

Release Note

RM Unify AD Sync v4 for CC4

Contents

About this Release Note	3
About RM Unify AD Sync	3
What it does	3
Components	3
Example installations	4
Some important considerations	5
Data protection	5
Initial password synchronisation	5
Requirements	6
RM Unify AD Sync Service requirements	6
RM Unify Password Filter requirements	6
Installation scenarios for new installs and upgrades	7
Pre-installation tasks	7
A. Reboot your domain controllers	7
B. Choose your AD Sync server	7
C. Ensure prerequisite software is installed	8
D. Back up your servers	8
E. Create CC4 security groups for users and admins	8
F. Gather the required network information	9
Installing RM Unify AD Sync	10
1. Install the RM Unify AD Sync Service	10
2. Run the configuration tool for the first time	12
3. Register your school network with RM Unify	13
4. Configure an establishment	15
5. Install RM Unify Password Filter	21
6. Force a password change at next logon	22
Changing your RM Unify AD Sync configuration	24
Appendix I: Identifying your current version of RM Unify AD Sync	26
Appendix II: Identifying 32- and 64-bit Windows servers	27
Windows Server 2008	27
Windows Server 2008 Server Core Edition	27
Windows Server 2012 and later	27
Appendix III: Upgrading from RM Unify AD Sync v2 or v3	28
Appendix IV: Installing prerequisites	31
Installing .NET Framework version 3.5 SP1	31
Installing Microsoft Visual C++ 2010 Redistributable	32
Appendix V: Default CC4 user role mappings	34
Appendix VI: Alternative mapping types	35
Profile Path	35

Organisational Unit	35
Group Membership	36

About this Release Note

This Release Note is written for network administrators who are installing and setting up RM Unify AD Sync v4 on a Community Connect 4® (CC4) network for the first time, or upgrading an existing installation of RM Unify AD Sync.

Do not use this Release Note if you want to install or upgrade RM Unify AD Sync on a standard Windows Server network without Community Connect network management tools, use *Release Note: RM Unify AD Sync for Windows Server networks* instead.

About RM Unify AD Sync

What it does

RM Unify is a single sign-on system, application library and management system for Cloud services.

RM Unify AD Sync synchronises your local school network user accounts with RM Unify, so that students and school staff can access 'cloud' services with the same username and password that they use on the local school computers.

The RM Unify AD Sync Service monitors changes in the local Microsoft® Active Directory (AD), including password changes. When students, teachers or other users join your school, their network accounts can be automatically synchronised to RM Unify. If specific attributes in a network account then change, for example a member of staff changes their surname, these changes will be synchronised to RM Unify via RM Unify AD Sync. When the time comes to delete user accounts, these will automatically be removed from RM Unify.

In order to use RM Unify AD Sync, your school must have an appropriate licence, e.g. an RM Unify Premium licence, or an RM SafetyNet User-Based Filtering subscription.

Components

You need to install two components to the product. These can be installed in different ways.

RM Unify AD Sync Service

This service is installed on just one server and scans the AD for changes to user accounts. This information, together with any password changes, is used to update its user database, which is synchronised to RM Unify.

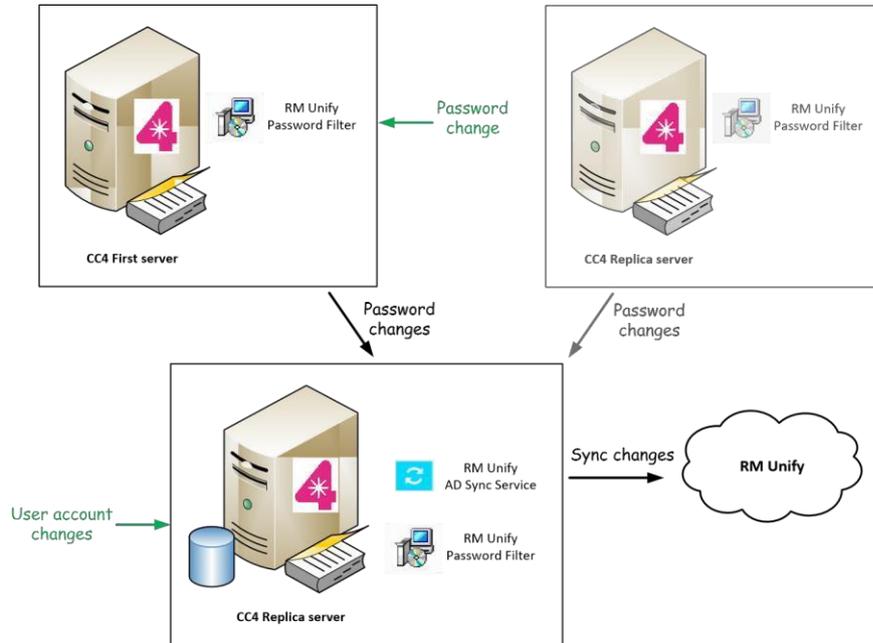
RM Unify Password Filter

This must be installed on all domain controllers (DCs) on the network, to capture any changes in users' passwords.

Example installations

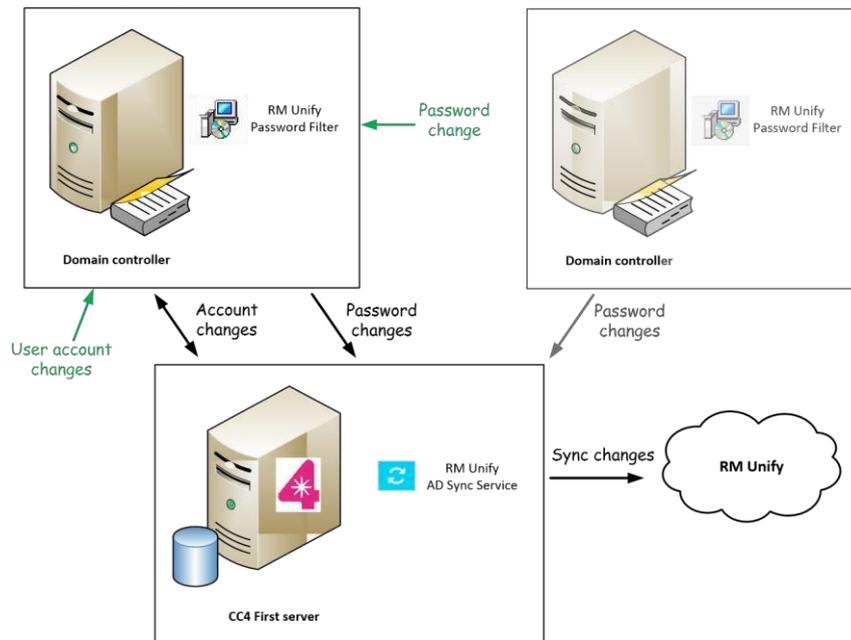
On a standard CC4 multi-server network, we recommend that you install RM Unify AD Sync Service on a CC4 Replica DC. RM Unify Password Filter is installed on all DCs including the First server.

Standard CC4 network



(If you have a single-server network, all components are installed on the CC4 First server).

CC4 Matrix environment



In a CC4 Matrix environment – for example a network that has moved to CC4 via TEN (Tools for Existing Networks) – we recommend that you

install the RM Unify AD Sync Service on the CC4 First server. RM Unify Password Filter is installed on all domain controllers – which does **not** include the CC4 First server in a CC4 Matrix environment.

Some important considerations

Data protection

The RM Unify AD Sync Service will connect to RM Unify from your local network and will transfer the following identity information to RM Unify:

- Active Directory objectGUID
- User credentials (Username and RSA-encrypted password)
- Name details (First name, Surname and Display Name) •
Role (Student, Teacher, Non-Teacher, Governor, Other)
- User account status.

Optionally, the following identity information can be transferred to RM Unify:

- Year of entry (for student users)
- Email address.

RM Unify is hosted in the European Economic Area (EEA).

Please ensure that this data transfer is agreed with your local school Data Controller (usually the Head teacher).

Initial password synchronisation

To ensure that your users have synchronised passwords between the local network and RM Unify, after the installation you will need to force all your users to change their network passwords. This can be done by setting all user accounts to require a password change at the next logon.

This is because RM Unify AD Sync Service can only detect a user's password when it is changed, as Microsoft Active Directory stores all passwords in a non-reversible encrypted form. A user will not be able to log onto RM Unify until they have changed their password on the local network and this has been automatically synchronised to RM Unify.

If you are upgrading RM Unify AD Sync, it is not necessary to force users to change their passwords.

Requirements

Both components of RM Unify AD Sync have several important prerequisites. Although many servers will already meet these requirements, you must verify that all these are present before installing or upgrading RM Unify AD Sync.

For instructions, see 'Appendix IV: Installing prerequisites'.

Note: If you do need to install prerequisites, please note that some of them require a **server reboot**. Please allow adequate time!

RM Unify AD Sync Service requirements

RM Unify AD Sync Service can be installed on a server that meets the following requirements:

- Operating system: Windows Server 2012 R2, WS 2016 or WS 2019

Note: Installation of the RM Unify AD Sync Service is not supported on any version of Windows Server Core.

- .NET Framework v3.5 SP1
For instructions to check for its presence, or install it, see 'Installing .NET Framework version 3.5 SP1'.
- To reduce network traffic we recommend that you install the RM Unify AD Sync Service on a domain controller, except in CC4 Matrix environments.

RM Unify Password Filter requirements

RM Unify Password Filter should be installed on all AD domain controllers on your network. Each DC must meet the following requirements:

- Operating system: Windows Server (WS) 2008, WS 2008 R2 Server Core, WS 2012, WS 2012 R2, WS 2012 Server Core, WS 2016 or WS 2019
- .NET Framework v3.5 SP1
For instructions to check for its presence or install it, see 'Installing .NET Framework version 3.5 SP1'.
- The appropriate version of **Microsoft Visual C++ 2010 Redistributable Package** for your server:

WS 2008 32-bit
Microsoft Visual C++ 2010 Redistributable Package (x86)

WS 2008 64-bit, WS 2008 R2 64-bit, WS 2012, WS 2012 R2, WS 2016, WS 2019
Microsoft Visual C++ 2010 Redistributable Package (x64)

For instructions check for its presence or install it, see 'Appendix IV: Installing prerequisites'.

Installation scenarios for new installs and upgrades

The steps required to prepare for and complete the installation of RM Unify AD Sync v4 depend on whether you need to:

- Install RM Unify AD Sync for a new RM Unify establishment. Please continue with the rest of this document.
- Upgrade from RM Unify AD Sync v2 or v3.
There is no in-place upgrade from v2 or v3 to v4. Please see 'Appendix III: Upgrading from RM Unify AD Sync v2 or v3.'

If you aren't sure what version of RM Unify AD Sync is currently installed, see 'Appendix I: Identifying your current version of RM Unify AD Sync' for instructions.

Pre-installation tasks

Check which of the following tasks applies to you and complete them in sequence.

A. Reboot your domain controllers

We strongly recommend that you reboot your CC4 First server and then each of your domain controllers, one after the other. This will ensure that any pending software updates and configuration changes take place before you install RM Unify AD Sync, avoiding simultaneous updates that could interfere with the installation.

B. Choose your AD Sync server

We do not recommend installing RM Unify AD Sync on your CC4 First server, unless it is the only server on your network or unless you have a CC4 Matrix environment. Otherwise, try to balance the traffic across your network by installing it on a Replica DC. You can also install it on a server that is not a DC, for example a member server, but this will increase the network traffic required for communication with Active Directory.

Ensure prerequisite software is installed

Find out in advance whether your servers meet all the 'Requirements' on page 6 before the day of installation. Refer to the appropriate instructions to see whether a server reboot is required and also to get an idea of the time required. Ensure all the prerequisite software is installed before you install or upgrade RM Unify AD Sync.

D. Back up your servers

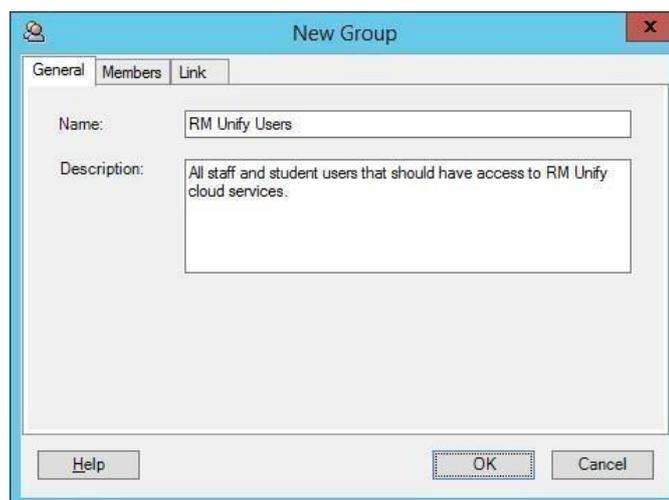
RM Unify AD Sync will make changes to your server and Active Directory. Ensure that before installing this software you have an up-to-date backup of all your network servers, including System State.

E. Create CC4 security groups for users and admins

Follow the instructions below if you want to create Active Directory (AD) groups to control which users get access to RM Unify. These will provide useful filters if the Organisational Unit (OU) containers in your AD contain different types of user, or users from different establishments.

For a single-site installation, create an RM Unify Users group and an RM Unify Admins group. For a multi-site installation, create two groups for each school (e.g. for a school with site code ABC, 'RM Unify UsersABC' and 'RM Unify Admins-ABC').

1. Log on to the RM Management Console as a System Administrator.
2. In the left-hand pane, right-click Security Groups and choose New Group.
3. On the General tab, enter the name **RM Unify Users** and enter a suitable description. Do not add any members at this stage.



4. Click OK to add the group.
5. Repeat steps 2–4 to create a group called **RM Unify Admins**.

F. Gather the required network information

If you are making a fresh installation of RM Unify AD Sync you will need to have information about your network, either to enter manually or to confirm values that have been detected automatically.

Make a note of the following:

- The AD Domain Controller server name that will be used for identifying user changes.

Where RM Unify AD Sync is being installed on a DC, use the local server name.

- Your proxy server or ISA server address and port number (if applicable).

Note: If your proxy server requires authentication (for example, a Microsoft ISA server), you will need to add an exception to ensure that your RM Unify AD Sync server is able to access <https://api.platform.rmunify.com/> anonymously. For instructions, please refer to the supplier's documentation for your proxy server.

- The name of the CC4 group or groups that will be used to control access to RM Unify, created in task G above ('RM Unify Users').
- If you have a multi-site network that includes more than one establishment, you will need to provide details of the AD Organisational Units on which user searches will be based.

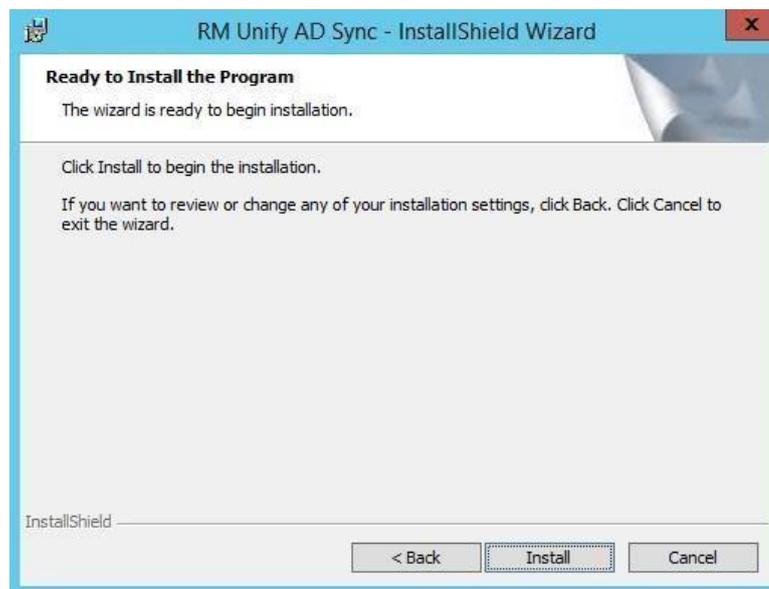
Installing RM Unify AD Sync

If you are upgrading from RM Unify AD Sync **v2** or **v3**, **do not** follow this section on installing the RM Unify AD Sync service. Please use the instructions in 'Appendix III: Upgrading from RM Unify AD Sync v2 or v3'.

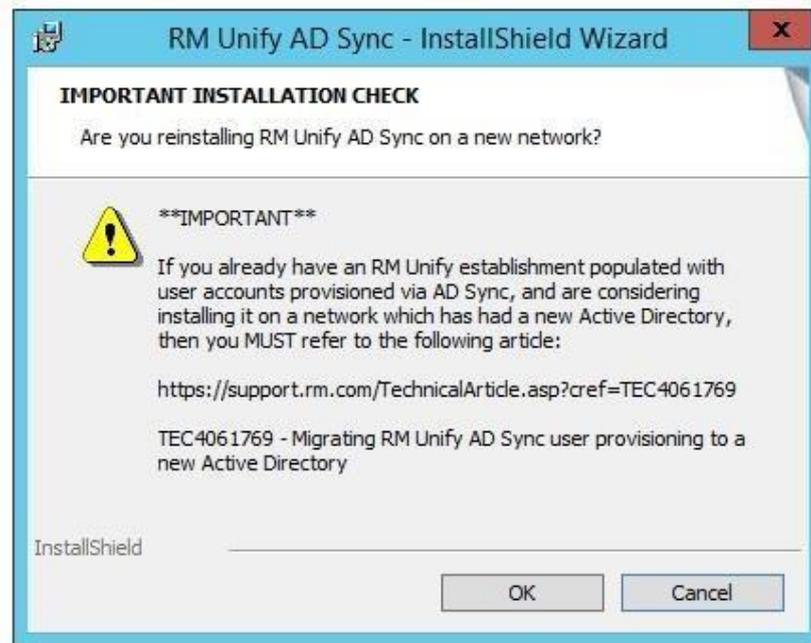
1. Install the RM Unify AD Sync Service

Please ensure you have completed all the 'Pre-installation tasks' that apply to you.

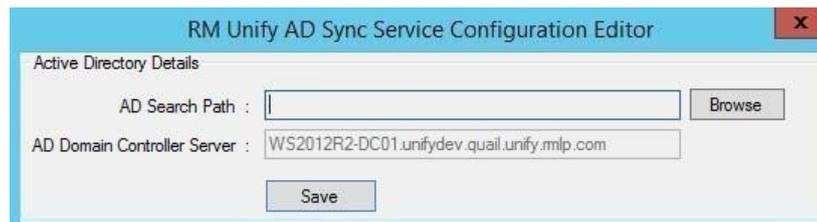
1. At the server you have chosen as the RM Unify AD Sync server, log on as a user who is a member of the Domain Admins and builtin Administrators groups (not as a CC4 system administrator).
2. Browse to the location where you extracted the files from the RM_Unify_AD_Sync_v4.zip download file. If the extracted files are not on this server, copy them to a convenient local folder.
3. Double-click the file **RM Unify AD Sync.msi** to launch the RM Unify Sync Service InstallShield Wizard.
4. At the Welcome screen, click Next.
5. Accept the Licence Agreement and click Next.



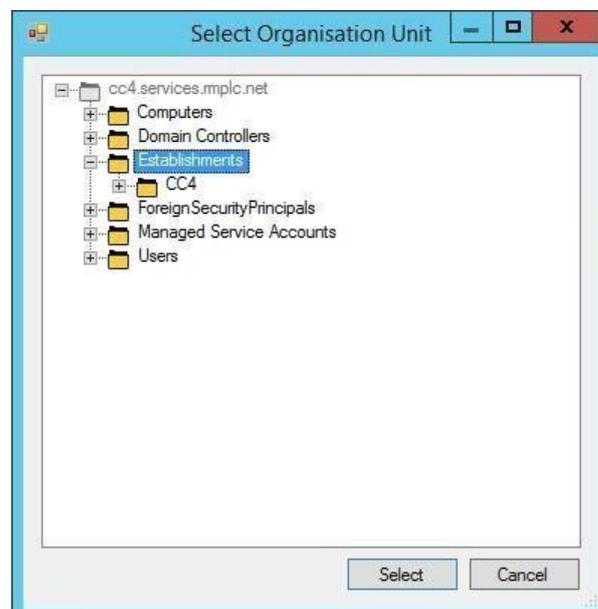
6. Click Install
7. At the Important Installation Check screen, read the message to confirm it does not apply to your installation and click OK



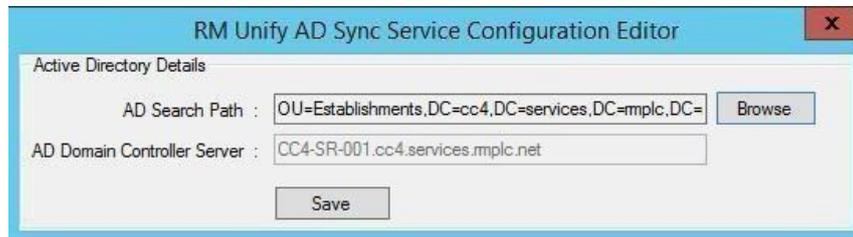
8. The Configuration Editor window is displayed.



9. You need to enter the base Organisational Unit that includes all the school network users who need accounts in RM Unify. If your users are spread across OUs which are non-hierarchical, you can select one of the OUs at this stage in order to proceed. It will be possible to configure the AD Sync filters at a later stage in order to include all your user OUs. Click Browse and then select the appropriate OU:



10. Click Select and then Save



11. When the installation is complete, click Finish.

The RM Unify AD Sync Service has now been installed and the identitiesyncservice user account is present in AD.

2. Run the configuration tool for the first time

When you run the configuration tool for the first time, it will create the RM Unify AD Sync database and start the RM Unify AD Sync Service.

1. From the Windows Start menu choose RM, RM Unify AD Sync, RM Unify AD Sync Configuration Tool. An RM Unify AD Sync Configuration Editor window is displayed.
2. In the 'Initial configuration' window, enter your proxy server details if required.

Note: If you use a transparent proxy (such as SmoothWall®), it may need to be configured so that a non-transparent version is available for use with the RM Unify AD Sync Service. For instructions, please refer to your proxy documentation.

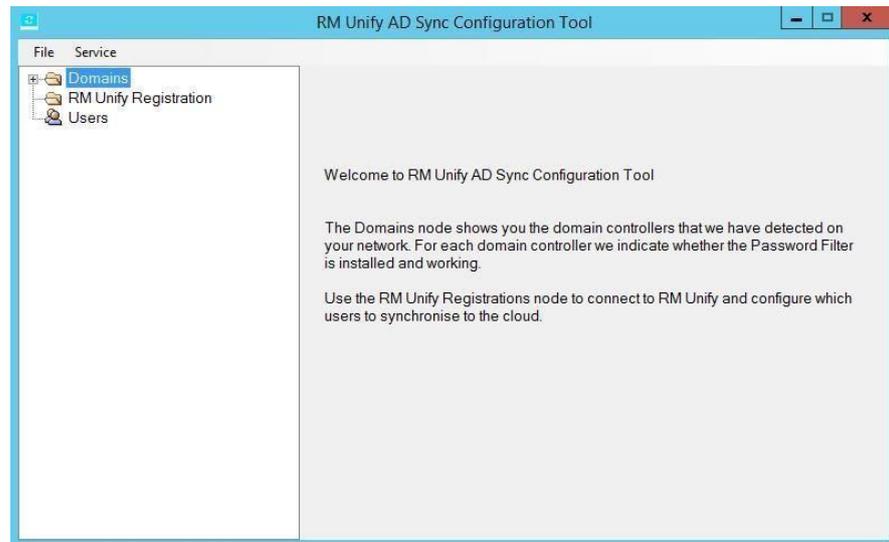
3. Click OK to start the RM Unify AD Sync Service. A message is displayed while it configures the database (this normally takes up a



minute).

Note: If the database configuration is taking excessive time, check the log files (in the LogFiles folder under the installation folder) for any error messages.

When the database configuration is complete, the RM Unify AD Sync Configuration Tool is displayed.



4. Browse to the location of the `rm_unify_adsync_settls.exe` file, right click and select Open.
5. Once the update has completed, the command window will report "Service started", and you may then close the command window.

Leave the RM Unify AD Sync Configuration Tool open while you continue with the next steps.

3. Register your school network with RM Unify

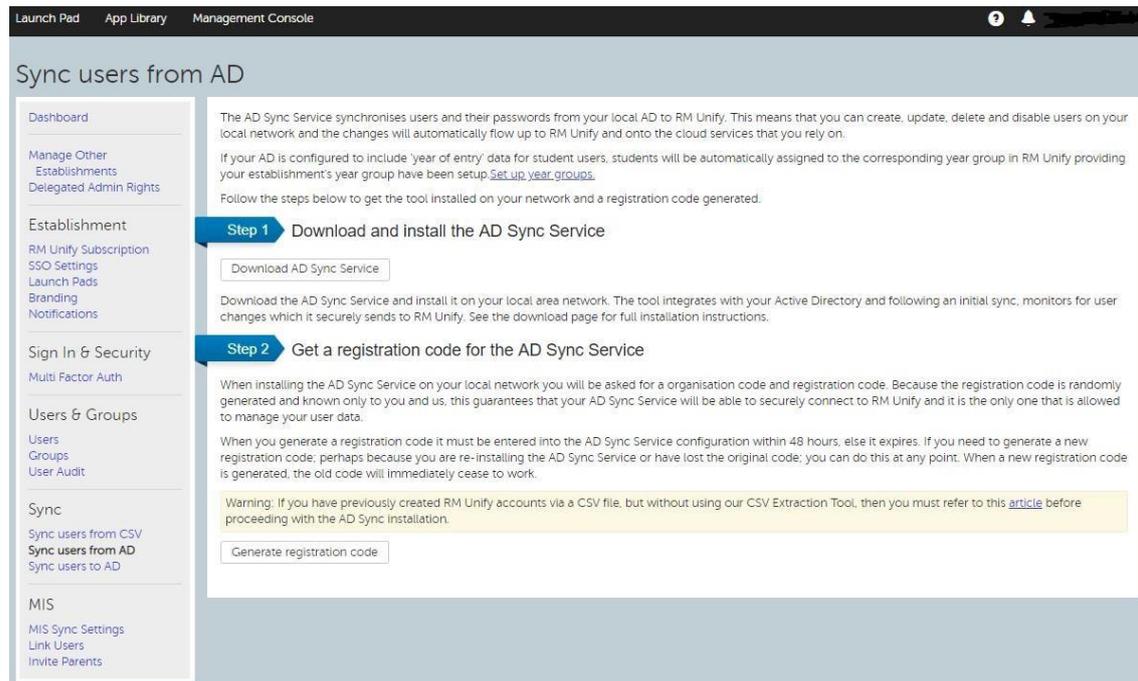
RM Unify provides a registration process that allows you to connect your instance of RM Unify AD Sync to the RM Unify Provisioning service.

► To register your RM Unify AD Sync service with the RM Unify service

1. Log on to RM Unify as an RM Unify Administrator user.

Note If you are configuring AD Sync for a multi-site AD (where several school establishments share the same AD), log in as the RM Unify administrator for the parent establishment. Your parent establishment will have been created by RM and is used to administer your cluster of schools. We will advise you of the parent establishment details when we send you the sign in credentials for all of your RM Unify establishments. Please contact RM Cloud Support if you are not sure which establishment is your parent.

2. In the top menu, select Management Console.
3. In the left pane, click 'Sync users from AD'.

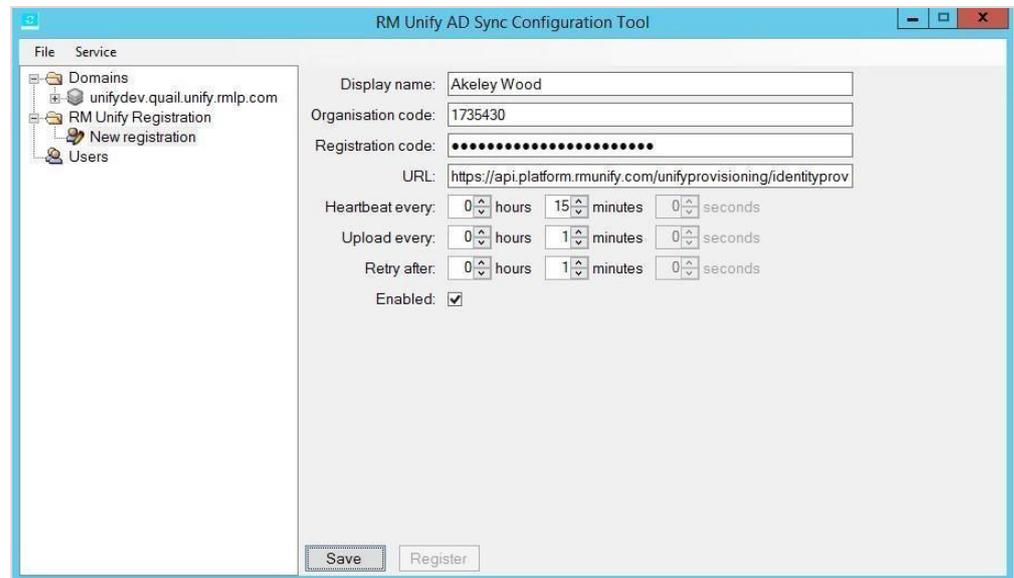


4. Click Generate New Registration Code (new installations) or Change Key (upgrades).
A registration code is displayed, with the format
XXXXX-XXXXX-XXXXX-XXXXX
where X is a letter or number.



5. You will need to enter this organisation code and your registration code in the AD Sync Configuration Tool, as follows.
Leave this window open, so you can copy and paste the values.
Alternatively, make a note of both codes.
6. Log on to your RM Unify AD Sync server as a domain Administrator (not a CC4 system administrator).
7. Return to the RM Unify AD Sync Configuration Tool.
 - In the left-hand pane of the configuration tool, select 'RM Unify registrations', right-click and choose 'New registration'.
8. Enter the required values for registration:
 - Enter a Display name to identify this registration.
We recommend using the organisation's display name.

- Enter your Organisation code and the Registration code including dashes.
You can copy and paste these from RM Unify if the window is still open.



Note: If you have a multi-site installation where several school establishments share the same AD, you only need to register once, using the parent establishment. Once that has been successfully registered, this tool will automatically display all child schools with Premium subscriptions that are linked to the parent.

9. Ensure the Enabled check box is ticked; then click Save and Register.
10. At the 'successful registration' message, click OK.
(If registration was not successful, check the log files for any error messages. You can find these in LogFiles under the installation folder).

When the registration process is complete, your establishment is displayed (and any child schools if applicable) in the tree under the new RM Unify registration.

The next task is to configure your establishment(s).

4. Configure an establishment

There are three configuration settings for your establishment:

- AD filters - each establishment can configure one or more AD filters to specify which users should be uploaded to RM Unify. You may find it helpful to start with two filters, one for RM Unify Users and one for RM Unify Admins.

Each filter consists of a container in the Active Directory and an optional control group.

- If no group is specified, all users in the container will be uploaded to RM Unify.
- If a group is specified – e.g. RM Unify Users, if you are registering a single site – only those users that are in both the container and the group will be uploaded.

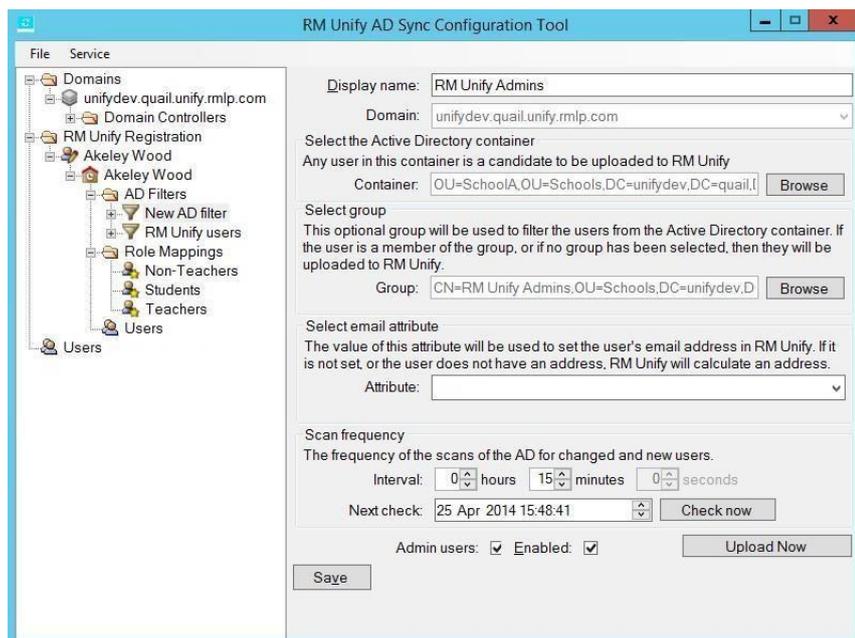
Note: As well as individual users, you can also add groups of users to the control group.

- Role mappings - each establishment also needs a set of role mappings to specify the role of each user in RM Unify. If a user is not assigned any role in RM Unify they will not be uploaded.
- Year of entry - if the 'Year of Entry' used by your establishment is not the year that the student entered the education system as a Year 1 student, then this can cause third-party applications to assign users to the wrong year group. RM Unify AD Sync lets you apply a year of entry offset to avoid such issues.

These settings are configured in the RM Unify AD Sync Configuration Tool.

► **To configure an establishment**

1. In the left-hand tree, select the establishment you want to configure.
2. In the right-hand pane, confirm that the Enabled check box is ticked and click Save.
3. In the left-hand tree, right-click the establishment and choose 'New AD filter'.



4. Configure the values as follows, to specify a set of required users:

-
- Enter a Display name to identify this AD filter. ○ Under 'Select the Active Directory container', enter the distinguished name of the AD OU that contains the users. Alternatively, click the Browse button to locate and select the container you require.
 - Under 'Select group', click Browse to locate and select the group that contains the users, e.g. RM Unify Users.

You created this group in pre-installation task E (see page 8). If no group is required, leave the group text box blank.

- RM Unify can be linked to (federated with) Office 365 and/or G Suite for Education and so if you want to manage your users' email addresses from AD, then under 'Select email attribute', select or enter the name of the source attribute (e.g. 'mail').

Note: By configuring the 'Select mail attribute' value in the Configuration Tool, you are instructing RM Unify to use the email address stored in that attribute. If your AD contains an incorrect email address for a user, that user will not be able to sign in to their Office 365 or G Suite account(s).

If you don't want to configure the 'Select mail attribute' setting, leave it blank. RM Unify will then provision your Office 365 or G Suite email address using the format:

<AD account name>@<cloud email domain>.

-
- If these users should be admin users in RM Unify, tick the 'Admin users' check box.

Note: All admin users must also be assigned to a role, using role mappings.

-
5. When you have finished, click Save.
 6. Repeat steps 3–5 to add additional AD filters as required, to specify all the users that must be uploaded.
A user may match more than one AD filter (see following Note).
 7. Verify that your AD filters are listed in the appropriate order.

Note Users are uploaded using the first AD filter they match (provided they have been mapped to an RM Unify role in the establishment). Filters are applied in their list order. The list order is applied across the establishment.

If you need to change the order of any AD filters, click the AD Filters node of the establishment and use the up/down buttons to re-order the filters as required.

The next step is to configure appropriate User Role Mapping rules for your network. You can enable a set of default mapping rules and also add, edit and delete mapping rules as required.

About User Role Mappings

RM Unify supports five user roles for automated provisioning:

- Students
- Teaching Staff
- Non-Teaching Staff
- Governor
- Other

CC4 networks support additional user types, for example System Administrators and Associates. You can map multiple local user types to a single RM Unify role. For example, you might choose to map the CC4 Associate user type to the RM Unify Non-Teaching Staff role, instead of using the default mapping to 'Other' (see 'Appendix VI: Alternative mapping types').

RM Unify AD Sync provides three methods to map the user accounts in your network to RM Unify user roles. The three methods are:

- profile path
- organisational unit
- group membership

Using profile path, users are mapped to RM Unify roles by looking for the Windows share name string in the user's profile path. This works well for CC4 networks using specific share names for different user types (for example, 'RMStudentProfiles').

CC4 UEV (User Environment Virtualisation), does not use profile paths so you should create mappings based on organisational unit or group membership instead. Please see 'Appendix VI: Alternative mapping types' for your options.

8. If your CC4 network uses profile paths and you want to use the default CC4 profile path role mappings, select the establishment in the lefthand tree, right-click and choose 'Add default CC4 role mappings'. The default CC4 role mappings are added. You can view them by expanding the Role Mappings node.

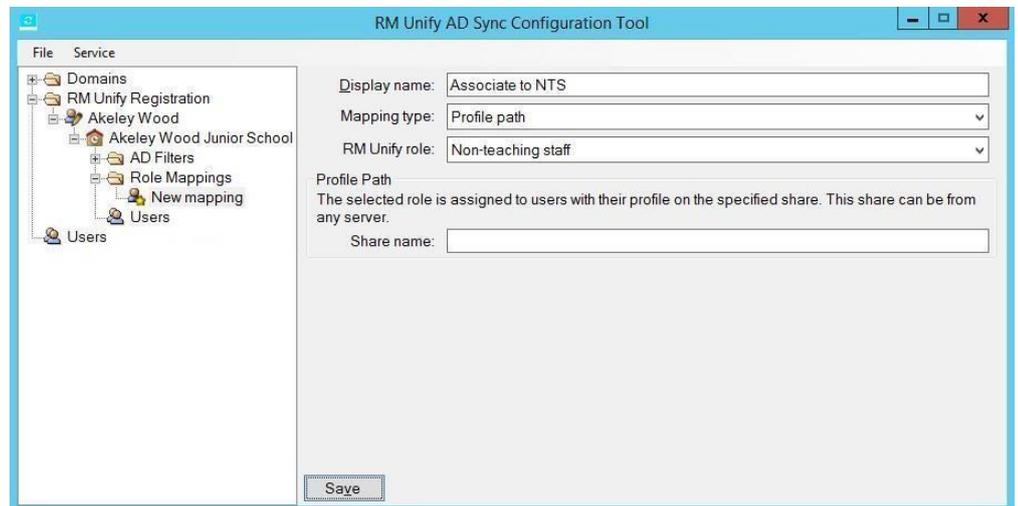
Users are uploaded automatically the next time the AD is checked.

Note: The initial scan of AD, population of the local AD Sync database and upload of user data can take up to 45 mins (based on 1500 users). Subsequent updates are faster, with password updates being sent every minute.

The default mappings may be all you need.

If you need to edit a mapping, select it in the left-hand tree, and then edit the settings as required in the right-hand pane. You can even change the type of mapping if required; for details see 'Appendix VI: Alternative mapping types'.

9. If your network is CC4 UEV, or you need to add a mapping rule, select the establishment in the left-hand tree, right-click and choose 'New role mapping'.



Configure the mapping rule as follows:

- **Display name:** Enter a name to identify this mapping.
- **Mapping type:** From the drop-down list, choose the mapping method to use (see 'Appendix VI: Alternative mapping types' for your options)
- **RM Unify role:** From the drop-down list, choose the role you are mapping to.
- Supply any additional information required for your chosen Mapping type. For Group membership, click Browse and select the desired security group.

When you have finished, click Save.

10. Repeat step 9 to add additional user role mapping rules as required. A user may match more than one mapping rule (see Note below).
11. Verify that your mapping rules are listed in the appropriate order.

Note: Users are mapped by the first mapping rule they match. Mapping rules are applied in their list order. The list order is applied across the establishment.

If you need to change the order of any mapping rules, click the 'Role mappings' node of the establishment and use the up/down buttons to re-order the rules as required.

12. If you have other establishments to configure, repeat steps 1–11 as required.

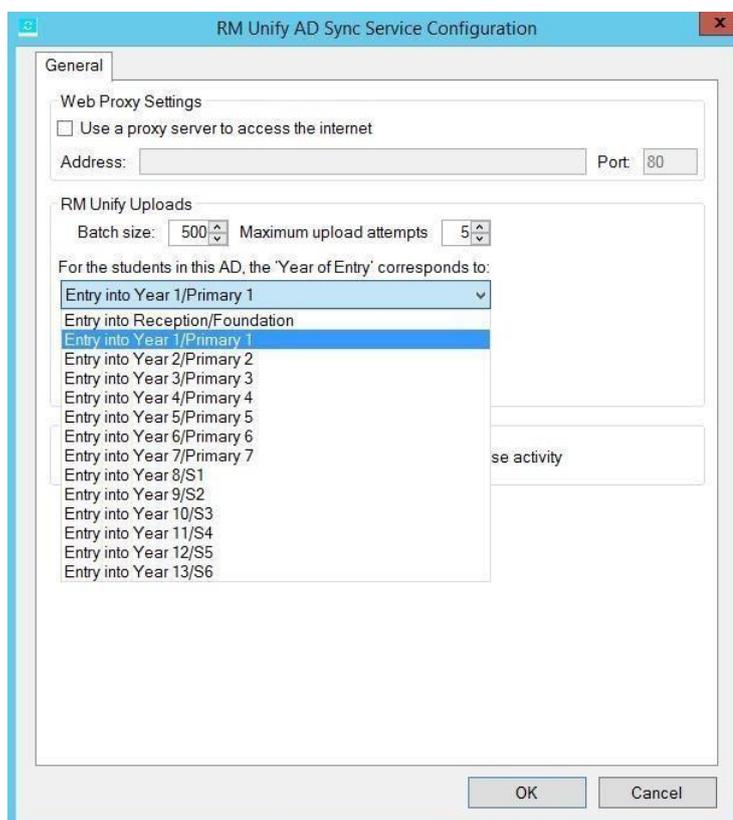
The final step in configuring your establishment is to apply a Year of Entry offset if required.

Year of Entry is also mapped automatically from CC4, and you can use this property to specify a year-appropriate Launch Pad and RM Unify Apps selection for student users. However different schools start at different points in a student's educational career – Year 1, Year 5, Year 7, Year 12, etc. If the Year of Entry used by your establishment is not the year that the student entered the education system as a Year 1 student, you can apply an offset to correct for this, as follows:

13. From the Service menu choose Settings.

The RM Unify AD Sync Service Configuration window is displayed.

14. Under RM Unify Uploads, click the 'For students in this AD, the 'Year of Entry' corresponds to:' drop-down and choose the appropriate year.



15. Click OK.

16 Close the RM Unify AD Sync Configuration Tool.

5. Install RM Unify Password Filter

The RM Unify Password Filter is provided in two versions, for 64-bit and 32-bit servers. It should be installed on all domain controllers (DCs), and this involves a server reboot.

Note: Ensure you deploy the correct version for your server. On a 64-bit server only the 64-bit version will work.

If you are not sure whether a DC is 64-bit or 32-bit, see 'Appendix II: Identifying 32- and 64-bit Windows servers'.

Ensure you have completed the 'Pre-installation tasks' on all the DCs.

► To install RM Unify Password Filter

Note As detailed below, the installation procedure differs slightly on Server Core editions of Windows Server, where there is no graphical user interface.

1. Log on to a DC as a user who is a member of the Domain Admins and builtin Administrators groups (not as a CC4 system administrator).
2. Browse to the folder where you extracted the files from the RM_Unify_AD_Sync_v4.zip download file.

(Alternatively, on Server Core you can locate the folder by changing directories at the command prompt).

If the extracted files are not on this server, copy them to a convenient local folder.

3. Locate the appropriate MSI file for your server OS version:
 - *64-bit OS versions*
Password Filter\64bit\RM Unify Password Filter 64bit.msi
 - *32-bit OS versions*
Password Filter\32bit\RM Unify Password Filter 32bit.msi
4. To start the installation, double-click the appropriate MSI.

(On Server Core, do this by entering **msiexec /I RM_Unify_Password_Filter_<version>.msi** at the command prompt.)

An InstallShield Wizard is displayed.

5. Click Next, click Install, and then click Finish.
6. When the installation is complete, click Yes to restart the server.

(On Server Core, do this by entering **shutdown /r /t 0** at the command prompt.)
7. When the reboot is complete, log on as the domain Administrator.
8. When the logon is complete, log off.

(On Server Core, do this by entering **logoff** at the command prompt).
9. Repeat steps 1–8 for any other DCs on your network, if applicable. You can deploy to more than one server at a time if desired.

6. Force a password change at next logon

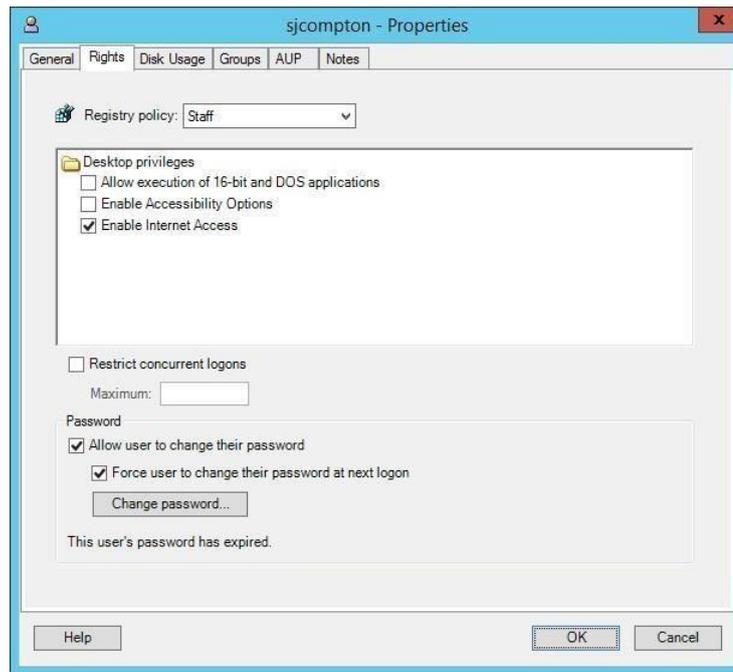
To ensure network users' passwords are synchronised with RM Unify, the password must be changed. You can do this conveniently in the RMMC by setting the user accounts to force a password change at the next logon.

Important: Only perform this task once you have completed the Password Filter installs, by rebooting all domain controllers.

Note: Forcing a password change at next logon will not work if the user tries to access the network remotely, e.g. via RM Portico. Instead, users will need to reset their password on a CC4 network computer before they can use remote access.

We recommend that you do this in batches of users, as it may generate questions and requests from your users.

1. Log on as a member of the System Administrators User Type.
2. Open the RM Management Console.
3. In the left-hand pane, expand Users.
4. Select the user account(s) for which you want to force a password change at next logon.
5. Right-click on the selected users and choose Properties.
6. On the Rights tab, tick 'Force user to change their password at next logon'.



7. Click OK to apply the change.

This completes the installation and setup of RM Unify AD Sync on your CC4 network. Verify that users in each CC4 User Type can successfully log on to RM Unify with their new password.

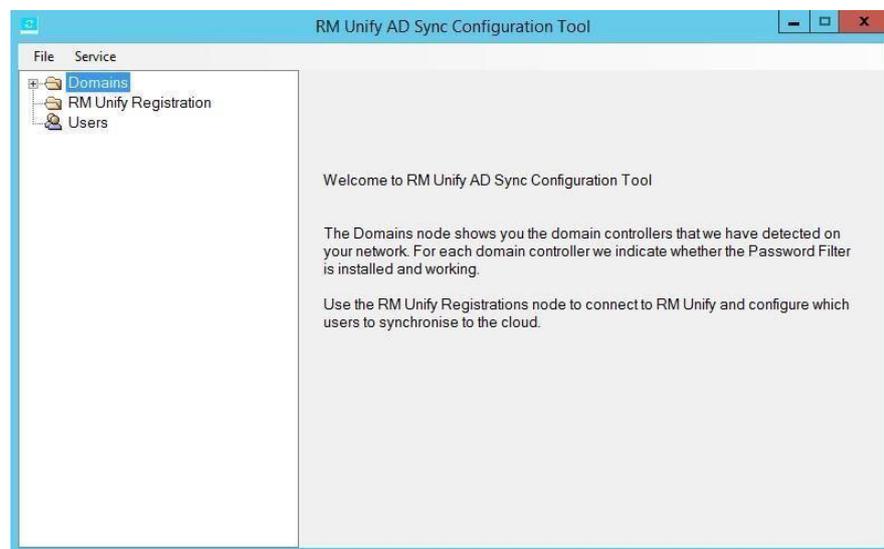
Changing your RM Unify AD Sync configuration

You can make changes to your RM Unify AD Sync configuration at any time, using the RM Unify AD Sync Configuration Tool.

1. To open the RM Unify AD Sync Configuration Tool, do one of the following:

- From the Windows Start screen start typing **RM Unify AD Sync Configuration Tool** and choose the correct application from the suggestions displayed.
- From the Windows Start menu choose RM, RM Unify AD Sync, RM Unify AD Sync Configuration Tool.

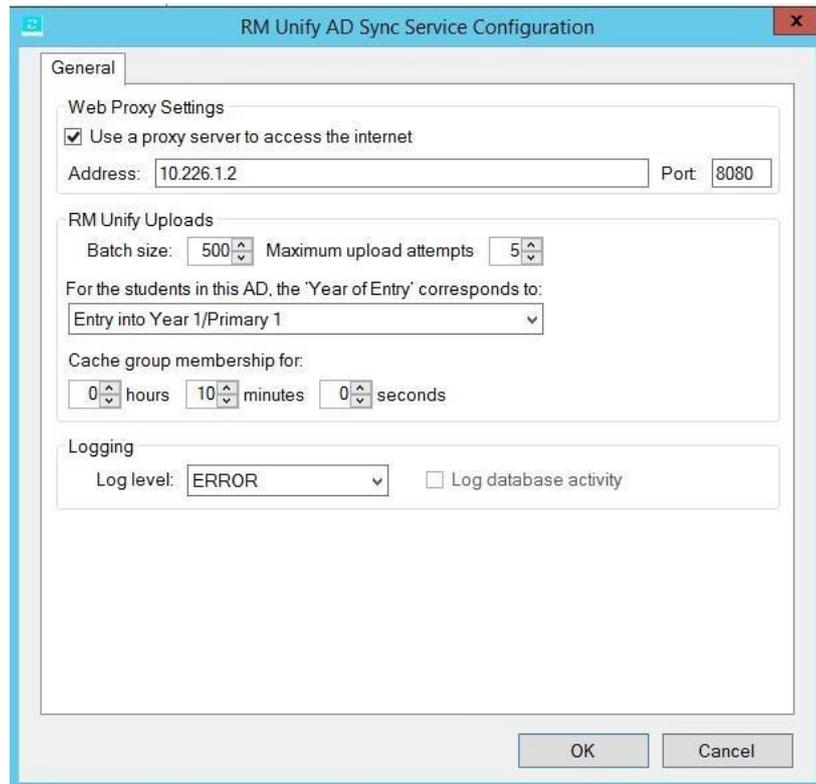
The RM Unify AD Sync Configuration Tool is displayed.



From this console you can:

- Modify any of the existing AD filters or role mappings.
- Add an additional establishment to synchronise to RM Unify, configuring new AD filters and role mappings.
- Temporarily disable any AD Filters.
- Remove any AD filters or role mappings that are no longer required.
- 'Resync' an establishment, re-sending all users for a given school up to RM Unify.

From the File menu, if you choose Service and then Settings, the Settings window is displayed.



From this dialogue you can:

- Set a 'year of entry' offset, to ensure that RM Unify AD Sync maps your CC4 students to the correct school year group.
- Change the proxy server details that were previously entered.
- Modify the frequency at which group membership is queried and cached.

By default, RM Unify AD Sync queries and caches Active Directory group membership every ten minutes, which is appropriate for most single-site networks. However, on large multi-site networks this may cause a reduction in available resources on the domain controller. If that happens on your network, we recommend you increase the group cache expiry time to anything up to one hour. Please be aware however that this change will mean that new users, as well as changes to existing users, will be uploaded slightly less frequently.

Appendix I: Identifying your current version of RM Unify AD Sync

On the server with RM Unify AD Sync currently installed:

1. Open Windows Explorer and browse to **C:\Program Files (x86)\RM\RM Unify AD Sync**.
 - If there is no RM Unify AD Sync folder, but there is a folder called RM Unify AD Sync Service, then AD Sync v1 is installed.
2. In the RM Unify AD Sync folder, use Notepad to open the file **RM.Networks.IdentityManagement.config** and check the line that begins with **<add key="DBVersion"**
 - If the full line is **<add key="DBVersion" value="2"**, then AD Sync v2 is installed.
 - If the full line is **<add key="DBVersion" value="3"**, then AD Sync v3 is installed.

Appendix II: Identifying 32- and 64-bit Windows servers

This guidance is based on this Microsoft resource:

<http://support.microsoft.com/kb/827218>

Windows Server 2008

If 'Windows Server 2008 R2' is displayed on the logon screen, the operating system is 64-bit. Otherwise:

1. Log on as Administrator.
2. From the Start menu choose Control Panel, System and Security.
3. Choose System.
The operating system is displayed in the System area as follows:
 - *64-bit*
System Type is '64-bit Operating System'
 - *32-bit*
System Type is '32-bit Operating System'.

Windows Server 2008 Server Core Edition

If Windows Server 2008 R2 is displayed on the logon screen, the operating system is 64-bit (all CC4 Matrix Domain Controllers and CC4.3 Servers are 64-bit). Otherwise:

1. Log on as Administrator.
2. Type **systeminfo | findstr "System Type:"**
 - *64-bit*
System Type is 'x64-based PC'
 - *32-bit*
Identifier registry value is 'x86 Family'.

Windows Server 2012 and later

The operating system is 64-bit.

Appendix III: Upgrading from RM Unify AD Sync v2 or v3.

There is no in-place upgrade available for existing RM Unify AD Sync v2 and v3 installations. To upgrade, please follow Parts A and B to copy the existing v2/v3 configuration and replicate it on a new installation of RM Unify AD Sync v4.

► Part A: Copy and Remove RM Unify AD Sync v2/v3

1. Log on to your RM Unify AD Sync Service server as a system administrator.
2. Open the RM Unify AD Sync Configuration Tool.
3. Expand the AD Filters and Role Mappings sections and take screenshots of, or otherwise record, your existing settings. You will need these later in the upgrade process.
4. Click OK, then close the RM Unify AD Sync Configuration Tool.
5. From the Start menu or screen, choose Control Panel and then choose 'Programs and Features'.
6. From the list of programs, locate RM Unify AD Sync, right-click and choose Uninstall.
7. Follow the prompts to uninstall the program.

► Part B: Install RM Unify AD Sync v4

1. Ensure you have completed all the steps in Part A.
2. Open Windows Explorer and browse to:
 - On a 64-bit operating system: C:\Program Files(x86)\RM\RM Unify AD Sync.
 - On a 32-bit operating system: C:\Program Files\RM\RM Unify AD Sync.
3. Rename the folder to 'RM Unify AD Sync Upgrade'.
4. Still in Windows Explorer, browse to where you saved the downloaded v4 file RM Unify AD Sync.msi.
5. Double-click RM Unify AD Sync.msi to launch the RM Unify Sync Service InstallShield Wizard. Follow the Steps 1-11 from the 1. Install the RM Unify AD Sync Service section on page 10.
6. Open the RM Unify AD Sync Configuration Tool, enter the proxy settings you recorded from Part A: step 4 and click OK.
7. Close the RM Unify AD Sync Configuration Tool. Do not

complete RM Unify Registration.

8. In Windows Explorer, browse to the 'RM Unify AD Sync Upgrade' folder from Step 3.
9. Right-click RM.Networks.IdentityManagement.config file and select to open with Notepad.
10. Find the line beginning with '<add key="IdentityGuidSource"'.

- 11. Does the line match the following text?

```
<add key="IdentityGuidSource" value="rmCom2000-UsrMgruPN" />
```

No, it does not match – it contains a different value (e.g. value="otherpager" or another attribute), make a note of the entry in value="xxxx", close the file without saving and proceed to Step 12.

Yes, it does match - close the file without saving and proceed to Step 17.

12. In Windows Explorer, browse to: C:\Program Files(x86)\RM\RM Unify AD Sync.
13. Right-click RM.Networks.IdentityManagement.config file and select to open with Notepad.
14. Find the line:


```
<add key="IdentityGuidSource" value="rmCom2000UsrMgruPN" />
```
15. Replace "rmCom2000-UsrMgr-uPN" with the value you copied in Step 11.
16. Save and close the file.
17. Open RM Unify AD Sync Configuration Tool.
18. Register the school (or parent in the case of multi-site AD Sync) and create new AD filters and role mappings, using the settings you recorded from your previous RM Unify AD Sync v2/v3 installation.

For detailed steps on registering and configuring AD filters, please refer to the earlier sections '3. Register your school network with RM Unify' and '4. Configure an establishment'.

For v2 upgrades, please continue with the next section to reinstall RM Unify Password Filter to complete the upgrade process.

For v3 upgrades, your upgrade to v4 is complete and you do not need to follow the next section.

► Remove RM Unify Password Filter

1. Log on to your existing RM Unify AD Sync Service server as a system administrator.

2. From the Start menu or screen, choose Control Panel and then choose 'Programs and Features'.
3. From the list of programs, locate **RM Unify Password Filter**, right- click and choose Uninstall.
4. Follow the prompts to uninstall
5. Reboot the domain controller to complete the uninstallation

► **Install RM Unify Password Filter**

1. Return to page 21 and complete the instructions in the sections 'To install RM Unify Password Filter' and 'Force a password change at next logon'.
2. Your upgrade to v4 is complete.

Appendix IV: Installing prerequisites

Note: To install the prerequisite software you should allow at least two hours, if all the following components are needed.

Installing .NET Framework version 3.5 SP1

Note: Depending on your current version of .NET Framework, a server reboot may be required.

Windows Server (WS) 2008 R2

1. Confirm whether .NET Framework version 3.5 SP1 is installed.

- If your server is a CC4 Server then .NET Framework 3.5 SP 1 is installed by default.
- Otherwise:
 - i. Run PowerShell by clicking the PowerShell icon on the Taskbar. Alternatively, on WS 2008 R2 Server Core, type **powershell** in the Command Prompt window and press Enter.
 - ii. Type **import-module servermanager** and press Enter.
 - iii. Type:
Get-WindowsFeature -Name NET-Framework-Core | fl Installed
and press Enter.

The display will indicate whether or not the component is installed.

2. If required, install .NET Framework version 3.5 SP1:

- i. Type:
Add-WindowsFeature -Name NET-Framework-Core and press Enter.
- ii. Repeat step 1 above to confirm the component has installed successfully.

Windows Server (WS) 2012 R2 and later

1. Confirm whether .NET Framework version 3.5 SP1 is installed.

- If your server is a CC4 Server then .NET Framework 3.5 SP 1 is installed by default.
- Otherwise:
 - i. Run PowerShell by clicking the PowerShell icon on the Taskbar. Alternatively, on WS 2012 Server Core type **powershell** in the Command Prompt window and press Enter.

- ii. Type:

Get-WindowsFeature -Name NET-Framework-Core | fl Installed and press Enter.

The display will indicate whether or not the component is installed.

2. If required, install .NET Framework version 3.5 SP1 as follows. You will need the original WS 2012 installation media. For the following example this is assumed to be in drive E:

- i. Type:

Install-WindowsFeature -Name NET-Framework-Core -source E:\sources\sxs

- ii. Repeat step 1 above to confirm the component has installed successfully.

Installing Microsoft Visual C++ 2010 Redistributable

The instructions vary depending on whether the server is running a 32bit or 64-bit operating system (see 'Appendix I: Identifying your current version of RM Unify AD Sync').

32-bit operating systems (WS 2008 32-bit)

1. Confirm whether Microsoft Visual C++ 2010 Redistributable (x86) is installed:

- i. Open a Command Prompt window.

- ii. Type **C:** and press Enter. iii. Type **cd**

%SYSTEMROOT%\system32 and press Enter.

- iv. Type **dir /b msvcr100.dll** and press Enter.

If the file is found, this command returns a single line of output with the same filename. This indicates that the Microsoft Visual C++ 2010 Redistributable (x86) package is installed.

If the command returns "File Not Found", the Microsoft Visual C++ 2010 Redistributable (x86) package is not installed.

2. If required, install Microsoft Visual C++ 2010 Redistributable (x86):

- i. Download the latest version of Microsoft Visual C++ 2010 SP1 Redistributable (x86).

- ii. Follow the instructions at this URL: <http://www.microsoft.com/en-gb/download/details.aspx?id=8328> iii. Run **vcredist_x86.exe** to

perform the installation.

- iv. Repeat step 1 above to confirm the component has installed successfully.

64-bit operating systems (WS 2008 R2 / WS 2012 / WS 2016 / WS 2019)

1. Confirm whether Microsoft Visual C++ 2010 Redistributable (x64) is installed:
 - i. Open a Command Prompt window.
 - ii. Type **C:** and press Enter.
 - iii. Type
cd %SYSTEMROOT%\system32
and press Enter.
 - iv. Type **dir /b msvcrt100.dll** and press Enter.

If the file is found, this command returns a single line of output with the same filename. This indicates that the Microsoft Visual C++ 2010 Redistributable (x64) package is installed.

If the command returns "File Not Found", the Microsoft Visual C++ 2010 Redistributable (x64) package is not installed.

2. If required, install Microsoft Visual C++ 2010 Redistributable (x64):
 - i. Download the latest version of Microsoft Visual C++ 2010 SP1 Redistributable (x64).
 - ii. Follow the instructions at this URL:
<http://www.microsoft.com/en-gb/download/details.aspx?id=13523>
 - iii. Run **vc redistrib_x64.exe** to perform the installation.
 - iv. Repeat step 1 above to confirm the component has installed successfully.

Appendix V: Default CC4 user role mappings

The default role mappings from CC4 to RM Unify, where CC4 UEV is not in use, are:

CC4 User Type	Profile Path	RM Unify Role
Students	RMStudentProfiles	Student
Non-Teaching Staff	RMNonTeacherProfiles	Non-Teacher
Teaching Staff	RMTeacherProfiles	Teacher
Associates	RMAssociateProfiles	Other
System Administrators	RMSysAdminProfiles	Non-Teacher

Note: You can provide multiple rules for a specific RM Unify role. In the case of a conflict, the first matching role is used.

See 'About User Role Mappings'.

Appendix VI: Alternative mapping types

RM Unify AD Sync provides three alternative methods of mapping user accounts in your network to these RM Unify user roles: Profile Path, Organisational Unit and Group Membership.

Note: For CC4 networks we recommend using Profile Path mapping, unless you have CC4 UEV (User Environment Virtualisation) in which case choose organisational unit or group membership.

Profile Path

This method uses the AD User 'Profile Path' attribute. It detects the Windows share name used in the user's profile path and compares it with the string provided.

This method is suitable for CC4 networks and other Windows Server networks that use specific share names for different user types.

For example, student user profiles in CC4 networks are all accessed through a common share name of 'RMStudentProfiles', so the Profile Path rule would be to match the string "RMStudentProfiles".

Profile path is not suitable for CC4 UEV networks. Please map roles using organisational units or group membership mappings.

Organisational Unit

This method uses your Organisational Unit (OU) structure within Active Directory. If your establishment has an AD structure that differentiates user types by OU location, this is an appropriate mapping method for you.

The string will match against any OU that appears in the path of a user account.

For example, if the OU structure is:



The common OU for all Students is 'Student Users', which includes users in all subordinate OUs. In this case the Organisational Unit rule would be to match the string "Student Users".

In the same example, for Non-Teachers you would set the Organisational Unit to match the string “NonTeaching Staff”.

Group Membership

This method maps users by AD group membership.

This method should be used if the other methods above cannot be implemented in your network – for example, if you have a flat AD OU structure and fixed profile paths for all users. You can use either your existing user groups, or create new groups specifically for RM Unify. The Group Membership rule would be used to match a string that equals the group name.

Note: The RM Unify AD Sync Service checks for user account and user role changes every 15 minutes. Note that if you use the Group Membership method, this checking is slower and may require more processing than with other methods
