Quest

Binary Tree Migrator Pro for Active Directory 20.11.1

User Guide

© 2023 Quest Software Inc. ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc.

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

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

Quest Software Inc.

Attn: LEGAL Dept

4 Polaris Way

Aliso Viejo, CA 92656

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

Patents

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

Trademarks

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

Legend

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

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

Migrator Pro for Active Directory User Guide
Updated - September 2023

Contents

Migration Project Management

Migrator Pro for Active Directory Architecture

The first step towards success on a project using Migrator Pro for Active Directory is to understand the product architecture and how this architecture will operate in your environment.

Migrator Pro for Active Directory consists of the following components:

- A directory synchronization engine
- A REST based web service
- A management interface
- A lightweight agent for workstations and member servers
- A database running on Microsoft SQL Server

The directory synchronization engine, the web service, and the management interface will all access the same SQL database. In most scenarios, these components will be installed on the same system. In larger or more complex network environments, the components can be distributed across multiple systems. If the directory synchronization engine, the web service or the management interface is installed on a separate system, it is important to ensure that all three components retain access to the same SQL database.

The directory synchronization engine is provided by Binary Tree Directory Sync Pro for Active Directory. Directory Sync Pro for Active Directory is included as part of Migrator Pro for Active Directory. Directory Sync Pro for Active Directory is responsible for synchronizing users and groups between source and target Active Directory domains. Directory Sync Pro for Active Directory also handles migrating key user properties such as SID History and user passwords.

User workstations and member servers are called computers in Migrator Pro for Active Directory. Computers communicate with the Migrator Pro for Active Directory web service using the Migrator Pro for Active Directory Agent. The Migrator Pro for Active Directory Agent is a lightweight application that installs as a service on Windows computers. Upon installation, the agent has the ability to autodiscover the location of the Migrator Pro for Active Directory web service.

To ensure that no firewall exceptions are required, the web service does not “call” the workstations or servers to be migrated. Instead, the Migrator Pro for Active Directory Agents contact the web service at defined polling intervals, using standard HTTPS or HTTP requests to recover jobs. Jobs include key tasks such as system discovery, updating the operating system, file system, and user profile permissions, and migrating the computer to the new domain.

Planning the Migration Project

A typical migration project using Migrator Pro for Active Directory can be broken up into phases.

- Phase 1: Installing and Creating the Synchronization Profile within Directory Sync Pro for Active Directory

- Phase 2: Register Computers (Concurrent with Phase 3)
- Phase 3: Identify Users, Resources, Contacts, and Groups to Migrate (Concurrent with Phase 2)
- Phase 4: ReACL Computers and NAS
- Phase 5: Cutover Computers
- Phase 6: Cleanup

The Cleanup process typically occurs several months after the completion of the project.

Best Practices

Best practices for each phase of the migration project are presented below:

Phase 1: Installing and Creating the Synchronization Profile within Directory Sync Pro for Active Directory

- Directory Sync Pro for Active Directory is used to synchronize objects and must be installed before installing the Migrator Pro for Active Directory Console and Web Service.
- The AD Migration/Synchronization profile should be set up to include every computer. However, not every computer needs to be migrated immediately. This process ensures they are in the database, ready to install the Migrator Pro for Active Directory Agent and register themselves. Computers can be blacklisted if you do not want to immediately migrate them.
- Carefully consider the Group Collision option (Merge, Skip, Rename). It is recommended that this option is not changed once migrations have been started. Additionally, it is strongly recommended to not select the Skip option. The Merge and Rename options are better in most cases.
- Synchronizing SID History is recommended.

Phase 2: Register Computers (Concurrent with Phase 3)

- The Migrator Pro for Active Directory Agent should be pushed out to computers via Group Policy (GPO) or third party tool.
- Sufficient time should be allowed to address any issues with computer registration with the server. Correcting registration issues can take more time than expected. A typical large company with a large number of computers may need a couple of weeks of off and on work to resolve registration issues with all computers.

- Resolving computer registration issues can be accomplished concurrently with identifying users, rooms, contacts, and groups to Migrate in Phase 3.

Phase 3: Identify Users, Rooms, Contacts, and Groups to Migrate (Concurrent with Phase 2)

- Before migrating users and groups, do some planning and analysis to see what users, rooms, contacts, and groups should be migrated, what groups need to be consolidated, how duplicates will be handled, etc.
- More than one synchronization profile can be used to control the target destinations of users, rooms, contacts, and groups.
- User Accounts should be disabled in the target.
- Identifying users, rooms, contacts, and groups to Migrate can be accomplished concurrently with resolving computer registration issues in Phase 2.

Phase 4: ReACL Computers and NAS

- Run a ReACL on as many computers as possible early in the process.
- ReACL is a non-destructive process that can be repeated as often as necessary up until Cutover in Phase 5.
- Troubleshoot any computers that did not successfully complete ReACL.
- Run a ReACL again close to the actual cutover date. This will allow you to complete most of the ReACL process early and provide time to resolve any issues with things such as anti-virus software and Group Policies.

Phase 5: Cutover Computers

- Create some test users, groups, and computers to verify a successful user and group migration and computer cutover.
- Create any custom jobs that may be required to run against users, rooms, groups, contacts or computers.
- Typically, a final ReACL would be run the weekend before the cutover to ensure any new users and other changes are processed.
- A workstation reboot is required after the target account is enabled, the source account is disabled, and the workstation cutover is complete. This is usually completed in the evening when fewer users are affected. The affected users should be alerted that this reboot is necessary.

Phase 6: Cleanup

- The cleanup phase typically takes place about two months after all device cutovers are complete. During the Cleanup phase, all permissions should be removed from the source domain and then the Migrator Pro for Active Directory Agent should be removed from the devices.
- Before executing the cleanup job to complete the cleanup process it is recommended that you disable SID filtering/quarantine to verify that there are no issues with application access.

Configuring the Synchronization Profile

A Synchronization profile must be created in Directory Sync Pro for Active Directory. Refer to the Directory Sync Pro for Active Directory documentation for AD Migration/Synchronization and Exchange Migration for detailed information on creating a Synchronization profile.

Using the Active Directory Pro Console

Refreshing Data

Use the Refresh View option to refresh the data currently displayed in the table. The refreshed data will display all previous changes to the database and the currently available Action menu options. All selected filter options will not be affected by refreshing.

To refresh the data displayed in the table:

1. Click REFRESH VIEW.

Migration Waves

Objects in the table can be grouped into Migration Waves for migration process management. Migration Waves allow for filtering to be able to sync smaller groups of objects. An item can be part of a single Migration Wave only.

To set Migration Wave for objects:

1. Select one or more objects in the list.
2. Select **Set Migration Wave** in the Actions menu and click the **Apply Action** button.
3. Select an existing Migration Wave from the drop-down list or click **New** to create a new Migration Wave for the selected objects. To remove a previously selected Migration Wave, select **<None>** from the drop-down list.
4. If creating a new Migration Wave, enter a Migration Wave name.
5. Click **Save**. The Migration Wave column is populated for the selected objects.

Import Migration Wave

The Import Migration Wave feature assigns objects to migration waves based on object name & Migration Wave name pairs listed in a CSV file.

- Object names can be the sAMAccountName (for Users, Rooms, Groups, and Computers) or the Distinguished Name (for Users, Rooms, Contacts, Groups, and Computers).
- Duplicate objects in the CSV file will not be assigned to a Migration Wave.

To import Migration Wave values:

1. Click the **Import Wave** button.
2. Click the **Choose File...** button.

3. Select a CSV file containing the object names and Migration Wave names and click **Next**.
   The CSV file should have two columns. The first column contains Object names and the second column contains Migration Wave names. An example file is below:
   jsmith,Windows 7 Group
   mjones,Windows 7 Group
   jtaylor,Windows 8 Group
   An example file entry for Contacts is below:
   CN=John Smith,DC=domain,DC=dom,Windows 7 Contacts

Using Exclusion Lists

Objects can be added to the exclusion list. Objects on the exclusion list will not be displayed unless the Show Blacklisted button is selected. Most actions cannot be selected for blacklisted objects.

To add objects to the exclusion list:

1. Select one or more objects in the list.
2. Select **Add to Exclusion list** in the Actions menu and click the **Apply Action** button. The selected objects are removed from the displayed list.
3. Click the **Show Exclusion listed** button to view the exclusion listed objects.

To remove objects from the exclusion list:

1. Click the **Show Exclusion listed** button to view the exclusion listed objects.
2. Select one or more objects in the list.
3. Select **Remove from Exclusion list** in the Actions menu and click the **Apply Action** button. The selected objects are removed from the displayed list.
4. Click the **Hide Exclusion listed** button to view the non-exclusion listed objects.

Filtering, Searching, and Sorting Tables

The data table can be filtered, searched, and sorted by column.

Filtering

To filter the data table by Synchronization Profile:

1. Select a profile from the Profiles drop-down list. The table is updated to display only objects associated with the selected profile. By default, objects from All Profiles are displayed.

To filter the data table by Migration Wave:

1. Select a Migration Wave from the Migration Wave drop-down list. The table is updated to display only objects in the selected Migration Wave. By default, objects from All waves are displayed.

Searching

To search the data table:

1. Enter text in the Search box.
2. Click the Search icon. Fields are only searched if that column is selected to be displayed in the table.

SORTING

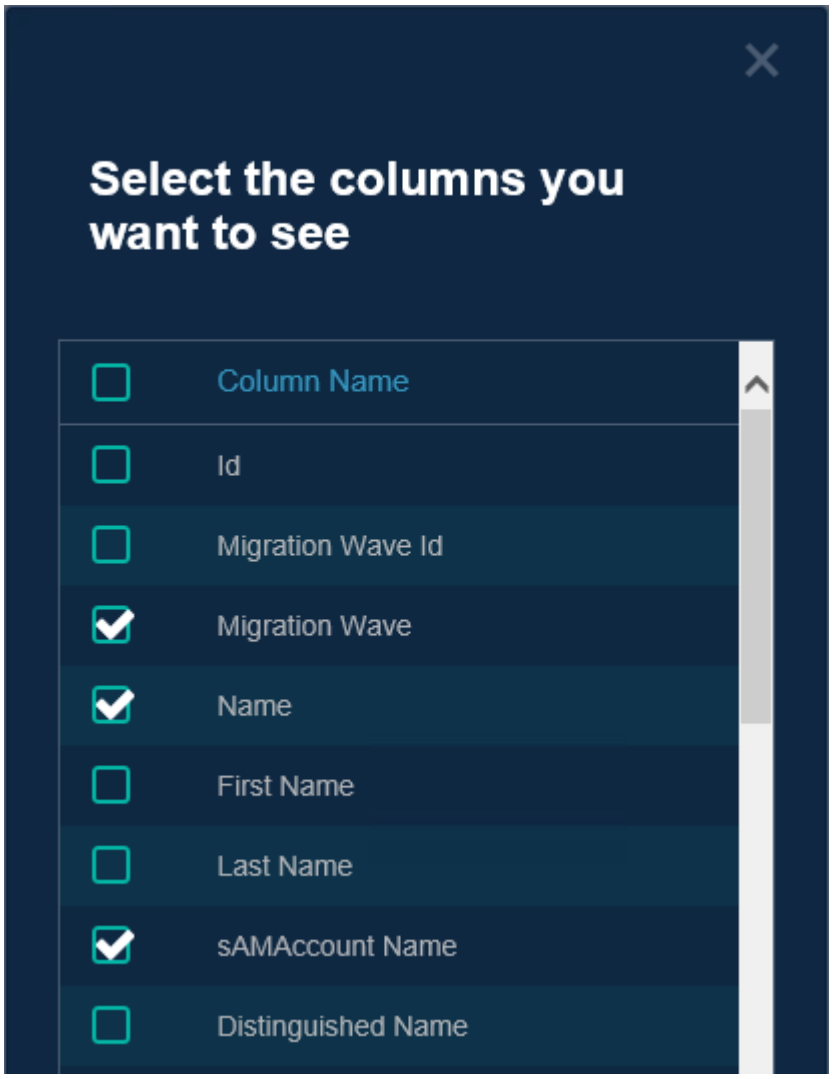
To sort the data table by column headers:

1. Click on a column header to sort the table by that column in ascending order.
2. Click the column header again to sort the table by that column in descending order.

Customizing Columns

The default data tables do not display every available column. However, the displayed columns can be customized. To choose displayed columns:

1. Click the **Gear** icon in the table header. The Select columns window appears.



2. Select the columns to display in the table.
3. Click **OK**. The table is updated with the selected columns.

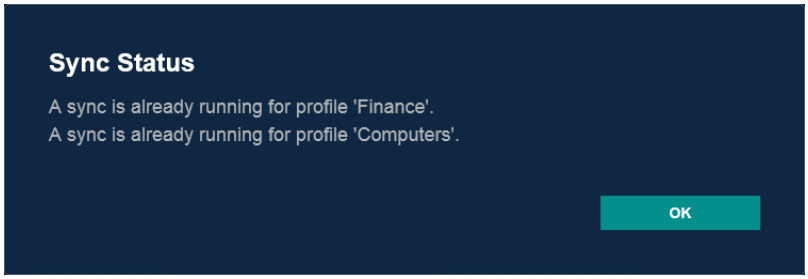
Triggering a Sync

Use the Run Sync button to sync the data currently displayed in the table. If **All Profiles** is selected, all of the Synchronization Profiles will be synchronized. Select a Synchronization Profile before starting a sync to synchronize only that profile. If a Synchronization Profile has been set to synchronize on a schedule, manually starting a sync is not necessary.

Only objects marked as "Sync Enabled" will be synced to the target.

To sync the data displayed in the table:

1. Click the **Run Sync** button.
2. After clicking the Run Sync button the following confirmation for the sync of the selected Synchronization Profiles will be displayed.



Exporting the Table

The view as it is currently sorted and filtered can be exported to a file.

To export the table:

1. Click the **Export** button below the table.
2. Enter a file name, select a type and then click **Export**.
3. Use the browser option to save and open the file.

Migration Actions

Migrating Users

The User Actions screen allows Users to be synced to the target as well as enabled and disabled on the source or target before cutover occurs.

Sync Users

To sync Users to the target:

1. Select one or more Users in the list.
2. Select **Sync Enabled** from the Actions menu and click the **Apply Action** button. The Sync Status column displays "Sync Enabled" for the selected Users. The selected Users are synced during the next synchronization cycle (scheduled in Directory Sync Pro for Active Directory or triggered manually with the Run Sync button in Migrator Pro for Active Directory).
3. To prevent the Users from syncing, select the Users, select **Sync Disabled** in the Actions menu, and click the **Apply Action** button.

Enable and Disable Users

To enable/disable Users on the source or target.

1. Select one or more Users in the list.
2. Select one of the following options from the Actions menu and click the **Apply Action** button:
    - **Enable on Target only**
    - **Enable on Target/Disable on Source**
    - **Enable on Source only**
    - **Enable on Source/Disable on Target**

    The Source UAC and/or Target UAC columns of the selected users is updated.

Mark as Migrated

As an optional way to mark which Users are fully completed and require no further action, the Migration Status column can be marked as " Migrated":

1. Select one or more Users in the list.
2. Select **Mark as Migrated** from the Actions menu and click the **Apply Action** button. The Migration Status column displays "Migrated" for the selected Users.

Admin Agent Menu Actions

If any Admin Agent actions have been created for Users, they will appear in the Actions menu:

1. Select one or more Users in the list.
2. Select an Admin Agent action from the Actions menu and click the **Apply Action** button.
3. In the Job Options window, check **Do not start before** and enter a date and time if you do not want the job to begin immediately. Select the **Admin Agent** and the **Agent Admin Credentials** to use from the drop-down lists.
4. Click **OK**. The Queue Summary appears.
5. Click **OK**.

User Columns

The following columns appear on the User Actions screen by default:

- Migration Wave- The Migration Wave name. Use the Actions menu **Set Migration Wave** option to change.
- Name - The name attribute of the source user account.
- sAMAccountName - The sAMAccountName attribute of the source user account.
- Blacklisted - This column is checked if the user is currently on the exclusion list. Use the Actions menu **Add to Exclusion list** option or **Remove from Exclusion list** option to change.
- Migration Status - This column displays an optional tag that can be manually set to track migration progress. Use the Actions menu **Mark as Migrated** option to change.
- Sync Status - This column displays "Sync Enabled" if the user account is currently ready to sync. Use the Actions menu **Sync Enabled** option or **Sync Disabled** option to change.
- Source UAC - This column indicates if the user account is enabled in the source. Use the Actions menu Enable/Disable User options to change.
- Target UAC - This column indicates if the user account is enabled in the target. Use the Actions menu Enable/Disable User options to change.
- Last Sync - Displays the date/time of the last sync.

The following additional fields can be displayed by customizing the columns:

- ID - SQL record number
- Migration Wave ID
- First Name
- Last Name
- Distinguished Name
- Target Distinguished Name
- Description
- Assistant
- Created

- Migrated
- Alias
- Assistant
- Company
- Country
- Country Code
- Country Name
- Deleted Item Flags
- Delivery Content Length
- Department
- Department Number
- Division
- Employee ID
- Employee Number
- Employee Type
- Extension 1 - 15
- Manager
- Object SID

Migrating Resources

The Resource Actions screen allows rooms and resources to be synchronized to the target.

Sync Resources

To sync Resources to the target:

1. Select one or more Resources in the list.
2. Select **Sync Enabled** from the Actions menu and click the **Apply Action** button. The Sync Status column displays "Sync Enabled" for the selected resources. The selected resources are synced during the next synchronization cycle (scheduled in Directory Sync Pro for Active Directory or triggered manually with the Run Sync button in Migrator Pro for Active Directory).
3. To prevent Resources from syncing, select the Resources, select **Sync Disabled** in the Actions menu, and click the **Apply Action** button.

Admin Agent Menu Actions

If any Admin Agent actions have been created for Resources, they will appear in the Actions menu:

1. Select one or more Resources in the list.
2. Select an Admin Agent action from the Actions menu and click the **Apply Action** button.
3. In the Job Options window, check **Do not start before** and enter a date and time if you do not want the job to begin immediately. Select the **Admin Agent** and the **Agent Admin Credentials** to use from the drop-down lists.
4. Click **OK**. The Queue Summary appears.
5. Click **OK**.

Resource Columns

The following columns appear on the Resource Actions screen by default:

- Migration Wave - The Migration Wave name. Use the Actions menu **Set Migration Wave** option to change.
- Room Number - The room number attribute of the source room.
- Distinguished Name - The distinguished name attribute of the source room.
- Target Distinguished Name - The distinguished name attribute of the target room. This column is populated when a room is synced.
- Description - The description attribute of the source room.
- Blacklisted - This column is checked if the room is currently on the exclusion list. Use the Actions menu **Add to Exclusion list** option or **Remove from Exclusion list** option to change.
- Sync Status - This column displays "Sync Enabled" if the resource is currently ready to sync. Use the Actions menu **Sync Enabled** option or **Sync Disabled** option to change.
- Created - This column is checked if the room has been created in the target.
- Last Sync - Displays the date/time of the last sync.

The following additional fields can be displayed by customizing the columns:

- ID - SQL record number
- Migration Wave ID
- Alias
- Assistant
- Company
- Country
- Country Code
- Country Name
- Deleted Item Flags
- Delivery Content Length
- Department
- Department Number
- Division
- Extension 1 - 15

- Manager
- Object SID

Migrating Contacts

The Contact Actions screen allows contacts to be synchronized to the target.

Sync Contacts

To sync Contacts to the target:

1. Select one or more Contacts in the list.
2. Select **Sync Enabled** from the Actions menu and click the **Apply Action** button. The Sync Status column displays "Sync Enabled" for the selected Contacts. The selected Contacts are synced during the next synchronization cycle (scheduled in Directory Sync Pro for Active Directory or triggered manually with the Run Sync button in Migrator Pro for Active Directory).
3. To prevent the contacts from syncing, select the Contacts, select **Sync Disabled** in the Actions menu, and click the **Apply Action** button.

Admin Agent Menu Actions

If any Admin Agent actions have been created for Contacts, they will appear in the Actions menu:

1. Select one or more Contacts in the list.
2. Select an Admin Agent action from the Actions menu and click the **Apply Action** button.
3. In the Job Options window, check **Do not start before** and enter a date and time if you do not want the job to begin immediately. Select the **Admin Agent** and the **Agent Admin Credentials** to use from the drop-down lists.
4. Click **OK**. The Queue Summary appears.
5. Click **OK**.

Contact Columns

The following columns appear on the Contact Actions screen by default:

- Migration Wave - The Migration Wave name. Use the Actions menu **Set Migration Wave** option to change.
- First Name - The first name attribute of the source Contact.
- Last Name - The last name attribute of the source Contact.
- Distinguished Name - The distinguished name attribute of the source Contact.
- Target Distinguished Name - The distinguished name attribute of the target contact. This column is populated when a Contact is synced.
- Description - The description attribute of the source Contact.

- Blacklisted - This column is checked if the Contact is currently on the exclusion list. Use the Actions menu **Add to Exclusion list** option or **Remove from Exclusion list** option to change.
- Sync Status - This column displays "Sync Enabled" if the contact is currently ready to sync. Use the Actions menu **Sync Enabled** option or **Sync Disabled** option to change.
- Created - This column is checked if the Contact has been created in the target.
- Last Sync - Displays the date/time of the last sync.

The following additional fields can be displayed by customizing the columns:

- ID - SQL record number
- Migration Wave ID
- Alias
- Assistant
- Company
- Country
- Country Code
- Country Name
- Deleted Item Flags
- Delivery Content Length
- Department
- Department Number
- Division
- Employee ID
- Employee Number
- Employee Type
- Extension 1 - 15
- Manager
- Object SID

Migrating Groups

The Group Actions screen allows Groups to be synchronized to the target.

How different types of groups (Domain Local, Global, and Universal Group) are created on the target and how group collisions are handled is defined on the AD Target Options of the synchronization profile.

Sync Groups

To sync Groups to the target:

1. Select one or more Groups in the list.
2. Select **Sync Enabled** from the Actions menu and click the **Apply Action** button. The Sync Status column displays "Sync Enabled" for the selected Groups. The selected Groups are synced during the next synchronization cycle (scheduled in Directory Sync Pro for Active Directory or triggered manually with the Run Sync button in Migrator Pro for Active Directory).
3. To prevent the Groups from syncing, select the Groups, select **Sync Disabled** in the Actions menu, and click the **Apply Action** button.

Admin Agent Menu Actions

If Admin Agent actions have been created for Groups, they will appear in the Actions menu:

1. Select one or more Groups in the list.
2. Select an Admin Agent action from the Actions menu and click the **Apply Action** button.
3. In the Job Options window, check **Do not start before** and enter a date and time if you do not want the job to begin immediately. Select the **Admin Agent** and the **Agent Admin Credentials** to use from the drop-down lists.
4. Click **OK**. The Queue Summary appears.
5. Click **OK**.

Group Columns

The following columns appear on the Group Actions screen by default:

- Migration Wave - The Migration Wave name. Use the Actions menu **Set Migration Wave** option to change.
- sAMAccountName - the sAMAccountName attribute of the source group account.
- Group Type - The type of group of the source group account.
- Distinguished Name - The distinguished name attribute of the source group account.
- Target Distinguished Name - The distinguished name attribute of the target group account. This column is populated when a group is synced.
- Description - The description attribute of the source group account.
- Blacklisted - This column is checked if the Group is currently on the exclusion list. Use the Actions menu **Add to Exclusion list** option or **Remove from Exclusion list** option to change.
- Sync Status - This column displays "Sync Enabled" if the Group is currently ready to sync. Use the Actions menu **Sync Enabled** option or **Sync Disabled** option to change.
- Created - This is checked if the group account has been created in the target.
- Last Sync - This column displays the date/time of the last sync.

The following additional fields can be displayed by customizing the columns:

- ID - SQL record number
- Migration Wave ID
- Alias

- Assistant
- Company
- Country
- Country Code
- Country Name
- Deleted Item Flags
- Delivery Content Length
- Department
- Department Number
- Division
- Extension 1 - 15
- Managed By
- Object SID

Migrating Computers

Workstations and Servers are referred to as Computers in Migrator Pro for Active Directory. The Computer Actions screen allows the administrator to register Computers, change the agent polling interval, set the ReACL profile, upload Computer migration logs, make a Computer an Admin Agent, and manage the Computer Discovery, ReACL, Cutover, and Cleanup processes.

The Migrator Pro for Active Directory Agent must be installed on a computer before it can be registered or have any actions applied to it. Refer to Installing the Migrator Pro for Active Directory Agent on Computers for more information.

Job Options

The Job Options view allows the administrator to effectively manage the server and workstation environment during the migration event by scheduling computer jobs to run at specific points of time in the future. Each job, when applied to a Computer, will open the Job Options view giving the option to set a “Do not start before” date and time. If a job is scheduled for a later date and time, then it sits in the job queue and is not considered an active job for that Computer when the agent polls for jobs.

View Jobs

To view Computer Jobs:

1. Select one or more Computers in the list.
2. Select **View Jobs** from the Actions menu and click the **Apply Action** button. The Computer Jobs window appears.

3. The Computer Jobs table includes the following columns:
    - Job ID - The ID of the job.
    - Queued Timestamp - The date and time the job was queued.
    - Do Not Start Before - The date selected if using the "Do not start before" option.
    - Command Name - The command name of the job.
    - Admin Agent - The Admin Agent computer the command will run on.
    - NAS - The NAS computer the job is run on.
    - Status - The current status of the job.
    - Cancel Requested - This column is checked if a cancel of the job has been requested
    - Message - Result codes and messages for the job
    - Timeout (sec) - The timeout in seconds.
    - Retry Count - The number of times the job has been retried.
    - Rollback Status - The status of a rollback.
    - Rollback Message - The status of a rollback.
4. To cancel a job, select the job and click the **Cancel** button or select **Cancel** from the Actions menu and click the **Apply Action** button. To refresh the jobs list, click the **Refresh** button.

Jobs can be canceled when the Status or Rollback Status is either Queued, Scheduled, Started, or In Progress.

View Properties

After the Discovery process has been completed for a Computer, you view the properties of that Computer.

To view a Computer's discovered properties:

1. Click on the table row to select a computer in the list.
2. Select **View Properties** from the Actions menu and click the **Apply Action** button. The Computer Properties window appears displaying the properties of the Computer and the user profiles associated with the Computer.
3. Click the **Export All** button to export the content of the window in Excel, text, CSV, or HTML format.

Polling Interval

By default the agent polling interval is set to 900 seconds (15 minutes). The polling interval tells the agent how frequently to contact the Migrator Pro for Active Directory Server and check for jobs. If the polling interval is set to a high number, such as 14400 seconds (4 hours), it is possible that any command sent to that computer may not execute for up to four hours. Setting a Computer’s polling interval to a high number until close to the cutover date can help minimize load on the web servers. However, to ensure adequate response time on the day of cutover, it is recommended that you decrease the polling interval in advance of the Cutover process. Note: In large scale environments, having too many agents polling the same server for jobs all at the same time may accidentally result in DDoS against that server, so additional planning of agent polling and cutover is recommended.

Computers will only obtain an updated polling interval when next contacting the Migrator Pro for Active Directory web service according to their currently configured polling interval.

To set polling interval:

1. Select one or more Computers in the list.
2. Select **Set Polling Interval**from the Actions menu and click the **Apply Action** button. The Set Polling Interval window appears.
3. Edit the Polling Interval (seconds) field and click **Apply**.

The polling interval default for all newly registered computers can be changed in SQL in the ADM_Setting table field PollIntervalSeconds.

Set Device ReACL Profile

To set Device ReACL Profile:

1. Select one or more Computers in the list.
2. Select **Set Device ReACL Profile**from the Actions menu and click the **Apply Action** button. The Set Computer Processing Profile window appears.
3. Select the Computer Processing Profile and click **Apply**.

Make Admin Agent

An agent currently running on a computer can be changed to be an Admin Agent to allow the computer to perform custom admin functions. Once changed to an Admin Agent, the computer will be removed from the Computers list and will appear in the Admin Agent list in Settings and will be able to only perform admin actions. Admin Agents cannot be changed back to a regular Computer agent.

To make a Computer an Admin Agent:

1. Select one or more Computers in the list.
2. Select **Make Admin Agent**from the Actions menu and click the **Apply Action** button. The confirmation window appears.
3. Click **Yes**. The Computer is removed from the computers list and appears in the in the Admin Agent list in Settings and can only be used to run custom admin functions.

Discovery

The Discovery process gathers properties (OS versions, network properties, and so on) from the computer to allow additional future functionality. The first discovery process begins for a computer when the computer becomes registered with the Migrator Pro for Active Directory server which will automatically occur after the Computer Agent has been installed, as long as the environment is properly configured.

To start the computer Discovery process manually:

1. Select one or more Computers in the list.
2. Select **Discovery** from the Actions menu and click the **Apply Action** button.

3. In Job Options window, click **Apply** to begin the Discovery process as soon as possible. To select when the process will begin check **Do not start before** and then enter or select a date and time. If using the **Do not start before** option, the Discovery Status will be displayed as Queued in the Computers table and the "Do Not Start Before" column in the Computer Jobs table will be populated with the selected date.
4. The Queue Summary window appears.
5. Click **OK**. The Discovery Status column is populated with the current status. Use the Actions menu **View Jobs** option to view the list of jobs for the specific Computer.

ReACL

The ReACL process updates the Computer's domain user profiles for use by the matching target user after cutover.

It is recommended to remove or disable anti-virus software immediately prior to the ReACL process and only after a recent clean scan has been completed.

At least one group must be migrated to populate the map.gg file or the ReACL process will fail. Before ReACL can occur, the target Users and Groups which have permissions set on the Computer must be migrated to the target.

To start the Computer ReACL process:

1. Select one or more Computers in the list.
2. Select **ReACL**from the Actions menu and click the **Apply Action** button.
3. In the Job Scheduling Options window, click **Apply** to begin the ReACL process as soon as possible. To select when the process will begin check **Do not start before** and then enter or select a date and time. If using the **Do not start before** option, the ReACL Status will be displayed as Queued in the Computers table and the "Do Not Start Before" column in the Computer Jobs table will be populated with the selected date.
4. The Queue Summary window appears.
5. Click **OK**. The ReACL Status column is populated with the current status. Use the Actions menu **View Jobs** option to view the list of jobs.

Two checks are performed at the start of the ReACL process. The first check is for invalid Source Profiles, which will be logged as a WARNING and those profiles will be skipped. The second check is for invalid Target Profiles, where a user may have created a profile with the target account before their machine is ReACL'd and cutover. By default, this is logged as a FATAL ERROR and will halt the ReACL process. However, it can be changed to a WARNING with the –t switch passed by editing the command in SQL.

The ReACL Agent will automatically create two files on the computer being ReACL'd, map.usr and map.gg. These files are used to find the source permissions and add the appropriate target permissions during the ReACL process. System groups, such as Domain\Domain Admins and Domain\Domain Users are included in the map.gg file for updating the group permissions during the ReACL process. If the Active Directory environment is non-English, the values in the sAMAccountName column of the BT_SystemGroup table in the SQL database will need to be changed after Directory Sync Pro for Active Directory is installed to have the appropriate non-English values.

If the Mapped Network Drive is being mapped via GPO or using an integrated credential such as the current Windows logon session, ReACL will create a warning entry in the log "…WARNING: The UserName value for drive U was empty and could not be mapped to the target user." This warning does not mean that the mapped drive cannot be accessed after Cutover.

For Windows 10 and Windows Server 2016 computers, the ReACL process is decoupled from the actions against files, folders, and the registry.

A ReACL against a Windows 10 or Windows Server 2016 computer will update all files and folders and registry entries found on the machine except for the user profile specific registry keys in HKLM, ntuser.dat, and usrclass.dat even if the user profiles option is selected in the ReACL profile.

After a ReACL has been run against a Windows 10 or Windows Server 2016 computer, the user profile components will not be prepared during a cleanup process.

The prepare and cleanup process should be completed along with the remaining ReACL activities against the user profile specific registry keys in HKLM, ntuser.dat and usrclass.dat at time of computer cutover (prior to domain join command).

Cutover

The Cutover process moves a Computer from the source domain to the new target domain.

To start the Cutover process:

1. Select one or more Computers in the list.
2. Select **Cutover**from the Actions menu and click the **Apply Action** button.
3. The Cutover Options window appears. Select a **Cutover Credential**, **Network Profile**, and **Migration Option** from the drop-down lists.
4. Check **Ignore ReACL Status** to cutover the computer regardless of the ReACL status (otherwise the cutover process will not proceed if there is an error with ReACL process).
5. Check **Do not start before** and then enter or select a date and time when the process will begin. If using the **Do not start before** option, the Cutover Status will be displayed as Queued in the Computers table and the "Do Not Start Before" column in the Computer Jobs table will be populated with the selected date. The Cutover process will begin as soon as possible if not using this option.
6. Click the **Apply** button.
7. The Queue Summary window appears.
8. Click **OK**. The Cutover Status column is populated with the current status. Use the Actions menu **View Jobs** option or double-click on a row to view the list of jobs.

Computers should not be ReACL'd once they have been cutover to the Target. This is not a best practice and is not supported as this can cause problems with the registry and user profiles.

The Cutover Options are set on the **Settings** screen.

Rollback

The Rollback process moves a Computer back to the original source domain and restores any modified network settings. The Computer must have attempted Cutover for this explicit Rollback process to work.

To start the Rollback process:

1. CSelect one or more Computers in the list.
2. Select **Rollback**from the Actions menu and click the **Apply Action** button.

3. In the Job Options window, click **Apply** to begin the Rollback process as soon as possible. To select when the process will begin check **Do not start before** and then enter or select a date and time. If using the **Do not start before** option, the "Do Not Start Before" column in the Computer Jobs table will be populated with the selected date.
4. The Queue Summary window appears.
5. Click **OK**. The selected Computers are sent back to their original domain and any modified network settings are restored. The Cutover Status column is updated with the current status.

Cleanup

The Cleanup process removes the Source SIDs after the Cutover process completes.

Cleanup should be done when the migration project is completed. Before running the Cleanup process if a trust is in place, the trust can be broken to test if any application permissions are broken.

To start the Cleanup process:

1. Select one or more Computers in the list.
2. Select **Cleanup** from the Actions menu and click the **Apply Action** button.
3. In the Job Options window, click **Apply** to begin the Cleanup process as soon as possible. To select when the process will begin check **Do not start before** and then enter or select a date and time. If using the **Do not start before** option, the Cleanup Status will be displayed as Queued in the Computers table and the "Do Not Start Before" column in the Computer Jobs table will be populated with the selected date.
4. The Queue Summary window appears.
5. Click **OK**. The Cleanup Status column is populated with the current status. Use the Actions menu **View Jobs** option to view the list of jobs.

ReACL Rollback

The ReACL Rollback process rolls back all changes made by the ReACL process. ReACL Rollback can be performed on Computers that have completed the ReACL process.

To rollback ReACL:

1. Select one or more Computers in the list.
2. Select **ReACL Rollback**from the Actions menu and click the **Apply Action** button.
3. In the Job Options window, click **Apply** to begin the ReACL Rollback process as soon as possible. To select when the process will begin check **Do not start before** and then enter or select a date and time when the process will begin. If using the **Do not start before** option, the "Do Not Start Before" column in the Computer Jobs table will be populated with the selected date.
4. View rollback results by viewing the Computer's job view.

Cache Credentials

The Cache Credentials process assigns a Cache Credentials job to workstation(s). See the Credential Cache and Offline Domain Join topic for more information.

Offline Domain Join

The Offline Domain Join process is similar to the Cutover process for machines that are directly connected to the network. See the Credential Cache and Offline Domain Join topic for more information.

WARNING: Do not perform the Cutover process on Offline Domain Join workstations. The Offline Domain Join process takes the place of Cutover for workstations connecting via VPN.

Admin Agent Menu Actions

If any Admin Agent menu actions have been created for Computers, they will appear in the Actions menu:

1. Select one or more Computers in the list.
2. Select an Admin Agent action from the Actions menu and click the **Apply Action** button.
3. In the Job Options window, check **Do not start before** and enter a date if you do not want the job to begin immediately. Select the **Admin Agent** and the **Agent Admin Credentials** to use from the drop-down lists. The Cutover options will also appear if the selected Admin Agent action includes the Cutover action.
4. Click **Apply**. The Queue Summary appears.
5. Click **OK**.

ComputerS List Columns

The following columns appear on the Computer Actions screen by default:

- Migration Wave - The Migration Wave name. Use the Actions menu **Set Migration Wave** option to change.
- sAMAccountName - The sAMAccountName attribute of the source computer.
- Distinguished Name - The distinguished name attribute of the source computer.
- Registered - This column is checked if the computer is registered with the Migrator Pro for Active Directory server.
- Agent Version - The version of the Migrator Pro for Active Directory Agent installed on the computer.
- Operating System Version - The version of the Computer's operating system.
- Agent Last Contact - This column displays the time and date of the last contact between the agent and the Migrator Pro for Active Directory Server.
- Description - The description attribute of the source computer.
- Blacklisted - This column is checked if the Computer is currently on the exclusion list. Use the Actions menu **Add to Exclusion list** option or **Remove from Exclusion list** option to change.
- Polling Interval - The time interval (in seconds) between polls. This is set to 900 seconds (15 minutes) by default. Use the Actions menu **Set Polling Interval** option to change. The Migrator Pro for Active Directory Agent will pick up the new polling interval value the next time it contacts the Web Service.
- Discovery Status - The status of the discovery process. Use the Actions menu **Discovery** option to start the Discovery process.

- ReACL Status - The status of the ReACL process. Use the Actions menu **ReACL** option to start the ReACL process.
- ReACL Profile - The ReACL Profile set for the Computer. Use the Actions menu **Set ReACL Profile** option to change. Device ReACL Profiles are defined in Settings.
- Cache Credential Status - The status of the Cache Credentials process for use with Offline Domain Join. Use the Actions menu **Cache Credentials** option to start the Cache Credential process.
- Offline Domain Join Status - The status of the Offline Domain Join process. Use the Actions menu **Offline Domain Join** option to start the Offline Domain Join process.
- Cutover Status - The status of the Cutover process. Use the Actions menu **Cutover** option to start the Cutover process.
- Cleanup Status - The status of the Cleanup process. Use the Actions menu **Cleanup** option to start the Cleanup process.
- Last Job Message - The last job status.

The following additional fields can be displayed by customizing the columns:

- ID - SQL record number
- Migration Wave ID - The Migration Wave ID.

Upload Logs

Log files from the Migrator Pro for Active Directory Agent can be uploaded to the Migrator Pro for Active Directory Web Server using Microsoft BITS. To enable this functionality, the installer enables BITS Server Extensions for IIS and create a virtual directory called **ComputerLogs** where all uploaded files will be stored.

To upload Log files from the Migrator Pro for Active Directory Agent:

1. Select one or more Computers in the list.
2. Select **Upload Logs** from the Actions menu and click the **Apply Action** button.
3. In the Job Options window, click **Apply** to begin the Upload Logs process as soon as possible. To select when the process will begin check **Do not start before** and then enter or select a date and time. If using the **Do not start before** option, the Do Not Start Before column in the Computer Jobs table will be populated with the selected date.

- The logs will be stored at the following location: C:\Program Files\Binary Tree\ADPro\DeviceLogs
- The computer logs will be zipped, and the file names will be in the following format with a unique file name: SMART-WIN7X86-1_201573111235.zip

Migrating File Shares

The File Share Actions screen allows you to ReACL File Share computers via a network share.

Add a File Share

To add a File Share computer:

1. Select **Add File Share** from the Actions menu and click the **Apply Action** button. The File Share window appears.
2. Enter values in the following fields:
    - UNC Path - the UNC path that will be the starting location for ReACL on the File Share computer
    - Device - The name of the Computer used to access the File Share computer. This computer must be local (same network, region, and so on) to the File Share device. This is a sAMAccountName, not an FQDN.
    - Username - The username to access the File Share device. UserPrincipalName values (user@domain.dom) or domain\username format are supported.
    - Password - the Password to credential access the File Share computer
3. Click **OK**. The File Share computer is added to the list.

Edit a File Share

To edit a File Share computer:

1. Select a File Share computer in the list.
2. Click the **Edit** button or select **Edit** from the Actions menu and click the **Apply Action** button. The Network Access Storage window appears.
3. Edit the values.
4. Click **OK**. The File Share computer is updated in the list.

Delete a File Share

To delete a File Share computer:

1. Select one or more File Share devices in the list.
2. Click the **Delete** button or select **Delete** from the Actions menu and click the **Apply Action** button. The File Share computer(s) are removed from the list.

Set File Share Processing Profile

To set File Share Processing Profile:

1. Select one or more File Share computers in the list.
2. Select **Set File Share Processing Profile**from the Actions menu and click the **Apply Action** button. The File Share Processing Profile window appears.
3. Select the File Share Processing Profile and click **Apply**.

ReACL

The ReACL process updates the File Share's domain user profiles for use by the matching target user after cutover.

To start the File Share ReACL process:

1. Select one or more File Share computers in the list.
2. Select **ReACL**from the Actions menu and click the **Apply Action** button.
3. In the Job Options window, click **Apply** to begin the ReACL process as soon as possible. To select when the process will begin check **Do not start before** and then enter or select a date and time. If using the **Do not start before** option, the ReACL Status will be displayed as Queued in the File Share table and the "Do Not Start Before" column in the File Share Computer Jobs table will be populated with the selected date.
4. The Queue Summary window appears.
5. Click **OK**. Use the Actions menu **View Jobs** option to view the list of jobs.

Cleanup

To start the Cleanup process:

1. Select one or more File Share devices in the list.
2. Select **Cleanup**from the Actions menu and click the **Apply Action** button.
3. In the Job Options window, click **Apply** to begin the Cleanup process as soon as possible. To select when the process will begin check **Do not start before** and then enter or select a date and time. If using the **Do not start before** option, the Cleanup Status will be displayed as Queued in the File Share table and the "Do Not Start Before" column in the File Share Computer Jobs table will be populated with the selected date.
4. The Queue Summary window appears.
5. Click **OK**. The Cleanup Status column is populated with the current status. Use the Actions menu **View Jobs** option to view the list of jobs.

View Jobs

To view File Share computer jobs:

1. Select one or more File Share computers in the list.
2. Select **View Jobs**from the Actions menu and click the **Apply Action** button. The Computer Jobs window appears.

3. The Computer Jobs table includes the following columns:
    - Job ID - The ID of the job.
    - Queued Timestamp - The date and time the job was queued.
    - Do Not Start Before - The date selected if using the Do Not Start Before option.
    - Command Name - The command name of the job.
    - Status - The current status of the job.
    - Cancel Requested - This column is checked if cancellation of the job has been requested.
    - Message - Result codes and messages for the job.
    - Timeout (sec) - The timeout in seconds.
    - Retry Count - The number of times the job has been retried.
    - Rollback Status - The status of a rollback process.
    - Rollback Message - The status of a rollback process.
4. To cancel a job, select the job and click the **Cancel** button or select **Cancel** from the Actions menu and click the **Apply Action** button. To refresh the jobs list, click the **Refresh View** button.

ReACL Rollback

The ReACL Rollback process rolls back all changes made by the ReACL process. ReACL Rollback can be performed on File Share computers that have completed the ReACL process.

To rollback ReACL:

1. Select one or more File Share computers in the list.
2. Select **ReACL Rollback**from the Actions menu and click the **Apply Action** button.
3. In Job Options window, click **Apply** to begin the ReACL Rollback process as soon as possible. Check **Do not start before** and then enter or select a date and time when the process will begin. If using the **Do not start before** option, the Do Not Start Before column in the File Share Computer Jobs table will be populated with the selected date.
4. View rollback results by viewing the File Share computer's job view.

File Share Columns

The following columns appear on the File Share Actions screen by default:

- ID - The migration ID.
- Device Name - The name of the device used to access the File Share computer. This device must be local to the File Share computer.
- File Share Path - The UNC path to the network share used to access the File Share computer.
- Username - The username to access the File Share computer.
- ReACL Status - The status of the ReACL process. Use the Actions menu **ReACL** option to start the ReACL process.

- Profile - The ReACL Profile set for the File Share computer. Use the Actions menu **Set File Share Processing Profile** option to change. Profiles are defined in Settings.
- Cleanup Status - The status of the Cleanup process. Use the Actions menu **Cleanup** option to start the Cleanup process.

Migration Options and Profile Settings

Migration Options

To add migration options:

1. On the Migration Options page, click the **Add** button. The Migration Options window appears.
2. Enter values in the following fields:
    - Profile Name - The name to identify the options (for example, "10 Second Reboot Delay").
    - Domain Join Delay - The delay before joining the domain.
    - Reboot Delay - The delay before rebooting.

      If set to any value other than zero (0), the user will receive a pop-up notification informing them that the workstation will be rebooted when the cutover is performed. If set to zero, no notification will appear.

    - Empty Recycle Bin? - How to handle the Recycle Bin during cutover, either **Empty** or **Don't Empty**

      Users may get an error message that their Recycle Bin has been corrupted after migration if the Recycle Bin is not empty. See Troubleshooting for more information about this issue.

    - Specify Target OU - The target OU where the Computers will be created. If this field is left blank, the computers will default to the Computers container.
3. Join to Existing Computer Account - Select **Yes** to join the Computer to the existing target Computer during cutover.
4. Click **Save Profile**. The new migration options profile is added to the list.

Network Profiles

To add network profiles:

1. On the Network Profiles page, click the **Add** button. The Network Profiles window appears.
2. Enter values in the following fields:
    - Profile Name - The name to identify this Network Profile
    - Set DNS Servers For the Computer? - Options include: **Don't Change This Setting**, **Use DHCP For DNS Server**, or **Manually Assign DNS Servers**.

      If you manually assign DNS settings, be sure that the DNS server(s) that you include here can resolve the Migrator Pro for Active Directory Agent SRV record.
    - Primary DNS Server - The preferred DNS server.
    - Secondary DNS Server - The alternate DNS server.
    - DNS Suffix For the Network Adapter - The primary DNS suffix that will be set on the network adapter.
    - Append DNS Suffixes to the Network Adapter - Options include **Don't Change This Setting**, **Preserve Current DNS Suffixes From the Network Adapter**, or **Set the Following DNS Suffixes**.
    - DNS Suffixes - Enabled if **Set the Following DNS Suffixes** is selected from the "Append DNS Suffixes to the Network Adapter" option. Enter each suffix and then press **Enter**.
    - Register the Network Adapter's Addresses in DNS - Options include **Don't Change This Setting**, **No**, or **Yes**.
    - if **Yes** is selected to the "Register the Network Adapter's Addresses in DNS" option, select **Don't Change This Setting**, **Include The Manual DNS Suffix**, or **Don't Include the Manual Suffix**.
    - Primary WINS Server - The preferred WINS server.
    - Secondary Wins Server - The alternate WINS server.
3. Click **Save Profile**. The new network profile is added to the list.

Device ReACL Profiles

The default Device ReACL profile is used if a different profile is not defined and set on the computers. The default Device ReACL profile can be edited.

To add Device ReACL profiles:

1. On the Device ReACL Profiles page, click the **Add** button. The Device ReACL Profile window appears.
2. In the **Profile Name** field, enter a name to identify this Device ReACL Profile.
3. Select a Logging Level, either **Informational** (default) or **Debugging**.

4. Select the components to process.

   Local Files/Folders: Selected by default.

   Registry Permissions: Selected by default.

   User Profiles: Selected by default.

   Local Group Memberships: Selected by default.

   Local Printer Permissions: Selected by default.

   Network Share Permissions: Selected by default.

   Printer Share Permissions: Selected by default.

   Roaming Profiles: Unselected by default.

   If you select **Roaming Profiles**, users must be logged out of their roaming profiles during the ReACL process.

   Windows Services: Selected by default. The **Windows Services** option will ensure that any source domain accounts that were given permission to a service will include the corresponding matched target domain account after a ReACL process.

   Windows Service Accounts: Unselected by default. We recommend that the **Windows Service Accounts** box is left UNCHECKED. A change in the ACL of the services accounts of the target may have an impact on the applications currently running. Although the ReACL process can usually be rolled back in case of issues, there could be a temporary disruption in service until that can be resolved. Selecting the **Windows Service Accounts** box will switch the domain account that Windows services are running under to the corresponding matched target domain account after a completed ReACL process.

   User Rights Assignments: Selected by default.

   System ACLs: Selected by default. The **System ACLs** option allows for the proper translation of accounts within the security audit logs.

   Preserve the "Archive" Bit: Unselected by default. If the **Preserve the "Archive" Bit** box is left unchecked, the archive bit will be reset. If checked, the archive bit will not be reset.

5. Click **Next**.

6. Normally all files and folders are included in the ReACL process. If it is preferred to provide a specific list, enter the list in the **Only Process the Following and Their Subfolders** box. Separate each entry by pressing **Enter**. You may use just a file path using backslashes, or provide an exact drive letter. If a drive letter is provided, the ReACL is limited to that exact path.

   Note that if you choose to list folders here, these are the ONLY folders that will be included in the ReACL process. (The exception is if you check the User Profiles box: those Profiles will always be included automatically in addition to your list.)

7. In the **Exclude These Paths From Processing** box, enter folder paths that will not be included in the ReACL process. Wild card characters (* and ?) can be used when specifying exclusion list folders. Separate the paths by pressing **Enter**. By default, the following folders are exclusion listed:

    - \Windows
    - \WINNT
    - \I386
    - \Windows\I386
    - \Program Files
    - \PROGRAM FILES (x86)
    - \MSOCACHE
    - \System Volume Information
    - \Recycler
    - \$RECYCLE.BIN
    - \CONFIG.MSI
    - \RECOVERY
    - \OEM
    - \Quarantine
    - \BOOT
    - \ProgramData\Microsoft\Windows Defender

8. In the **Exclude These Registry Keys From Processing** box, enter registry keys that will not be included in the ReACL process. A leading '\' is not necessary. Separate the paths by pressing **Enter**. The following wild card characters are permitted when specifying registry keys:

    - * matches zero or more characters in a key name, but not the '\' path delimiter.
    - ? matches any single character.
    - ** matches zero or more parent keys.

    Examples:

    - HKEY_LOCAL_MACHINE\SOFTWARE\XYZ – a single key
    - HKEY_LOCAL_MACHINE\SOFTWARE\XY* – all keys starting with "XY" in HKEY_LOCAL_MACHINE\SOFTWARE
    - HKEY_LOCAL_MACHINE\SOFTWARE\?YZ – all 3-character keys ending with "YZ" in HKEY_LOCAL_MACHINE\SOFTWARE
    - HKEY_LOCAL_MACHINE**\XYZ – all keys named "XYZ" anywhere under HKEY_LOCAL_MACHINE
    - **\XYZ – all keys named "XYZ" in any registry hive

9. Click **Next**.

10. The **Reparse Point Processing Rules page** appears. Reparse Points like Symbolic Links, Mount Points, and OneDrive folders will be processed by ReACL. Additional Reparse Tags can be added to the rules list in the Advanced view to change how ReACL will process those items. Click the **Show Advanced** button to edit the rules list.

    When Show Advanced is clicked the rules list is displayed. Additional Reparse Points can added to the list in the "ReparseTag:Action" format. Skip, Recurse, Update, and Full are the available actions. Separate rules by pressing **Enter**.

11. Click **Next**.

12. Select an option from the **Elevated Permissions Failure Action** drop-down list to choose the action that should be taken if any part of the ReACL process encounters errors.

    In order to successfully adjust permissions, Migrator Pro for Active Directory must create a process with a security token that has been assigned additional permissions. The token is said to have elevated rights/permissions. If this process fails, it is likely that the ReACL will be largely unsuccessful in updating the operating system for use by target user accounts.

    - The default is **Terminate processing with fatal error**, meaning the ReACL process for that computer is stopped as soon as an error occurs. This is a time-saving option. The ReACL process is reported as **Failed** in the Computers View. A computer cannot be Cutover if the ReACL process reports as Failed. This is the recommended setting.
    - If you choose **Log error entry**, the entire process will attempt to complete when an Elevate Failure error is encountered, but the process will still be reported as **Failed**. This selection may take significantly more time than Terminate processing with fatal error" because the entire process will attempt to finish before reporting as **Failed**.
    - If you choose **Log warning entry**, a warning entry will be logged, however the process will be reported as **Successful**. This choice allows experienced migration architects to analyze the logs and choose to Cutover anyway based on their analysis of the results.
    - If you choose **Log informational entry**, an info entry will be logged, however the process will be reported as **Successful**. This choice allows experienced migration architects to analyze the logs and choose to Cutover anyway based on their analysis of the results. We suggest choosing Warning over Info as that will make the entries easier to locate in the log.

13. Select an option from the **Profile Failure Action** drop-down list to choose the action that should be taken when an invalid or duplicate profile exists in the target.

    - The default is **Terminate processing with fatal error**, meaning the ReACL process for that computer is stopped as soon as an error occurs. This is a time-saving option. The ReACL process is reported as **Failed** in the Computers View. A computer cannot be Cutover if the ReACL process reports as Failed. This is the recommended setting.
    - If you choose **Log error entry**, the entire process will attempt to complete when a Profile Failure error is encountered, but the process will still be reported as **Failed**. This selection may take significantly more time than "Terminate processing with fatal error" because the entire process will attempt to finish before reporting as **Failed**.
    - If you choose **Log warning entry**, a warning entry will be logged, however the process will be reported as **Successful**. This choice allows experienced migration architects to analyze the logs and choose to Cutover anyway based on their analysis of the results.
    - If you choose **Log informational entry**, an info entry will be logged, however the process will be reported as **Successful**. This choice allows experienced migration architects to analyze the logs and choose to Cutover anyway based on their analysis of the results. We suggest choosing Warning over Info as that will make the entries easier to locate in the log.

14. Select an option from the **Preserve Rollback Metadata in ACLs** drop-down list.

    Migrator Pro for Active Directory inserts a "breadcrumb" during the ReACL process to allow seamless rollback of the ReACL process if needed. You can control the insertion of these breadcrumbs (which are removed during the Cleanup process) if desired, here.

    - The default is **Always** and does not affect performance. We recommend this setting. This is the only setting where the changes performed by the ReACL process can be rolled back, or undone, in all scenarios.
    - If you choose **Only If Ambiguous**, metadata will only be included when the rollback settings would be ambiguous. Only If Ambiguous results in the addition of fewer breadcrumbs, preserving usage for times when it may be impossible to determine the original file or folder permissions. For example, when users have accounts in multiple domains that will be consolidated into a single domain.

      Note that Only If Ambiguous guarantees a ReACL can be rolled back to the original state only when the file system permissions remained unchanged. Modification of ACLs on the file system could create a state where a rollback cannot complete with 100% success. To ensure the ability for a ReACL Rollback in all scenarios, Always should be selected.
    - If you are an experienced migration architect, you may choose **Never** to never include metadata.

      If **Never** is selected, a complete rollback may not be possible.

15. Select **Yes** under **Run Processing in Simulation Mode** to simulate the results of the ReACL process without actually making any changes to the ACL. Visit the logs/reports to determine any potential issues and correct them before running an actual ReACL process. You might use this setting to create a Device ReACL Profile specifically for testing purposes.
16. Click **Save Profile**. The new Device ReACL Profile is added to the list.

NAS ReACL Profiles

The default NAS ReACL profile is used if a different profile is not defined and set on the NAS computers. The default NAS ReACL profile can be edited.

To add NAS ReACL profiles:

1. On the NAS ReACL Profiles page, click the **Add** button. The NAS ReACL Profile window appears.
2. In the **Profile Name** field, enter a name to identify this NAS ReACL Profile.
3. Select a Logging Level, either **Informational** (default) or **Debugging**.
4. Enter the network errors that will trigger a retry in the **Retry If the Following Error Codes Are Encountered** box. By default, errors 53 and 64 will trigger a retry.
5. Enter the number of retries to attempt in the **Retry Count** field. The default retry count is 10 times.
6. Enter the number of seconds between network error retries in the **Retry Interval** field. The default interval is 1 second.
7. Click **Next**.
8. Select the components to process.

   If the **Preserve the "Archive" Bit** box is left unchecked, the archive bit will be reset. If checked, the archive bit will not be reset.
9. In the **Exclude These Paths From Processing** box, enter folder paths that will not be included in the ReACL process. Wild card characters (* and ?) can be used when specifying exclusion list folders. Separate the paths by pressing **Enter**. By default, the following folders are blacklisted:

   - \Windows
   - \WINNT
   - \I386
   - \Windows\I386
   - \Program Files
   - \PROGRAM FILES (x86)
   - \MSOCACHE
   - \System Volume Information
   - \Recycler
   - \$RECYCLE.BIN
   - \CONFIG.MSI
   - \RECOVERY
   - \OEM
   - \Quarantine
   - \BOOT
   - \ProgramData\Microsoft\Windows Defender

10. In the **Exclude These Registry Keys From Processing** box, enter registry keys that will not be included in the ReACL process. A leading '\' is not necessary. Separate the paths by pressing **Enter**. The following wild card characters are permitted when specifying registry keys:

    - * matches zero or more characters in a key name, but not the '\' path delimiter.
    - ? matches any single character.
    - ** matches zero or more parent keys.

    Examples:

    - HKEY_LOCAL_MACHINE\SOFTWARE\XYZ – a single key
    - HKEY_LOCAL_MACHINE\SOFTWARE\XY* – all keys starting with "XY" in HKEY_LOCAL_MACHINE\SOFTWARE
    - HKEY_LOCAL_MACHINE\SOFTWARE\?YZ – all 3-character keys ending with "YZ" in HKEY_LOCAL_MACHINE\SOFTWARE
    - HKEY_LOCAL_MACHINE**\XYZ – all keys named "XYZ" anywhere under HKEY_LOCAL_MACHINE
    - **\XYZ – all keys named "XYZ" in any registry hive

11. Click **Next**.
12. The **Reparse Point Processing Rules** page appears. Reparse Points like Symbolic Links, Mount Points, and OneDrive folders will be processed by ReACL. Additional Reparse Tags can be added to the rules list in the Advanced view to change how ReACL will process those items. Click the **Show Advanced** button to edit the rules list.

    When Show Advanced is clicked the rules list is displayed. Additional Reparse Points can added to the list in the "ReparseTag:Action" format. Skip, Recurse, Update, and Full are the available actions. Separate rules by pressing **Enter**.
13. Click **Next**.

14. Select an option from the **Elevate Permissions Failure Action** drop-down list to choose the action that should be taken if any part of the ReACL process encounters errors.

    In order to successfully adjust permissions, Migrator Pro for Active Directory must create a process with a security token that has been assigned additional permissions. The token is said to have elevated rights/permissions. If this process fails, it is likely that the ReACL will be largely unsuccessful in updating the operating system for use by target user accounts.

    - The default is **Terminate processing with fatal error**, meaning the ReACL process for that computer is stopped as soon as an error occurs. This is a time-saving option. The ReACL process is reported as **Failed** in the Computers View. A computer cannot be Cutover if the ReACL process reports as Failed. This is the recommended setting.
    - If you choose **Log error entry**, the entire process will attempt to complete when an Elevate Failure error is encountered, but the process will still be reported as **Failed**. This selection may take significantly more time than "Terminate processing with fatal error" because the entire process will attempt to finish before reporting as **Failed**.
    - If you choose **Log warning entry**, a warning entry will be logged, however the process will be reported as **Successful**. This choice allows experienced migration architects to analyze the logs and choose to Cutover anyway based on their analysis of the results.
    - If you choose **Log informational entry**, an info entry will be logged, however the process will be reported as **Successful**. This choice allows experienced migration architects to analyze the logs and choose to Cutover anyway based on their analysis of the results. We suggest choosing Warning over Info as that will make the entries easier to locate in the log.

15. Select an option from the **Preserve Rollback Metadata in ACLs** drop-down list.

    Migrator Pro for Active Directory inserts a "breadcrumb" during the ReACL process to allow seamless rollback of the ReACL process if needed. You can control the insertion of these breadcrumbs (which are removed during the Cleanup process) if desired, here.

    - The default is **Always** and does not affect performance. We recommend this setting. This is the only setting where the changes performed by the ReACL process can be rolled back, or undone, in all scenarios.
    - If you choose **Only If Ambiguous**, metadata will only be included when the rollback settings would be ambiguous. Only If Ambiguous results in the addition of fewer breadcrumbs, preserving usage for times when it may be impossible to determine the original file or folder permissions. For example, when users have accounts in multiple domains that will be consolidated into a single domain.

      Note that **Only If Ambiguous** guarantees a ReACL can be rolled back to the original state only when the file system permissions remained unchanged. Modification of ACLs on the file system could create a state where a rollback cannot complete with 100% success. To ensure the ability for a ReACL Rollback in all scenarios, **Always** should be selected.
    - If you are an experienced migration architect, you may choose **Never** to never include metadata.

      If **Never** is selected, a complete rollback may not be possible.

16. Select **Yes** under **Run Processing in Simulation Mode)** to simulate the results of the ReACL process without actually making any changes to the ACL. Visit the logs/reports to determine any potential issues and correct them before running an actual ReACL process. You might use this setting to create a Device ReACL Profile specifically for testing purposes.

17. Click **Save Profile**. The new NAS ReACL Profile is added to the list.

Credential Settings

Credential Cache and Offline Domain Join

Description

Microsoft's Offline Domain Join (ODJ) process allows a workstation to join a domain without contacting a Domain Controller. Migrator Pro for Active Directory builds upon this functionality to allow machines to be cutover to the new domain without contacting a target domain controller.

This means that Migrator Pro for Active Directory can allow the workstation to join the new domain without having the user connect to the corporate VPN and manually join their workstation to the new domain.

Normally, VPN users can't login right after joining a new domain and rebooting because Windows must be able to contact the target domain to authenticate against a domain controller for the very first login. Typically, this would mean that a remote user would need to log in to their machine first and then establish a VPN connection.

Migrator Pro for Active Directory resolves this by taking advantage of Windows ability to cache credentials. If users have logged in to a domain previously, Windows can still log them in even if they can no longer reach a domain controller by using their cached credentials. Therefore, Migrator Pro for Active Directory has functionality to have a user pre-login to the new domain before the computer is cutover so the target credentials can be cached and used for the first login without the need to contact a domain controller first.

The computers that the ODJ process is being run on must have network connectivity to BOTH the source and target environments at the same time in order to have the Cached Credentials function work properly.

Creating ODJ files for each workstation

The first step will be to use Microsoft's DJOIN utility to create a provisioning file. Only the provisioning part of the DJOIN process is needed. Complete information on DJOIN can be found here:

https://technet.microsoft.com/en-us/library/offline-domain-join-djoin-step-by-step(v=ws.10).aspx

The Provision, Domain, Machine, and Savefile parameters are required at a minimum. There is the option to control where the target machine will be created using the MachineOU parameter as in the sample shown here.

DJOIN.EXE /Provision /Domain BTADLAB.com /Machine Sales220 /Savefile "C:\Program Files\Binary Tree\ADPro\Downloads\ODJ\Sales220.txt" /MACHINEOU OU=SalesComputers,OU=Sales,DC=BTADLAB,DC=COM

The file must be saved in the ODJ folder in the downloads path that was chosen during the installation.

By default, this is C:\Program Files\Binary Tree\ADPro\Downloads\ODJ.

This can be completed for all relevant workstations early in the migration process.

WARNING: Be sure to name each text file with the exact matching machine name.

Configuring the Credential Cache Profile

The next step is to configure the existing Default Credential Cache profile with the IP address of a Target domain controller, or to create a new profile.

Click on **Add** to create a new profile, or **Edit** to modify an existing profile. If you choose to use the Default profile, you must edit it to include a Target DC IP address.

- The **Target Domain Controller Ping Interval** setting determines how long the script will sleep before pinging the DC again.
- The **Timeout Before Job Failure** setting determines the Credential Cache app timeout value that will be used for the job once downloaded to the agent managed machine.
- The **Timeout For User Credential** setting determines how long the user is presented with a dialog box to enter their target domain credentials.

Cache Credential Jobs

Now that a profile has been configured with a target DC IP address, we can assign a Cache Credentials job to the workstation(s).

In the Computers list, select one or more Computers. Select **Cache Credentials** from the Actions menu and click the **Apply Action** button. The Credential Cache Options box appears.

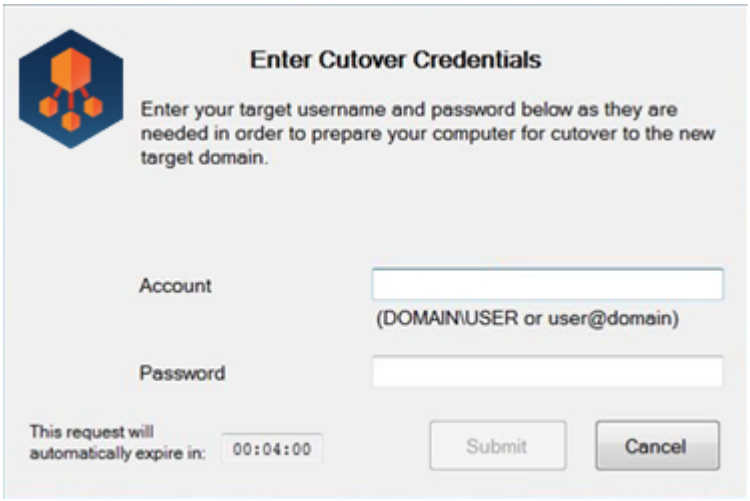
Select a Credential Cache Profile.

A date and time for the Cache Credentials job can be chosen to run the job at a later time. This date/time combination represents the earliest time that this job could run. The actual time thereafter depends on the Polling Interval of the workstation.

If a date/time is not chosen, this job will run on the workstation the next time the agent checks for jobs.

The Computers list will reflect a status of "Queued". When the job is collected by the agent the status will change to "In Progress", and then finally it will transition to a status of "Completed" or "Failed".

On the workstation side, when the Cache Credentials Job is received, the user will be prompted to enter their target credentials. Below is an example of what the user will see when the Cache Credential job runs:



ReACL

The next recommended step is the ReACL process. The ReACL process can be run repeatedly as needed before ODJ, but it is suggested to be run at least once right after the Cache Credentials process is run.

Offline Domain Join Job

The final step is the actual Offline Domain Join. This is similar to the Cutover process for machines that are directly connected to the network.

WARNING: Do not perform the Cutover process on Offline Domain Join workstations. The Offline Domain Join process takes the place of Cutover for workstations connecting via VPN.

In the Computers list, select one or more Computers. Select **Offline Domain Join** from the Actions menu and click the **Apply** button.

The Job Options box appears. A specific date/time combination can be chosen for when to run the job, or just click **Apply Action** to have this job received by the workstations during their next check for jobs.

WARNING: The Offline Domain Join (Job Scheduling Options dialog box) start date and time must be set AFTER the Cache Credentials job (Cache Credential Options dialog box) start date and time.

The Offline Domain Join process does not support rollback.

Credentials

Use the Credentials page to add credentials used for either a computer Cutover or for an Admin Agent.

The specified cutover credentials must be able to join and disjoin a computer from the specified domain and well as disable a computer in the specified domain. A trust between the source and target domain is not required.

To add Cutover credentials:

1. Click the **Add** button. The Add Your Credentials window appears.
2. Enter a **Credential Name** to identify the credentials (for example, "DomA to DomB Admins").
3. Select **Cutover** from the **Credentials Type** drop-down list. The Source and Target fields appear.
4. Enter values in the following fields under Source Domain Credentials:
    - FQDN of Domain - The domain FQDN of the source in source.domain.dom format.
    - Username - The username to access the source domain in domain\username or UPN (username@domain.dom) format.
    - Password - The password credential to access the source domain.
5. Enter values in the following fields under Target Domain Credentials:
    - FQDN of Domain - The domain FQDN of the target in target.domain.dom format.
    - Username - The username to access the target domain in domain\username or UPN (username@domain.dom) format.
    - Password - The password credential to access the target domain.

6. Click **Save Profile**. The cutover credentials are added to the list.

To add Admin Agent credentials:

1. Click the **Add** button. The Add Your Credentials window appears.
2. Enter a **Credential Name** to identify the credentials (for example, "Move User Credentials").
3. Select **Admin Agent** from the **Credentials Type** drop-down list. The Credentials fields appear.
4. Enter values in the following fields Credentials:
    - FQDN of Domain - The domain FQDN in domain.dom format.
    - Username - The username to access the domain in domain\username or UPN (username@domain.dom) format.
    - Password - The password credential to access the domain
5. Click **Save Profile**. The Admin Agent credentials are added to the list.

Agents and Customizations

Admin Agents

The Admin Agents screen allows you to designate one or more machines as remote workstations that can perform customized tasks, such as running PowerShell scripts that can be triggered against Computers, Users, Resource Mailboxes, Contacts, or Groups as needed. For example, an organization may want to designate a machine to move users from a temporary OU in the target, to what is later designated as their final destination.

Typically, the Admin Agent will be run on a computer outside the scope of the Synchronization profile being used. You also have the option to convert an existing machine already running the Agent into an Admin Agent computer on the Computer Actions screen. The Admin Agent cannot perform both roles, so Admin Agent computers are typically chosen from the target forest as they do not need to be cutover.

If you are choosing a machine from the target as an Admin Agent computer, you should create it on the Admin Agents tab under Settings before installing the Agent software. Existing computers that were converted to an Admin Agent computer will appear there automatically.

Click on **Add** to define a new Admin Agent computer, or **Edit** to modify an existing Admin Agent computer.

- The **sAMAccountName** identifies the machine name the Admin Agent will run on.
- The **Domain** identifies where the machine is located.
- The **Description** is an optional field used to describe the machine.
- The **Polling Interval, Every** setting determines the length of time between polls. The Polling Interval is set to 1 minute by default.

After adding a machine to the Admin Agents screen, you can install the Agent software on the Admin Agent machine. You should see the computer register here after refreshing the screen. If you can ping the computer from the Migrator Pro for Active Directory console, but it never registers, check that the Agent software has been successfully installed using the Event Viewer on the Admin Agent machine.

After the Admin Agent computer is added and registered, credentials to be used for the Admin Agent computer can be added to the Credentials screen and custom tasks (marked as "Run On Admin Agent") can be created on the Actions screen. These new tasks can then be added to actions available for Users, Resource Mailboxes, Contacts, Groups, or Computers.

Polling Interval

The Admin Agent polling interval is set to 1 minute by default. The polling interval tells computers how frequently to contact the Migrator Pro for Active Directory Server and check for jobs. If the polling interval is set to a high number, such as 240 minutes (4 hours), it is possible that any command sent to the computer may not execute for up to four hours.

Computers will only obtain an updated polling interval when next contacting the Migrator Pro for Active Directory Server according to their currently set polling interval.

View Jobs

To view Admin Agent jobs:

1. Select one or more Admin Agent computers in the list.
2. Select **View Jobs** from the Actions menu and click the **Run Action** button. The Admin Agent Jobs window appears.
3. The Admin Agent Jobs table includes the following columns:
    - Job ID - The ID of the job.
    - Queued Timestamp - The date and time the job was queued.
    - Do Not Start Before - The date selected if using the "Do Not Start Before" option.
    - Command Name - The command name of the job.
    - Admin Agent- The Admin Agent the job is run on.
    - NAS - The NAS computer the job is run on.
    - Status - The current status of the job.
    - Cancel Requested - This column is checked if a cancellation of the job has been requested.
    - Message - Result codes and messages for the job.
    - Timeout (sec) - The timeout in seconds.
    - Retry Count - The number of times the job has been retried.
    - Rollback Status - The status of a rollback process.
    - Rollback Message - The status of a rollback process.
4. To cancel a job, select the job and click the **Cancel** button. To refresh the jobs list, click the **Refresh View** button.

View Properties

After the Discovery process has been completed for an Admin Agent computer, you can view the discovered properties of that Computer.

To view an Admin Agent computer's properties:

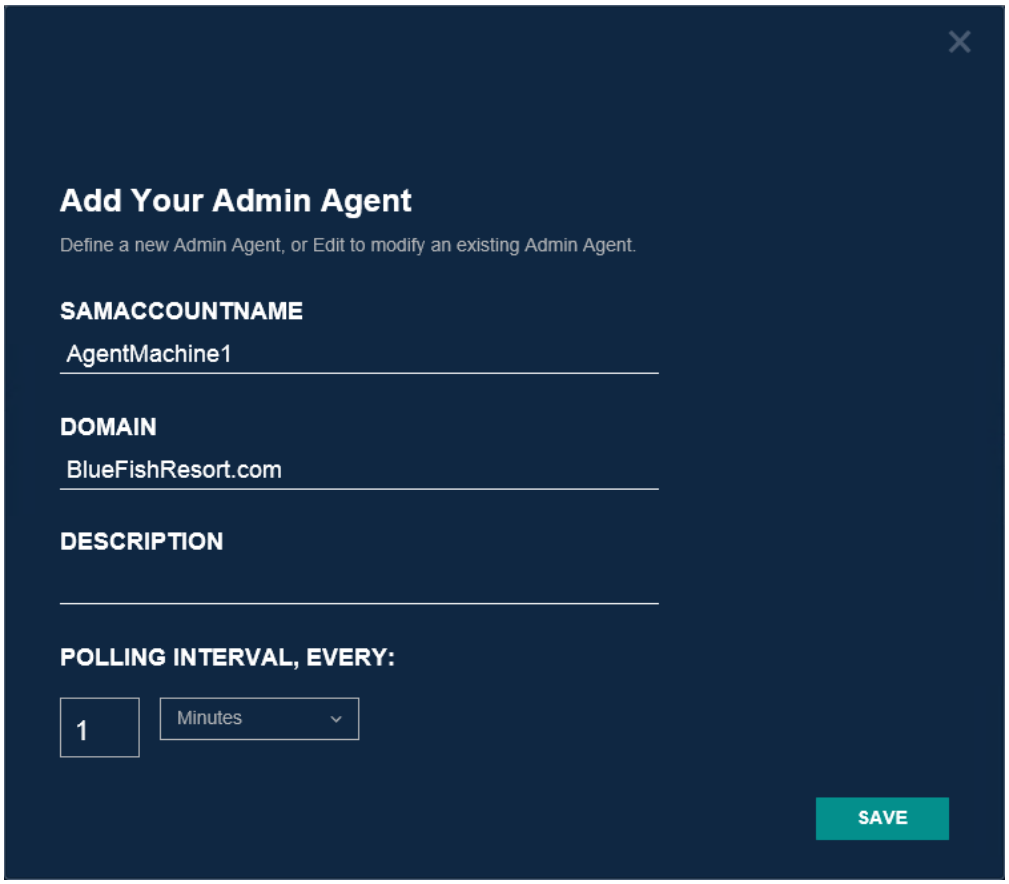
1. Select a Computer in the list. Select **View Properties** in the Actions menu and click the **Run Action** button. The Computer Properties window appears displaying the properties of the Computer and the user profiles associated with the Computer.
2. Click the **Export All** button to export the content of the window in Excel, text, CSV, or HTML format.

Admin Agent Example

Scenario: The administrator wants to designate a machine to move users from a temporary OU in the target, to what is later designated as their final destination. Any specific PowerShell modules (like Active Directory) or any other script dependencies should be installed on the desired Admin Agent machine prior to these activities to ensure the necessary scripts can execute successfully.

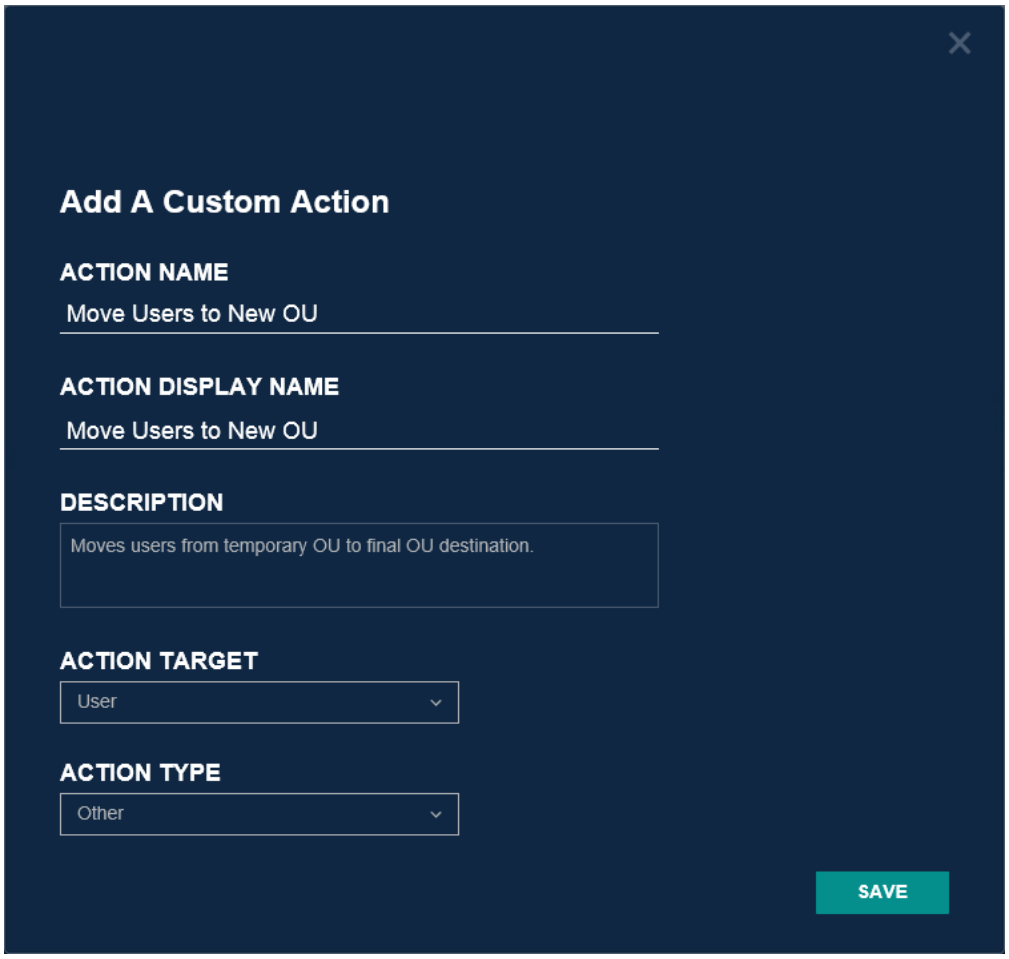
Steps:

1. Add the machine to the Admin Agents list on the Agents screen.

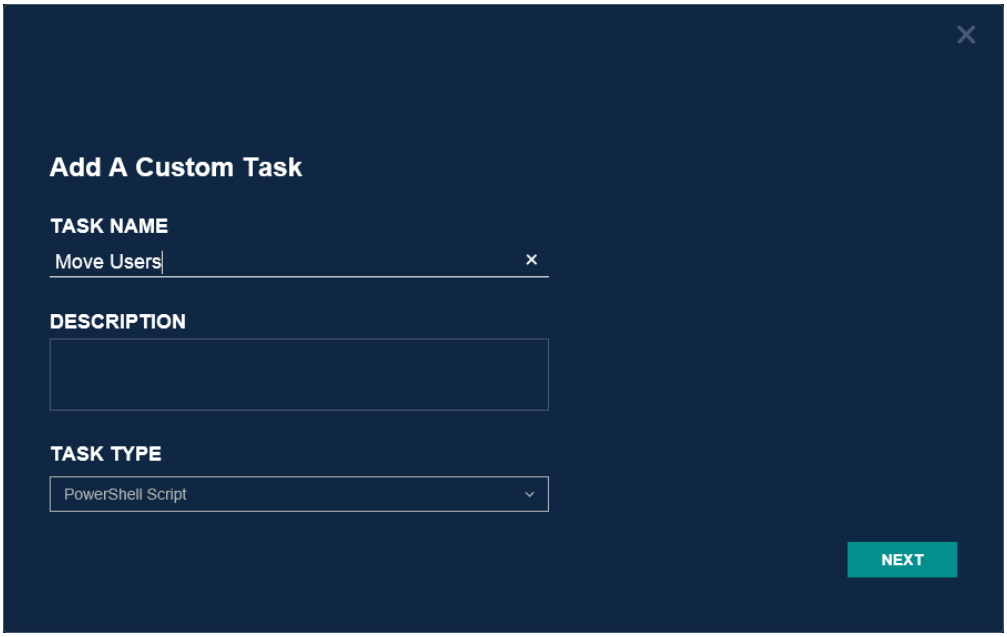


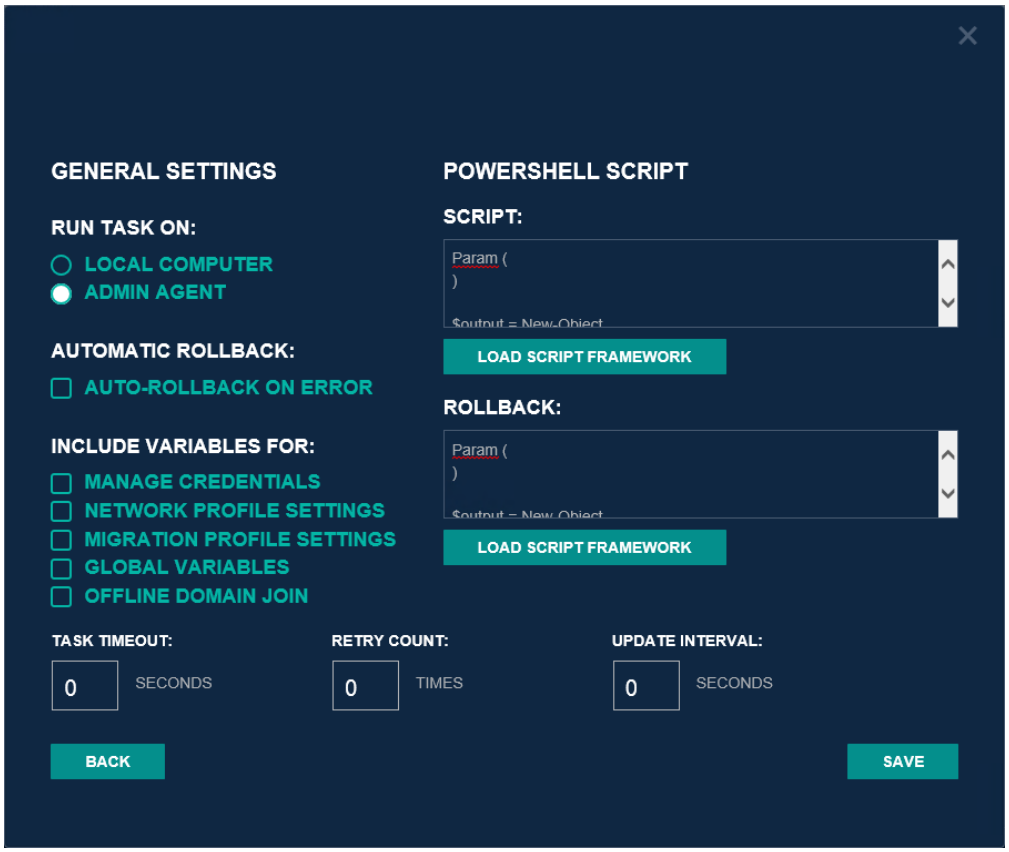
2. Install the Migrator Pro for Active Directory Agent on a machine outside the scope of Directory Sync Pro for Active Directory Synchronization profile which will be used to migrate Computers. This is going to be the Admin Agent machine used for running custom admin actions. You should see the Computer register after refreshing the screen.

3. On the Actions screen, add a new custom action with Action Target "User" selected. This will create an Actions menu option on the User Actions screen.

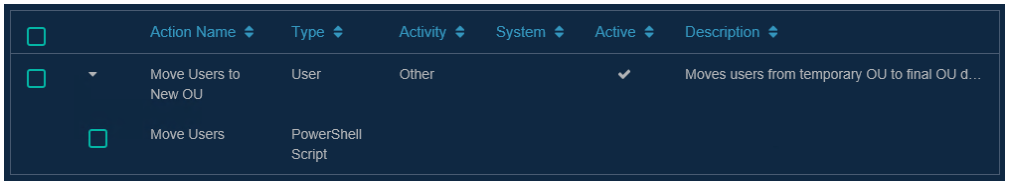


4. Add a Task to the new Custom Action. The "Run On Admin Agent" option must be checked. For this scenario, select "PowerShell Script" and edit the script. The script can call whatever credentials the PowerShell script should run under on the Admin Agent. The provided PowerShell script needs to clearly identify what Users are required to move and where the final destination is. A sample PowerShell starter script that moves users from one OU to another is available here. The provided sample script is meant to showcase the flexibility of the Admin Agent and is not representative of the definitive or best practices scripting method by which to accomplish moving users from one OU to another.

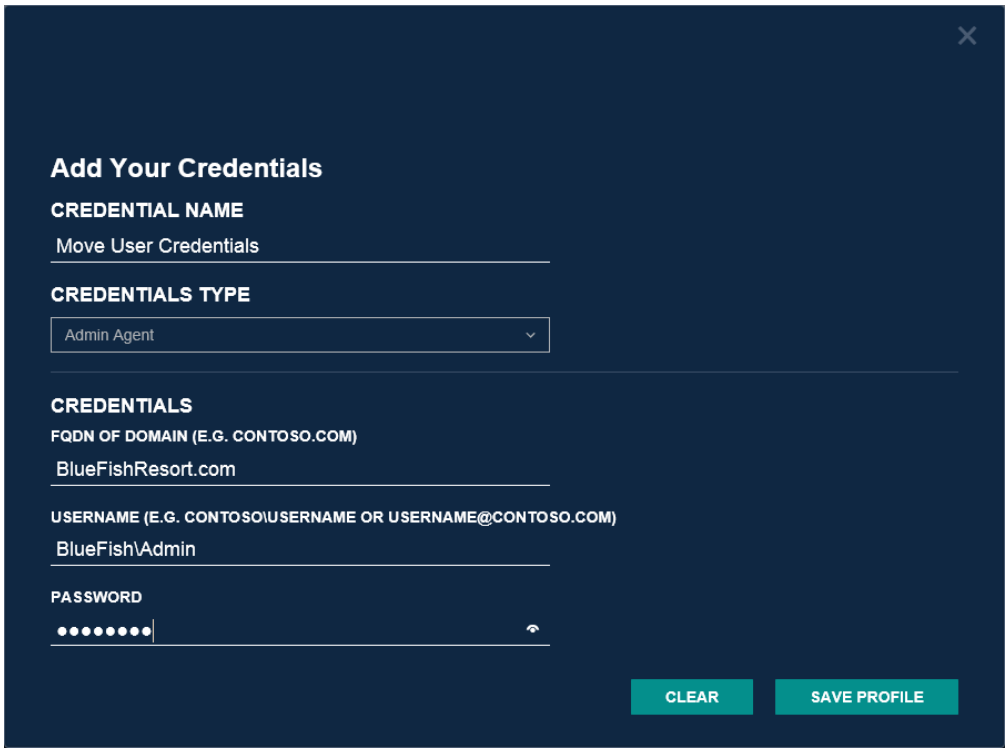




5. Add the task to the new CustomAction by selecting that row of the tasks table and then selecting the name of the new Custom Action in the Add to Action dropdown and clicking Add.



6. On the Credentials screen, add credentials the Admin Agent machine will use.



7. On the User Actions screen, select the Users you want to move, select the new Custom Action from the Actions menu, and click **Apply Action**.
8. Select the Admin Agent machine and the credentials on the Job Options window and click **Apply** to start the job. Instead of individual jobs for each User, a CSV file of Users to move is downloaded to the Admin Agent machine to run.
9. On the Agents screen, select the Admin Agent computer, select **View Jobs** in the Actions menu and click the **Apply Action** button to see the move job results.

Creating Mapping Files

Use the Mapping Files page to generate the User Mapping File (Map.usr) and Group Mapping File (Map.gg). These files are automatically created during the ReACL process so the only time they need to be created manually is when re-permissioning SQL databases.

To create the mapping files:

1. Click the **Export Mapping Files** button.
2. Use the browser options to open or save the mappings.zip file containing the User Mapping File (Map.usr) and Group Mapping File (Map.gg).

Each time the Create Mapping Files process is run, the Map.usr and Map.gg files are overwritten.

If the Active Directory environment is non-English, the values in the sAMAccountName column of the BT_SystemGroup table in the SQL database will need to be changed after Directory Sync Pro for Active Directory is installed to have the appropriate non-English values.

Global Variables

Global variables can be defined and be used across multiple scripts when defining Custom Actions. For example, a global variable to add the current date can be added to multiple scripts. Global variables will appear when selecting a starter script when creating a Custom Action if the "Requires Global Variables" option is selected.

To add a Global Variable:

1. Click the **Add** button.
2. Enter values in the following fields:
    - **Variable Name** (Required): Enter a name for the global variable. The name must contain alphanumeric characters and underscores only.
    - **Variable Value** (Required): The value of the global variable. Check the **Encrypted** box to encrypt the value in the database and hide the variable value in the interface.
3. Click the **Save** button.

Actions

Custom Actions and Tasks

New Custom Actions that appear in the Actions menu can be created on the Actions screen. Actions are a sequence of Tasks to complete a process.

The Actions screen will allow you to create a new Custom Actions that can be performed against Accounts, Computers or File Shares. Existing or new tasks can be added to a the desired Custom Action and then ordered as necessary to complete the custom process.

It is important to note that System actions and tasks can only be viewed or copied, they are not editable.

Adding or copying aN Action

To add or copy an action: Below the table, click **New** or select an existing Custom Action and click **Copy**. Check **Show System** to view and select any existing Systemactions.

- **Action Name** (Required): Enter a name for the Custom Action. The Action Name must be unique.
- **Description:** Enter a description for the action.
- **Action Display Name:** Enter the name that appears in the Actions menu.
- **Action Target:** Select one of the options from the drop-down list.
    - *Computer:* The Action will appear in the Actions menu on the Computers screen.
    - *File Share:* The Action will appear in the Actions menu on the File share screen.
    - *User:* The action will appear in the Actions menu on the Users screen.
    - *Contact:* The action will appear in the Actions menu on the Contacts screen.
    - *Resource Mailbox:* The action will appear in the Actions menu on the Resources screen.
    - *Group:* The action will appear in the Actions menu on the Groups screen.
    - *Admin Agent:* The action will appear in the Actions menu on the Admin Agents screen.
- **Action Type:** Select one of the options from the drop-down list. The Action Type determines what validations are applicable to the job, and which status columns are updated when the job runs. For example, a Custom Action with the ReACL type, will have the same validations as the System ReACL action.
    - *Other* (default): An action not related to any System action. No predefined validations are applicable. By default, new Actions are assigned as type Other.
    - *Discovery:* Gathers properties from the computer.
    - *ReACL:* Updates computer domain user profiles for use by the matching target user after cutover.
    - *ReACLRollback:* Rolls back all changes made by the ReACLShare process.
    - *ReACLShare:* Updates the File Share's domain user profiles for use by the matching target user after cutover.
    - *ReACLRollbackShare*: Rolls back all changes made by the ReACL process.
    - *Cutover:* Moves a computer from the source domain to the new target domain.
    - *Cleanup:* Removes the Source SIDs after the Cutover process completes.
    - *CleanupShare:* Removes the Source SIDs after the Cutover process completes.
    - *ExplicitRollback:* Rejoins a computer back to the source domain.
    - *UploadLogs:* Uploads log files from the Migrator Pro for Active Directory Agent to the Migrator Pro for Active Directory Server using Microsoft BITS.
- **Menu Selection Type:** This option is not editable. System types are read-only. User types can be edited.

Adding or copying a Task

To add or copy a task: Below the Tasks table, click **New** or select an existing task and click **Copy**. Check **Show System** to view and select an existing Systemtask.

- **Task Name** (Required): Enter a name for the task. The Task Name cannot begin with "BT-" which is used to identify system tasks.

- **Task Type** (Required): Select one of the options from the drop-down list.
    - *PowerShell Script:* Allows you to define a PowerShell script for the process on the Command and Rollback screens. Global Variables can be added and used in the script.
    - *Command Line:* Allows you to define a Command Line command for the process on the Command and Rollback screen. Global Variables can be added and used in the command line.
    - *Download File:* Downloads a file to the predefined Downloads folder.
- **Description:** Enter a description for the menu action.
- **General** : Mark or unmark the following checkboxes and enter the following options if adding or copying a PowerShell script or Command Line command:
    - *Automatic Rollback:* if checked, automatic rollback is added to the task.
    - *Requires Cutover Credentials:* if checked, the PowerShell script or Command Line command includes the $CutoverCredentials_XXXXX parameters.
    - *Requires Network Profile*: if checked, the PowerShell script or Command Line command includes the $NetworkProfile_XXXXX parameters.
    - *Requires Migration Options:* if checked, the PowerShell script or Command Line command includes the $MigrationOption_XXXXX parameters.
    - *Requires Global Variables:* if checked, the PowerShell script or Command Line command includes the Global Variables.
    - *Requires Offline Domain Join:* if checked, PowerShell script or Command Line command includes the Offline Domain Join parameters.
    - *Run On Admin Agent:* if checked, the PowerShell script or Command Line command can only be used on Admin Agents computers.
    - *Timeout (Seconds):* For PowerShell script or Command Line command, enter the number of seconds the process will be attempted before timing out.
    - *Retry Count:* For the PowerShell script or Command Line command, enter the number of times the process will be retried.
    - *Update Interval (Seconds):* For PowerShell script or Command Line command, enter the number of seconds between process runs.
- **Script:** Enter a PowerShell script or Command Line command. If creating a PowerShell script, click **Starter Script** to populate the entry box with the basic framework of a script. Enter or edit the Command Line command or PowerShell script. Text is required. The return value of the script or command will determine success or failure.
- **Rollback:** Enter a PowerShell script or Command Line command to run in case of failure/Rollback. Ideally this would undo the effects of the above script. If creating a PowerShell script, click **Starter Script** to populate the entry box with the basic framework of a script. Enter or edit the Command Line command or PowerShell script. Text is required. The return value of the script of command will determine success or failure.

- **Download:** Enter the following options if adding or copying a Download File task. When a new download job is created for a managed workstation, the specified file that is stored on the Migrator Pro for Active Directory Server (by deafault: c:\Program files\Binary Tree\ADPro\Downloads\) will be downloaded to c:\Program files\Binary Tree\ADPro Agent\Downloads\ on the workstation's local disk.
    - *File Name* (required): The file name. Based on the File Location for Download Jobs used during installation The File Name cannot contain invalid filepath characters and cannot use the following reserved file names: map.usr, map.gg, and ReACL-config.json.
    - *Target Location:* The Target Location of the download job. The Target Location cannot contain invalid filepath characters and cannot use the following reserved file names: map.usr, map.gg, ReACL-config.json. A Target Location is required if the File Name contains environment variables.
    - *Retry Count:* For PowerShell script or Command Line commands, enter the number of times the process will be retried.
    - *Update Interval (Seconds):* For PowerShell scripts or Command Line commands, enter the number of seconds between process runs.
    - *Timeout (Seconds):* For PowerShell scripts or Command Line commands, enter the number of seconds the process will be attempted before timing out.

The local download folder on an Migrator Pro for Active Directory managed machine will be secured with permissions only for the BUILTIN\Administrators group.

If rights other than BUILTIN\Administrators are required then the administrator will need to make a change on the local downloads folder (c:\Program files\Binary Tree\ADPro Agent\Downloads\) on the Agent machine.

Adding Tasks to Actions

To add a Task to an Action: Select a Task in the Tasks table, select an Action in the Select Action drop-down menu and click the **Add To** button.

Under a given Action the Tasks are listed in the order in which they will be executed. Drag and drop tasks to reorder them. Tasks can be viewed, copied, or removed by selecting the tasks and clicking the appropriate button.

Tasks marked as "Run On Admin Agent" can be added to Computer, User, Room, Contact, or Group Object Type menu selections (File Share is not supported). Tasks designed to run on computers or File shares can be added to Computer or File Share Object Type Actions only.

Activating Actions

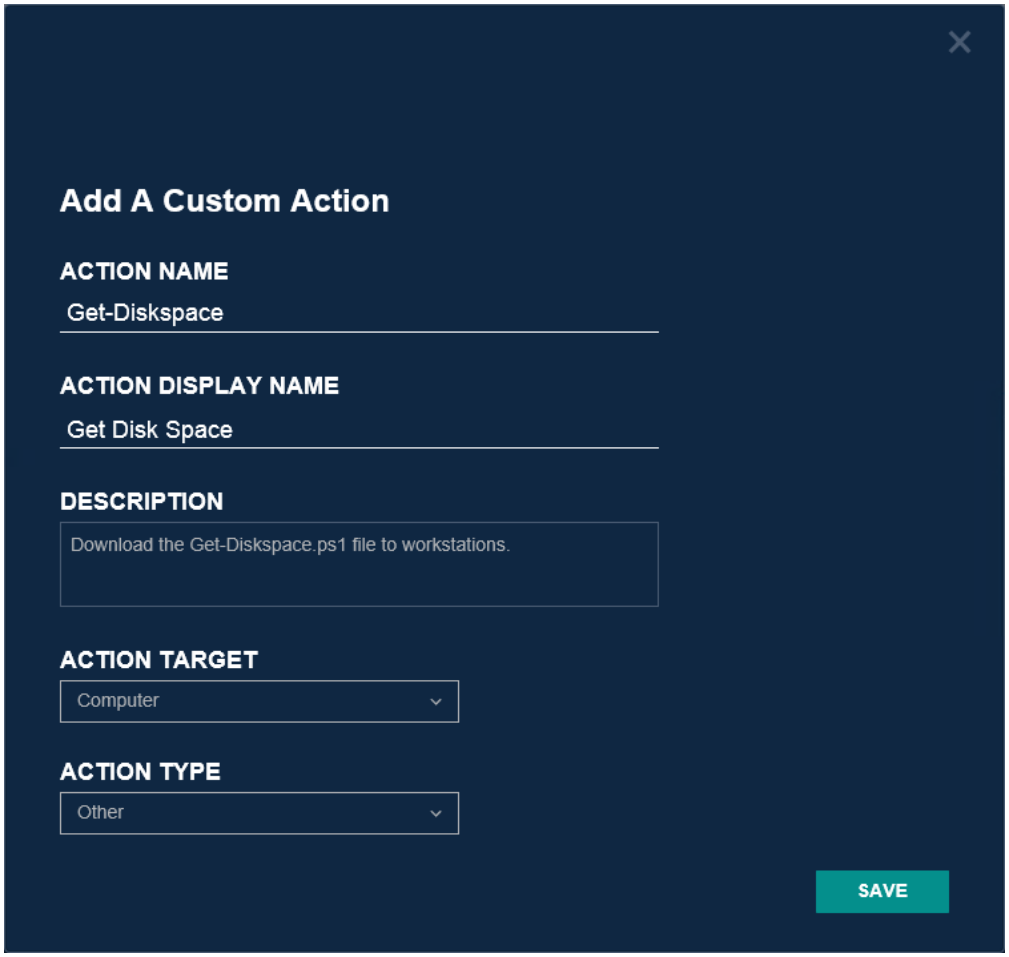
Only Actions marked as Active will appear in the Actions menus. Select an Action in the table and click the **Disable** or **Enable** button to change the active status of the Action. Inactive actions can be displayed in the table by clicking the **Show Disabled** button. You may want to create a new action, enable it, and then disable the corresponding System action.

Custom Action Example

Scenario: The administrator wants to download the Get-DiskSpace.ps1 file on selected workstations.

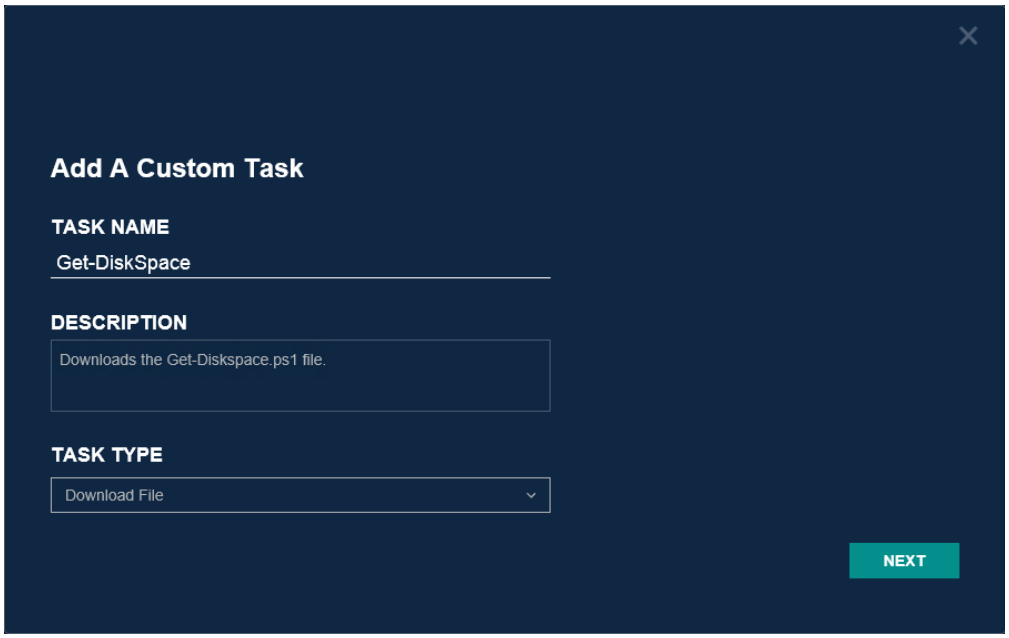
Steps:

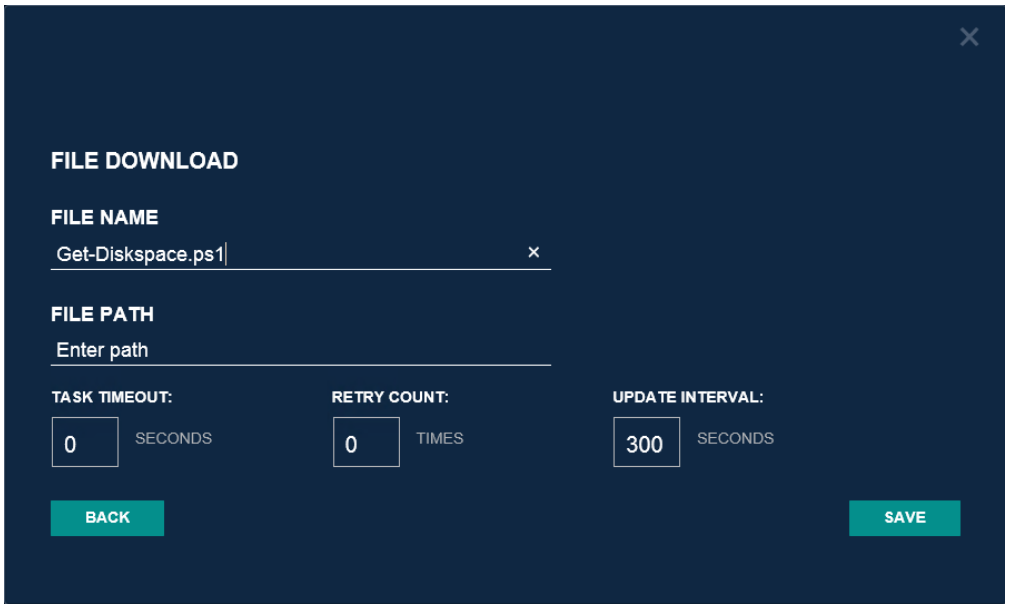
1. Copy the Get-DiskSpace.ps1 file into the file location for download jobs selected during the installation of Migrator Pro for Active Directory, *c:\Program files\Binary Tree\ADPro\Downloads* by default.
2. On the Actions screen, click the **New** button under the Actions table.
3. Add a Custom Action named "Get-Diskspace". The Action Display Name is how the option will appear in the Actions menu. Select the "Computer" Action Target so the menu option will appear in the Actions menu on the Computer Actions screen.



4. Click the **New** button under the Tasks table.

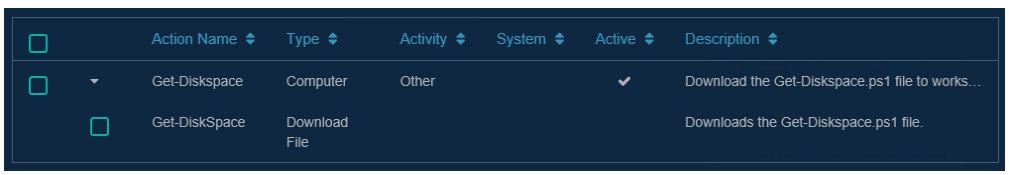
5. Select the "Download File" Task Type and enter the File Name. The full path to the file should not be entered.





6. Select the task, select "Get-Diskspace" from the Select Action drop-down menu and click the **Add To** button.

   Ensure the Action is active. The action can be expanded to view the associated Task.



7. On the Computer Actions screen, select the computers and then select the new "Get Disk Space" option from the Actions menu. When the new download job is run successfully against a machine, the Get-DiskSpace.ps1 file will reside locally on disk at c:\Program files (x86)\Binary Tree\ADPro Agent\Downloads.

Reports

The Migration Reports screen allows you to view reports for the current AD migration, devices, migration groups, and users. Reports are available only if the Reporting feature was installed and configured.

Dashboard

The Dashboard report is a high level status report of the current AD Migration.

To view the Dashboard Report:

1. Select **Dashboard** from the drop-down list.
2. To filter the report to display a specific Migration Wave, select an option from the **Select Migration Group** (Migration Wave) drop-down list and click the **View Report** button. If no Migration Groups have been created, the only option available is **ALL** which displays all objects.

The report displays the following data:

- User Preparation Status - Displays the number of Users prepared and not prepared for migration.
- User Migration Status - Displays the number of Users migrated and not migrated.
- Device Preparation Status - Displays the number of Computers prepared and not prepared for cutover.
- Device Cutover Status - Displays the number of Computers that have completed cutover and have not completed cutover.
- Devices that Failed to Cutover - Displays the number of Computers that failed cutover and completed cutover.
- User Profiles to Devices Relationship - Displays the Users that have logged onto each computer.

Device Detail Report

The Device Detail Report is a detailed report of computer information.

To view the Device Detail Report:

1. Select **Device Detail Report** from the drop-down list.
2. To filter the report to display a specific record, select an option from one or more drop-down lists and click the **View Report** button.

The report displays the following data for each Computer:

- Migration Group - The Migration Group (Migration Wave) name if assigned.
- Name - The sAMAccountName attribute of the source Computer.
- Device Not Checking In - Is the Computer failing to check in with the server.
- Source DN - The distinguished name attribute of the source Computer.

- Registered - Is the Computer registered with the server.
- Discovery - The status of the Discovery process.
- ReACL - The status of the ReACL process.
- Cutover - The status of the Cutover process.
- Cleanup - The status of the Cleanup process.
- Prepared for Migration - This column is checked if the Computer has successfully started the Cutover process.
- Last Contact - The time and date of the last contact between the Agent and the Migrator Pro for Active Directory Server.

This report includes an extra blank page that can be ignored.

Devices that Failed to Cutover

The Devices ailed to Cutover report is a report displaying computers that did not successfully complete the Cutover process.

To view the Devices that Failed to Cutover Report:

1. Select **Devices that Failed to Cutover** from the drop-down list.
2. To filter the report to display a specific Migration Wave, select an option from the **Migration Group** drop-down list and click the **View Report** button. If no Migration Groups have been created, the only option available is **ALL** which displays all Computers.

The report displays the following data for each Computer:

- Device Name - The sAMAccountName attribute of the source Computer.
- Migration Status - The status of the migration.
- Last Job Message - The last job status.

Migration Group Status

The Migration Group Status report displays metrics information about all migration objects.

To view the Migration Group Status Report:

1. Select **Migration Group Status** from the drop-down list.
2. To filter the report to display a specific Migration Wave, select an option from the **Migration Group** drop-down list and click the **View Report** button. If no Migration Groups have been created, the only option available is **ALL** which displays all objects.

User Status Report

The User Status Report is a detailed report of User information.
To view the User Status Report:

1. Select **User Status Report** from the drop-down list.
2. To filter the report to display a specific record, select an option from one or more drop-down lists and click the **View Report** button.

The report displays the following data for each User:

- Migration Group - The Migration Group name.
- Display Name - The display name attribute of the source user account.
- Source User ID - The User ID of the source user account.
- Target User ID - The User ID of the target user account.
- Source DN - The distinguished name attribute of the source user account.
- Target DN - The distinguished name attribute of the target user account.
- Source UAC - Indicates if the user account is enabled in the source.
- Target UAC - Indicates if the user account is enabled in the target.
- Migrated - This column shows any users that have been manually tagged with the Migrated status. This is an optional tag for tracking purposes and does not necessarily represent a successful user migration.
- Prepared for Migration - A value of True verifies that the user has been synchronized with the target.
- Ready to Sync - User has been marked as Ready-to-Sync.
- Failed to Sync - If the Ready-to-Sync value is True, AND Failed to Sync value is True, this means that the synchronization has actually failed. Examine the log for details. If the Ready-to-Sync value is False, and Failed to Sync is a value of True, this means that synchronization has not yet been attempted for this User.
- Status Message - The last status. No message is displayed if Failed to Sync is False.
- Migration Group ID - The ID of the Migration Group.

User Profile to Device Relationship Report

The User Profile to Device Relationship Report is a report showing the users that have logged onto each computer.
To view the User Profile to Device Relationship Report:

1. Select **User Profile to Device Relationship** from the drop-down list.
2. To filter the report to display a specific Migration Group (Migration Wave), select an option from the **Migration Group** drop-down list and click the **View Report** button. If no Migration Groups have been created, the only option available is **ALL** which displays all computers.

The report displays the following data for each User:

- Device Name - The name of the Computer which this User has logged into.
- sAMAccountName - The sAMAccountName of the User.
- First Name - The first name of the source User.
- Last Name - The last name of the source User.
- Profile Last Used - The last date the profile was used.

Report Options

Report options are available above the displayed report.

- Paging - Click the **First Page**, **Previous Page**, **Next Page**, and **Last Page** arrows to page through a multi-page report.
- Refresh - Click the **Refresh** icon to update the data in the report. This option is also available in the right-click menu while hovering over the report.
- Zoom - Click the drop-down list and select a zoom option. This option is also available in the right-click menu while hovering over the report.
- Export - Click the **Export** icon to select a format to export. This option is also available in the right-click menu while hovering over the report.
- Print - Click the **Print** icon to open printing options. This option is also available in the right-click menu while hovering over the report.
- Find / Next - Enter a value to search for in the report and click **Find**. Click **Next** to find the next instance of the value.

User Management

The User Management page allows you to enable role-based access control. When using role-based access control, users can be assigned a role to limit actions and access to information in the application.

The User Management page can be accessed by selecting Manage Roles under Settings in the action menu. This page is visible to all users if no Global Administrators have been defined and only to Global Administrators when one or more have been defined.

User Roles

Global Administrator

- Allows creation of new profiles
- Allows modification of configuration in the application/database for all profiles
- Allows creation or modification of Cutover activities and custom actions for all profiles
- Can submit migration events, including ReACL and Cutover actions for workstations, as well as user Cutover actions (enable/disable) for all profiles
- All configuration pages can be accessed

Profile Administrator

- Cannot create of new profiles
- Can submit migration events, including ReACL and Cutover actions for workstations, as well as user cutover actions (enable/disable)
- All configuration pages can be accessed
- Allow modification of configuration in the application/database
- Allow creation or modification of Cutover activities and custom actions

Migration Operator

- Can submit migration events, including ReACL and Cutover actions for workstations, as well as user cutover actions (enable/disable)
- Configuration pages cannot be accessed
- Cannot modify configuration in the application/database
- Cannot create or modify Cutover activities and custom actions

Read Only User

- Can view directory synchronization results and logs
- Can view Active Directory Cutover status
- Configuration pages cannot be accessed
- Cannot modify configuration in the application/database
- Cannot create or modify Cutover activities and custom actions

Troubleshooting

- **Problem:** What do you do when a user tries to use a network printer post ReACL process and/or Cutover and receives an access denied error?

  Solution: Synchronize the SID History for that User to resolve the problem.

- **Problem:** ASP.NET will sometimes not register properly with IIS, which can cause errors when the Migrator Pro for Active Directory Agent tries to communicate with the Web Service. How do I address this?

  Solution: During installation, the installer needs to enable the IIS feature for the Server if the feature was not enabled so that web-service can be installed and configured. To address this problem, you should manually re-register the ASP.NET with IIS. To do this, run the below command on the server under C:\Windows\Microsoft.NET\Framework\v4.8:

  aspnet_regiis -i

- **Problem:** What do I do if the Agent_<datetime>.log shows an Error: Login failed for user 'IIS APPPOOL\ADM AppPool' in System.Data.SqlClient.SqlException?

  Solution: To fix this:

  1. Open SQL Management Studio where Directory Sync Pro for Active Directory databases were setup
  2. Go to SQL Server Security -> Logins
  3. New Login
  4. User name: IIS APPPOOL\ADM AppPool
  5. Click on **User Mappings**
  6. Select BTCodex for the database
  7. Select db_datareader and db_datawriter for Roles
  8. Click **OK**
  9. Restart the Agent on the workstation or wait for the next polling interval

- **Problem:** Observed Access Denied error when trying to ReACL a Windows NAS Shared Drive.

  Solution: To fix this:

  1. Add the user credential in the NAS Profile screen in the Migrator Pro for Active Directory Console. This user should be installed on a workstation with Local Admin Rights
  2. After the Agent is installed on the workstation, change the Migrator Pro for Active Directory Agent Service account from Local System to the user credential specified in step 1. This user should also be logged in on the workstation as well
  3. Turn off UAC on the workstation
  4. ReACL the Windows NAS Shared Drive

- **Problem:** Users are getting an error message that their Recycle Bin has been corrupted once their computer has been migrated.

  Solution: This is a common issue with Domain Migrations and is caused when the Recycle Bin is not empty. This is happening because the name of the Recycle Bin is the user's SID and the Recycle Bin cannot be ReACL'd. After the workstation has been ReACL'd and migrated when the user logs on, if the existing Recycle Bin is not empty the user cannot access it. But if the existing Recycle Bin is empty a new one is created and the Target user's SID is the name of the Recycle Bin.

  Resolution: Empty the Recycle Bin as part of the Cutover process

- **Problem:** Directory Sync Pro for Active Directory does not start if SQL Authentication method is used with Windows Authentication.

  Solution: Manually add the computer account to the SQL server and grant it the sysadmin role. To accomplish this, perform the following steps.

  1. Via the SQL Management Studio, open a new query window and enter the below script
  2. CREATE LOGIN [Domain\machine_name$] FROM WINDOWS
  3. Via the Security and Logins, locate the newly created Computer Name
  4. Grant this user with sysadmin role

- **Problem:** A workstation that has been successfully cutover no longer responds to any additional jobs, such as Cleanup.

  Solution: If a workstation that has been successfully cutover now fails to respond to any additional jobs, such as Cleanup, check the Application event log. If you see a *"The remote name could not be resolved"* error, this most likely means that the SRV record for the Migrator Pro for Active Directory Server can no longer be resolved due to a DNS lookup failure.

  If you cannot "Ping" the Migrator Pro for Active Directory server from any other machines in the target domain, then you will need to remedy this on a more global scale, such as creating a conditional forwarder on the target machines' current DNS server pointing to the appropriate location.

  If you are able to "Ping" the Migrator Pro for Active Directory server, then check the Network Profile that was used during the Cutover to verify that the DNS settings were correct in that profile.

Password Sync Troubleshooting

- **Problem:** If you encounter "Access is denied" errors when syncing passwords with Directory Sync Pro for Active Directory.

  Solution: This is most likely because the utility (psexec.exe) used for remote calls to the Global Catalog is failing. Some things you can try are:

  1. Try the GC server's IP address, FQDN and Shortname. IP address often works when others do not.
  2. From the Directory Sync Pro for Active Directory machine browse to \\[GC]\admin$ with the admin username\password
  3. Run the Directory Sync Pro for Active Directory service with credentials that have access to the GC instead of as LocalSystem
  4. Firewalls\Anti-Virus software should not be a problem but turning them off may help

Migrator Pro for Active Directory Agent Installation Troubleshooting

- **Problem:**The Computer registers, but does not get discovered (Discovery Status remains blank in the Migrator Pro for Active Directory console).

  Solution: Install PowerShell 2.0 or higher on the client. Operating systems earlier than Windows 7 do not natively include PowerShell.

- **Problem:** During manual installation, a "wizard interrupted" error appears.

  Solution: Install .NET 4.5.2 or higher on the client and run the installer again.

- **Problem:** After a successful manual install, an "Unable to register" error appears in the Event Viewer.

  Solution: Verify the path to the Migrator Pro for Active Directory server is correct and complete.

- **Problem:** After a successful manual install, an "Unable to auto-discover" error appears in the Event Viewer.

  Problem: The SRV records are missing, incorrect, or unreachable. Verify SRV records are set up properly.

Migrator Pro for Active Directory BITS Troubleshooting

- **Problem:** The Migrator Pro for Active Directory UI issued the 'Upload Logs' command to the Agent for a device, but nothing was uploaded to the web server.

Solutions:

From the IIS Web Server where Migrator Pro for Active Directory Web Service is installed:

1. Open IIS Manager.
2. Verify that Default Web Site > adm > DeviceLogs exists
    a. Verify there is a BITS Uploads option icon in the Feature View (at the bottom)
    If not, use PowerShell to install
    Import-Module ServerManager
    Add-WindowsFeature BITS-IIS-Ext
    b. Verify in the BITS Upload view, that "Allow clients to upload files" is checked

1. Open IIS Manager
2. Go to Default Web Site -> adm -> DeviceLogs
3. Click on Basic Settings in the right pane
    a. Verify the Application Pool is set to "ADM AppPool"
4. Click on Edit Permissions -> Security tab
    a. Verify the IUSR account is in the list and has the following permissions: Modify, Ready & execute, List folder contents, Read, Write

On the Device where the 'Upload Logs' command was issued:

1. Navigate to C:\Program Files (x86)\Binary Tree\ADPro Agent\Files
2. Open the agent_<date>.log in Notepad
    a. Verify the URI for the server /api and /devicelogs location is correct

1. Navigate to C:\Program Files (x86)\Binary Tree\ADPro Agent\Files
2. Open the PowerShell-<date>-<time>-BT-UploadLogs.log file
    a. Check for problems or errors

1. Go to Start -> Run -> services.msc
2. Verify the Background Intelligent Transfer Service is started

Additional Information

Cutover Job Result Codes

Result Code	Error	Rollback Possible
1	Unidentified Error - PowerShell Command Error	No
2	Source Domain could not be contacted	No
4	Bad Source Credentials	No
8	Target Domain could not be contacted	No
16	Bad Target Credentials	No
32	Target DNS Server could not be contacted or could not resolve the target DNS domain	No
64	Change Obtain DNS by DHCP	
128	Set DNS Server IPs	
256	Set WINS Servers	
512	Register NIC with DNS	
1024	Clear DNS Suffix Search List / Set to use NIC	
2048	Set Alternate DNS Suffix List	
4096	Enable Dynamic DNS Registration	
8192	Set NIC Specific DNS Suffix	
16384	Domain Disjoin Failed	
32768	Domain Join Failed	
65536	Source domain name does not match the system's domain	No
131072	Computer Reboot failed	
262144	Target Domain Name could not be resolved via existing DNS, and new DNS Servers were not provided	No

An odd numbered result code represents an error running the Cutover PowerShell script. The most common cause of an odd numbered result code during Cutover is that the computer either has no network card with a default gateway or more than one network card with a default gateway.

Result codes are additive. There are likely multiple errors if the result code is not represented in the table.

Upload Logs Result Codes

This table includes result codes for BT-UploadLogs PowerShell jobs.

Result Code	Error	Rollback Possible
32	(zip folder) could not be created.	No
64	Failed to Zip log files on computer.	No
128	Upload failed to contact the server. Please verify the URL (url) is correct and BITS is enabled.	No

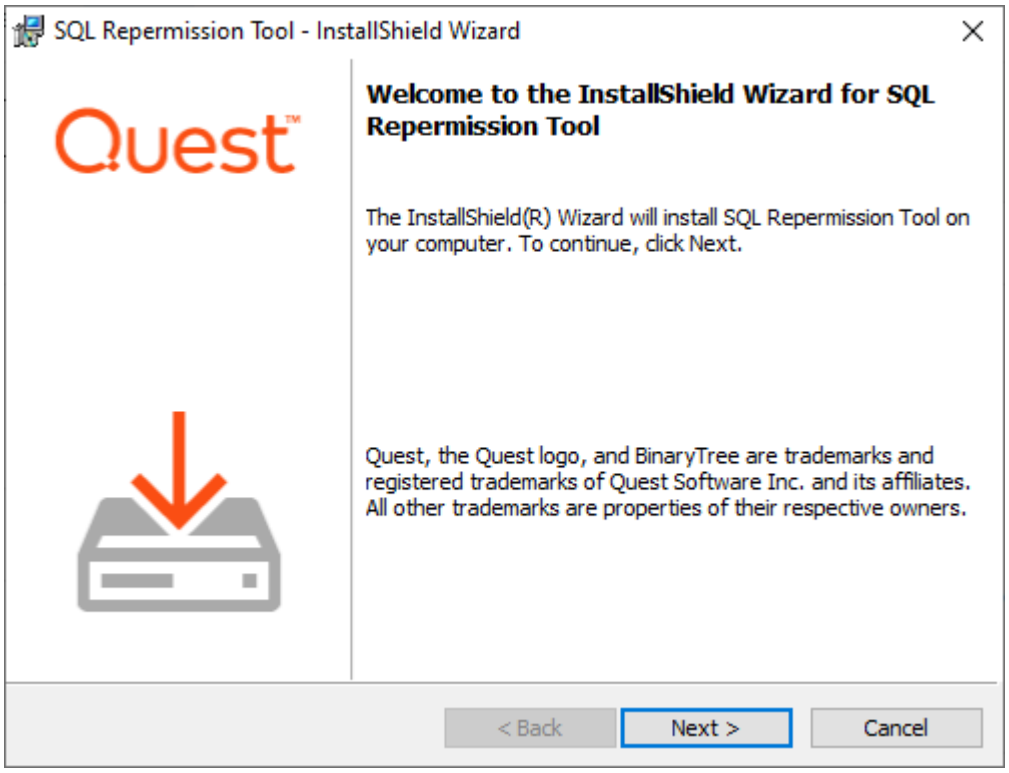
SQL Repermission Tool

Use the SQL Repermission Tool to update a SQL Server's Source AD Windows Authentication Group Login permissions and their associated database users for the Target domain to which the user and group objects have been migrated.

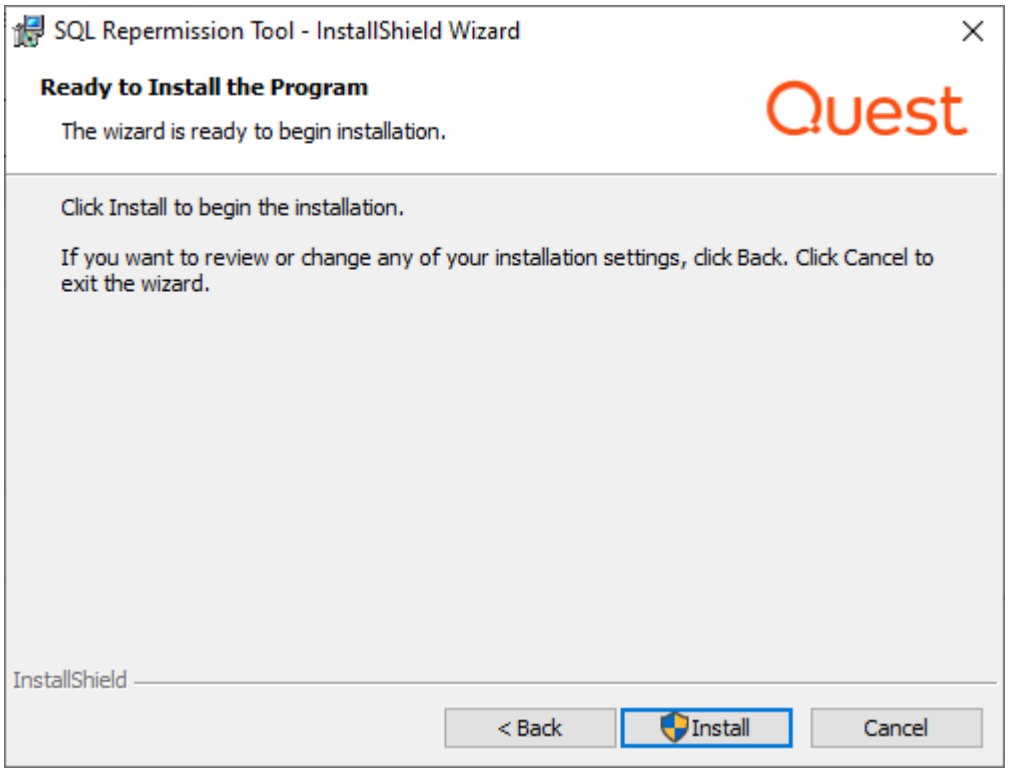
Prior to re-permissioning SQL servers, accounts must be migrated and Mapping Files created using Migrator Pro for Active Directory.

1. Open the **SQL Repermission.msi** file included in the installation.
2. Run the installer on the Migrator Pro for Active Directory Server or any machine that will have access to the SQL Server instance and databases to be re-permissioned.

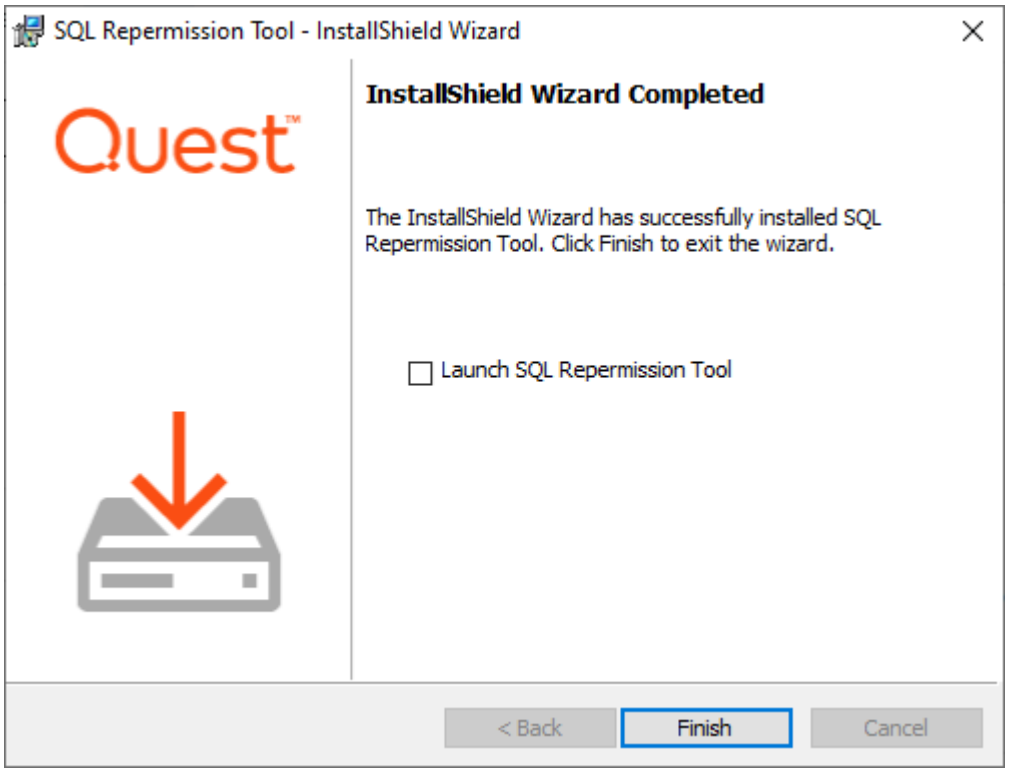
3. The Welcome screen appears. Click **Next** to continue.



4. The "Ready to Install the Program" screen appears. Click **Install** to begin the installation.

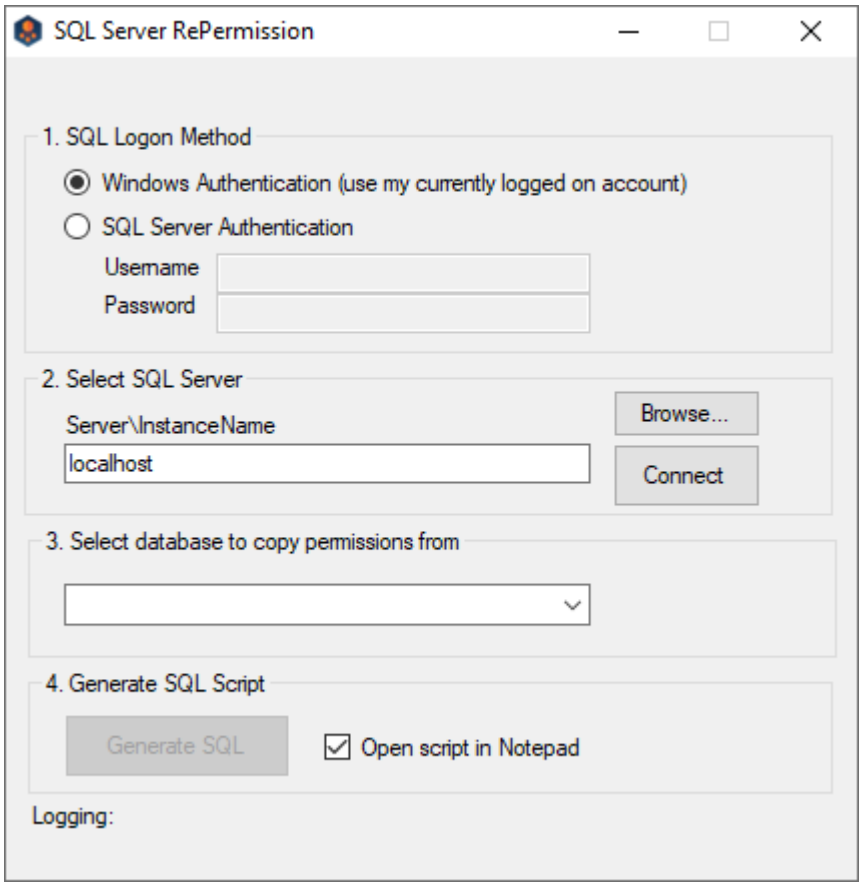


5. When the installation completes, the "InstallShield Wizard Completed" message appears. Click **Finish** to close the wizard.



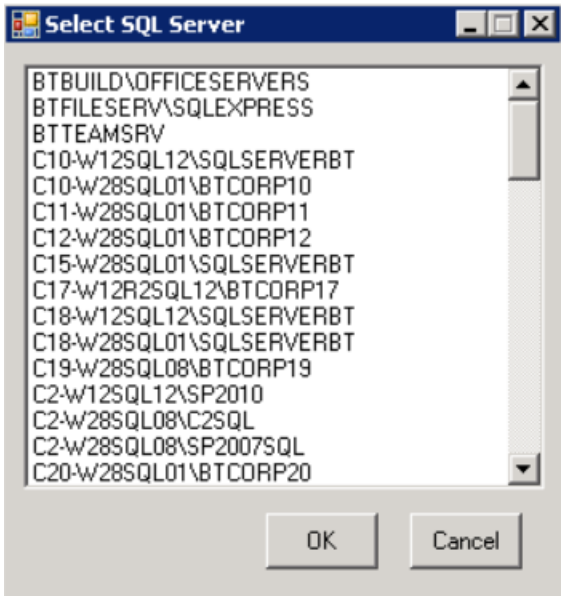
6. Copy the **map.usr** and **map.gg** files created using Migrator Pro for Active Directory to a folder on the same machine.

7. Launch the SQL Repermission Tool from the Apps screen or the Start menu.

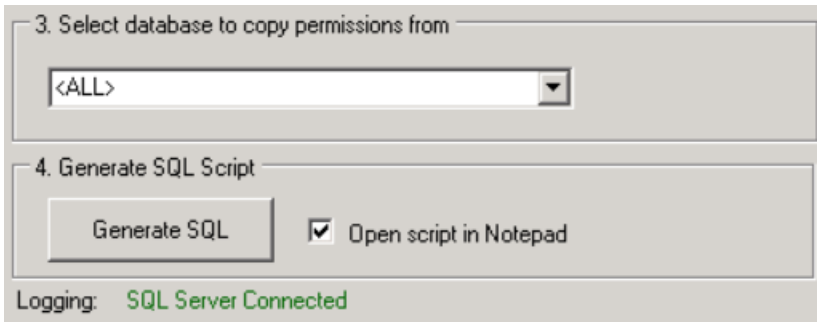


8. Select the **SQL Logon Method**. If SQL Server Authentication is selected, enter the Username and Password. If Windows Authentication will be used, you must be logged onto the machine with an account that has access to the SQL Server instance and databases to be re-permissioned.
9. Click on **Browse** to select the SQL Server instance to be re-permissioned.

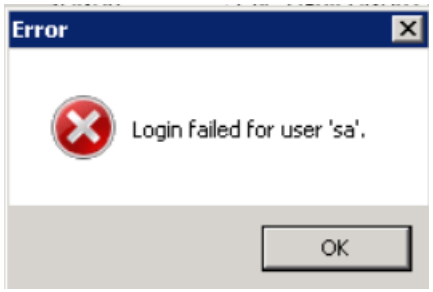
10. Select the SQL server instance from the list and click on **OK**.



11. Click on the **Connect** button. If connection is successful, the Logging message should read “SQL Server Connected” and there should be databases available to pick from in the drop-down list.



Note: If the login information is incorrect, the following error will be received. The credentials to connect to the SQL server instance should be corrected, and then the Connect should be retried.



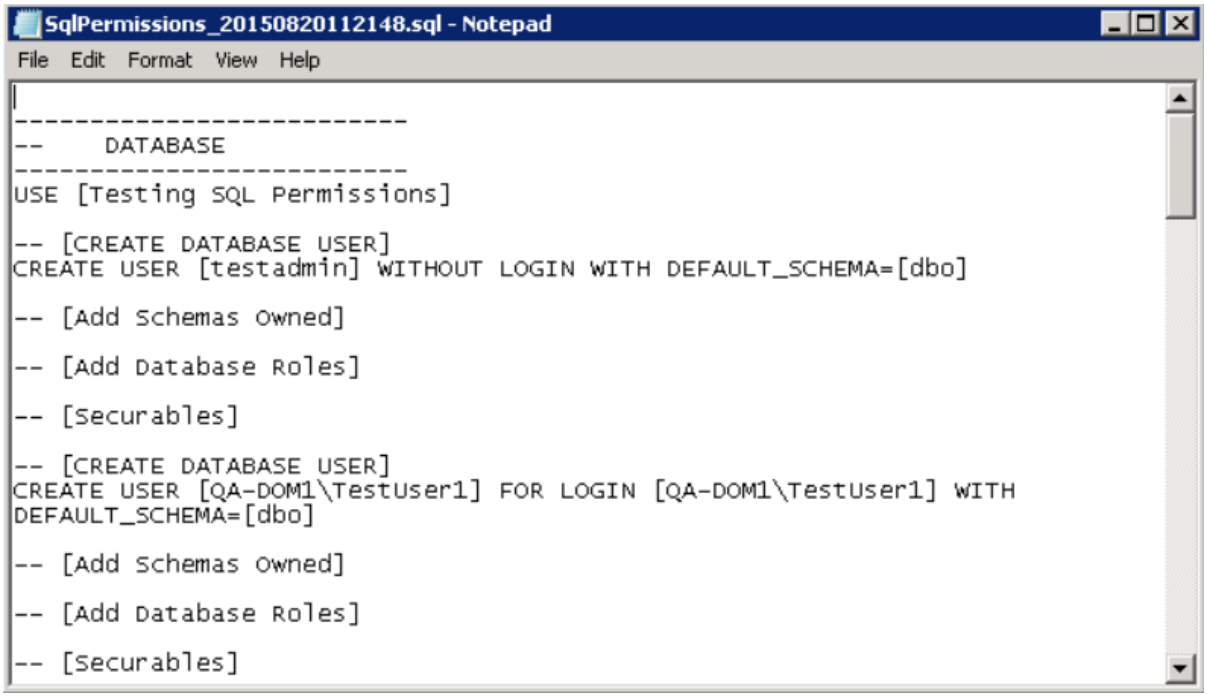
12. Once successfully connected to the SQL Server instance, in the drop down select either **<ALL>** or a specific database that needs to be re-permissioned.

13. Click on the **Generate SQL** button. If the **Open script in Notepad** option is left checked, the results will be displayed when completed.

14. The Logging information will display the name of the SQL file created in the directory that the application is located.

15. If the option to open the file in Notepad was not checked, navigate to where the file was saved and right-click and choose **Open with Notepad**.

16. The results of the process can be reviewed prior to actually executing it on the SQL Server instance.



17. When the SQL file has been reviewed, either open the file in SQL Server Management Studio or create a new Query in SQL Server Management Studio and copy/paste the contents of the file into the Query.

18. Execute the Query and the new target credentials will be created.

Installing and Configuring SQL Server Reporting Services

Installing SQL Server Reporting Services

These instructions are for existing SQL Server installs where reporting services are being added.

1. Load the ISO into the DVD drive.
2. Open **My Computer**.

3. Double-click on the DVD drive to run the **SQL Server Installation Center** dialog.
4. Select **Installation** from the left.
5. Select **New installation or add features to an existing installation**.
6. Click the **OK** button on the Setup Support Rules page if everything passed.
7. Click the **Install** button on the SQL Setup Files page.
8. Click the **Next** button on the Setup Support Rules page if everything passed.
9. Select **Add features to an existing instance of SQL Server** (verify your instance is shown).
10. Click the **Next** button.
11. Check the **Reporting Services** box and click the **Next** button.
12. Click the **Next** button on **Installation Rules**.
13. Click the **Next** button on **Disk Space Requirements**.
14. Click in the **Account Name** field and select **NT AUTHORITY\NETWORK SERVICE**.
15. Click the **Next** button.
16. Click the **Next** button on the **Reporting Services Configuration** to **Install, but do not configure the report server** option.
17. Click the **Next** button.
18. Click the **Next** button on Installation Configuration Rules page if everything passed.
19. Click the **Install** button on the Ready to Install page.
20. If you have a green checkmark on the 'Complete' page, click the **Close** button.
21. Close the SQL Server Installation Center dialog.

Configuring SQL Server Reporting Services

1. Click **Start** > **All Programs** > **Microsoft SQL Server** > **Configuration Tools**.
2. Click on **Reporting Services Configuration Manager**.
3. Click the **Connect** button.
4. Select **Service Account** from the left.
    - Verify Network Service is set for the built-in account.

5. Select **Database** from the left.
    - Click the **Change Database** button.
    - Verify 'Create a new report server database' is selected and click the **Next** button.
    - Set your security type and click the **Next** button.
    - Leave the defaults. Verify 'Report Server Mode' is set to 'Native' (Reporting will fail to work if not in Native Mode)
    - Click the **Next** button.
    - Click the **Next** button.
    - Click the **Next** button and it will begin to configure the database.
    - Click the **Finish** button.
6. Select **Web Service URL** from the left pane.
    - Click the **Apply** button.
7. Select **Report Manager URL** from the left pane.
    - Click the **Apply** button.
8. Click the **Exit** button.

Your Report URLs

Browseable URL

http://<servername>/Reports
or
http://<servername>/Reports_InstanceName (if SQL Server is installed as an instance)

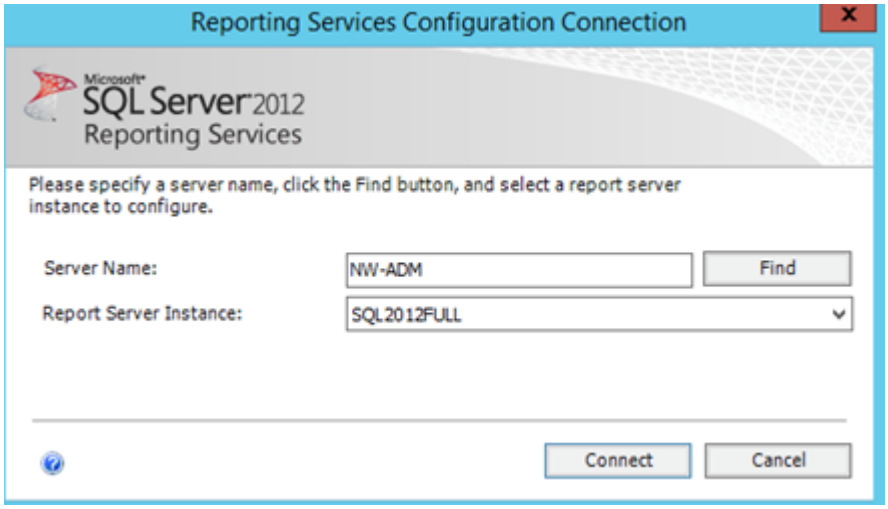
Web Service URL

http://<servername>/ReportServer
or
http://<servername>/ReportServer_InstanceName (if SQL Server is installed as an instance)

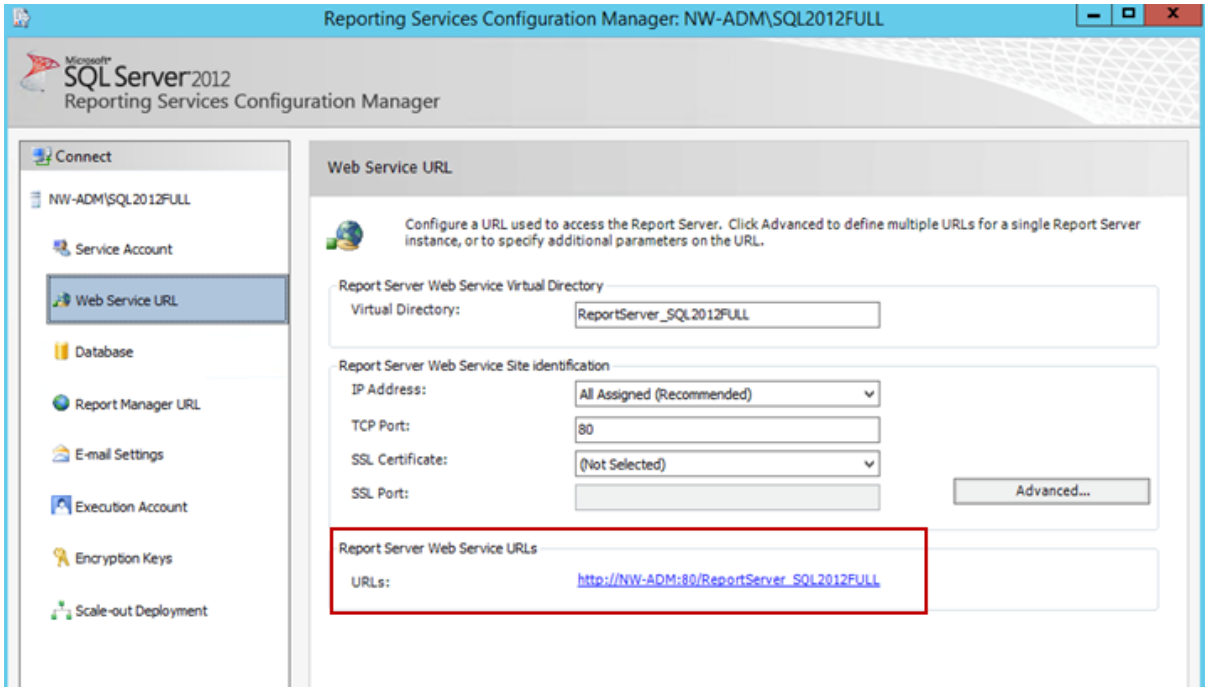
Verifying the Report Server URL

The Report Server URL is needed when installing the Reporting feature. Use the following steps to verify the correct URL to use.

1. Open up Reporting Services Configuration Manager.
2. Provide the SQL Server Name and Report Server Instance name and click **Connect**.



3. In the left folder navigation, select **Web Service URL**.
4. The Report Server URL appears in the Report Server Web Service URLs section.



Creating a Linked Exchange Account

This process supports customers that require completing their AD migration before their Exchange migration by creating a linked Exchange account. This allows users to log into their mailbox that still resides in the source Domain, using their target credentials.

After an account has been migrated, the computer ReACL'd and Cutover to the target, follow these steps in order to link the target account to the Exchange mailbox still residing in the source.

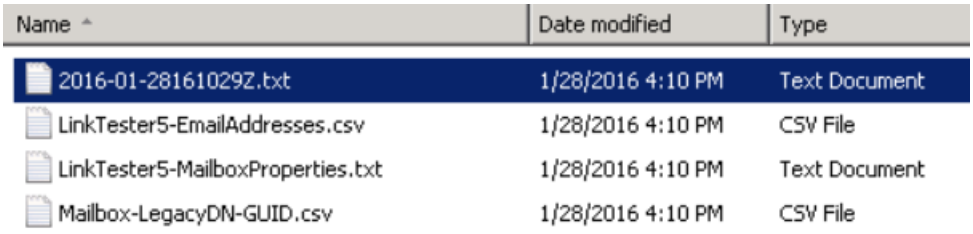
- In the Migrator Pro for Active Directory Console:
    1. Run the Action on the migrated user accounts "Enable on Target/Disable on Source".
    2. Execute Sync in Migrator Pro for Active Directory for that Directory Sync Pro for Active Directory Synchronization Profile.
    3. Run the "Mark as Migrated" Action on the above user accounts.
    4. Filter on the "Migrated" column as "True" and verify only the accounts to be actioned are in the grid.
    5. Export the Migrator Pro for Active Directory Grid to a CSV.
- On the Source Exchange server:
    1. Download the script file to a local directory and rename BT-ConvertMBX-to-Linked.ps1. The script can be obtained by contacting Support.
    2. Copy the updated CSV created from export of the Migrator Pro for Active Directory grid to the same local directory.
    3. Run the following Exchange PowerShell command – replace items in red date with actual data.

.\BT-ConvertMBX-to-Linked.ps1 –InputCsvPath c:\temp\Export.csv –OutputFolder c:\temp\outputlog –SourceDomainDC E2E-DC1.DOM1.E2E.dom –SourceDomainGC E2E-DC1.DOM1.E2E.dom –TargetDomainController QA-E2E-DC1.QA-Dom1.QA-E2E.dom

Results:

```
[PS] C:\temp>.\BT-ConvertMBX-to-Linked.ps1 -InputCsvPath c:\temp\Export.csv -OutputFolder 'ExchangeBackup'
DC E2E-DC1.DOM1.E2E.dom -SourceDomainGC E2E-DC1.DOM1.E2E.dom -TargetDomainController QA-E2E-DC1.QA-Dom1.QA-
Output Directory present

Transcript started, output file is .\ExchangeBackup\2015-11-12101045Z.txt

Start Processing Mailbox:  Link Tester7
Source Mailbox Disabled  Link Tester7
Primary Mailbox re-enabled for attached to user

Setting Mailbox Properties
Processing Complete for Mailbox:  Link Tester7

Transcript stopped, output file is C:\temp\ExchangeBackup\2015-11-12101045Z.txt
[PS] C:\temp>_
```

Log output will also be created in the directory specified in the PowerShell command.



Verification:

- Check the following AD attributes:
    1. msExchMasterAccountSid of the source account should contain the target account objectSID value.
    2. Check that the legacyExchangeDN on the both the source and target account has not changed.
- Check the mailbox using Outlook
    1. Log in to computer using target account.
    2. Launch Outlook.
    3. Outlook should launch without prompting for credentials (should us pass-through authentication).
    4. Check that any additional proxyaddress' are still present on the source user mailbox.
    5. Spot check in Outlook for the retention of signatures, tool bar edits, etc.

Additionally:

- Once all of the above has been completed and verified, migrate the mailbox to the target Exchange and verify that it is still accessible.

Sample Admin Agent PowerShell Script

This is a sample PowerShell starter script that moves users from one OU to another. You may want to use this as a baseline on which to build your own custom scripts. Be sure to test your scripts in a non-production environment.

```
Param (

    [System.String] $Credentials_Username = $null,

    [System.String] $Credentials_Password = $null,

    [System.String] $DomainController = $null,

    [System.String] $TargetOU = $null
)

$WarningMessages = New-Object System.Collections.ArrayList

try
{
    #Migrator Pro for Active Directory PowerShell Output Object
    #This object is used to report status to the Migrator Pro for Active Directory Console
    $output = New-Object BinaryTree.ADMigrator.Agent.PSHelpers.PSOutput

    #Verify input parameters are not $null.
    if($Credentials_Username -eq $null -OR $Credentials_Password -eq $null -OR $DomainController -eq $null -OR $TargetOU -eq $null)
```

```
    {
        #Write-Error will show in Migrator Pro for Active Directory Log
        Write-Error 'Credentials_Username, Credentials_Password, DomainController,
and TargetOU parameters are required.'
        $output.ResultCode = 1
        return ($output)
    }

    #Output object's AgentFilePath is the download directory for the local agent
installation
    [System.String]$downloadsDirectory = $output.DownloadsPath

    #Migrator Pro for Active Directory Agent will download AdminAgent.csv file to
the downloads directory before each job
    #This CSV contains a list of Users to perform actions on
    [System.String]$adminAgentCSVPath = Join-Path -Path $downloadsDirectory -
ChildPath 'AdminAgent.csv'

    #Read Credentials_Password input parameter and convert to a secure string to be
used by a PSCredential object
    $securePassword = $Credentials_Password | ConvertTo-SecureString -AsPlainText
-Force
    #Build the credential using $Credentials_Username and $securePassword
    $credential = New-Object System.Management.Automation.PSCredential($Credentials_
Username, $securePassword)

    #Create a Remote PowerShell Session to the server $DomainController and provide
PSCredential object
    $session = New-PSSession -ComputerName $DomainController -Credential $credential

    #Invoke-Command to ensure the ActiveDirectory modules are imported.
    Invoke-Command -Session $session -ScriptBlock { Import-Module ActiveDirectory }

    #Merge the remote PowerShell Session's ActiveDirectory module to the local
session
    Import-PSSession -Session $session -Module ActiveDirectory -AllowClobber

    #Verify $adminAgentCSVPath exists
    if((Test-Path $adminAgentCSVPath) -eq $false)
    {
        Write-Error "Admin Agent CSV does not exist at path: $adminAgentCSVPath"

        #Different ResultCodes can be used to troubleshoot script errors
        $output.ResultCode = 2
        return ($output)
    }
```

```
    #Read Admin Agent CSV into $users variable
    $users = Import-CSV $adminAgentCSVPath

######## Admin Agent User Script Here ########

    #For each user in the list
    foreach($user in $users)
    {
        #Move the object to the $TargetOU
        Move-ADObject -Identity $user.TargetDN -TargetPath $TargetOU -
Confirm:$false -Verbose
    }

######## Admin Agent User Script Here ########

    #ResultCode of 0 is a success, set and return
    $output.ResultCode = 0
    return ($output)
}
catch
{
    #Generic unexpected ResultCode
    $output.ResultCode = 99

    #Construct generic error message and include Exception message text.
    $errorMessage = $_.Exception.Message
    Write-Error "ERROR: $errorMessage"

    #Return $output object to Migrator Pro for Active Directory Agent for reporting
to Migrator Pro for Active Directory Console
    return ($output)
}
```

Windows 10 Offline Domain Join

Please see the Credential Cache and Offline Domain Join topic for more information.

How to Process GDPR Requests

What is a GDPR Request?

The General Data Protection Regulations (GDPR) is the new European Union (EU) data protection regulations which go into effect May 25th, 2018. Under the GDPR individuals have certain rights to their personal data. They can make requests to exercise those rights to the data controller, and the controller must respond within 1 month. It is expected that the controller will verify the identity of the requestor.

There are four primary types of GDPR requests:

1. **Export** – Request for a copy of all personal data about an individual held by this controller and any related processors. Must be in a commonly accepted portable data format.
2. **Update** – Request to rectify inaccurate personal data.
3. **Delete** – Request to remove all personal data about an individual from our systems. Can be initiated by an individual or by a revocation of consent process. Includes burden of proof. (Ideally follow a Delete with an Export to show no remaining data)
4. **Hold** – Request to halt processing of personal data but not delete that data.

How to handle GDPR Requests for Migrator Pro for Active Directory

When Migrator Pro for Active Directory is installed, the data associated with the application is hosted locally within the client's environment. The client has full control over this data. By default, the user and configuration data is stored in the SQL database called, "DirectorySyncPro_<*date*>". It is assumed the operator has the proper administrative SQL Permissions to execute the following methods outlined.

SQL Tables containing User data:

- [DirectorySyncPro_<Date>].[dbo].[BT_Person]
  Unique Key Look-up Columns:
  [SAMAccountName]
  [TargetSAMAccountName]
  [TargetUserPrincipalName]
  [OriginalSAMAccountName]
  [OriginalUserPrincipalName]
  [UserPrincipalName]
  If user data is used for matching (e.g. SAMAccountName, UserPrincipalName, etc.) then those values will also appear in one of the following columns:
  [MatchValue1]
  [MatchValue2]
  [MatchValue3]
  [MatchValue4]

- [DirectorySyncPro_<Date>].[dbo].[BT_Groups]
  Unique Key Look-up Columns:
  [MatchValue1]
  [MatchValue2]
  [MatchValue3]
  [MatchValue4]

Be aware that data can be mapped to different Internal Fields (table columns) depending on customer specific configuration, so just about any SQL column could theoretically contain user data if so configured. For example, if SAMAccountName has been mapped to Custom001 or to any other Internal Field selectable in the mappings then that field could contain personal data. Therefore this process should be undertaken by someone knowledgeable about the schema and attribute mappings in use. It may also be helpful to work with Support when completing these requests if your administrator is not comfortable with the database.

Where does the Migrator Pro for Active Directory get its user data?

All user data within Migrator Pro for Active Directory is derived from the source Active Directory Forest configured in the product. Therefore, the authoritative source of any user related data stored in Migrator Pro for Active Directory is Active Directory. Any remediation required from a GDPR request should first be remediated in Active Directory or the source feeding Active Directory. Once that user data is updated in the source directory, running a new discovery within the product will update those values as well.

The following sections will provide guidance on fulfilling the 4 primary GDPR request types.

1. **Exports** – Request for a copy of all personal data about an individual held by this controller and any related processors. Must be in a commonly accepted portable data format.

For the purposes of this document, using PowerShell with the SQLPS Module is the recommended method to refine the results of the output. The administrator may export any SQL Query result to a CSV file. Below is an example script to do so. Replace the variables to conform to your environment.

```
Import-Module sqlps
$SQLquery='SELECT * FROM [DirectorySyncPro_<Date>].[dbo].[BT_Person]'
$result=invoke-sqlcmd -query $SQLquery -serverinstance <servername> -database <dbname>
$result |export-csv c:\temp\ExportQueryResults.csv -notypeinformation
```

2. **Updates** – Request to rectify inaccurate personal data.

As previously stated, all user data within Migrator Pro for Active Directory is derived from the source Active Directory Forest configured in the product. Therefore, the authoritative source of user data is Active Directory. Any remediation required from a GDPR request should first be remediated in Active Directory or the source feeding Active Directory and it will be pulled into the product during the next discovery process.

If editing the user data within SQL is still required, using any SQL editor such as SQL Server Management Studio, run an update command against one or more columns for one or more records. Below are examples to accomplish this. Note however, that any new discovery will update the values based on the source Active Directory.

Update multiple columns for a single record:

```
UPDATE [DirectorySyncPro_<Date>].[dbo].[BT_Person]
SET <Column1 Name> = <New Value1>, <Column2 Name> = <New Value2>
WHERE userPrincipalName='<Unique ID>'

UPDATE [DirectorySyncPro_<Date>].[dbo].[BT_Person]
SET <Column1 Name> = <New Value1>, <Column2 Name> = <New Value2>
WHERE userPrincipalName='<Unique ID>'
```

Update multiple columns for multiple records:

```
UPDATE [DirectorySyncPro_<Date>].[dbo].[CMTEUP_Person]
SET <Column1 Name> = <New Value1>, <Column2 Name> = <New Value2>
WHERE DistinguishedName='<Unique ID>' OR DistinguishedName='<Unique ID>'

UPDATE [DirectorySyncPro_<Date>].[dbo].[CMTEUP_PersonADData]
SET <Column1 Name> = <New Value1>, <Column2 Name> = <New Value2>
WHERE userPrincipalName='<Unique ID>' OR userPrincipalName='<Unique ID>'
```

Update multiple columns for multiple records using a list:

```
UPDATE [DirectorySyncPro_<Date>].[dbo].[BT_Person]
SET <Column1 Name> = <New Value1>, <Column2 Name> = <New Value2>
WHERE DistinguishedName IN ('<Unique ID1>', '<Unique ID2>', '<Unique ID3>')

UPDATE [DirectorySyncPro_<Date>].[dbo].[BT_Person]
SET <Column1 Name> = <New Value1>, <Column2 Name> = <New Value2>
```

WHERE userPrincipalName IN ('<*Unique ID1*>', '<*Unique ID2*>', '<*Unique ID3*>')

3. **Deletes** – Request to remove all personal data about an individual from our systems. Can be initiated by an individual or by a revocation of consent process. Includes burden of proof. (Ideally follow a delete with an Export to show no remaining data.)

Using any SQL editor such as SQL Server Management Studio, run a Delete command against one or more records. Below are examples to accomplish this. However, as previously stated, if the user is not deleted in the source Active Directory then during any subsequent new discovery the user will be re-populated into SQL. The only way to truly remove the data is to delete the source user or delete the entire SQL database when it is no longer required.

Delete a single record then verify:

DELETE FROM [DirectorySyncPro_<*Date*>].[dbo].[BT_Person]
WHERE SAMAccountName='<*Unique ID1*>'

SELECT * FROM [DirectorySyncPro_<*Date*>].[dbo].[BT_Person]
WHERE SAMAccountName='<*Unique ID1*>'

DELETE FROM [DirectorySyncPro_<*Date*>].[dbo].[BT_Person]
WHERE userPrincipalName='<*Unique ID1*>'

SELECT * FROM [DirectorySyncPro_<*Date*>].[dbo].[BT_Person]
WHERE userPrincipalName='<*Unique ID1*>'

Delete multiple records then verify:

DELETE FROM [DirectorySyncPro_<*Date*>].[dbo].[BT_Person]
WHERE SAMAccountName='<*Unique ID1*>' OR SAMAccountName='<*Unique ID2*>'

SELECT * FROM [DirectorySyncPro_<*Date*>].[dbo].[BT_Person]
WHERE SAMAccountName='<*Unique ID1*>' OR SAMAccountName='<*Unique ID2*>'

DELETE FROM [DirectorySyncPro_<*Date*>].[dbo].[BT_Person]
WHERE userPrincipalName='<*Unique ID1*>' OR userPrincipalName='<*Unique ID2*>'

SELECT * FROM [DirectorySyncPro_<*Date*>].[dbo].[BT_Person]
WHERE userPrincipalName='<*Unique ID1*>' OR userPrincipalName='<*Unique ID2*>'

Delete multiple records then verify:

DELETE FROM [DirectorySyncPro_<*Date*>].[dbo].[BT_Person]
WHERE SAMAccountName IN ('<*Unique ID1*>', '<*Unique ID2*>', '<*Unique ID3*>')

SELECT * FROM [DirectorySyncPro_<*Date*>].[dbo].[BT_Person]
WHERE SAMAccountName IN ('<*Unique ID1*>', '<*Unique ID2*>', '<*Unique ID3*>')

DELETE FROM [DirectorySyncPro_*<Date>*].[dbo].[BT_Person]
WHERE userPrincipalName IN ('*<Unique ID1>*', '*<Unique ID2>*', '*<Unique ID3>*')

SELECT * FROM [DirectorySyncPro_*<Date>*].[dbo].[BT_Person]
WHERE userPrincipalName IN ('*<Unique ID1>*', '*<Unique ID2>*', '*<Unique ID3>*')

4. **Holds** – Request to halt processing of personal data but not delete that data.

This can also be accomplished using the product interface. Halting a user from processing within Migrator Pro for Active Directory can be achieved using the Exclusion List feature.

About us

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Office 365 management, and cyber security resilience, Quest helps customers solve their next IT challenge now. Around the globe, more than 130,000 companies and 95% of the Fortune 500 count on Quest to deliver proactive management and monitoring for the next enterprise initiative, find the next solution for complex Microsoft challenges and stay ahead of the next threat. Quest Software. Where next meets now. For more information, visit www.quest.com.

Technical support resources

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

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

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