Migrating RM Unify Provisioning

Transition to a new Active Directory

# Introduction

RM Unify can currently provision users from three different sources:

* An Active Directory (AD) in a school (standard or CC4)
* CSV files
* MIS

This document details the process of linking existing RM Unify accounts to users in a new Active Directory. If you have a CC4 network then this is not the right document for you. Please see “Migrating RM Unify Provisioning – Transition to a new CC4 Active Directory”.

# Overview

Please take the following steps in order to link users in their new Active Directory to their existing RM Unify accounts.

1. Download a CSV of users from RM Unify
2. Add AD name to the CSV
3. Uninstall RM Unify AD Sync Service if this is currently installed
4. Run the migration script to import PersonID and UnifyEmailAddress values to your AD
5. Install and configure the latest version of RM Unify AD Sync
6. Check an AD user is linked to their existing account
7. Change AD user passwords

# Download a CSV of users from RM Unify

1. Logon to RM Unify as a user with admin rights.
2. Click Management Console>Sync users from CSV
3. Click on “Generate a CSV of all my RM Unify users”

# Add AD username to the CSV

In summary, the ‘new’ AD accounts need to be seeded with the identifiers of the old AD accounts that were used to provision into RM Unify

This is achieved by writing an extra user attribute to your AD, containing the RM Unify PersonID for the user (first column in the spreadsheet you just downloaded). If it exists, we also import the UnifyEmailAddress value for each user into the “mail” AD attribute to ensure your AD users are linked to the same, named email account. We provide a PowerShell migration script to help with this (see step 4).

To prepare for running the PowerShell script, you will need to add the AD account name for each user to the CSV file you downloaded in step 1:

1. Open the downloaded CSV file “EstablishmentUsers” in a spreadsheet
2. In column M of the CSV, write “ADName” (without quotes) in row 1.
3. For each subsequent row, write the AD Name (ie. Name attribute) corresponding to the RM Unify user.

The AD Name of your users is displayed under the Name column showing in Active Directory Users and Computers. See the screenshot below.


4. Save the file as a .CSV format

# Uninstall RM Unify AD Sync if currently installed

1. On your AD Sync server, uninstall RM Unify AD Sync from Add/Remove Programs (or Uninstall a Program). You do not need to uninstall RM Password Filter.
2. Rename the residual folder(s) from:
*C:\Program Files\RM\RM Unify AD Sync or C:\Program Files\RM\RM Unify AD Sync Servi*ce
to:
*RM Unify AD SyncOLD*.

If the AD Sync server is using a 64-bit operating system you will find the residual folder in the location: *C:\Program Files (x86)\RM*

1. It is important to rename the residual folder to ensure the new installation of RM Unify AD Sync in Step 5 creates a new database.

# Preview and run migration script

The migration script will add the RM Unify PersonID and UnifyEmailAddress, if it exists, to your AD.

You will need to choose an unused AD attribute that can be populated with the RM Unify PersonID value. The same attribute must be used for all users and should not be one that is likely to be used in future. We recommend the “otherpager” attribute, though you can pick an alternative.

If a value in the “UnifyEmailAddress” column exists in the spreadsheet, the script will also populate the AD “mail” attribute with the values from the “UnifyEmailAddress” column.

To run the script, you will need to logged in as a domain administrator to either a domain controller with Windows Server 2008 r2 or better, or a domain-joined workstation with the [Remote Server Administration Tools](http://www.google.co.uk/search?q=remote+server+administration+tools) installed (these require Windows 7 or better).

1. Create a new folder c:\ADSyncMigration on the computer
2. Save the script and your CSV file to c:\ADSyncMigration
3. Open a command prompt and type “powershell get-executionpolicy”.
4. Make a note of the policy in place eg. RemoteSigned
5. Temporarily change the policy by typing “powershell -ExecutionPolicy unrestricted”.
6. Type “cd C:\ADSyncMigration\” and press Enter to change the directory location
7. Run the following command to check the recommended “otherpager” attribute is unused by all users:

$checkattribute='otherpager'
get-aduser -filter {$checkattribute -ne "$null"} -Properties name, $checkattribute |select name, @{N="$checkattribute";E={$\_.$checkattribute -join ","}} |export-csv c:\adsyncmigration\$checkattribute.txt
8. In Windows Explorer, open the file c:\ADSyncMigration\otherpager.txt. It will list all users, if any, that already have a value in the otherpager attribute.
9. If one or more users are listed in otherpager.txt then **stop** this process and do not proceed to the next step. Please contact RM Cloud Support for further assistance. They will help you check whether to use otherpager or an alternative attribute.
10. If no users are listed in otherpager.txt then proceed to the next step
11. Run the following command to check if the default “mail” attribute is already in use by some or all users:

get-aduser -filter {mail -ne "$null"} -properties name, mail |select name, mail |export-csv c:\ADSyncMigration\mailaddresses.txt
12. In Windows Explorer, open the file c:\ADSyncMigration\mailaddresses.txt. It will list all users, if any, that already have an email address populated in the ‘mail’ attribute.
13. If the mailaddresses.txt file contains users then **stop** this process and do not proceed to the next step. Please consult RM Cloud Support team for further assistance. They will help you make further checks on whether the “mail” attribute or another attribute should be populated with the UnifyEmailAddress values.
14. If the mailaddresses.txt file does not contain any users, proceed with the next step.
15. Run the following command to give you a preview of what the migration script will do. No user changes will be made at this point:

.\Set-RMUnifyPersonID.ps1 EstablishmentUsers.csv -ADAttribute otherPager –WhatIf

Note: this command assumes you will use the recommended otherPager attribute to store RM Unify PersonID. Modify the command above if you intend to use an attribute other than otherPager.

1. The script will output a summary on screen and save details to the file c:\ADSyncMigration\RMUnifyPersonID.log.
2. In Windows Explorer, open c:\ADSyncMigration\RMUnifyPersonID.log file
3. Carefully review all output in the log file, paying attention to the errors and warnings. Make changes as necessary to resolve errors and warnings.
4. If you made changes to resolve errors and/or warnings, re-run the command in Step 15 and review the RMUnifyPersonID.log file again.
5. Once you are happy with the preview output, run the script again without the -WhatIf option:

.\Set-RMUnifyPersonID.ps1 EstablishmentUsers.csv -ADAttribute otherPager

Note: this command assumes you will use the recommended otherPager attribute to store RM Unify PersonID. Modify the command above if you intend to use an attribute other than otherPager.

By default, the script will not overwrite any existing values in the attributes it modifies. If you would like it to, add the -Force attribute to the command-line eg.

.\Set-RMUnifyPersonID.ps1 EstablishmentUsers.csv -ADAttribute otherPager -force

1. The script will output a summary on screen and save details to the file c:\ADSyncMigration\RMUnifyPersonID.log.
2. In Windows Explorer, open c:\ADSyncMigration\RMUnifyPersonID.log file
3. Review the output in the log file.
4. Change the Powershell execution policy back to its original setting by typing “powershell -ExecutionPolicy xxxxx”, where xxxx is the policy you recorded in Step 3.

# Install and configure RM Unify AD Sync Service

1. Download the latest version of RM Unify AD Sync from the RM Unify Management Console
2. Follow the instructions in the RM Unify AD Sync Release Note to install the software and complete the RM Unify AD Sync – InstallShield Wizard.
3. Open the RM Unify AD Sync Configuration Tool for the first time and enter Web Proxy Settings if required. **Do not** register your RM Unify establishment yet.
4. Close the RM Unify AD Sync Configuration Tool
5. Using Notepad, open: C:\Program Files (x86)\RM\RM Unify AD Sync Service\RM.Networks.IdentityManagement.config

Find the line that reads:
<add key="IdentityGuidSource" value="rmCom2000-UsrMgr-uPN" />

Modify rmCom2000-UsrMgr-uPN to the AD attribute you chose to use in Step 15 eg.

<add key="IdentityGuidSource" value="otherpager" />

1. Click File, Save and then close the file
2. Re-open the RM Unify AD Sync Configuration Tool
3. Register your RM Unify establishment as per the RM Unify AD Sync Release Note
4. Create AD filters as required. For each AD filter, set the email attribute to “mail” if the Powershell script above imported the UnifyEmailAddress values into your AD. This will ensure your AD users will be linked to their existing RM Unify provisioned email account.
5. Create role mappings as required
6. Wait up to an hour for users to show as provisioned under each AD filter

On first run the RM Unify AD Sync Service will find all users matching an AD filter and:

* Any user in your AD that has an RM Unify PersonID in the specified attribute will be linked to their existing RM Unify account.
* Any user in your AD that does not have an RM Unify PersonID in the specified attribute will be created as a new user in RM Unify.
* Any user in RM Unify that is not associated with an AD user will continue to exist, but will not be updated in future. RM Cloud Support can assist you with instructions on how to delete these users at a later date if required.

# 6. Check an example AD user is linked to their existing RM Unify account

1. Change the AD password of a user that had an existing RM Unify account
2. Wait 5 minutes
3. Confirm the user can sign into RM Unify with their existing Unify username and new AD password, and get access to their existing RM Unify account and data including any linked apps such as Microsoft Office 365.

# 7. Change AD user passwords

1. Change the AD password of all users with an RM Unify account to ensure their AD password and RM Unify password are in synchronisation.
2. All RM Unify users provisioned from your AD will now be able to sign into RM Unify using their existing RM Unify username and their current AD password.