint during the first time. The fingerprint is stored in the registry at HKLM\Software\Sys-Manage\CopyRight\PKI\Fingerprints or HKLM\Software\Wow6432Node\Sys-Manage\CopyRight\PKI\Fingerprints depending on the computers operating system and the version of CopyRight you have installed (32-bit or 64-bit).

In case of copying data across a VPN or if your network has TCP/IP encryption enabled on the network level, you do not need to enable this option as it will only slow down the copy process because the data is encrypted twice.

Compression

Use this option to enable compression for any data exchanged. CopyRight2 supports LZ4 (optimized for speed) and GZIP (optimized for size). If bandwidth is your limiting factor and if your computers have enough processing power, you may want to favour GZIP over LZ4.

Disable Nagle Algorithm

Use this option to disable the TCP/IP Nagle algorithm

Encode data in Radix64 (HTTP only)

Use this option to encode all data with Radix64. This may be required in case some proxy servers or other equipment are in between that do not support transferring raw data over HTTP. If the sender and receiver can communicate directly with each other, it is not required to enable this option.

Send HTTP result code (HTTP only)

If this option enabled, CopyRight2 will send a result code after each received HTTP request. If the sender and receiver can communicate directly with each other, it is not required to enable this option.

TCP buffer size in bytes

Use this option to control the TCP send and receive buffer size in bytes. By default, it is set to 1048576 bytes (1MB).

Package length in bytes

Use this option to control the maximum package length in bytes. By default, it is set to 65536 bytes (64KB).

Enable NAS Compatibility Mode

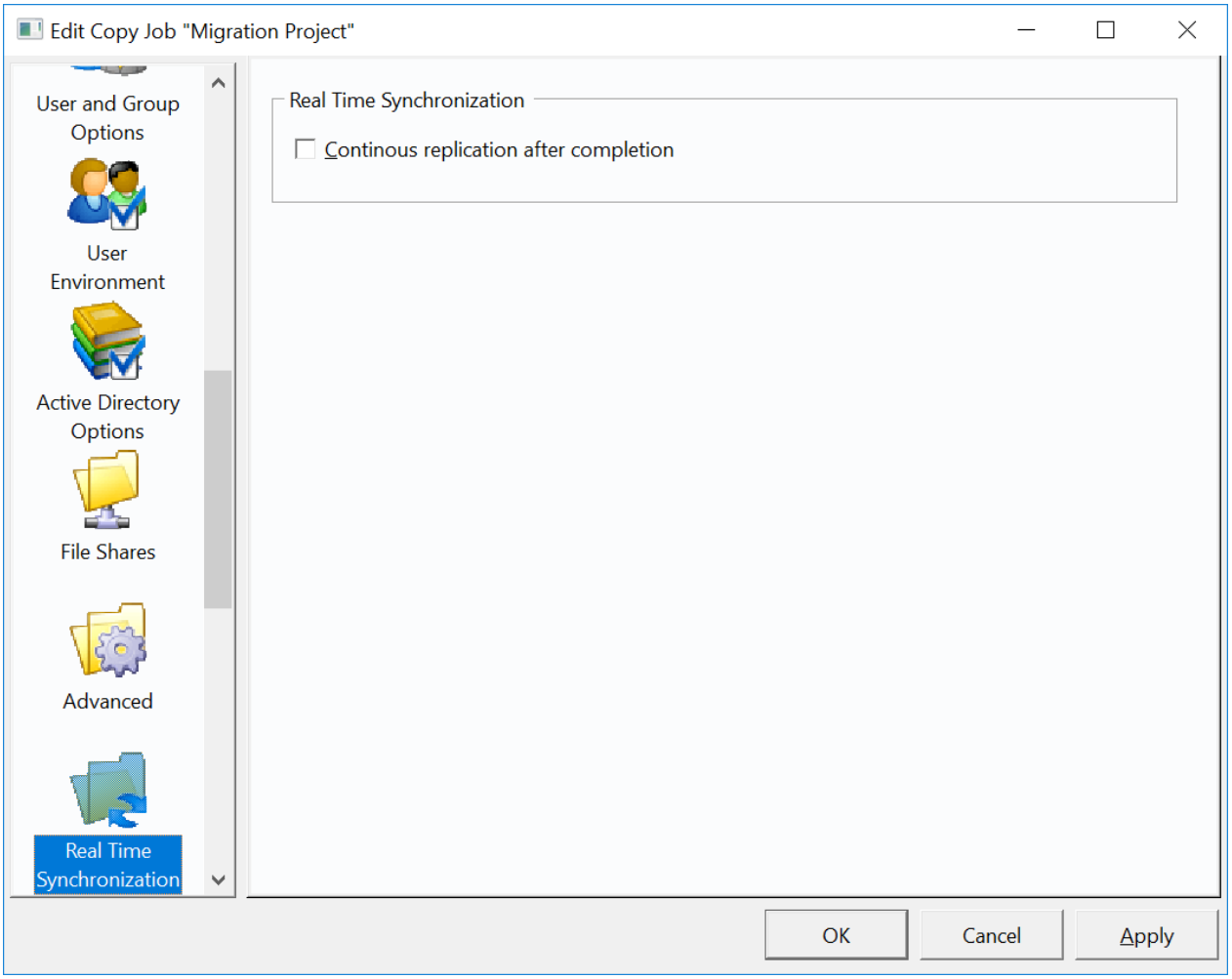
CopyRight2 contains multiple workarounds that are required if the destination server is for example a Network Appliance Filer running OnTap. If you encounter unexpected access denied errors, you should try the NAS compatibility mode.

File Checksum Algorithm

Select one of the existing algorithm to compare source and target files with. You can select CRC32, MD4, MD5, SHA1, RIPEMD160, SHA2-256, SHA3-256. Using block transfer protocol requires this option to be enabled. If enabled, you can find statistics in the log file’s footer section about hash matches and mismatches.

Real Time Synchronization

Within this tab you can enable the real-time synchronization feature.



Real Time Synchronization

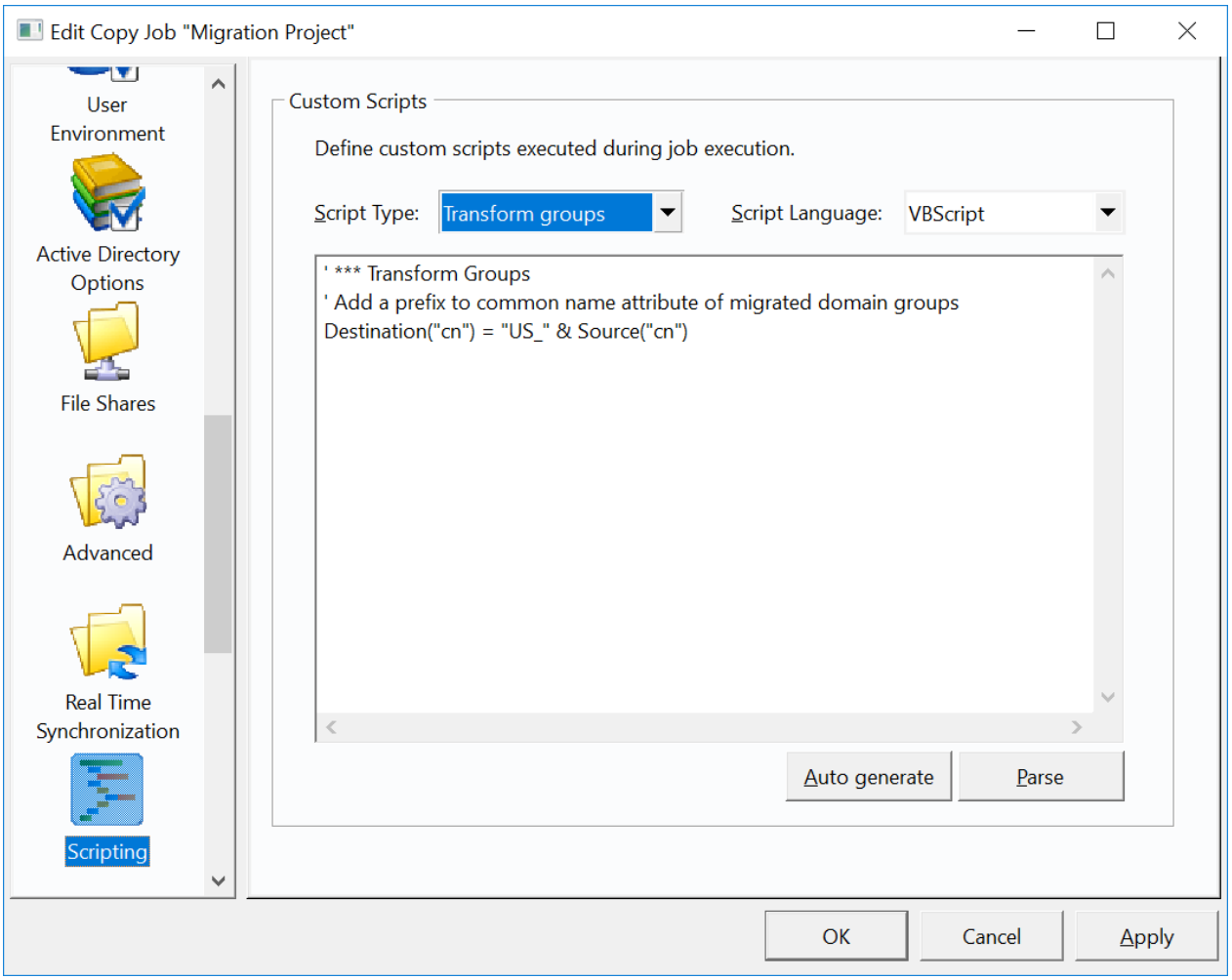
Use this option to minimize user down-time during the actual cut-over. If enabled the copy job will switch into real time synchronization mode, once the copy job completes to keep the specified source and destination pairs continuously in sync. The copy progress dialog will display the number of queued file changes (new files, changed files and updated files). If the number of queued files is 0, then the source and destination are in sync. You can stop the real time synchronization by clicking on the “Stop Sync” button. After stopping synchronization, you can resume it by launching the copy job again. If there were too many changes, CopyRight2 cannot resume the synchronization and will instead restart from scratch. You can see in the “Error Log” and log file if resuming was successful or not.

You can combine this feature with the volume shadow copy option to copy files that are in use (see “Use Volume Shadow Copy”).

Note: This feature requires execution on the source computer because of Windows restrictions. It requires the source to reside on an NTFS volume and administrative access to it.

Scripting

Within this tab you can define multiple custom scripts to get executed during specific events, for example when the copy job starts and also scripts executed during the migration of specific types of objects. You can use VBScript, which is the default option) or any other installed ActiveScript language to define the script's code. Please see the chapter "Using ActiveScript" for more information about how to write scripts.



Script Type

Please select the type of script. You can define scripts executed when the copy job starts and when it ends. You can also specify a script executed when two individual servers, specified as source and destination, do start and end

copying. Additionally, you can define scripts for each type of object that gets migrated (Users, Groups, Contacts, OUs).

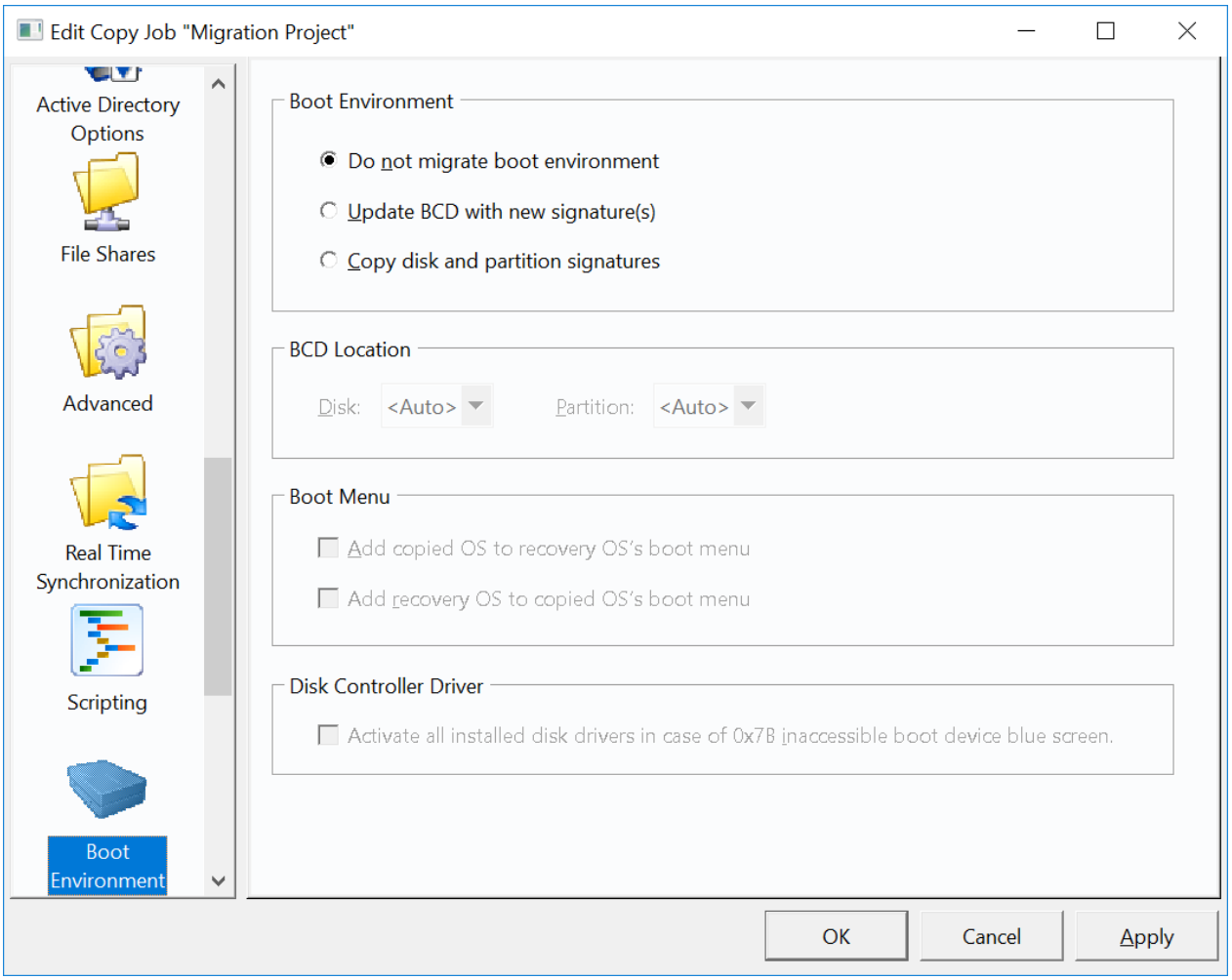
Script Language

The script language setting allows you to select which script language to use to code the scripts.

Boot Environment

The boot environment tab optionally allows you to migrate (or backup) the Windows installation and boot environment from the source to the target computer. This is useful for physical server migrations onto new hardware platforms but also for physical to virtual (P2V) and virtual to physical (V2P) migrations.

During such a migration the entire OS will get copied including user account database (SAM or Active Directory), so as a consequence of this there is no user or group migration required because any SIDs remain the same. Please make sure that you select the “Copy permissions without migrating users and groups“ option in the “ACL and Owner Permissions” tab. Otherwise any users and groups would get migrated to the recovery OS!



Boot Environment

The default setting of “Do not migrate boot environment” will not migrate files required to boot a copied Windows installation to the target. Selecting the “Update BCD with new signature(s)” will copy the required files and automatically update the copied boot configuration data (BCD) with the unique signature of the target disk &

partition. If selecting “Copy disk and partition signatures” it will copy the required files as well and update the target’s disk and partition signatures with the ones of the source disk. Changes to disk and partition signatures will only get applied to the disk/partition holding the copied Windows installation.

BCD Location

Usually CopyRight2 detects the location of the BCD on the destination. If this should fail, you can use the “Disk” and “Partition” options to select the corresponding location.

Boot Menu

The option “Add copied OS to recovery OS’s boot menu” adds the copied OS to the recovery OS’s boot menu so you can select it when booting the recovery OS. CopyRight2 will automatically append “(Restored)” to the boot menu entry so you can distinguish the entry from others. The option “Add recovery OS to copied OS’s boot menu” does the same to the copied OS’s boot menu. It will append “(Recovery)” to the boot menu entry of the recovery OS.

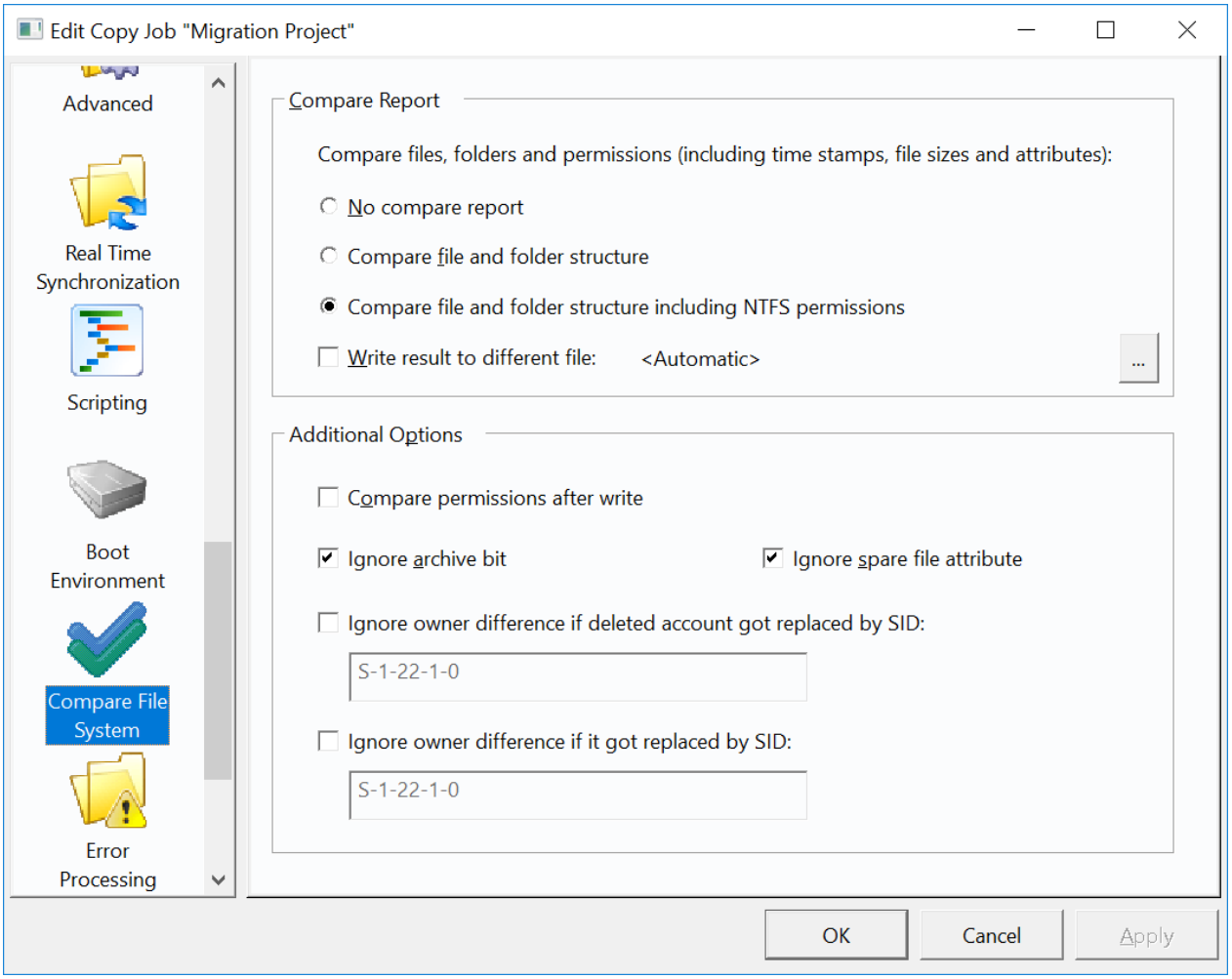
Disk Controller Driver

Try the “Activate all installed disk drivers in case of inaccessible boot device blue screen (0x7B)” option if the copied OS refuses to boot with a 0x7B blue screen usually indicating a missing boot driver required to access the disk.

By default, Windows disables loading of any drivers not needed to boot for performance reasons. So if you migrate from a system having a SCSI controller onto a system having an IDE controller the corresponding driver is possibly disabled and not loaded during boot time causing the blue screen error 0x7B. The performance impact is usually negligible, it will at worst increase the boot time by a few seconds.

Compare File System

You can use settings from the “Compare File System” page, to create a report comparing source and destination after a data copy job ran.



No Compare Report

The default option “No compare report” will not compare source and destination.

Compare File and Folder Structure

The “Compare file and folder structure” option, will compare files and folders and add the result to the copy jobs log file or to the specified file, depending on whether “Write compare result to a different file” is enabled or not.

Compare file and folder structure including NTFS permissions

If this option is enabled, CopyRight2 will compare the files, folders and additionally the NTFS permissions of each file and folder between source and destination.

Write compare result to a different file

By default, the result of the comparison is added to the copy job's log file. You can enable this option to let the program write the result to a different file.

Additional Options

The additional compare options are visible only after enabling them in "Options" (see chapter "Advanced Options").

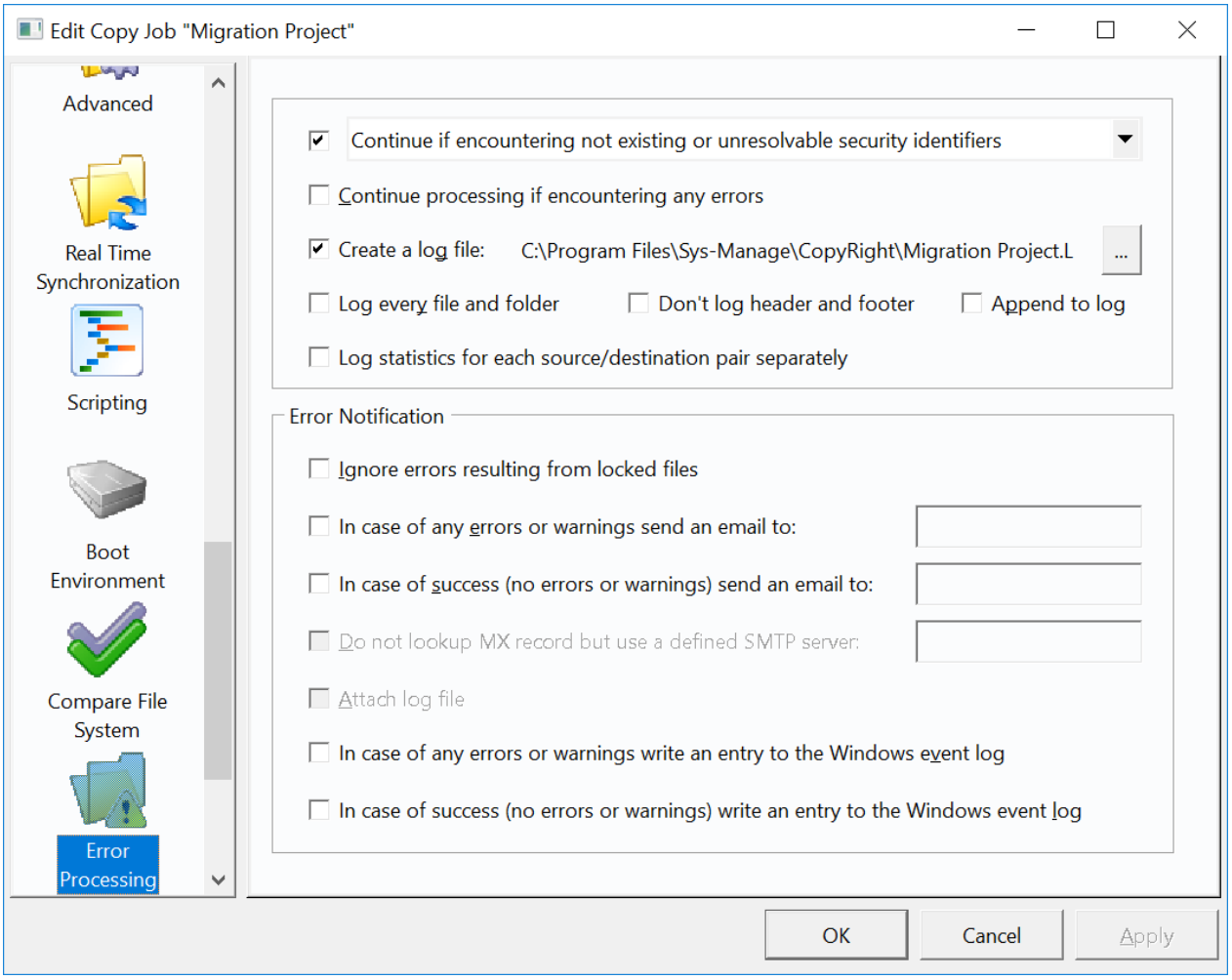
If enabled you can use "Compare permissions after write" to run the comparison of permissions immediately after a file or folder was copied, instead of comparing permissions after the job completed.

The "Ignore archive bit" and "Ignore Sparse File" options are enabled by default and can be disabled to compare those attributes. Usually you do not want to compare the archive bit, because the bit has to be set on the target and gets reset once the target server has been backed up. The sparse file attribute may get set on the target files and folders if the target server is using the Windows deduplication feature or an archiving solution.

If the target system is a NAS and it replaces SIDs of deleted accounts used as a file/folder owner in NTFS permissions by a well-known SID, such as the SID of the root account, you can enable the corresponding setting along with specifying the SID of the accounts they get replaced with.

Error Processing

Within this tab you specify how CopyRight2 should treat specific errors or errors in general. You can specify log file options and whether you want to receive a notification.



Ignore unresolvable security identifiers

By default, CopyRight2 continues and ignores errors resulting from unresolvable security identifier within a file, folder or share permission when copying data. If you want CopyRight2 to log the error and continue, select the option “Log and Continue if encountering unresolvable security identifiers”. If you want CopyRight2 to abort in case of this specific error, remove the check mark instead. Please note that such unresolvable security identifiers may exist if your source server has permissions containing accounts from domains that doesn’t exist anymore that were never removed.

Ignore any errors and continue processing

CopyRight2 stops a copy job if an error is occurring by default. It might be desirable to ignore any errors, for example in a multi-phase copy approach, where some data is copied initially (maybe even reoccurring) and a final copy job transfers the missing delta between source and destination server.

Log File

By default, CopyRight2 creates a log file within the installation folder going by the name of the specific copy job with a .LOG file extension. You can specify a custom path if clicking on the "…" button or disable the log file entirely by removing the check mark. To log every file and folder copied check the "Log every file and folder option". By default, CopyRight2 log files have a header and a footer part containing statistics. If you do not want the log file to contain those, you can check the "Don't log header and footer option".

Log Every File and Folder

If enabling this option, CopyRight2 will log every file and folder copied to the log file.

Don't Log Header and Footer

If enabling this option, CopyRight2 will not log the header and footer information to the log file.

Append to Log File

If this option is enabled, CopyRight2 will not overwrite the log file, but instead append to the end of the log file, each time the job is run. If you have enabled log file history in "Options", to keep a specific amount of log files and then rollover, this option should be disabled.

Ignore Locked Files

To skip any files locked by users actively working on the source computer, please check the "Ignore errors resulting from locked files" option. This will cause CopyRight2 to ignore any files that it cannot open because of file locking. This would make sense, for example, in a two phase approach, where the first copy job, ran during normal business hours copies as much data as possible while a second copy job, ran during an eventually small maintenance window, transfers only the files that have changed in the meantime (the delta).

Create Windows Event Log Entries for Job Results

If you want CopyRight2 to create Windows Event Log Entries after a job's completion, please select the "In case of any errors or warnings write an entry to the Windows Event Log" and/or the "In case of success (no errors or warnings) write an entry to the Windows Event Log. This will cause CopyRight2 to write to the event log of the computer the job has been running on.

Automatically Send Status Reports via SMTP

CopyRight2 can keep you updated about the result of any jobs by sending out emails via SMTP. To define such a notification, open up the “Error Processing” tab of your job and select “In case of any errors or warnings send a email to” and/or “In case of success (no errors or warnings) send an email to” and provide a valid email address in the format account@domain.com.

By default, CopyRight2 attempts to lookup the mail server using a DNS query. You can alternatively provide a fixed SMTP server that will be sent to by using the option “Do not lookup MX record but use a defined SMTP server” together with a valid SMTP server DNS name or IP address.

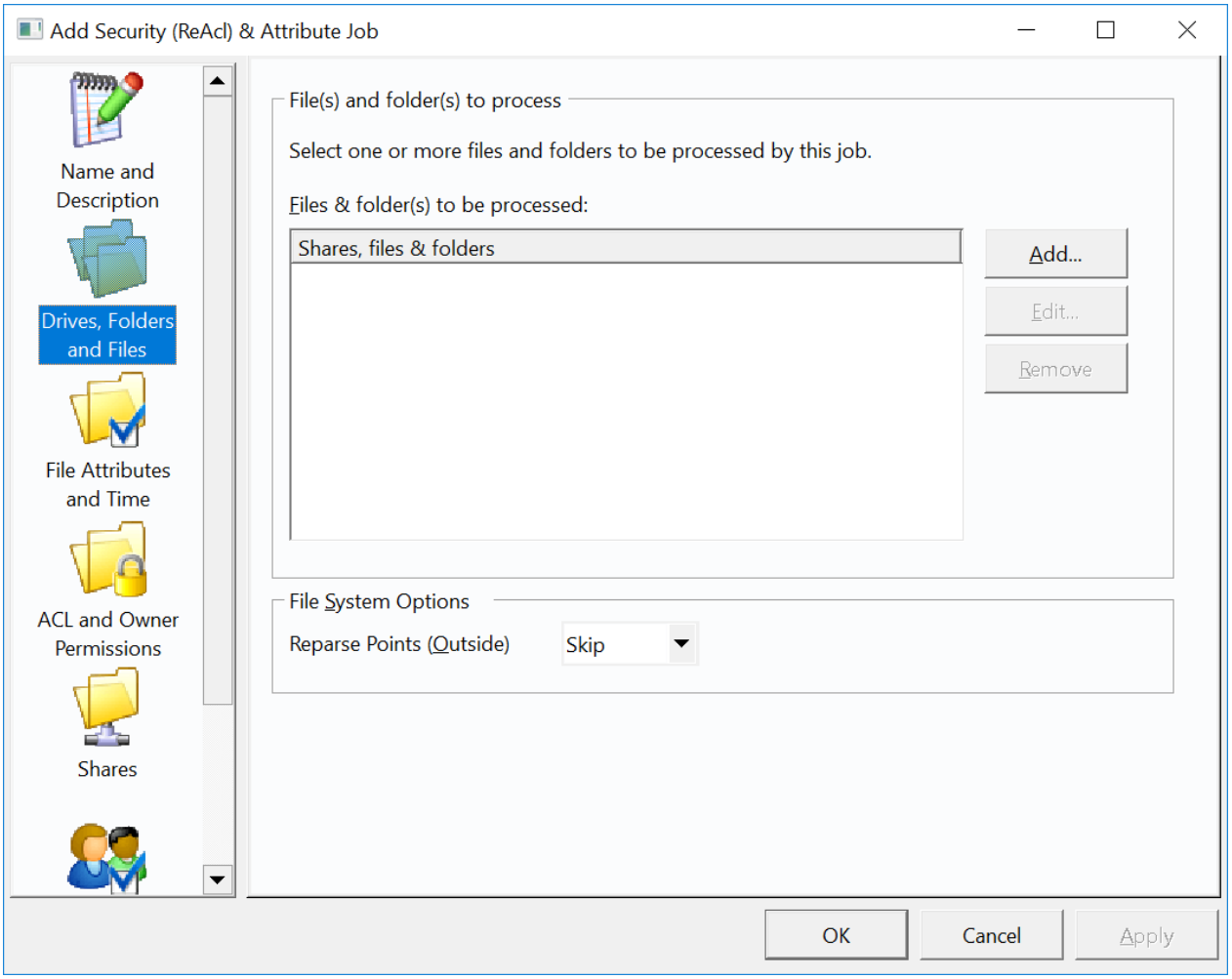
CopyRight2 can attach the job’s log file automatically to the email being sent. To do so, select the “Attach log file option”.

Adding or Editing a Security and Attributes Job

A “Security and Attributes” job allows you to modify files, folders and shares without actually moving the data. This is useful to apply changes to the security of files, for example to replace user and group accounts or to remove specific user and group accounts. You can apply changes to the compression attribute or the file time as well.

Source and Destination

Within this tab you specify the files and folders that you want to process with this job.



File(s) and folder(s) to process

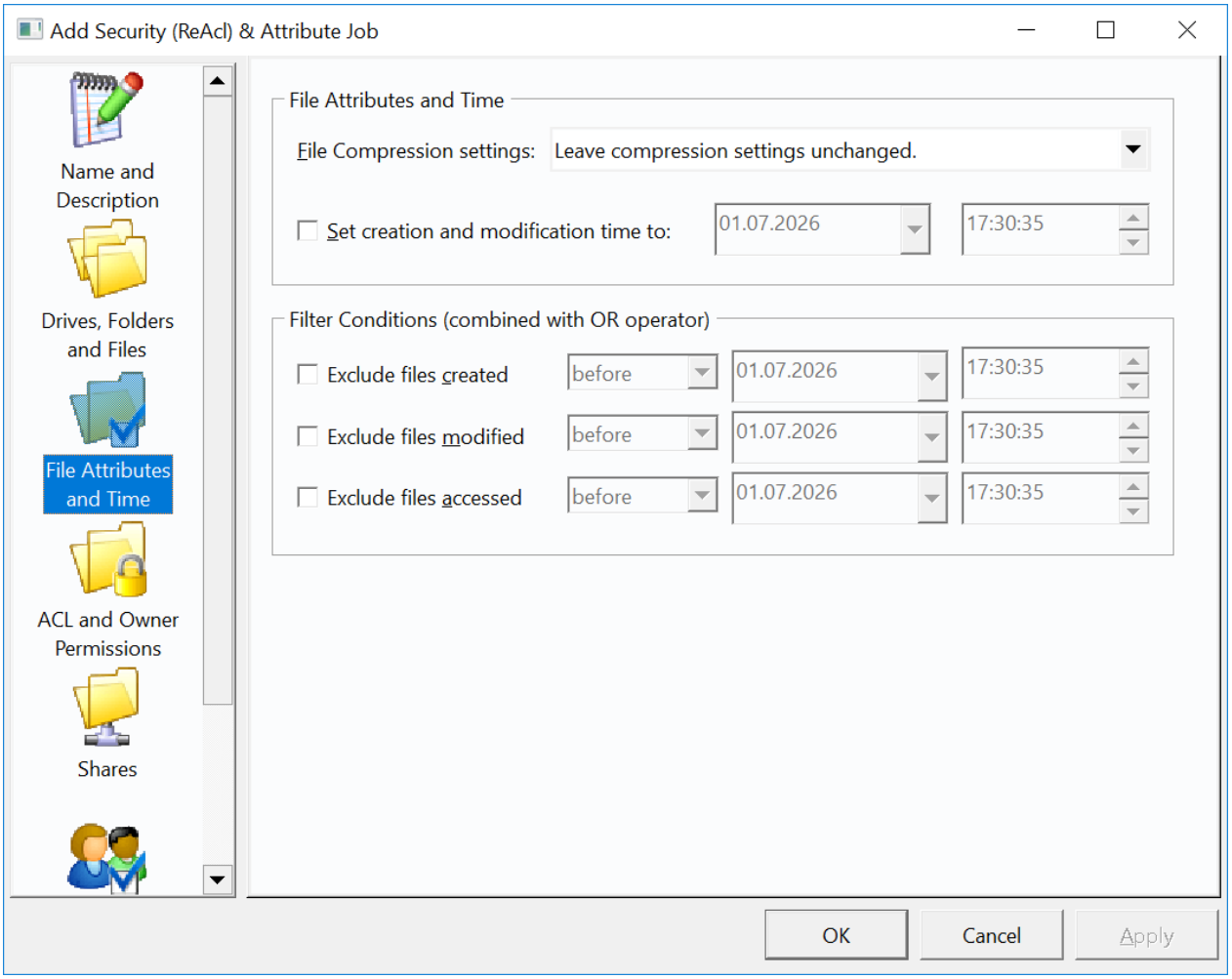
You can add, edit and remove files and folders that you want to process with this job.

Skip Junction Points (Symbolic and Hard Links)

This option is enabled by default and causes CopyRight2 to skip any encountered junction points. Junction points were introduced heavily with windows 2008 / windows vista and are basically like shortcuts to another folder. If clicking on them with the Explorer, you will receive an access denied error. This should stop Backup and Copy programs from recursively accessing what is below the junction point (which makes sense as the data below is located somewhere else which might get copied/backup twice unintentionally).

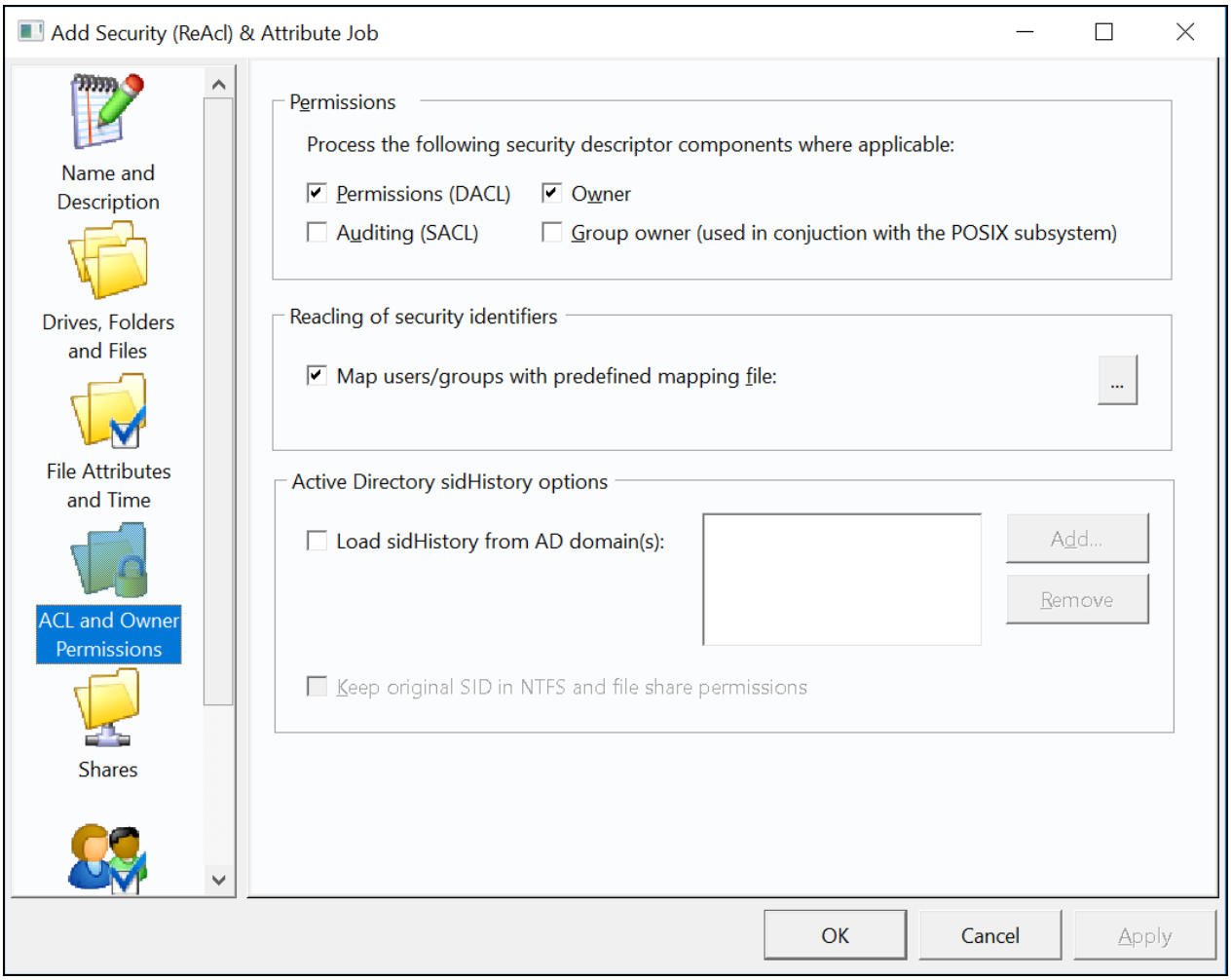
File Attributes and Time

Within this tab you can specify how CopyRight2 should treat the file compression attribute of files and folders. You can change the modification time of files to a predefined date and optionally define a filter to exclude files and folders based on their file date. File Attributes and Time is a subset of the options available to regular copy jobs. Please see “File Attributes and Time” for copy jobs for an explanation.



ACL and Owner Permissions

Use this tab to define how the job should process permissions. You can select a mapping CSV file defining which accounts should be replaced or load the mapping from an Active Directories sidHistory attribute.



Permissions

These options control which part of the NTFS security descriptor should be reACLed by the job.

ReACLing of Security Identifiers

You can define a so-called mapping file with the “User and Group Assignment” tool from the CopyRight2 start menu group, to define the relationship between accounts in the source and the destination environment. After creating the mapping file, you can enable the “Map Security Identifiers with a Predefined Mapping Table” option and then select

the mapping file. You can read more about creating mapping files in the chapter “Creating a Mapping Definition File to Reassign Permissions”.

Load sidHistory from AD domain(s)

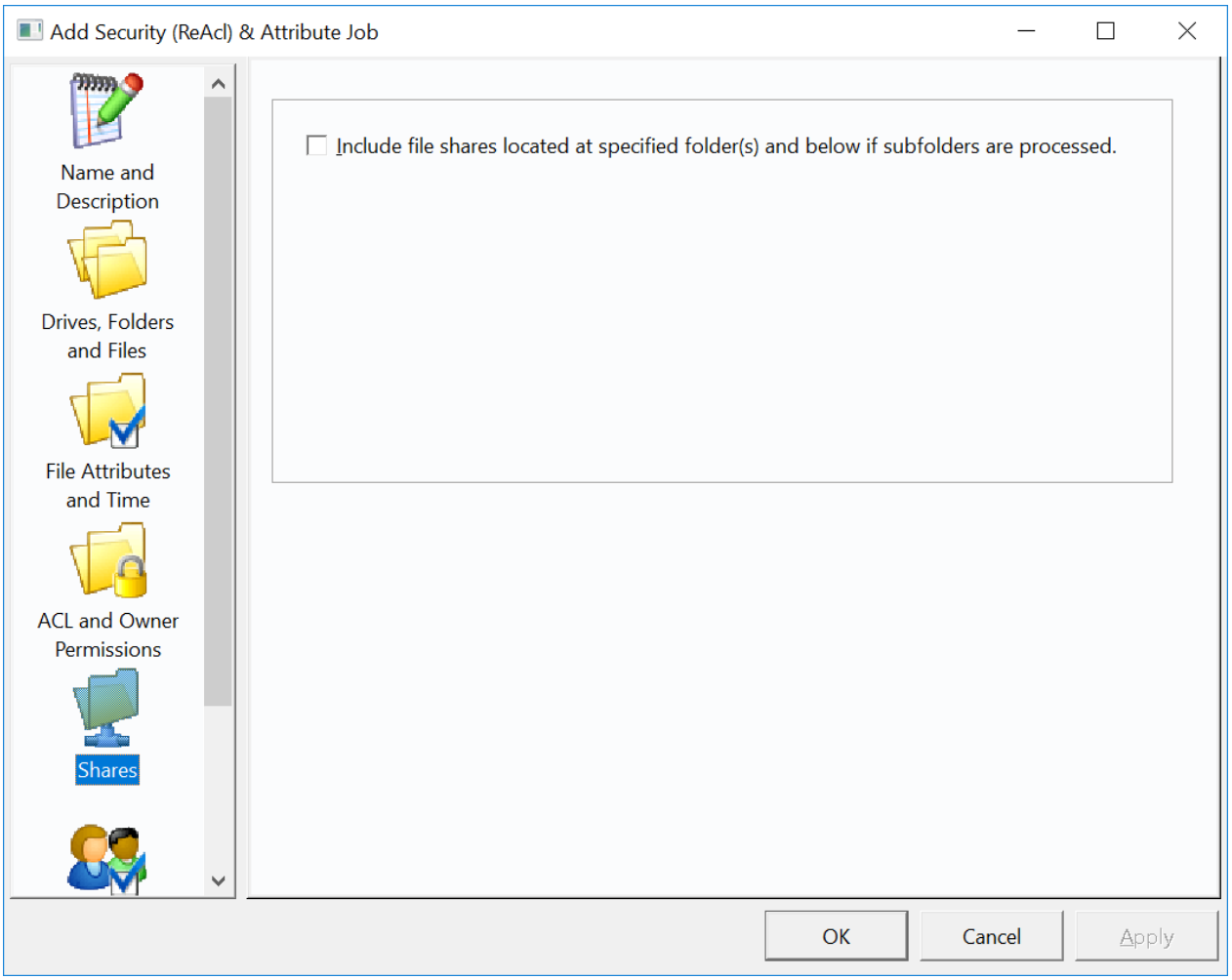
Use this option to specify one or more Active Directory domains that contain users or groups having the sidHistory attribute populated with the users original SIDs. You can either specify a domain controllers NetBIOS name (for example DC9999) or a fully qualified DNS name of the domains (for example domain1.mycorp.com).
If you use this option CopyRight2 will query the specified domains for any user or group object that has the sidHistory attribute populated with one or more old SIDs and map them to the objects new SID to clean up the file systems NTFS and file share permissions by replacing the old SID(s) with the new corresponding SID.

Keep original SID in NTFS and file share permissions

Use this option if you want to keep the original SID within permissions of the file system (NTFS) and file shares. If enabling this option CopyRight2 will add the identical permission (for example READ, EXECUTE, FULL ACCESS) for each user or group encountered, allowing the “old” user and group objects, that were migrated to Active Directory using SID-History the same access they had before. This usually requires an additional clean up job, that should be run after all user and group objects were migrated to Active Directory, using a “Security and Attributes” type of job clean up the file system and file share permissions at a later time (see defining a “Security and Attributes” job).

File Shares

Within this tab you specify if CopyRight2 should copy file shares from the source to the destination computer.



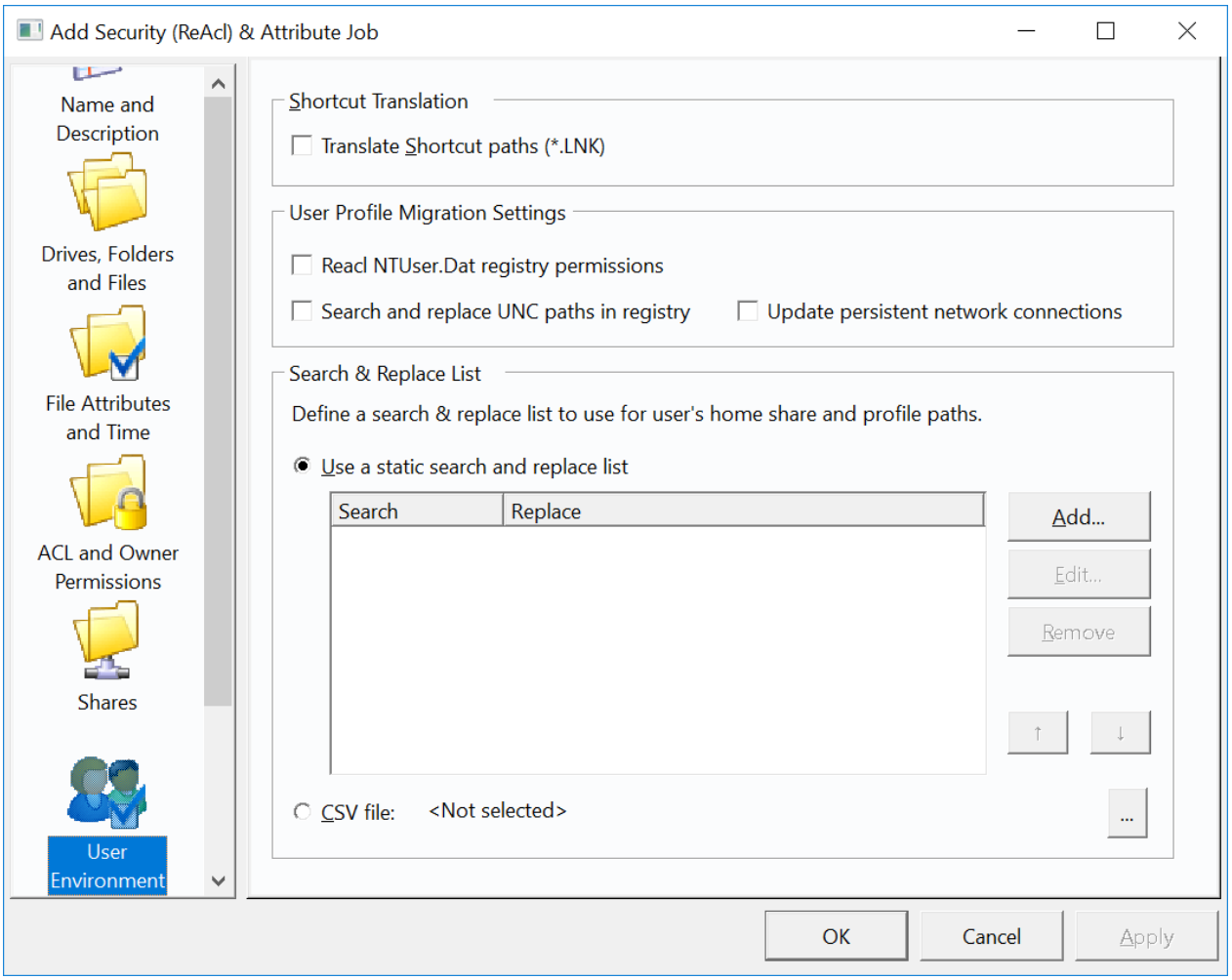
Include File Shares

If you want CopyRight2 to automatically replace permissions of any share located at or below the specified source paths, enable the “Include File Shares” option.

User Environment Migration

Within this tab you specify how CopyRight2 should treat LNK shortcuts and if it should process/reACL Windows user profile permissions (NTUser.Dat and NTUser.Man), search and replace server names or paths in the registry globally or only for persistently stored network connections. You can define a static search and replace list containing server names (server01 -> server02) or folder paths in case of local user accounts (for example c:\home -> x:\homeshares) or use a comma separated CSV file that is loaded dynamically at run-time.

These features work for local and server-based user profiles.



Translate Shortcut Path

If enabled CopyRight2 will automatically translate paths used in Windows shortcut files (.LNK) from source to destination.

Reacl NTUser.Dat registry permissions

If enabled CopyRight2 will automatically reacl Windows user profiles on-the-fly while copying, replacing user (or group) accounts in permission with the corresponding accounts of the destination. It will process regular and mandatory user profiles.

Search and Replace UNC paths in registry

If this option is enabled CopyRight2 will translate references within user profiles, from source path to destination path, for example to take care of recently opened document lists contained in the user profile.

Update persistent network connections

If this option is enabled CopyRight2 will translate persisent network connections within user profiles, from source path to destination path, to take care of connected user profiles contained in the user profile.

Adding or Editing a User and Group Migration Job

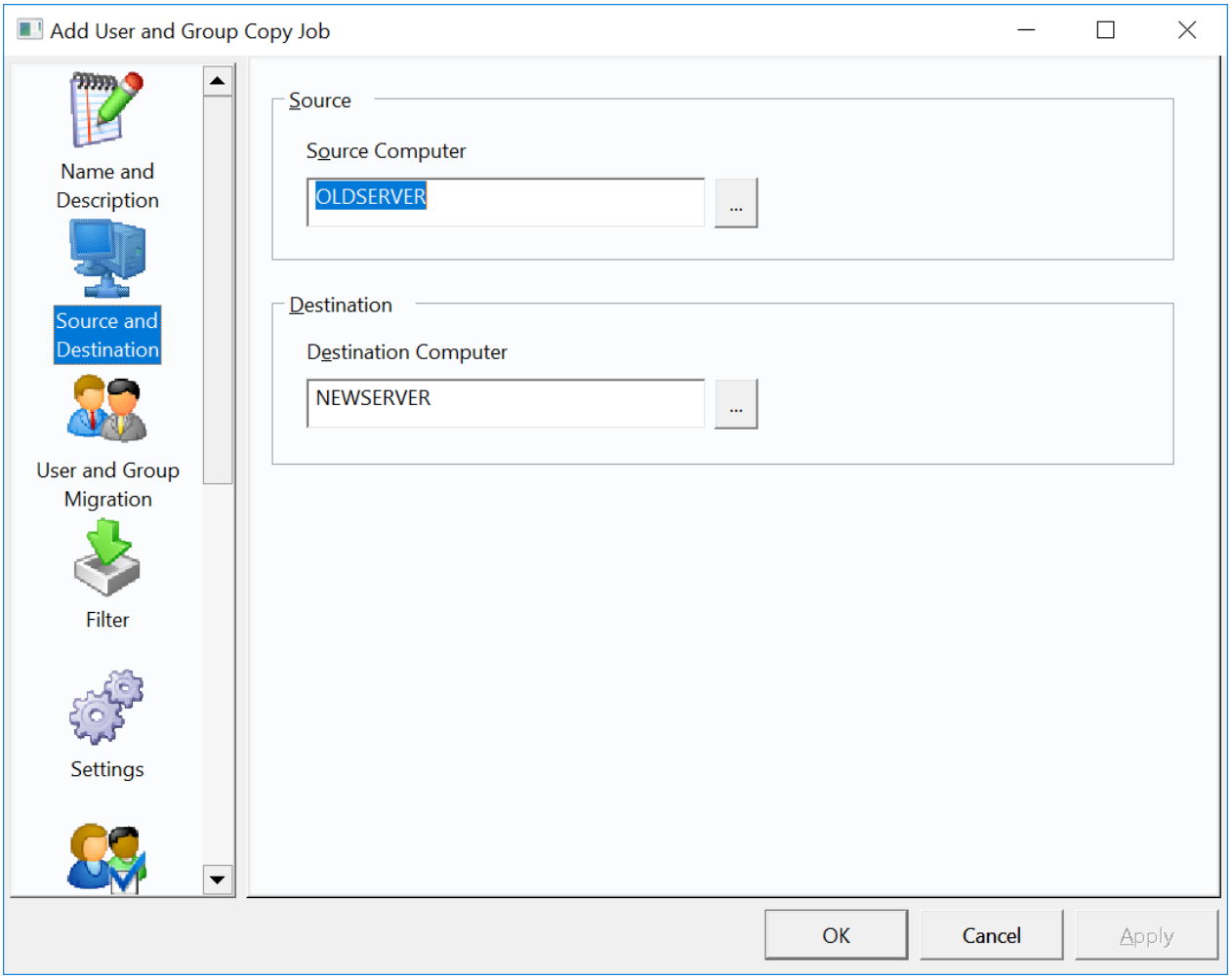
Users and Group Copy Job's allow you to migrate user and group accounts selectively or by selecting an account type like all users, all local groups or all global groups. You can choose accounts from an Active Directory if available, otherwise only local accounts will be displayed.

CopyRight2 supports all possible migration scenarios:

Destination / Source	Member Server (Same Domain)	Domain Controller (Same Domain)	Member Server (Foreign Domain)	Domain Controller (Foreign Domain)	Workgroup
Member Server	Supported, requires copying local groups and local users.	Supported, requires copying local groups and local users.	Supported, requires copying global groups, global users, local groups and local users.	Supported, requires copying global groups, global users, local groups and local users.	Supported, requires copying global groups, global users, local groups and local users.
Domain Controller	Supported, requires copying local groups and local users in pre W2K AD mode. In native mode local groups are domain local and can be used on member servers without copying.	**Note:** Not necessary to migrate any accounts	Supported, requires copying global groups, global users, local groups and local users.	Supported, requires copying global groups, global users, local groups and local users.	Supported, requires copying global groups, global users, local groups and local users.
Workgroup	Supported, requires copying global groups, global users, local groups and local users.	Supported, requires copying global groups, global users, local groups and local users.	Supported, requires copying global groups, global users, local groups and local users.	Supported, requires copying global groups, global users, local groups and local users.	Supported, requires copying global groups, global users, local groups and local users.

Source and Destination

Within this tab you can specify the source and the destination server names.



Source Computer

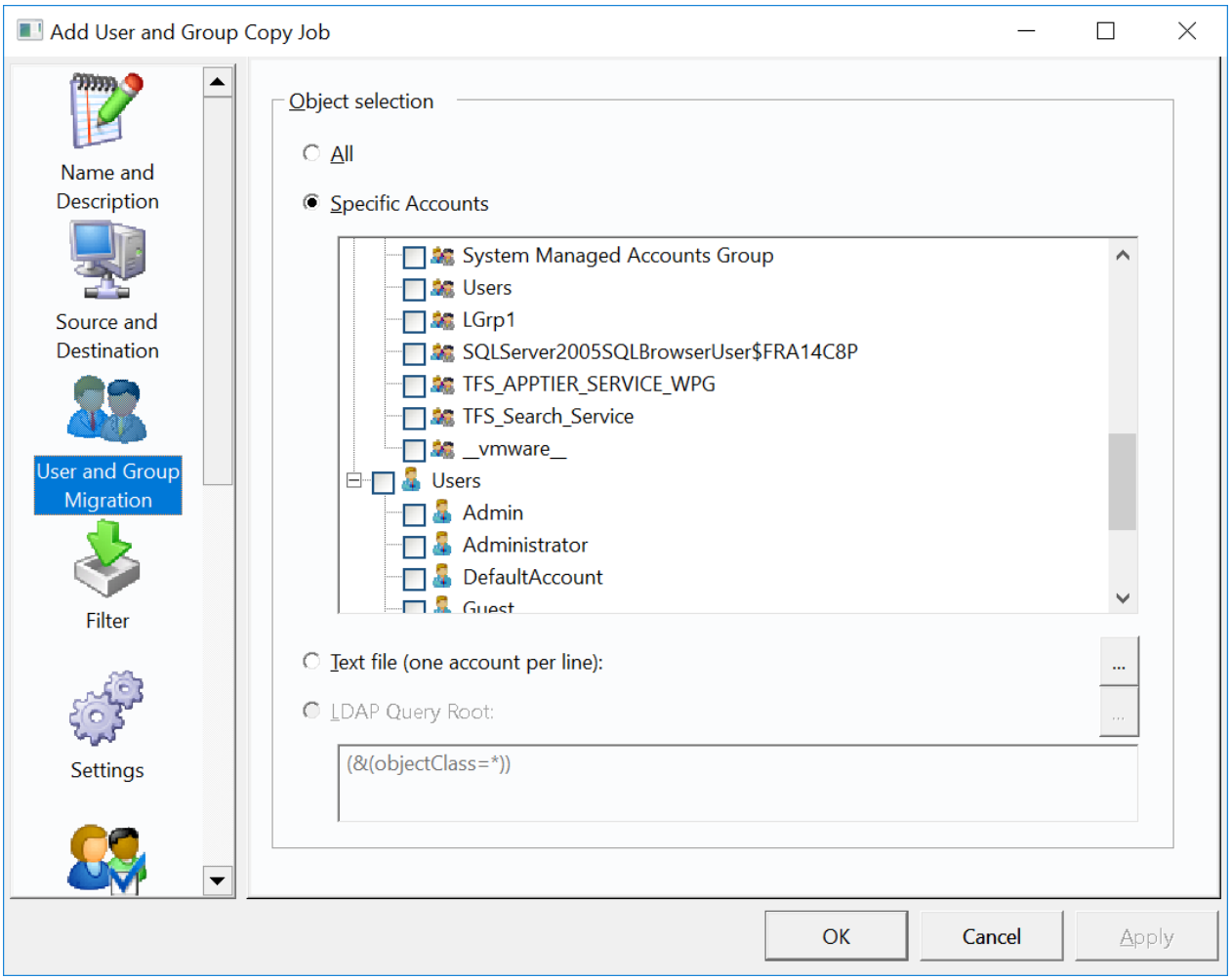
Specify the name of the source computer, where the user and/or group accounts you want to migrate are located at.

Destination Computer

Specify the name of the destination computer where you want to migrate the user and/or group accounts to.

User and Group Migration

Within the “User and Group Migration” tab you can select the accounts being migrated by this “User and Group Copy Job”.



Object Selection

You can either decide to...

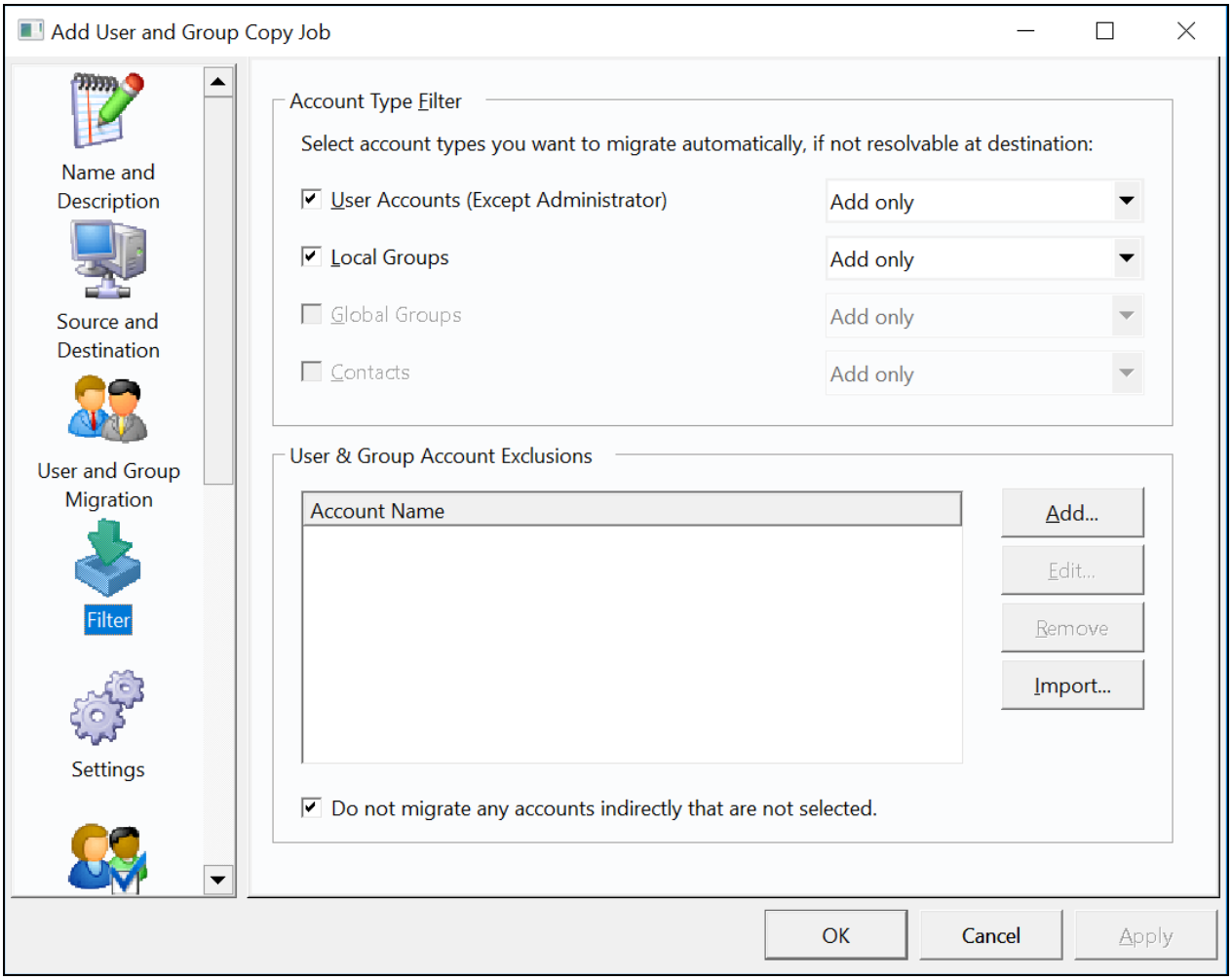
- ...copy all existing accounts.
- ...choose specific accounts from your Active Directory, Windows Domain or local account database.
- ...specify a file containing the user and group account names without domain prefix (one account per line).

- …select source accounts by specifying an Active Directory LDAP query filter condition and a query root as entry point defining where to start the search from.

In any way the selection will be filtered according to the selection of the account type filter (see description of the “Filter” page).

Filter

The filter tab contains settings to control which accounts are copied from the source to the destination. CopyRight2 will only migrate object types that are activated in this filter. It also contains a list of account names you want to exclude from the migration, using the samAccountName in case of users and groups or the common name in case of contacts.



Account Type Filter

The account type filter allows you to filter the types of accounts being copied. If you uncheck “Local Groups” for

example, no local groups will be copied by this job. You can also define how CopyRight2 should treat existing objects. You can define “Add Only” to skip any existing accounts, “Add/Update” to add missing accounts but also update existing accounts or “Add/Update/Remove” to additionally deleted orphaned accounts, that once existed at the source, but were deleted (or renamed) since the copy job was executed the last time.

User & Group Account Exclusions

Use the “Add”, “Edit”, “Remove” and “Import” buttons to define an account exclusion list. You can specify samAccountNames of users and groups and the common name of contacts. In case of specifying a contact’s common name, please use the syntax “CN=Objects_CN_Name”.

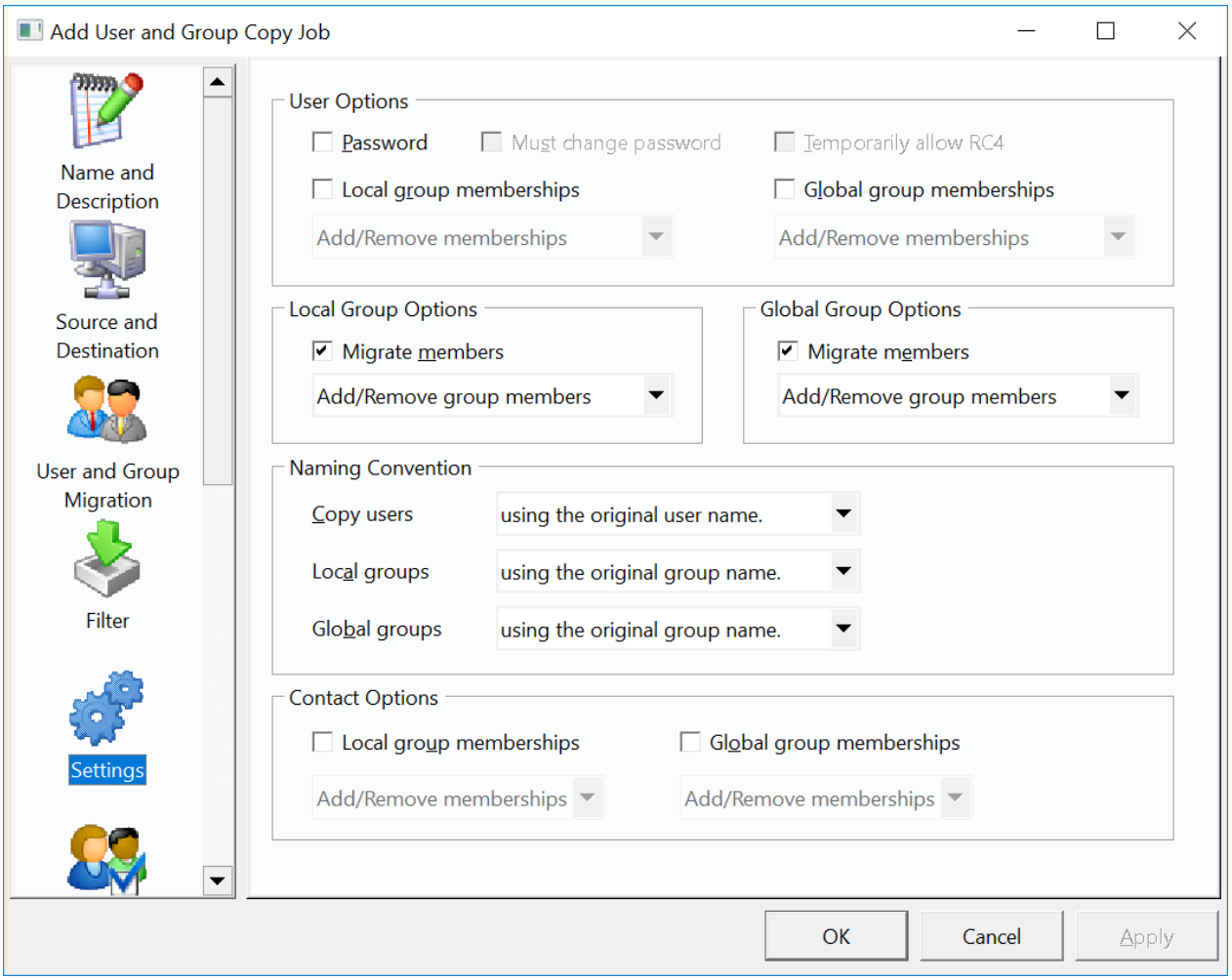
Do Not Migrate Any Accounts Indirectly That Are Not Selected

If this option is checked (default setting), CopyRight2 will only migrate objects that are selected in the “User and Group Migration” page. It will not migrate objects indirectly.

If unchecking this option, CopyRight2 will migrate objects indirectly as well. For example, if the option is unchecked, and there is a single group selected and the object filter is set to migrate groups and users and the migration of group members is enabled, it will migrate any group members indirectly as well. If additionally, the migration of user’s group memberships is enabled, it will migrate any group that any of the migrated user accounts is a member of as well.

Settings

Within the “Settings” tab of the “User and Group Copy Job” you can set general options that are applied to users and groups being migrated.



Migrate User Passwords / Must Change Password

If you have installed the separately available “PwdSync Addon for CopyRight2” you can copy the user’s password hashes (a.k.a. NT-Hash) as well. Please note that this option is disabled if you have not installed the add on. Additionally, you can enable the “Must change password” option to force the user to change the password during first logon.

Temporarily Allow RC4

Enabling this option, will set the msDS-SupportedEncryptionTypes attribute of migrated target AD user objects to decimal 60, effectively allowing the RC4 Kerberos encryption type. Microsoft turned RC4 off in April 2026. This option can be combined with the Must Change Password option, to force users logging on to the target domain, to immediately change their password, causing the creation of required AES keys. Windows automatically picks the best available encryption type. Alternatively, you can use the password synchronization method to migrate user passwords in advance (see "**Password Synchronization & Migration Add-On Manual**") working completely RC4 free and not requiring any other weakening configurations on domain controllers.

Local and Global Group Memberships of User Accounts

With these options you can control how CopyRight2 should treat a copied user account's local and global group membership. If any of these options is enabled, CopyRight2 will add the destination account to the same groups as well. If required and if the account type filter has the corresponding groups type enabled, CopyRight2 will create those groups automatically if required. You can control if you want CopyRight2 to add and remove memberships or if you want to add memberships only, which is useful in server or domain consolidations and other scenarios.

Local and Global Group Members

With this option you can control how CopyRight2 treats members of local or global groups. If it is enabled CopyRight2 will attempt to copy any group members as well. You can control if you want CopyRight2 to add and remove members or if you want to add members only, which is useful in server or domain consolidations and other scenarios.

Naming Convention

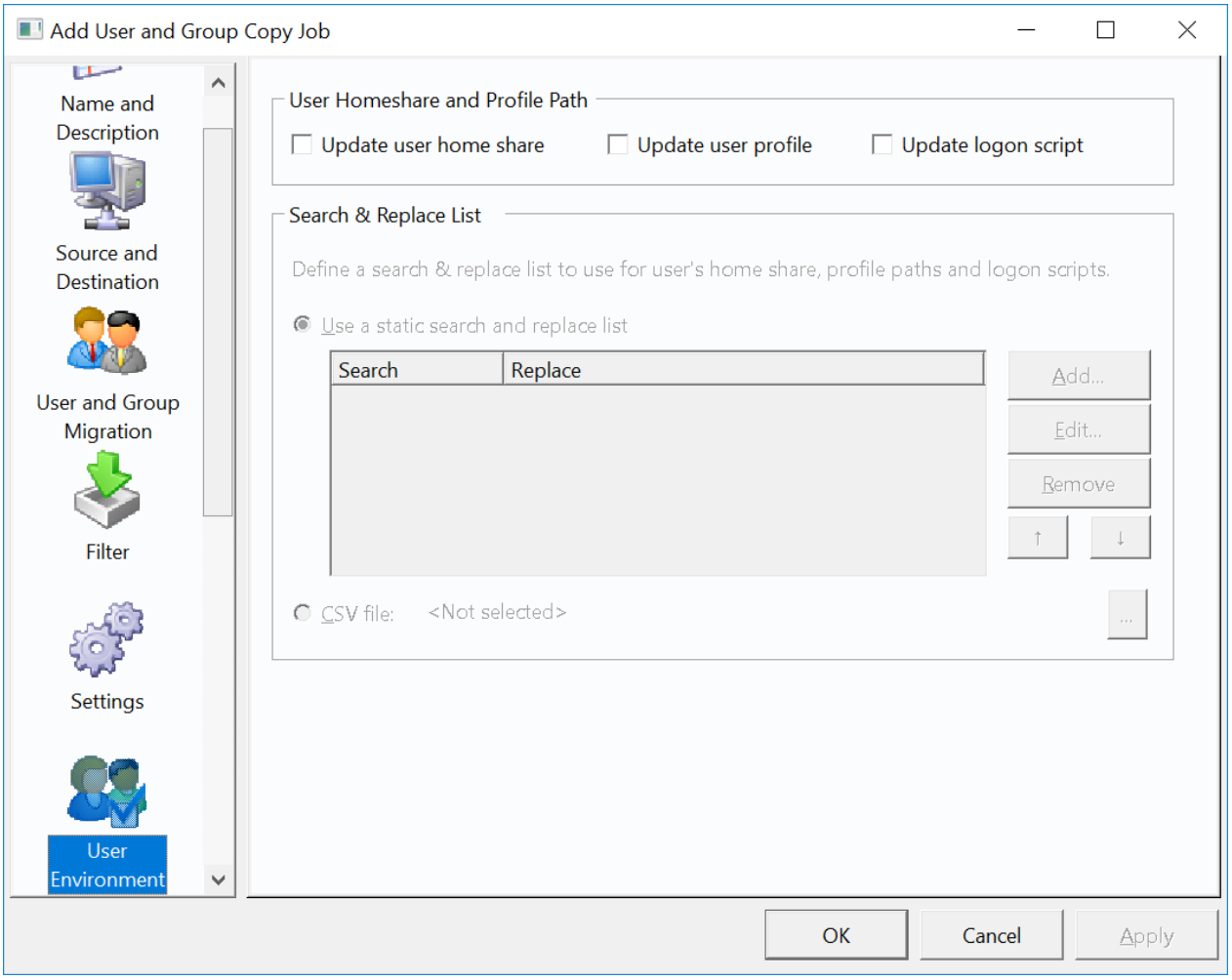
You can optionally apply prefixes and suffixes to the account names of the users being copied or synchronized. Simply choose the type of change you want to apply to the naming convention and enter a prefix or suffix. The prefix or suffix will be appended or prepended to the account name being migrated.

Contact Options

The contact options control if CopyRight2 should migrate contact's local and global group memberships. You can also control how CopyRight2 should treat group memberships of contacts that already exist at the destination. You can select to add group memberships only or to add and remove group memberships.

User Environment Migration

Within this tab you specify if CopyRight2 should update home share and profile paths of local or domain user settings.

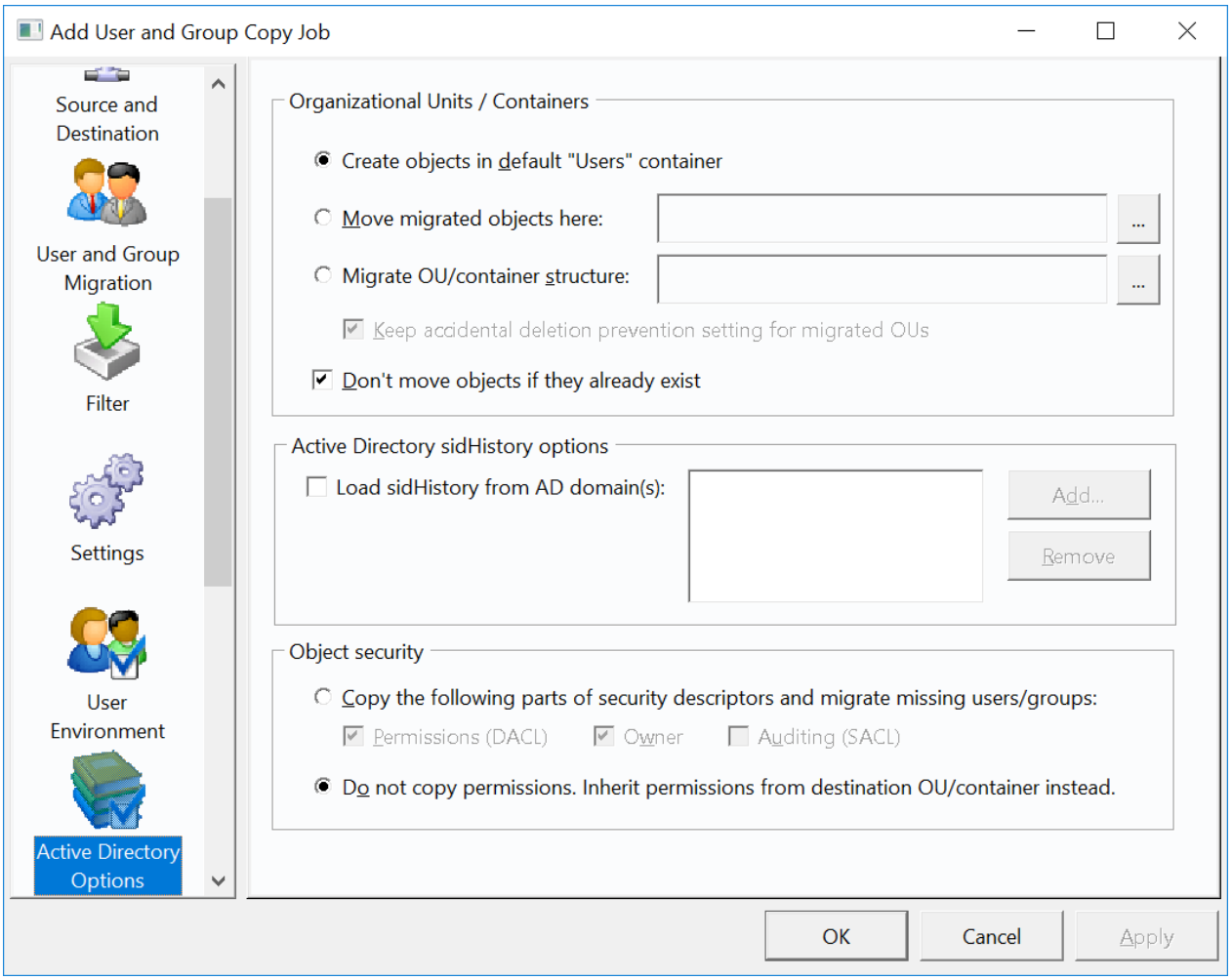


Update User Homeshare & User Profile Path

If enabled CopyRight2 will automatically replace the user home share path or profile path in local or domain user settings. You can define a static search and replace list using the “Add…”, “Edit…” and “Remove” buttons or alternatively select a comma separated CSV file containing the search and replacement server names.

Active Directory Options

Within the tab you can set options regarding the migration of Active Directory domain objects, for example to control where objects should be created in the destination domain.



Create Objects in Default "Users" Container

The default option will migrate any corresponding users and groups into the "Users" container. This includes domain users and groups requiring migration but also local accounts getting migrated to the domain because the "Create Users and Groups in Destination Domain" option is checked.

Move migrated Objects Here

This option will move any migrated objects into the specified OU or container. This includes domain users and groups requiring migration but also local accounts getting migrated to the domain because the "Create Users and Groups in Destination Domain" option is checked.

Migrate OU & Container Structure

This option migrates the source's OU and container structure to the specified location of the destination's Active Directory tree. By default, it uses the destination domains root as a target, causing any OU or container to get created at the same level of the directory tree.

Load sidHistory from AD domain(s)

Use this option to specify one or more Active Directory domains that contain users or groups having the sidHistory attribute populated with their original SIDs. You can either specify a domain controllers NetBIOS name (for example DC9999) or a fully qualified DNS name of the domains (for example domain1.mycorp.com). If activated the job will use Active Directory to determine the existing mapping between old account SIDs and new account SIDs during job execution.

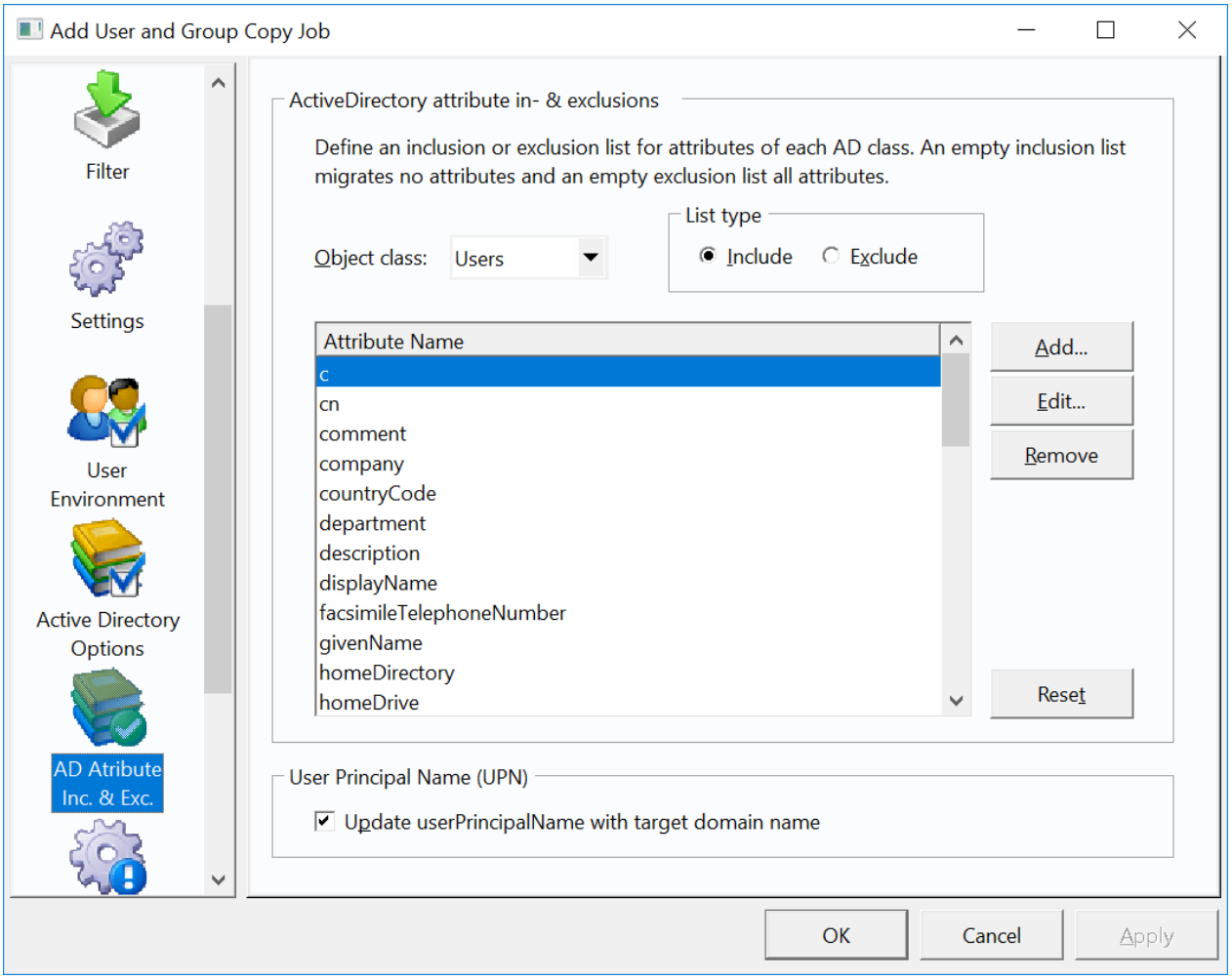
If you use this option CopyRight2 will query the specified domains for any user or group object that has the sidHistory attribute populated with one or more old SIDs and map them to the objects new SID to clean up the file systems NTFS and file share permissions by replacing the old SID(s) with the new corresponding SID.

Object Security

The object security settings control how CopyRight2 should treat Active Directory object permissions. You can either inherit permissions from the destination OU/container or you can migrate the permissions (DACL), auditing settings (SACL) and the object owner.

Active Directory Attribute In- and Exclusion List

The options located in the Active Directory attribute in- and exclusion list allow control over which attributes are migrated between the source and destination domains. You can either define an inclusion list, an exclusion list or an empty list which causes all attributes defined in the schema to get copied.



Object class

Use the object class combo box to select the object type you want to define an inclusion or exclusion list for. You can select either “Users”, “Contacts”, “Groups” or “OUs”.

List Type

Select either “include” to define an inclusion list or “exclude” to define an exclusion list.

Add/Edit/Remove

Use the “Add”, “Edit” and “Remove” button to remove attributes from the list. Please note that you can select multiple attributes and remove them in a single “Remove” operation.

Reset

Use the “Reset” button to reset to the default set of attributes defined for the selected object class. The default list includes all attributes that are visible in Window’s “Active Directory Users and Computers” MMC snap-in.

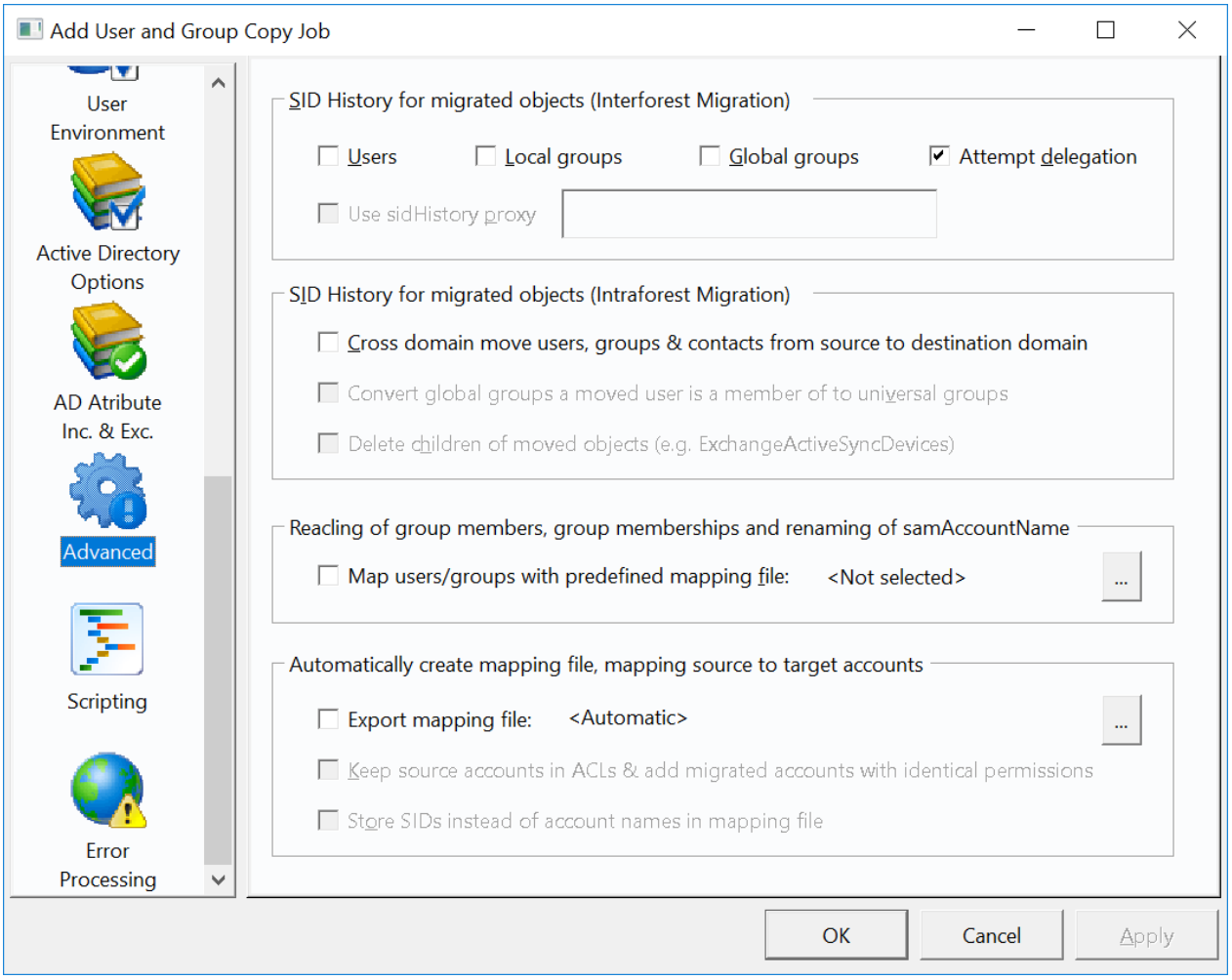
Update userPrincipalNames

Enable this option to update each user’s userPrincipalName attribute in Active Directory by replacing the source domain name with the target domain name, while preserving the portion before the “@” sign.

For example: john.smith@source.com → john.smith@target.com

Advanced

The advanced options tab contains advanced settings, such as sidHistory settings (see chapter “USING SID-HISTORY FOR ACTIVE DIRECTORY MIGRATIONS”). It also contains settings to enable the use of a mapping file, in case accounts need to be renamed during the migration. Additionally, it contains settings to let the User & Group Migration job automatically create a mapping file, containing each migrated source and target object, to be used for example in a Security & Attributes job to perform replacements in NTFS and share level permissions.



SID History for Migrated Objects (Interforest Migration)

Enable this option, if you want to populate the destination object’s sidHistory attribute with the SID of the original source account. You can enable this option for users, local groups and global/universal groups. This is the correct option to use if you migrate between two domains that do not reside in the same Active Directory forest.

The “Attempt delegation” option controls the behavior of the Windows sidHistory API regarding the callers context. If enabled, CopyRight will let this Windows API attempt to delegate the security context used to communicate with the target domain controller, towards the source domain controller. This requires that the user account of the target

domain is a member of the built-in Administrators group of the source domain. It additionally requires that delegation is not disabled for that user account and that delegation is not disabled for the target domain controller's computer object.

If the option is disabled, CopyRight will let the API use the context used to communicate with the source domain controller instead, if it has already been provided or request credentials for an account in the source domain that is a member of the builtin Administrators group.

SID History for Migrated Objects (Intraforest Migration)

Enable the "Cross domain move" option, if you want to populate the destination object's sidHistory attribute with the SID of the original source account. You can enable this option for users, local groups and global group. This is the correct option to use if you migrate between two domains that do reside in the same Active Directory forest. In this case the source object cannot be cloned, because the forest requires each SID to uniquely identify an object. Therefore, the option causes CopyRight2 to move the object to the destination domain instead, causing it to disappear in the original source domain. Due to the move to a new domain, the objects will get a new SID consisting of the destination domains SID with a new RID appended to it. After the move, CopyRight2 will populate the sidHistory with the SID of the original source object, to allow access to resources protected by permissions.

Enable the "Automatically convert global groups" option, if you want to migrate user accounts that are members of global groups in the source domain that you want to migrate at a later time. This is required because a global group can only contain members of the domain the group resides in. If enabled this option will additionally convert global groups that the global group is a member of.

If you have installed the CopyRight2 RPC service on the target domain controller defined in your job's settings, you can optionally enable the proxy functionality allowing user accounts previously granted permission to use the proxy, to add to the sidHistory attribute in the target domain, even if those users do not posses the "Migrate SID-History" permission. If enabled, you will need to provide the security context the RPC service is running under for mutual authentication purposes. You can read more about the configuration of the CopyRight2 RPC service in the chapter "Using CopyRight2's GUI" -> "Options" -> "RPC Service".

Reacling of Group Members, Group Memberships and Renaming of samAccountNames

Use this option to supply the copy job with a mapping file, that is used to process migrated group's members, user"s group memberships and/or to rename migrated objects samAccountNames using the advanced option 3 in the mapping file (see chapter "Rename samAccountName of target account").

Automatically Create Mapping File, Mapping Source to Target Accounts

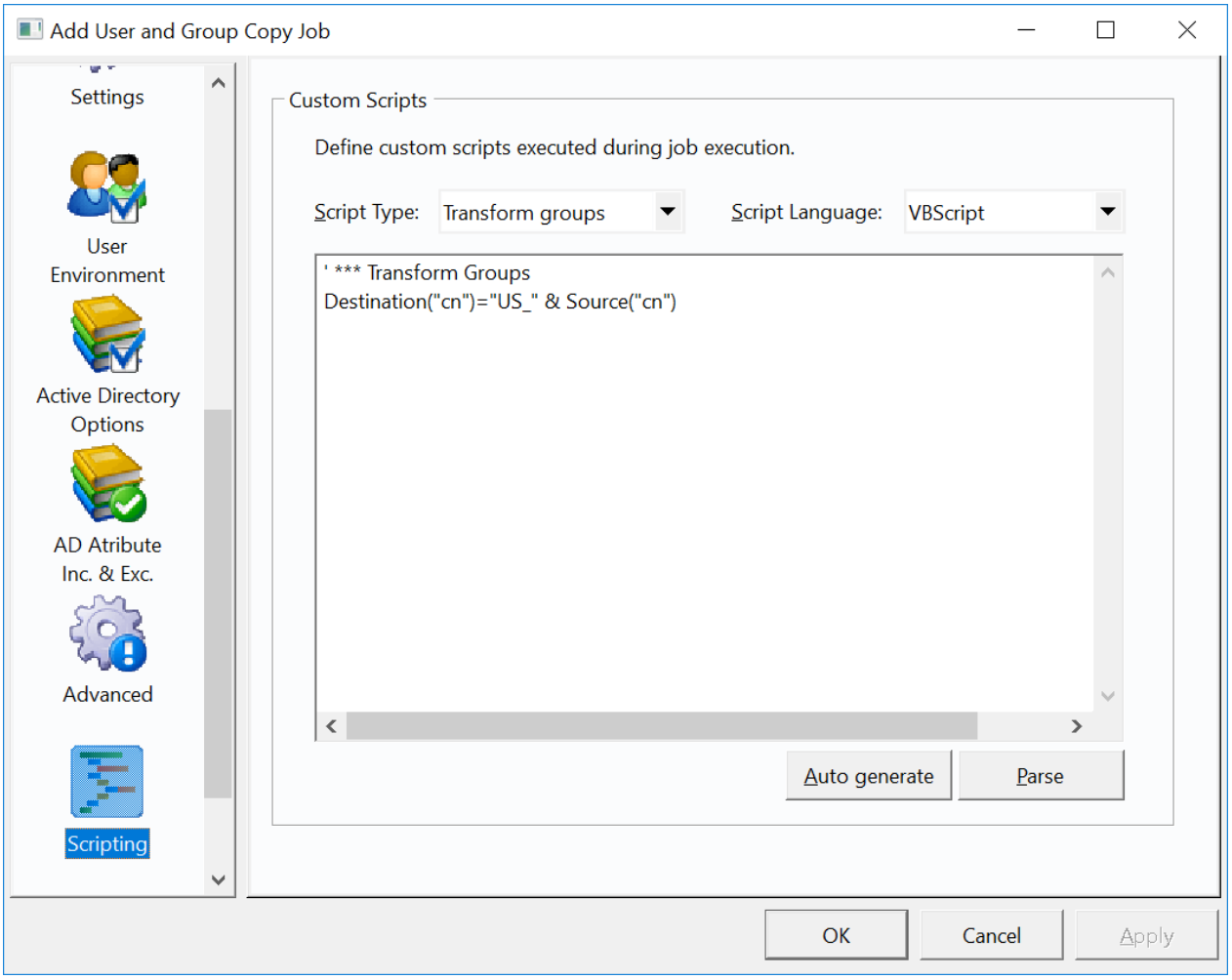
If the "Export mapping file" option is enabled the job will create a mapping file during its execution that can be used in a separately executed "Security & Attributes" job, for example to change NTFS and file permissions of member servers that reference the migrated accounts.

You can optionally decide to keep the source accounts in permissions if enabling the "Keep source accounts" option. The migrated target accounts will then get added with identical permissions the source accounts had.

Optionally you can store SIDs in the mapping file instead of clear-text account names by enabling the "Store SIDs" option.

Scripting

Within this tab you can define multiple custom scripts to get executed during specific events, for example when the copy job starts and also scripts executed during the migration of specific types of objects. You can use VBScript, which is the default option) or any other installed ActiveScript language to define the script's code. Please see the chapter "Using ActiveScript" for more information about how to write scripts.



Script Type

Please select the type of script. You can define scripts executed when the copy job starts and when it ends. You can also specify a script executed when two individual servers, specified as source and destination, do start and end copying. Additionally, you can define scripts for each type of object that gets migrated (Users, Groups, Contacts, OUs).

Script Language

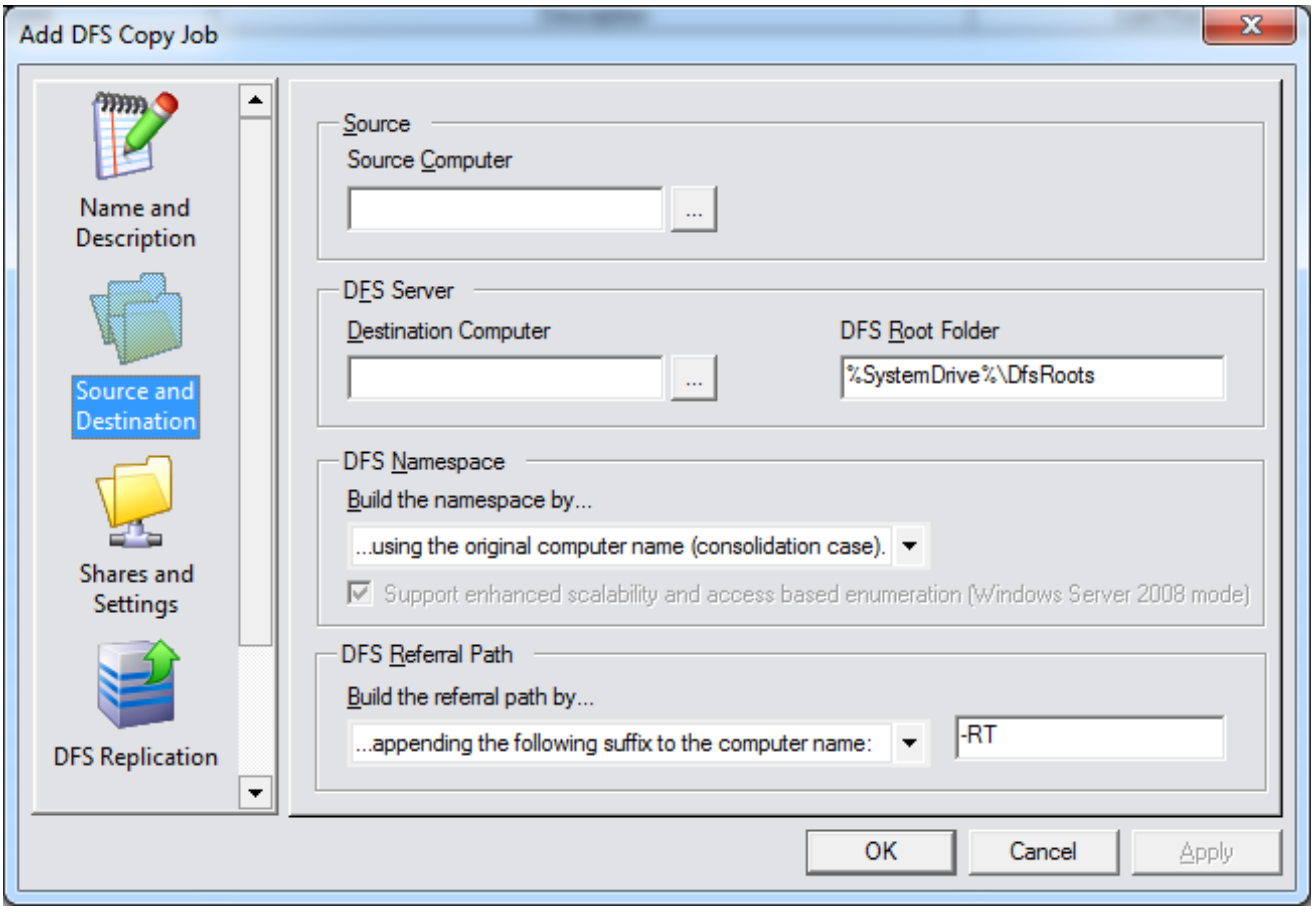
The script language setting allows you to select which script language to use for this job.

Adding or Editing a DFS Copy Job

DFS Copy Job's allow you to create DFS links within a DFS server, pointing to a source computer's share(s). You can use this feature to migrate / centralize file servers while keeping existing NetBIOS names (and UNC namespaces) or to introduce centralized file share access using DFS. It supports domain-based and stand-alone DFS configurations.

Source and Destination

Within this tab you specify the files and folders that you want to process with this job.



Source Computer

Specify the name of the source computer, whose shares you want to migrate.

DFS Server

Please specify the name of your DFS server. In case of a clustered DFS environment, please specify the clusters "DFS Namespace Server" resource's name and not the name of a node.

DFS Root Folder

Please specify the folder that the DFS computer should use to create the DFS root. By default, Windows uses "%SystemDrive%\DfsRoot". In case of a cluster you can leave the default setting. CopyRight2 will automatically use the clusters disk volume that is assigned to this "DFS Namespace Server" resource. Alternatively, you can specify an absolute path (for example "S:\DfsRoot").

DFS Namespace

This setting controls the namespace you want to use. The namespace is what users will put in front of the share name when connecting.

For example, you could use the source computer's original name to preserve existing logon scripts, GPOs or persistent network connections. This requires that you rename the source computer's NetBIOS name, for example by appending "-RT" to the computers name, using the "DFS Referral Path" option, after you imported the computer's shares into DFS, otherwise a duplicate computer name would exist on the network. In order for this to work, you will have to configure your DFS installation appropriately. You can find information about how to configure DFS to maintain old server names in TechNet article KB829885 (https://support.microsoft.com/en-us/help/829885/distributed-file-system-update-to-support-consolidation-roots-in-windo). You can configure DFS to support additional names, after you have created the file shares in DFS.

You could use a stand-alone namespace using the specified value. In this case users would connect to shares using the following UNC path consisting of the DFS server's DNS or NetBIOS name, the namespace name (in this case "Public") and the share name: \\DFS-SERVER-NETBIOS-NAME\Public\Share-01. You can define multiple namespaces.

You could use a domain-based namespace using the specified value. In this case users would connect to shares using the following UNC path consisting of the domain's DNS name, the namespace name (in this case "Public") and the share name: \\MyDomain.Com\Public\Share-01. You can define multiple namespaces.

Option	Description
Using the original computer name (consolidation case)	This option can be used in migration scenarios, where you want to maintain the source servers NetBIOS/DNS names. It will create an additional namespace using the source server's name. This requires to rename the name of the source server at a later time and to use the DFS Referral path option to use this updated name. Users can then connect through DFS to the shares of the source server and you can let the copy job update the location to the target server once a share has been migrated successfully.
Using the specified value (stand-alone namespace)	Create the shares within the specified stand-alone DFS namespace. You could for example specify a value of "Public".
Using the specified value (domain-based namespace)	Create the shares within the specified domain-based DFS namespace. You could for example specify a value of "Public".

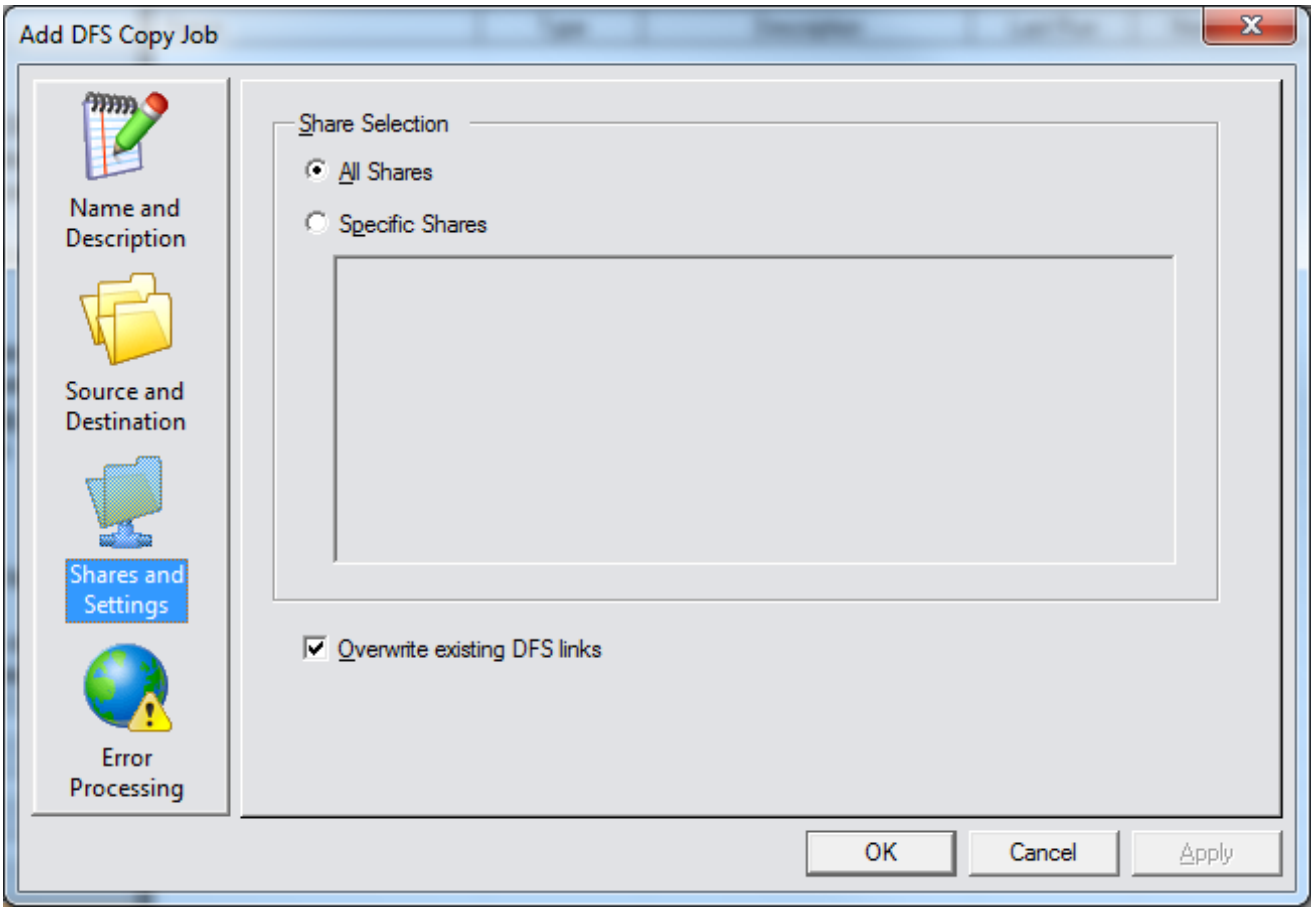
DFS Referral Path

The DFS referral path, defines where the DFS shares point to. You can let the point to the original computer name, if you want to introduce a domain-based or stand-alone DFS, or in case of the consolidation case, where the DFS server takes over the source server's original NetBIOS name, to let it point to a name with a prefix, suffix or entirely different name.

Using the original computer name	Create links using the original computer name. This option will create fully functional DFS links pointing to the specified source computer name. You can use this option to import all file shares of the source computer into your DFS hierarchy, in case you want to introduce DFS. You could then make corresponding changes to your environment (logon scripts, GPOs, …) to make sure users connect to the corresponding DFS path instead of using the server name in UNC paths. Once all users are connecting through DFS, you could then use copy jobs that update the DFS location after data was moved successfully (see chapter "Update DFS after share was migrated to new location.").
Prepending the following prefix	Add the specified prefix to the computer name the DFS link points to. This option is useful if migrating data while keeping existing NetBIOS names intact.
Appending the following suffix (DEFAULT)	Add the specified suffix to the computer name the DFS link points to. This option is useful if migrating data while keeping existing NetBIOS names intact. The default option "-RT" would add –RT to the source servers NetBIOS name so all DFS links of source server "MyServer" would point to "MyServer-RT".
Using the specified value	Use the specified computer name. Use this option if you plan to rename the source computer to an entirely different name.

Shares and Settings

Within this tab you specify whether you want to copy all existing shares or specific shares.



Share Selection

Either choose all shares, which will be evaluated at the jobs runtime or select specific shares you want to migrate to DFS.

Overwrite existing DFS links

If checked causes CopyRight2 to overwrite existing DFS links. If this option is not checked, the copy job will only create new share links but skip any existing ones that were potentially already updated to point to a new location.

Note: Please note that running a DFS copy job with the “Overwrite existing DFS links” option enabled will overwrite any existing links to point to the source server again!

Adding or Editing a Computer and Profile Migration Job

A Computer and Profile Migration type of job provides the ability to remotely schedule, execute and track the migration of computer accounts and/or user profiles located on those remote computers between domains, from workgroup mode towards a domain, from a domain towards Microsoft Entra or from Microsoft Entra towards a domain.

For the purpose of profile migrations, it will automatically track if the accounts associated with local user profiles have been migrated to the target domain already.

By default, it will stop processing a computer scheduled for a profile migration if there are un-migrated accounts.

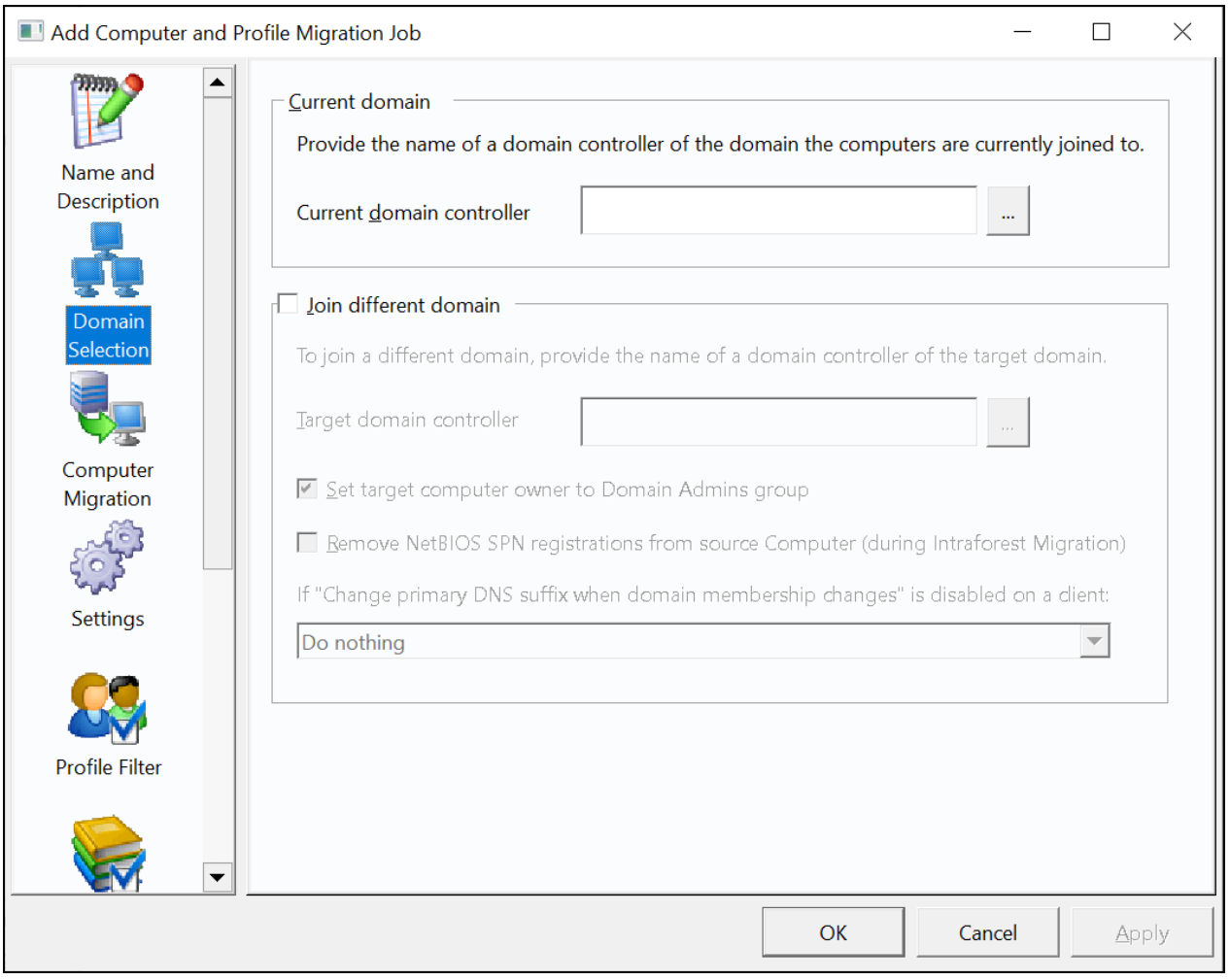
Optionally you can run the job in simulation mode, where it will not apply changes to the profiles but merely collect information about the local profiles found and the state of the associated accounts. The collected information, to assist in decision making, consists of account activation state, last domain logon (+- 14 days), last modification of local profile and more.

This allows to either migrate those missing user accounts before attempting the computer migration again or to specify an option to ignore those profiles. This is useful for cases where the source domain account has not been used and the associated person has probably left the organization for example.

Source and Destination

In the source and destination tab you need to provide the names of domain controllers of the source and target domain, in case you want to switch the remote computers domain membership.

If you do not want to change the computers domain membership, you will simply need to specify a domain controller of the domain the computers currently belong to without enabling the “Join different domain” option.



Current Domain

Select or specify the name of a domain controller of a domain the remote computers are currently joined to.

Join Different Domain

Activate this option if you want the remote computers to change their domain. Once activated you will need to provide a target domain controller and the credentials of at least a domain user account of the target domain.

The “Set target computer owner to Domain Admins group” option can be used if the currently used context is an Enterprise Admins group member to change the computer owner from Enterprise Admins to Domain Admins.

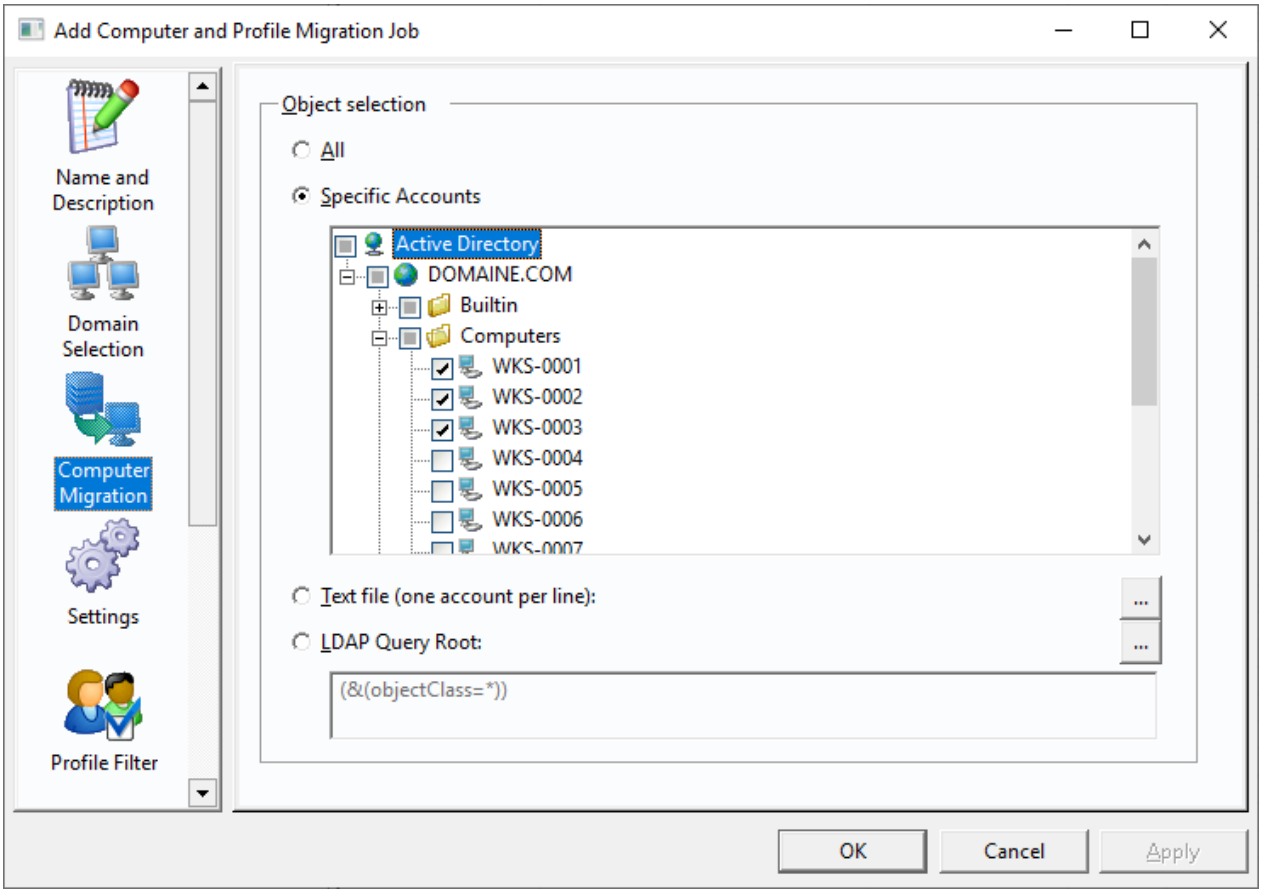
The “Remove NetBIOS SPN” option will remove a computers SPN registrations using the NetBIOS name to maintain uniqueness of such registrations in case of a migration taking place between two domains residing in the same forest.

The “If ‘Change primary DNS suffix when domain membership changes’ is disabled on a client” option can either re-enable this option, which is usually enabled on a default Windows installation or enable it once to let the client join domain and change the DNS suffix to the suffix of the target domain.

When the job is launched, the computer account(s) will be created in the target domain automatically in the OU or container specified in the job’s settings.

Computer Migration

In the Computer Migration page, you can, similar to the selection of accounts in a User and Group migration job, select the computers to process.



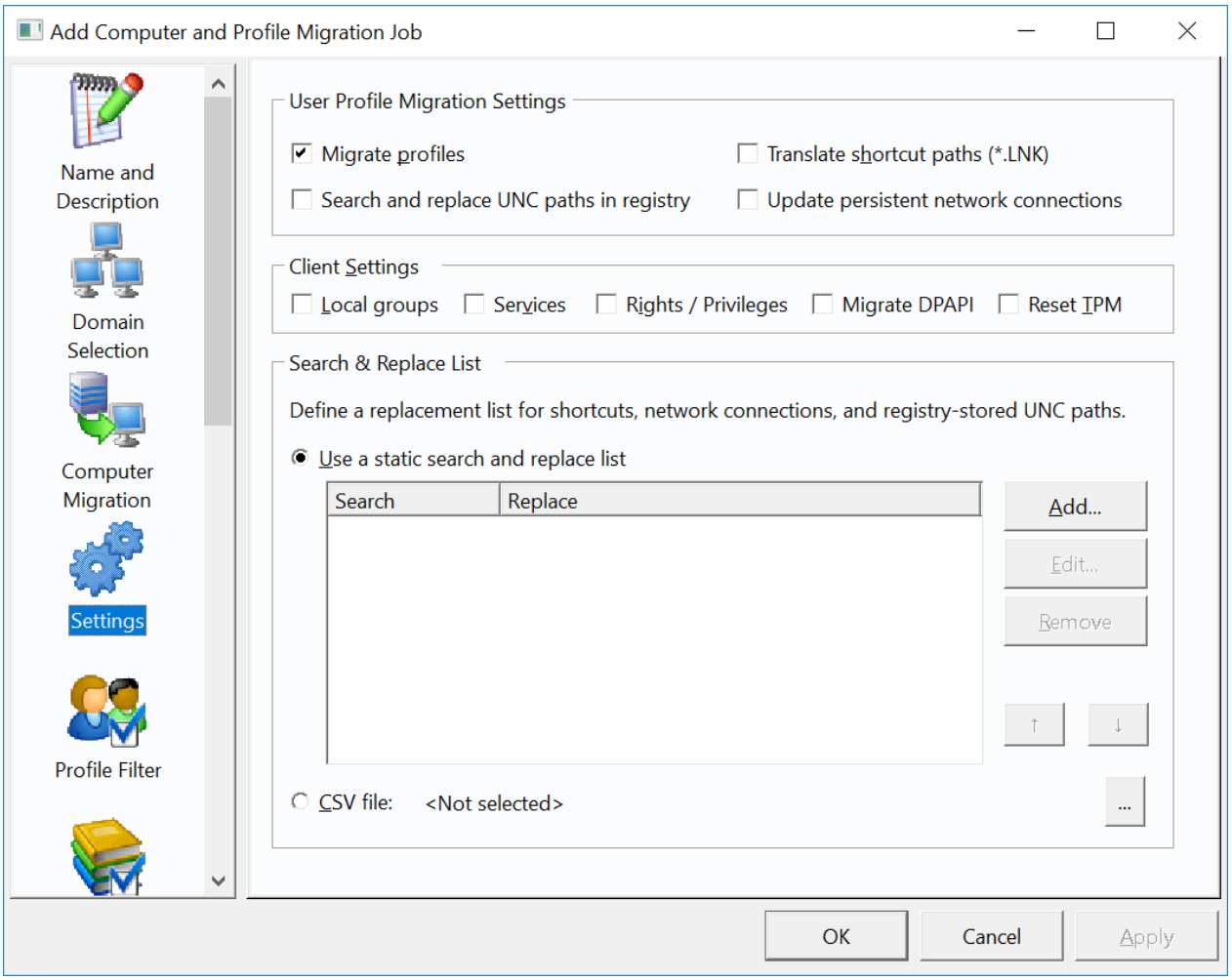
Object Selection

You can either decide to...

- ...process all existing computer accounts.
- ...choose specific computer accounts from your Active Directory, Windows Domain or Network Browser
- ...specify a file containing the computer account names without domain prefix (one account per line).
- …select computer accounts by specifying an Active Directory LDAP query filter condition and a query root as entry point defining where to start the search from.

Settings

In the settings page you can configure the changes you want the job to apply to the selected computers.



User Profile Migration Settings

This group of options allows you to enable the migration of profiles (change permissions accordingly to the new target account), translate UNC paths of LNK shortcuts located in the profile, search and replace strings in the user part of the registry (for example server names in most recently used file lists and update persistent network connections. The replacement will be done according to the data provided in the Search and Replace List.

Local Groups

Enable this option to let the job migrate local group members on the targeted remote computers.

Services

If enabled, the job will migrate accounts used to start services located on targeted remote computers.

Rights/Privileges

Enable this option to migrate accounts that were assigned LSA rights/privileges as shown under Local Security Privileges.

Migrate DPAPI

The “Migrate DPAPI” option will, if enabled, install an additional program on the client computers, that will execute during the user’s first logon with the migrated profile. This additional program will query the user for the password used in the source domain in order to decrypt and re-encrypt the users DPAPI master keys used to encrypt browser stored passwords, RDP passwords, user certificates and other information that 3rd party programs may have encrypted with this Windows API.

Reset TPM

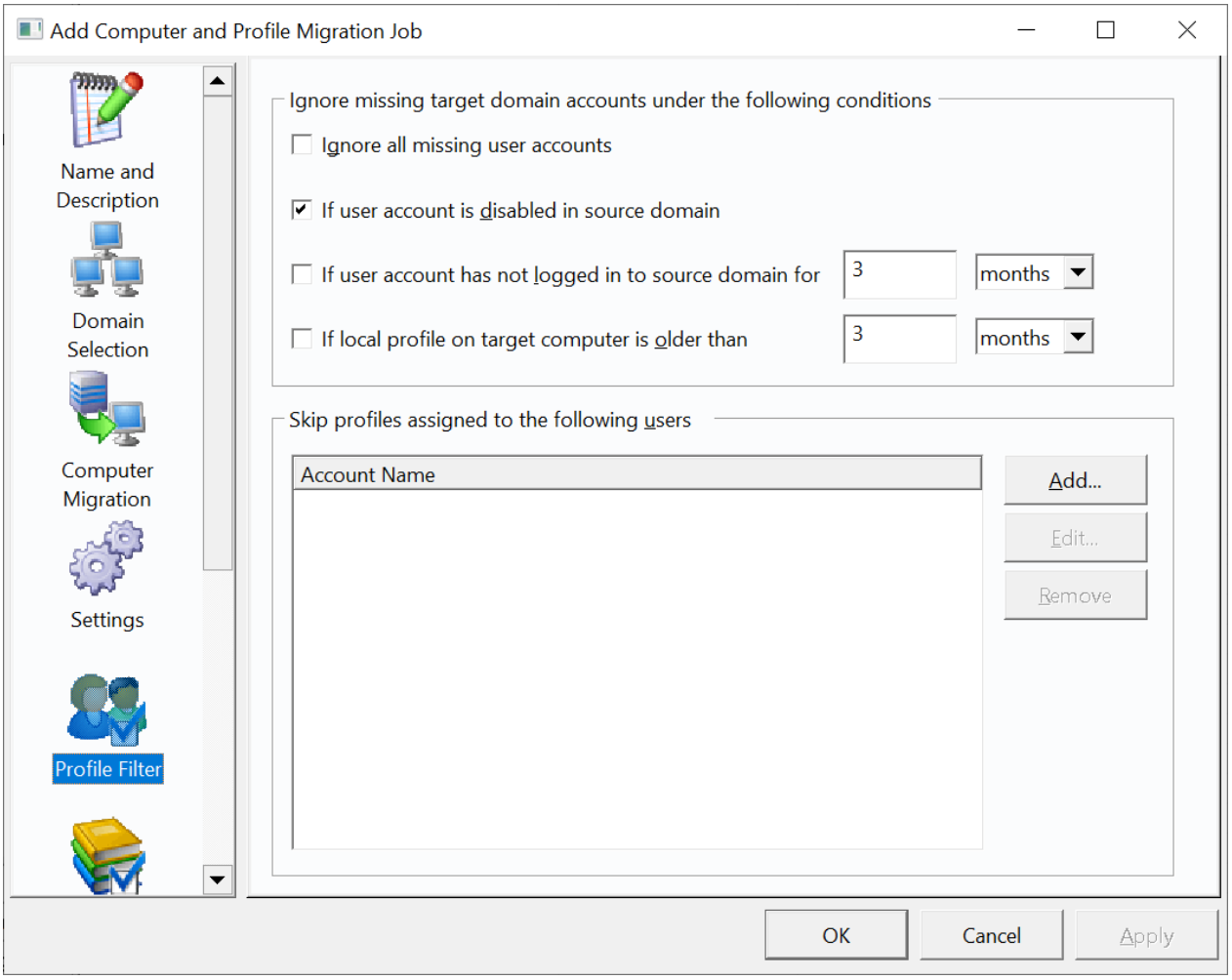
In some environments, users may experience repeated password prompts or error 80090016 when signing into Microsoft 365 services such as Teams, Outlook, or OneDrive after a domain migration. This option clears the cached authentication tokens that were bound to the old domain, forcing users to re-authenticate once and resolve the issue.

Search & Replace List

The search & replace list is used for replacements made in the remote computer’s registry, for LNK shortcuts and persistent network connections. You can either use a static list that is a part of the copy job or alternatively provide the path to a CSV file having 2 columns containing 1 row per replacement.

Profile Filter

In the Profile Filter page, you can define conditions that exclude specific Windows profile from raising an error during the job's execution due to the corresponding user account missing in the target domain.



Ignore Missing Target Domain Accounts Under the Following Conditions

All conditions defined in this section are used in conjunction (logical or operator), so it is sufficient if one of the defined conditions becomes true to ignore a missing target account.

The option "If user account is disabled in source domain" is enabled by default and will ignore missing target accounts for users that are disabled in the source domain.

You can ignore accounts that have not logged on to the source domain for a specified amount of time by using the second option. Please note that the login time stamp used as a comparison is updated by Windows with an accuracy of +-14 days.

Additionally, you can ignore profiles on workstations that are older than a specified amount of time by using the third option.

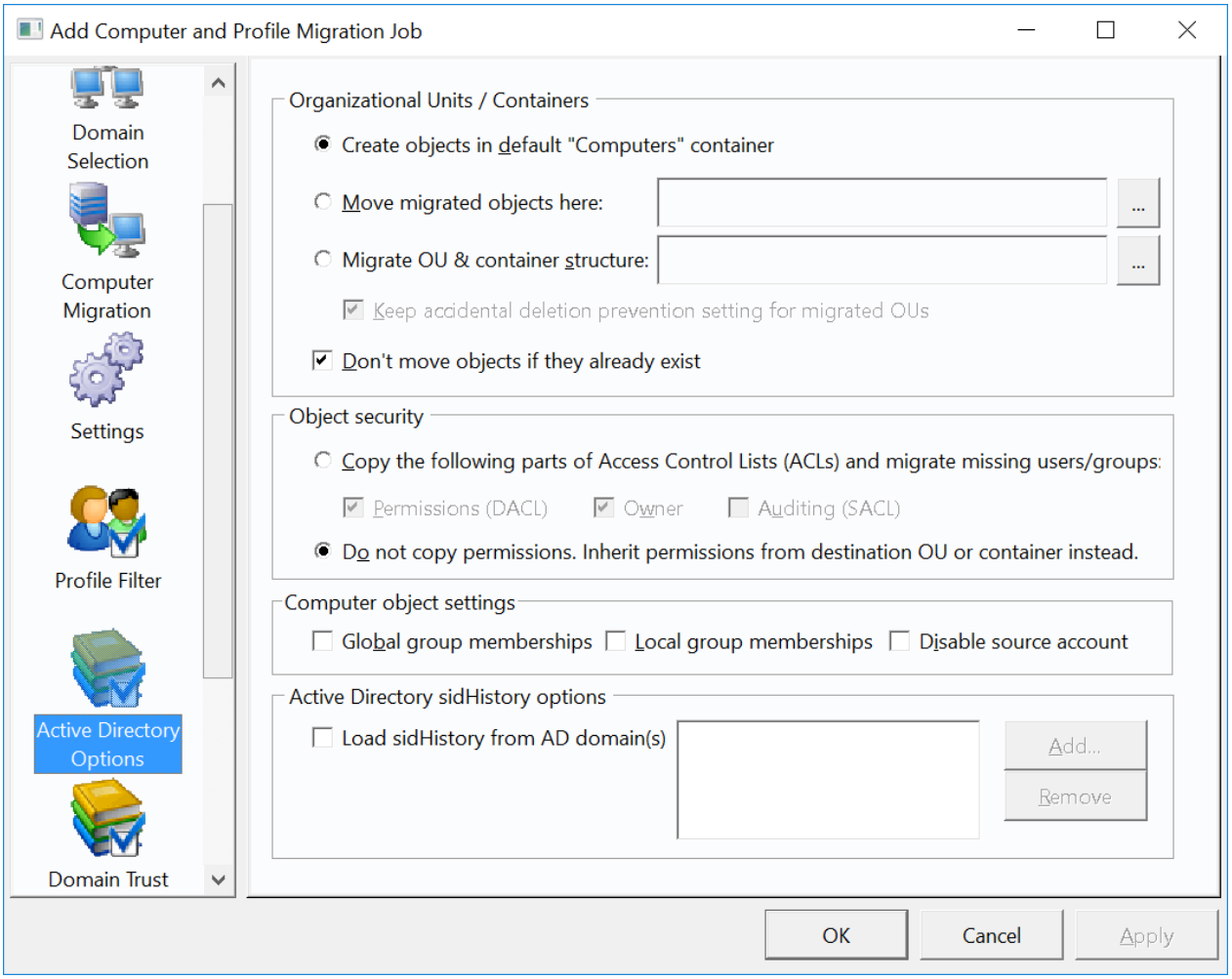
Skip Profiles Assigned to the Following Users

In this section you can define user accounts by samAccountName whose profiles should be ignored during a job's execution. This is useful for example if service accounts should have created Windows user profiles on workstations.

Active Directory Options

If a domain switch is enabled for the job, the Active Directory Options page is used to provide information about where the computer objects should be created in the target domain and how to treat Active Directory permissions of copied computer accounts.

Additionally you can load sidHistory from one or more AD domains. The job will then use the information contained in that attribute to decide which old user (or group) accounts get migrated to which target user (or group) account.



Create Objects in Default “Computers” Container

The default option will migrate any corresponding computers into the “Computers” container.

Move migrated Objects Here

This option will move any migrated computers into the specified OU or container.

Migrate OU & Container Structure

This option migrates each source computer's OU and container structure to the specified location of the destination's Active Directory tree. By default, it uses the destination domains root as a target, causing any OU or container to get created at the same level of the directory tree in the target domain. Additionally, you can configure if you want to preserve the accidental deletion flag or not.

Object Security

The object security settings control how CopyRight2 should treat Active Directory object permissions. You can either inherit permissions from the destination OU/container or you can migrate the permissions (DACL), auditing settings (SACL) and the object owner.

Computer Object Settings

In this section you can configure if the job should migrate computer accounts including their global and local group memberships. Activating the global group option will also migrate group memberships in Universal groups.

The "Disable source account" option will disable the computer object in the source domain after the job completed.

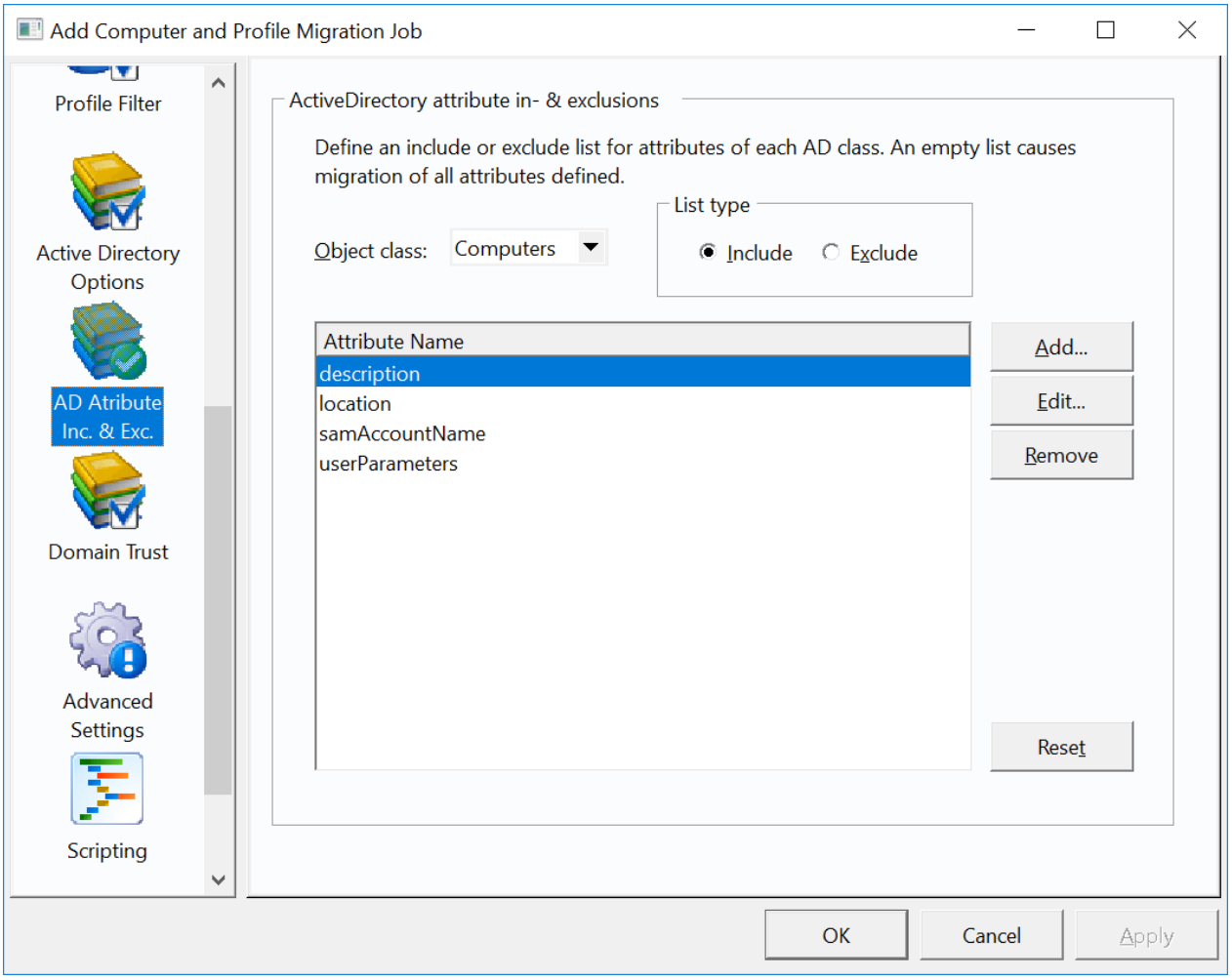
Load sidHistory from AD domain(s)

Use this option to specify one or more Active Directory domains that contain users or groups having the sidHistory attribute populated with their original SIDs. You can either specify a domain controllers NetBIOS name (for example DC9999) or a fully qualified DNS name of the domains (for example domain1.mycorp.com). If activated the job will use Active Directory to determine the existing mapping between old account SIDs and new account SIDs during job execution.

This is useful if users and groups have been migrated including sidHistory in scenarios where you would otherwise require a mapping file.

Active Directory Attribute In- and Exclusion List

The options located in the Active Directory attribute in- and exclusion list allow control over which attributes are migrated between the source and destination domains. You can either define an inclusion list, an exclusion list or an empty list which causes all attributes defined in the schema to get copied.



Object class

Use the object class combo box to select the object type you want to define an inclusion or exclusion list for. Computer and Profile Migration jobs only migrate the “Computers” object class.

List Type

Select either “include” to define an inclusion list or “exclude” to define an exclusion list.

Add/Edit/Remove

Use the “Add”, “Edit” and “Remove” button to remove attributes from the list. Please note that you can select multiple attributes and remove them in a single “Remove” operation.

Reset

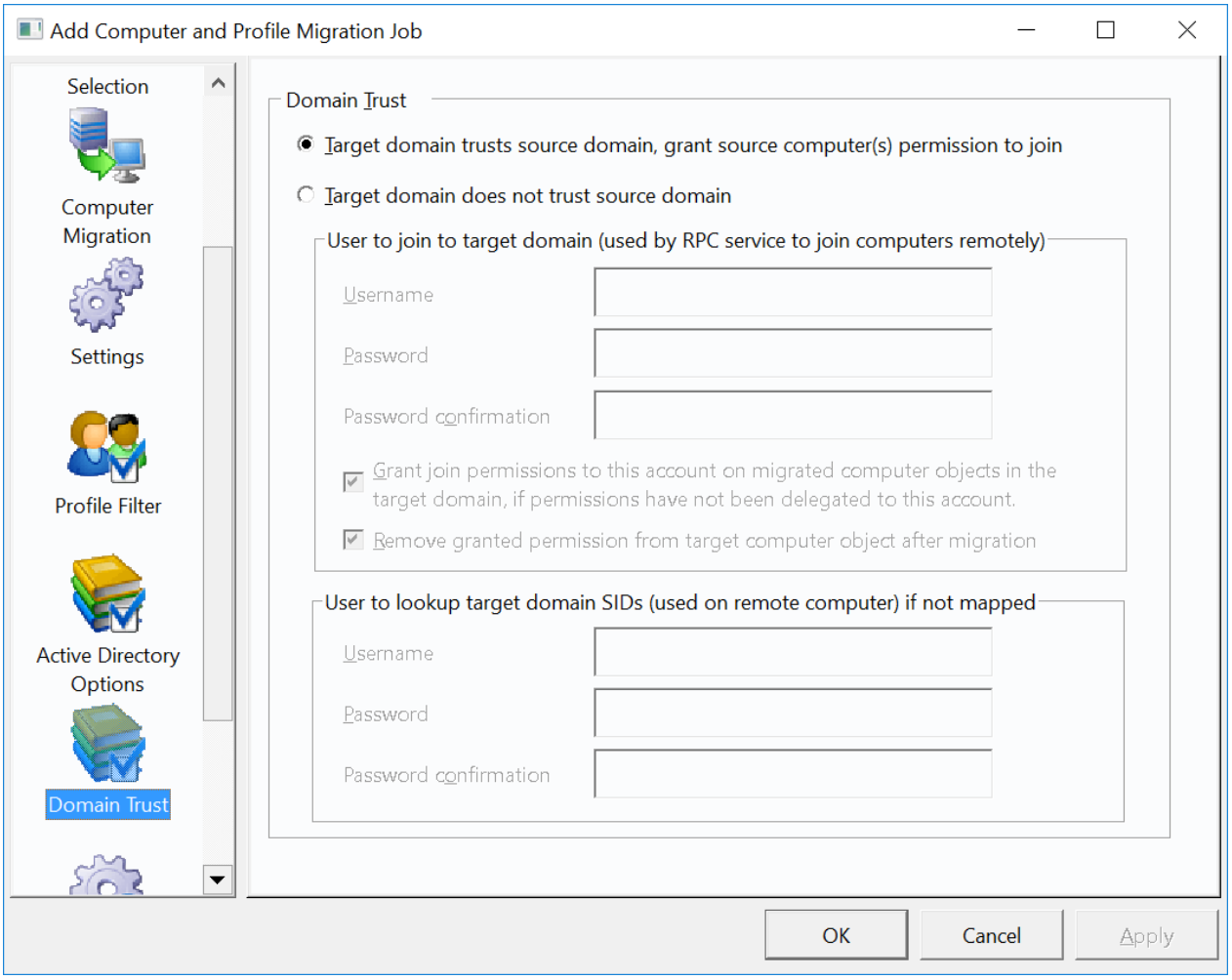
Use the “Reset” button to reset to the default set of attributes defined for the selected object class. The default list includes all attributes that are visible in Window’s “Active Directory Users and Computers” MMC snap-in.

Domain Trust

In the domain trust page you can configure the trust relationship between target and source domain.

If the target domain trusts the source domain, the program will grant the existing source computer object, permissions on the target computer object to join it to the target domain.

If the target domain does not trust the source domain, you can install the RPC service (under Menu -> Options -> RPC Service) on the computer where you run CopyRight2 in the source domain and define the account to be used to join to the target domain and an additional Domain User account to be used for name to SID lookups in the target domain. You can omit a lookup user if you are using a mapping file (under Advanced Settings). Technically the domain join user can be a Domain User account as well.



Target Domain Trusts Source Domain

Select the first option if the target domain trusts the source domain or if it is an intra-forest migration (same forest implying a trust).

Target Domain Does Not Trust Source Domain

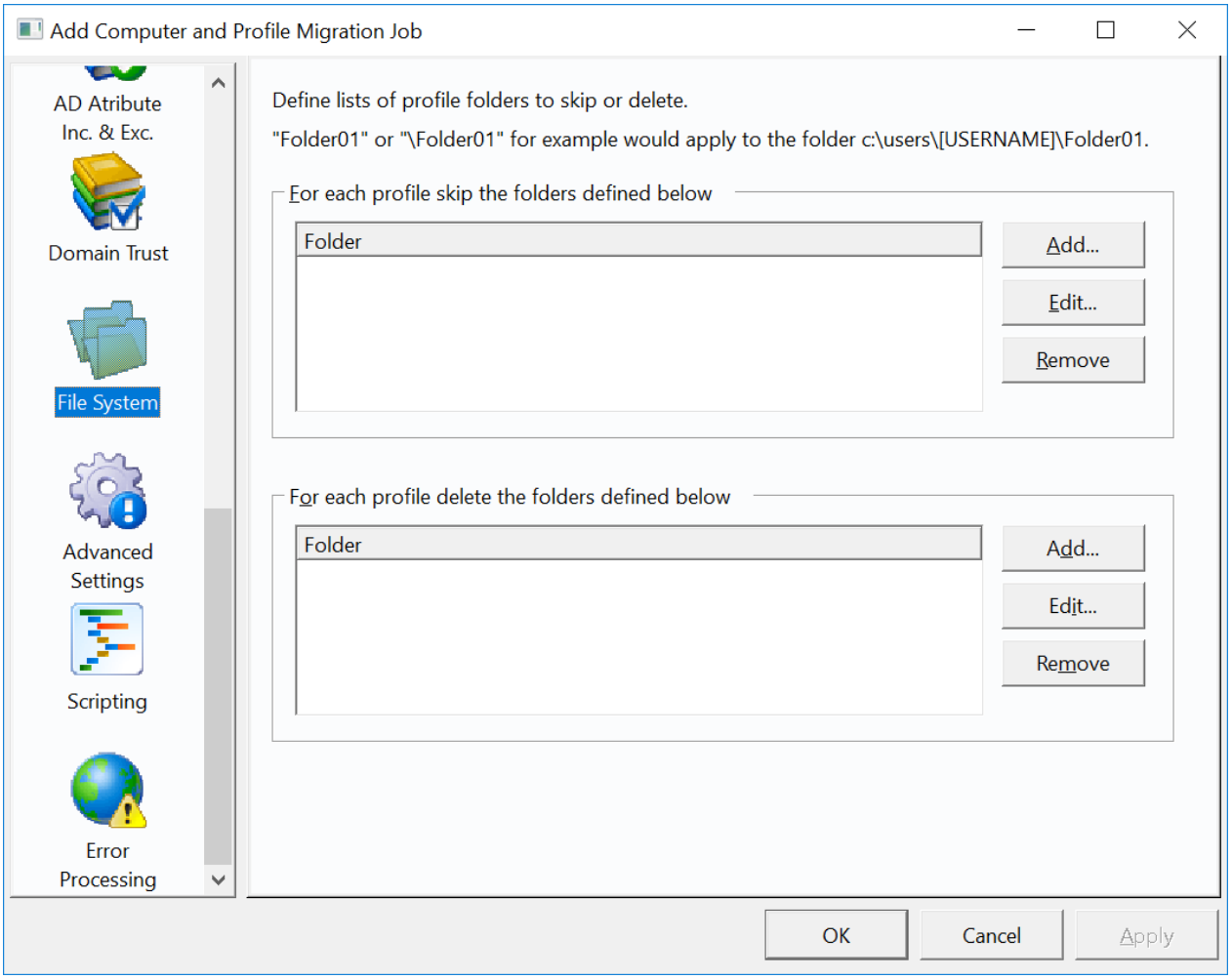
Select the second option if the target domain does not trust the source domain. In this case, provide a user account used by the RPC service to join the computer to the target domain and additionally an account used on the client computer to lookup SIDs by name (to reacl the profiles). You can omit the lookup user account if you supply a mapping file, either manually created or created by a User and Group Migration job.

Grant and Remove Join Permissions

Additionally, you can automatically grant and revoke the specified account's permissions required to join it to the domain. Even if selected, the explicit permission will only be granted if the OU or container the computer object is located in, does not grant permissions to this account already through delegation.

File System

In the file system page, you can define lists of folders to be skipped or deleted during the profile migration phase. The folders are either relative to the profile folder, for example “Folder01\Folder02” or “\Folder01\Folder02” to exclude these folders for each processed profile or absolute, like “c:\users\MyUser\FolderToExclude” to target a folder of a single profile only.



Skip Profile Folders

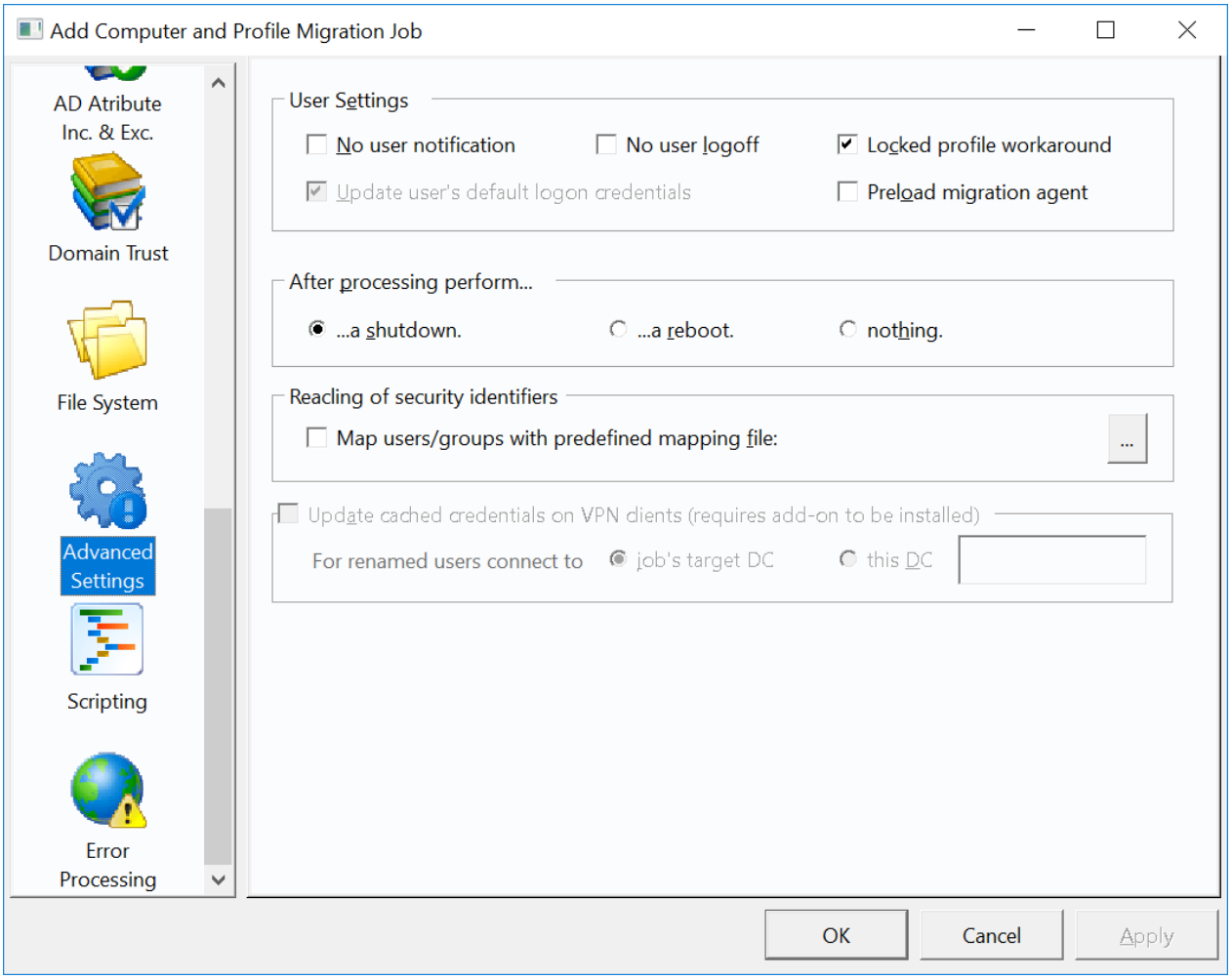
The specified folders will be excluded from being reACLed and get skipped.

Delete Profile Folders

The specified folders will be deleted during execution of the Computer and Profile Migration job by renaming them.

Advanced Settings

In the Advanced Settings page you can configure additional options to be used by the job that influence the workflow and user experience.



No User Notification

Enabling this option, turns off end user notifications on targeted computers. Instead of displaying the default or the customized message and waiting for user feedback or the configured time out to elapse, the job will directly begin processing.

No User Logoff

By default, the currently logged on user on a targeted remote computer will be logged off. This can cause issues for VPN clients opening the VPN tunnel or Wifi clients authenticating to the network, from an application running within

the user's logon session, as such applications get terminated during sign out.

Enabling this option requires either that the "Locked profile workaround" option is enabled as well or that the currently logged on user on the targeted remote computer is either a local account or a domain account not requiring its profile to be migrated.

Locked Profile Workaround

This option is intended to be used in conjunction with the "No user logoff" option. Without enabling this option, the profile of the currently logged on user is locked and cannot be migrated.

It can additionally resolve issues with 3rd party applications not releasing user profiles and keeping file and registry handles open, if a user is logging out due to software faults or bad design choices.

Update User's Default Logon Domain to Target Domain

This option controls if the migration process should update the last logged on user's domain on remote computers to the target domain. If enabled it will additionally handle the case where a mapping file has been configured in the job's settings due to different samAccountName's of source and target users, to update the samAccountName or UPN name accordingly.

Preload Migration Agent

If this option is enabled, a two-phased approach to deploy the migration agent onto targeted computers will be used. During the first phase, the job will deploy the migration agent and validate that all domain profiles on the remote computer have an associated account in the target domain. If that succeeds, the computer will show a state of "Preloaded". After changing the state to "Primed" from the "View Job Status" dialog and running the same job again, the job will be launched.

For Each Profile Delete the Folders Defined Below

The specified list of folders, relative to the profile path, will be deleted automatically in each migrated user profile.

After Processing

Here you can control what should happen on the client side after the computer has been processed. The default option will shut down the remote computer but you can optionally issue a reboot or nothing instead.

Reacling of Security Identifiers

You can provide the process with a mapping file, that you previously prepared or for example one created automatically during the execution of a User and Group Migration job.

This is useful in case the target user, group or computer accounts have different samAccountNames due to the naming convention.

You can rename target computers using the same format you would use, to let the software create users and groups with different samAccountNames by specifying the ";3" option (see chapter "Rename samAccountName of Target Account"):

```
Src-Domain\WKS01$;Dst-Domain\WKS-0001$;3
Src-Domain\WKS02$;Dst-Domain\WKS-0002$;3
…
```

Renaming Computer Accounts Example

Please note the appended dollar sign.

Updating Cached Credentials on VPN Clients

This option is only selectable after installing the Cached Credential Update Add-On. If the add-on is not installed, the option will be grayed out.

It enables processing of cached credentials in case you are using a VPN client without a so-called GINA.DLL, depending on a cached credential logon before the VPN tunnel can be opened from an application running inside the user's logon session. The same applies to Wi-Fi clients requiring an additional form of authentication, for example based on certificates, taking place after the Windows logon and from within the user's logon session.

If a mapping file is used to change the samAccountName's of users, you will need to install the CopyRight2 Password Migration Filter on the targeted domain controller if the "job's target DC" option is used or on the specified domain controller, if the "this DC" option is used.

Additionally, you will need to set the registry value "HKLM\Software\Sys-Manage\CopyRight\PwdFilter\Options" to a REG_DWORD of either 0 (to allow password hash migrations AND cached credential migrations of renamed users) or 1 (to disable password hash migrations but enable cached credential migrations of renamed users).

Changing this option requires a reboot. You can set the option, before the filter gets loaded, right after its installation.

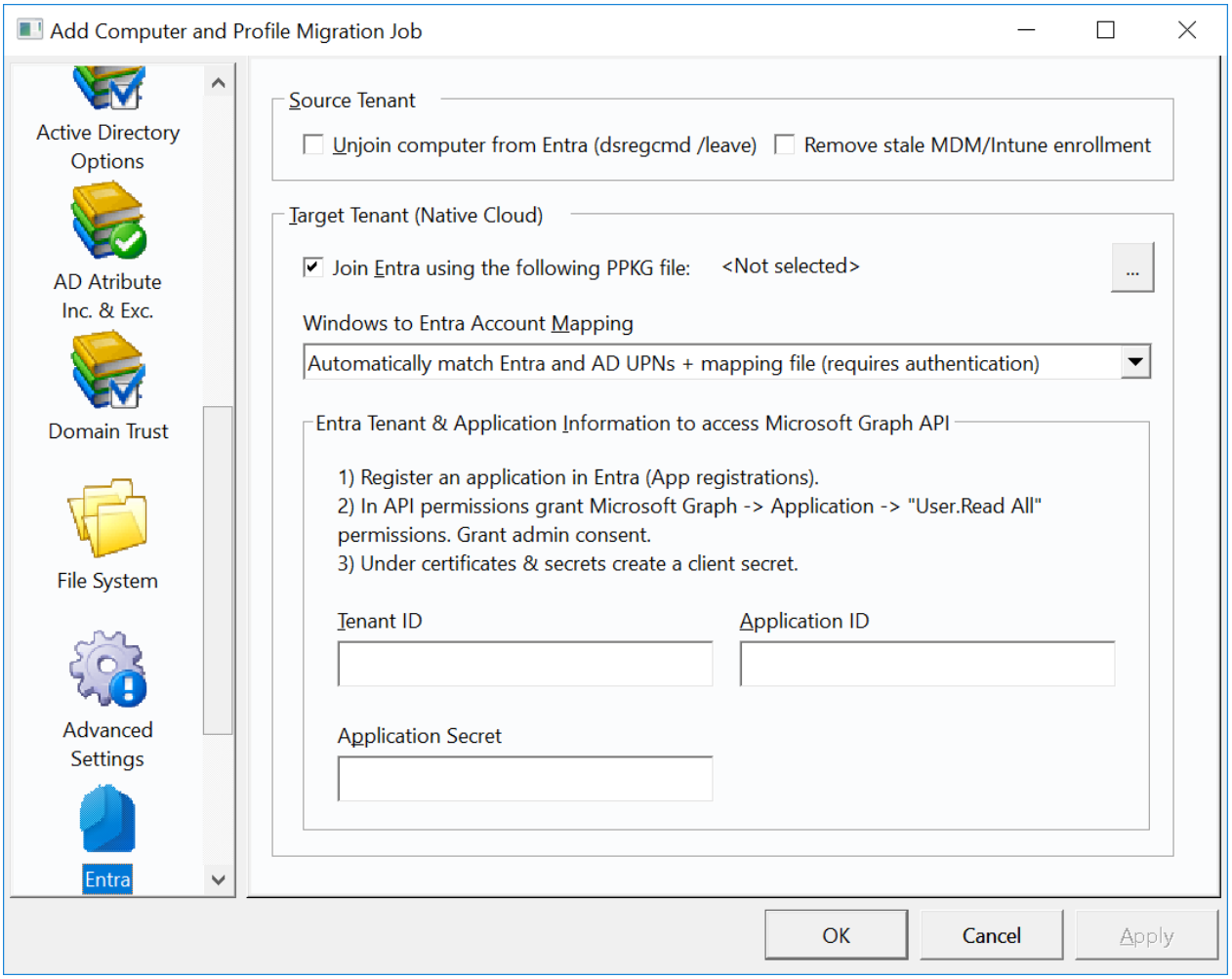
Entra

Within this tab you can configure options for Microsoft Entra device joins. You can let devices leave an existing joined Entra tenant and/or join a new Entra tenant.

To join an Entra Tenant use the Microsoft Windows Configuration Designer available in the Windows store and assign the created PPKG file in the job's settings. You can find more information about how to create the PPKG file in the "Creating a PPKG File with Microsoft Windows Configuration Designer" chapter.

The job settings control how existing profile owners should be mapped to user objects residing in the Entra tenant.

Depending on the mapping method, you may need to register an application in Entra and provide authentication information. You can find more information on how to configure authentication in the "Configuring Authentication for Microsoft Entra Device Migrations" chapter.



Unjoin Computer from Entra

If the “Unjoin computer from Entra” option is enabled, the remote computer will execute a “dsregcmd /leave” command before attempting to join the target domain or the target Entra tenant.

Remove stale MDM/Intune enrolment

Enable this option, to let the client automatically clean up stale MDM/Intune registration information, in case of issues enrolling to the target tenant.

Join Entra Using the Following PPKG File

Use this option to enable a Microsoft Entra device join by assigning a previously created PPKG file.

Windows to Entra Account Mapping

CopyRight2 currently offers 3 methods to map profile owners to Windows Entra accounts.

Option	Description
Mapping file using Entra GUIDs	The job has a mapping file assigned, that maps Windows accounts to target Entra users by their Entra ID GUID. In this case no Entra authentication is required.
Mapping file using Entra User-Principal-Names and GUIDs	The job has a mapping file assigned, that maps Windows accounts to target Entra users by their Entra User-Principal-Name. In this case Entra authentication is required.
Automatically match Entra and AD UPNs	This job does not necessarily have a mapping file assigned. Users are mapped by matching Windows and Entra User-Principal-Names automatically.

Tenant ID, Application ID and Application Secret

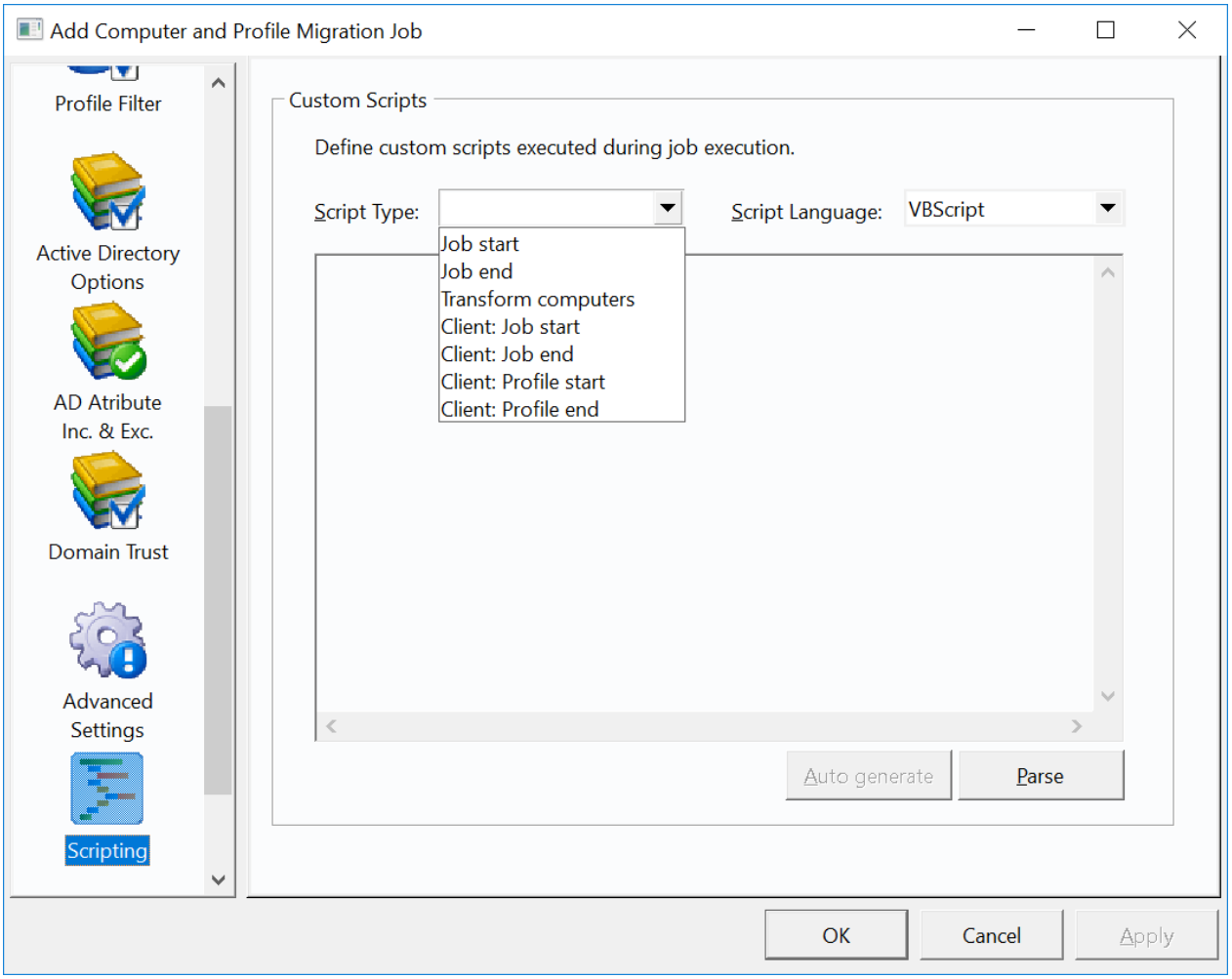
Provide information required to authenticate to the target Entra tenant. You can find more information on how to configure the Entra application in chapter “Configuring Authentication for Microsoft Entra Device Migrations”.

Note: The application secret is encrypted using the currently logged on user’s session key. If the job should be scheduled for background execution, please ensure the scheduled job is running under the same credentials. The decryption will fail in case another user account is used.

Scripting

Within this tab you can define multiple custom scripts to get executed during specific events, for example when the computer migration job starts or ends, to transform the migrated computer objects or when an instance of a profile is being migrated. The script types prefixed with “Client:” are running on the client side.

You can use VBScript, which is the default option) or any other installed ActiveScript language to define the script’s code. Please see the chapter “Using ActiveScript” for more information about how to write scripts.



Script Type

Please select the type of script. You can define scripts executed when the copy job starts and when it ends. You can also specify a script executed when two individual servers, specified as source and destination, do start and end copying. Additionally, you can define scripts for each type of object that gets migrated (Users, Groups, Contacts, OUs).

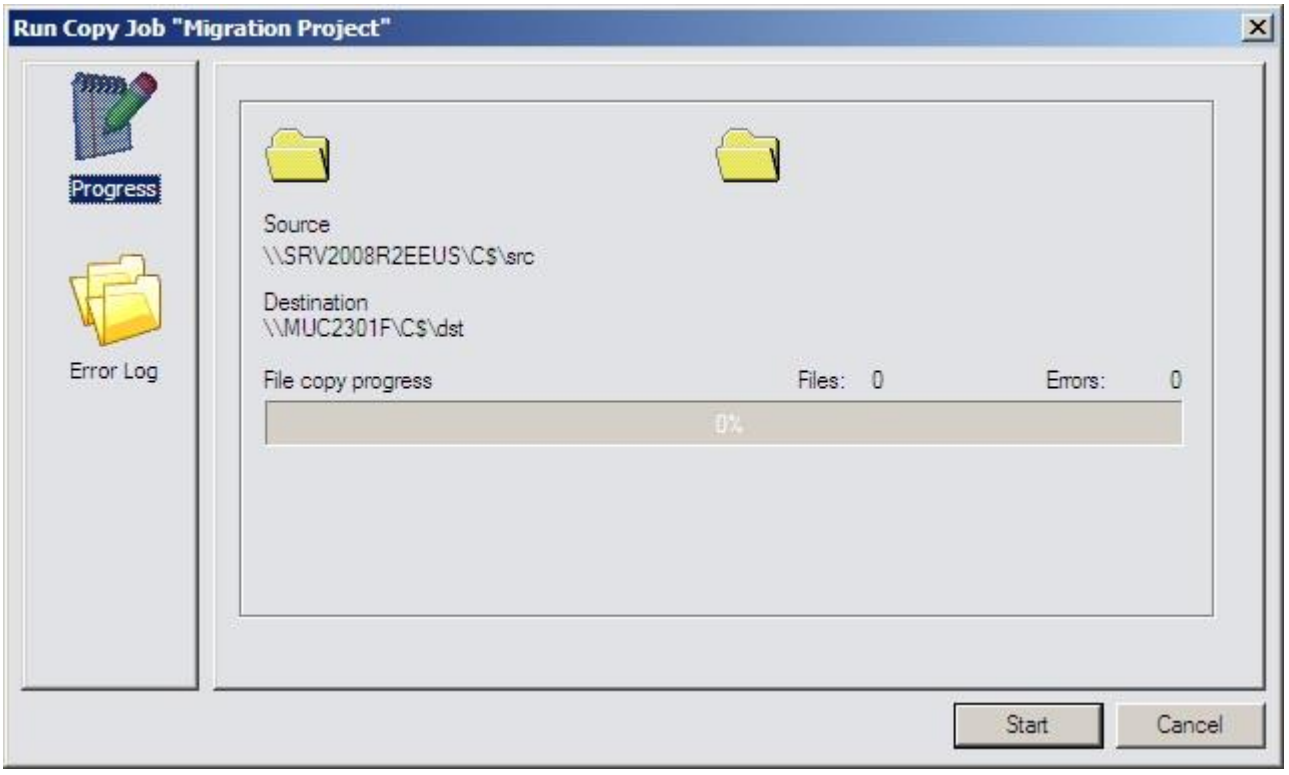
If you need your script to write to the HKEY_CURRENT_USER hive of the currently processed profile, please ensure to use the “Client: Profile start” event. When scripts for this event are processed, it is guaranteed that HKEY_CURRENT_USER will point to the hive of the currently processed user. If other events, such as “Client: Job start” is used HKEY_CURRENT_USER may point to the HKEY_USERS\.DEFAULT hive.

Script Language

The script language setting allows you to select which script language to use to code the scripts.

Running a Job Interactively

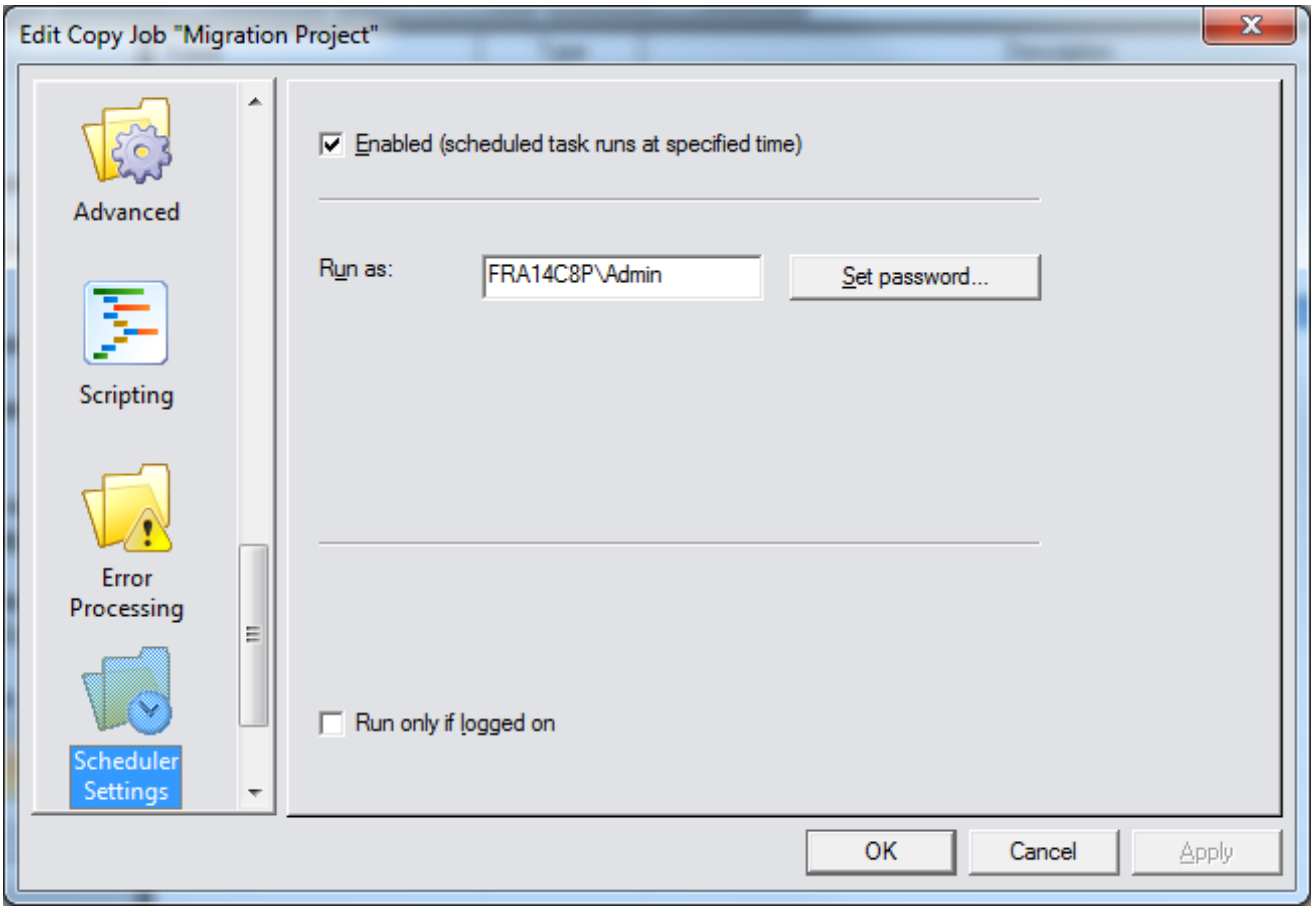
You can run a job locally once it has been defined using the Scheduler by clicking on the “Run Now” button. A Job progress dialog will show up that you will have to confirm to actually start the job. During the job’s execution a bar will indicate how the job is progressing; any error output will be available within the “Error Log” tab of the progress dialog. After the job has completed please click on “Close” to close the dialog. Please note that copy jobs will not run remotely unless scheduled for remote execution (see next chapter). Instead they run locally on the computer where the Scheduler GUI is executed currently. This results in the data being transferred from the source computer to the computer executing the GUI and back again to the target computer. You can however, execute the Scheduler GUI (e.g. using Terminal Services) on the source or target computer to prevent this from happening. To maximize performance, it is recommended that you run it on the target computer.



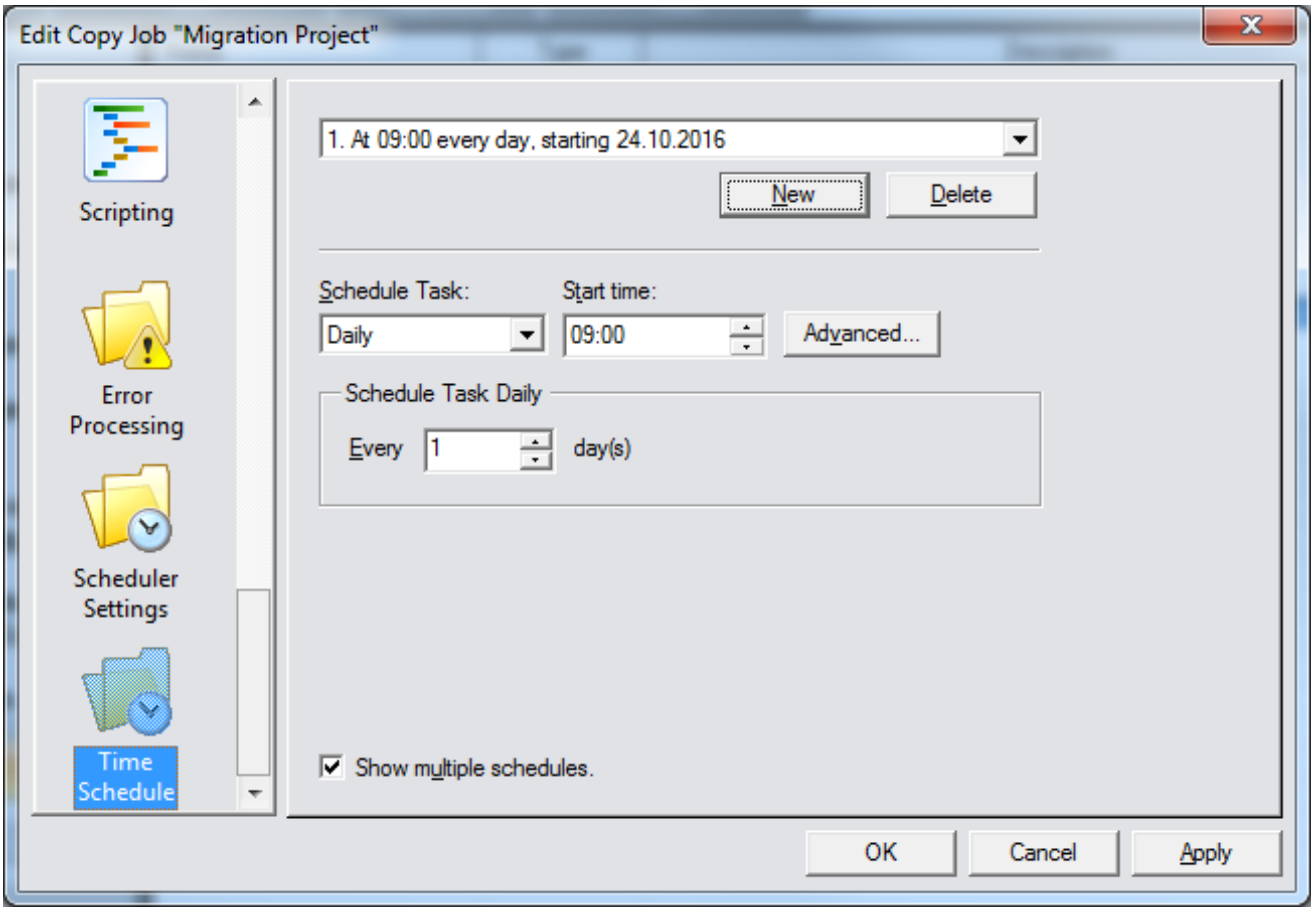
Scheduling a Job for Background Execution

You can schedule any job for remote execution by using the “Scheduler Settings” and “Time Schedule” tab from within the job’s definition.

You will have to provide a valid account that has the required privileges and the account’s password within the “Scheduler Settings” page:



Next define a schedule within the “Time Schedule” page that you want the job to run under. This will remotely create a job within Window’s Scheduler. The job will run automatically in the background using that schedule without the requirement of leaving the CopyRight2 Scheduler running on the management computer. You can check the remote job’s log file at a later time (see Viewing a Job’s Log File).



Viewing a Job's Log File

To view the currently selected job's error log after its completion you can click on the "View Log File" button. This will open up the log file with notepad. If the button "View Log File" is grayed out, there is no log file available.

Copying and Pasting a Job Definition

You can copy and paste a job to duplicate an existing job's setting. You can use copy & paste within the same server or remotely to copy a job definition to another server.

To copy and paste a job definition from one server to another by opening two instances of the Scheduler connecting to each server. Next select the job you want to cut or copy and use the corresponding button to actually cut or copy it to the clipboard. Then open the target instance and use the paste button to create an identical job on the target server.

InfraStructure Reporting

The CopyRight2 InfraStructure Reporting feature can be used to gather information about your environment in a variety of different formats, such as text files (CSV), Microsoft Access Databases or directly imported into a Microsoft SQL Server database. If using Microsoft SQL Server to import the data, you can use Microsoft Reporting Services and CopyRight2's preinstalled reports, define your own reports and run ad-hoc queries using the collected data.

The collected data includes the following.

File and File Share Information:

- Files
- Folders
- NTFS Permissions
- File Shares
- File Share Permissions
- Version Information (DLL, EXE and SYS Files)
- File Hashes for Files and Folders (MD4, MD5, SHA1, RIPEMD160, CRC 8-Bit, SHA-256, SHA3-256)

Local Account Information:

- Local Users
- Local Groups
- Local Group Members
- Rights (Privileges)

Computer Information:

- Installed Software Applications
- Installed Windows Components
- Services
- Drivers

Active Directory Information:

- Users
- Groups (Local, Global, Universal)
- Distribution Lists
- Contacts
- Built-in Accounts
- Organizational Units (OU's) and Containers
- Computers
- Trusts

CopyRight2 uses 3 types of jobs to scan remote systems and collect the results:

Name	Description
Computer Scan	Used to collect file & share information, local account information and computer information. It can scan one or more systems and uses a remote agent for maximum performance.
LDAP Scan	Used to collect information from Active Directory.
Scan Import	Used to import the collected data, either into the "Data" folder located below the installation folder or directly into a Microsoft SQL Server database.

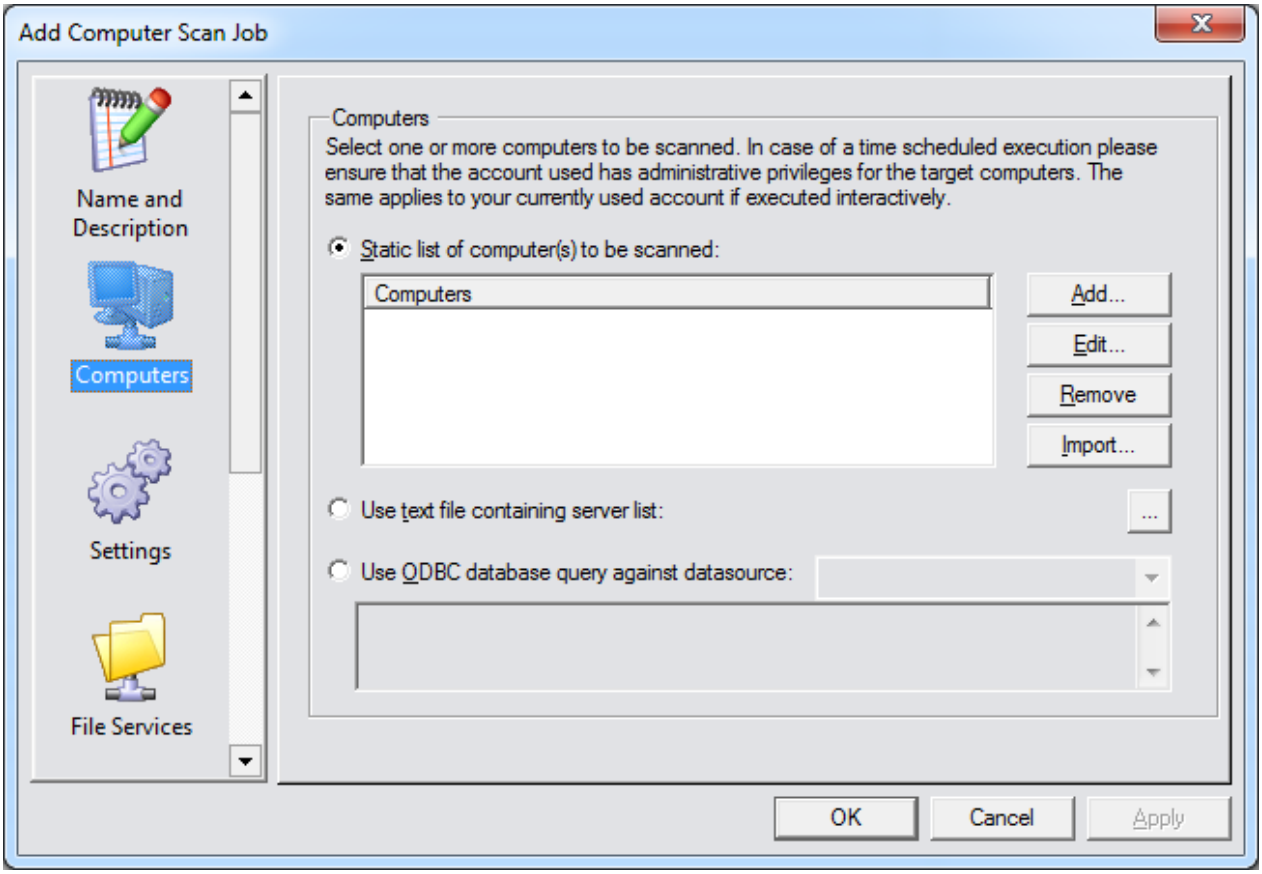
You can find how to add those type of jobs in the following chapters. The jobs can be scheduled for background execution to collect the data in a specified interval, for example daily or weekly.

Note: Please watch the 3-part tutorial in our YouTube channel for more information on how to setup SQL Server with Reporting Services and how to define the 3 jobs to produce data.

Adding or Editing a Computer Scan Job

A “Computer Scan” job, provides information about files & file shares, local accounts and computer information. Each job can scan one or more remote systems. During execution CopyRight2 will temporarily install a service on the remote Windows computer or in case of NAS appliances, use the assigned Windows PC, preferably located in the same network location.

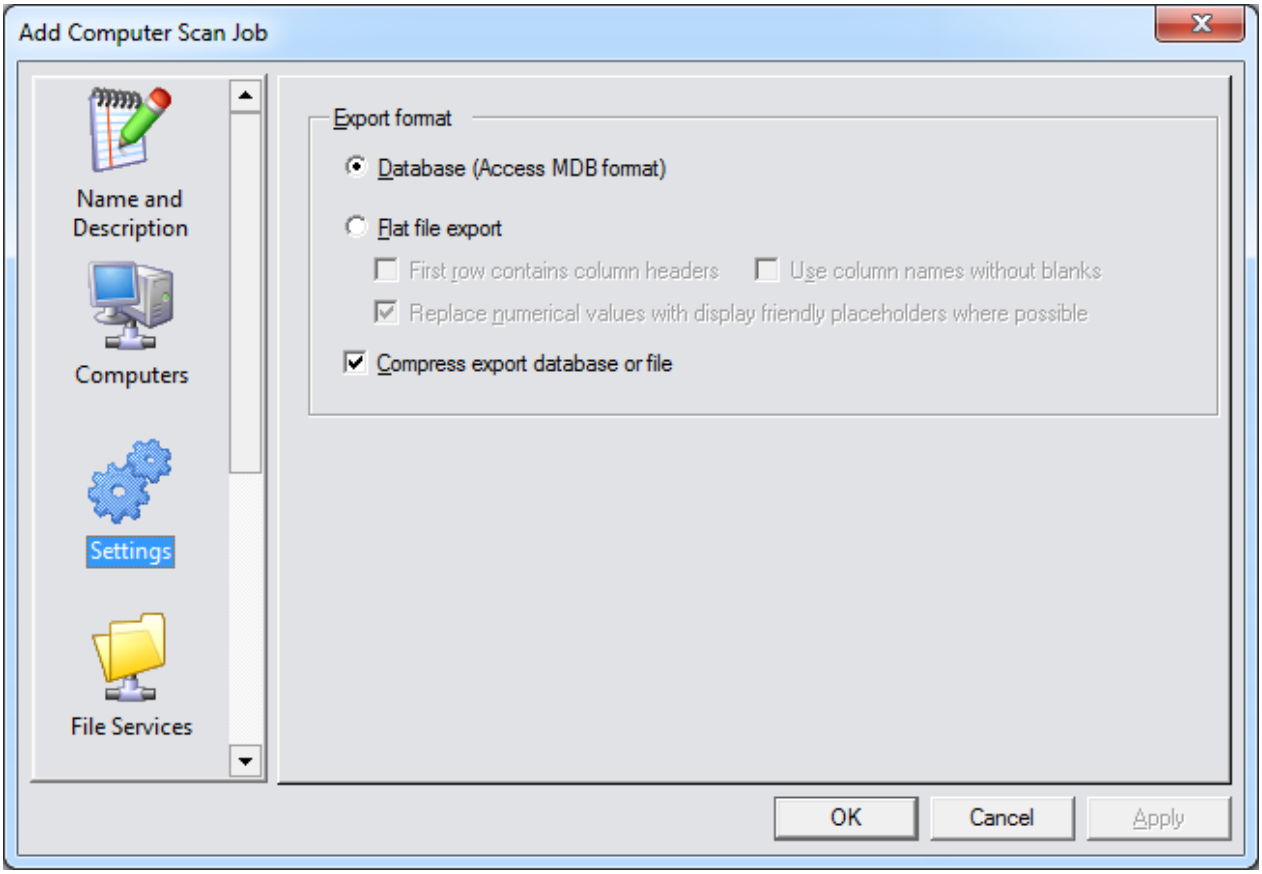
Computers



Computers

You can either specify a static list of computers (or NAS systems), the path to a text file containing the computer names or an ODBC data source and a SQL query producing the computer names to get scanned. The result of specifying a text file or a SQL query work dynamically and are executed every time the job is executed.

Settings



Export Format

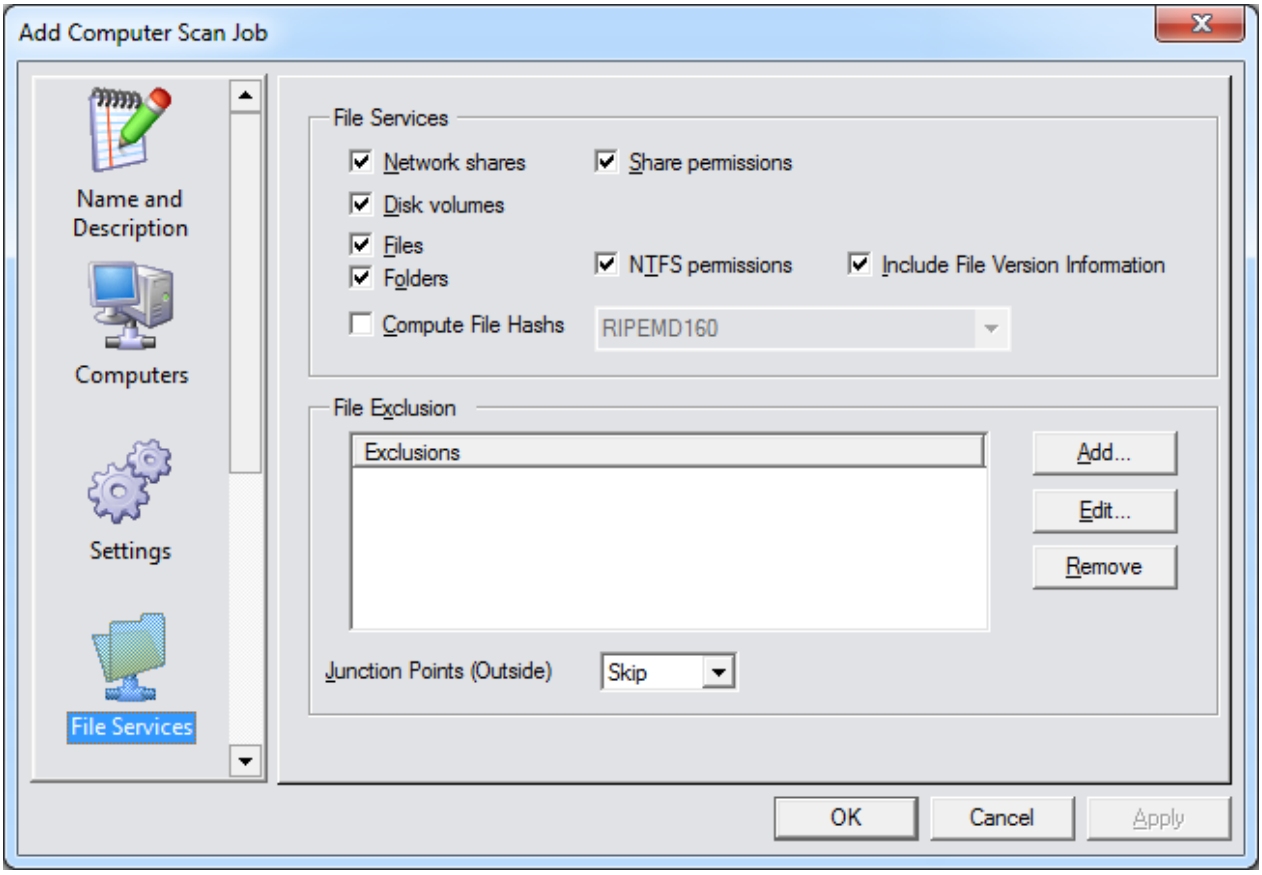
The collected data can be exported either in Microsoft Access MDB format or in text format as a flat file. If exporting in flat file format, you can additionally enable a first row header containing the column names, database "friendly" column names without blanks and automatic replacement of numerical values with clear text values.

If you want to import the data into Microsoft SQL Server, for example to use the predefined Microsoft Reporting Server reports, it is required to select the "Database" format.

If text file output is sufficient for your purposes and/or you don't want to run a SQL Server you can select "Flat File Export" instead.

The "Compress export database or file" option will compress the produced output before transmission and uncompress it when the "Scan Import" job is run to pull the data to reduce the amount of data transferred.

File Services



Network Shares / Share Permissions

If enabled the software will collect existing network shares and optionally share level permissions.

Disk Volumes

If enabled, the software will collect information about disk volumes, such as capacity, remaining disk space and cluster sizes.

Files, Folders and NTFS Permissions

If enabled the software will collect information about files, folders and their NTFS permissions. It will scan the entire file system of the target system.

Include File Version Information

This options controls whether the software should collect version information for executables, DLLs and device drivers.

Compute File Hashes

If enabled, the software will calculate a hash checksum for each file and each folder. The folder checksum includes all the files & folders below. You can select different hash algorithms, for example “RIPEMD160”, “MD4”, “MD5”, “SHA1”, “SHA-256” and “SHA3-256”.

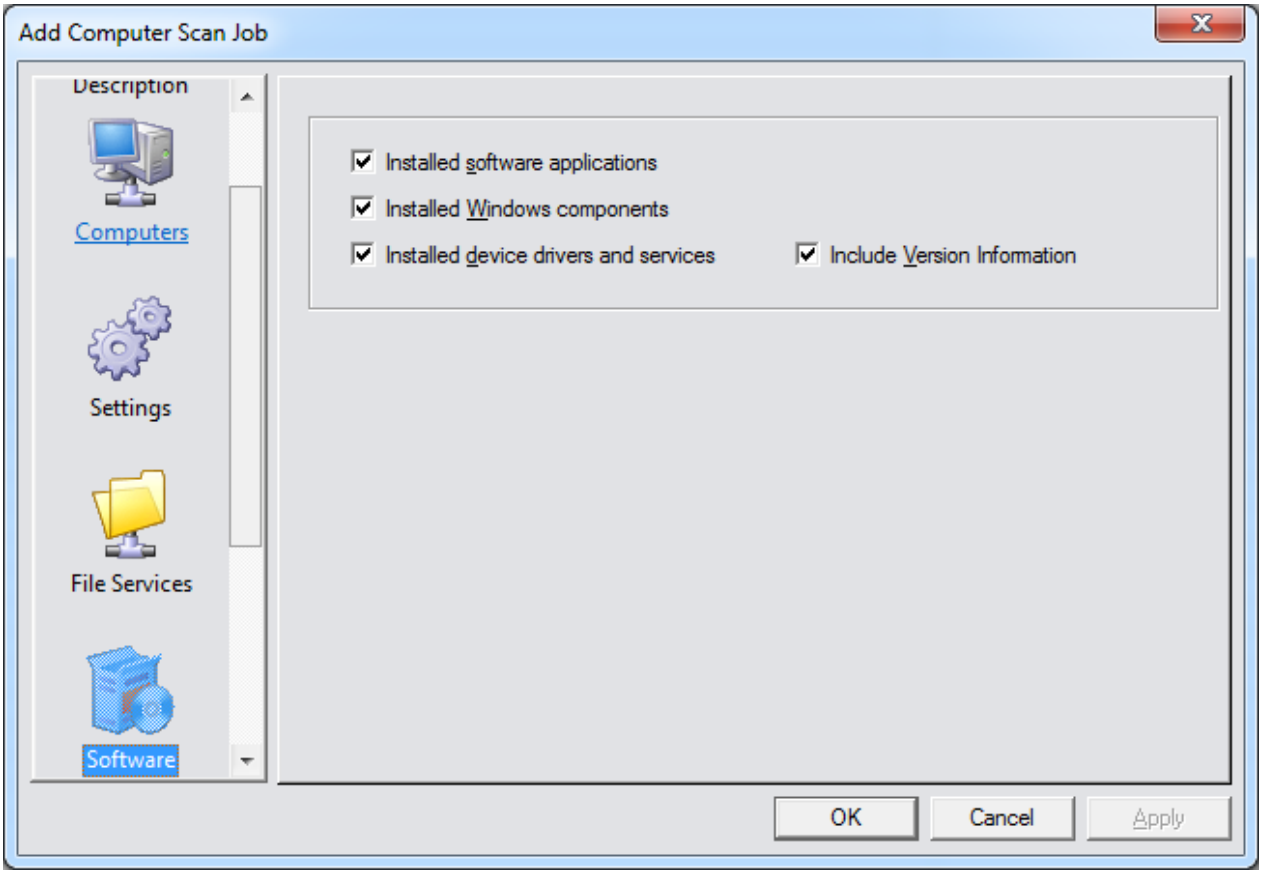
File Exclusion

Here you can define certain files, file types or folders to get excluded from the scan.

Junction Points (Outside)

This option defines how junction points are treated during file scan, by default they will get skipped.

Software



Installed Software Applications

If enabled, the agent will collect the installed software applications from the Windows computer.

Installed Windows Components

This options controls if the agent should collect installed Windows components.

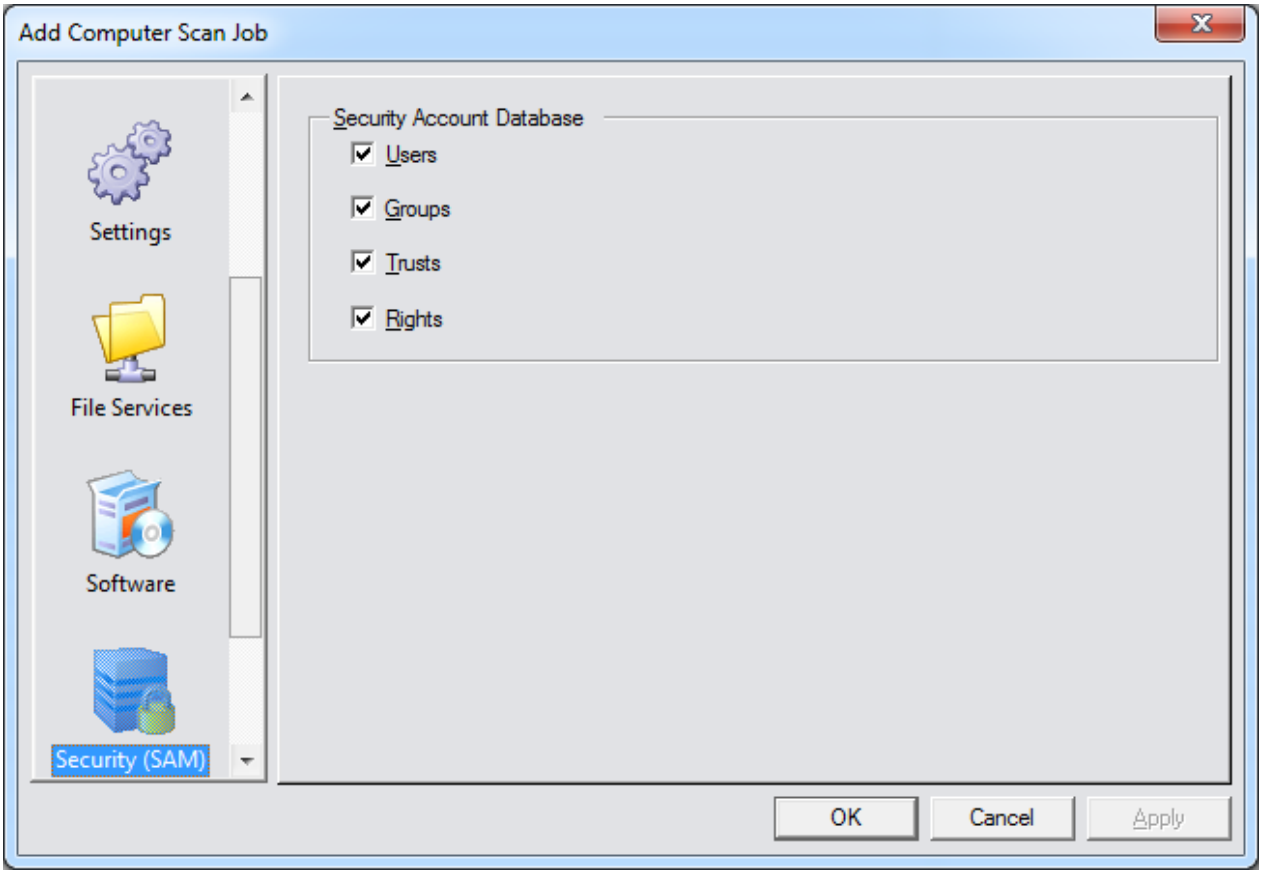
Installed Device Drivers and Services

This options controls if the agent should collect installed device drivers and services.

Include Version Information

This option controls if the agent should additionally collect the file version information of services and device drivers.

Security (SAM)



Users, Groups and Trusts

This setting controls whether to collect local users, local groups and domain trusts (incoming or outgoing) from the target systems. Those settings are ignored for Active Directory domain controllers, instead a LDAP scan will collect the required information from the domain controllers.

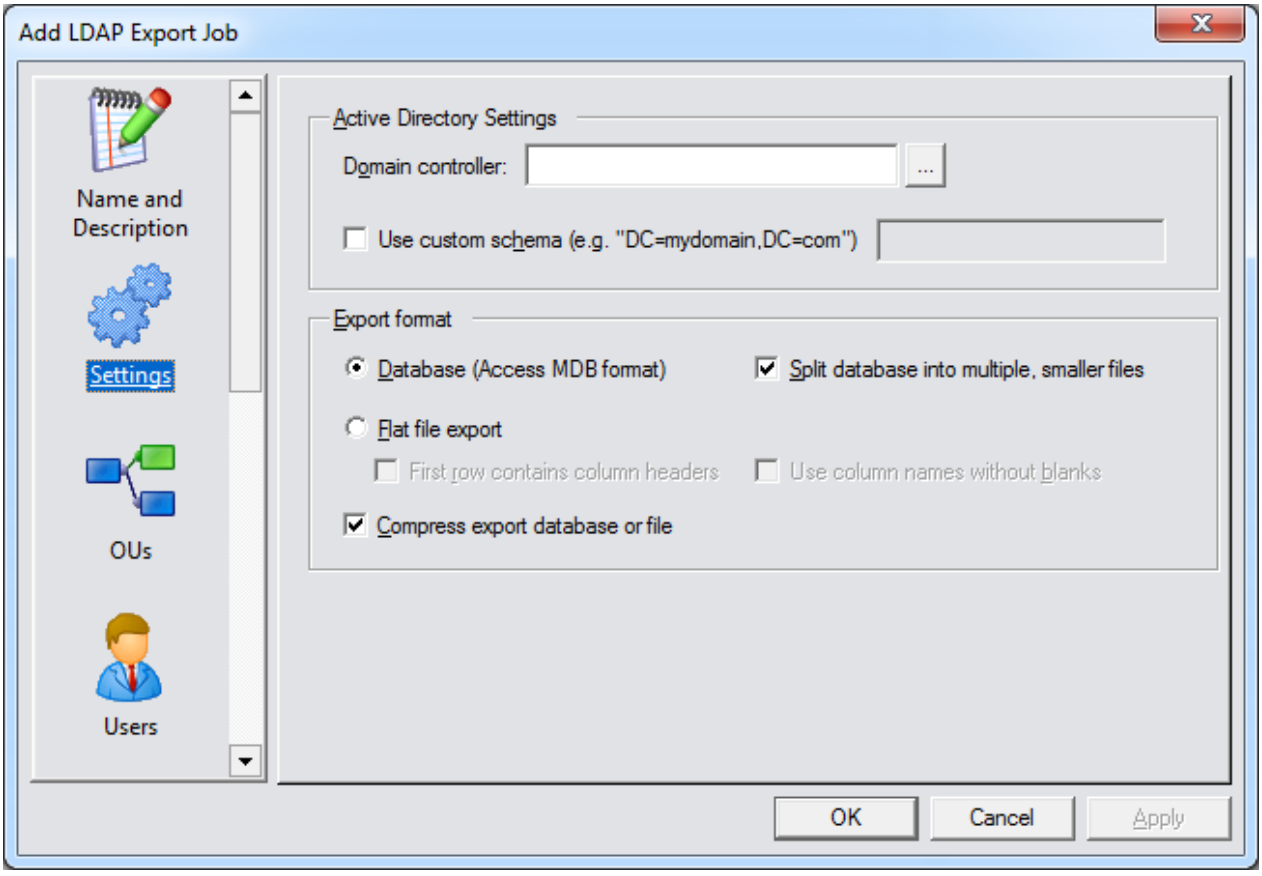
Rights

This settings controls if CopyRight2 should collect Windows privileges (rights) from the target systems.

Adding or Editing a LDAP Scan Job

A “LDAP Scan” job, collects Active Directory information from the specified domain controller. You can define one or more jobs in case of multi-domain environments.

Settings



Domain Controller

Specify the NetBIOS name of a domain controller of the Active Directory to scan.

Use Custom Schema

Enable this option to specify that the Active Directory schema is located in a root domain.

Export Format

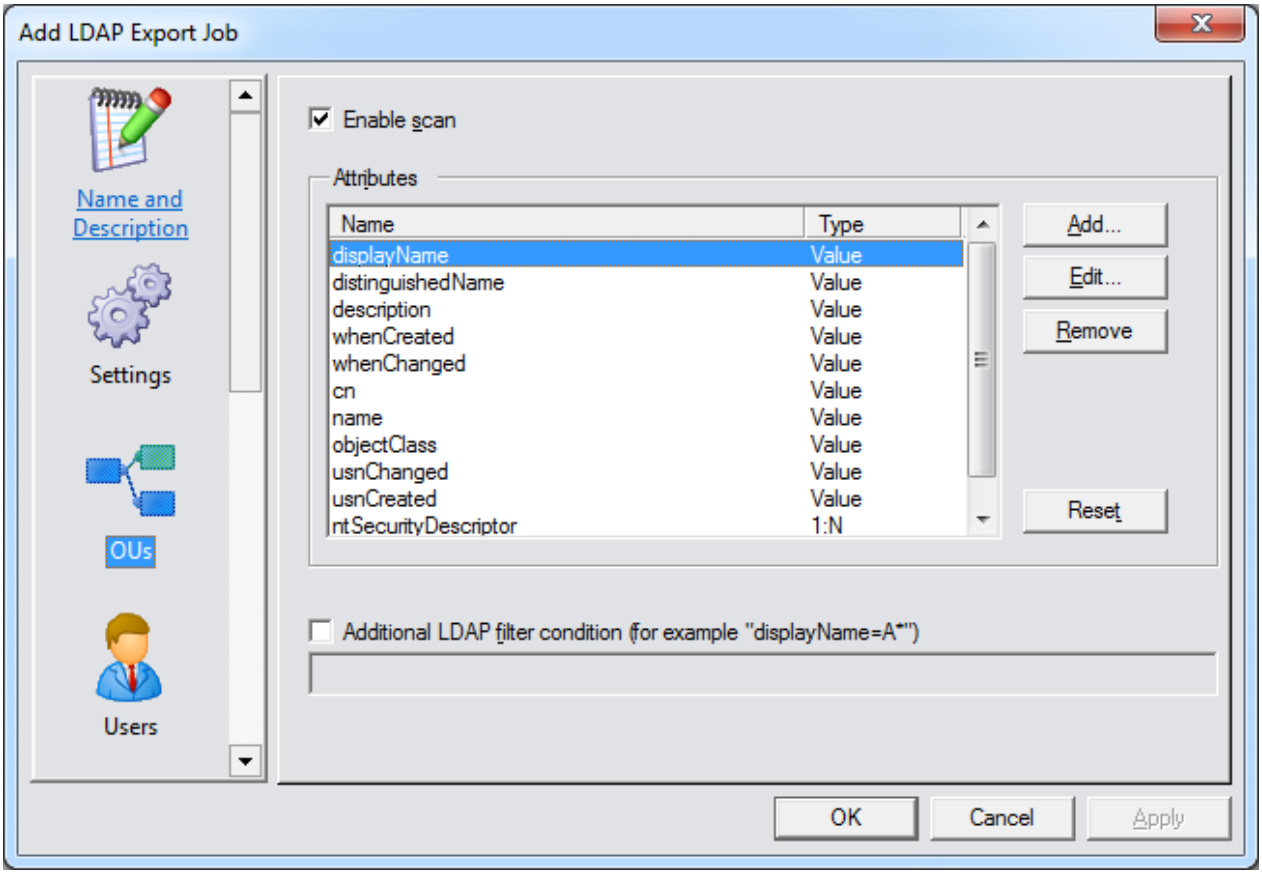
The collected data can be exported either in Microsoft Access MDB format or in text format as a flat file. If exporting in flat file format, you can additionally enable a first row header containing the column names, database “friendly” column names without blanks and automatic replacement of numerical values with clear text values.

If you want to import the data into Microsoft SQL Server, for example to use the predefined Microsoft Reporting Server reports, it is required to select the “Database” format.

If text file output is sufficient for your purposes and/or you don’t want to run a SQL Server you can select “Flat File Export” instead.

The “Compress export database or file” option will compress the produced output before transmission and uncompress it when the “Scan Import” job is run to pull the data to reduce the amount of data transferred.

OUs, Users, Groups, Contacts, Computers and Built-In Accounts



Enable Scan

Use this checkbox to enable/disable scanning the selected types of objects.

Attributes

The attribute list controls which attributes are collected for the corresponding object/class type. You can collect the content as value or in form of a sub table (1:N). The list is prepopulated with the Active Directory default attributes. If you should want to collect additional attributes, for example attributes added with a schema extension you can define them here.

Additional LDAP Filter Condition

If enabled, you can define an additional filter condition for each object type/class in LDAP syntax.

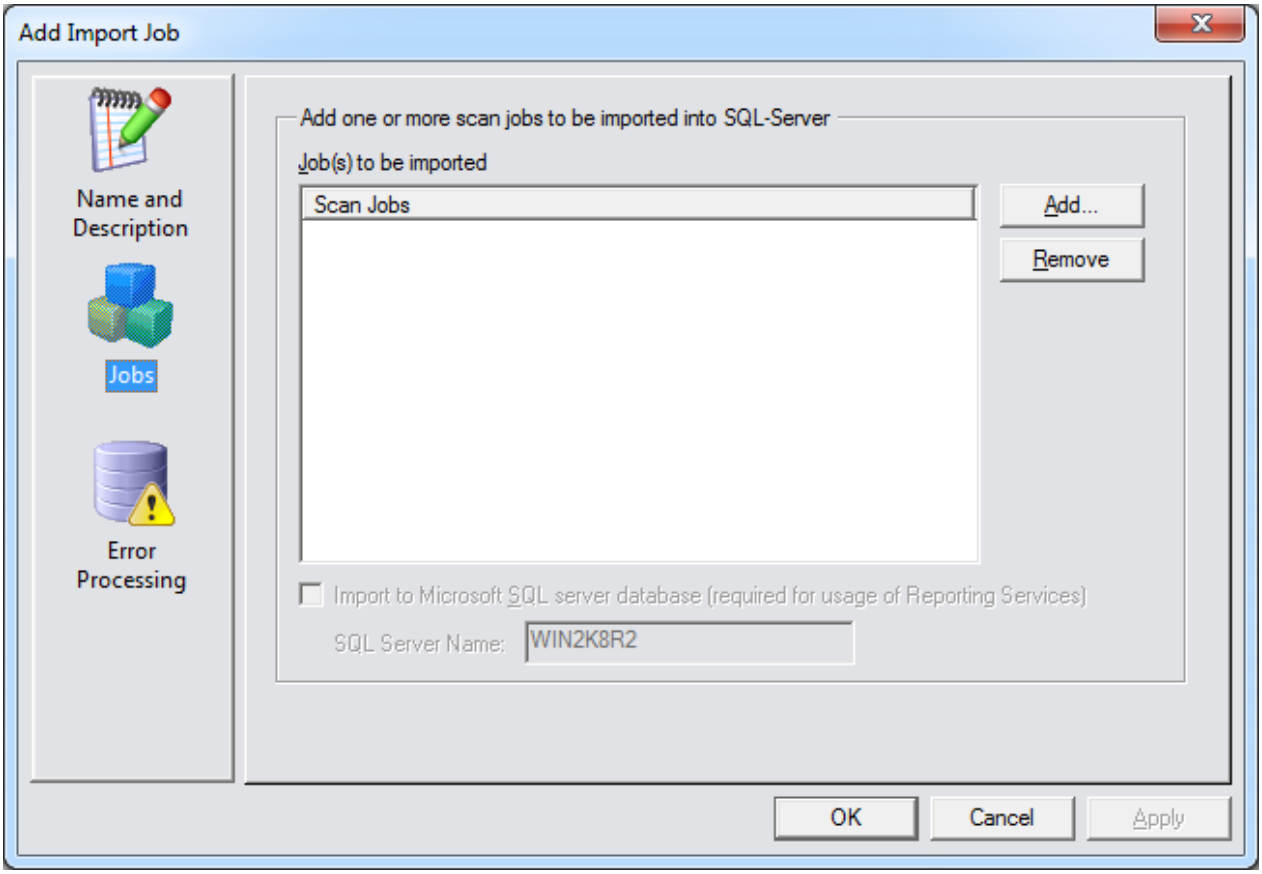
Adding or Editing a Scan Import Job

A “Scan Import” job is used to import the data generated by the “Computer Scan” and “LDAP Scan” jobs, either into the “Data” folder located below the CopyRight2 installation folder or into a SQL Server database.

The import job will create a database and tables on the target SQL server if they should not exist. Once the data is imported and if the server has Reporting Services installed, you can start to use the predefined reports, define your own reports or make ad-hoc queries using the database.

Note: Importing into a SQL-Server database requires that the export format of the scan jobs is set to Microsoft Access MDB.

Jobs



Jobs to be Imported

This list defines, which Computer & LDAP Scan jobs should be imported by running the import job.

Import to Microsoft SQL Server Database

If enabled, you can specify the SQL-Server's name that you want to import the data into. If SQL import is not enabled, the resulting output files (text and MDB format) will get collected and store in the "Data" folder located below the CopyRight2 installation folder.

Using Pre-Defined Reporting Services Reports

After importing the data into SQL-Server and if Reporting Services is installed, you can begin using the pre-defined reporting services reports, automatically deployed to the reporting server, for example:

- Users and memberships
- User home shares and profiles
- Users without logon scripts
- Users with logon scripts
- User contact details
- Users and eMail addresses
- Users not logged on recently
- Recently logged on users
- User last logon time
- Locked out user accounts
- Domain users that never logged on
- Deactivated users
- Users with never expiring passwords
- Users with passwords older than 1 month
- Users password last set
- Users with password expired
- Users with passwords changed within last month
- Users that cannot change passwords

- Groups and members
- Local users and memberships
- Local groups and memberships
- Empty local groups
- Empty domain groups

- Recently changed users
- Recently changed groups
- Recently changed computers

- Organizational units

- Computers
- Computer last logon time
- Deactivated computer accounts

- File and print shares
- File share permissions

- NTFS file and folder permissions
- Volume capacity
- Duplicate files (across network)
- Duplicate files by computer

Additionally, you can use the Microsoft Query builder to build your own custom reports.

Rollout Planning

The rollout planning feature is intended to accelerate large scale file server and storage solution migration scenarios.

The process consists of the following 6 steps:

1. CopyRight2 installation on one central systems, from where the migration is coordinated
2. Agent folder preparation
3. CSV file preparation (for example with Microsoft Excel)
4. CSV file import
5. Deployment
6. Cutover

It automatically deploys CopyRight2 to the defined remote agent, either the source, the target or a 3rd Windows computer in case of migrations between two storage solutions, along with one or more template based migration jobs that get customized automatically to migrate from the corresponding source to the corresponding target system. The Windows computer used, in case of a migration between storage solutions, can run Windows 10 or a Window Server operating system.

During deployment the remote jobs get scheduled with Windows Task Scheduler for automatic execution, according to the roll out plan. The jobs will then automatically execute in the background.

If any errors should occur, they can be tracked and viewed from the central console(s).

Additional instances of CopyRight2 can connect to the central system, to allow multiple persons to track the migration progress, check for errors and perform cut-overs.

The rollout planning feature's list, displays a status column, containing the remote agent's OS version, the CopyRight2 version and the result of the last execution. If the result code is 0, it means that no error(s) occurred. In the "Last Run" and "Next Run" columns you can see the last and the next scheduled execution time.

When the cut-over should be performed, the final copy can be launched remotely from the central console(s) and if successful (0 errors) the corresponding rollout planning job can be deactivated.

You can export the list in CSV format and then delete deactivated systems from time to time, if desired, to keep the list small. It has been successfully tested by customers with up to 370 rollout planning jobs (740 source/destination systems in total).

Note: Please watch the video explaining the rollout planning feature hosted in our YouTube channel to see how this feature works.

CopyRight2 Installation

The rollout planning feature requires an installation of CopyRight2 on a central system, from where the migration is coordinated. Additional installations of CopyRight2 can connect to this central system to check the progress of the migration, view log files, troubleshoot and perform cut-overs.

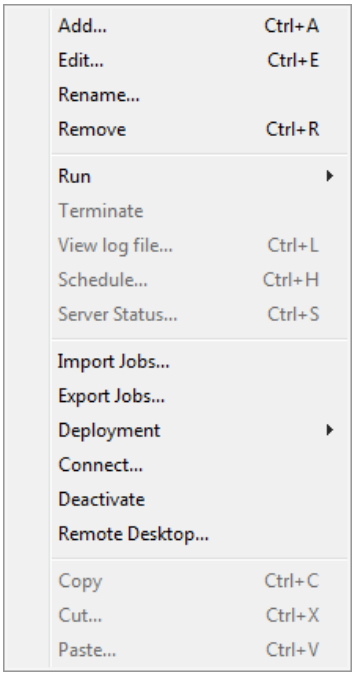
Note: The central installation's CopyRight2 installation folder should be part of a regular backup, to ensure the data can be recovered in case of a system failure or catastrophic event!

Agent Folder Preparation

Before deployment, the corresponding version of CopyRight2's MSI installer files have to be copied into the corresponding platform folder below the "Agents" subfolder of the CopyRight2 installation folder. This applies to the main program and any additional add-ons such as the password migration add-on. During deployment the MSI file will get automatically installed onto the target.

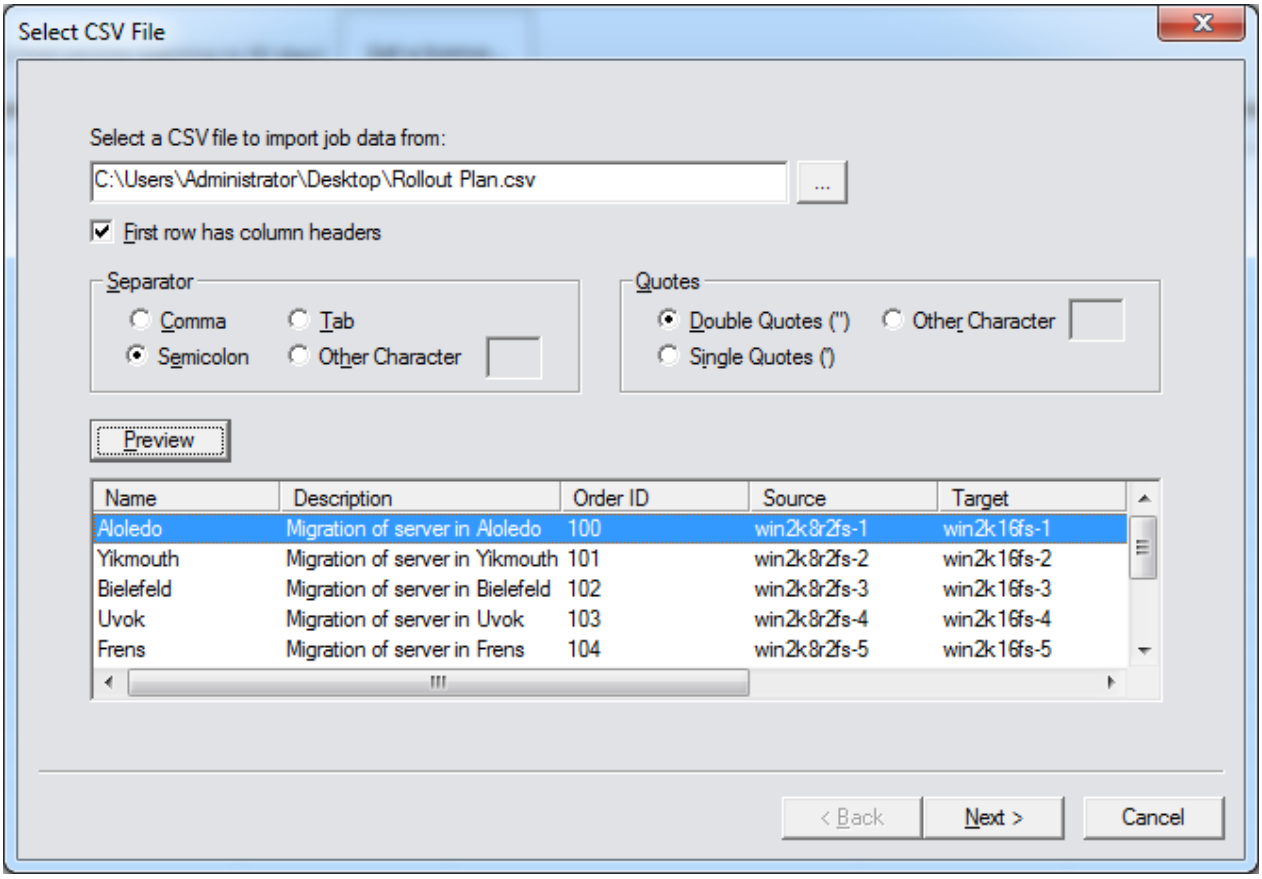
CSV Import Wizard

The CSV import wizard is intended to import a previously prepared roll-out plan, You can open up the CSV import wizard, by opening up the context menu and then selecting the "Import Jobs…" command:



Select CSV File

In the first page, you can select the path of the previously prepared CSV file, whether the first row contains column names, to define the column separator being used and the character to quote data in case it contains the separator character.



First Row Has Column Headers

If checked, the first row of the specified CSV file should contain the column names, later assigned to the corresponding import fields the rollout feature expects.

Separator

This field defines the character used to separate columns, either a comma, tab, semicolon or other character.

Quotes

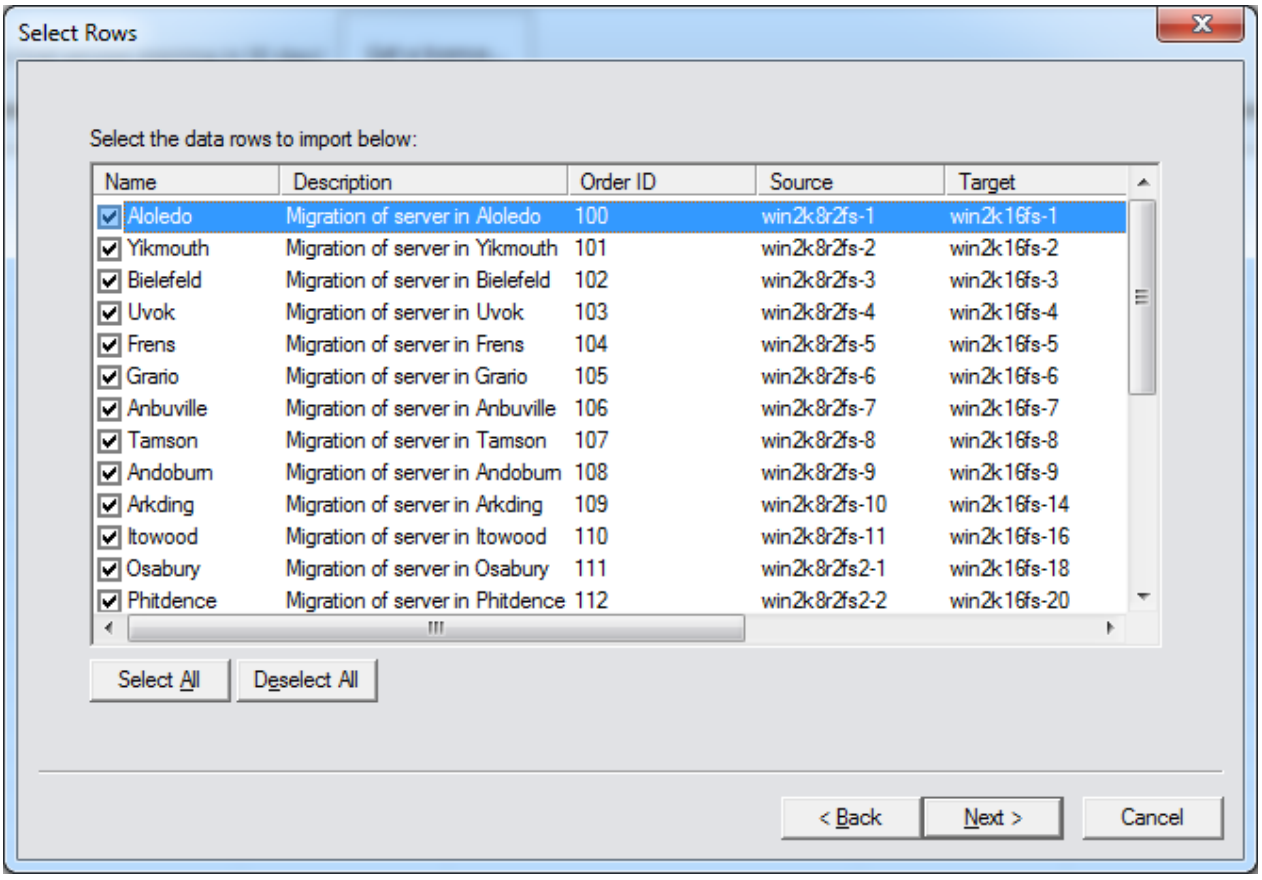
This field defines the quote character used for values containing the defined separator character.

Preview

Use the preview button, to check if the specified CSV file is parsed correctly, by displaying the first ten rows. After clicking on “Preview” you should see the data split into the corresponding columns.

Select Rows

The “Select Rows” page allows to define which rows from the CSV should get imported. By default, all rows are selected.



Select All

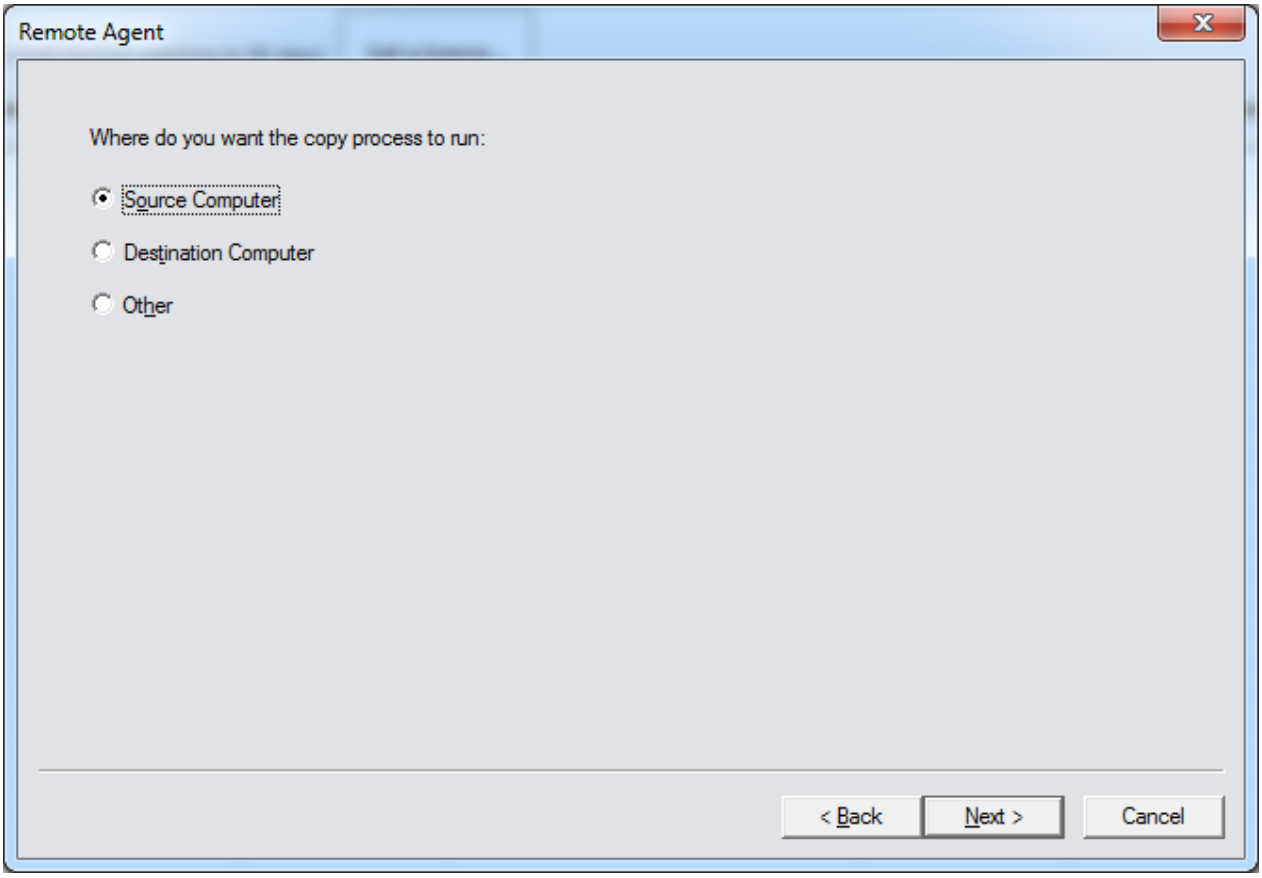
Clicking on the “Select All” button selects all the rows from the CSV file.

Deselect All

Clicking on the “Deselect All” button unselects all CSV file rows.

Remote Agent

The “Remote Agent” pages defines where execution of copy jobs should take place.



Source Computer

If this option is selected, the copy job will run on the source computer and push the data to the destination computer.

Destination Computer

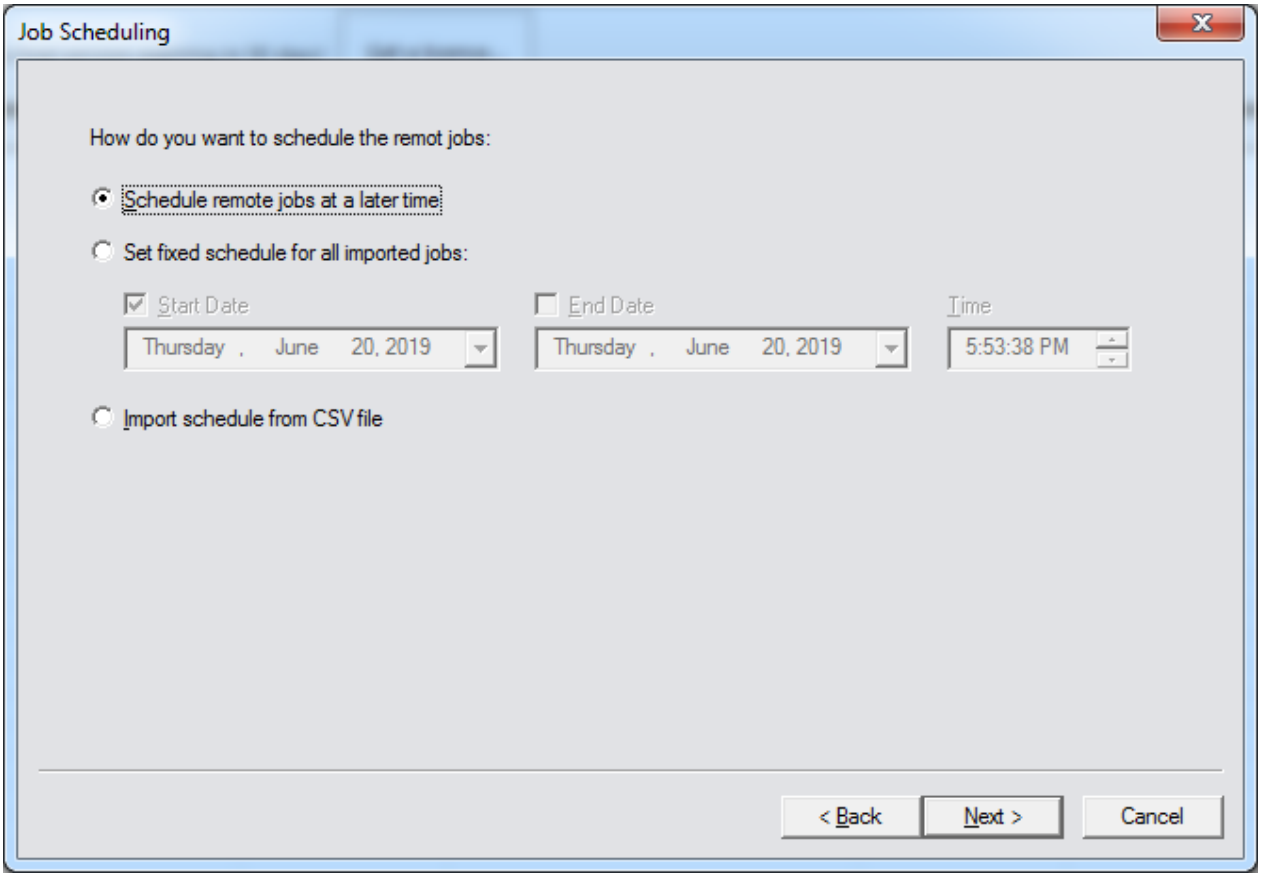
If this option is selected, the copy job will run the destination computer and pull the data from the source computer.

Other

If this option is selected, the copy job will run on a 3rd Windows computer instead. This option should be used only if both, source and destination are NAS storage solutions.

Job Scheduling

The “Job Scheduling” page defines the time a job should run.



Schedule Remote Jobs at a Later Time

If this option is selected, the copy jobs will not get scheduled. You could schedule the jobs manually at a later time by editing each imported “Rollout Planning” job.

Set Fixed Schedule for all Imported jobs

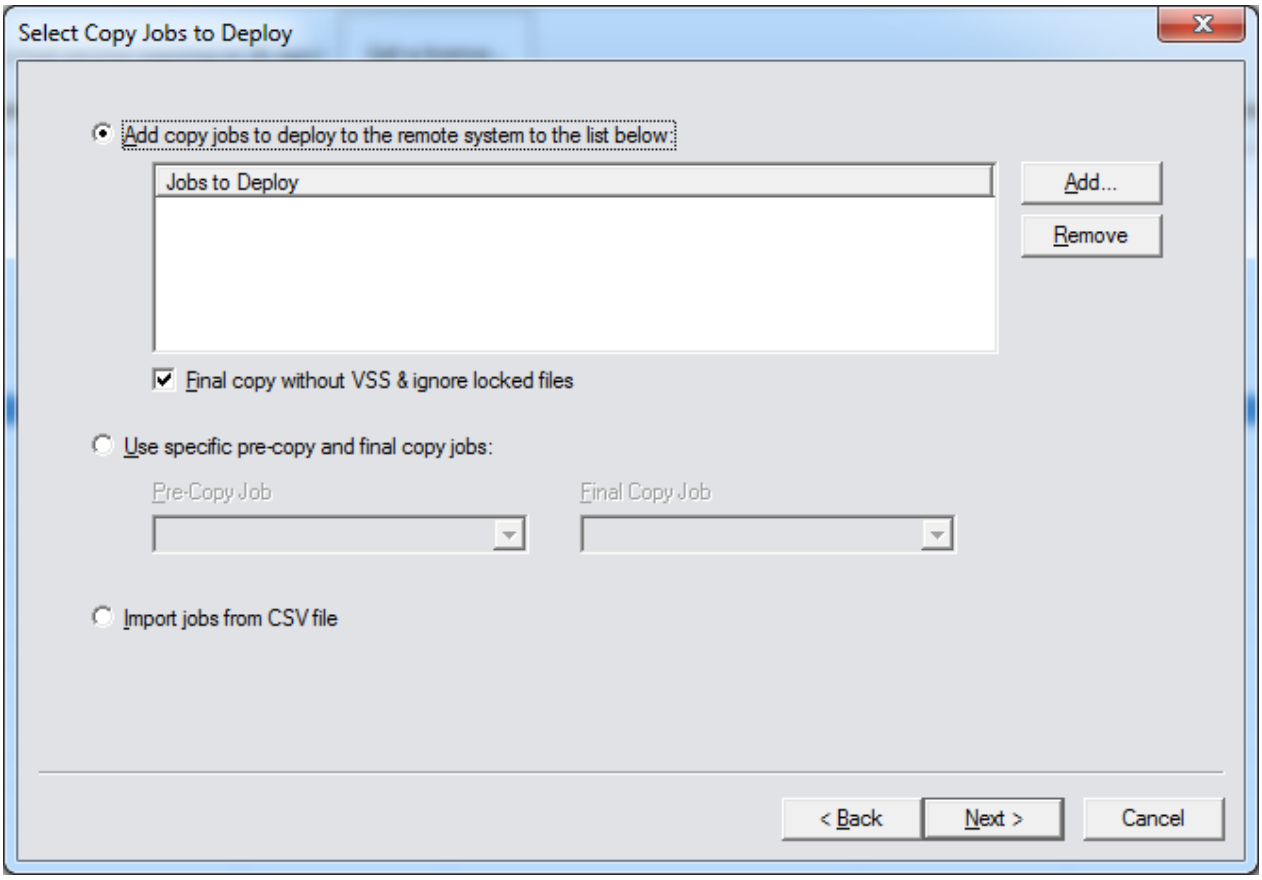
This option allows the definition of a fixed schedule for all imported jobs. This is useful if all data migration jobs should use the same schedule.

Import Schedule from CSV File

This option allows the definition of an individual schedule for each imported “Rollout Migration” job, using a “Start Date”, “End Date” and “Time” column in the CSV file.

Select Copy Job to Deploy

In the wizard's "Select Copy Jobs to Deploy" page you can select previously defined copy jobs used as templates. During deployment to the selected remote agent, they will get updated with the corresponding source and destination



Add Copy Jobs to Deploy to the Remote System to the List Below

Here you can define one or more previously defined CopyRight2 jobs to deploy to the corresponding remote agent.

Final Copy Without VSS & Ignore Locked Files

If enabled, the context menu's "Run" command will turn into a sub-menu containing a "Pre-Copy…" and a "Final Copy…". The final copy will then ignore and run without the "Volume Shadow Copy" and "Ignore errors resulting from locked files" options.

Use Specific Pre-copy and Final Copy Jobs

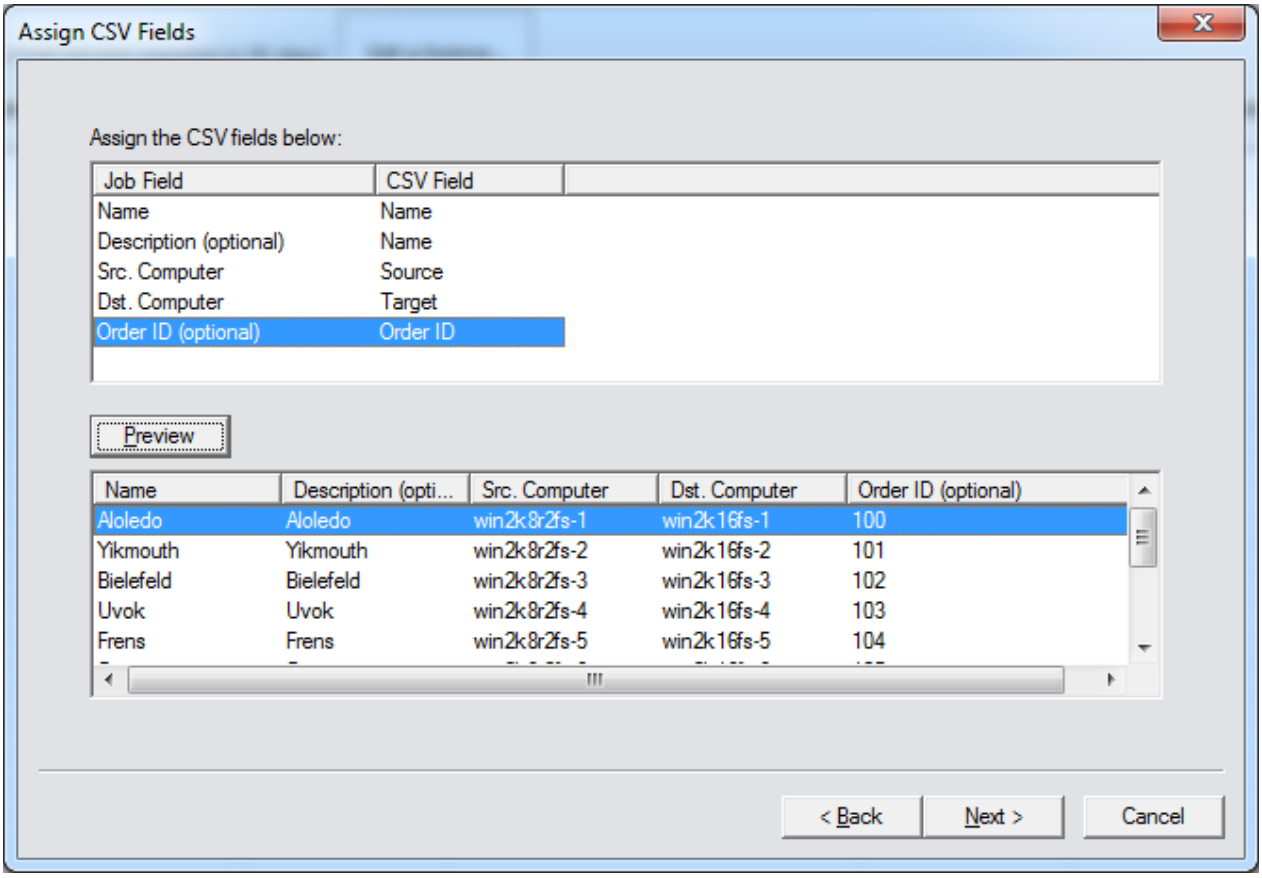
This option is useful in case you want to define two templates, one for the pre- and one for the final copy, that differ beyond just the "Volume Shadow Copy" and "Ignore errors resulting from locked files" options.

Import Jobs From CSV File

If using this option, you can define the templates used as a field in the CSV file using a semicolon as delimiter, unless the CSV file is itself delimited by semicolon, in which case the templates are specified comma delimited.

Assign CSV Fields

In the “Assign CSV Fields” you can assign the fields from the CSV file to the fields required by the import process.



Assign the CSV Fields Below

To assign the fields, double click onto the field in the CSV field column to display a combo box containing the fields from the CSV file, either by name or by ordinal number.

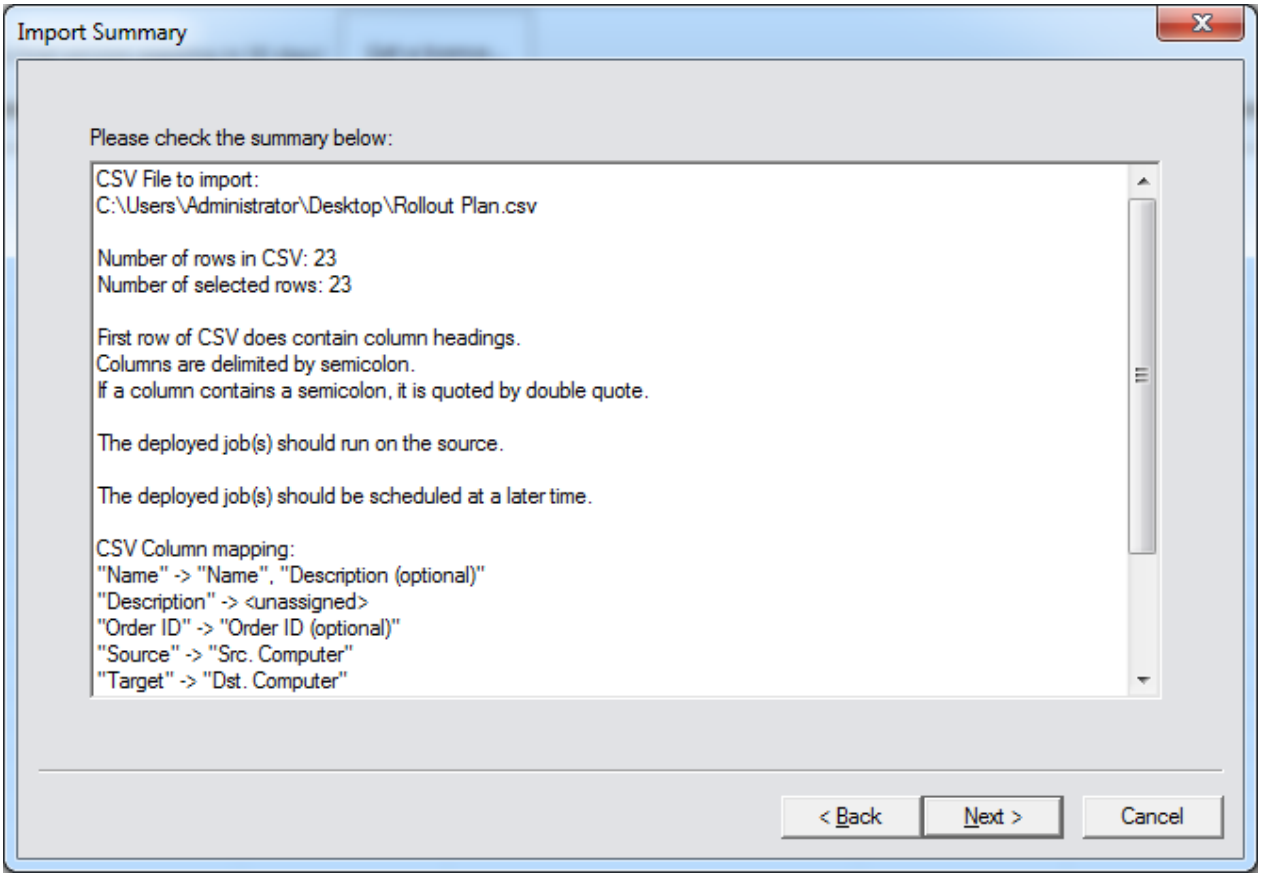
Optional job fields have the suffix “(optionall)” any other fields are mandatory.

Preview

Press the “Preview” button to populate the table below the button with the data from the CSV file’s first 10 rows to see if the column assignment is correct.

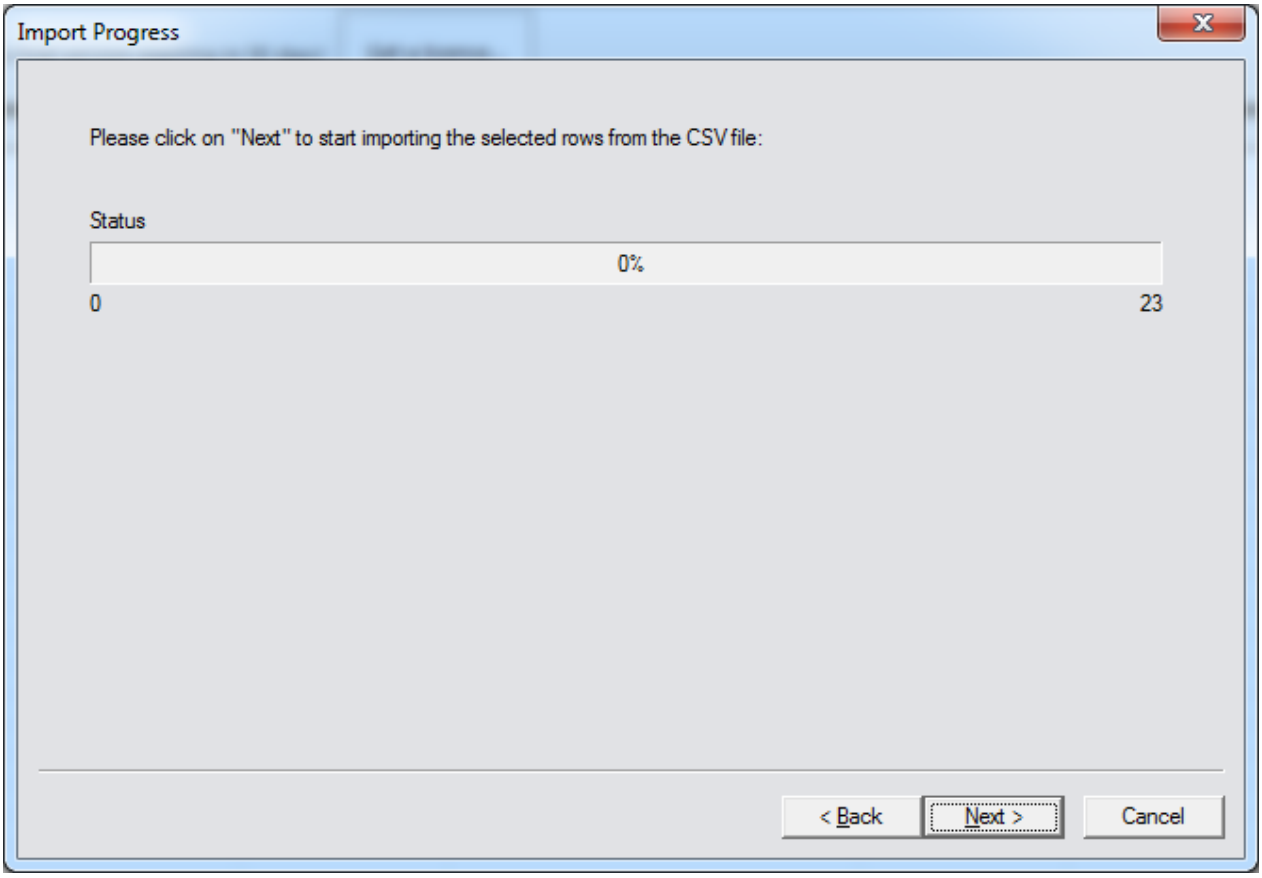
Import Summary

The import summary page lists all the previously made settings, before the import actually takes place.



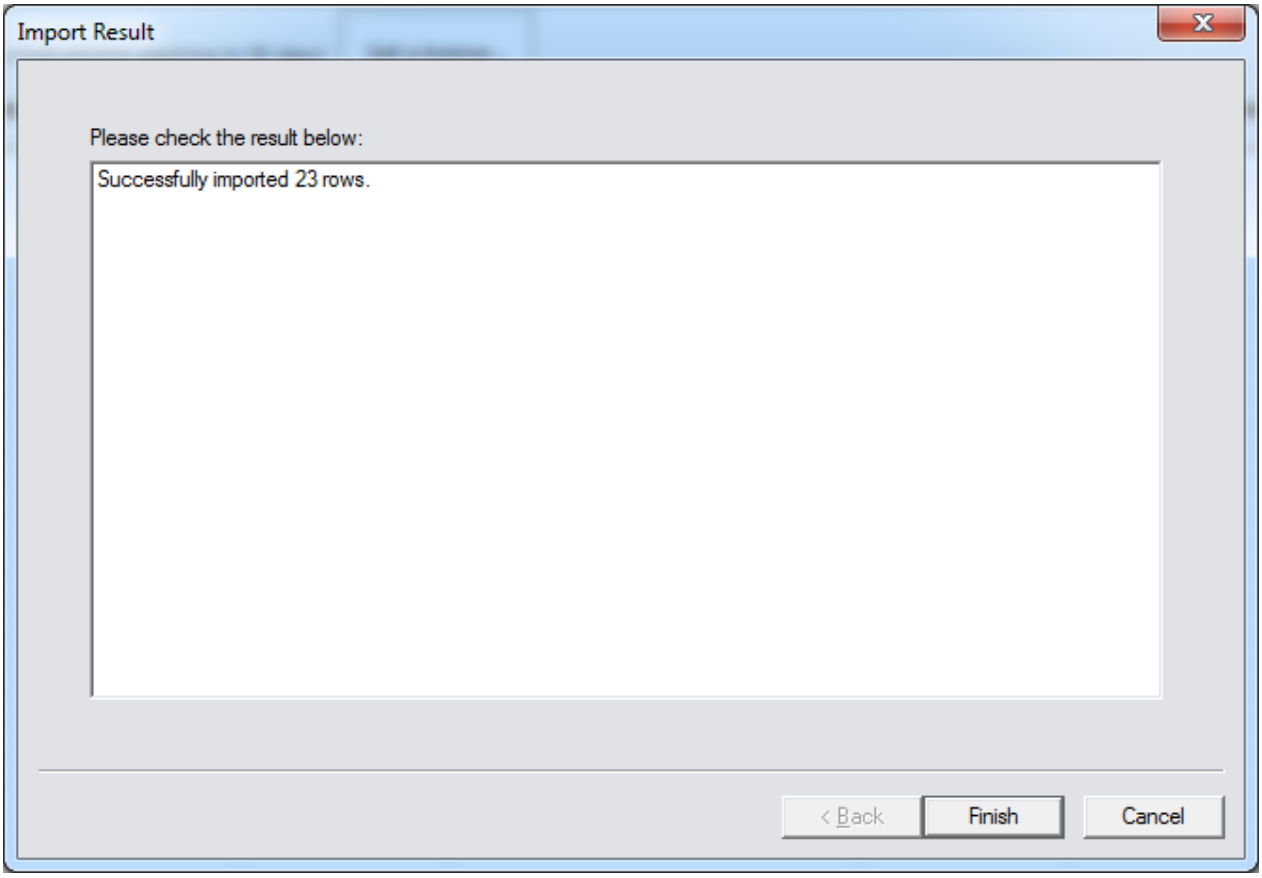
Import Progress

The import progress page displays the import progress. After clicking on “Next” the import begins.



Import Result

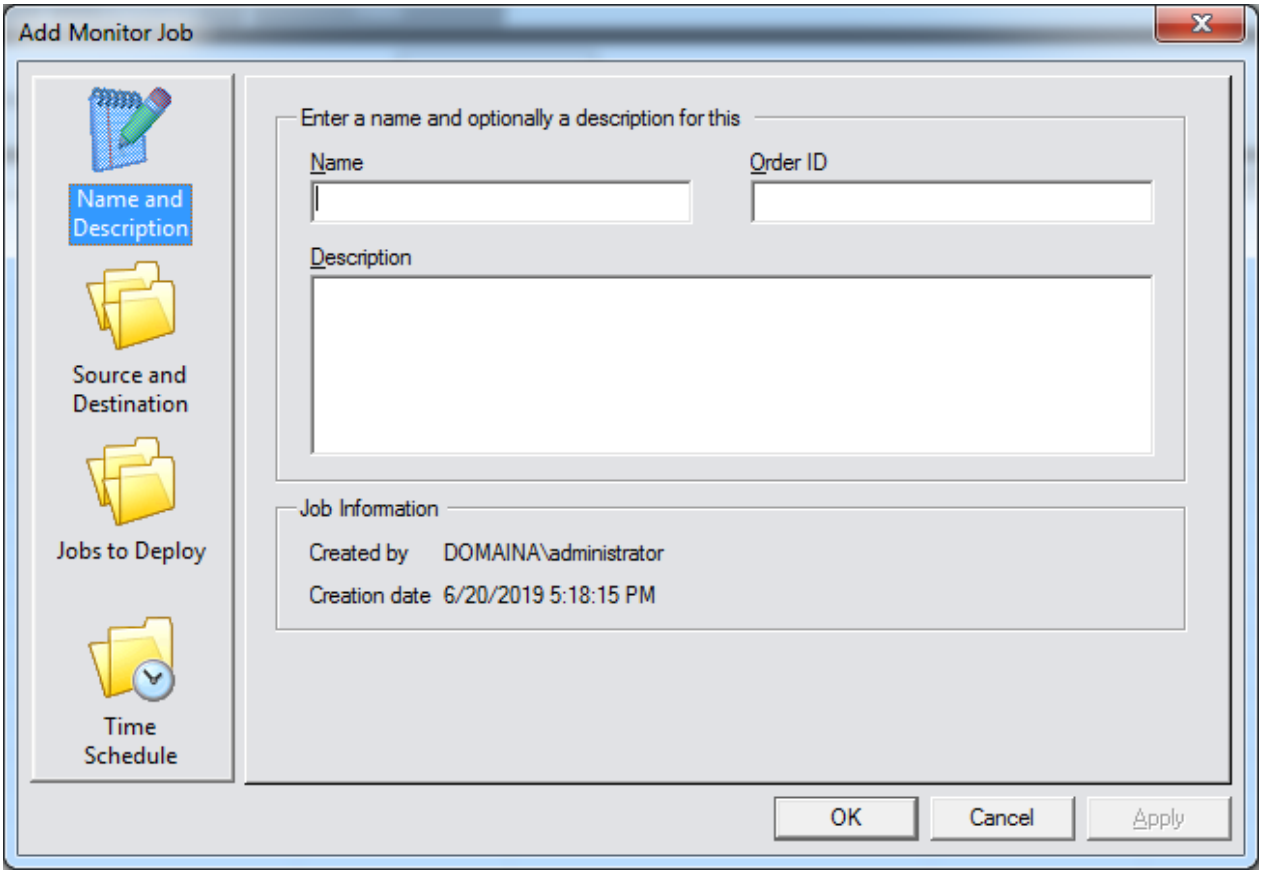
The import result page displays the result of the import and how many jobs were imported.



Adding or Editing a Rollout Planning Job

You can add or edit a rollout planning job just like any other CopyRight2 job, even though they are usually imported using the import wizard. However, you can use the edit command to make changes to the job's settings.

Name and Description



Name

Like with the other job types, this field contains a name for the job.

Order ID

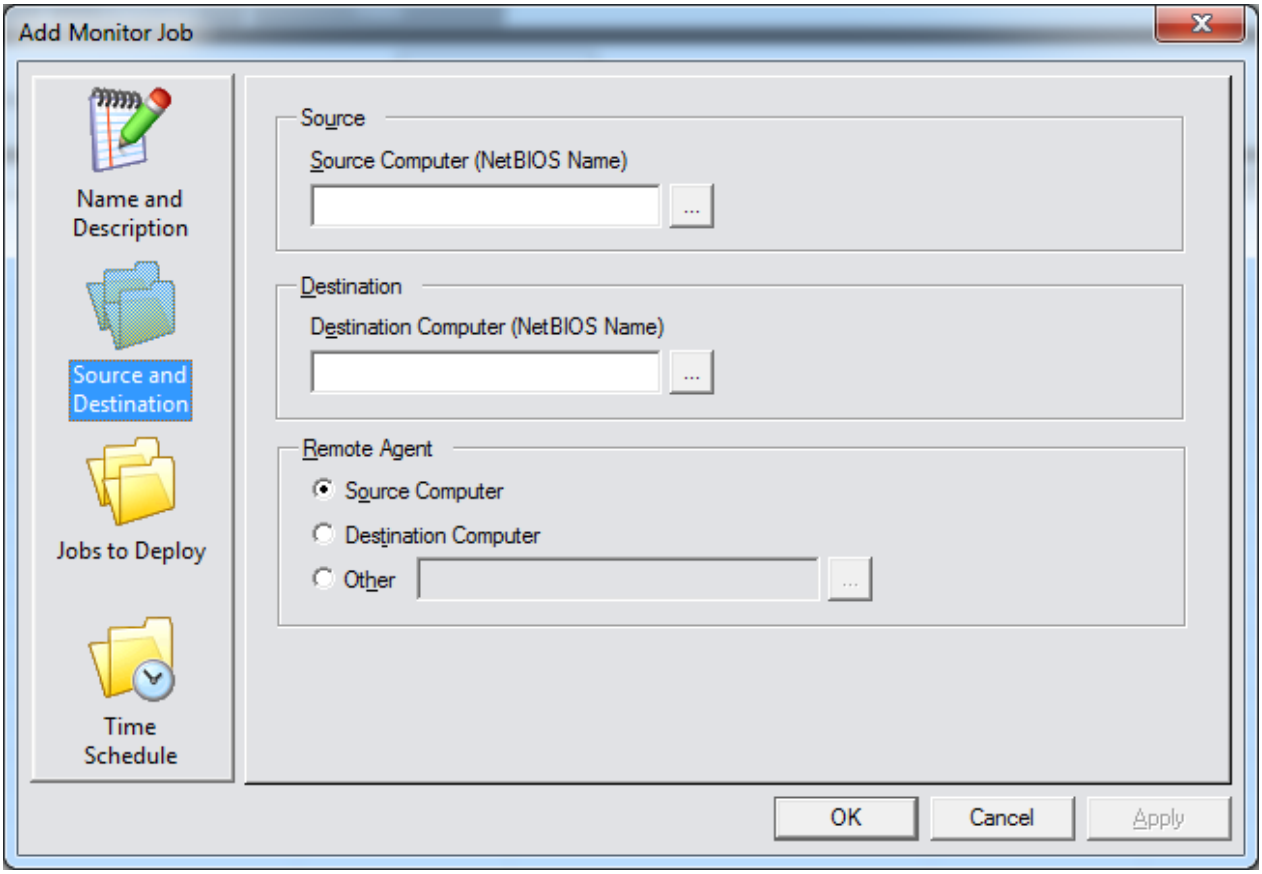
This field contains an optional order ID assigned to this planned migration. This number could originate, for example, from an external system that is used to track migrations.

Description

Like with the other job types, this field contains an optional description.

Source and Destination

This page defines the source, the destination and the location where the copy job gets executed.



Source Computer (NetBIOS Name)

This field specifies the name of the source server or NAS system.

Destination Computer (NetBIOS Name)

This field specifies the name of the target server or NAS system.

Remote Agent

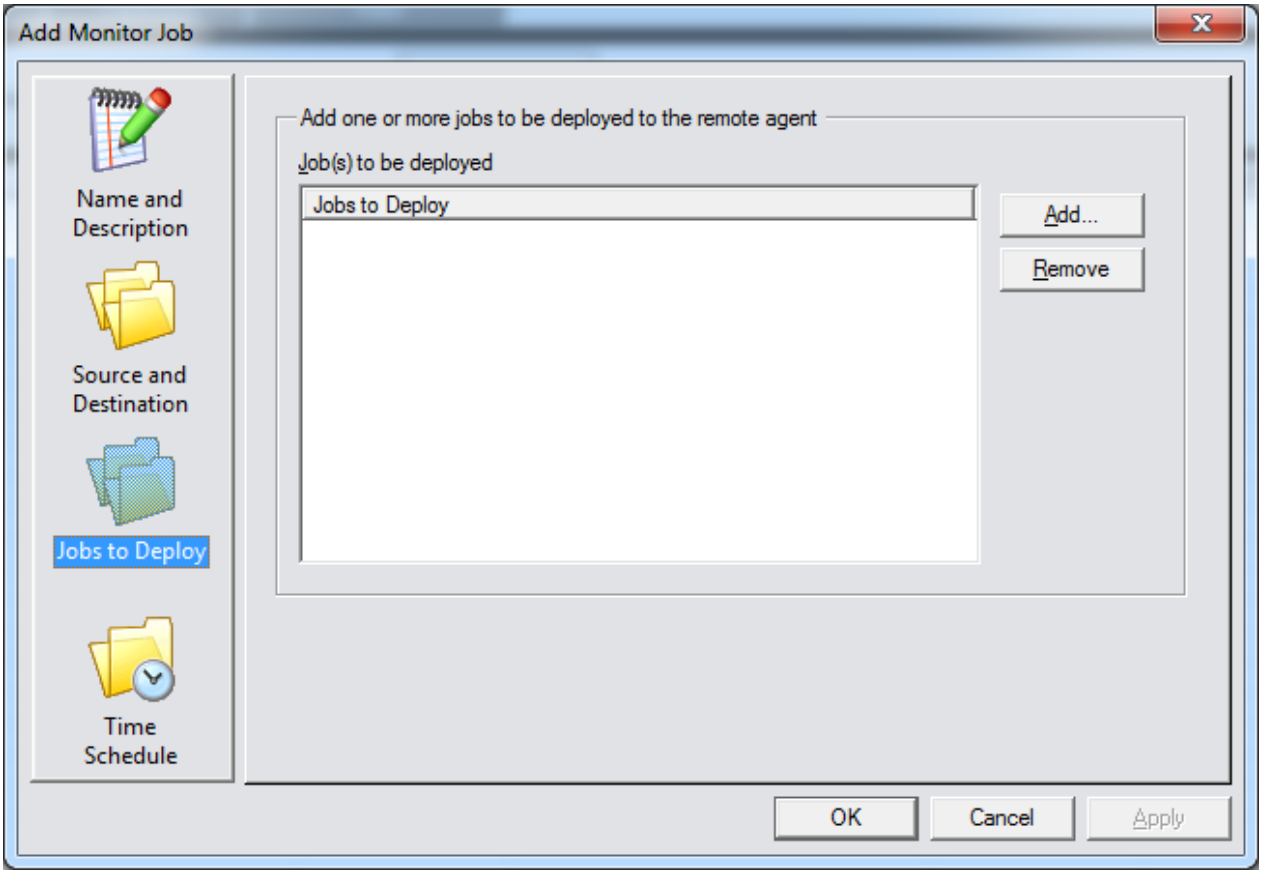
This field specifies where the copy job should get executed. This could be the source, the destination or a 3rd Windows computer in case you want to migrate between two NAS systems.

Domain Controller

If the “Display Domain Controllers” option is enabled in advanced options (see chapter “Advanced Options”), you will also see a domain controller field for source and target, where you can define a domain controller to use for account lookups for that specific rollout planning job. This is useful if the “Active Directory Sites & Services” are not properly defining the network structure to prevent lookups from being performed across slow WAN links for example.

Jobs to Deploy

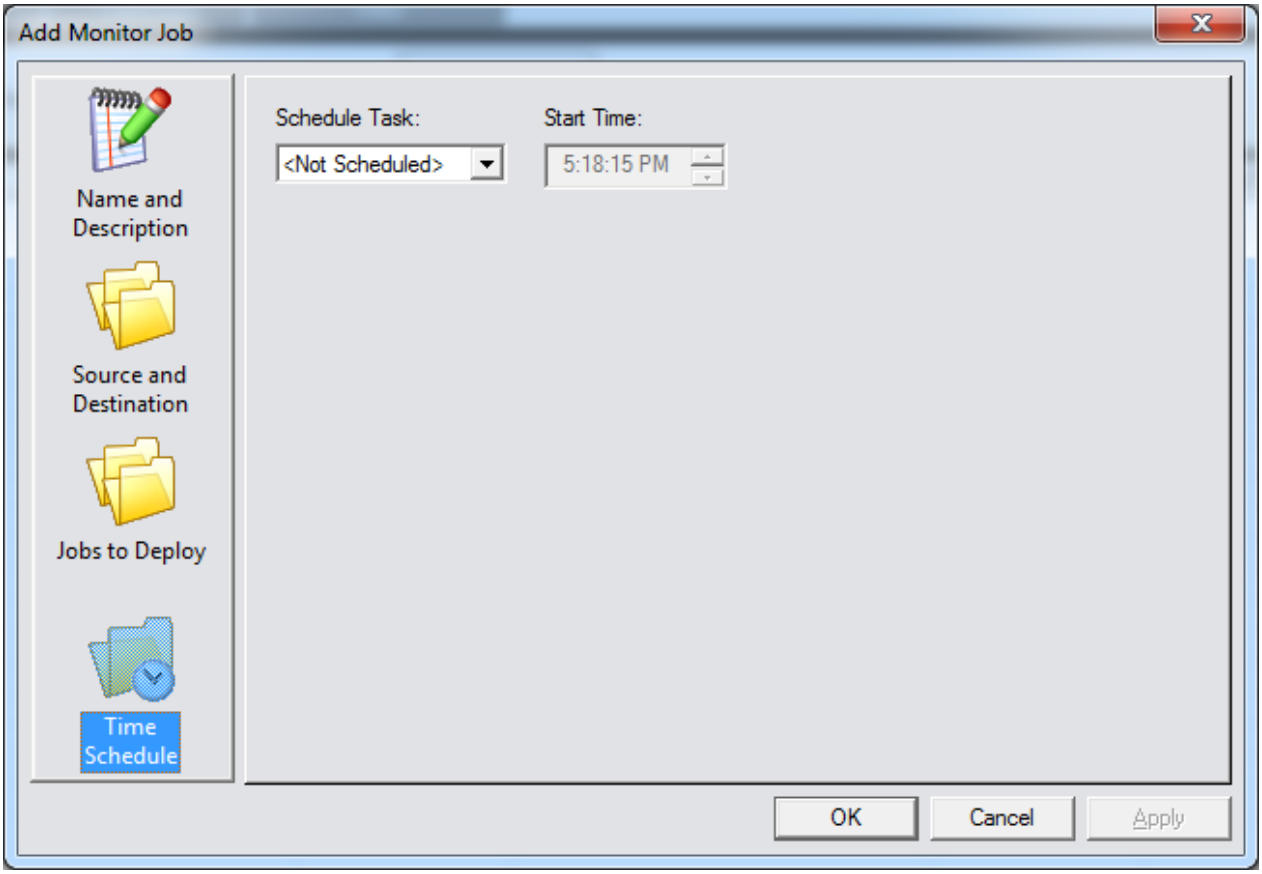
This page defines the copy job templates to deploy to the target. This can be a single job or multiple jobs, for example if you want to use a different configuration for the pre- and the final-copy.



Add / Remove Buttons

You can use the “Add…” and the “Remove” buttons to add or remove a previously defined template copy job.

Time Schedule



Schedule Task

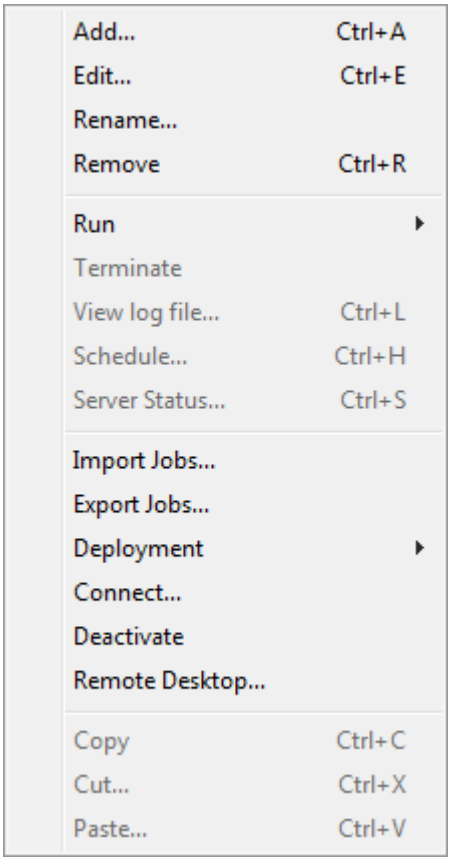
Here you can define an interval (daily or once) to define if this job should get executed only once or daily.

Start Time

This field defines the time for the execution of this copy job.

Export Data to CSV File

You can export the job data at any time using the “Export Jobs…” command from the context menu.



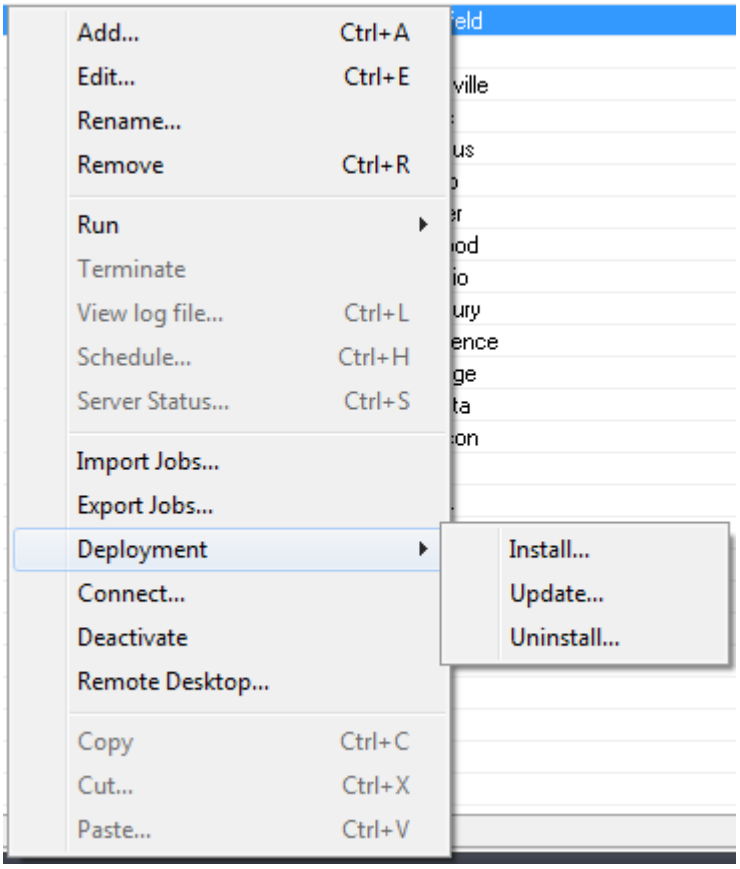
Next select a target file name and folder to export the data to.

Deployment

The context menu's "Deployment" menu contains a command to "Install…", "Update…" and "Uninstall…" CopyRight2 from the remote system(s) selected. You can select multiple rows if you want to run the same command on multiple systems. The target will be the computer set as remote agent, so either the source, the destination or a 3rd Windows computer, in case of a migration between two storage solutions.

During the deployment, the CopyRight2 software (and additional add-ons) will get install on the corresponding target system, along with the copy jobs defined as template in the rollout planning job. If a schedule is defined, it will also schedule the jobs according to the rollout planning job's settings.

Note: If you want to uninstall CopyRight2 from the target system(s) and you have copied a newer version into the Agent\X64 or Agent\X86 folder, please update the target system to that version first and then perform the uninstall.



Connecting to Remote Server

The "Connect…" context menu command will open up an additional CopyRight2 window, connected to the remote agent of the selected rollout planning job.

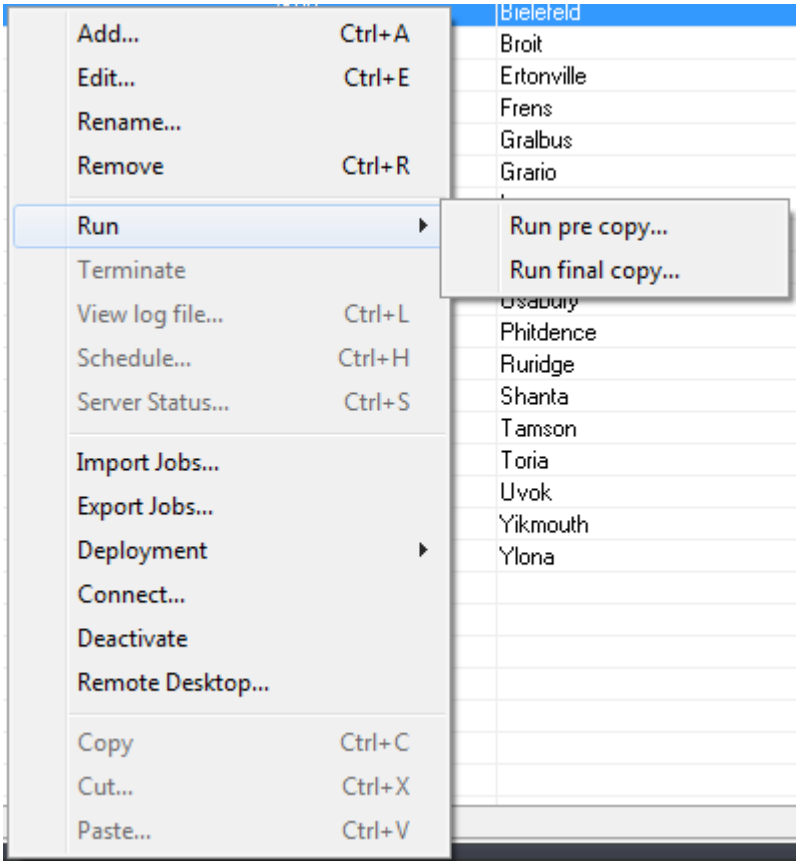
The “Remote Desktop…” context menu command will open up an RDP connection to the remote agent defined in the rollout planning job.

Run a Job

If the rollout planning job was imported having “Final Copy Without VSS & Ignore Locked Files” checked (default setting) or if there were two templates specified for pre- and final copy, the context menu will contain a “Run” menu having two commands, one for pre- and one for final copy.

If the rollout planning job was imported without having “Final Copy Without VSS & Ignore Locked Files” checked there will be a “Run…” command directly in the context menu instead.

After clicking on either menu commands, CopyRight2 will ask for confirmation and if confirmed, run the corresponding job on the remote agent.



Deactivate a Job

You can use the “Deactivate” command to deactivate a copy job. It will disable the job on the remote agent and then display a stop sign as icon for the corresponding job, once the job was successfully deactivated.

This command is usually used, after the cut-over of a migrated server, to prevent running the job again, after the cut-over, potentially overwriting data on the target with older versions of files and deleting files that were created after the cut-over.

Reactivate a Job

You can use the “Reactivate” command to enable a previously deactivated job again.

Add-Ons

In this chapter you can find documentation for the CopyRight2 Add-Ons. You can find the add-ons on the CopyRight2 download page. Please install the corresponding platform version of the add-ons, if you have installed the 64-bit version of CopyRight2, please install the 64-bit version of the add-ons and if you have installed the 32-bit version of CopyRight2, please install the 32-bit version of the add-ons.

Note: We have begun restructuring the documentation and the add-ons will get their own separate documentation instead.

Password Migration Add-On

Detailed information about password synchronization and migration is no longer included in this manual.

Please refer to the Password Synchronization & Migration Add-On Administrator Guide, which provides comprehensive installation instructions, prerequisites, configuration details, advanced scenarios, and troubleshooting information: https://www.sys-manage.com/Portals/0/downloadableItems/Password%20Migration%20Add-on.pdf

IIS FTP/HTTP Migration Add-On

The IIS FTP/HTTP Migration add-on will add two additional pages to “Data Migration” jobs where you can configure the migration of FTP and HTTP site settings of folders hosting FTP and HTTP sites. Additionally, it will add a new job type called “IIS Site Migration” that can be used to migrate the site configuration solely without migrating files and folders. This is useful for sites being hosted on 3rd computers or storage systems.

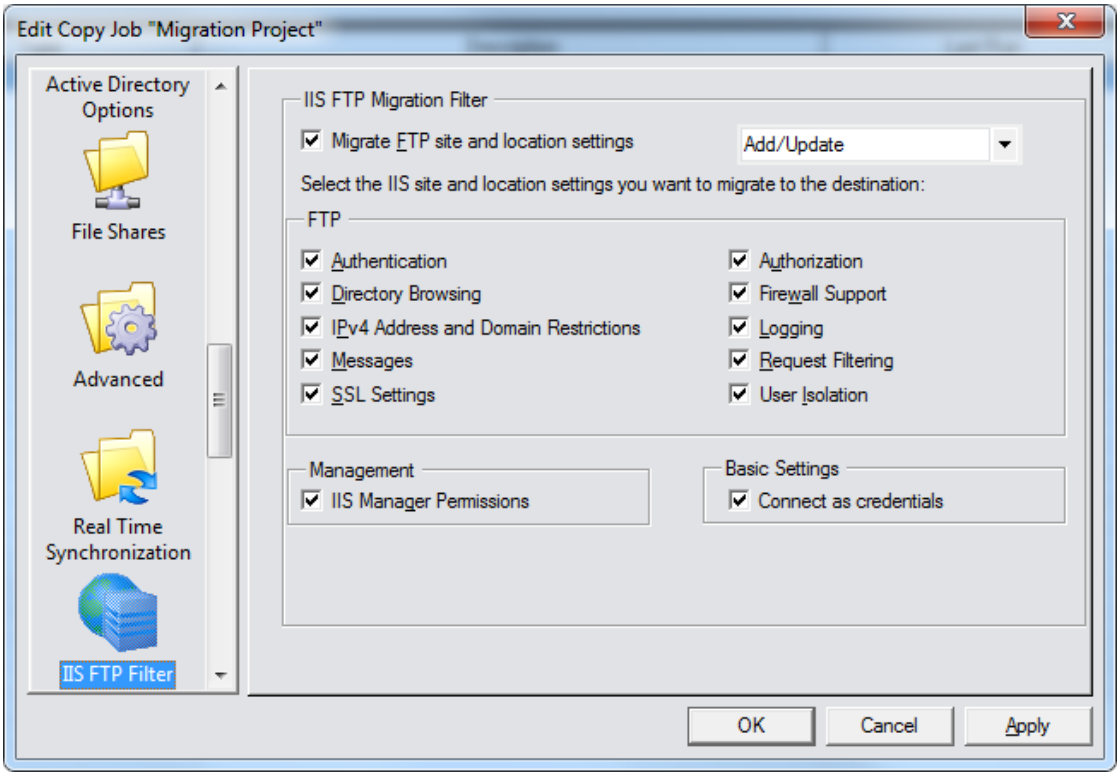
The add-on supports IIS version 6.0 (Windows 2003) up to IIS version 10.0 – Build 1809 (Windows 2019) as a source and IIS version 7.5 up to 10.0 – Build 1809 (Windows 2019) as a target computer.

Migrate IIS FTP/HTTP Site Configuration During Data Migration

After installation of the add-on, you will find two additional pages in your data migration jobs, one for FTP sites and a second one for HTTP sites.

IIS FTP Filter

In the “IIS FTP Filter” page, you can control if and how any FTP site located at or below the specified source path(s) of your data migration job is migrated.



Migrate FTP and Site Location Settings

The “Migrate FTP site and location settings” option enables/disables the migration of FTP sites located at or below the specified source path(s) of your data migration job. You can select a disposition of “Add only” to migrate settings if the site does not yet exist on the target, or “Add/Update” in case you want the copy job to update existing sites, for example if you run the same data migration job again at a later time.

FTP

In the “FTP” box you can select the FTP settings you want to migrate from source to target. In an option is not checked, the settings will be inherited from the default settings of the target.

Management

In the “Management” box you can select whether you want to migrate “IIS Manager Permissions” or not.

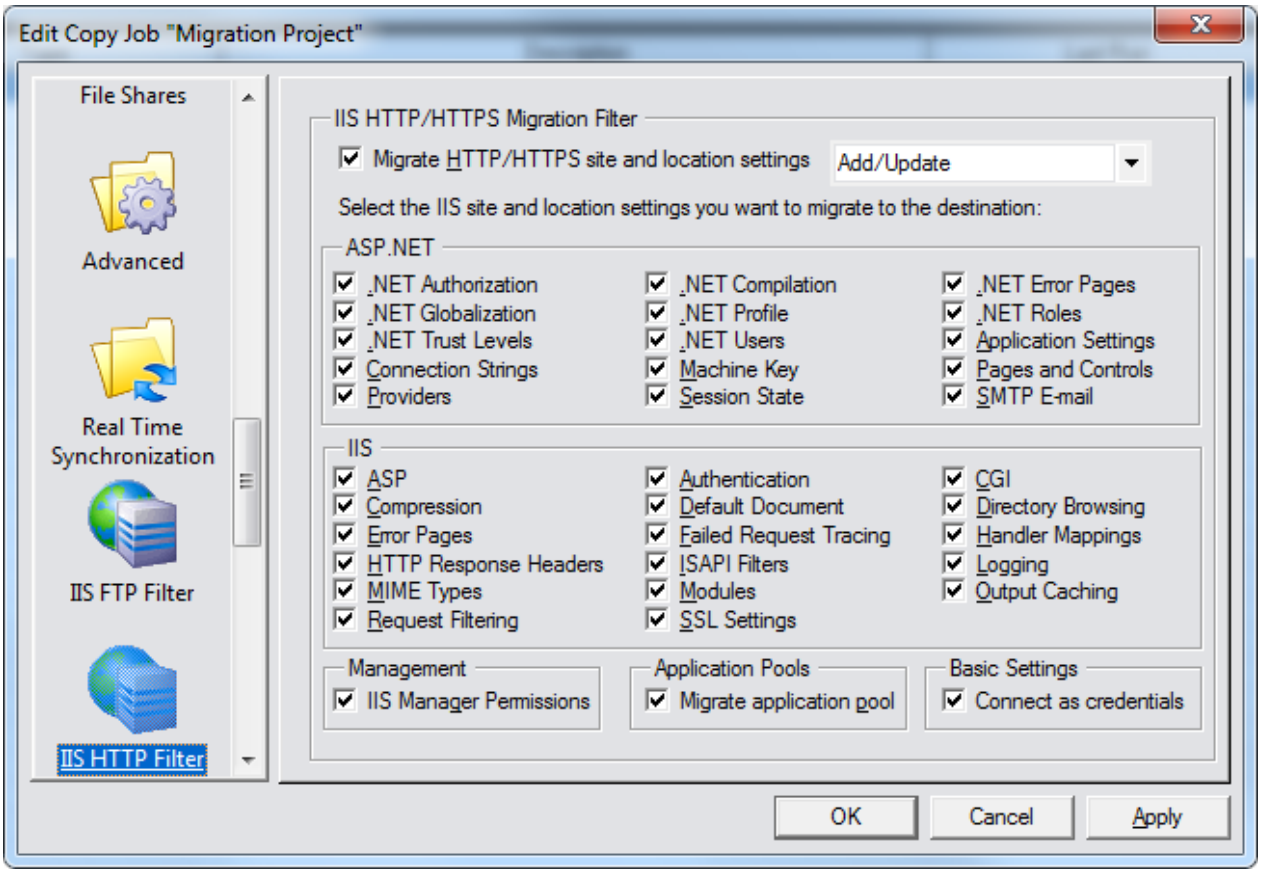
Basic Settings

In the “Basic Settings” box you can select whether you want to migrate “Connect as credentials” for sites and virtual directories or not. Please ensure that the firewall rules allow accessing DCOM on the remote system in order to migrate the encrypted “Connect as” credentials. Please check the chapter “Firewall Configuration” for more details

on the required TCP ports that have to be opened on the remote system, for the system that is running the migration job.

IIS HTTP

In the “IIS FTP Filter” page, you can control if and how any HTTP site located at or below the specified source path(s) of your data migration job is migrated.



Migrate HTTP/HTTPS Site and Location Settings

The “Migrate HTTP/HTTPS site and location settings” option enables/disables the migration of web sites located at or below the specified source path(s) of your data migration job. You can select a disposition of “Add only” to migrate settings if the site does not yet exist on the target, or “Add/Update” in case you want the copy job to update existing sites, for example if you run the same data migration job again at a later time.

ASP.NET

In the “ASP.NET” box you can control the migration of ASP.NET settings define in IIS Manager, for your data migration job.

IIS

In the “IIS” box you can control the migration of IIS settings defined in the IIS Manager.

Management

In the “Management” box you can select whether you want to migrate “IIS Manager Permissions” or not.

Application Pools

The “Migrate application pool” option, controls whether you want to migrate application pools associated with the migrated web site(s).

Basic Settings

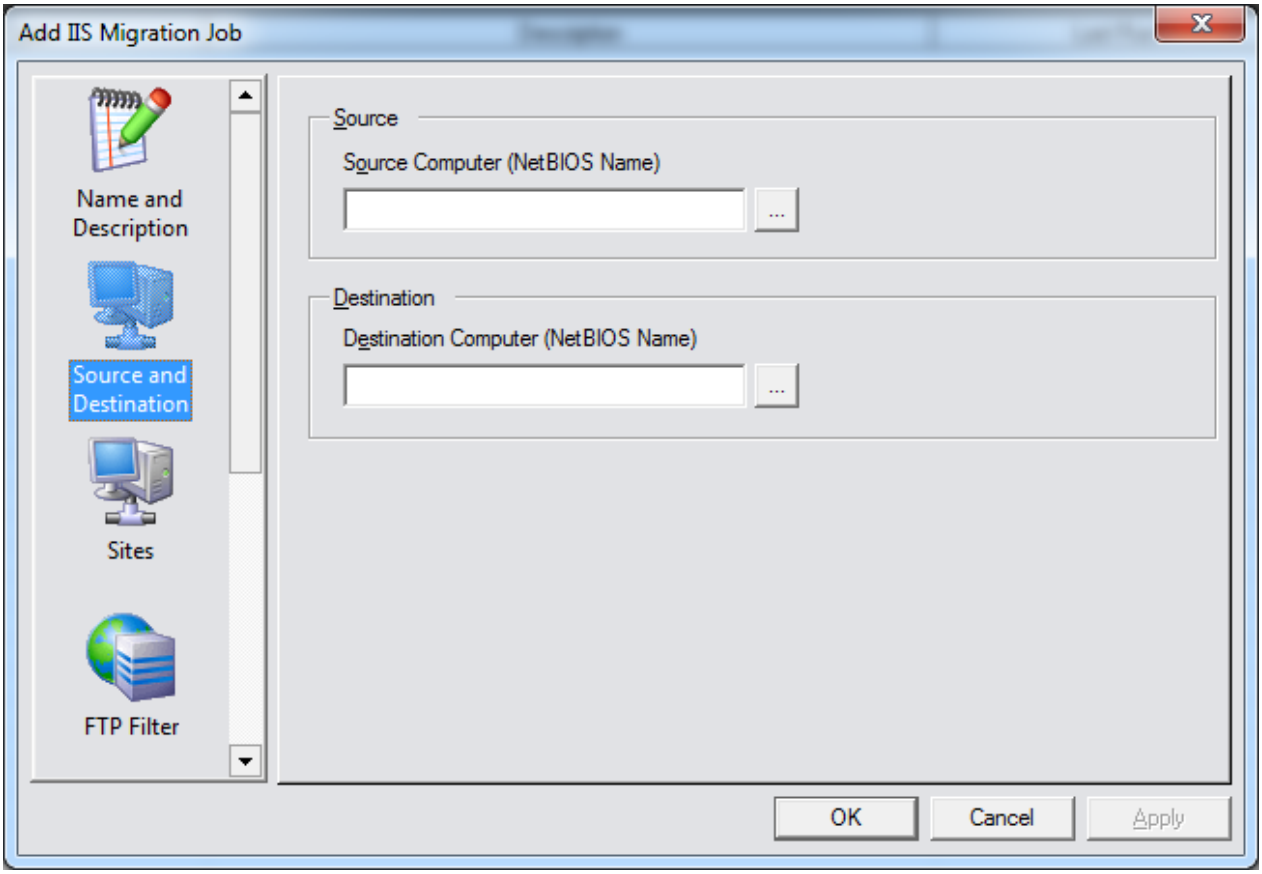
In the “Basic Settings” box you can select whether you want to migrate “Connect as credentials” for sites and virtual directories or not. Please ensure that the firewall rules allow accessing DCOM on the remote system in order to migrate the encrypted “Connect as” credentials. Please check the chapter “Firewall Configuration” for more details on the required TCP ports that have to be opened on the remote system, for the system that is running the migration job.

Migrate IIS FTP/HTTP Site Configuration Without Data Migration

After installation of the add-on, you will a new job type called “IIS Site Migration”, that can be used to migrate IIS site configurations without copying data. This type of job is to be used for sites not being hosted locally on the IIS server, where the data is located on a 3rd system (Windows or Storage Solution). CopyRight2 will migrate the site settings defined at the root level and also additional settings defined for locations below the root.

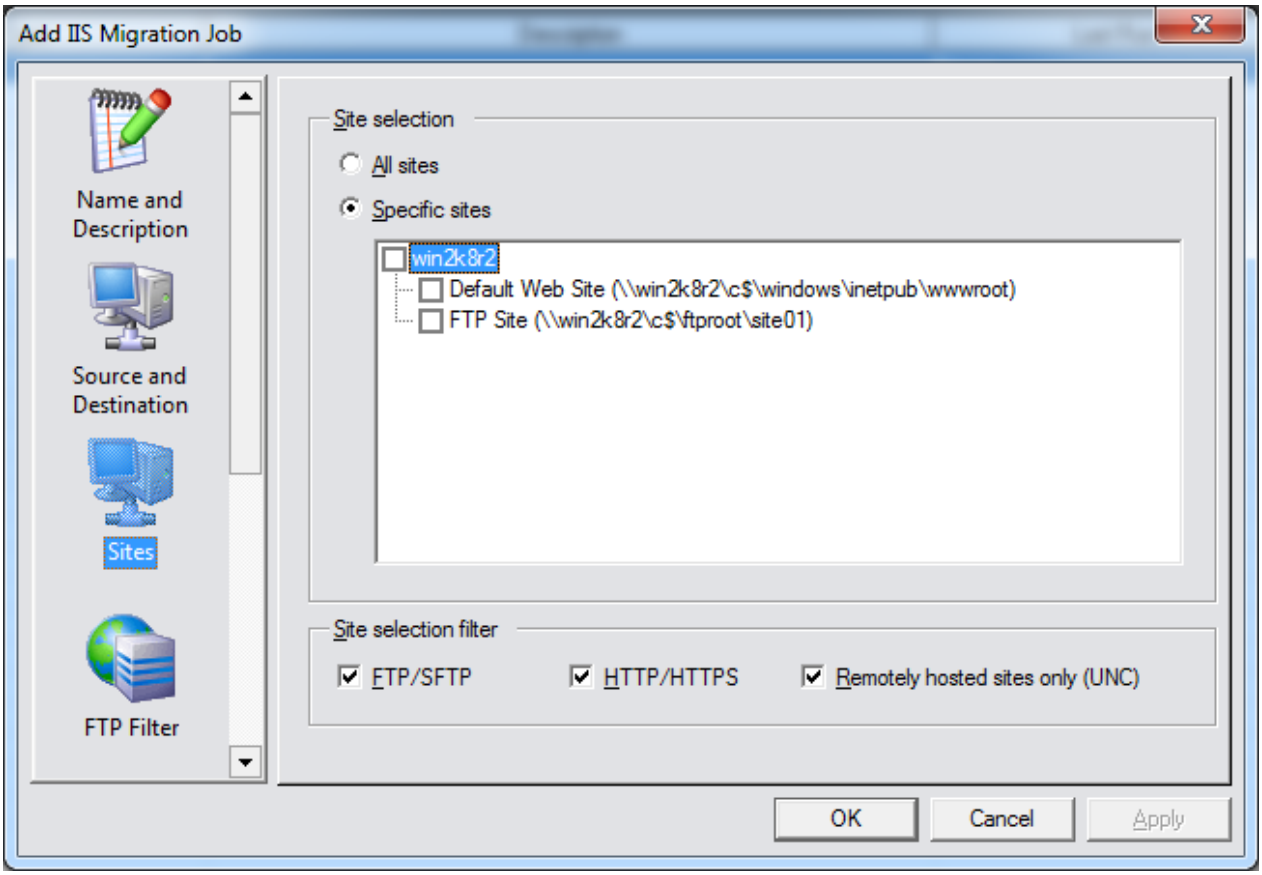
Source and Destination

In the source and destination page, you can specify the names of the source and the target computer running Microsoft IIS.



Sites

In the sites page, you can select the FTP and HTTP sites that you want to migrate from the specified source to the target.



Site Selection

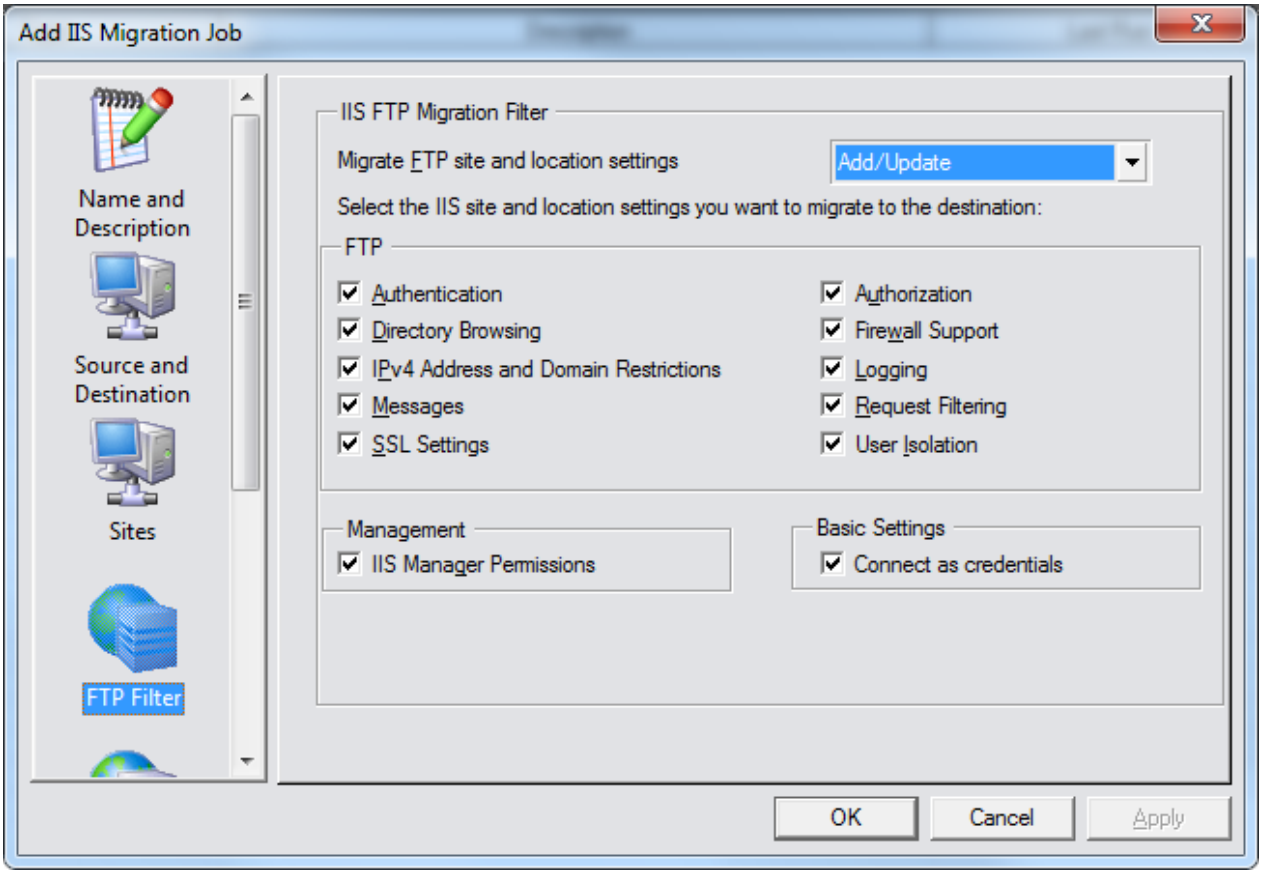
In the site selection box, you can select whether you want to migrate all existing sites or select specific sites.

Site Selection Filter

You can use the site selection filter to display only specific sites in the tree control. The “FTP/SFTP” checkbox controls if FTP/SFTP sites are shown. Likewise, the HTTP/HTTPS checkbox controls if web sites are shown in the tree. The “Remotely hosted sites only (UNC)” checkbox controls if locally hosted web sites are displayed or not. Usually locally hosted sites, should be migrated with a “Data Migration” job instead of a “IIS Site Migration” type of job.

FTP Filter

In the FTP filter page, you can control which IIS FTP settings you want to migrate.



Migrate FTP Site and Location Settings

You can select either “Add only” to migrate sites only if they do not yet exist on the target, or “Add/Update” to migrate sites regardless if they exist or not. “Add/Update” will update existing settings with the settings of the source, in case you run the same job again at a later time.

FTP

In the “FTP” box you can select the FTP settings you want to migrate from source to target. In an option is not checked, the settings will be inherited from the default settings of the target.

Management

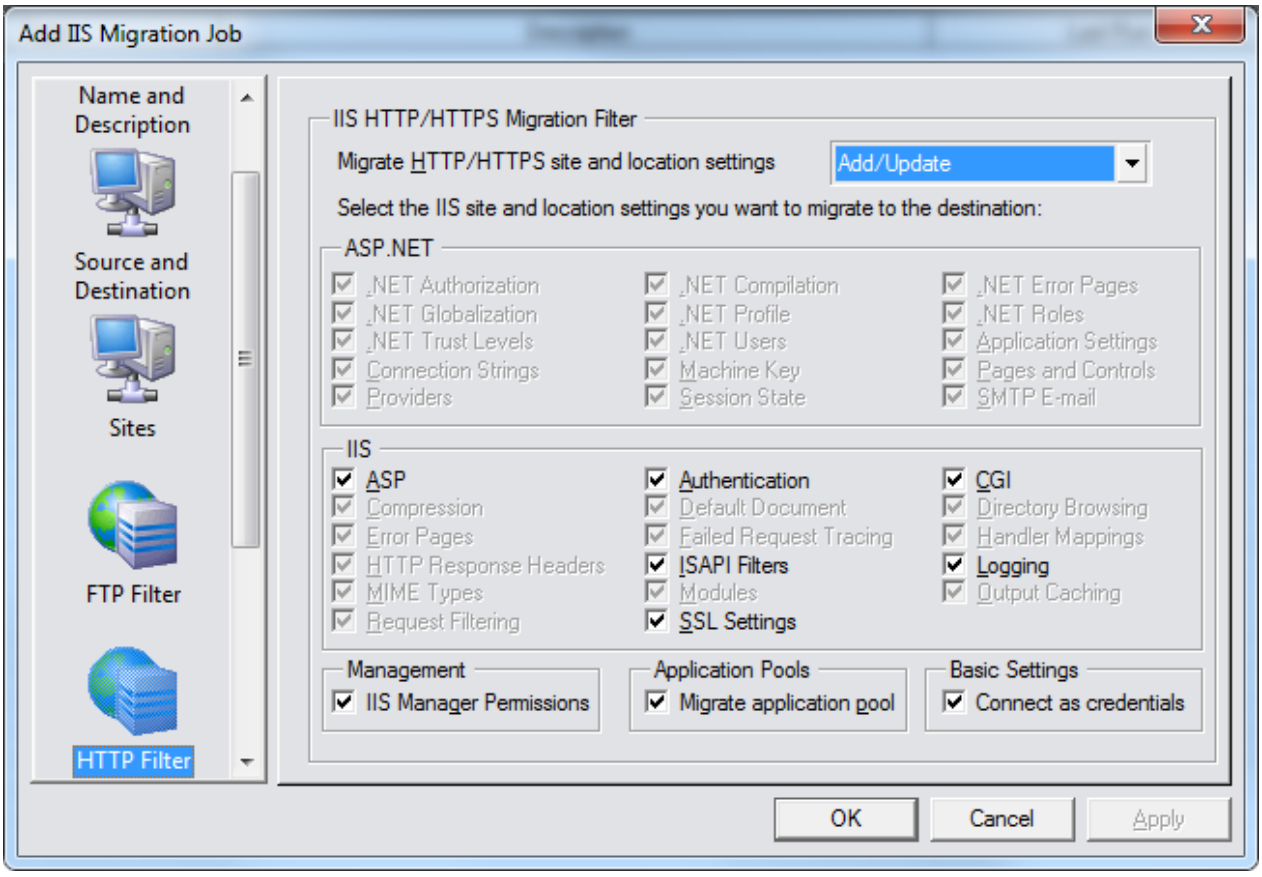
In the “Management” box you can select whether you want to migrate “IIS Manager Permissions” or not.

Basic Settings

In the “Basic Settings” box you can select whether you want to migrate “Connect as credentials” for sites and virtual directories or not. Please ensure that the firewall rules allow accessing DCOM on the remote system in order to migrate the encrypted “Connect as” credentials. Please check the chapter “Firewall Configuration” for more details on the required TCP ports that have to be opened on the remote system, for the system that is running the migration job.

HTTP Filter

In the HTTP filter page, you can control which IIS HTTP settings you want to migrate. Any options contained in the web.config files are grayed out, because an “IIS Migration” job, opposed to a “Data Migration” type of job does not migrate any files, therefore no web.config files are getting migrated.



Migrate HTTP/HTTPS Site and Location Settings

You can select either “Add only” to migrate sites only if they do not yet exist on the target, or “Add/Update” to migrate sites regardless if they exist or not. “Add/Update” will update existing settings with the settings of the source, in case you run the same job again at a later time.

ASP.NET

All of these options are located in the web.config file residing in the root folder of the HTTP/HTTPS site. Therefore, those options are grayed out in an “IIS Site Migration” type of job, opposed to a “Data Migration” type of job.

IIS

In the “IIS” box, you can select IIS settings that you want to migrate. Options located in the web.config file, residing in the root folder of the HTTP/HTTPS site are grayed out in an “IIS Site Migration” type of job, opposed to a “Data Migration” type of job.

Management

In the “Management” box you can select whether you want to migrate “IIS Manager Permissions” or not.

Application Pools

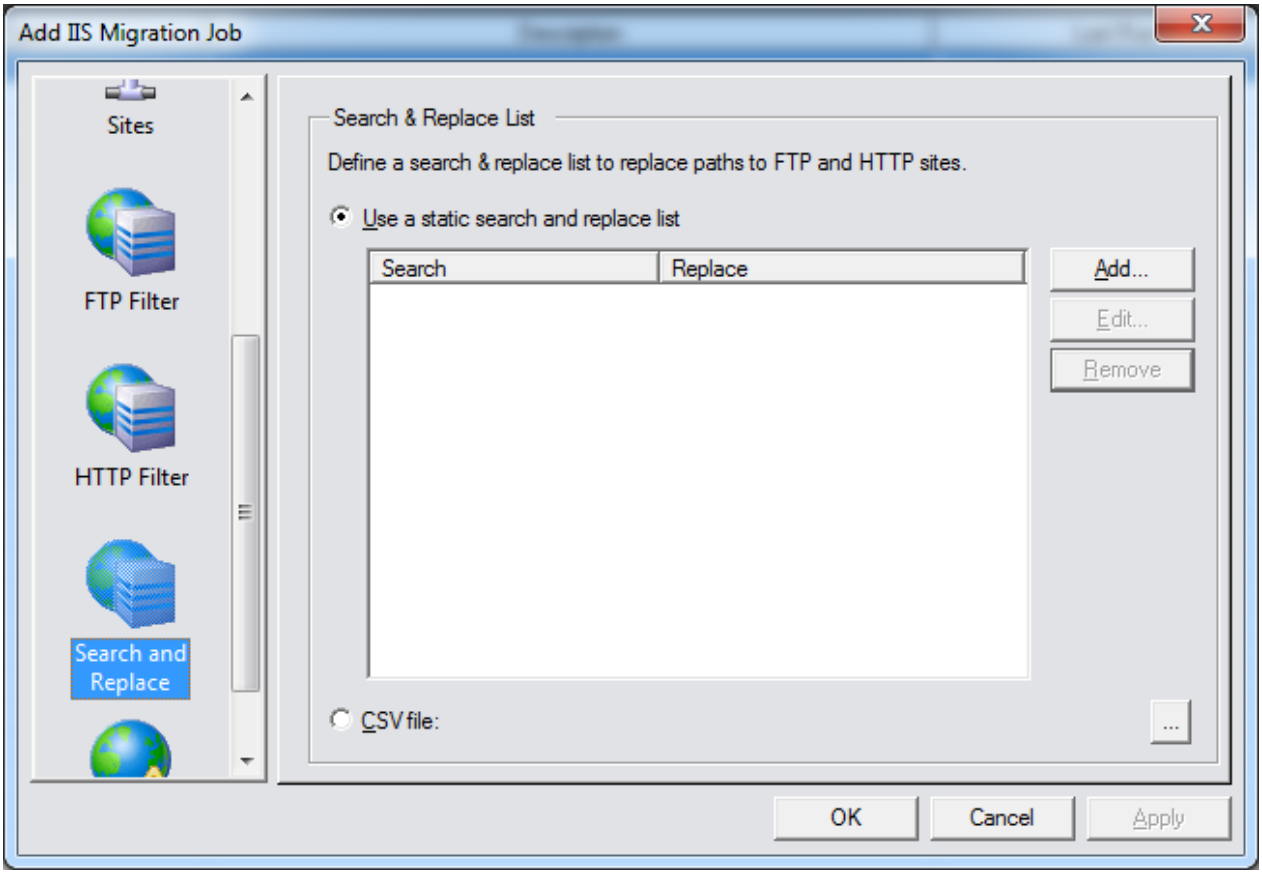
The “Migrate application pool” option, controls whether you want to migrate application pools associated with the migrated web site(s).

Basic Settings

In the “Basic Settings” box you can select whether you want to migrate “Connect as credentials” for sites and virtual directories or not. Please ensure that the firewall rules allow accessing DCOM on the remote system in order to migrate the encrypted “Connect as” credentials. Please check the chapter “Firewall Configuration” for more details on the required TCP ports that have to be opened on the remote system, for the system that is running the migration job.

Search and Replace

In the “Search and Replace” page, you can define a replacement for locations defined in IIS site settings. You could, for example replace a computer name, from “OLD-IIS-SERVER” to “NEW-IIS-SERVER” or change the location of sites from “C:\FTPROOT” to “D:\FTPROOT” in case you want to change the drive the site is located on.



Use a Static Search and Replace List

You can use the “Add…”, “Edit…” and “Remove” buttons to make changes to the list of search & replace pairs.

CSV File

You can specify a CSV file, using a semicolon as delimiter, to specify the search & replacement pairs. The file should contain 2 columns, with the value to search for in the 1st column and the value to replace with in the 2nd column.

DFS Replication (DFSR) Add-On

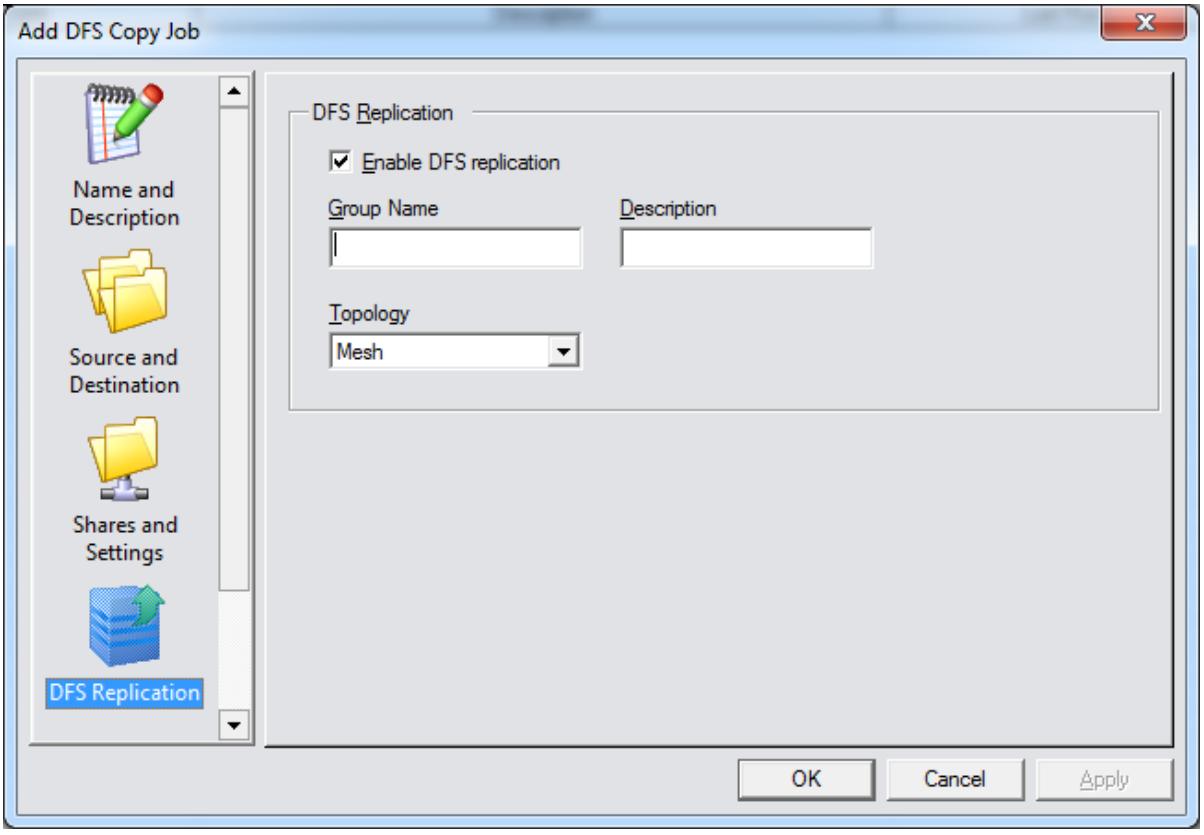
The DFS replication add-on will add an additional page of settings to DFS share consolidation jobs that enables you to configure DFS replication (DFSR) between specified DFS members. It is only available for the 64-bit version of CopyRight2.

You can use the DFS Replication page to set up DFS replication (DFSR) automatically. Currently it supports the mesh (every server replicates bidirectional with every server) and star (every server replicates bidirectional with the first specified server) topology.

Before this option can be enabled, please ensure that you have installed the DFSR Add-On. The Add-On is available on the CopyRight2 download page and requires to use the 64-bit version of CopyRight2. Furthermore, check the "Source and Destination" page, to ensure that you have selected a domain-based DFS and that the DFS referral option is set to "Use specified computer name". You can enter one or more comma separated computer names into the computer name field to setup the replication between them.

DFS Replication

In the DFS Replication page you can configure the replication group name, an optional description and the desired replication topology.



Group Name & Description

Enter the name of the replication group you want to create. You can provide an optional description.

Topology

The DFSR Add-On currently supports the creation of a mesh (every node replicates with every other node) or star topology (first specified server replicates with each other node).

Azure Add-On

The CopyRight2 Azure Add-On is designed to facilitate the migration to Azure storage accounts. It can migrate file shares including share level permissions. The add-on works in conjunction with a data migration job or stand-alone in case you want it to create/update the file shares only, without copying any data.

The add-on can automatically sanitize file share names for the naming convention used by Microsoft storage account file shares. (Lowercase letters, numbers and hyphens only. The file share names must begin and end with a letter or number and cannot contain two consecutive hyphens).

In order to use the add-on, please provide the fully qualified DNS name, the platform (Azure) and the role of the storage accounts in “Options” -> “OS types, roles and DCs”.

The add-on additionally supports the use of DFS to let a “Data Migration” job automatically update corresponding DFS entries to let them point to their new location in the cloud.

Using the add-on requires that you have previously installed Azure AD Connect to replicate the Active Directory accounts of your on-premise Active Directory (AD) to Azure AD (AAD). Furthermore, you need to create the storage accounts and join them to your on-premise domain (a.k.a. Hybrid Mode). You will also need to register an app in Azure AD to allow CopyRight2 access to the APIs required to create/update the storage account file shares and set permissions accordingly.

To join a storage account to an on-premise domain, please download Microsoft’s PowerShell scripts from Github and follow Microsoft’s instructions for this process.

When setting up a job, you will need the Azure subscription ID, the Azure primary domain name (FQDN), the tenant ID, the ID of the registered App, the client secret of the registered app and optionally the storage account secret.

You can find a video in our YouTube channel outlining the entire process including setting up “Azure AD Connect”, registering the app, creating the storage account, joining it to the on-premise domain and additionally how to use DFS in conjunction with the storage account migration to transparently switch from the on-premise file server hosting the data to the storage accounts in the cloud.

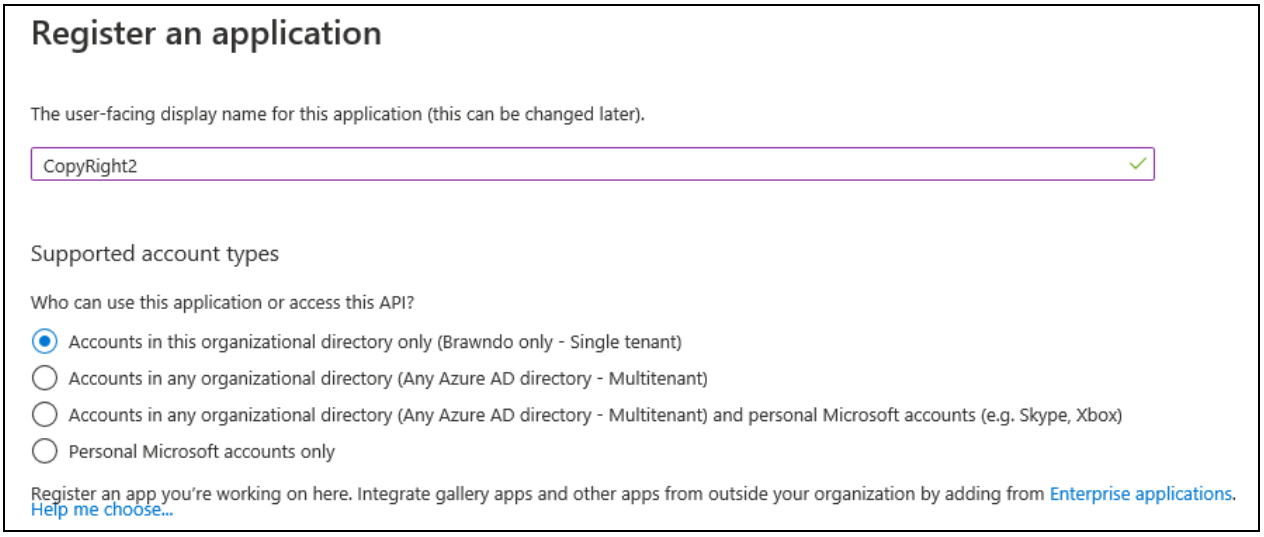
Replacing References to the Everyone Group

If migrating file shares to your Azure storage account and your file shares use the well-known group Everyone, which doesn’t exist in Azure AD, you will need to create a group in your on-premise domain first and replicate it using Azure AD Connect. Once replicated you can define a mapping file using the following format to replace occurrences of everyone with that group (and replace NetBIOS-Domain-Name and Replacement-Group accordingly):
{S-1-1-0};NetBIOS-Domain-Name\Replacement-Group

Once you have created the mapping file, assign it in your job setting’s ACL and Owner Permissions page.

Azure App Registration

Before the add-on can be used, you will need to define an app registration in Azure to allow CopyRight2 to call Azure management APIs:



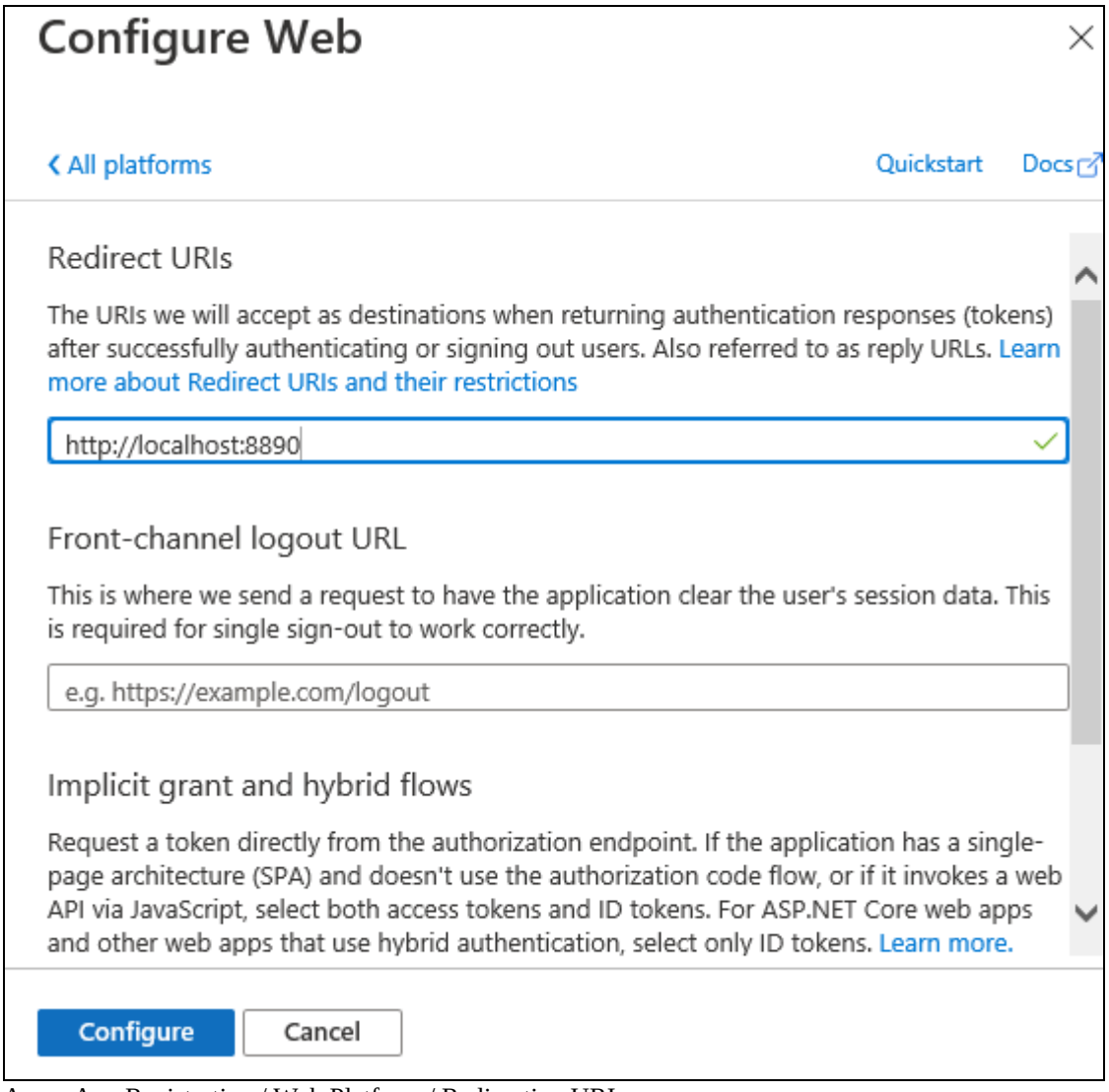
Adding Azure AD App Registration

After adding the app registration, please click on "Add a Redirect URI" to configure the redirection URI:



Azure AD App Registration Overview

Next click on the "Add a platform" link and select the "Web" platform. Enter "http://localhost:8890" as redirection URI and then click on the "Configure" button to save it.



Azure App Registration / Web Platform / Redirection URI

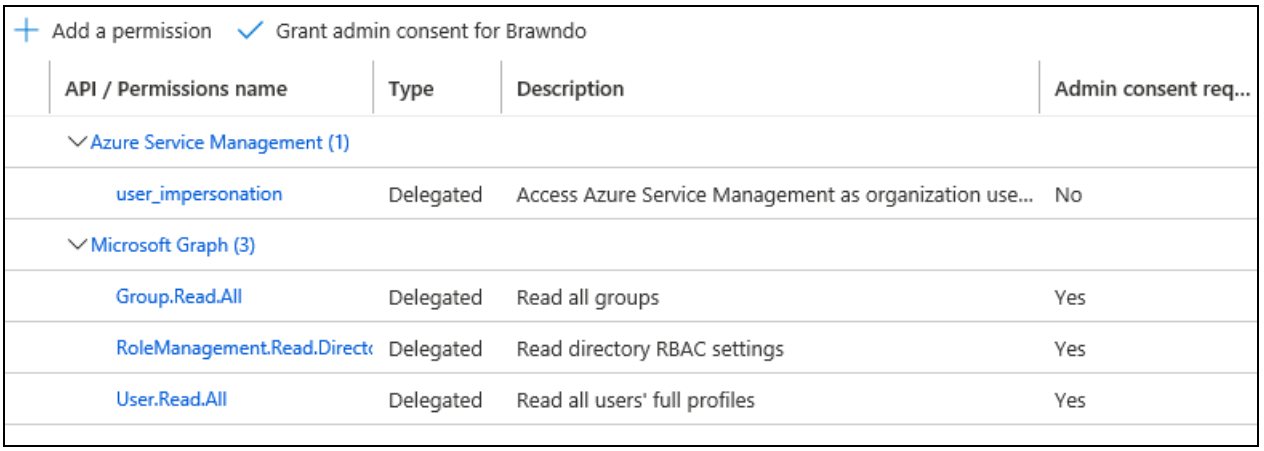
This is the URI a user authenticating to Azure will get redirected to.

Note: When running the job, CopyRight2 needs a so-called token that it can present along with requests going to Azure, such as retrieving information about existing shares in the Storage Account, retrieving information about share permissions, adding shares, setting permissions and so on.

To authenticate CopyRight2 will launch the default browser and navigate to the Azure authentication web page.

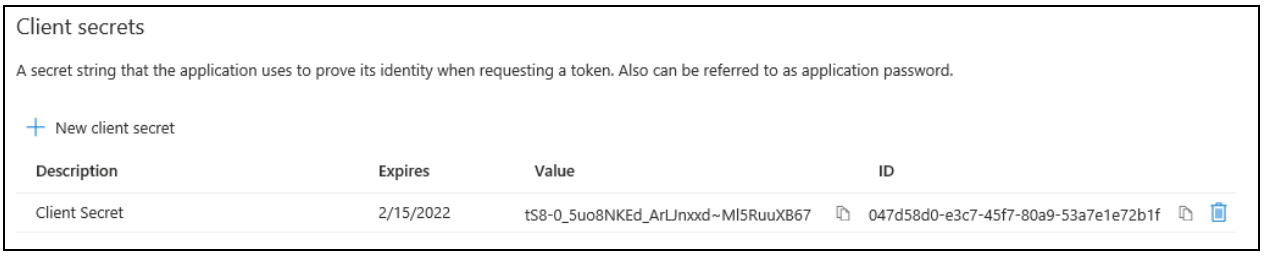
After providing credentials and logging on successfully, the Microsoft page executes a JavaScript page that redirects to the URL specified in the Azure configuration and along with the resulting token as a parameter. In this case it is http://localhost::8890. Before CopyRight2 launches the browser it opens up that local port 8890 and waits for the token. It will send the string “OK” to the browser page once the token has been received. After that the port will be closed again and the user can close the browser. There is no SSL needed, because it takes place computer internally.

After configuring the URI, please configure the “API Permissions” for the registered app as shown below in order to allow CopyRight2 to provision the shares and grant corresponding file share permissions:



Azure App Registration / API Permissions

Finally define a client secret.



Azure App Registration / Client Secret

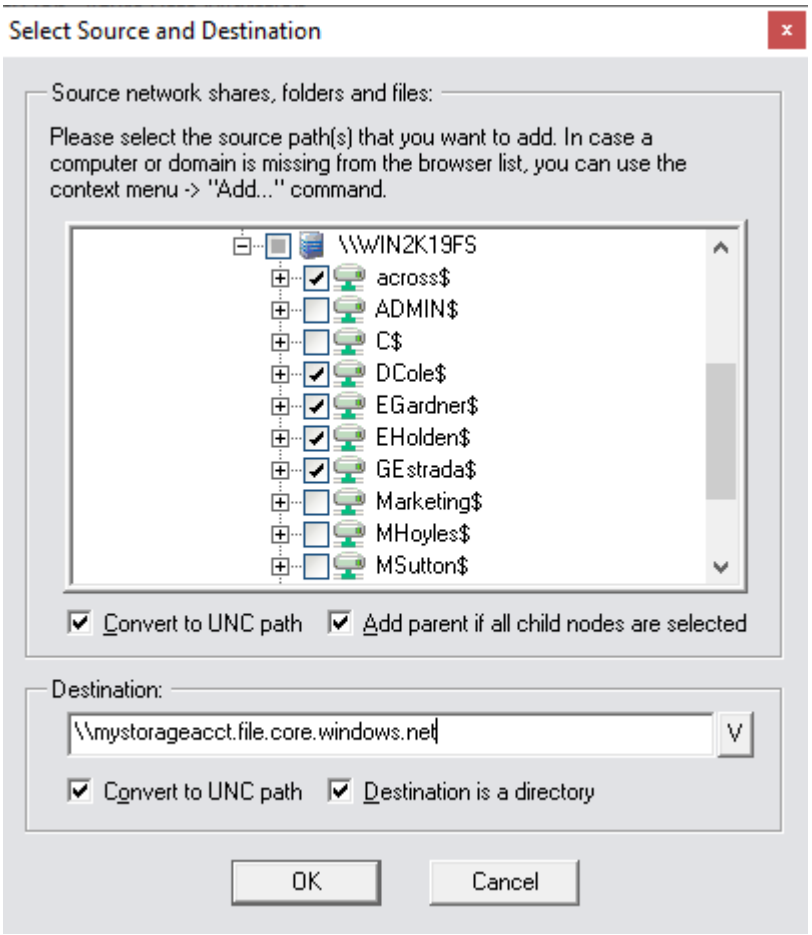
Migrate File Shares to Azure Storage Accounts During Data Migration

The add-on fully integrates with a regular CopyRight2 “Data Migration” type of job. After installing the add-on, you will get an additional “Azure Options” page, where you can define information required to provision file shares in Azure storage accounts. Additionally, you can select file shares in the “Source and Destination” page of the “Data Migration” job and provide the FQDN of a storage account to automatically generate the source & destination pairs.

Adding File Shares to the Job

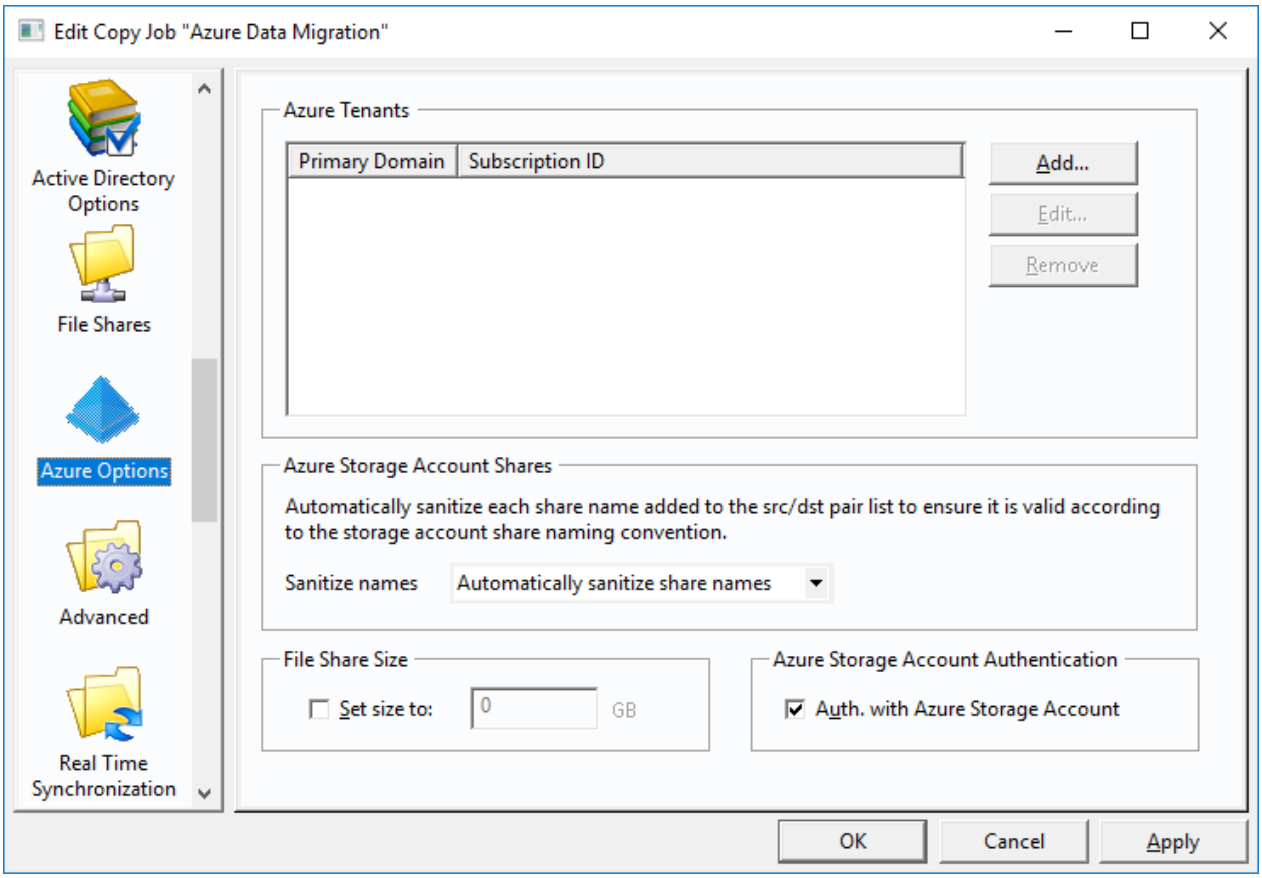
If the add-on is installed you can specify the FQDN of a storage account, previously defined as Azure Storage Account in “Options” -> “OS type, roles and DCs”, as a destination for the selected source shares. CopyRight2 will then automatically create the corresponding source & destination pairs for the selected file shares.

In the example below the destination is the storage account “mystorageacct”:



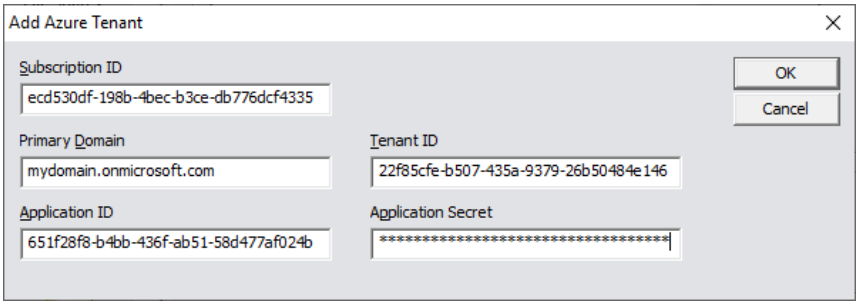
Azure Options

In the “Azure Options” page you define the information required to let CopyRight2 and the Azure add-on provision file shares in the Azure storage accounts.



Azure Tenants

After clicking on “Add” or “Edit” you can define the Azure subscription ID, the FQDN of the Azure AD, then tenant ID, the ID of the registered app and the client secret of the registered app:



Azure Storage Account Shares

Here you can enable the job to automatically sanitize share names, to work properly with Azure's storage account file share naming convention. Alternatively, you can provide a file share name manually.

File Share Size

If enabled, you can specify the size of Azure storage account file shares in GB.

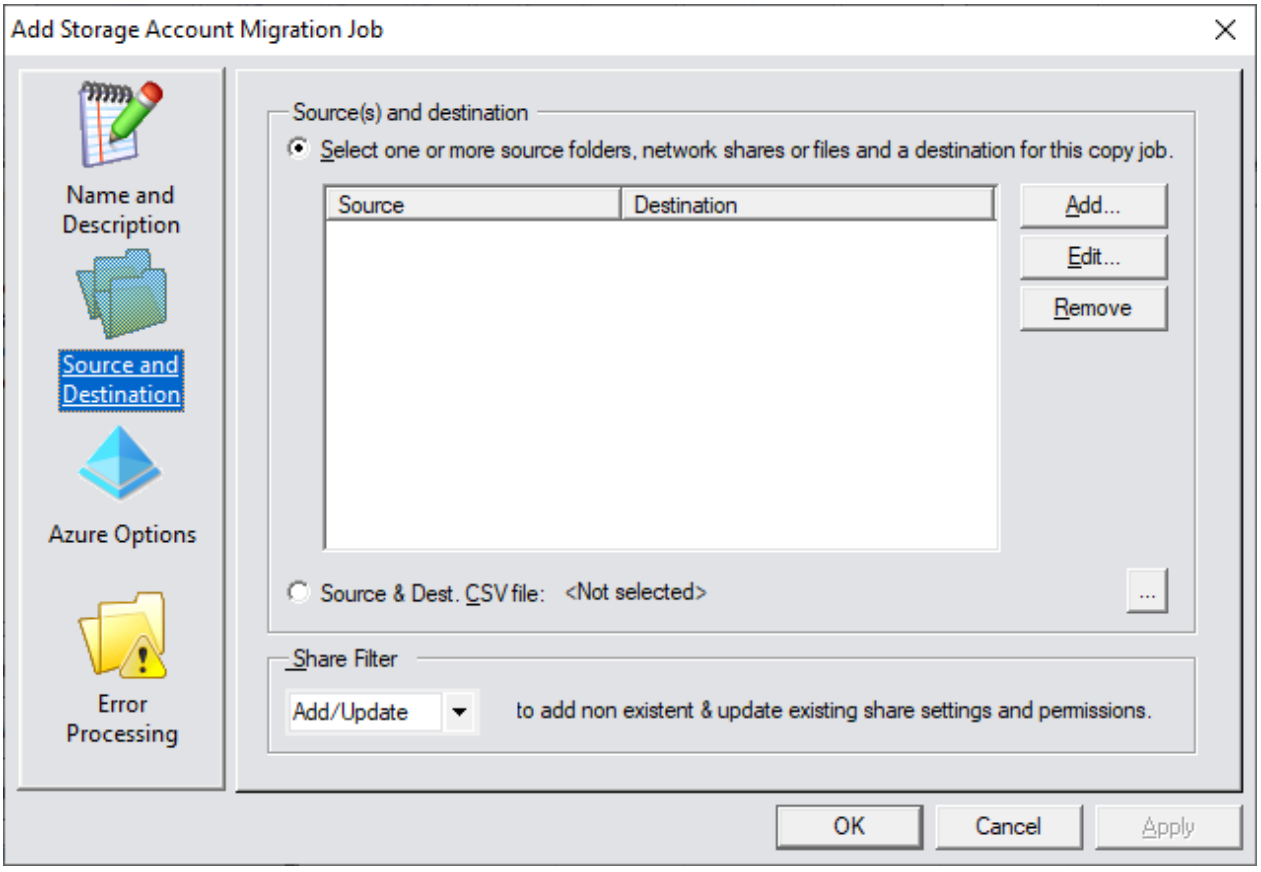
Azure Storage Account Authentication

If enabled, the copy job will prompt for the storage account's access key to bypass any restrictive NTFS permissions, for example home shares only allowing access to the corresponding user account, but not for the Administrators group. This is quite similar to using the backup/restore privileges on a Windows system.

Migrate File Shares to Azure Storage Accounts Without Data Migration

The new job type “Storage Account Migration” is available after the Azure Migration add-on has been installed and allows the definition of a job that solely creates the file shares in the storage account without migrating any data.

Source and Destination



Source(s) and destination

Here you can define the source and target shares. For example, to migrate the file share “\\MyServer\MyUser$” to the storage account share “\\mystorageacct.file.core.windows.net\MyUser”.

Share Filter

The share filter defines whether file shares should be added only if they do not yet exist (“Add only”) or if existing file shares should get updated as well (“Add/Update”).

Azure Options

This page is identical to the “Azure Options” page of a regular data migration job. Please refer to chapter “Migrate File Shares to Azure Storage Accounts During Data Migration” for an explanation of available settings.

PowerShell Integration Add-on

The PowerShell Integration Add-on adds the ability to use PowerShell in your ActiveScript scripts defined in the job settings (object transformation scripts, job start/end scripts, copy start/end scripts).

To call a PowerShell cmdlet either as a function or a sub-routine you need to prefix the call with the '#' character.

In case of a function, the add-on will automatically convert the returned data into either a single variant, a list of variants (1-dimensional) or a table of variants (2-dimensional). It will return a Variant of type VT_Empty, in case of something that has no value set to differentiate from the case where an empty string is returned.

You can use ActiveScript variables and functions as parameters when calling PowerShell cmdlets.

If calling a cmdlet as a sub-routine the cmdlet's output will get appended to the job's log file automatically. If the cmdlet is assigned to an ActiveScript variable the output will not get logged unless you set the log level for ActiveScript component in Options -> Extended Logging to at least level 3.

Below you can find some examples:

```
…
#write-output "Hello World"
…
```

Call PowerShell as Sub to Write Something to the Log File using the Write-Output Cmdlet

This is the easiest case, where the PowerShell cmdlet is called as a sub-routine. Output will get redirected to the log file.

```
…
psOutput=#write-output "Hello World"
MsgBox psOutput
…
```

Redirect PowerShell Output to an ActiveScript Variable and Show it in a Message Box | Single Variant

This short two-line script shows how to redirect the output into an ActiveScript variable and then display the content of the variable using ActiveScript's MsgBox.

```
…
sid = #get-localuser Destination("samAccountName") | select "Sid"
MsgBox "SID=" & sid
…
```

Call Get-Localuser Cmdlet for the Current Target User and Filter for its SID Attribute using Select | Single Variant

This example shows how to pass parameters to a PowerShell cmdlet. It calls CopyRight2's Destination() ActiveScript function to retrieve the content of the samAccountName attribute for the object currently being migrated. Additionally you can see how to combine it with a Select to filter the output to the Sid attribute.

Important: "Sid" has to be put inside of double quotes to differentiate from an ActiveScript variable called Sid.

```
…
sids=#get-localuser | select "Sid"
for i = 0 to UBound(sids)
   MsgBox sids(i)
Next
…
```

Call Get-Localuser Cmdlet for all Local Users and Filter for the SID Attribute using Select | List of Variants

This example shows how to deal with a list of Variants being returned. You can use ActiveScript's UBound() and LBound() on the returned Variant to get the upper and lower bounds. The lower bound will always be zero. It will go through the list and display each Variant contained in the list.

```
…
localUsers=#get-localuser | select "Sid", "Description", "Name"
MsgBox "Rows=" & UBound(localUsers, 1)+1
MsgBox "Cols=" & UBound(localUsers, 2)+1
for r = 0 to UBound(localUsers, 1)
  for c = 0 to UBound(localUsers, 2)
      MsgBox localUsers(r, c)
  next
next
…
```

Call the Get-LocalUser Cmdlet for all Local Users and Filter for the Sid, Description and Name | Table of Variants

This example shows how to deal with a table of Variants being returned having 2 dimensions. Again you can use UBound() to get the table's boundaries for each of the two dimensions, with rows being the 1st dimension and columns the 2nd dimension. The example displays each cell of the table from left to right and top down.

```
…
var=#ps-cmdlet | select "SomeAttribute"
if IsEmpty(var) then
  MsgBox "Var is empty"
else
  MsgBox "Var is not empty"
endif
…
```

Test if a Returned Value is Empty Using IsEmpty()

This example shows how to use ActiveScript's IsEmpty() function to test if the returned Variant is empty and differentiate from the case where it contains the string "".

```
…
#Add-PSsnapin -Name "Microsoft.Exchange.Management.PowerShell.SnapIn" -ErrorAction "SilentlyContinue"
…
```

Add an Additional PowerShell Snap-in using Add-PsSnapIn from Job Start Script to Execute It Only Once

This example shows how to load additional PowerShell snap-ins, for example the Exchange Management PowerShell Snap-In.

```
…
#import-module "d:\program files\Sys-Manage\CopyRight\Data\MyPSScript.psm1"
…
```

Import a PowerShell module from Job Start Script to Execute It Only Once

This example shows how to load a PowerShell module.

```
…
Function Adjust-User {
  [CmdletBinding()]
  param (
    [Parameter(Mandatory, Position = 0)]$Identity
  )

  $ErrorActionPreference = "silentlycontinue"

  Write-Output "Calling Adjust-User for user $($Identity)"
}
…
```

Example PowerShell Function in a Custom Defined Module

The example above shows, how to define a function in a PowerShell module.

```
…
#Adjust-User Source("samAccountName")
…
```

Calling a Function of a Custom Defined Module

The example above shows how to call the Adjust-User PowerShell function defined in a PowerShell module.

Using ActiveScript

CopyRight2 supports ActiveScript based scripts to allow customization of copy jobs. You can define custom scripts executed during job start and completion, for example to stop and start running services or to integrate the migration process with other existing processes. Additionally, you can define transformation scripts that get executed during the migration of specific object types.

Script Type	Description
Job Start	Executed when the copy job starts.
Job End	Executed when the copy job has completed.
Copy Start	Executed when the next source/destination pair of the copy job is processed.
Copy End	Executed when the currently executed source/destination pair has completed.
Transform Users	Executed during migration of any local or global user account.
Transform Contacts	Executed during migration of any Active Directory contact.
Transform Groups	Executed during migration of any local or global group account.
Transform OUs	Executed during migration of any Active Directory OU.

You can use any ActiveScript compatible script language that is installed on the computer running the copy job, for example VBScript, JScript or other 3rd party implementations such as PHP or Python.

Note: In case of a "User and Group" type of copy job, having only a single source and destination computer as parameters, the behaviour of "Job Start / Job End" scripts is identical to "Copy Start / Copy End".

Global Variables

There are some pre-defined variables that are defined in the executing script's context, containing for example the name of the currently executing copy job.

Name	Description
JobName	Contains the name of the currently running copy job instance.
SourceComputer	Contains the source computer's NetBIOS name.
DestinationComputer	Contains the destination computer's NetBIOS name.
SourceDomain	Contains the source computer's NetBIOS domain name.
DestinationDomain	Contains the destination computer's NetBIOS domain name.
SourceObject	In case of a transformation script, contains the corresponding IADs source object for Active Directory objects (for example IADsUser for user objects).
DestinationObject	In case of a transformation script, contains the corresponding IADs destination object for Active Directory objects (for example IADsUser for user objects).
UserProfile	Only for Computer and Profile Migration jobs: The absolute path of the currently migrated user profile. This should not be needed as the current directory is changed to the currently processed profile's root folder and relative paths can be used from there in scripts.
UserProfileReg	Only for Computer and Profile Migration jobs: Registry path to the user profile currently being processed. This should not be needed as HKEY_CURRENT_USER is automatically replaced by the value of this global variable.

Transformation of Attributes

The transformation scripts are executed during the migration of local and Active Directory objects. You can access the attributes of the source and destination object using the “Source” and “Destination” methods specifying the attribute name as an argument. In case of Active Directory objects, you can use any attributes defined in the directories schema for the corresponding object class.

If you would like for example, to add the prefix “US_” to any migrated groups common name attribute (cn), you could use the following line of VBScript code for the “Transform Groups” script:

```
…
Destination("cn")="US_" & Source("cn")
…
```

Accessing Local Account’s Attributes

In case of non-domain (workgroup or member server) local groups or NT4 domain groups, you can use the “samAccountName” and “description” attribute to access the corresponding values.

In case of non-domain users or NT4 domain users, you can use the attribute names listed below to access the corresponding values, which are mostly identical to the attribute names used in Active Directory:

User Attribute Name
samAccountName
description
homeDrive
homeDirectory
scriptPath
displayName
comment
userParameters
userWorkstations
logonServer
profilePath
logonHours
userAccountControl
accountExpires
maxStorage
countryCode
codePage
rid
primaryGroupId
passwordExpired

Terminal Server, Citrix and Remote Access Server (RAS) Attributes

You can use the following attribute names to access Terminal Server/Citrix and Remote Access Server (RAS) specific attribute values that are usually encoded into the userParameters attribute as binary large object (BLOB):

Attribute Name	Attribute Type
TerminalServicesHomeDirectory	String
TerminalServicesHomeDrive	String
TerminalServicesProfilePath	String
TerminalServicesProfilePath	String
TerminalServicesWorkingDirectory	String
TerminalServicesInheritInitialProgram	String
AllowLogon	Integer (0=No, 1=Yes)
MaxConnectionTime	Integer (Time in minutes)
MaxDisconnectionTime	Integer (Time in minutes)
MaxIdleTime	Integer (Time in minutes)
ConnectClientDrivesAtLogon	Integer (0=No, 1=Yes)
ConnectClientPrintersAtLogon	Integer (0=No, 1=Yes)
DefaultToMainPrinter	Integer (0=No, 1=Yes)
BrokenConnectionAction	Integer (0=No, 1=Yes)
ReconnectionAction	Integer (0=No, 1=Yes)
EnableRemoteControl	Integer (0=No, 1=Yes)
ModemCallbackSettings	Integer (0=No, 1=Yes)
ModemCallbackPhoneNumber	String

Logging and WScript Functions

Below you can find supported logging and helper functions:

Name	Description	Example
LogError	Writes a string to the log file and increases the currently running job's error counter by one.	LogError "An error has occurred!"
Wscript.Echo	Writes a string to the log file.	WScript.Echo "Hello World"
WScript.Sleep	Sleeps for the specified amount of milliseconds.	WScript.Sleep 3000
WScript.Stdout.WriteLine	Same as WScript.Echo	WScript.Stdout.WriteLine "Hello World"
WScript.Stderr.WriteLine	Same as LogError	WScript.Stderr.WriteLine "Some error occurred!"

Creating a Mapping Definition File to Reassign Permissions

Additionally, to the options to copy users and groups from the source to the destination environment, there is the possibility to define a static mapping table that assigns user and group accounts used in permissions to corresponding accounts in the destination environment.

To create a map file, start the “User and Group Assignment” shortcut from the CopyRight2 start menu group.

The mapping file assigns users and groups from the source environment to corresponding accounts in the destination environment. CopyRight2 uses this file while running a copy process (the “Paste with CopyRight…” command”) or when reassigning permissions (the “ReAcl with CopyRight…”).

If you want to change an existing mapping file, you can use the command „Open...“ from the “File” menu to open the file.

The assignment is visually displayed in the shape of a list. For each row the left column of the list is containing one or more user or group accounts in the source environment that should be replaced within permissions by the user or group account contained in the right column. You can define 1:1, 1:0, 1:n, n:1, and n:0 relationships. If using n:1, multiple accounts in the source environment will all be replaced by the same account in the destination environment.

Relationship	Name	Description
1:1	Replace Account (Reacling)	This will replace one user or group account with another.
1:0	Remove Account	This will remove one user or group.
1:n	Replace Account by Multiple Accounts (AddAcling)	This will replace one user or group account with multiple other accounts. **Note:** Please note that you can specify the source account as one of the multiple destination accounts. This will add the listed accounts while retaining the original account that had permission. (Not reacling but addacling).
n:0	Remove Multiple Accounts	This will remove any of the listed user or group accounts.
n :1	Replace Multiple Accounts by a Single Account	This will replace any of the listed user or group accounts by the specified destination account.

To add an entry to the list, run the command „Add...“ from the “Edit” menu. You can enter multiple values into the field “Users or groups in the source environment”, using comma separated format, that should be replaced within permissions. You can use the button “…” to select the user or group accounts interactively.

Next enter the name of the user or group account that should replace the previously defined users or groups within permissions. You can use the “…” button to graphically select the accounts.

Next click on OK to add the entry to the list.

To edit an entry already contained in the list, select the entry and then run the „Edit...“ command from the “Edit” menu.

When you are finished with preparing the mapping definition, use the command „Save as...“ from the “File” menu to save the definition into a file with a MAP file extension.

You can use the saved mapping definition with the Windows Explorer extension of CopyRight2 by activating the option „"Map security identifiers with a predefined mapping table". If you are using the command line interface of CopyRight2 you can use the mapping definition file by specifying the option „/G:Filename.Map".

You can use such a definition file in addition to the options /CU, /CL and /CG to copy users, local groups and global groups from the source to the destination environment. Groups or user accounts contained in the mapping definition file will not be copied, but assigned as defined in the mapping file instead.

If the option „Store SID's in file" from the „Edit" menu is activated, the mapping file will contain only so called security identifiers (SIDs) instead of clear-text user and group names.

Using SIDs instead of user and group names speeds up the copy process and additionally prevents problems that might occur if account names from the source environment cannot be resolved correctly into SID's in the destination environment.

Mapping File Format

The mapping file is technically a semicolon delimited text file. Each row defines one mapping. The file can contain accounts specified as domain\account in case of domain accounts, computer\account in case of local accounts or by SID.

{Src Account}[,{Src Account}…];{Dst. Account}[,{Dst Account}…][;{Advanced Option}]

Source and Destination Account Format

Format	**Example**
NetBIOS-Domain-Name\SAM-Account-Name	Contoso\User001
FQDN-DNS-Domain-Name\SAM-Account-Name	Contoso.com\User001
User-Principal-Name	User001@Contoso.com
\\NetBIOS-Computer-Name\SAM-Account-Name	\\DC01\User001 (*)
\\FQDN-DNS-Domain-Name\ SAM-Account-Name	\\DC01.Contoso.com\User001 (*)
{S-1-5-…}	{S-1-1-0} (Everyone)
{Entra-GUID}	{F4753DCB-1F52-4EC8-BE8B-5101F1FF6D23}
{Entra:User-Principal-Name}	{Entra:User001@ContosoTenant.Com} (**)

(*) Specifying a domain controller with two leading backslashes can be used to force the software to use the specified domain controller instead of letting Windows perform a domain controller lookup, for example to evade replication issues.

(**) Specifying an Entra User-Principal-Name requires configuration of Entra authentication.

Reacling

The easiest case is a 1:1 replacement (reacling) of a source user or group account with an account from the destination. For example, if you would like to replace the user MOldDomain\JDoe with the account MyNewDomain\JohnD, you could add the following line to the mapping file:

```
…
MyOldDomain\JDoe; MyNewDomain\JohnD
…
```

AddAcling

If you would like to define a 1:n relationship (addacling) to replace the account MyOldDomain\JSmith with the account MyNewDomain\SmithJ while retaining the old permission you could add the line:

```
…
MyOldDomain\JSmith; MyOldDomain\JSmith, MyNewDomain\SmithJ
…
```

Beginning with build 450, you can also use the following syntax to Add an account by using the advanced option 4:

```
…
MyOldDomain\JSmith; MyNewDomain\SmithJ; 4
…
```

Alternatively, you can specify SIDs as well. A specified SID has to be enclosed in curly brackets. For example, {S-1-1-0} represents the well-known everyone SID.

DeAcling

If you would like to remove specific accounts, you can use a 1:0 relationship (deacling). For example if you would like to remove the account MyOldDomain\PeterM:

```
…
MyOldDomain\PeterM;
…
```

Mapping File Advanced Options

The optional advanced option is a numeric value that enables special processing for the specified SID. It enables you to remove SIDs of accounts of a specific domain by either defining a negative list of domains to be removed or by defining a positive list of domains that should be kept while all other SIDs of other domains will be removed.

Option	Name	Description
0	Mapping Entry	Normal mapping entry
1	Domain Mapping (Negative List)	Special entry containing a domain SID (without RID), that defines a domain whose SIDs should be removed from permissions. This can be useful to clean-up permissions after a specific domain has been disabled
2	Domain Mapping (Positive List)	Special entry containing a domain SID (without RID), that defines a domain whose SIDs should be kept within permissions. Please note that you can specify multiple entries of the type 2 by specifying multiple lines of text. All other SIDs of other domains not specified using the option 2 will be removed from permissions.
3	Rename samAccountName of target account	If option 3 is specified and the target account does not exist, it will get created using the samAccountName specified in the 2nd column.
4	AddAcling	If option 4 is specified the account specified in the 2nd column will get added with permissions identical to those found for the account specified in the 1st column (AddAcling).

Domain Mapping (Negative List)

You can for example define a mapping file that removes any encountered domain SIDs of two specific domains:

```
…
{S-1-5-21-2141040004-1731178622-1653586129};;1
{S-1-5-21-3453453453-1345345343-2345345342};;1
…
```

Domain Mapping (Positive List)

You can specify a mapping file that only keeps domain SIDs of two specific domains, while removing any other SIDs of other domains:

```
…
{S-1-5-21-2141040004-1731178622-1653586129};;2
{S-1-5-21-3453453453-1345345343-2345345342};;2
…
```

Rename samAccountName of Target Account

To migrate accounts from source to target and create the target account if it does not yet exist, with a different samAccountName, or to synchronize existing objects with existing objects in the target having a different samAccountName you can use the option 3.

For example:

```
…
MyOldDomain\PeterM;MyNewDomain\PMaier;3
MyOldDomain\Group01;MyNewDomain\Group-01;3
…
```

If 3 is not specified, a copy job will fail if the target account does not exist, because it will not create the object with the samAccountName different from the samAccountName of the source account.

This option works for user, group and computer objects.

AddAcling

Beginning with build 450, you can specify the advanced option 4 in the third column, to simplify the AddAcling format used in previous versions, where you had to specify the original account and the account you want to add comma separated in the 2nd column of the semicolon delimited file. The original format is still valid and supported.

Let's say you want to add the account DstDomain\Account01, everywhere where SrcDomain\Account01 was referenced with the identical permissions you can now use this format:

```
…
MyOldDomain\Account01;MyNewDomain\Account01;4
…
```

This old format is still valid:

```
…
MyOldDomain\Account01;MyOldDomain\Account01,MyNewDomain\Account01
…
```

Creating a Mapping File based on NTFS and/or Share Permissions

In case you want to create a mapping file for the migration of a specific folder and/or shares that are located at or below that folder, you can use the /DX command line option to create a consolidated list of accounts that are used in NTFS and/or share permissions. The output file is named PermAccounts.Txt by default.

The /DX command line option can be used in conjunction with the /DD (dump directory), /DF (dump file) and /DS (dump share) options. You can combine it with the /DH (dump header) to include a first row of column headers.

The resulting file has the following format:

Column	Name	Description
1	Computer	Name of the computer.
2	Account Domain And Name	Domain name and account name.
3	SID	SID
4	Account Type	Type of account
5	Timestamp	Timestamp

You can use Microsoft Excel for example to use column 2 or 3 to produce a mapping file containing the required accounts.

To create a PermAccounts.Txt file containing all users and groups used in NTFS permissions (Permissions, Auditing and Owner) of the folder "c:\myfolder", you could run the following command line statement:

```
Copyright c:\myfolder /dd /df /dx /dh
```

If you would like to additionally include accounts used in share permissions of any share located at "c:\myfolder" or below that folder you could run the following command line statement:

```
Copyright c:\myfolder /dd /df /ds /dx /dh
```

If you would like to produce a PermAccounts.Txt file containing all the user and group accounts used in any share level permission of all the shares hosted on the local computer, you could run the following command line statement:

```
Copyright /ds /dx /dh
```

Using the Windows Explorer Extension

Copying with the Windows Explorer extension

Start up a new instance of the Windows Explorer by running the command “Windows Explorer” from the folder “Programs” and its subfolder “Accessories”.

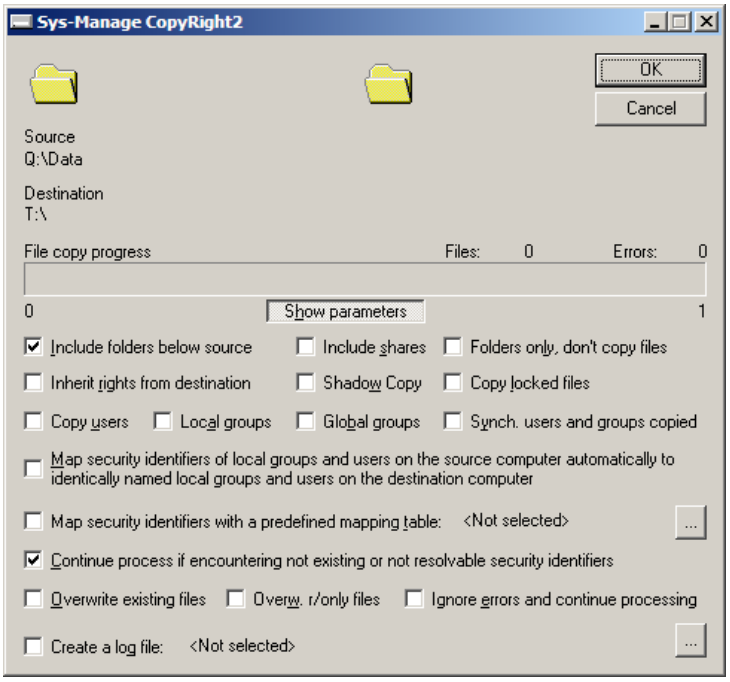
You can either use the Windows Explorer to navigate to the location of the files you want to copy or enter the locations absolute or UNC path within the corresponding Windows Explorer field. This could be for example \\SourceServer\C$ or C:\Marketing Data.

Select the folder you want to copy within the left side of the Windows Explorer.

Open up the context menu by clicking on the right mouse button, while the folder is still selected. Run the command “Copy” from within this menu.

Next use the Windows Explorer to navigate to the folder where you want to insert the files selected in the previous step, you can enter the destination location into the corresponding field of the “Windows Explorer”. This could be for example \\DestinationServer\D$ or T:\Marketing Data.

Then use the tree view of the Windows explorer, located on the left side of the window, to select the folder, where you want to insert the files. Open up the context menu by clicking on the right mouse button while the folder is still selected. Run the command “Paste with CopyRight…”. A window will open up, where you can specify the options required to copy files, folders and shares:



The options of the Windows Explorer extension are described in the following table:

Option	Description	Corresponds to command line parameter
Include folders below source	This option controls whether subfolders of the selected folder(s) should be copied too. This option is selected by default.	/S
Include shares	This option controls whether network shares should be copied from the source to the destination. If enabling this option all network shares of folders affected by the copy process are included.	/H
Copy locked files	This option controls whether locked files should be copied during the copy process.	/X
Shadow copy	This option will make use of a shadow copy of the source folder to circumvent errors resulting from locked files. This option only supports local files and folders as the source. Remote UNC paths and connected network shares are not supported.	/ShadowCopy
Inherit rights from destination	Enabling this option prevents security information from being copied. Instead the copied files inherit the security information from the destination folder(s).	/Z
Copy users	Enabling this option causes CopyRight2 to automatically copy users not existing at the destination. The password of the created user is empty initially and needs to be set by the administrator. This is the reason why the newly created user is created in a deactivated mode and needs to be activated by the administrator before it can be used. If you use this option in combination with the option “Synch. users and groups created“ the attributes of users in the destination will be synchronized with those of the source environment.	/CU
Local groups	Enabling this option causes CopyRight2 to automatically copy local groups not existing at the destination. If you use this option in combination with the option “Synch. users and groups created“ the attributes of groups in the destination will be synchronized with those of the source environment.	/CL
Global groups	Enabling this option causes CopyRight2 to automatically copy global groups not existing at the destination. If you use this option in combination with the option “Synch. users and groups created“ the attributes of groups in the destination will be synchronized with those of the source environment.	/CG

Synch. users and groups copied	This option affects the options “Copy users”, “Local groups” and “Global groups”.	/CU+ oder /CL+ oder /CG+
Map security identifiers of local groups and users on the source computer automatically to identically named local groups and users on the destination computer	This option automatically assigns users and groups used within security permissions that do not exist or cannot be resolved within the destination environment, to identically named users or groups.	/M
Map security identifiers with a predefined mapping table	This option reassigns automatically reassigns permissions according to a previously created mapping file that assigns user and groups of the source domain to user and groups of the destination domain. How to create such a mapping file is described later in detail.	/G:<Datei.Map>
Continue process if encountering not existing or not resolvable security identifiers	Enabling this option forces the copy process to continue, if encountering errors caused by not existing or not resolvable user and group accounts.	/A
Overwrite existing files	This option causes existing files to be overwritten automatically without the users confirmation.	/O
Overw. r/only files	This option causes existing, write protected files to be overwritten automatically without the users confirmation.	/W
Ignore errors and continue processing	This option forces the copy process to continue even if errors of any kind are encountered.	/I
Create a log file	This option enables a log file to be created.	Corresponds to the option /R in combination with a redirection of the command’s output by adding “>Logfile.Txt“ to the command.

Reassigning permissions (ReAcling)

CopyRight2 can reassign the permissions of existing data without actually copying files. For this purpose, a mapping definition file has to be created as described earlier.

To begin reassigning permissions, use the Windows Explorer select the folder where you want to start the process at. Open up the context menu by clicking the right mouse button while the folder is still selected. Run the command "ReAcl with CopyRight…" from the menu shown.

During this process all users and groups contained in permissions will be changed according to the predefined mapping definition file.

You can use this option…

- …during a two-phased migration. Within the first step all the data is copied from the source to the destination without changing any permissions. During the second step the permissions are changed by using a mapping file.

- ...during domain migrations. You can use a mapping definition file to assign groups and users from the source domain to groups and users from the new destination domain. When all the accounts of the source domain have been replaced, the source domain can be removed by uninstalling this domain's domain controllers.

Enable Backup / Restore Privilege for Windows Explorer

If the current user account has been granted the backup and restore privilege either locally or on the domain controller level (in case of a domain controller), you can enable and disable this privilege for the currently running instance of Windows Explorer. Any local or domain administrator accounts have this privilege granted by default. Enabling the privilege gives you the opportunity to traverse through paths that normally would deny any access in order to pick a source or destination for a "Paste with CopyRight…" operation. After the privilege has been used, you can disable it again.

Using a DFS Server to Maintain the existing UNC Namespace

CopyRight2 supports the use of a Microsoft DFS (Distributed File System) server to maintain the existing UNC client namespace.

You can use CopyRight2 to create DFS links of an existing server's shares. By creating a DFS namespace beginning with the '#' character and by setting a certain registry value the server will serve NetBIOS requests for the old server name. This requires of cause that the old server has been renamed because otherwise a NetBIOS name conflict would be the result. You prepare the DFS namespace in advance of your migration to point to the old server's replacement name.

Using DFS differs depending on whether your DFS server runs in a cluster or not.

After you have created the DFS namespace you can create CopyRight2 copy jobs using the "Update DFS" option to update the DFS links after a share was successfully migrated to a new location.

Please note: Any persistent share mappings that users have created manually (for example using explorer with the "Restore this connection" option), will have to be reconnected manually. Shares mapped with logon scripts for example are not affected by this Microsoft limitation.

Please note: The server running the DFS server cannot be a domain controller. Furthermore, the source server cannot be a domain controller as well. Please move the domain controller role to another computer in this case.

Please note: There is a DFS client cache timeout that can be configured on your DFS server using the DFS management snap in. The default value of 30 minutes can be lowered to a more reasonable value during migration. This is the amount of time it can take until a client "sees" a share actually in its new location.

Non Clustered DFS Server

1. Install a server running the "File Services" role. Please do not install the "Domain Controller" role!

2. Install the "Distributed File System" role service by using the Server Manager. DFS Replication is not required. During the installation you will be asked if you want to create a namespace, please choose to create a namespace later.

3. Create a "DFS Copy Job" to migrate all or specific shares of your source server(s) to your DFS server. You can use the default option that applies a suffix of "-RT" to the server name pointed to by the DFS links.

4. Rename the old file server into the name specified by the "DFS Copy Job". If you specified a suffix of "-RT" you would append "-RT" to the existing computer name. To change the computer name, open up the start menu, then open up the computers context menu by clicking on the right mouse button. Next choose "Properties" from the context menu. Finally select "Change Settings" to open up a dialog where you can modify the computer name. Please note that you might need a domain administrator's username and password to rename the computer in the domain. Reboot the computer after its name has been changed.

5. Open up regedt32 on the DFS server and go to the registry key "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Dfs\Parameters\Replicated" and add a new

DWORD value with the name “ServerConsolidationRetry”. Set it to a value of 1. You can optionally set the value “LogServerConsolidation” to a DWORD of 1 to enable referral logging, which will cause every redirection to be written to the event log.

6. Please make sure that your DFS server has DNS automatic updates enabled for its network adapters. Otherwise you might have to update your DNS servers manually to point to the replacement server.

7. Open up regedt32 on the DFS server and go to the registry key “HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Dnscache\Parameters”. Add a new registry value with the name “AlternateComputerNames” of the data type “Multi-String Value”. In the value data box, type the fully qualified DNS names of your old server(s).

8. Run the command “ipconfig /registerdns” on the DFS server from a command prompt. This will register the defined server names within DNS.

9. Open up regedt32 on the DFS server and go to the registry key “HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters”. Add a new value “OptionalNames” of type “Multi-String Value”. In the value data box, type the NetBIOS names of the older servers each on their own line. Then click on OK. This value will cause a registration of the server names within WINS upon Server Service restart.

10. Restart the Server Service on the DFS server.

At this point in time accessing file share data using the existing UNC namespace should work and the share by share migration can begin.

To roll back the server name change, please follow the steps below:

1. On your DFS server, remove the old server’s name from the registry value “HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Dnscache\Parameters\AlternateComputerNames”

2. On your DFS server, remove the old server’s name from the registry value “HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters\OptionalNames”

3. Restart the Server Service on the DFS server

4. Rename your old server back to its original name and reboot.

Clustered DFS Server

1. Make sure that your cluster nodes have the “File Service” role installed. Make sure that your cluster nodes are not running the “Domain Controller” role.

2. On each node install the “File and Storage Services” -> “File and iSCSI Services” -> “DFS Namespaces” role (“Distributed File System” on pre Windows 2012) by using the Server Manager. DFS Replication is not required.

   Note: During the installation you will be asked if you want to create a namespace if installing on pre Windows 2012, please choose to create a namespace later.

3. Use the Cluster Administrator to create a “DFS Namespace Server” resource. You can enter any cluster resource and namespace name you like for example “Namespace”. This resource and namespace will not be used for the share-by-share migration. If you want to use the cluster beyond that purpose, you may want to provide names that make sense in your environment. You may change the DFS cluster resource and the namespace name at a later time as well. Please note that the “DFS Namespace Server” will require a cluster volume to store the DFS shares.

4. On the node that currently owns the DFS Namespace Server, open up regedt32 and go to “HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Dfs\Parameters\Replicated” and add a new DWORD value with the name “ServerConsolidationRetry”. Set it to a value of 1. You can optionally set the value “LogServerConsolidation” to a DWORD of 1 to enable referral logging, which will cause every redirection to be written to the event log.

5. The next step requires use of the “Cluster.Exe” management tool. On Windows 2012 and newer, this tool is not installed by default. To install it, use the following PowerShell command on the node that currently owns the DFS Namespace Server:

   ```
   Install-WindowsFeature –name RSAT-Clustering-CmdInterface
   ```

6. Next open up a command prompt on the node that currently owns the DFS Namespace Server and run the command

   “cluster res <DFS Namespace Server Name>
   /addcheckpoints:System\CurrentControlSet\Services\Dfs\Parameters\Replicated”.

   Please replace <DFS Namespace Server name> with the name of the namespace server you created in step 3.

   Adding the checkpoint will make sure the required registry values get transferred if the “DFS Namespace Server” is moved from one cluster node to another.

7. Create a “DFS Share Consolidation” job to migrate all or specific shares of your source server(s) to your DFS server. You can use the default option that applies a suffix of “-RT” to the server name pointed to by the DFS links.

8. Rename the old file server into the name specified by the “DFS Share Consolidation” job. If you specified a suffix of “-RT”, you would append “-RT” to the existing computer name. To change the computer name, open up the start menu, then open up the computers context menu by clicking on the right mouse button. Next choose “Properties” from the context menu. Finally select “Change Settings” to open up a dialog where you can modify

the computer name. Please note that you might need a domain administrator's username and password to rename the computer in the domain. Reboot the computer after its name has been changed.

9. Use the cluster administrator to add a "Client Access Point" to the DFS server using the original server's name.

10. Use the cluster administrator to bring the "DFS Namespace Server" and the "Client Access Point" online.

At this point in time accessing file share data using the existing UNC namespace should work and the share by share migration can begin. You can test if the failover works at this point in time.

To roll back the server name move use the following steps:

1. Use cluster admin to delete the client access point ("Server Name") using the original server's name.

2. Delete the computer account for the original file server's name, created by cluster services, in your Active Directory. This computer account has a description of "Failover cluster virtual network name account" and should be a deactivated account at this point showing a down pointing arrow in the "Active Directory Users and Computers" snap-in.

3. Rename your old server back to its original name and reboot. This step will create a new computer account in the Active Directory domain.

Using SID-History for Active Directory Migrations

CopyRight2 supports Windows sidHistory attribute to migrate users and security groups between Active Directory domains in different forests (inter-forest migration) or between domains in the same forest (intra-forest migration).

Using the sidHistory attribute will allow migrated users and members of migrated groups to access data that grants permissions to the original source account. This feature disconnects the Windows account migration from the migration of resources, such as file sharing or mailboxes and also from the rollout of new workstation PC.

Inter-forest SID-History Migration Requirements

Please carefully read about the sidHistory requirements documented below. After these requirements are met, a migration of user or group accounts having sidHistory enabled will succeed without errors and migrated accounts will have the original accounts SID added to their sidHistory attribute.

Note: Built-in domain accounts, including Domain Admins, Domain Users, Domain Computers, Domain Controllers, and Domain Guests, do not support SID-History. This behavior is defined by Windows and is not specific to CopyRight2. To translate these accounts correctly, a separate mapping must be defined in a mapping file.

Trust, Special Local Group & Auditing

Before sidHistory can be used to migrate between two domains residing in two different forests, the following list of requirements has to be fulfilled:

1. The source domain has to trust the destination domain, allowing accounts from the destination domain access to resources still located in the source domain.

2. Create a local group in the source domain having the NetBIOS domain name as group name with 3 dollar signs appended. If the NetBIOS domain name of the source domain would be “Contoso”, you would have to create a domain local group called “Contoso$$$”. Note: Do not add any members to this group, otherwise sidHistory migration of accounts will fail.

3. Enable auditing of account management in the source and the destination domain (part 1).

   On Windows 2008 (and newer) You can do so by starting the “Group Policy Management” from “Administrative Tools”. Next navigate to the node “Forest” -> “Domains” -> “Your Domain Name” -> “Domain Controllers” -> “Default Domain Controllers Policy”, right click on “Edit”. In the “Group Policy Management Editor” navigate to “Computer Configuration” -> “Policies” -> “Windows Settings” -> “Security Settings” -> “Local Policies” -> “Audit Policy”.

   On Windows 2003 you can do so by starting the “Domain Controller Security Policy” from “Administrative tools. Next navigate to the node “Security Settings” -> “Local Policies” -> “Audit Policy”

4. Enable auditing of account management in the source and the destination domain (part 2).

Now right click on “Audit account management” in the details pane to the right side and then click on “Properties…”. Now click on “Define these policy settings” and then click on “Success” and “Failure” and confirm the settings by clicking on “Apply” and then on “OK”. In the details pane, right click on “Audit Directory Service Access” and then click on “Properties…”. Click on “Define these policy settings” and next on “Success”. Again click on “Apply” and “OK” to confirm the settings. If you don’t want to wait until the changed settings are replicated, you can use the “gpupdate /force” command to enforce updating the GPOs.

Advanced Auditing

If your source or target domain should have used Advanced Auditing in the past, introduced with Windows Server 2008, you may still receive an error indicating that auditing in the source or target domain is not enabled even though you followed the steps above.

If this is the case additionally:

1. Navigate to “Computer Configuration” -> “Policies” -> “Windows Settings” -> “Security Settings” -> “Advanced Audit Policy Configuration” -> “Audit Policies” -> “Account Management” and enable all subcategories for success and failure auditing.

2. Navigate to “Computer Configuration” -> “Policies” -> “Windows Settings” -> “Security Settings” -> “Advanced Audit Policy Configuration” -> “Audit Policies” -> “DS Access” and enable all subcategories for success auditing.

Source Domain Controller

While adding sidHistory, the process will automatically communicate with the PDC emulator of the source domain, so it is not a requirement to specify this domain controller.

Please specify a source domain controller that is “near” the computer running the migration job for optimal performance.

Security Context Requirements

The Windows sidHistory API requires the “Migrate SID history” permission in the target Active Directory. This permission is granted by default to the “Domain Admins” and “Enterprise Admins” groups. You could either make the account a member of one of those groups or alternatively grant the “Migrate SID history” permission. Granting the permission works with a standard Domain User account, assuming it has been delegated the “Create, delete and manage users” and/or “Create, delete and manage group” on the corresponding target OU.

Since build 657, you do not necessarily need “Migrate SID history” in the target domain if you configure the sidHistory proxy functionality (see below for more information).

It is best practice to use an account of the target domain, that has been made a member of the source domain's Administrators group.

You can use this account of the target domain to logon to systems in the source and in the target domain, due to the trust established between source and target domain. That means you can either run it in a push configuration from a system in the source domain or in a pull configuration on a system in the target domain.

Naming Resolution

The target DC needs to be able to resolve the computer name of the source domain controller. You can either work with a DNS conditional forwarder in the target domain, that forwards requests for the source domain to a DNS server of the source domain or alternatively use an LMHOSTS file.

When sidHistory is added using the corresponding Windows API, an RPC call will be issued to the target domain controller. The target domain controller will then communicate with the specified source domain controller, requiring naming resolution to work properly. An access denied error can occur if the naming resolution does not work while adding sidHistory.

The creation of a trust between the source and the target domains requires the source domain's DNS servers to be able to resolve names of the target domain. Please set up a conditional forwarder in the source domain as well, forwarding requests for the target domain to a DNS server of the target domain.

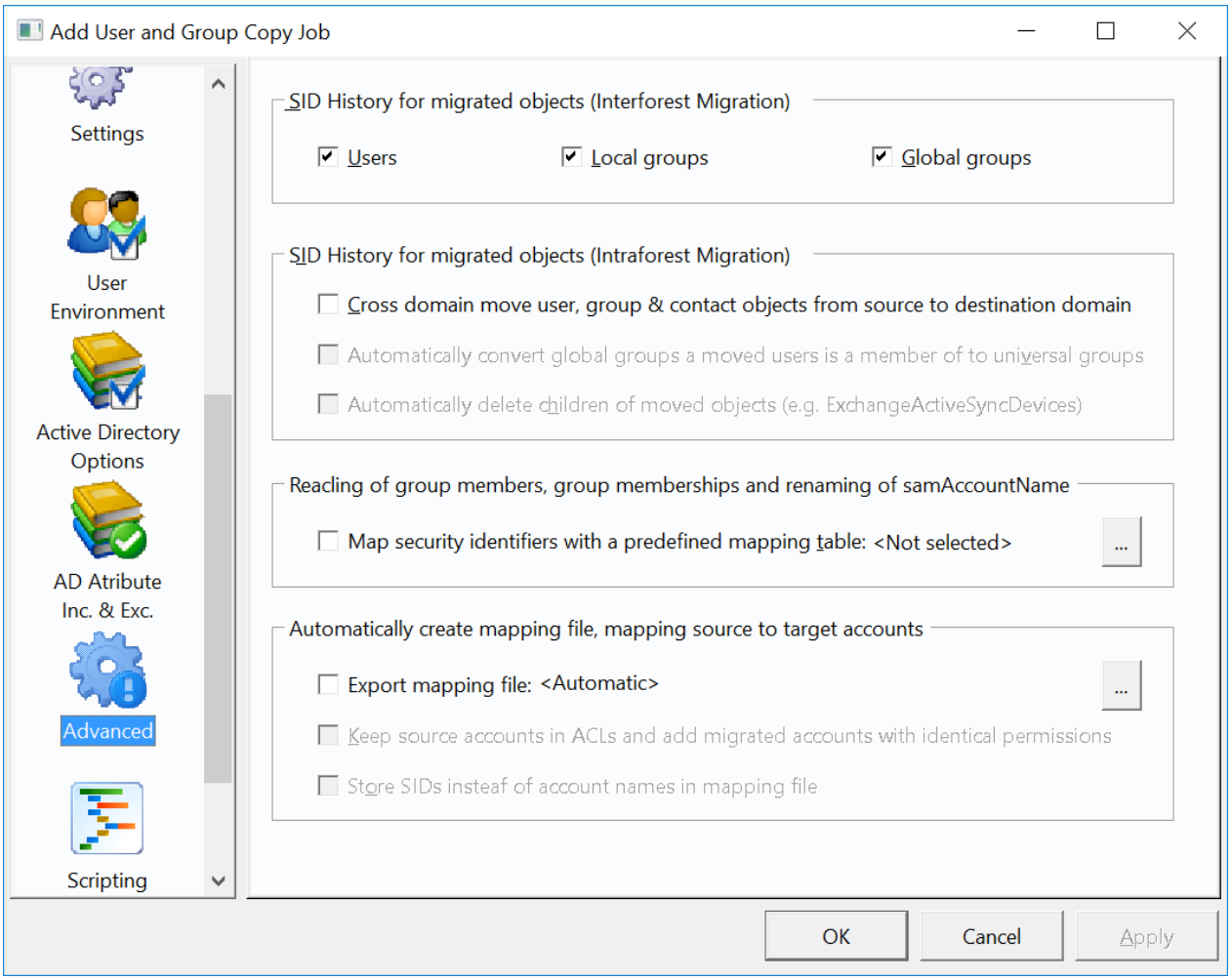
Using SID-History in User and Group Copy Job

After the requirements for sidHistory migrations have been met you can enable the corresponding option of the CopyRight2 job depending on the type of migration you want to perform.

Inter-forest SID-History Migration (Different Forests)

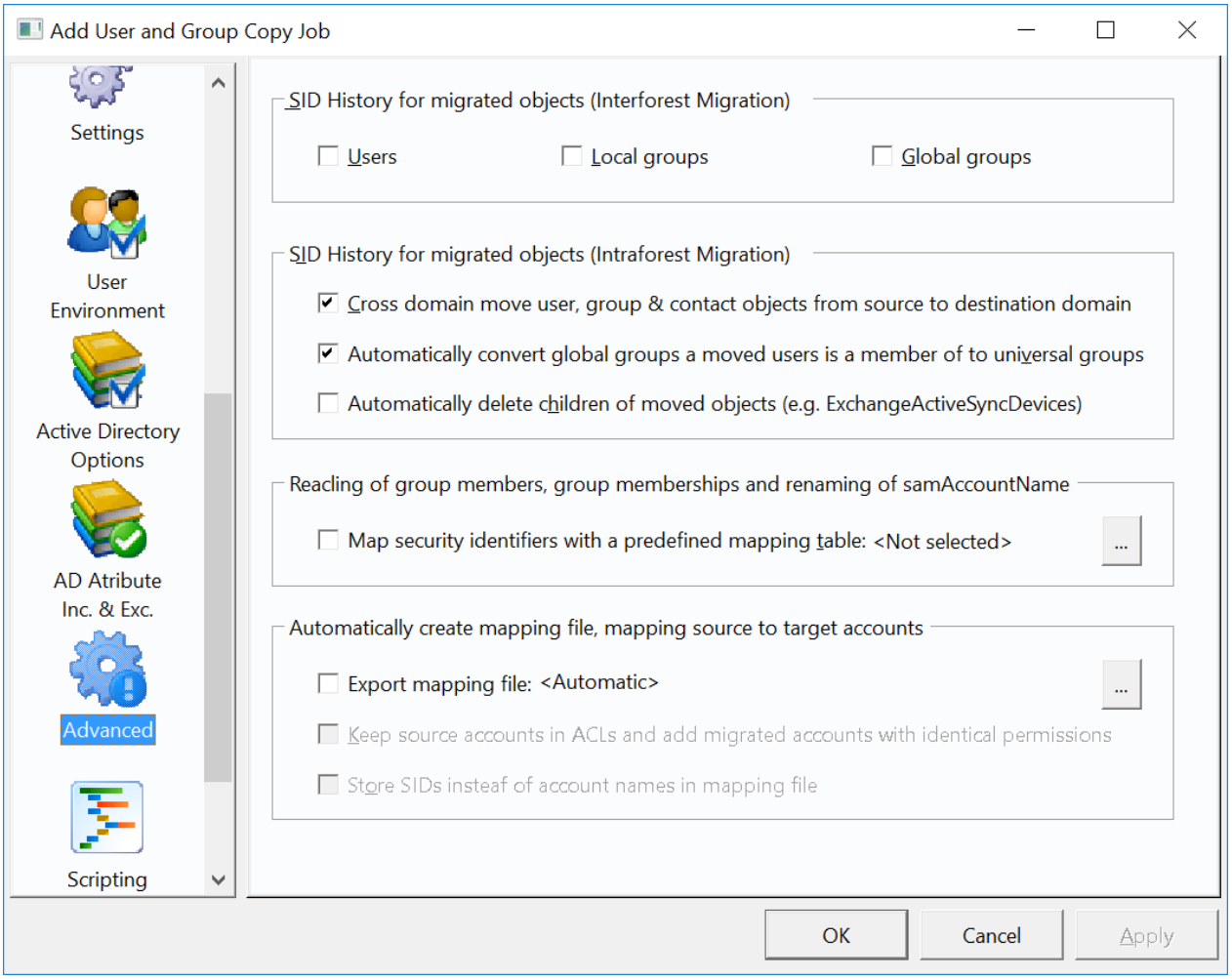
In case of an inter-forest domain relationship, where the two domains reside in different forests, you can copy existing accounts from the source domain to the destination domain.

To add the original SID to migrated user and group objects sidHistory attribute, please enable the following option for users and/or group accounts:



Intra-forest Domain sidHistory Migration (Same Forest)

In case of an intraforest migration, where the soure and the destination domain reside in the same forest, you can use the „Cross domain move“ option instead to move the account from the source domain to the destination domain. In case of both domain residing in the same forest it is not possible to copy the source accounts, because one requirement of a domain forest is, that accounts have unique SIDs, uniquely identifying accounts within the forest. You can enable a cross domain move by enabling the “Cross domain move” option below:



Important: Please note that in case a moved user object is a member of a global group of the source domain and that global group is not getting migrated (yet), the user cannot remain a member of that group without converting it into a universal group. This is due to the restriction that global groups can only contain members of the domain the group resides in. You can automatically convert such groups into universal groups by enabling the “Automatically convert global groups” option. Furthermore, it needs to recursively convert any other global groups that the group in question is a member of in case you are using nested groups.

Disabling SID Filtering for Inter-Forest Domain Migrations

To allow migrated accounts access to resources still residing in the source domain, the SID filtering settings have to be adjusted before access is granted. This step differs slightly, depending on whether a domain trust or a forest trust is used between the source and the destination domain.

In case of a domain trust, execute the following command on the destination domain's PDC to disable SID filtering (Please replace SourceDomainName with the source domain's NetBIOS name, DestinationDomainName with the destination domain's NetBIOS name and "***" with the password of the Administrator account in the source domain):

```
Netdom trust SourceDomainName /domain:DestinationDomainName /quarantine:no
/Usero:SourceDomainName\Administrator /Passwordo:***
```

In case of a forest trust, execute the following command on the destination domain's PDC instead to disable SID filtering:

```
Netdom trust SourceDomainName /domain:DestinationDomainName
/enableSIDhistory:yes /Usero:SourceDomainName\Administrator /Passwordo:***
```

Note: If you are using a localized version of Windows, you may need to replace the "no" or "yes" parameter with the corresponding word translated to that language. To enable SID-History for a forest trust on a German Windows version, you may need to replace "/enableSIDhistory:yes" with "/enableSIDhistory:ja" for example in order for the command to succeed.

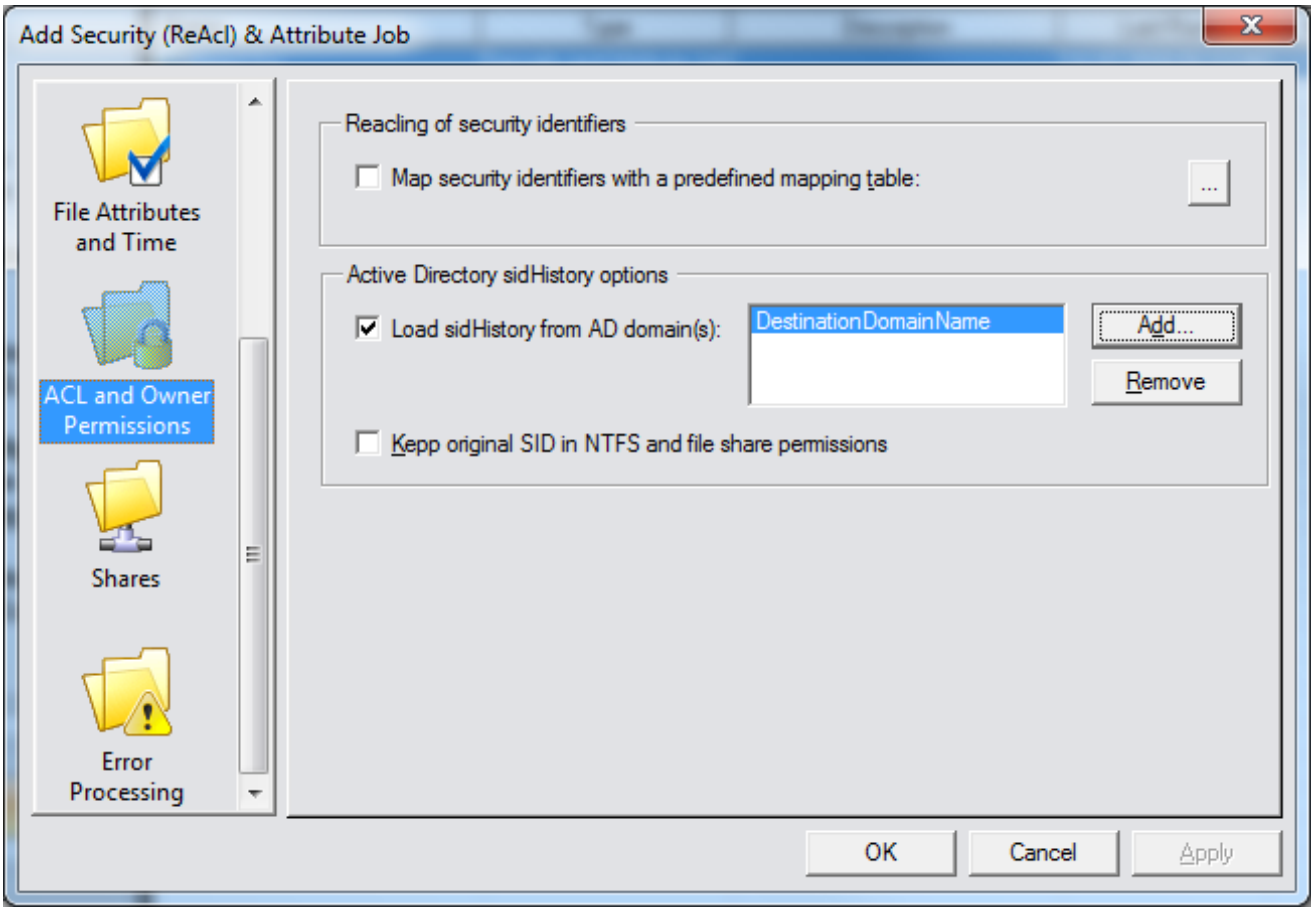
Note: Disabling SID filtering requires a level of trust between the source and the destination domains. With SID filtering disabled it is possible for a domain administrator of the destination domain, even without being a member of the source domain's administrators group, to "clone" an existing SID from the source domain and add it to an existing account of the destination domain, to gain access to any data still residing in the source domain. Disabling SID filtering is basically identical to adding the administrators of the destination domain to the administrators group of the source domain. If this would happen anyways, or if the source and destination domain are administered by the same administrators or if all the data from the source domain should be migrated to the destination, this is not of concern.

Note: Please mind that after April 2026, Microsoft disabled the RC4 Kerberos encryption type. If your migrated user only has an NT hash, you will need to use the "Must Change Password" option, to force the user to generate AES keys during first logon in order for SID-History access to work, as the source domain most likely has RC4 disabled as well, Alternatively, you can use the password synchronization method to migrate user passwords in advance (see "**Password Synchronization & Migration Add-On Manual**") working completely RC4 free and not requiring any other weakening configurations on domain controllers.

SID-History Clean-Up After Migration

SID-History is meant as a temporary solution during migrations. The fact that a user account possesses multiple SID's may cause problems with Windows built-in administration tools as well as 3rd party software. After the account and the resource migration have been completed, the resource permissions should be cleaned up (for example by using a CopyRight2 Security and Attributes job), replacing any occurrences of old SIDs with the SIDs of the migrated accounts. Once all the resource permissions have been cleaned up, the sidHistory attribute of migrated user and group accounts can be emptied because it is no longer used.

You can use the following option of a "Security and Attributes" copy job to clean-up NTFS and share permissions, adding the NetBIOS name of the destination domain or a domain controller of the destination domain:



Setting this option causes CopyRight2 to retrieve a mapping of old SIDs to new SIDs from the specified domain(s) when the job starts, to replace any occurences in NTFS or file share permissions accordingly. You can optionally keep the original SID in permissions, effectively adding the SID of the migrated accounts with identical permissions.

Computer and User Profile Migration

Using the Graphical User Interface

You can perform computer and profile migrations graphically by defining a Computer and Profile Migration job.

This job type provides you with the ability to migrate profiles existing on remote computers, being associated with an account from the source domain, to be usable by an account that has been previously migrated to the target domain or Microsoft Entra.

It is possible to migrate profiles for user accounts that have been migrated with sidHistory and without sidHistory.

CopyRight2 supports migrations of computer accounts and profiles within the same or across different Active Directory forests.

You can find an explanation of the possible settings in the chapter “Adding or Editing a Computer and Profile Migration Job”.

You can run the job in simulation mode, configurable on the Name page of the job’s settings. If run in simulation mode the job will not apply any changes to the remote client but instead simply collect information about the user profiles found locally.

Note: It is required to run the job from a system in the source domain if it is an interforest migration (across forest boundaries), if the target domain does not trust the source domain. If the target domain trusts the source domain or it is an intra-forest migration (same forest, implying a trust), the location where you run the job, does not matter.

Configuring the Computer Connection Point and Other Options

Before you can run the job, you will need to ensure that a computer connection point has been configured under Menu -> Options -> Computer and Profile Migration -> Computer connection point. You can find more information about configuring the computer connection point in the chapter “Configuring the Computer Connection Point”.

In case you are performing an inter-forest migration and the target domain does not trust the source domain, it is required to install the RPC service under Menu -> Options -> RPC Service. You will need to provide a domain user account of the source domain that is a member of the local Administrators group on the remote computers. This context will be used to join the remote computers to the target domain.

Note: If the target domain trusts the source domain or if it is an intra-forest migration (same forest, implying a trust), you can configure the CPM$ share to grant permissions to the Domain Computers group of the source domain in order to allow status and log file uploads shown in the GUI.

Migrating from a Synology Directory Server Domain

If you want to migrate from a Synology Directory Server domain, not allowing trust relationships with Windows Active Directory domains, you will need to install the Sys-Manage CopyRight RPC Service on the system where you have installed CopyRight2 and the computer connection point (CPM$ Share).

Additionally, you will need to set the servicePrincipalName attribute of the user account being used to run the RPC Service and ensure it includes the value “cr2/FQDN-OF-CR2-SERVER” where you replace FQDN-OF-CR2-SERVER with the fully qualified DNS name of the server where you have CopyRight2 installed.

To set the attribute, you can either install Active Directory Management tools on a Windows system and use the graphical user interface or alternatively set it by command line as shown below where you would replace FQDN-OF-CR2-SERVER with the server’s FQDN name and DOMAIN\USER-ACCOUNT with the domain and user name of the account used to start the CopyRight RPC service:
Setspn -S cr2/FQDN-OF-CR2-SERVER DOMAIN\USER-ACCOUNT

You can use the command below to validate if the SPN has been set:
Setspn -Q cr2/*

After defining the SPN, please restart the CopyRight2 RPC service.

If the SPN is not defined, the Computer & Profile Migration agent, running on the client side, will fail to contact the RPC service as otherwise mutual Kerberos-based authentication will fail.

Creating a PPKG File with Microsoft Windows Configuration Designer

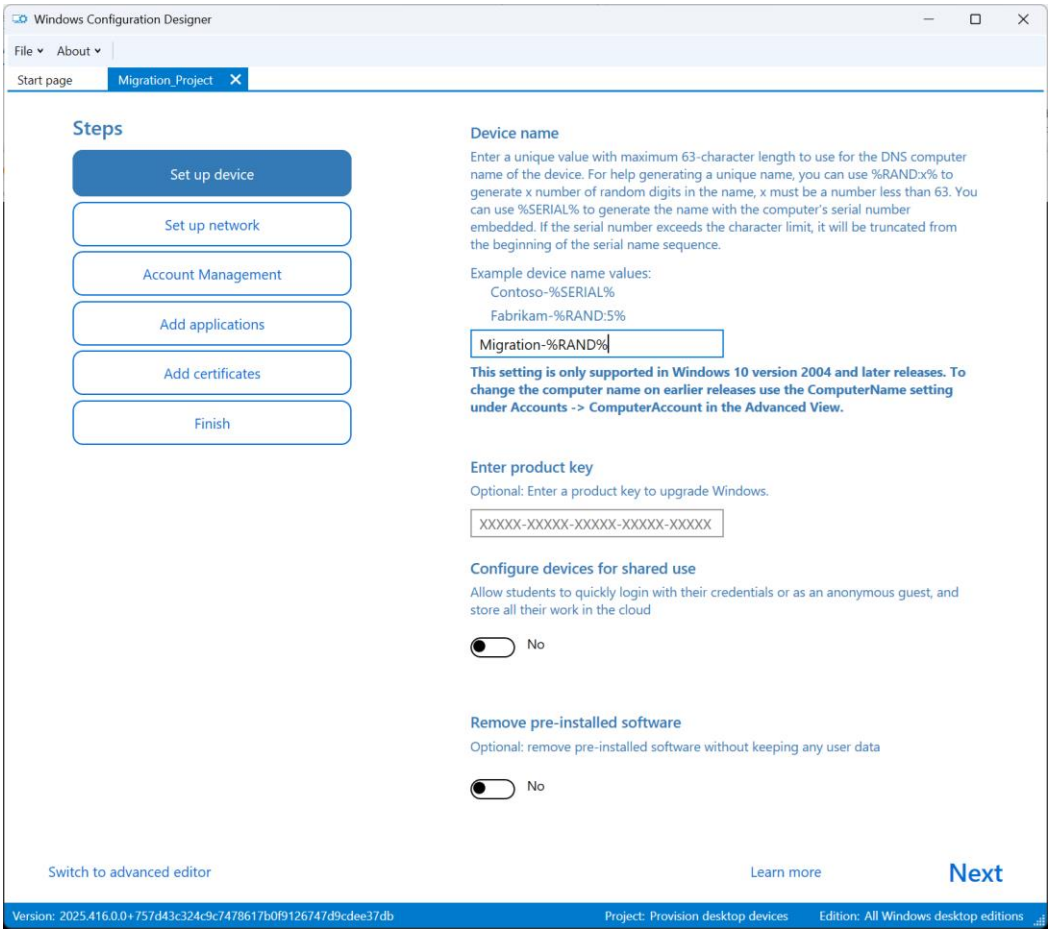
The Microsoft Windows Configuration Designer, which is available in the Windows store, allows the configuration of how an Entra device join should be performed. We will start with the Provision desktop devices wizard (the simple view) to acquire the bulk token, and then switch to the Advanced Editor to finalize the computer naming and disable Windows Hello.

Phase 1: Simple Wizard Setup

1) **Set up device**

   After launching Windows Configuration Designer and selecting **Provision desktop devices**, you are presented with the "Set up device" screen.

   - **Device Name:** Enter a temporary placeholder name (e.g., TempName-%RANDOM%). Unfortunately, filling out a device name pattern is strictly *required* in the simple view wizard to proceed, even if you intend to keep the existing computer name later.



2) Set up network

The wizard will next prompt you to configure wireless network settings.

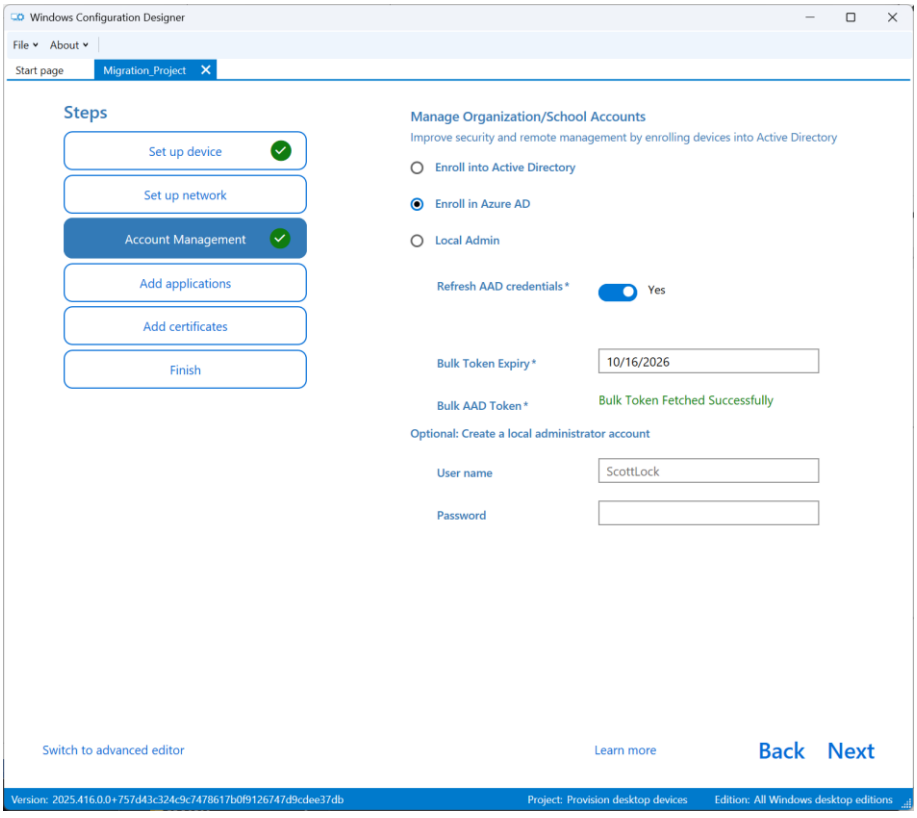
- Toggle **Wifi** to **Off**.
- *Important:* Only leave this on if you intend to explicitly configure wireless details. If the devices are connected via ethernet or you don't intend to force a Wifi join, you must turn this off to prevent the prompt from halting the deployment.

3) Account Management

This is where we link the package to your Entra ID (Azure AD) tenant.

- Select **Enroll in Azure AD**.
- Click **Get Bulk Token**.
- You will be prompted to authenticate. You must log on at least once with an account that has device enrollment permissions. At this stage, WCD contacts Entra ID to fetch and embed the bulk token into your project.

Note: During testing, you may find that you need to refresh AAD credentials and ensure the logon completes successfully before the "Bulk Token fetched successfully" confirmation appears.



Phase 2: Advanced Configuration

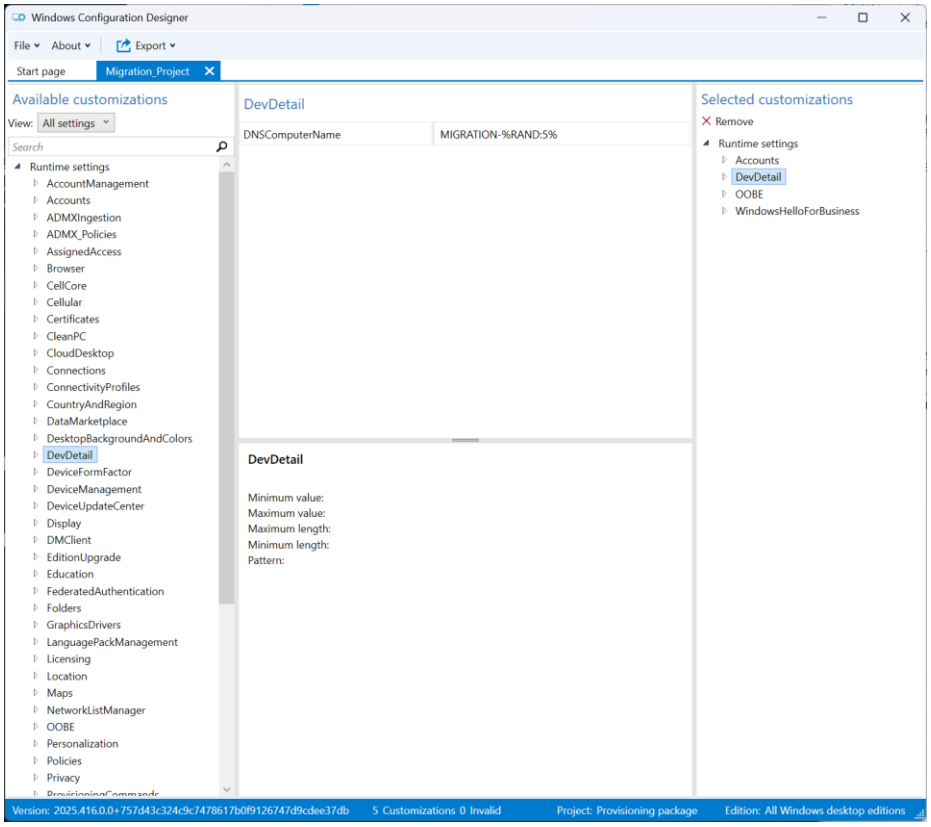
Because the simple view forces us to rename the computer, and doesn't expose Windows Hello settings, we must now convert the project to the Advanced Editor. At the bottom-left of the WCD window, click “Switch to advanced editor”.

Important note on switching views: Microsoft explicitly designed WCD so that switching to the Advanced Editor is irreversible. You cannot switch back to the simple view once you have converted the project. If you realize you made a mistake that requires the simple wizard, you will have to create a new project from scratch. WCD will display a permanent warning prompt to confirm before it converts the view.

4) Keep the Existing Computer Name

Now that we are in the Advanced Editor, we can remove the forced computer rename.

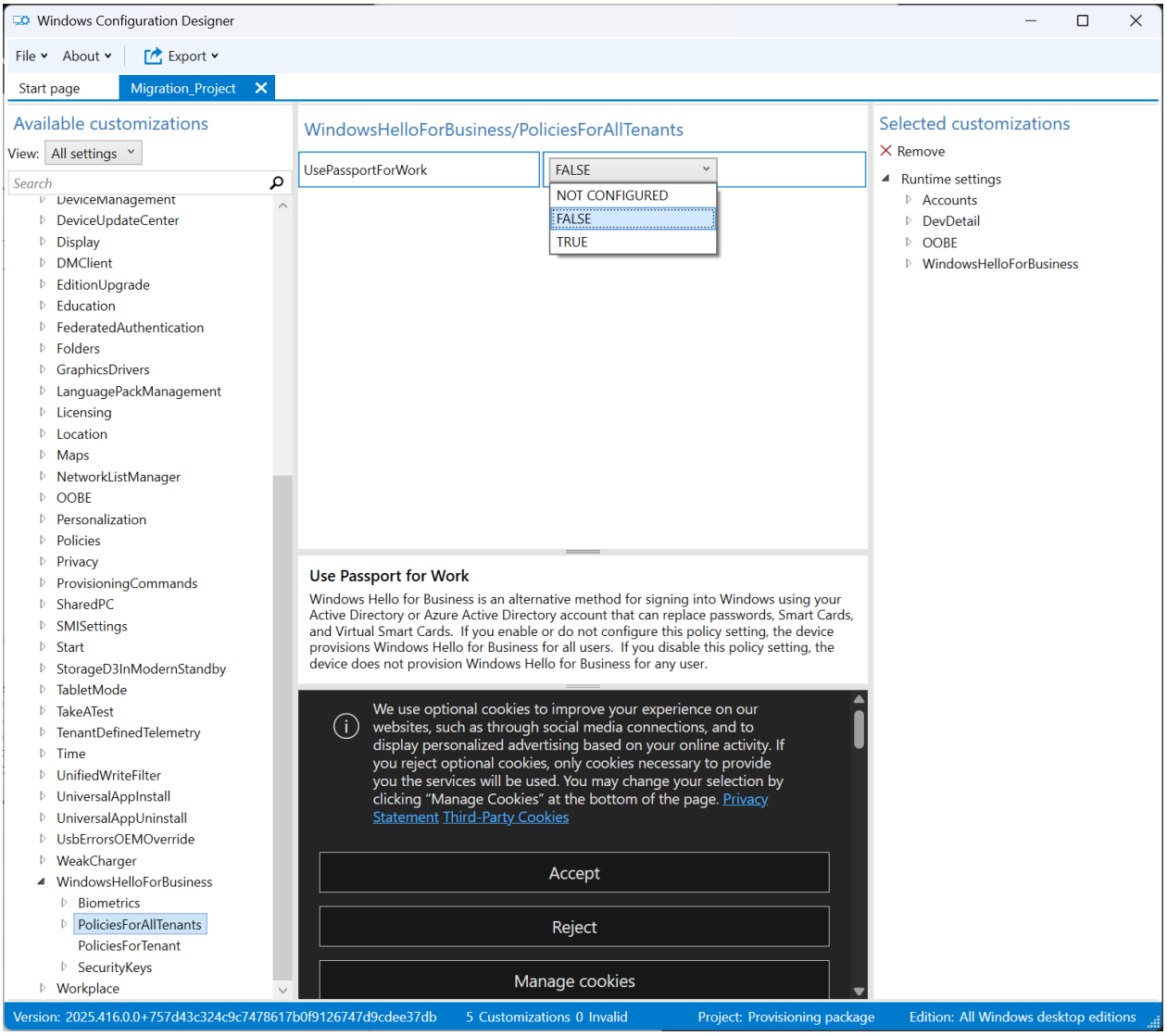
- In the left pane, navigate to **DevDetail**.
- In the right pane, locate the setting for **DNSComputerName** (which will contain the temporary name you entered in step 1).
- Clear or revert this field so it is no longer pushed by the package. This ensures the target computer simply keeps its existing name when the PPKG is applied.



5) Disable Windows Hello

To prevent users from being prompted to set up Windows Hello / PIN during their first logon after the migration, we will disable the Passport For Work policy.

- In the left pane, navigate to **WindowsHelloForBusiness** > **PoliciesForAllTenants**.
- Click on **UsePassportForWork**.
- In the middle pane, change the value from "Not Configured" to **False** (or Disable).



Once you are finished, click **Export** > **Provisioning package** in the top menu to build your final .ppkg file!

Configuring Authentication for Microsoft Entra Device Migrations

If you plan to migrate devices directly to Microsoft Entra (called Microsoft Entra joined) instead of performing a hybrid-join, where the computers are still joined to the on-prem Active Directory, you may need to configure additional options to allow the software to map profile owners accordingly.

Using a mapping file that contains Entra IDs (GUIDs) or properly translated Entra SIDs (beginning with a “S-1-12-1-“ prefix) does not require authentication.

If the mapping should take place automatically based on a match of the User-Principal-Name in the source Active Directory and Entra, or if the mapping file uses entries with the {Entra:User-Principal-Name} format, authentication is required.

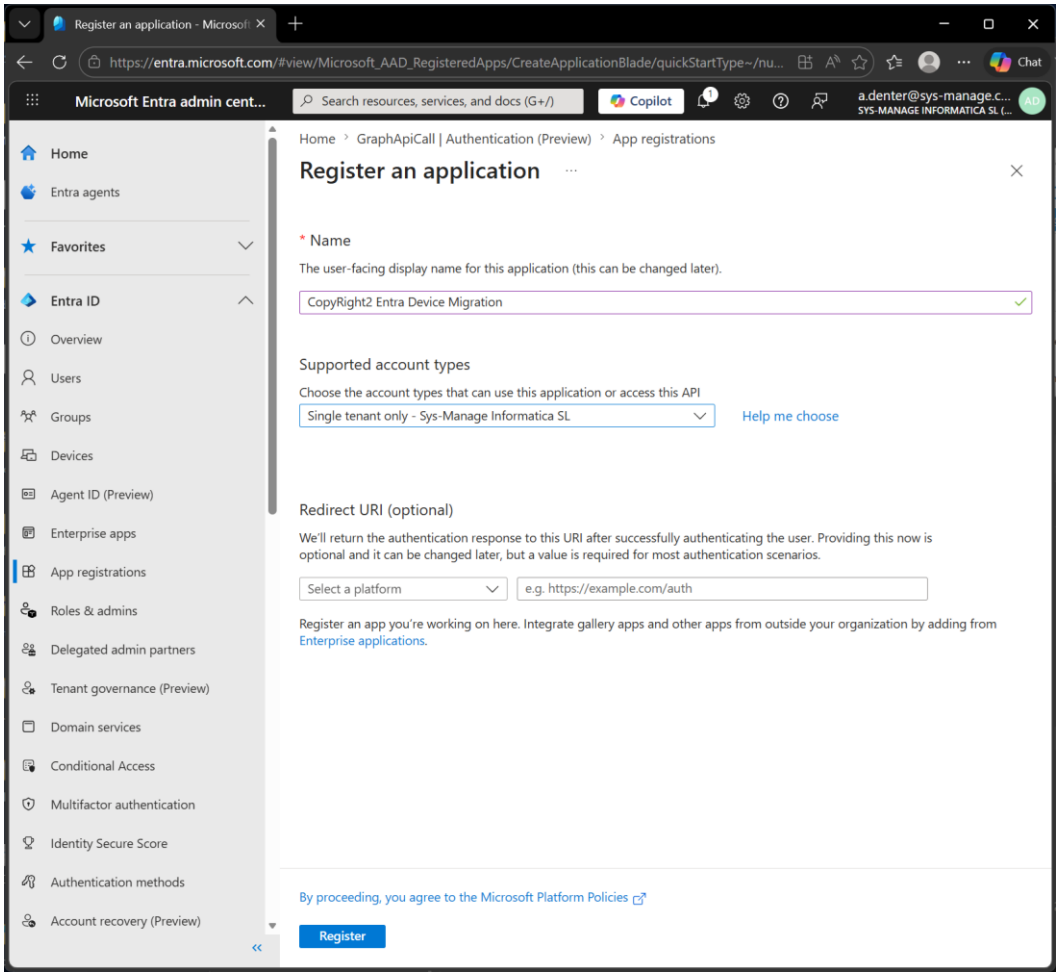
Please follow the steps below to configure authentication either using delegation (for interactive use) or client credentials (for background execution):

1) **Create the App Registration**

   First, we need to create the identity for the application in your tenant.

   - Navigate to the Microsoft Entra admin center and sign in with an administrator account.
   - Go to **Identity** > **Applications** > **App registrations**.
   - Click **New registration**.
   - Name the application (e.g., CopyRight2 Entra Device Migration).
   - Under **Supported account types**, choose **Accounts in this organizational directory only**.

- Click **Register**.



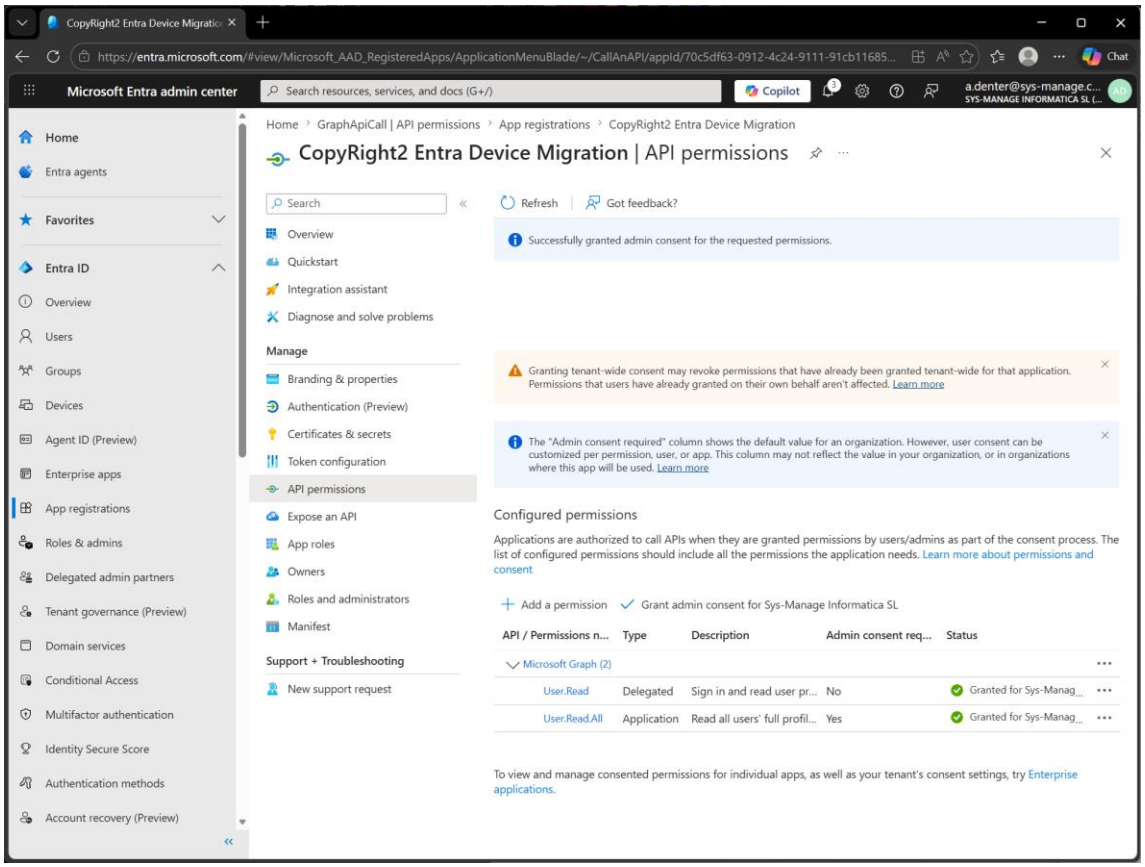
2) Assign API Permissions

The application requires the User.Read.All Application permission to query Graph.

- Go to **API permissions** in the left menu.
- Click **Add a permission** > **Microsoft Graph**.
- Click **Application permissions**, search for User.Read.All, and select it.

- Click **Add permissions**.

Important: Because this permission allows reading all user profiles, you must click the **"Grant admin consent for [Directory Name]"** button on this screen. Ensure the status column changes to green checkmarks.

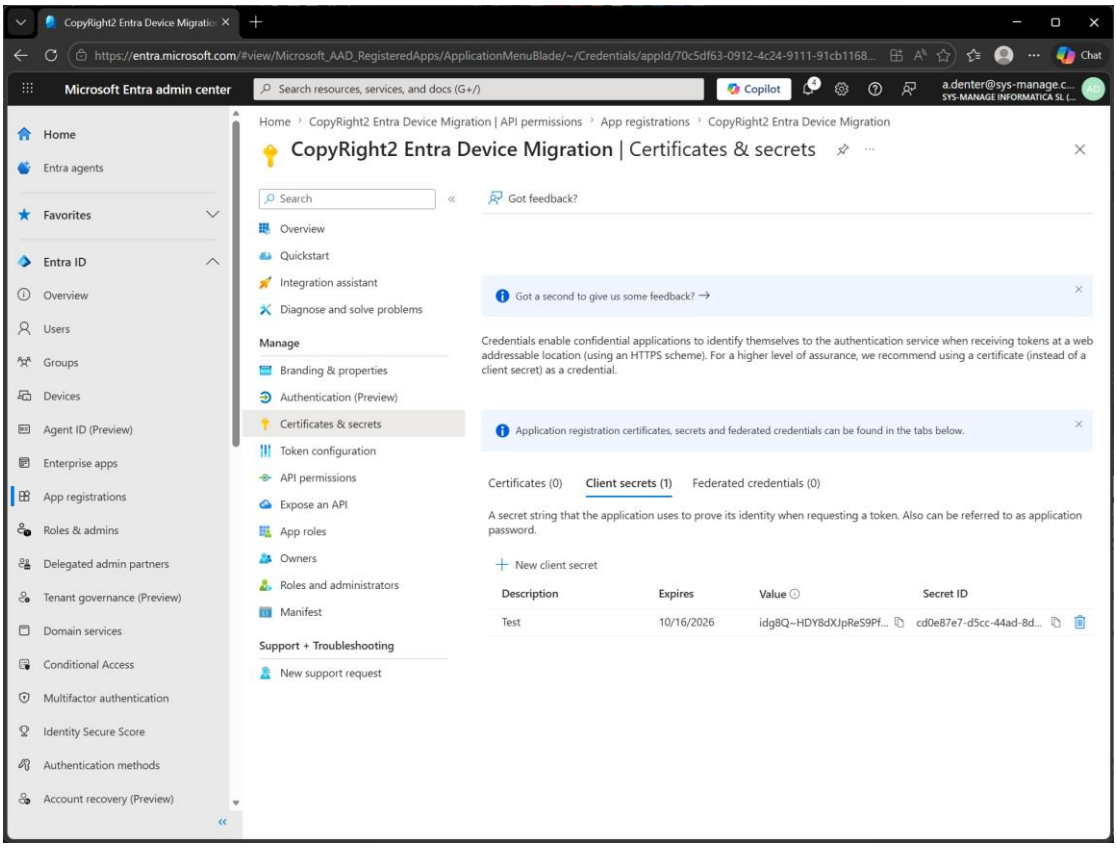


3) Generate a Client Secret

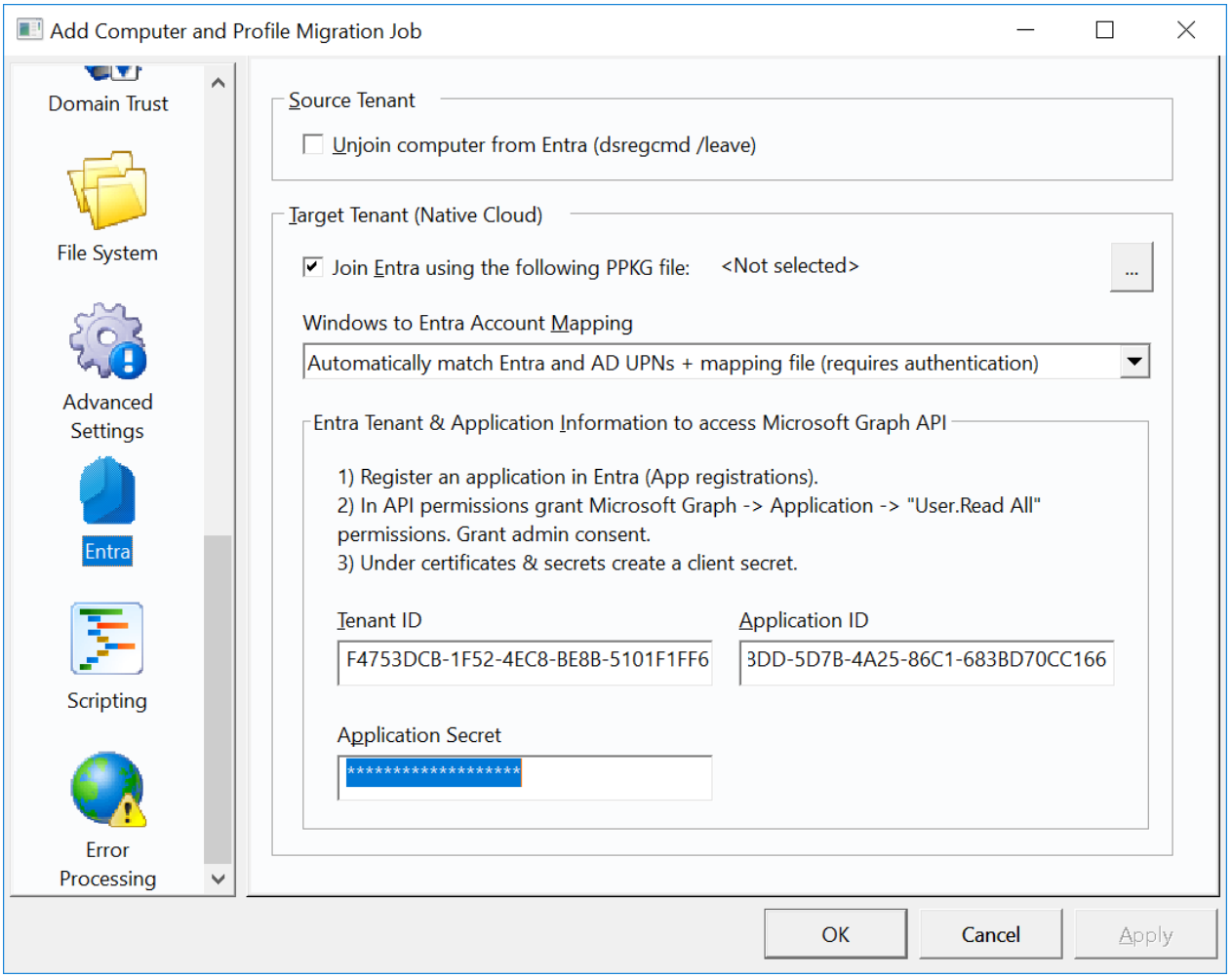
For the application to authenticate automatically, it needs a Client Secret.

- Go to **Certificates & secrets** in the left menu.
- Under the **Client secrets** tab, click **New client secret**.
- Provide a description (e.g., "Graph Access Secret") and choose an expiration duration.
- Click **Add**.

- **Copy the Secret Value immediately.** You will not be able to see it again after leaving the page.



- Paste the secret into the Application Secret field of your job settings.



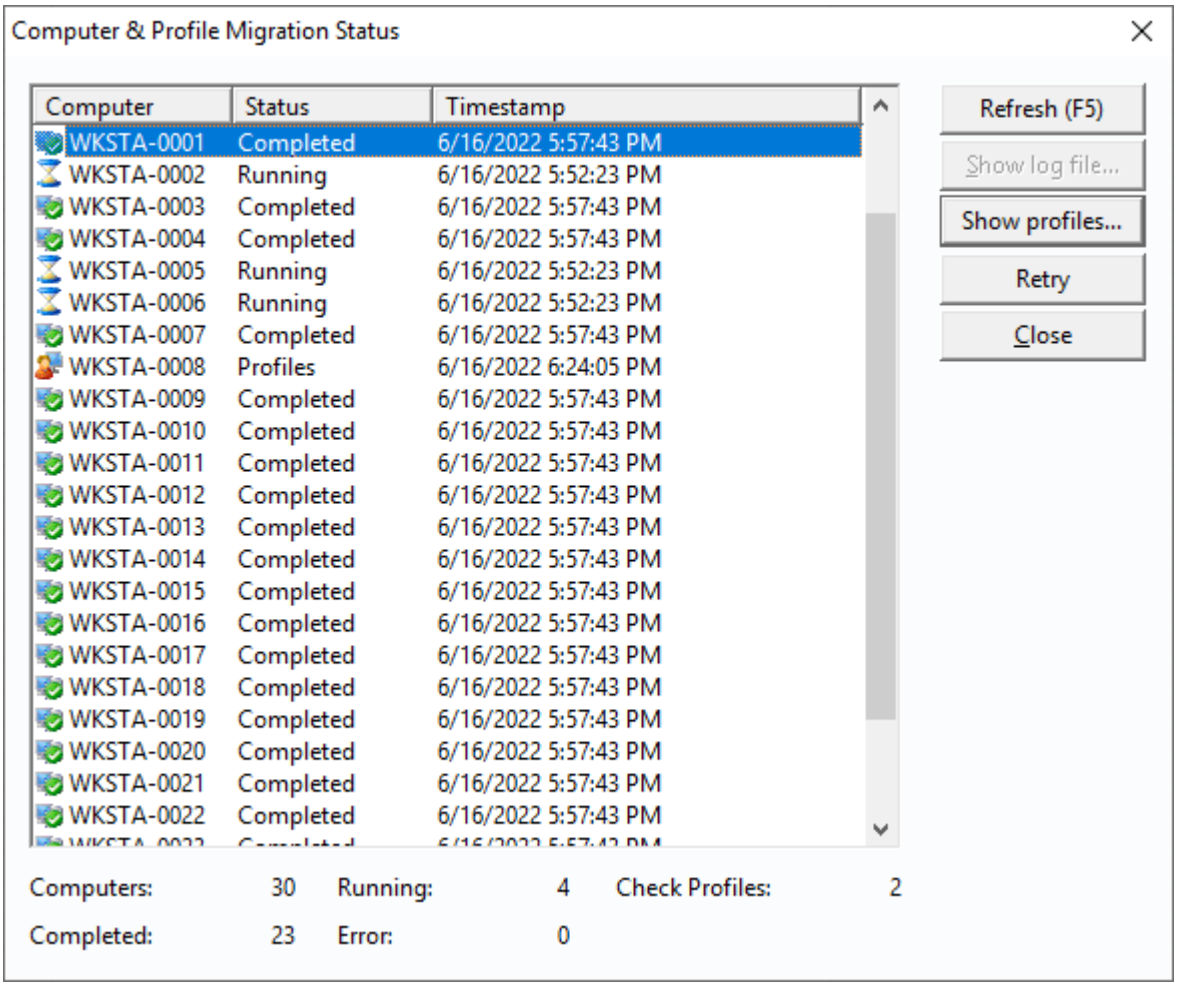
Running the Job

During job execution a service will be deployed onto the computers the job is targeting. It will be deployed to multiple computers in parallel. The maximum number of threads is configurable in Menu -> Options -> Computer and Profile Migration.

After the job has deployed the service to all computers you will receive feedback about whether it was successful or not. You can consult the jobs log file for details and statistics.

Tracking Execution Results

You can track each individual computer's status by selecting the corresponding job and then clicking on the View Job Status button. You should then see the following dialog:



You can see each computer targetted in the job along with its current status and some more statistics on the bottom of the dialog.

The status can be either:

Status	Description
Scheduled	Computer will be targeted during jobs next execution.
Running	Remote process is still active on remote computer.
Error	An error has occurred during remote execution.
Completed	The remote process has completed successfully.
Profiles	There are one or more profiles for users in the source domain that could not be found in the target domain.

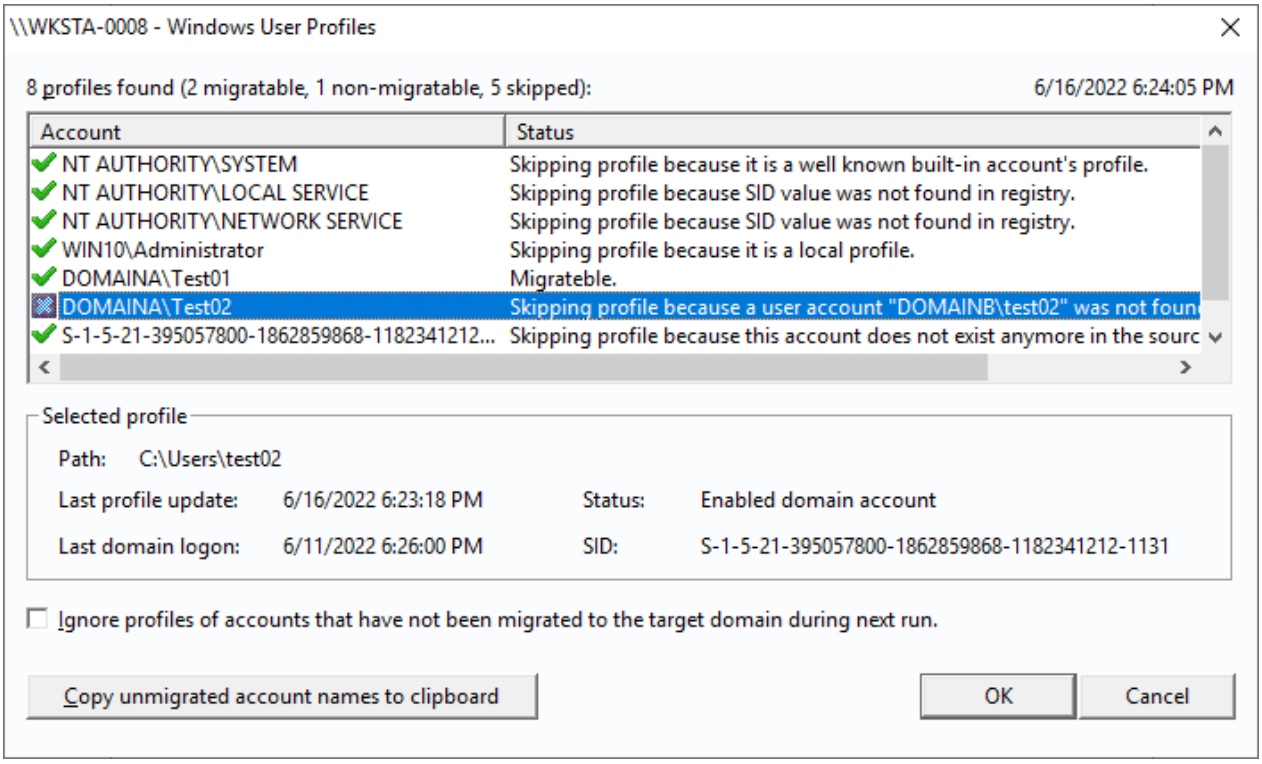
If the job's "Preload migration agent" option is enabled for a two-phased approach, separating the deployment of the migration agent and its execution, there are two additional states a client computer can be in:

Status	Description
Preloaded	The first phase of the migration, the deployment of the migration agent, completed successfully and the "Prime" button can be used to change the selected computer(s) status to "Primed".
Primed	The computer will perform the second phase, the actual migration, during the job's next execution.

To resolve errors, you can click on "Show log file…" to see the log file produced during the execution on the remote computer.

To run a specific computer again, click on the "Retry" button to change its current status back to scheduled.

In case you receive the Profiles status, because of user profiles found on the remote computer that do not have a matching account in the target domain, you can click on "Show profiles…" for more information about those profiles and accounts:



In the upper part of the dialog you can find a list of porfiles found locally on the remote computer. The time stamp in the upper right corner tells you when this information was collected.

In this example, there were 8 profiles found locally on the remote computer \\WKSTA-0008. There is one non-migratable profile found, not having a corresponding user account in the target domain.

The group box below the list of profiles shows detail information for the currently selected profile. Is shows the local path of the profile (revealing the user name of accounts deleted in the source domain), the last profile update on the workstation, the last domain logon (+- 14 days!), the domain account status (enabled, disabled) and the account's SID. Please note that there will be no profile warnings shown for profiles belonging to accounts that have been deleted in the source domain.

If there were non-migratable profile(s) found on a computer you can use the information shown to decide if those accounts either need to be migrated or can be ignored.

You can use the "Copy unmigrated account names to clipboard" button to copy those account names to the clipboard.

If you check the "Ignore profiles of accounts that have not been migrated to the target domain" option, the job will ignore the profiles of unmigrated accounts and proceed with the profiles that are migratable.

Performing an Undo to Reverse Changes

To undo changes made on a client by a Computer and Profile Migration job, please logon to the client as local Administrator and perform the steps below to rollback profile changes. The undo will also reverse changes made to the domain membership of the computer if the job changed it.

1. Open up an administrative command prompt.
2. Change into the corresponding job's folder on the client, which is located in c:\windows\syswow64\[YOUR-JOB-NAME.CR].
3. Run the following command:
   copyrights –debug –undo

It will undo changes made to profiles and at the end attempt to join back to the source domain if the job had changed the domain membership. It will prompt you for a username and a password of the source domain that has permissions to join the computer to the source domain. If the client computer account does not exist in the source domain, it will attempt to create it. If the domain join should fail, you can manually change the domain of the computer.

After the undo has completed, please reboot the computer.

Using the Command Line Interface

You can migrate computers and optionally user profiles of local or domain accounts, using a command line interface.

It can either be run locally on the computer or deployed in case you have some sort of software distribution available, such as Microsoft Operations Manager (MOM), IBM Tivoli, PDQ Deploy or similar.

Additionally, it supports a push method that can be used if no such software is available to you.

Note: If you have moved user accounts (not copied!) within the same forest (intraforest domain migration) with sidHistory you will not need to take care of the user profiles. Windows handles that case during logon of the migrated account. You can still use the /JoinDomain option to migrate the workstation to the target domain without the /FixProfiles option.

Command Line Parameters

You can use the following command line parameters to change a computers domain membership, update the locally existing profiles of local and domain user accounts and preserve cached credentials:

CopyRight [/JoinDomain:<NetBIOS or DNS Domain Name>] [/JoinAccount:<User Name>] [/JoinPassword:<Password of User Name>] [/JoinTitle:<Title of Logoff Notification Window] [/JoinMessage:<Message of Logoff Notification>] [/JoinMessageTimeout:<Seconds> [/NoUserNotification] [/NoLogoff] [/NoReboot | /NoShutdownOrReboot] [/FixProfiles] [/UpdateCachedCredential] [/Remote:<NetBIOS or DNS computer name>]

Parameter	Description
[/JoinDomain:<NetBIOS or DNS Domain Name>]	Join des Workstation to the specified domain.
[/JoinAccount:<User Name>]	If the account being used does not have permissions to join the specified domain you can provide an account name to be used instead.
[/JoinPassword:<Password of User Name>]	Password for the account to be used to join the target domain.
[/JoinTitle:<Title of Logoff Notification Window]	Title of the user notification window shown to inform the user that a logoff is required. The default title is “Domain Migration”.
[/JoinMessage:<Message of Logoff Notification>]	Text of the user notification window shown to inform the user that a logoff is required. The default text is “Your workstation will switch to a domain now. Please save any pending work and then click on OK to continue the process. After the system has rebooted you can login again.”.
[/JoinMessageTimeout:<Seconds>]	The time the notification message is shown to the user. The default value is 60 seconds. After that time has passed the user will be forced to logoff.
[/NoUserNotification]	Disable the user notification message entirely.
[/NoLogoff]	Do not logoff the currently working user.
[/NoShutdownOrReboot]	If used, the system will not shutdown or reboot after the workstation has been joined to the target domain.
[/Reboot]	Optionally reboot the client after domain join, instead of

	shutting it down.
[/FixProfiles]	If used, the locally found Windows user profiles of local and domain users will be processed. **Note:** This option is not needed if moving user accounts within the same forest while using sidHistory.
[/LoginMessage:<Message to Login Again>]	Text of user notification after profiles have been processed and if using /FixProfiles withjout /JoinDomain,
[/Shutdown]	If used in conjunction with /FixProfiles and without /JoinDomain, the client will shut down after profiles have been processed instead of displaying an information that the user can login again.
/JoinOU:<OU Distinguished Name>	Create the computer account in the specified OU of the target domain. For example: /JoinOU:"OU=My OU,DC=DOMAIN,DC=COM"
/JoinDC:<Domain Controller Name>	Join the target domain using the specified domain controller (either specified as NetBIOS or fully qualified DNS Name).
[/OutLog;<Log-File-Path.Log>]	This option will set the location of the log file. You could for example redirect it to the workstation's temp folder.
[/Remote:<NetBIOS or DNS computer name>]	If enabled the command will be executed on the specified remote computer.

Remote Execution (Push Method)

If /Remote is not used to specify a remote computer, the operation will change the local computers domain membership! If /Remote is specified along with a remote computer's name (push method), CopyRight2 will temporarily install a service on the remote computer, start the service, immediately uninstall it again and then perform the operation (see "Using CopyRight2's Command Line Interface (CLI)" -> "Remote Execution"). If the account you are currently logged on with does not have administrative permissions to remotely install a service (not a member of the local Administrators group either directly or indirectly), you can optionally specify credentials using the /RUser:<user name> and /RPwd:<Password>.

Logging

You can use the command line parameter /Outlog:<Name of log file> to redirect errors to a log file (see "Using CopyRight2's Command Line Interface (CLI)"). By default, the log file will be called "CopyRight.Log".

If executing the command remotely in conjunction with the "/Remote" parameter (push method) you can find it in the folder %SystemRoot%\System32\CR folder of the remote system.

VPN Users / CopyRight2 Cached Credential Update Add-On

One known potential issue you may face in case you have VPN users is that Windows will delete the cached credentials if a computer is changing the domain it belongs to. This can become a problem if your VPN client does not ship with a so-called GINA.DLL that extends the logon process, allowing you to open up the VPN tunnel from

the login screen. The Cisco VPN client for example has such a GINA.DLL, whereas OpenVPN and other derivates based on OpenVPN do not.

This problem is solved by the CopyRight2 Cached Credential Update Add-On.

The workaround for that problem is usually to let the end-user logon one time with a local account, open the tunnel, use the switch user functionality of Windows to get back to the logon screen and then logon with a domain account. Another possibility is to visit the corporate network to logon one time with the domain account while connected to the network. Both will cache the credentials.

With the Cached Credential Update installed and if using the "/UpdateCachedCredential" along with the '/JoinDomain" parameter, CopyRight2 will switch the domain while preserving the existing cached credentials and if necessary update them so that a migrated user account still can login after the domain changed without having to use the two workarounds mentioned above.

Required Files if Using Remote Deployment Software

In case you want to run the process using some sort of remote deployment software, you will need to include the following files in your package. You can find them in the CopyRight2 installation folder. The CCU.Dll is only needed if you use the /UpdateCachedCredential feature. As the installation folder contains platform dependent executables (32- or 64-bit), you may need to temporarily install the corresponding version of CopyRight2 (32- or 64-bit) to get the executables, for example on a separate system. The 32-bit version of the files can be used on 32- and 64-bit systems. All executables must match the same platform (either x86 or x64). You can verify the platform they were built for, by displaying the file properties with Windows Explorer.

File Name	Description
CopyRight.Exe	Main executable file.
Mapping.Dll	DLL containing code for mapping user and group accounts.
CCU.Dll	Optional file if using the cached credential update feature.
CopyRightS.Exe	Service executable.
CopyRight.Dll	DLL containing service messages for event viewer.

Examples

Here you can find some examples on how to use the command line interface.

Push Installation Using Administrative Account

The command line below will perform a push operation and uses the domain Administrator account of the target domain to join the domain. This allows the creation of the computer account in case it does not yet exist in the target domain.

It assumes that the caller has administrative permissions on the workstation in order to be able to install the CopyRight2 service on the remote system:

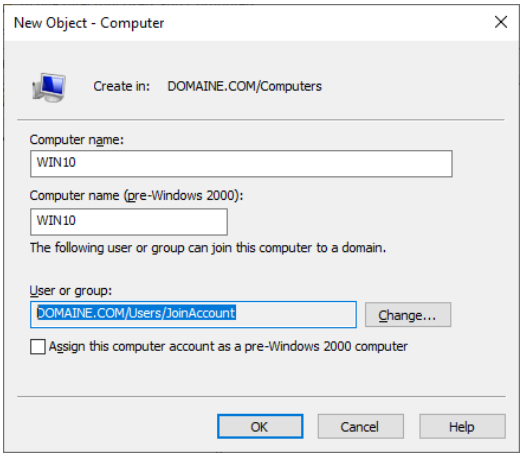
```
copyright /a /joindomain:NetBIOS-DOMAIN-NAME /joinaccount:administrator /joinpassword:PWD
/FixProfiles /Remote:REMOTE-COMPUTER-NAME
```

Push Installation Using Non-Administrative Account

The command below is similar but uses a different user account. JoinAccount, as the account is called in this example, can be a regular Domain User and the pre-created computer account needs to have this account enabled as manager:

```
copyright /a /joindomain:NetBIOS-DOMAIN-NAME /joinaccount:joinaccount /joinpassword:PWD
/FixProfiles /Remote: REMOTE-COMPUTER-NAME
```

When creating the computer account, it is important to specify either the account directly or (even better) a domain group that the account used to join the domain is a member of:



Push Installation using the Cached Credential Update Add-on

The example below, shows how to use the /UpdateCachedCredential option. Other than that it is identical to the first example "Push Installation Using Administrative Account":

```
copyright /a /UpdateCachedCredential /joindomain:NetBIOS-DOMAIN-NAME /joinaccount:administrator
/joinpassword:PWD  /FixProfiles /Remote:REMOTE-COMPUTER-NAME
```

It requires the Cached Credential Update Add-on to be present on the computer from where you run the command.

Running Locally on the Workstation

The example below is intended to run locally on the workstation from an administrative account:

```
copyright /a /joindomain:NetBIOS-DOMAIN-NAME /joinaccount:administrator /joinpassword:PWD
/FixProfiles /NoLogoff
```

Please note that it is using the /NoLogoff parameter. It should not be run while a user is still logged on, but instead after logging on with an administrative account locally.

Migrating Profiles Without Changing Domain Membership

The example below shows how to migrate a workstation's profiles without changing the domain membership, for example in case the domain membership was changed manually:

```
copyright /remote:REMOTE-COMPUTER-NAME /fixprofiles /a
```

Note: The workstation will not reboot or shutdown at the end of the process. Instead a user notification will be displayed, customizable with the /LoginMessage parameter, informing the user that the process has been completed.

Customizing Login and Domain Join Messages

The example below shows how to use the "\n" place holder (carriage return) to format custom messages specified using the /JoinMessage and /LoginMessage parameters:

```
copyright /remote:REMOTE-COMPUTER-NAME /fixprofiles /a /LoginMessage:"Line 1\nLine 2\n\nLine 4"
```

Running Profile Migration Using Remote Deployment Software

The example below is intended to be run from a deployment software and assumes that you are using in an administrative context:

```
copyright /a /joindomain:netbios-domain-name /joinaccount:JoinAccount /joinpassword:PWD
/FixProfiles
```

Please note that, since /NoLogoff is not specified, the currently working user will be logged out first as one of the first steps of the process. The process will still continue to run in the background.

Changing Domain Membership Without Updating Profiles

The example below is useful in the case where you have moved user accounts between two domains located in the same forest (intraforest) using sidHistory instead of copying user accounts. Under these circumstances the Windows client will automatically migrate the profile to the new account that has the original SID the account had in the source domain in its sidHistory attribute.

```
copyright /joindomain:domaine /joinaccount:administrator /joinpassword:Test123#
```

Using CopyRight2's Command Line Interface (CLI)

CopyRight2 has a command line interface and can be integrated into batch file processing. CopyRight2 returns process state information by setting the value of the environment variable %ERRORLEVEL% according to the error that might have occurred. This variable can be evaluated by the batch process to decide on further processing.

If copying important data, a log file of the messages should be created in any case. You can either use the option provided with the Windows Explorer extension to create such a log file or by running the command line statement in the following way:

CopyRight \\Server1\E$\Usr \\Server2\E$\Usr /R >H:\Error.Log

The command line interface of CopyRight2 allows you to copy single or multiple files / directories, optionally including their subdirectories:

CopyRight [path\\]{source file(s)} [path\\][destination file(s)] [/H[+]] [/CU[+] [/CP]] [/CL[+]] [/CG[+]] [/G:File.Map] [/J] [/Q] [/T] [/W] [/R] [/K] [/Y[+]] [/X] [/ShadowCopy] [/B] [/L] [/S] [/I] [/D|/F] [/O] [/M|/N] [/Z] [/V] [/CopyEnc] [/MSync]

Parameter	Description
[path]	Optionally an absolute / relative or an UNC path
{source file(s)}	Path to the source files
[destination file(s)]	Path to the destination files
[/H[+]]	Copy including network shares and their permissions. If enabled, any file share located at or below the specified source path will be copied to the destination computer. If the optional '+' character is appended the command will also update existing file shares, if not, any existing file shares will be skipped.
[/S]	Copy including all subdirectories
[/D]	The destination specifies a directory
[/F]	The destination specifies a file
[/O]	Overwrite existing files without any questions
[/W]	Automatically overwrite Read-Only files
[/Q]	Simulation of the copy process. When simulating a copy process, no data is actually transferred. Instead only an access check is performed, whether the files can be accessed in the source and can be written to in the destination. Because not data is moved, a simulation runs much faster than a copy process and can show up potential problems before they occur during a real copy process.
[/T]	Copy files and folders without date and time information. The newly created files and folders receive the current system time instead of the time of the source files and folders.
[/K]	Keep existing files. Do not overwrite any existing files in the destination.
[/Y]	Do not overwrite any newer files existing in the destination. By applying this option, you can prevent newer, changed files in the destination, from being overwritten by older files from the source environment. It limits the copy process to only those file, not yet existing, or existing in an older version within the destination.
[/Y[+]]	This option works like /Y but additionally deletes files at the destination that do not exist at the source. Be careful using this option, if you specify for example by mistake an empty source folder, all files at destination will be deleted.

[/X]	Copy including locked files. By applying this option, even locked files will be copied.
[/ShadowCopy]	Copy including locked files. This option creates a shadow copy of the source folder that will be used instead of the source path, to circumvent errors resulting from locked files. This option only supports local files and folders as the source. Remote UNC paths and connected network shares are not supported.
[/I]	Do not stop the process if any errors are encountered
[/M]	Automatically map accounts to identically named accounts on the destination server
[/N]	Do not automatically map accounts to identically named accounts on the destination server. Please note that any accounts contained in permissions have to be resolvable at the destination.
[/Z]	Do not copy file/directory rights but inherit them from destination dir instead
[/A]	Continue copy process, even when encountering SIDs that do not exist in the destination and cannot be resolved within the destination environment.
[/V]	Do not display each file copied.
[/CopyEnc]	Specify this option to copy encrypted file's raw data in case of experiencing access denied errors. The graphical version of CopyRight2 (GUI) uses this option by default. Please note that the end users accessing this file will need the same password used previously to access the file!
[/MSync]	Enables the block transfer mode for this copy operation. This option will automatically install the required service at the peer computer and start it. Please make sure that the firewall has port 8082 open on both peers (sender and receiver) to allow communication between them. You can specify a different port by using the /MSyncSend and MSyncReceive options (see advanced).

NOTE: If you specify the source directory including a filename or some wildcards like *.*, the security information of the root folder of the copy process, will not be copied! To copy the security information of the root folder of the copy operation, you have to specify the root folder without any filename or wildcard parameters.

Advanced Parameters

Parameter	Description
[/B]	Use large file buffers. This option speeds up the copy process when copying large files.
[/L]	This option enables CopyRight2 to process command line options passed in, using the ANSI format instead of the usually used ASCII format. If using batch file based copy processes, those batch files can be maintained with Notepad or Excel for example, which both use ANSI format when saving files.
[/DontSkipJunctionPoints]	By default CopyRight2 skips any junction points encountered. If you want CopyRight2 to treat junction points just like regular folders enable this option. Please note that this can cause infinite recursion if there is junction points defined pointing to themselves for example.
[/NasWorkaround]	Certain Network Attached Storage (NAS) Solutions require workarounds regarding the implementation of the backup operator privilege. If encountering unexpected access denied errors when copying to a NAS, you can try to enable these workarounds by using the option /NasWorkaround.
[/SlowLink]	This advanced option will disable certain copy features (e.g. multithreading) of CopyRight2 to facilitate troubleshooting.

[/Disco]	Usable if the source part of this copy operation specifies a share. CopyRight2 will disconnect all users from the specified share before starting the copy process.
[/ErrLog:<file>]	This option will cause an error log to be created containing only error messages.
[/OutLog:<file>]	This option will cause a log to be created containing any non-error messages.
[/MigLog:<file>]	This option will cause a log file to be created containing all migrated accounts (semicolon delimited). The log file contains the original account (from source) and the migrated account (at destination).
[/Exclude:{File Specifier}[,{File Specifier},...]]	This option will cause CopyRight2 to skip any given file specifiers (wildcards). You can for example skip any PDF and PST files by specifying "/Exclude:*.pdf,*.pst". To skip any instance of a XYZ.TXT file you could specify "/Exclude:*\XYZ.TXT".
[/Include:{File Specifier}[,{File Specifier},...]]	This option will cause CopyRight2 to copy only the given file specifiers (wildcards). You can for example copy only PDF and PST files by specifying "/Include:*.pdf,*.pst"
[/ex:%day.%month.%year %hour:%minute:%second]	This option will cause CopyRight2 to skip any files not modified after the specified date. You can for example skip any files older than 13.12.2011 by specifying the following: "/ex:13.12.2011 00:00"
[/Event:S|E]	Enable writing to the event log upon success or error. To write to the event log in both cases, specify /Event:S and /Event:E-
[/SMTP:S|E,{user@domain.com},{smtp server name or ip address}]	Enable sending a SMTP mail upon success (S) or error (E). Send an email to the specified user using the specified SMTP server.
[/TimeFrameEnd:%d.%m.%y %hour:%min or %y/%m/%d %hour:%min]	Specify a time frame after which CopyRight2 should automatically end itself. The timeframe can be specified either as %d.%m.%y %hour:%minute or %y/%m/%d %hour:%min.
[/MSyncReceive:{Remote-Computer[:Port]}]	This command will start a block transfer receive operation. It only requires a destination path to be specified. This command does not install the service on the remote peer but expects it to be started manually. You can optionally specify a TCP Port (default is 8082).
[/MSyncSend:{Remote-Computer[:Port]}]	This command will start a block transfer send operation. It only requires a source path to be specified, without a destination path. This command does not install the service on the remote peer but expects it to be started manually. You can optionally specify a TCP Port (default is 8082).
[/MSyncDisableNagle]	This option will disable the TCPIP nagle algorithm for the connection.
[[/MSyncCompression]	This option will enable LZ4 compression (optimized for speed).
[/MSyncCompressionSlow]	This option will enable GZIP compression (optimized for size).
[/MSyncEncryption]	This option will enable encryption for the block transfer operation.
[/MSyncPackageLen:{Len}]	This option allows you to change the packet size for each packet. The default size is 65536 bytes.
[/MSyncTcpWindowSize:{Len}]	This option allows you to change the TCP window size. The default size is 1048576 bytes (1MB).
[/MSyncPublicKey:{public key in hex format}]	This option is used together with /MSyncEncryption on the receiving peer to set the public key of the sending peer.

Share and NTFS Permission Modifications

Parameter	Description
[/SetShrPerm:{\\computer\share},{object}={Permission}]	This will overwrite the specified shares permission. You can for example run "/SetShrPerm:\\FRA14C8P\Shr$,Everyone=F" to set the Shr$ permission to everyone full access.
[/AddShrPerm:{\\computer\share},{object}={Permission}]	This will add the specified permission to an existing share. To block any access to a specific share you can add an access denied ace for everyone by specifying the following option: /AddShrPerm:\\FRA14C8P\Shr1$,Everyone=N After migrating the share to it's new destination you can run a similar operation targeting the copy of the share to allow access again: /DelShrPerm:\\NEWSERVER\Shr1$,Everyone=N Please note that CopyRight2 adds entries to the top of the list, even access denied ACEs, which would usually be added to below the access allowed ACEs.
[/DelShrPerm:{\\computer\share},{object}={Permission}]	This will remove the specified permission.
[/SetShrCsc:{\\computer\share},manual|auto|autoopt|none]	This will set the specified share's client side caching options. You can for example run "/SetShrCsc:\\FRA14C8P\Shr$,none" to disable CSC for a specific share.
[/SetNTFSPerm:{File or Folder},{object}={Permission}]	This will overwrite the specified file's or foler's permissions. You can for example run "SetNTFSPerm:c:\myfile.txt,Everyone=F" to set c:\myfile.txt's NTFS permissions to everyone full access.
[/AddNTFSPerm:{File or Folder},{object}={Permission}]	This will add the specified permission. Please note that CopyRight2 adds entries to the top of the list, even access denied ACEs, which would usually be added to below the access allowed ACEs.
[/DelNTFSPerm:{File or Folder},{object}={Permission}]	This will remove the specified permission.

User and Group Migration and Reacling

Parameter	Description
[/CU][+]	Copy user accounts not existing at the destination computer. The additional option '+' synchronizes existing accounts between source and destination environment.
[/CP]	Copy user account passwords as well. Please note that this option requires the CopyRight2 Password Addon to be installed.
[/CL][+]	Copy local group accounts not existing in destination computer. The additional option '+' synchronizes existing accounts between source and destination environment.
[/SLG]	Skip local group members if copying a local group. If not specified the entire group member will be migrated as well.

[/CG][+]	Copy global group accounts not existing in destination computer. The additional option '+' synchronizes existing accounts between source and destination environment.
[/SGG]	Skip global group members if copying a global group. If not specified the entire group members will be migrated as well.
[/G:<File.Map>]	Use a predefined mapping file File.Map, previously created with the "User and Group Assignment" tool, to assign not existing user and group accounts.
[/R]	Do no copy files, but reassign (REACL) permissions of the source files specified. To be used in conjunction with the option /G: to specify a mapping file to use for reassigning permission. In case of /R the specification of a destination directory is not necessary.
[/SkipOwner]	Do not copy the owner information of NTFS permissions. This will cause the owner to be automatically set to the security context that the job is running under. If this account is a member of the "Administrators" group the owner will be set to the "Administrators" group instead.
[/SkipDacl]	Do not copy the access list of permissions.
[/SkipSacl]	Do not copy the system audit permissions.
[/SkipGroup]	Do not copy the group attribute of permission. This property is usually not visible within Windows Explorer and used only in conjunction with the POSIX subsystem of Windows. It is similar to the owner attribute and contains a SID of a user or group account.

Migrating User and Group Accounts without Copying Files or Shares

You can use the command line interface to migrate selective user and/or group accounts.

CopyRight {\\source computer} {\\destination computer} [/CU[+] [/CP]] [/CL[+]] [/CG[+]] [/CopyAccounts:{samAccountName[,…]}] [/SyncAccounts: {samAccountName[,…]}] [/A] [/I] [/NoUPNUpdate] [/LdapNoDefaultAtt:class1[,class2[,...]]] [/LdapAttAdd:class|att1[,att2[,...]]] [

Parameter	Description
{\\source computer}	The source computer (either workgroup, member or domain controller)
{\\destination computer}	The destination computer where you can to copy the accounts to.
[/CopyAccounts:…]	Specify one or multiple accounts you want to copy from the source to the destination computer. Separate multiple accounts by using a "," without blank at the end. This option will skip existing accounts.
[/SyncAccounts:…]	Specify one or multiple accounts you want to synchronize between the source and the destination computer. Separate multiple accounts by using a "," without blank at the end. This option will synchronize existing account's properties and group memberships.
[/CU][+]	Copy all user accounts not existing at the destination computer. The additional option '+' synchronizes existing accounts between source and destination environment.
[/CP]	Copy user account passwords as well. Please note that this option requires the CopyRight2 Password Addon to be installed.
[/CL][+]	Copy all local group accounts not existing in destination computer. The additional option '+' synchronizes existing accounts between source and destination environment.
[/SLG]	Skip local group members if copying a local group. If not specified the

	entire group members will be migrated as well.
[/CG][+]	Copy all global group accounts not existing in destination computer. The additional option '+' synchronizes existing accounts between source and destination environment.
[/SGG]	Skip global group members if copying a global group. If not specified the entire group members will be migrated as well.
[/G:<File.Map>]	Use a predefined mapping file File.Map, previously created with the "User and Group Assignment" tool, to assign not existing user and group accounts.
[/A]	Continue copy process, even when encountering SIDs that do not exist in the destination and cannot be resolved within the destination environment.
[/I]	Do not stop the process if any errors are encountered
[/NoUPNUpdate]	Disable automatic domain replacement applied to the userPrincipalName attribute during domain user migrations.
[/LdapNoDefaultAtt:class1[,class2[,...]]]	Purge list of default Active Directory attributes to copy during domain migrations for specific classes.
[/LdapAttAdd:class|att1[,att2[,...]]]	Add one or more attributes to a specific classes attribute list.
[/LdapAttRemove:class|att1[,att2[,...]]]	Remove one or more attributes from a specific classes attribute list.

Note: Valid Active Directory classes are user, group, contact, OU and computer.

Remote Execution

You can execute CopyRight2 remotely on any Windows computer. This requires administrative privileges on the computer that you want to run the command on. CopyRight2 will automatically install an instance on the remote computer and then forward the command line parameters to this instance running as a service.

Parameter	Description
[/Remote:<computer>]	Execute the specified command on the specified remote computer.
[/Ruser:<user>]	Execute the specified command on the remote computer using the specified user context.
[/Rpwd:<password>]	Password for the remote execution security context.
[/Wait]	Wait until the remote operation has completed.
[/IsActive]	Check whether the copy job is still running remotely. Will return error level 1 if active or 0 if inactive.
[/CleanUp:<computer>]	This will remove a previously ran command and remove any log files that still might exist on the remote computer specified.
[/OrderID:<ID>]	In case of multiple running remote jobs, specify a unique ID to identify a specific copy job. This can be used with any of the remote execution options.

To copy the files from c:\users to d:\users on the remote computer FRA14C8P you would run the following command:

```
Copyright c:\users d:\users /s /d /o /w /remote:FRA14C8P /ruser:Admin /rpwd:P@ssw0rd1 /wait
```

Text File Inventory

You can use a combination of the command line parameters below to create a text file inventory using a tab delimited format. The output file(s) will be created in the current working folder. You can find the default file name for the output file below. The file name can be customized by appending a colon along with the desired file name.

Parameter	Description
/du	Dump user accounts to user.txt file.
/dts	Dump terminal server / RDP specific attributes as well for each user.
/dl	Dump local groups to localgroup.txt file.
/dlm	Dump local group members localgroupmember.txt file.
/dg	Dump global groups to globalgroup.txt file.
/dgm	Dump global group members to globalgroupmember.txt file.
/dc	Dump computer accounts to computer.txt file.
/ds	Dump file shares to share.txt file.
/dss	Dump file share permissions to shareperm.txt file.
/dt	Dump domain trusts to trust.txt file.
/df	Dump files to file.txt file.
/dfs	Dump file NTFS permissions to fileperm.txt file.
/dfc	Dump file hash for each file as well. (Hash can be selected using /hash parameter).
/hash: CRC|MD4|MD5|RIPEMD|SHA1||SHA2|SHA3	Use the specified hash algorithm. The default, if not specified is MD5.
/dd	Dump dirs. To dir.txt file.
/dds	Dump directory NTFS permissions to dirperm.txt file.
/dr	Dump privileges to right.txt file.
/dv	Dump device drivers and services to service.txt file.
/de	Include Windows version information for files, services and device drivers. This option works in conjunction with /df and /dv.
/di	Dump drive list (including capacity/used capacity) to drvie.txt file.
/dw	Dump installed software to software.txt file.
/dm	Dump installed Windows components to component.txt file.
/dh[db]	Include a header row in each output file consisting of column names. Column names can contain blanks if /dh is used. To use database friendly names, specify /dhdb instead.
/ReplaceNumValues	Replace numeric values, such as bitmasks with clear text information (e.g. permissions, file attributes, …).
/d:<remote computer>	Dump information of the specified remote computer over the network. If not specified the local computer is used to retrieve information from.

DFS Update

You can use the /UpdateDFS and /RollbackDFS parameters to manually update entries of the specified DFS server. It supports domain based and standalone DFS servers.

These parameters work either with a specified source and target path or by specifying a job file using the "/J:Jobname" parameter to let it process all source/destination pairs defined in the copy job definition.

Parameter	Description
/UpdateDFS:<DFS Server Name>	Update entries on the specified DFS server to point to the new location on the target.
/RollbackDFS:<DFS Server Name>	Rollback any corresponding changes pointing to the target server to point to the source server again in case of a roll back.
/j:<job file.job>	The file name of the copy job containing the source/destination pairs and additional parameters.
/s	Include sub directories in case you specify source and destination along with /UpdateDFS or /RollbackDFS
/d	The target is a directory.
/i	Ignore errors and continue processing.
/h[+]	Migrate file shares (/h) or update file shares (/h+).

The example below would update all DFS entries on DFS server "DFS-SERVER-NAME" pointing to the specified source path (or a folder below) to the corresponding destination path:

```
Copyright \\Src-Server\c$\folder1 \\Dst-Server\c$\folder1 /UpdateDFS:DFS-SERVER-NAME /s /d /i
```

To roll back the changes made to DFS you can run this command using the /RollbackDFS parameter instead:

```
Copyright \\Src-Server\c$\folder1 \\Dst-Server\c$\folder1 /RollbackDFS:DFS-SERVER-NAME /s /d /i
```

You can also use a job file in conjunction with the /UpdateDFS and /RollbackDFS parameters as in the example below:

```
Copyright /j:"Copy Job Name.job" /UpdateDFS:DFS-SERVER-NAME
```

In case of using a job file, you don't need to specify /s, /d, /i because those parameters are defined in the copy job. If a job file is specified, the output of the process will automatically get appended to the existing log file of the copy job.

Offline Migrations of Disconnected Systems

CopyRight2 supports so-called offline migrations for cases where the source and destination system are not directly connected by a network. In this case you can export any files, folders, network shares, users, groups and network permissions to a locally connected NTFS formatted hard drive or other device which you will later connect to the destination system to import from. Alternatively, you can use a tool such as WinRAR or FreeARC to create an archive containing the files and folders including NTFS permissions, time stamp information and reparse point information (symbolic links and mount points).

Export and Import of Users, Groups, Group Members and File Shares

Parameters for exporting and importing users, groups, group members and file shares including share permissions:

Export Parameter	Import Parameter	File Name	Description
/DU	/IU	User.Txt	Export/import user accounts.
/DP[+|:PASSWORD]	/IP[+|:PASSWORD]	(Additional column in User.Txt file)	Export/import user accounts including password hashes. If specifying a password (/DP:MYPWD or /IP:MYPWD) will encrypt/decrypt the password hashes with the specified password. If specifying + (/DP+ or /IP+) the program will prompt for a password to encrypt/decrypt the hashes with (AES256).
/DTS	/ITS	(Additional column in User.Txt file)	Export/import user accounts including Windows/Citrix Terminal Server user settings.
/DL	/IL	LocalGroup.Txt	Export/import local groups.
/DLM	/ILM	LocalGroupMember.Txt	Export/import local group memberships.
/DG	/IG	GlobalGroup.Txt	Export/import global groups.
/DGM	/IGM	GlobalGroupMember.Txt	Export/import global group memberships.
/DS	/IS	Share.Txt	Export/import file shares.
/DSS	/ISS	SharePerm.Txt	Export/import file share permissions.
/DH	/IH	(Each export file)	Includes an additional first row containing the column heading.
	/CU+		Update existing user accounts in case they already exist on the target.
	/CL+		Update existing local groups in case they already exist on the

			target.
	/CG+		Update existing global groups in case they already exist on the target.
	/H+		Update existing shares in case they already exist on the target.

To export users, local groups and local group memberships please run the following command to create a User.Txt, LocalGroup.Txt and LocalGroupMember.Txt file:

```
Copyright /DU /DL /DLM
```

To import the 3 previously created files you could run the following command on the destination computer, assuming that the computer has CopyRight2 installed and that the 3 files are located in the current working folder:

```
Copyright /IU /IL /ILM
```

This command will not overwrite/update any existing users or local groups. To update existing users and groups append the "/CU+" and "/CL+" options during import:

```
Copyright /IU /IL /ILM /CU+ /CL+
```

Export and Import of Files, Folders and NTFS Permissions

Additionally, to exporting and importing user accounts, group accounts and file shares, you can also export files, folders and NTFS permissions to a local or connected network drive by specifying the corresponding source and destination path as a command line parameter.

CopyRight <Src-Path> <Temporary-Storage-Path> /S /D /O /W /N

Parameters for exporting files and folders including NTFS permissions:

Parameter	Description
/S	Include sub-directories.
/D	Destination is a directory.
/O	Overwrite existing files at the specified destination.
/W	Overwrite read-only files existing at the specified destination.
/N	Copy raw NTFS security descriptor to destination.

The parameter /N will make sure that the raw NTFS permissions are kept when creating the copy. During import those permissions will be reacled to replace the SIDs of the original source accounts with the SID of the corresponding accounts on the destination.

You could for example export all files and folders of the C:\Data drive to a folder on a temporary drive T, including NTFS permissions, file shares, file share permissions, users (including passwords), local groups and memberships using the following command line statement:

```
Copyright c:\Data t:\Data /s /d /o /w /n /dh /du /dp /dl /dlm /ds /dss
```

If there should be additional folder you would like to export you can export them without the command line switches used to export users, groups and shares:

```
Copyright d:\OtherFolder t:\OtherFolder /s /d /o /w /n
```

When importing the data along with the user accounts, please use the following command line statement, assuming that the temporary storage drive is called T again and that the exported text files containing the user and groups information is located in the current working folder:

```
Copyright t:\Data /s /d /o /w /m /ih /iu /ip /il /ilm /is /iss /cu+ /cl+ /h+
```

When importing any additional folders please use the command line statement below:

```
Copyright t:\OtherFolder /s /d /o /w /m /ih /iu /il /cu+ /cl+
```

Using WinRAR for an Offline Migration

WinRAR supports creating archives preserving NTFS security, time stamp information, reparse points and hard links. This is useful if you cannot connect a hard drive or USB device to the source and/or destination computer as intermediary storage.

Export Users, Local Groups, Local Group Memberships, Shares and Share Permissions

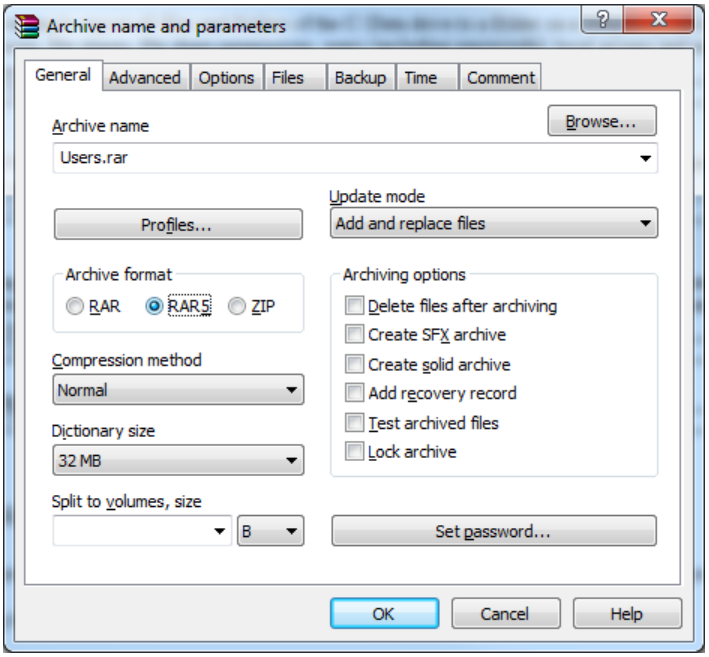
You can use the following options to export users (including passwords and terminal server user's settings), local groups, local group memberships, shares and share level permissions:

```
Copyright /dh /du /dp /dts /dl /dlm /ds /dss
```

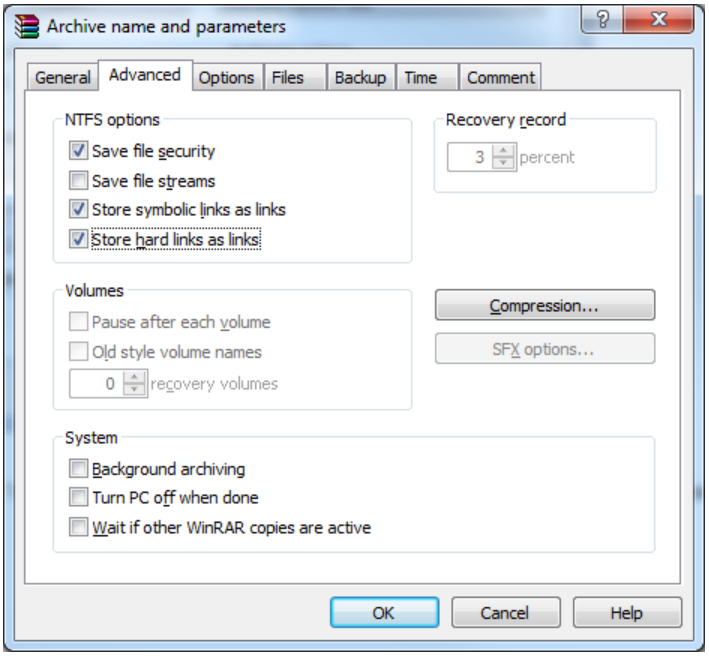
This command will create 5 files called User.Txt, LocalGroup.Txt, LocalGroupMember.Txt, Share.Txt and SharePerm.Txt containing the corresponding information for a later import.

Exporting Data into a RAR File

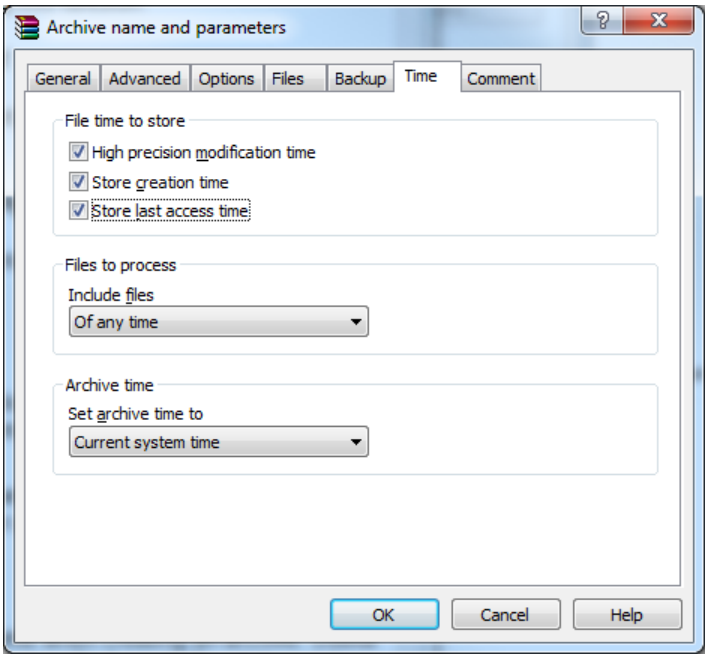
When creating the archive on the source computer, make sure to select the RAR4 or RAR5 format, depending on your version of WinRAR:



Next click on “Advanced” and activate the following options to store NTFS permissions (“Save file security”) and optionally, if you also want to copy user profile folders for example the reparse points (“Store symbolic links as links”) and hard links (“Store hard links as links”) options:



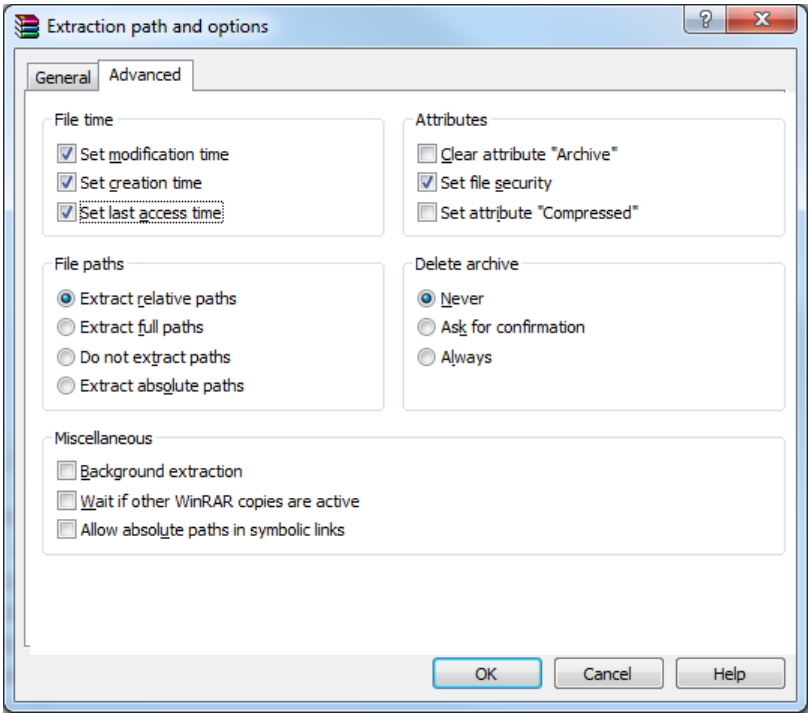
Finally select the „Time“ tab to select the following options to preserve creation, modification and last time opened time stamps:



Next click on „OK“ to create the RAR archive.

Unpacking RAR File to Temporary Folder

Transfer the RAR file to the disconnected destination system and unpack it into a temporary folder using the following options in “Advanced” to make sure timestamps are set:



Importing Users, Local Groups, Shares, Share Permissions and Data

Transfer the 5 previously exported text files to the destination system and copy them into a folder. Next open up an administrative command prompt and change into the directory where the files are located at.

Run the following command, replacing <Temporary Folder> with the path to the folder the RAR file was unpacked to and <Destination Folder> with the path to the folder the data should be copied to:

```
Copyright <Temporary Folder> <Destination Folder> /s /d /o /w /m /ih /iu /ip /its /il /ilm /is
/iss
```

You may want to additionally specify the “/CU+” and “/CL+” option to also update user and group accounts already existent on the destination computer. If those options are not specified, existing users and groups will not get updated with data from the corresponding User.Txt and LocalGroup.Txt files.

Another useful option you may want to add is either “/A” or “/A+”. These two options will ignore deleted user and group accounts in NTFS, file share and during import of group memberships. “/A” will write an informational

message to the console or log file and "/A+" will silently ignore deleted accounts.

In case you are importing user profiles you can also specify the "/TranslateProfiles" to replace permissions inside the user's registry files. You can also use the "/RegistryReplace" or "/UpdateNetworkConnections" as well as "/TranslateShortcuts" options to replace references to the old server name. In case the old and the new server names are different, you can use the "/Replace:<search,replace>" option to change server name references in the user profile (registry) or in shortcuts (LNK files).

Importing Samba (Linux) Password Hashes

CopyRight2 allows the import of user account password hashes from a "pdbedit -Lw" export created on a Linux system running Samba. The "/Samba" command line option can be used in conjunction with the user import option, to import password hashes, allowing migrated users to login with their existing passwords.

Parameter	Description
/IU:<filename>	Import the password hashes from the following file.
/IP	Import password hash.
/CU+	Update existing accounts.
/Samba	The specified file is a "pdbedit -Lw" export file.

You could for example use the following command to import and export file called "PdbEditDump.txt":

```
Copyright /IU:PdbEditDump.Txt /IP /CU+ /Samba
```

Samples

Copy the directory \\Server1\E$\Usr including all subdirectories to \\Server2\E$\Usr. This sample will copy NTFS permissions to the destination computer, including the permissions set on the root folder. If any files or directories are using local user or group accounts, CopyRight2 will ask if you wish to map those to existing and identically named accounts on the destination system. These accounts must be created before running the CopyRight2 command. If you encounter some so-called “BUILT-IN” groups, using hard-coded ID’s built into Windows-NT, they do not necessarily have to be named identically. You can, for example, copy files from an English NT-Server to a German one and vice versa, without any problems.

```
CopyRight \\Server1\E$\Usr \\Server2\E$\Usr /S /D /V
```

Copy the files on drive H: including all subdirectories to Q:. In his case the security information of the root folder will not be copied to Q:\ because the source path is specified with wildcards (*.*). If you would need to do so, you would have to execute the command line statement below to include the permissions of the root folder, but not copying sub-directories. This sample logs all error messages, if any are occurring, to the log file H:\CopyRight.Err. If errors should occur, the copy process will still continue to run, because of the option /I to ignore errors.

```
CopyRight H:\*.* Q:\ /S /I 2>h:\CopyRight.err
CopyRight H:\ Q:\  /I 2>h:\CopyRight.err
```

The following sample copies the directory ”directory1“ with all its files, located below the current directory (relative path) to \\server2\e$\directory1. This operation will copy the security information of the folder “directory1”

```
CopyRight Directory1 \\server2\e$\directory1
```

Copy all .DOC files located below the folder \\Server1\E$\Usr, including their security information to \\Server2\E$\Usr. This sample will not copy the rights of the root folder of the copy operation to the destination server. This command line makes use of the /M option, which answer all questions, regarding the account mapping automatically with yes.

```
CopyRight \\Server1\E$\Usrr\*.doc  \\Server2\E$\Usr /S /D /V /M
```

Copy a single file, located at G:\Dir\File1.Xls to \\Server\e$\excel\sheet:

```
CopyRight g:\dir\file1.xls \\Server\E$\Excel\Sheet /S /D /V
```

The next sample copies the files from the folder \\Server01\Marketing$ to \\Server02\Marketing$. During the copy process, all users and groups not existing in the destination environment should automatically be copied from the source environment. Therefore, the options "/CU", "/CL" and "/CG" are specified.

```
CopyRight \\Server01\Marketing$ \\Server02\Marketing$ /CU /CG /CL /S
```

The next sample copies the files from the folder \\Server01\Marketing$ to \\Server02\Marketing$. During the copy process, all users and groups not existing in the destination environment should automatically be copied from the source environment. In this case the accounts from the source and destination environment need to be synchronized, since the copy process will be run from time to time, to migrate the data partially. Therefore, the options "/CU+", "/CL+" and "/CG+" are specified.

Setting the option /H causes all file shares from the source to be copied to the destination. The options /O and /W cause an overwriting of existing files without asking.

```
CopyRight \\Server01\Marketing$ \\Server02\Marketing$ /CU+ /CG+ /CL+ /S /H /O /W
```

The next sample copies the files from the folder \\Server01\Marketing$ to \\Server02\Marketing$. During the copy process, all users and groups not existing in the destination environment should automatically be copied from the source environment. In this case the accounts from the source and destination environment need to be synchronized, since the copy process will be run from time to time, to migrate the data partially. Therefore, the options "/CU+", "/CL+" and "/CG+" are specified.
Furthermore, some group and user accounts need to be replaced during the copy process as defined in the previously created mapping file Marketing.Map.

```
CopyRight \\Server01\Marketing$ \\Server02\Marketing$ /CU+ /CG+ /CL+ /S /G:Marketing.Map
```

Required file(s):

```
CopyRight.Exe
Mapping.Dll
```

Domain.Ini File

An optional domain.ini file can be created in the CopyRight2 folder to control certain aspects of the migration, such as which domain controller should be used and if a specific account should get added on the target to migrated folder migrated.

You can create a section for each server/NAS using its NetBIOS name to specify the following INI entries:

Entry Name	Description
DomainController	Use this domain controller for the specified source or target server.
AddAdminAccount	Add the specified account with “Full Access” to each folder migrated to the target if it is not already contained in permissions.
AddAdminAccountOnError13	Add the specified account with “Full Access” to each folder migrated to the target if it is not already contained in permissions and if no access is granted on the target system, for example if the target NAS does not support the “Restore File & Folder” privilege / “Backup Operators” group.
Synology	If set to 1, the specified NetBIOS name is that of a Synology NAS.
HDI	If set to 1, the specified NetBIOS name is that of a Hitachi HDI NAS.

For example:

```
[SRC-SERVER]
DomainController=DC-999

[DST-SERVER]
DomainController=DC-123
```

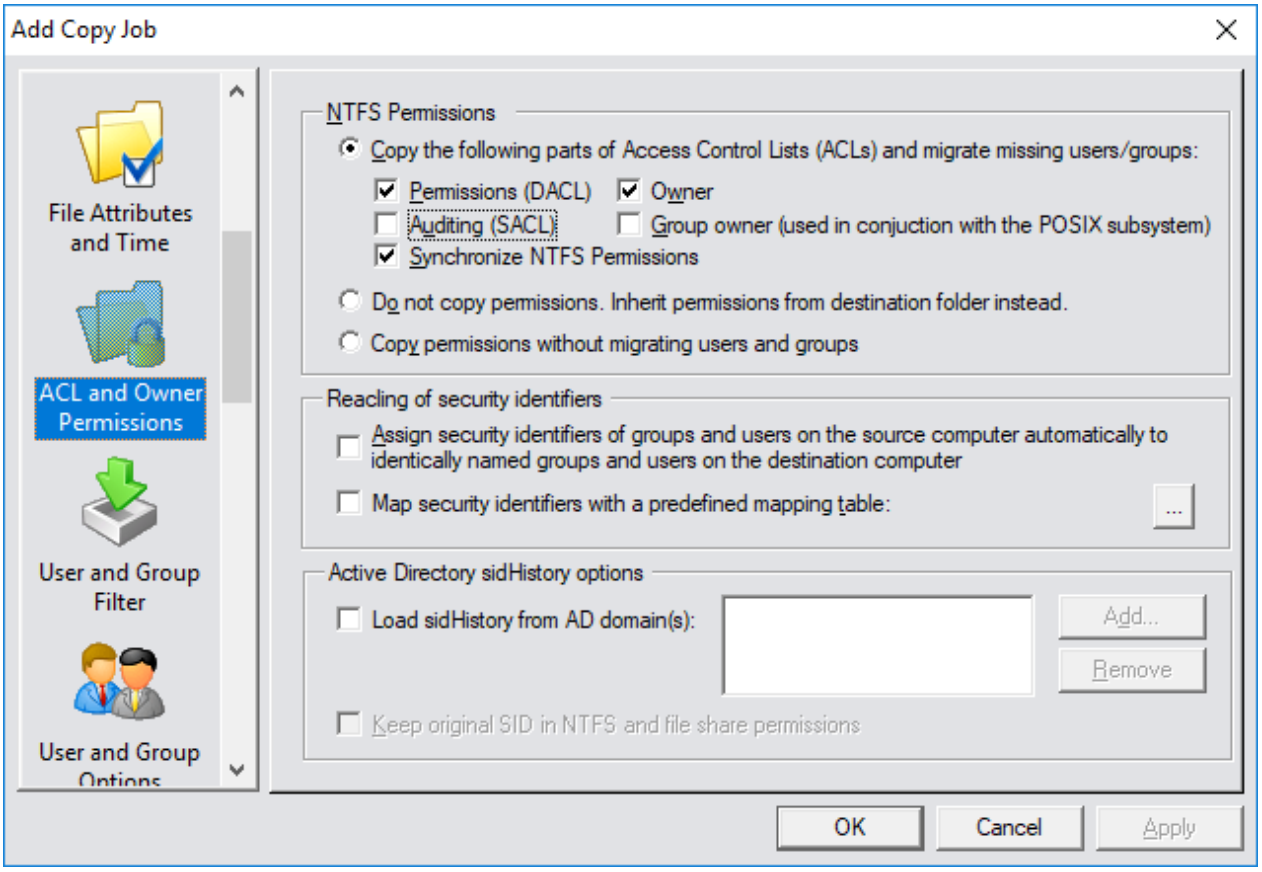
Domain.Ini Example

NAS Migrations

If the source or the target of your migration are NAS systems, you may need to deviate from the standard settings used to migrate a Windows server.

Auditing No Supported

Not all NAS systems support NTFS auditing. You can verify if your source or target supports auditing by displaying the advanced NTFS permissions with Windows Explorer. If there is no “Auditing” tab, then the system does not support auditing. In this case, please disable the migration of the SACL (Auditing) in the copy job’s settings.

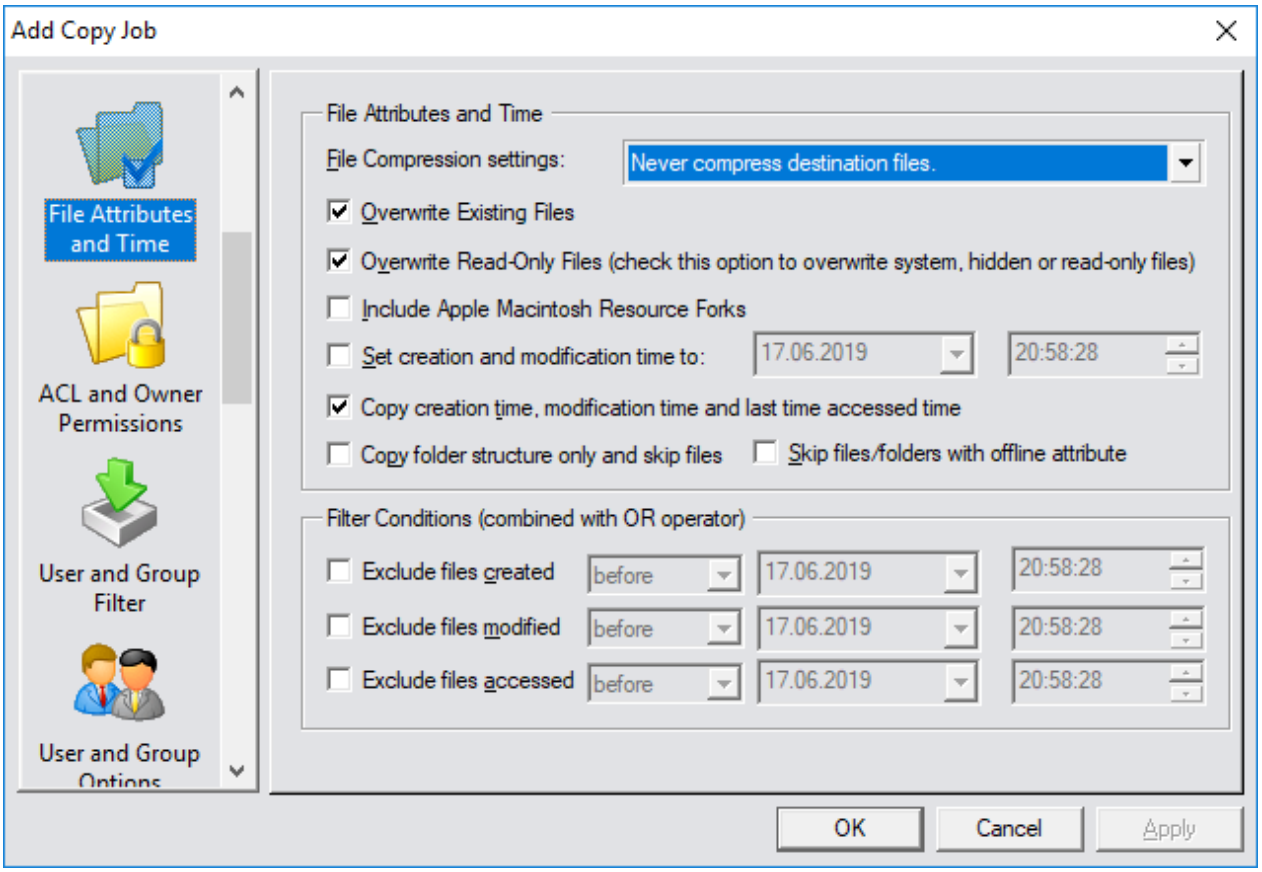


Compression Not Supported

Most NAS systems do not support the compression attribute, because they are using more efficient methods based on the deduplication of blocks below the file system.

You can validate if the target system supports NTFS compression by displaying the attributes of a file located on the target system with Windows Explorer. If the option to compress files/folders is not shown, the target system does not support compression.

If your target system does not support compression, please select the “Never compress destination files.” option in the “File Attributes and Time” page:



Administrative Override / Backup Operators

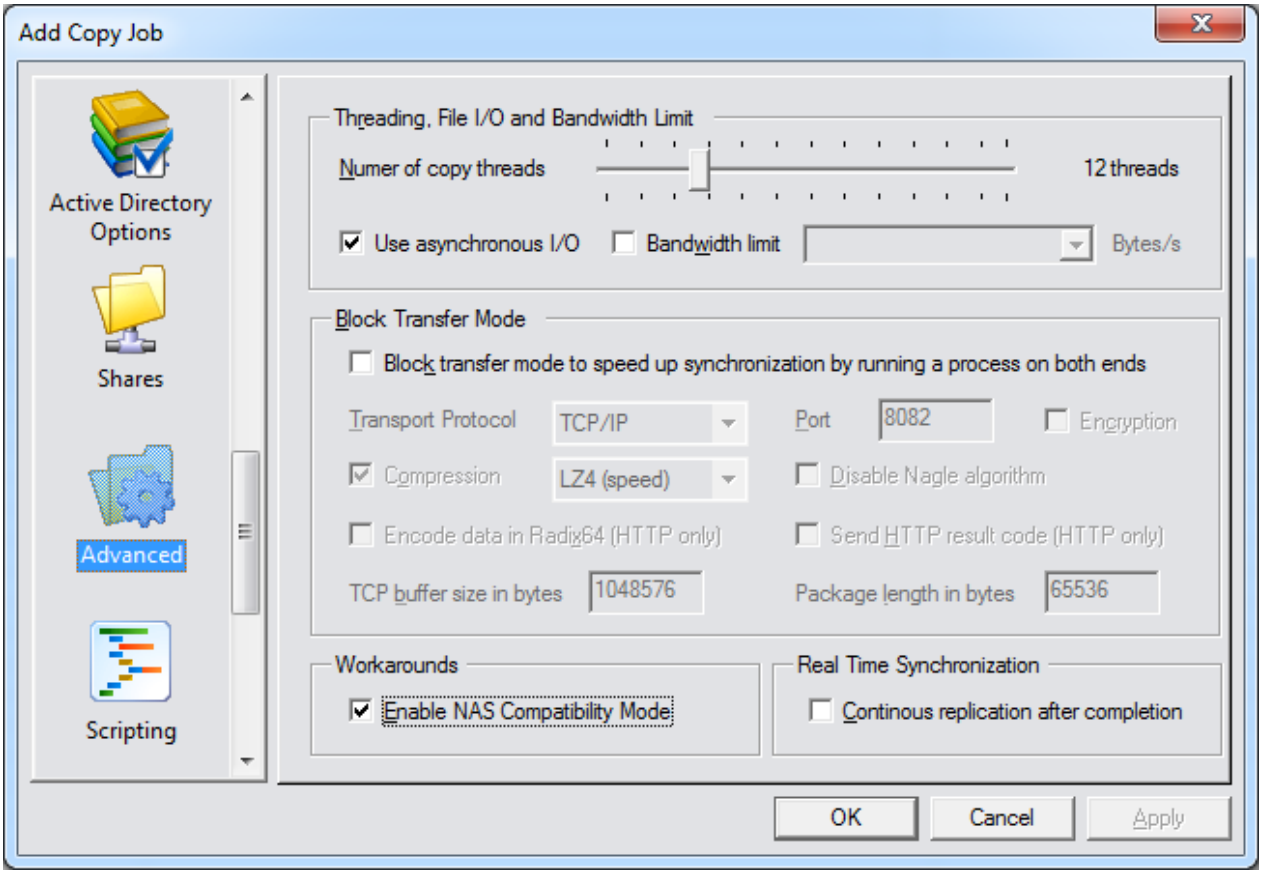
Administrative override is used in case NTFS permissions are locked down, preventing the account being used to run the migration, from accessing data on the source or writing it to the target. On Windows it uses privileges called Backup Files & Folders" and "Restore Files & Folders", which are granted by default to the local "Administrators" group and the "Backup Operators" group, allowing to bypass NTFS permissions in order to perform a backup or in this case a data migration.

Most NAS systems have a backup operators group that enables a functionality similar to the Windows "Backup Files & Folders" and "Restore Files & Folders" privileges for their members.

If there is no such group and you are getting an access denied error while migrating locked down folders, please try to connect to the NAS system using the built-in root account instead.

Access Denied Errors

In case of unexplainable access denied errors during the job execution, please try to check the "Enable NAS Compatibility Mode":



Synology NAS as Source

In case of a Synology NAS as source, please use the "OS Types, Roles and Domain Controllers" dialog to configure the domain.ini file accordingly (see chapter "OS Types, Roles and Domain Controllers"). Please add an entry for the Synology's NetBIOS name and enable the "Synology" OS Type along with the corresponding role "Auto detect" for workgroup mode, domain member along with a domain controller name the Synology belongs to or domain controller if the Synology is configured as a domain controller.

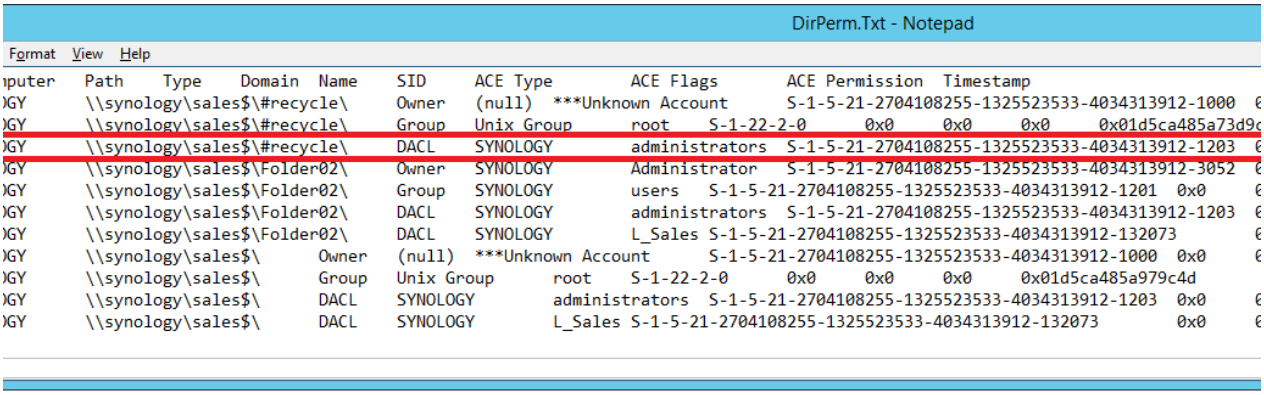
Additionally, you will have to find out the SID of the Synology's Administrators group. Usually this well-known group has a well-known SID of "S-1-5-32-44", but unfortunately not so on Synology, where the group has two SIDs. In NTFS and share level permissions a second SID is used that cannot be retrieved by any other way than inspecting a NTFS permission using this group account.

To find the SID, please run the following command against a Synology file share to dump the NTFS permissions into 4 text files:

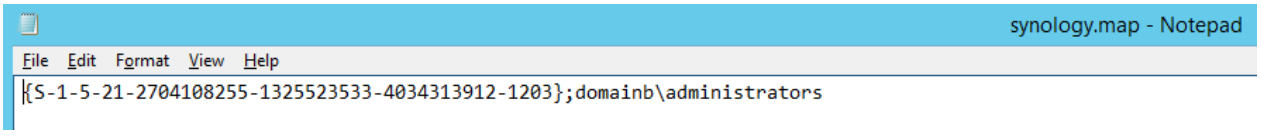
```
Copyright \\Synology\Sales$ /df /dfs /dd /dds /dh
```

Dump Synology File Share NTFS permissions

After running this command, you will find 4 files in the current working folder called File.Txt, FilePerm.Txt, Dir.Txt DirPerm.Txt. Next open up the DirPerm.Txt file to investigate the SIDs used in NTFS permissions:



Next copy the SID into a mapping file and store it for example as "Synology.Map" in the CopyRight2 installation folder:



In this example case, the data is migrated to a Windows domain controller, so the group is mapped to the domain's local Administrators group.

Please make sure you have the following in place:

- Proper configuration of the Synology in "OS Types, Roles and Domain Controllers".
- A mapping file, mapping the Administrators group of the Synology by SID to the local administrators group of your target (either the domain's local group or the member server's local group).

- Data copy job has migration of auditing (SACL) disabled, as this is currently not supported by Synology and other NAS systems.
- Data copy job has “NAS Compatibility Mode” enabled in the Advanced tab of the job definition.

You can either migrate user and group accounts implicitly with a data migration job or perform a two-phased migration where you migrate the users and groups with a “User and Group Migration” type of copy job and then the data with a “Data Migration” job.

Synology NAS as Target

In case of a Synology NAS as target, please use the “OS Types, Roles and Domain Controllers” dialog to configure the domain.ini file accordingly (see chapter “OS Types, Roles and Domain Controllers”). Please add an entry for the Synology’s NetBIOS name and enable the “Synology” OS Type along with the corresponding role “Auto detect” for workgroup mode, domain member along with a domain controller name the Synology belongs to or domain controller if the Synology is configured as a domain controller.

Please make sure you have the following in place:

- Proper configuration of the Synology in “OS Types, Roles and Domain Controllers”.
- Data copy job has migration of auditing (SACL) disabled, as this is currently not supported by Synology and other NAS systems.
- Data copy job has compression set to “Never” as this is not supported by Synology and other NAS systems.
- If the system is the target of a migration, a mapping file has to be defined, mapping the local Administrators group to another user or group, for example to “Domain Admins”. Otherwise instances of “Administrators” may show up as “root” on the target, for example as NTFS file or folder owner.
- The migration of file shares is disabled. File shares have to be created through the NAS administration interface.
- Data copy job has “NAS Compatibility Mode” enabled in the Advanced tab of the job definition.
- A share.ini file is present in the CopyRight2 installation folder, setting the “CopyRootPermissions” entry to 0 for the source system, to prevent overwriting the target shares root permissions from being overwritten!

If the system is the target of a migration, you can migrate users and groups in a first step. Then create the file shares on the target, using the NAS administration interface and finally migrate the data using a “Data” copy job.

There are several differences between the implementation of file shares on Windows and on Synology. On Synology a file share, shares a volume, while on Windows it is a folder that is being shared. This is by design and does not allow nested shares on a Synology for example. If you want to check if your source system has nested shares you can run a “copyright /ds /dh” command to produce a list of file shares and then check if those type of shares exist (see chapter “Export and Import of Users, Groups, Group Members and File Shares”).

Please make sure that shares are setup for advanced sharing if you want to maintain share level permissions and set those permissions identical to the share level permissions you had on the source system. Also make sure that you set the permissions identical to the NTFS permissions the shared folder had on the source system. Do not enable the migration of file shares in your data copy job!

To prevent overwriting the root level NTFS permissions, set within the Synology administration interface, define a share.ini file with a section for the source server of your migration:

```
[SRC-SERVER]
CopyRootPermissions=0
```

Share.Ini Example

The data copy job will still migrate NTFS permissions of any files and folders below the root level of the share.

If the Synology is the target and you want to map the local administrators group of the source to the domain admins group of the target domain, your mapping file should contain the following line:

```
\\SRC-MEMBER01\Administrators;TARGET-NETBIOS-DOMAIN\Domain Admins
```

Mapping File Example

Store the mapping file in UNICODE format in the CopyRight2 installation folder and assign it in the "ACL and Owner Permission" page of your data copy job.

Synology is supported in Workgroup mode, domain member mode or domain controller mode. You can use data migration and user and group migration type of jobs.

In case of any problems, please check that computer roles are detected properly in the resulting log file. It should show either Workgroup, Member or DC depending on the actual role along with the corresponding NetBIOS domain name.

If there are any problems during your migration, please contact Sys-Manage support.

Migration of Password Hashes from or to Synology NAS Systems

If you want to migrate password hashes of user accounts from or to a Synology NAS running as member server or configured with Synology Directory Server as a domain controller please ensure that you fulfill the following requirements:

1. Installed CopyRight2 Password Migration Add-On.

2. Installed Putty (32 or 64 bit). Plink.Exe is required for the SSH communication taking place with the Synology.

3. Enabled SSH service on port 22 in Synology web management interface (Control Panel -> Terminal & SNMP).

4. Defined the Synology as a Synology under Menu -> Options -> OS Types, Roles and DCs. Additionally, configure the proper role Domain Member or Domain Controller depending on the configuration of the Synology NAS.

5. Enable the "Migrate password" option in your Data or User and Group Migration job.

Support for Veritas Enterprise Vault

CopyRight2 supports Veritas Enterprise Vault. By default, any placeholders on the source servers will get retrieved by Enterprise Vault and then get copied over to the target. There are no special settings needed for that level of support, however, you need to ensure that the source drive(s) have sufficient disk space available to retrieve the content of all placeholders, which can be a potential problem. Additionally, more time will be needed if all placeholders are retrieved from the database and written to disk. Activating pass-thru in EV may be another possible strategy, to let EV leave the placeholder intact and forward the data from the database to the application (in this case CopyRight2).

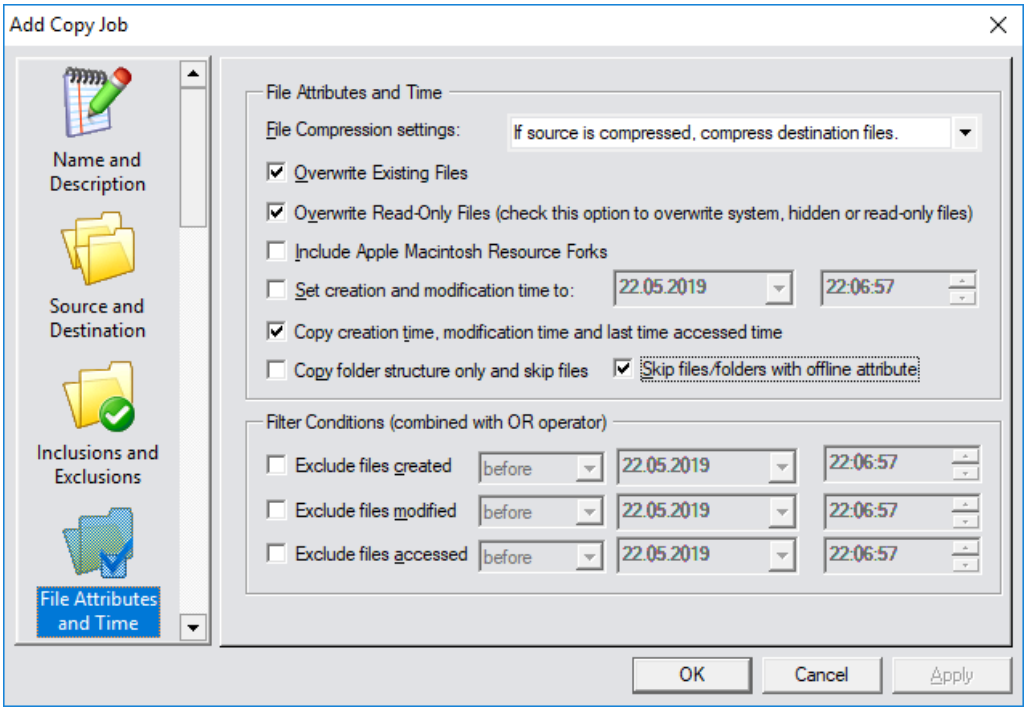
Below you can find two possible solutions, either skipping the placeholders and migrating them with FSAUtility or by copying the placeholders with CopyRight and then recalling the files from the databse with FSAUtility.

You can find more information about Veritas FSAUtility.Exe in the documentation:
https://www.veritas.com/content/support/en_US/doc/122261504-122261508-0/v40136615-122261508

Method 1: Skip offline files (placeholders) – Preferred Method

You can use a two-step approach to copy all the data that was not turned into a placeholder (or technically a Windows reparse point) and then use Veritas FSAUtility.Exe to copy the placeholders directly between source and target or to retrieve all placeholders from the Vault to their original location.

1. Copy the data having the “Skip files/folders with offline attribute” option checked from the “File Attributes and Time” page in your copy job definition to skip any placeholders during the copy process:



2. Either use Veritas FSAUtility.Exe to

   a) migrate the placeholders directly between source and target server (FSAUtility -pm)

   or

   b) retrieve all placeholders from the Veritas Vault (FSAUtility –c) to their original location.

Note: This method does not migrate any user or group accounts! If that should be required and you don't have enough disk space on the source or not enough time to fetch the data from the database, please revert to method 2, which will migrate any accounts used in permissions appropriately.

Method 2: Migrate placeholders with CopyRight2 & Recall them with FSAUtility

CopyRight2 can migrate the placeholders without having Enterprise Vault retrieving the file content if activating a specific option. This functionality can be enabled by enabling the corresponding setting in "Advanced Options". Please read the chapter "Advanced Options" for more information on how to enable this setting.

1. Activate copying of "Veritas Enterprise Vault" placeholders.

2. Close the CopyRight2 GUI and reopen it in case you had it open.

3. Run your copy job to copy the data including placeholders.

4. After the copy is done recall them using FSAUtility.Exe (FSAUtility -b) to convert them temporarily into the original files and then run the corresponding file system archiving task from the Enterprise Vault Administration Console to turn them into placeholders again.

Troubleshooting

Below is a list of known problems and solutions.

Error Message during Installation

A message box appears during installation reading “Error reading from file {path to a file}. Verify that the file exists and that you can access it”.

Solution: Please try to move the MSI installation file to a different location. This can occur because of the folder depth or because of security reasons. Please verify the MSI file’s security permissions.

Name Resolution Problems If Specifying Servers by IP Address

Solution: To enable name to IP resolution for specific computers, create a LMHOSTS file within the folder %systemroot%\system32\drivers\etc. It should have no file extension. Specify one line of text for each name you want to resolve to an IP address.

The format for member servers / computers is:
{IP Address} {Computer NetBIOS Name} #PRE

In case of a domain controller the format is:
{IP Address} {Computer NetBIOS Name} #PRE #DOM:{NetBIOS Domain Name}

Please make sure that you capitalize the letters for the “#PRE” or “#DOM” parameters.

After saving the file, open a command line prompt with administrative privileges and run the command “NBTSTAT –R” to load the LMHOSTS file. You can test name resolution by running a ping {Computer NetBIOS Name} command.

For example a LMHOSTS could look like this:

```
…
1.2.3.4 MYFILESERVER #PRE
5.6.7.8 MYDC #PRE #DOM:MYDOMAIN
…
```

LMHOSTS Example

Locked Files Cause Errors during File Copy

Solution: Please enable the “Ignore Locked Files” option on the copy job’s error processing tab.

While Moving a Share Server Internally an Error Indicates Share is Already Existing

Solution: Please enable the “Synchronize File Share” option within the copy job’s file share tab.

Error 266 Password Policy Problem While Synchronizing a User Account

Solution: This error occurs because the password of the user at the source computer fails the password policy at the destination computer. Please assign this user at the source computer a password that is not violating the password policy and then run this job again. The error should now disappear.

The System Freezes When Using the GUI of CopyRight2 on a VMWare Guest

Solution: This is a known VMWare bug with the VMWare SVGA II driver. Please switch to the standard VGA driver by updating the installed “VMWare SVGA II driver” to “Standard VGA” from within the device manager in control panel.

A Blue Screen Occurs During File Copy

Solution: Usually blue screens are caused by underlying system drivers. Please check for updates of your drivers for your hard drive controller, network adapter and graphic card. Some customers experienced blue screens because of outdated VPN access software while trying to copy over a VPN connection.

DFS Copy Job feature is not showing up

Solution: In case you updated and under the condition that the “DFS Copy Job” is not showing up in the CopyRight2 GUI, please uninstall CopyRight2 and reinstall it. This step will be required one time only and will cleanup existing registry keys.

Error 84 or 77 when copying data between servers because of Virus Protection

This error can occur if the file in question was deleted by a Virus Scanner at the destination. Please verify if you can copy the file manually, using Windows Explorer, from the source to the destination. After copying it, press F5 to refresh the destination directory. If the file is gone after refreshing, it was most likely deleted by a virus scanner. This can happen if the source computer uses no virus scanner at all or uses a different manufacturer or version or virus database version. Please check the log file of the virus scanner running at the destination computer.

To validate if the file in question contains a virus or other malicious code, we recommend to use the online virus scanner “http://www.virustotal.com”.

Network Problems Causing Windows Error 59 or 64

These two errors can occur in conjunction with different CopyRight2 internal error codes if there are problems during communication with the source or destination computer.

Windows Win32 Error Code	Description
59	An unexpected network error occurred.
64	The specified network name is no longer available.

It could be caused by hardware or software problems on the source, the destination or anywhere in between the two systems, such as firewalls or network components like cables, hubs, switches or routers.

You could try to reboot both, the source and the destination system, which can sometimes resolve the problem.

If this should not resolve the issue you could try to increase network timeouts to give the outstanding network requests more time to complete, by increasing the SMB session timeout parameter in the registry. The registry value is called “SessTimeout” and is of type REG_DWORD and located in the registry key “HKLM\System\CurrentControlSet\Services\LanmanWorkstation\Parameters”. You could try to increase the value to 300 (decimal) for 5 minutes. This change requires a reboot before the new setting takes effect.

If the problem should still occur, you could try to increase the number of retries the TCP/IP stack uses for the transmission of data. The corresponding registry value is called “TcpMaxDataRetransmissions” and is of type REG_DWORD and located in the registry key “HKLM\System\CurrentControlSet\Services\Tcpip\Parameters”. You could try to increase the number of retries to 10 (decimal). This change requires a reboot before the new setting takes effect.

Authentication Problem Migrating from or to Windows Workstations

If you are getting prompted for a password repeatedly, even though the password and user account entered are correct, it could be because of the default security restrictions on Windows workstation operating systems preventing remote administration. This problem does not occur with Windows server operating systems.

Please follow the steps below to configure Windows workstation operating systems for remote administration:

1. Make sure to run Windows update.

2. Ensure that the firewall allows SMB/NetBIOS communication between source and destination or if using CopyRight2 on a 3rd computer between this 3rd computer and both source and destination. You will have to allow incoming TCP port 445 or alternatively TCP/UDP ports 137 & 138 (NetBIOS over TCP/IP) on the destination. If migrating passwords this is a requirement on the source and on the destination system.

3. Make sure that the Windows Remote Administration service on the destination system. This service is disabled by default on workstation operating systems.

4. Use regedt32.exe to set "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\LocalAccountTokenFilterPolicy" to REG_DWORD 1 on the destination system. This is required on Windows workstation operating systems to allow delegation of administrative contexts.

5. Reboot the destination system.

Error 89 if Copying to a System That Does Not Support File Level Compression

If you are copying files that have the compression attribute set to a system that does not support compression, you will get an error 89 with a corresponding Win32 error code. In this case please select the "Never compress destination files" option in the copy job's settings in the "File Attributes and Time" tab to resolve the issue.

Error 3500 (Win32Err=87) During Password Migration

Please check if you are running some kind of Anti Virus or Host Intrusion Prevention system on the target server. If yes, please have a look at the solutions log files. You may have to add an exception for CopyRight2's CrPwdSvc.Exe file.

Firewall Configuration

CopyRight2 requires the following network ports depending on the copy job's configuration, depending on where you run the software at (source, destination or on a 3rd computer):

Description	Source (Push)	Destination (Pull)	3rd Computer
Copying from source to destination running the software on source without password migration.	Outgoing traffic to destination using either TCP port 445 or TCP/UDP ports 137 & 138 if using NetBIOS over TCP/IP.	Incoming traffic from source to either TCP port 445 or TCP/UDP ports 137 & 138 if using NetBIOS over TCP/IP.	-
Copying from Source to Destination running the software on destination without password migration.	Incoming traffic from destination to either TCP port 445 or TCP/UDP ports 137 & 138 if using NetBIOS over TCP/IP.	Outgoing traffic to source using either TCP port 445 or TCP/UDP ports 137 & 138 if using NetBIOS over TCP/IP.	-
Copying from Source to Destination running the software on source or destination and if password migration is enabled.	Incoming traffic from destination to either TCP port 445 or TCP/UDP ports 137 & 138 if using NetBIOS over TCP/IP.	Incoming traffic from source to either TCP port 445 or TCP/UDP ports 137 & 138 if using NetBIOS over TCP/IP.	-
Copying from Source to Destination running the software on source without password migration.	Incoming traffic from 3rd computer to either TCP port 445 or TCP/UDP ports 137 & 138 if using NetBIOS over TCP/IP.	Incoming traffic from 3rd computer to either TCP port 445 or TCP/UDP ports 137 & 138 if using NetBIOS over TCP/IP.	Outgoing traffic to source and destination using either TCP port 445 or TCP/UDP ports 137 & 138 if using NetBIOS over TCP/IP.
Using the block transfer protocol to enable byte level copy, reusing existing data at the destination to minimize traffic if copying across high latency WAN links using the GUI on source.	Outgoing traffic to destination using either TCP port 445 or TCP/UDP ports 137 & 138 if using NetBIOS over TCP/IP. Additionally incoming & outgoing traffic to the TCP port configured in advanced settings (default 8082).	Incoming traffic from source to either TCP port 445 or TCP/UDP ports 137 & 138 if using NetBIOS over TCP/IP. Additionally incoming & outgoing traffic to the TCP port configured in advanced settings (default 8082).	-
Using the block transfer protocol to enable byte level copy, reusing existing data at the destination to minimize traffic if copying across high latency WAN links using the GUI on destination.	Incoming traffic from destination to either TCP port 445 or TCP/UDP ports 137 & 138 if using NetBIOS over TCP/IP. Additionally incoming & outgoing traffic to the TCP port configured in advanced settings (default 8082).	Outgoing traffic to source using either TCP port 445 or TCP/UDP ports 137 & 138 if using NetBIOS over TCP/IP. Additionally incoming & outgoing traffic to the TCP port configured in advanced settings (default 8082).	-

Description	Source (Push)	Destination (Pull)	3rd Computer
Using the block transfer protocol to enable byte level copy, reusing existing data at the destination to minimize traffic if copying across high latency WAN links using command line version on source (/MSyncSend) and destination (/MSyncReceive).	Incoming & outgoing traffic to the TCP port configured in advanced settings (default 8082).	Incoming & outgoing traffic to the TCP port configured in advanced settings (default 8082).	-
IIS Site Migration job, migrating "Connect as" credentials for sites or virtual directories. (*)	Incoming TCP port 135 (DCOM Mapper) on destination system for source system. On Pre-Windows 2008: Incoming TCP port range 1024-4999 on destination system for source system. Windows 2008 and newer: Incoming TCP port range 49152-65535 on destination system for source system.	Incoming TCP port 135 (DCOM Mapper) on source system for destination system. On Pre-Windows 2008: Incoming TCP port range 1024-4999 on source system for destination system. Windows 2008 and newer: Incoming TCP port range 49152-65535 on source system for destination system.	Incoming TCP port 135 (DCOM Mapper) on source and destination system for 3rd computer. On Pre-Windows 2008: Incoming TCP port range 1024-4999 on source and destination system for 3rd computer. Windows 2008 and newer: Incoming TCP port range 49152-65535 on source and destination system for 3rd computer.

(*) The TCP port range required for DCOM can be configured to a fixed port if required. To do so, use dcomcnfg.exe and configure the ahadmin object in "DCOM Config". Next select the "Endpoints" tab, select "Connection-oriented TCP/IP" and then "Use static endpoint" to assign the TCP port to use instead of the range. This has to be done on the remote system if running on source (push) or destination (pull) or in case of running CopyRight2 on a 3rd computer on the source and on the destination.

Source or Target NAS Role Shows up as Workgroup Mode Instead of Domain Member

If you have a NAS as source or target, there are cases where the role is incorrectly identified as workgroup mode instead of domain member. This problem usually occurs because some Windows API's, that are not important during "normal" use of the system, are not 100% compatible. A side effect of this problem, is that the domain name is not identified and it will show the computer name instead in the job's log file. This in turn can lead to follow up problems, like the program attempting to migrate domain accounts to the target system, even though the source and target systems are in the same domain.

In this case you can create a domain.ini file in the CopyRight2 installation folder and tell CopyRight2 the domain

controller to use for this system. This is also helpful in case the network infrastructure (subnets) are not configure correctly in Active Directory Sites & Services.

Here is a “domain.ini” example, configuring CopyRight2 to use domain controller “DC99” for the NAS having the NetBIOS name “NAS01” and the domain controller “DC321” for the NAS having the NetBIOS name “NAS-123”. After placing the file in the CopyRight2 installation folder, running the job should produce the correct domain membership role and domain name in the job’s log file:

```
[NAS01]
DomainController=DC99

[NAS-123]
DomainController=DC321
```

Domain.ini example

During a large scale migration, you can configure the domain controllers using the migration rollout planner for each source and target system, for example during CSV file import.

Slow Performance Due to Anti-Virus Real-time Scan on Source and/or Target

If you should experience slow performance during file copy, please check if any Anti-Virus (or Windows defender) real-time scan is enabled and try to disable it. Windows defender is especially slow if processing ZIP files, because it relies on Windows built-in zip engine. After the migration completed you can run a full scan on the target to make sure it is clean.

Unexplainable Errors Due to Anti-Virus Real-time Scan

During a data migration, all files will be touched on the source server and all the data will be written to the target. If there is a real time Anti-Virus running, it will intercept those calls and do a full scan for each file. If both, source and target run an Anti-Virus, this effectively means that every file will get scanned twice (see “Slow Performance Due to Anti-Virus Real-time Scan on Source and/or Target”. For a user mode software, such as CopyRight2, it is by design impossible to prevent that interception/detection.

If there is a different version of the Anti-Virus software running or software of a different vendor or a different virus signature database, you may encounter situations where the source server does not detect something as a virus, but the target does. In some cases, this will really indicate that a virus was found, in other cases it could be a so-called false positive, especially if there is a heuristic detection method being used, not relying on a signature database. If in doubt, we usually recommend to use virustotal.com (a google company) to scan the data with 60+ virus scanners in parallel, in case you want to find out if it is really a virus or a false positive.

Unfortunately, we have no influence on the actions of the Anti-Virus software after a detection happens. In most cases, it will interrupt the current operation. This could be an open, read or write operation and it will then fail with an error code that may differ depending on the Anti-Virus software used. In most cases it will be “Access Denied”. Some Anti-Virus software will go further and place the software it identified as offending into some type of “jail” to limit its activities. In this case it is unfortunately CopyRight2, because it has read or even worse written what the Anti-Virus thinks is possibly a virus. If this should happen, please check the log files of your Anti-Virus and make exceptions as necessary.

The best way to circumvent those problems altogether and to prevent having to spend time on virus analysis, we recommend to turn it off during the course of the migration, at least on the target. Run a full scan on the source of all files, to make sure that the source data is virus free, from the perspective of the Anti-Virus you are using, to prevent it from interrupting the migration. You can enable the Anti-Virus on the target after the migration is completed and run a full scan as well.

Administrators Prompted with „You Don't Currently Have Permission to Access This Folder"

After a migration to a new server, administrators may get prompted with "You don't currently have permission to access this folder" allowing them to click on "Continue" to have access permanently granted. After clicking on "Continue", the current user account will get added explicitly to the ACL with "Full Control".
The reason for that is that Windows UAC (User Account Control) is enabled and the Administrator is logged in with a non-built-in account being member of either the "Domain Admins" or the "Local Administrators" group. This behavior is by design and the problem usually occurs if transitioning between a server having UAC turned off and a server having UAC turned on. UAC was introduced with Windows 2008 R2 and is enabled by default.
If UAC is enabled, an account logging on belonging to an administrative group will get a duplicated logon token having those memberships removed to reduce the account to a regular user account. This restricted token is used to start the window session after logging on. Subsequently any tasks started will run with this restricted logon token. This also applies to Windows Explorer. A duplicate of the full token, having those memberships and granting administrative access, is stored and used only if an administrator chooses to run a task with "Run as Administrator" or if an application requests during startup to run with administrative permissions. Both require a confirmation of the user before the program is actually started.

The reason for this design choice is to reduce the attack surface of some malware accidentally launched by an administrator.

Possible Workarounds:

- Login as built-in Administrator. The built-in Administrator account has UAC turned off.
- Educate the administrators to convince them of the advantage UAC provides.
- Change UAC to the same level the source server had. While this may not be the optimal setting, it will not be less secure than your previous configuration.
- Use another tool to administer the file services. These tools allow you to start elevated, with the administrative permissions. For example, without endorsing any specific product: "Explorer++", "Total Commander", "Free Commander", …
- Terminate Exporer.Exe with Task-Manager or by holding the "Ctrl" & "Shift" key and then opening up the start menu and right clicking on the menu to run the "Exit Explorer" command. Next start "Explorer.Exe" with "Run as Administrator".
- Grant access to a group such as "IT-Group" and put the administrators into that group. CopyRight2 can optionally add a custom account to each NTFS permission encountered either on-the-fly, while copying data, or without moving data if using a "Security & Attributes" type of job in conjunction with a mapping file (see chapter "CREATING A MAPPING DEFINITION FILE TO REASSIGN PERMISSIONS"). This will prevent administrators from having to confirm to get access to each folder, because the account is a member of that group and this group is not removed from the logon token by UAC as this is only done to the built-in admin groups. You can specify an additional account to add to every NTFS permission by providing a "domain.ini" file containing a section with the NetBIOS name of the source or target computer of the copy

job with the following content:

[SRC-COMPUTER]
AddAdminAccount=MYDOMAIN\MYGROUP

UAC configuration and the resulting security impact:

UAC Configuration	Description
UAC turned OFF	With UAC turned off the result will be the biggest attack surface, because malware, usually ransom ware, can access all the data and even Windows system files (such as the System32 folder) with write permission.
UAC turned ON, Access granted to custom user or group account	Turning UAC on and previously granting additional permissions on your data to an individual account (user or group) on the target reduces the attack surface to all the data folders. System files (such as System32) would still be protected from access.
UAC turned ON (default setting)	Turning UAC on will reduce the attack surface to data folders, that the specific administrator has previously been granted access to by clicking on “Continue”. The attack surface will grow over time as administrators visit more and more folders during their daily work.
UAC turned ON + Accounts get automatically removed from NTFS permissions in an interval	To reduce the attack surface further, you could schedule a CopyRight2 “Security & Attributes” type of job that you run daily, weekly or monthly removing the permissions again, that were previously added after clicking on “Continue”. This provides ever better security than the Windows UAC default settings because the attack surface will not grow over time but get reset frequently. On the other hand, admins may face the “You don’t currently have permissions…” message more frequently. To do so, provide the job with a mapping file containing “1:0” mappings to remove all the administrator accounts (see chapter “CREATING A MAPPING DEFINITION FILE TO REASSIGN PERMISSIONS” of the CopyRight2 manual).

Note: Another disadvantage of the default UAC behavior is that it adds individual admin accounts to NTFS permissions. With that in mind, you may have to watch out if some administrator is for example leaving the “IT” department for the “Developer” department, thinking it would be sufficient to remove the account’s domain admin and administrator membership. Such an account may still have NTFS permissions scattered across the file system granting access. Instead it would be better to disabled the admin account and create a new user account in such a case.

Reference: https://support.microsoft.com/en-us/help/950934/when-you-click-continue-for-folder-access-in-windows-explorer-your-use

Cannot Find Computer or NAS System When Selecting Source Folder

When adding new source & destination path pairs to a Data Migration job, you can specify multiple source paths by selecting from a tree control and a single target path by providing the path in an edit field.

Depending on the scenario and the network configuration you may find yourself sometimes looking for a specific system that does not show up. This could for example be the case if it is in workgroup mode and the Windows browser service simply does not show it, either because of some problem or it has not yet been propagated. Or you may be you are logged on with a local account that does not have access to Active Directory, so there will be no "Active Directory" node to select from.

While the target path can be changed through an edit field, without selecting from the drop down tree control, you may have the need to add a computer to the source path selection tree.

This can be achieved by adding the domain, workgroup or computer manually. To achieve that, you can select "Microsoft Windows Network", then open up the context menu (right mouse button click) to add it using the "Add missing domain/workgroup…".

Likewise, if a computer you are looking for should be missing, you can select a workgroup or domain below "Microsoft Windows Network" and then use the context menu and "Add missing computer…" to add it. This only needs to be done once and will then be stored for future use. You can remove manually added workgroups, domains and computers the same way using the context menu.

Error 296 during sidHistory Migration

The occurrence of error 296 indicates an issue migrating sidHistory. The additional Win32 error is helpful to detect the root cause of the issue.

Win32 Error Code	Win32 Error Code Description	Possible Reason
5	"Access is denied"	This error can occur for multiple reasons: 1) Delegation restrictions: • Target Domain Controller: The computer object of the target domain controller may be configured to disallow delegation (e.g., "Do not trust this computer for delegation"). • User Account Restrictions: The account used for authentication in the target Active Directory may have the "Account is sensitive and cannot be delegated" setting enabled. 2) Domain Local Group Permissions: • Permissions on the domain local group in the source domain (formatted as the source domain's NetBIOS name + "$$$") may be

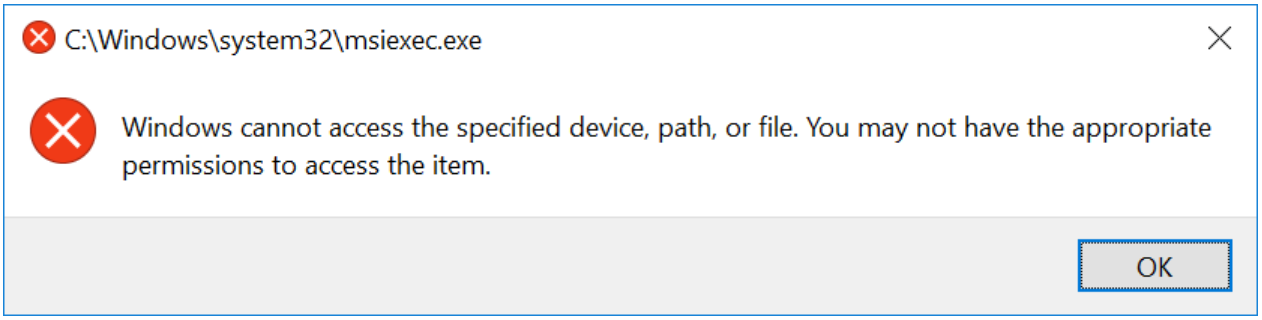
		restrictive. If the account used for the migration job or authentication to the target Active Directory lacks permission to modify this group's members, access will be denied.
6	"The handle is invalid"	1) Name Resolution Issue: The target domain controller cannot resolve the source domain controller's name to an IP address. 2) Firewall Blocking RPC Communication: A firewall between the source and target domain controllers may be blocking RPC communication, preventing the operation from succeeding.

Product Uninstallation from Settings -> Apps & Features Fails if UAC is Disabled

To work around the issue, you can either logon with a different user account that has UAC enabled or alternatively use the classic control panel -> Programs and Features.

This issue is a known limitation in Windows that arises when User Account Control (UAC) is disabled. This can happen either if UAC is turned off system-wide or if you log in using the built-in Administrator account, which automatically disables UAC for its session. The root cause appears to be a dependency between Windows' new Settings app and UAC.

When attempting to uninstall, the following error message may appear:



To resolve this issue, you can either:

1) Log in with a different user account that has UAC enabled, or

2) Use the classic Control Panel -> Programs and Features to complete the uninstallation process.

Contacting Support

Please specify the following information when contacting support:

1. Your product and build number (visible in about dialog, shown if you click on the blue question mark within the main application window)
2. Your source server operating system version, service pack level and processor architecture (x86 or x64)
3. Your destination server operating system version, service pack level and processor architecture (x86 or x64)
4. The role of the source server. Is it a domain member or a domain controller or in workgroup mode?
5. The role of the destination server. Is it a domain member or a domain controller or in workgroup mode?
6. The log file if applicable. CopyRight2's log file is located in the program's installation folder having the same name as the copy job with a ".LOG" file extension.
7. The copy job definition file if applicable. The copy job definition file, containing the settings of the copy job, is located in the CopyRight2 installation folder having the same name as the copy job with a ".JOB" file extension.

Our support might ask you for additional required information after receiving your support request.

Contact Information

If you should have further questions regarding the product or its documentation, please feel free to contact us any time:

By eMail:

Support@Sys-Manage.Com

By phone / fax:

Phone: +1 (408) 345-5199
Phone: +1 (360) 227-5673
Phone: +44 (0) 8455273028
Phone: +49-(0)69-99999-3099
Phone: +34-810 10 15 34
Fax: ++49-69-99999-3083