

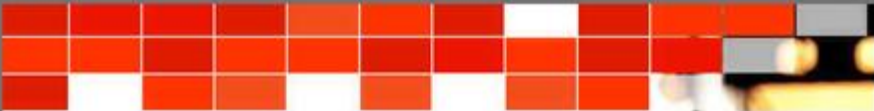
Redlands Live@edu

Identity Lifecycle Manager Setup Guide

Step by Step installation guide for provisioning Microsoft Live@edu with ILM and Password Sync



Microsoft®
Live@edu



Identity Lifecycle Management

Automate Identity and Access Management

Contents

Introduction	4
Before You Begin.....	4
Prerequisites	4
Password Change Notification Service	5
Create an on-premises OLSync service account	6
Assign the Service Principal Name	7
Assign the Password Change Notification Service to Specific Group	7
Prepare your on-premises organization	8
Install Microsoft Identity Lifecycle Manager (ILM)	8
Install Powershell V2.....	13
Install ILM Cmdlets.....	15
Install The ILM Hotfix	16
Configure Outlook Live Accounts & Authentications for OLSync	18
Connect Windows PowerShell on your local computer to Outlook Live	19
Assign the GALSynchronizationManagement RBAC role to the OLSync service account.....	19
Give the OLSync service account access to WinRM.....	19
Test the OLSync service account.....	20
Run OLSync setup	21
Test the configuration to verify the import of the OLMA configuration	24
Configure the OLSync Hosted management agent.....	25
Test the configuration of the Hosted management agent	27
Configure the On-Premises Management Agent.....	28
Specify which on-premises organizational units you want to synchronize with Outlook Live.....	28
Enable Password Synchronisation	29
Perform a full data synchronization.....	30
Synchronize Using Windows PowerShell	30
Verify that the on-premises accounts have been synchronized.....	31
Perform Subsequent OLSync Data Synchronizations to Outlook Live	32
Logging in to Live@edu.....	33
Adding an Accepted Domain to Live@edu	34
Creating Mail-Enabled Users.....	36

Appendix	37
SQL Server Issues	37
MVWindowsLiveAttributeName.....	37
Branding.....	37
Common problems	38
Passwords aren't syncing.....	38
I see Access Denied error messages in Event Log.....	38
Error 25082	38
Misc.....	38
Populating Student Email Address in Active Directory	39

Introduction

This document is a step-by-step guide for using Microsoft Identity LifeCycle Manager 2007 FP1 to provision accounts and replicate password changes, from Active Directory. It also shows how to create Mail-Enabled users in live@edu from local accounts who have an on-premise exchange (in our case, our staff had a local exchange account, but we also wanted their addresses listed in the live@edu Global Address List, and for them to have access to SkyDrive etc, but not to have a live@edu mailbox)

Some of the text in this document has been collated from the Microsoft Outlook Live help pages.

This guide makes the following assumptions:

- A domain has been correctly registered and configured to work with Live@edu
- An SQL Server (2005+) is already installed and running on a server (for best performance SQL Server and ILM should run on the same machine)
- All the users you wish to sync passwords with are members of a common group in Active Directory (eg, Students, Domain Users, etc), they all have a password of minimum 6 characters (Live@edu requirement) and they all have the *email* field in Active Directory populated with the live@edu address to be used
- The users to have a live@edu mailbox do not currently have an On-Premise exchange mailbox.

Before You Begin

Prerequisites

A Windows 2003/2008 Enterprise Server (32bit Only)

Microsoft Identity Manager 2007 FP1

Microsoft Powershell V2 (<http://support.microsoft.com/kb/968929>)

ILM Powershell cmdlets (<http://go.microsoft.com/fwlink/?LinkId=152464>)(MAConfigSetup.msi)

ILM 2007 FP1 strong naming hot fix (<http://go.microsoft.com/fwlink/?LinkId=3052&kbid=960765>)

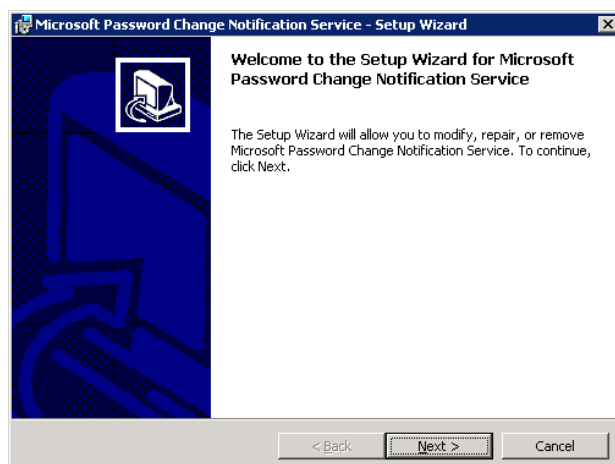
Galsync R4 v2 (<http://go.microsoft.com/fwlink/?LinkId=164627>)(Galsync R4 v2.msi)

It is highly advisable to register a test live@edu domain, and get things up and running in that before attempting to do this with the domain you will be using for production.

Password Change Notification Service

The Password Change Notification Service (PCNS) intercepts password changes, and forwards them to the ILM server, which then assigns the new password to the corresponding account at live@edu. Due to the way this works, the PCNS needs to be installed on **all** of your Domain Controllers. The installation requires the Domain Controllers to be rebooted.

PCNS is located in the \MIIS\Password Synchronization\ folder of the ILM CD-ROM, and there is a version for both x86 and x64 based systems.



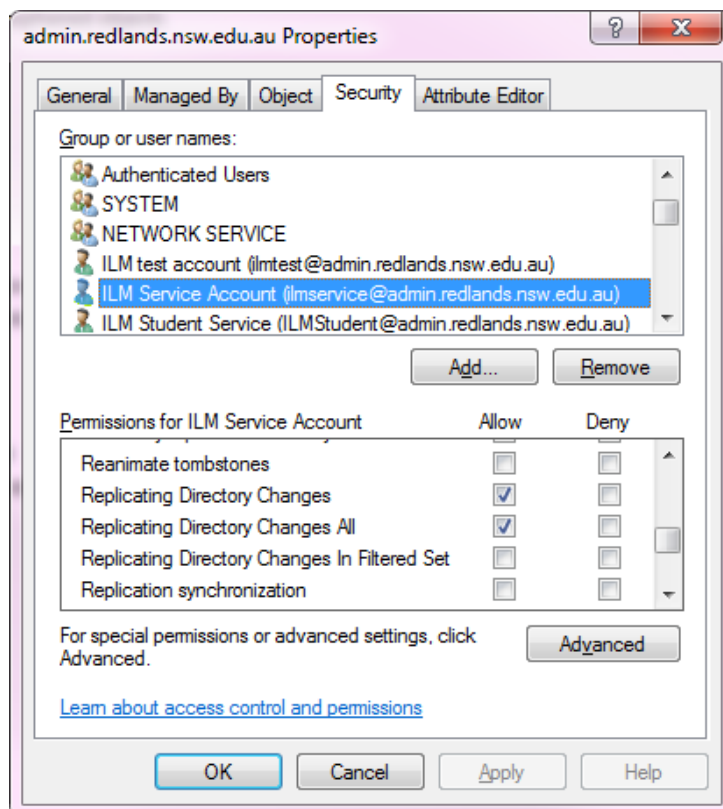
You may be informed you need to upgrade the Schema of the domain. To do this, a user account with the schema admin and enterprise admin group memberships is required.

Create an on-premises OLSync service account

To collect up-to-date information from the on-premises Active Directory Domain Services (AD DS) or Active Directory directory service, you need to give Outlook Live Directory Sync (OLSync) authorization to access data and view replicated data in the directory. Here's how:

1. Create a OLSync service account to access the on-premise domains by creating a user account in the on-premises Active Directory forest.
2. Grant "Replicating directory changes" permissions on the OLSync service account.
The OLSync service account that you created in step 1 must have permissions on the on-premises domains to view replicated directory changes. Perform the following steps in each domain where OLSync needs to access account data.
 1. Open Active Directory Users and Computers.
 2. On the View menu, click Advanced Features.
 3. In the tree view, right-click the domain node for the on-premises provisioning domain, and then click Properties.
 4. On the domain Properties page, select the Security tab.
 5. On the Security tab, click Add, and enter the alias for the OLSync service account. In the search results, select the OLSync service account. Under Permissions for <OLSync service account name>, select the Allow box that corresponds with the permission, "Replicating directory changes."

Click Apply and then click OK.

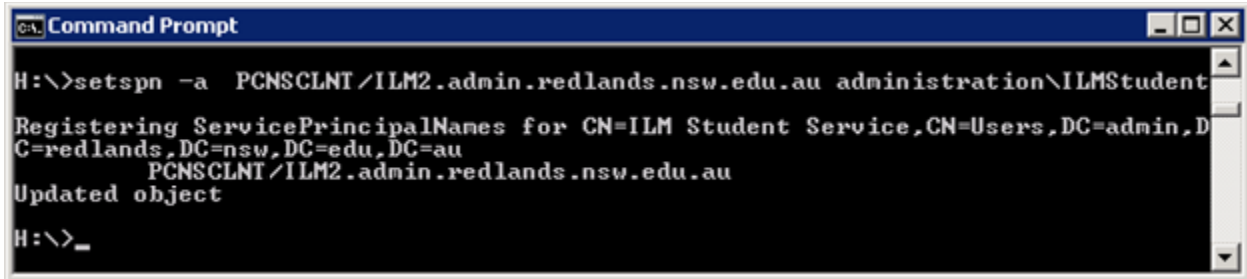


Assign the Service Principal Name

This part is critical to the correct functioning of the Password Change Notification Service.

In the example below:

ILM2	is the Server running ILM
ilm2.admin.redlands.nsw.edu.au	is the FULL QUALIFIED DOMAIN NAME (FQDN)
Administration	is the name of the domain
PCNSCLNT	is the name of the target.
ILMStudent	is the name of the Service Account created for ILM



```

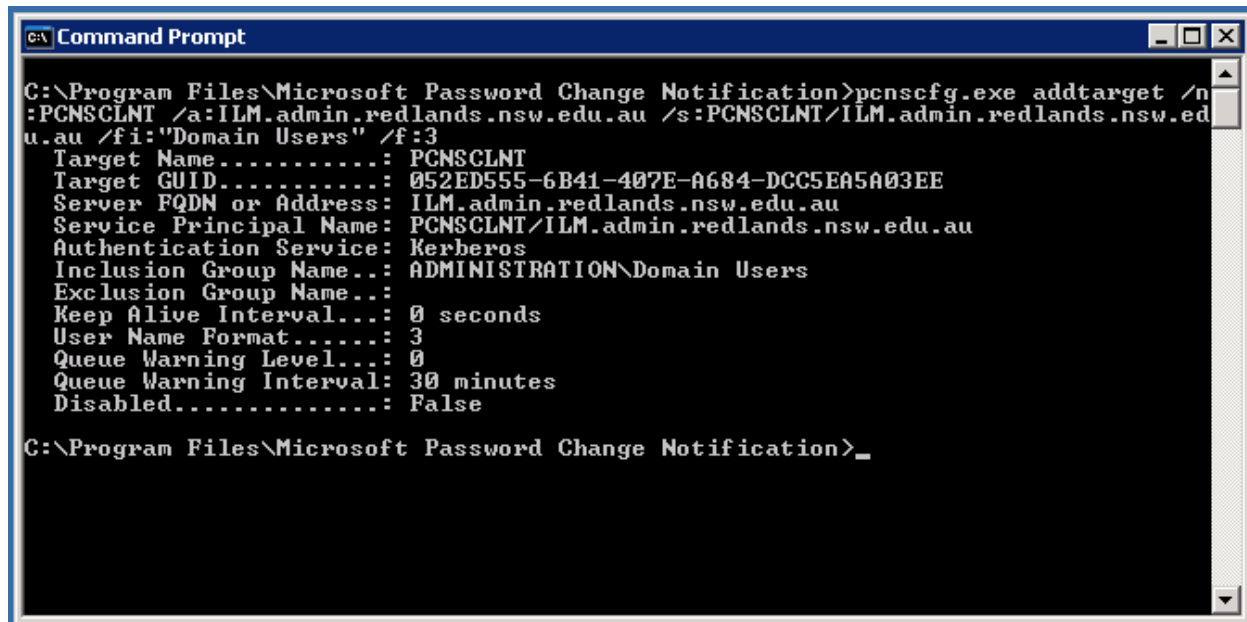
C:\>setspn -a PCNSCLNT/ILM2.admin.redlands.nsw.edu.au administration\ILMStudent
Registering ServicePrincipalNames for CN=ILM Student Service,CN=Users,DC=admin,DC=redlands,DC=nsw,DC=edu,DC=au
PCNSCLNT/ILM2.admin.redlands.nsw.edu.au
Updated object
H:\>_
  
```

Assign the Password Change Notification Service to Specific Group

On a domain controller, open the Command Prompt and navigate to *C:\Program Files\Microsoft Password Change Notification*

In the example below the **PCNSCLNT** is the name of the target we specified in the previous step. The **/fi:"Domain Users"** part tells the PCNS that it will only notify of changes to all domain users

(Note: in the screenshot below, the ILM server being targeted differs from above, as the screenshots were taking from 2 separate installs. The ILM server specified should be the same for both commands)



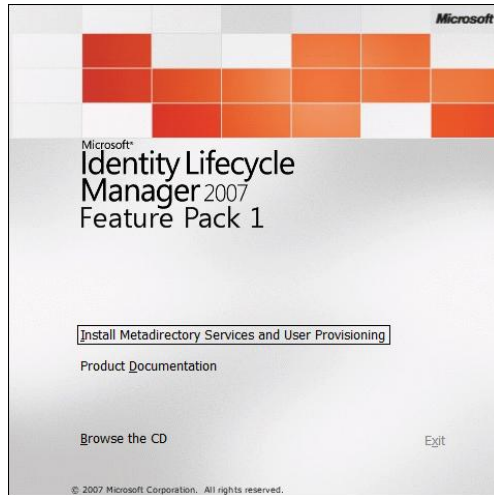
```

C:\Program Files\Microsoft Password Change Notification>pcnscfg.exe addtarget /n
:PCNSCLNT /a:ILM.admin.redlands.nsw.edu.au /s:PCNSCLNT/ILM.admin.redlands.nsw.edu
u.au /fi:"Domain Users" /f:3
Target Name.....: PCNSCLNT
Target GUID.....: 052ED555-6B41-407E-A684-DCC5EA5A03EE
Server FQDN or Address: ILM.admin.redlands.nsw.edu.au
Service Principal Name: PCNSCLNT/ILM.admin.redlands.nsw.edu.au
Authentication Service: Kerberos
Inclusion Group Name..: ADMINISTRATION\Domain Users
Exclusion Group Name..:
Keep Alive Interval...: 0 seconds
User Name Format.....: 3
Queue Warning Level...: 0
Queue Warning Interval: 30 minutes
Disabled.....: False
C:\Program Files\Microsoft Password Change Notification>_
  
```

Prepare your on-premises organization

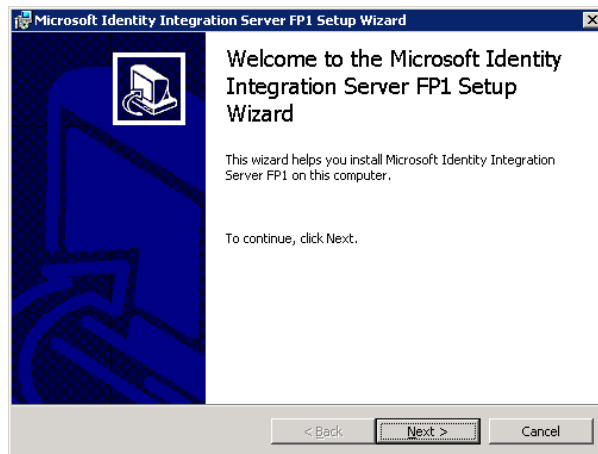
If any of the installations fail, and it is not apparent why they are failing, it is worth trying to run the setup utilities from an elevated command prompt.

Install Microsoft Identity Lifecycle Manager (ILM)

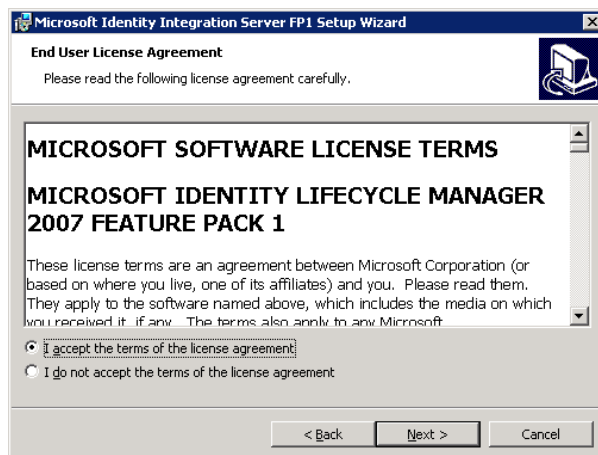


The start screen from ILM 2007.

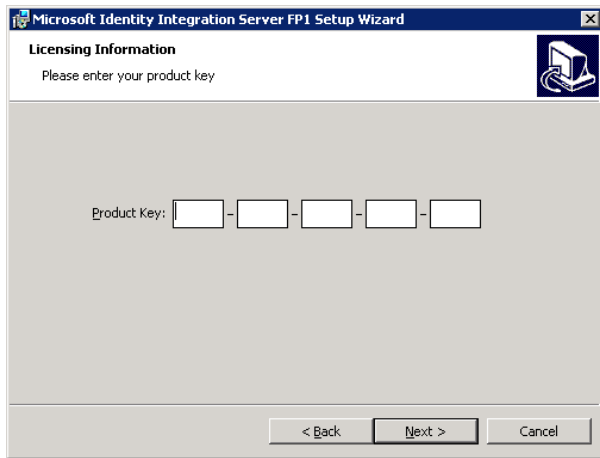
Click Install...



Next to continue..



Accept the terms, and Next..



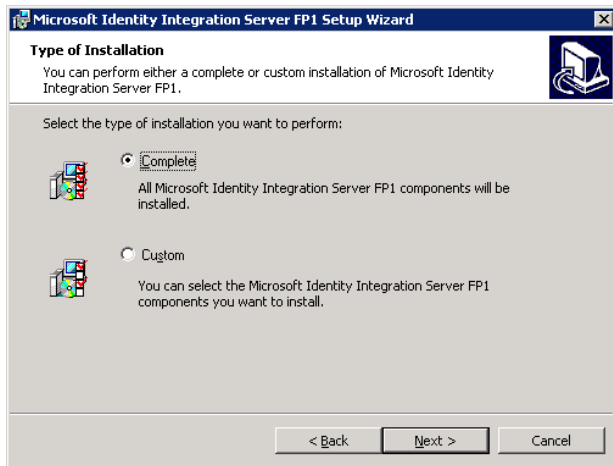
Microsoft Identity Integration Server FP1 Setup Wizard

Licensing Information
Please enter your product key

Product Key: - - - -

< Back Next > Cancel

Enter the Serial Number associated with your ILM Installation CD



Microsoft Identity Integration Server FP1 Setup Wizard

Type of Installation
You can perform either a complete or custom installation of Microsoft Identity Integration Server FP1.

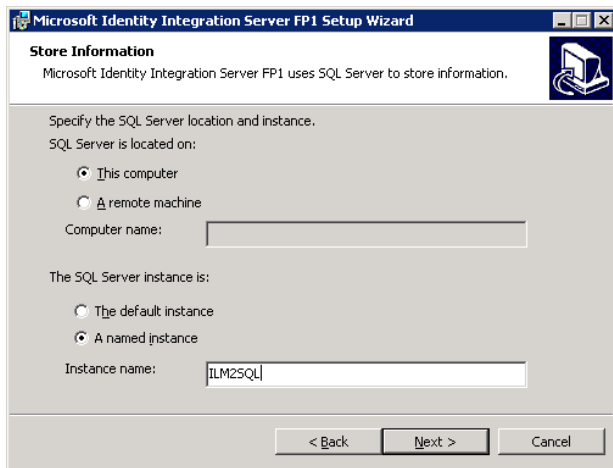
Select the type of installation you want to perform:

☒ **Complete**
All Microsoft Identity Integration Server FP1 components will be installed.

☐ **Custom**
You can select the Microsoft Identity Integration Server FP1 components you want to install.

< Back Next > Cancel

For this installation, we do a Complete Install



Microsoft Identity Integration Server FP1 Setup Wizard

Store Information
Microsoft Identity Integration Server FP1 uses SQL Server to store information.

Specify the SQL Server location and instance.

SQL Server is located on:

☒ This computer

☐ A remote machine

Computer name:

The SQL Server instance is:

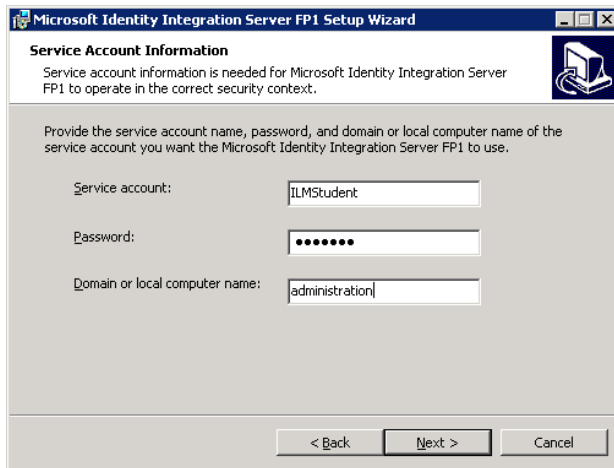
☐ The default instance

☒ A named instance

Instance name:

< Back Next > Cancel

We are running SQL Server on the computer which we are installing ILM. The SQL Instance is called ILM2SQL



Microsoft Identity Integration Server FP1 Setup Wizard

Service Account Information

Service account information is needed for Microsoft Identity Integration Server FP1 to operate in the correct security context.

Provide the service account name, password, and domain or local computer name of the service account you want the Microsoft Identity Integration Server FP1 to use.

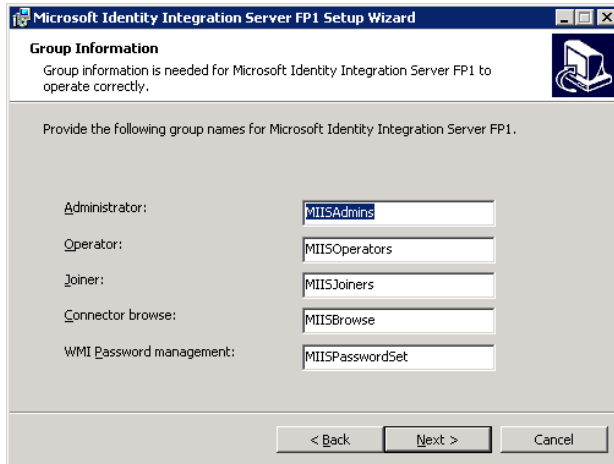
Service account:

Password:

Domain or local computer name:

< Back Next > Cancel

Enter the Username and Password of the Service account you created earlier, and the name of your Domain



Microsoft Identity Integration Server FP1 Setup Wizard

Group Information

Group information is needed for Microsoft Identity Integration Server FP1 to operate correctly.

Provide the following group names for Microsoft Identity Integration Server FP1.

Administrator:

Operator:

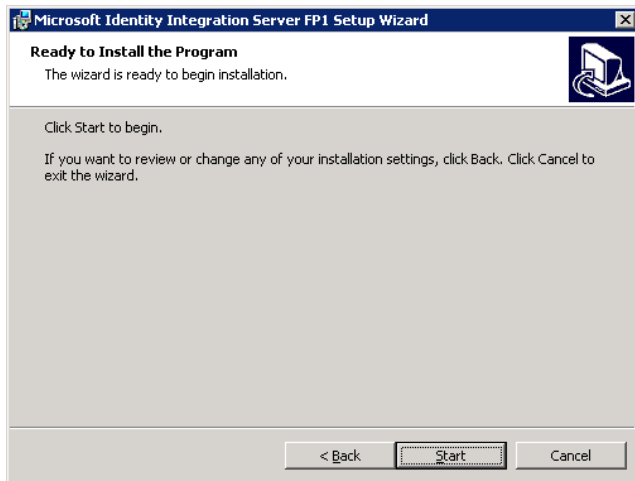
Joiner:

Connector browse:

WMI Password management:

< Back Next > Cancel

These are the groups that the ILM installation creates in Active Directory for managing ILM. These can be left as default.



Microsoft Identity Integration Server FP1 Setup Wizard

Ready to Install the Program

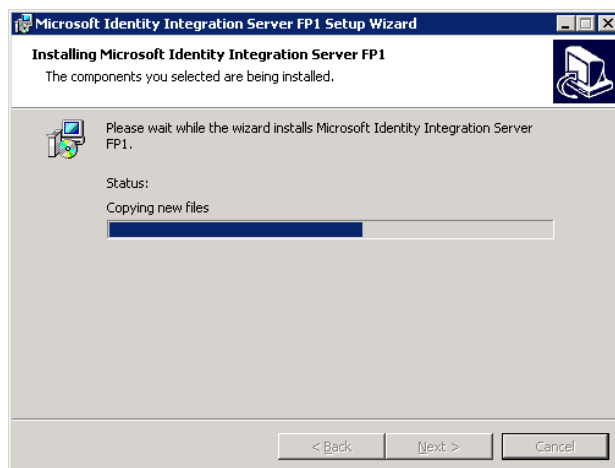
The wizard is ready to begin installation.

Click Start to begin.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

< Back Start Cancel

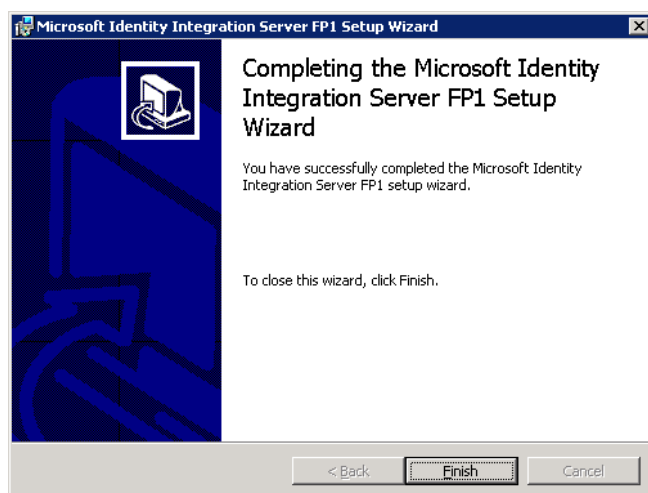
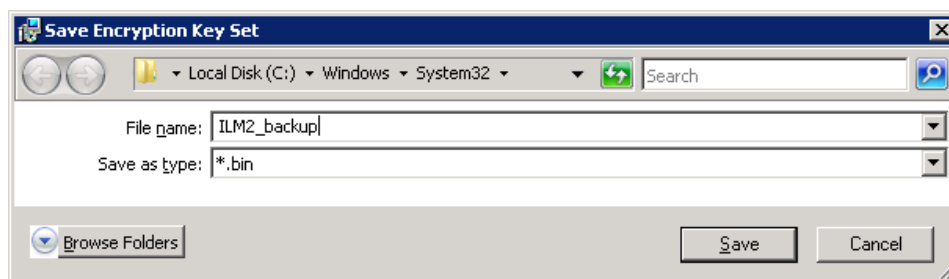
Click Start to begin the installation



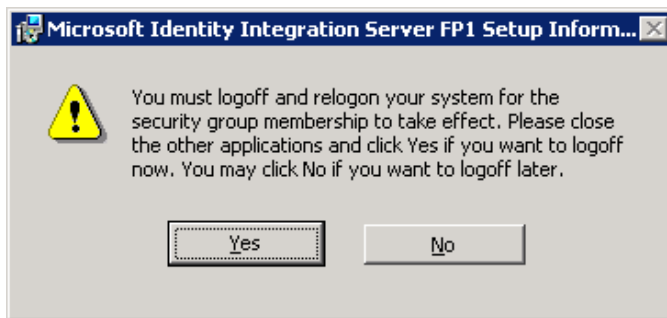
Setup begins copying the files and configuring the SQL Database



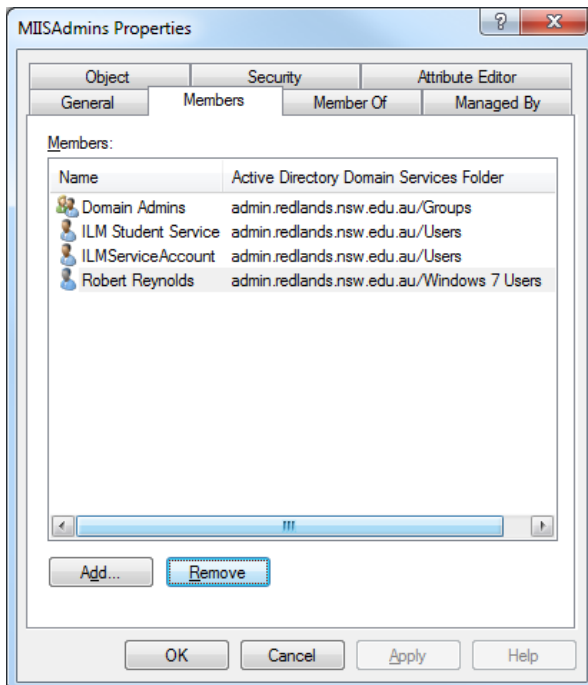
THE ILM setup lets you backup the encryption key in case you need to do a reinstall. Click OK to continue, and then type a name for the backup file



After it has finished installing, simply click Finish.



You need to log off and log back on for the group membership changes to work. ILM will not run until this is done.

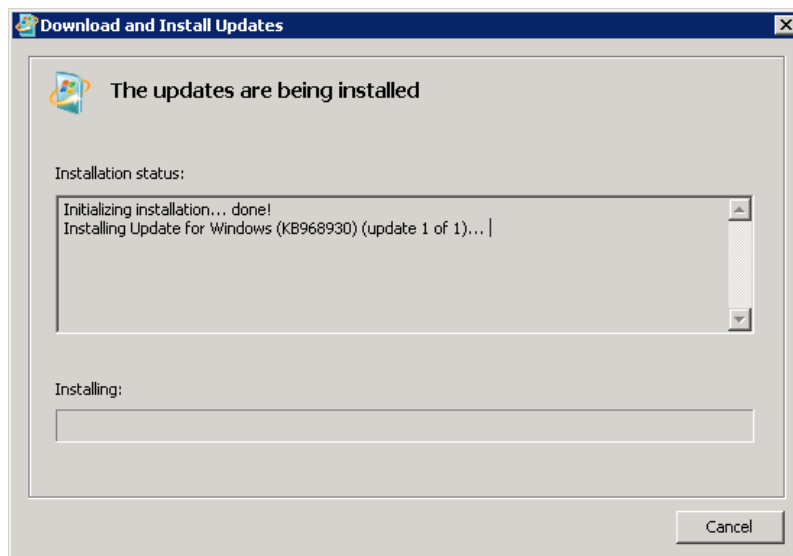
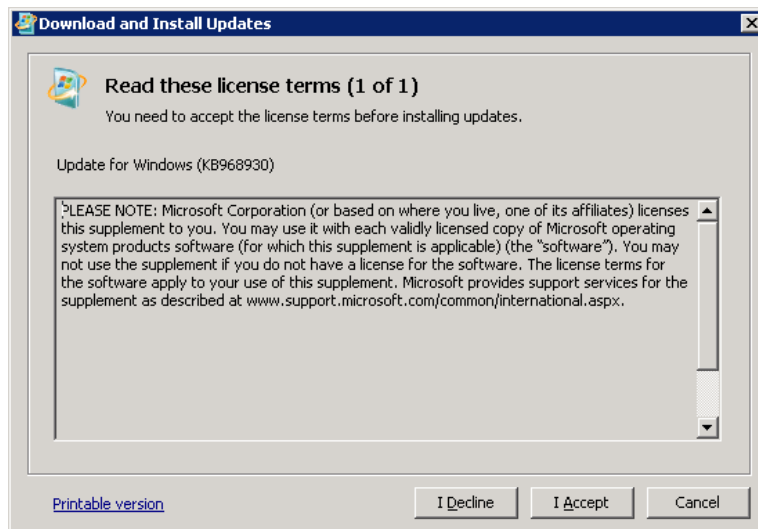
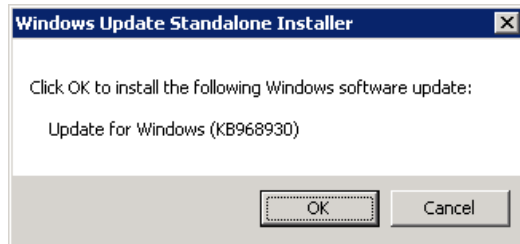


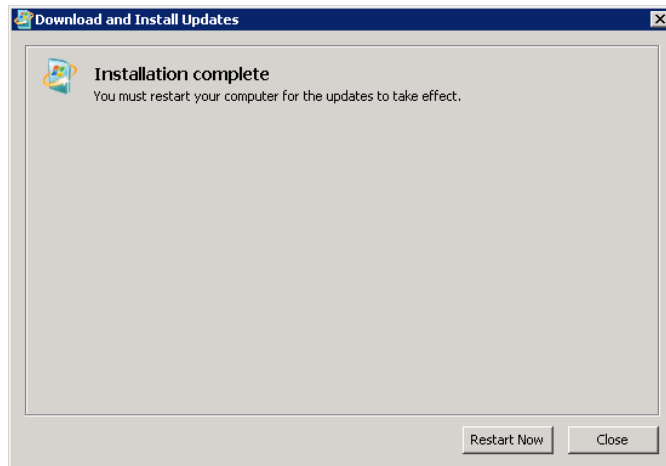
The ILM Installation adds the Service account you created to the *MIISAdmins* Group.

You should also add in here any user you wish to be able to manage the ILM installation.

Install Powershell V2

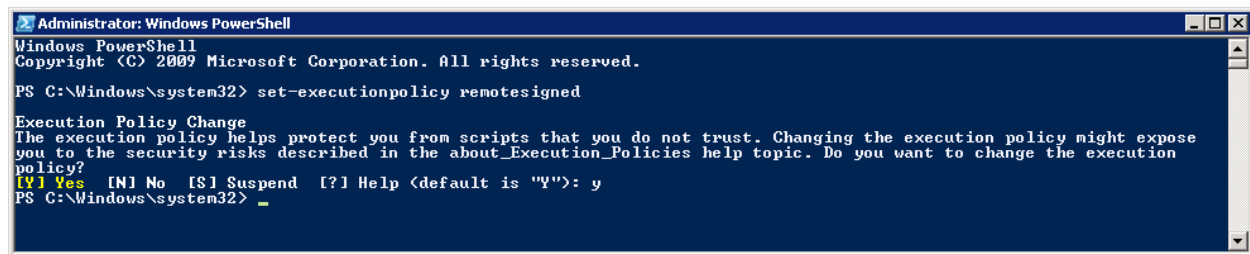
Powershell V2 needs to be installed, along with specific *cmdlets* for use with ILM.





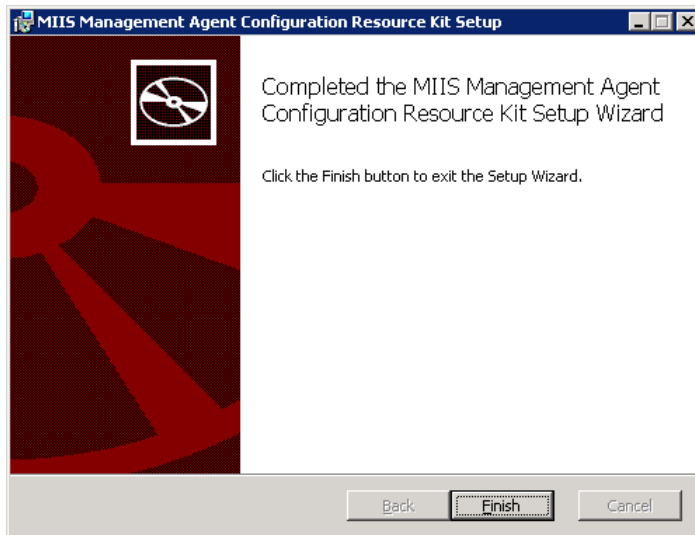
If powershell has never been used on the server before, you have to execute the following command in a PowerShell session. You need to open powershell in Administrator mode (right click, Run as Administrator)

```
set-executionpolicy remotesigned
```



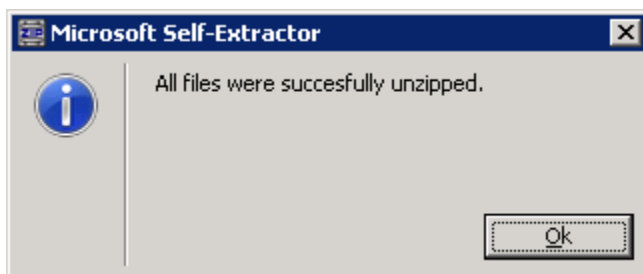
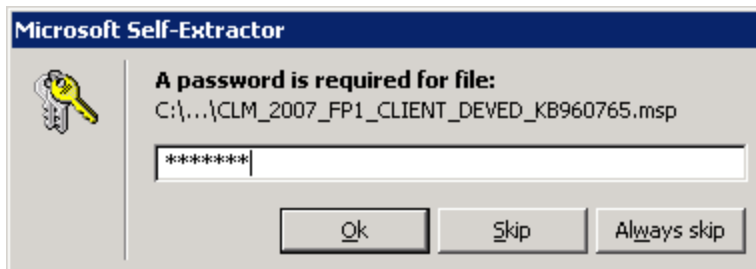
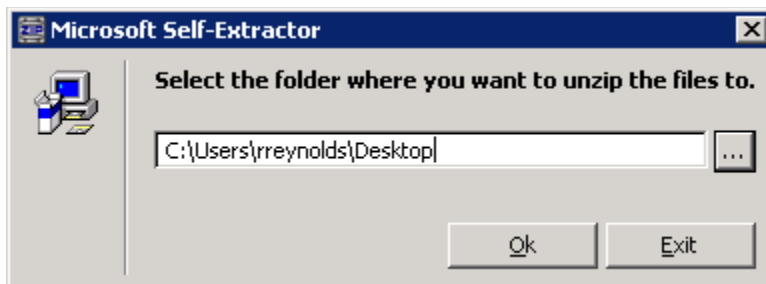
Install ILM Cmdlets

Run the setup for the ILM cmdlets.



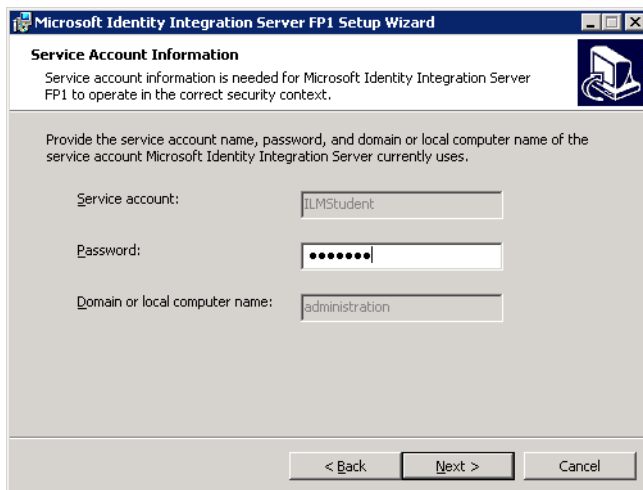
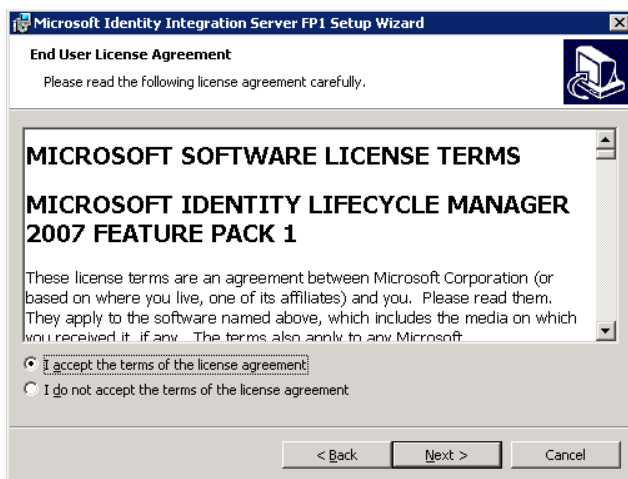
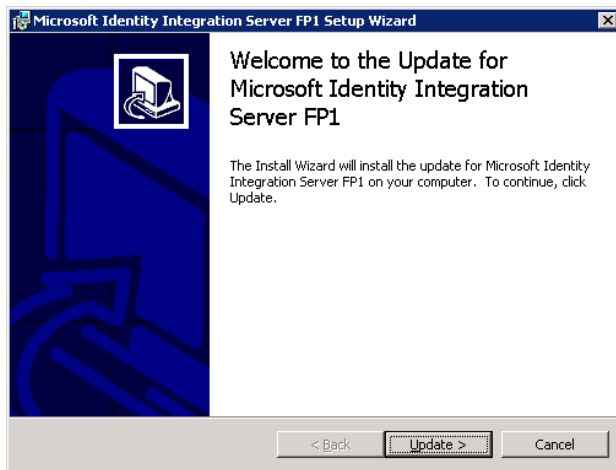
Install The ILM Hotfix

This has to be requested to be downloaded from Microsoft, who will email a link to download the patch, and a password to extract the files.



This will extract a number of files to the chosen location. The only one we are interested in is the *ILM_2007_FP1_ENT_KB960765.msp* file.

Double clicking on this file will launch the Updater

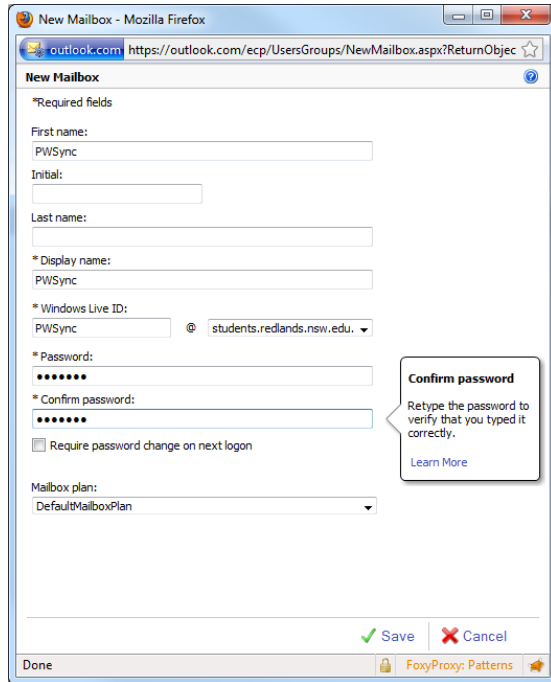


Configure Outlook Live Accounts & Authentications for OLSync

Microsoft recommended best practice is to create 2 accounts; one for provisioning and one for changing passwords, eg:

OLSync@students.redlands.nsw.edu.au

PWSync@students.redlands.nsw.edu.au



New Mailbox

*Required fields

First name: PWSync

Initial:

Last name:

* Display name: PWSync

* Windows Live ID: PWSync @ students.redlands.nsw.edu.

* Password:

* Confirm password:

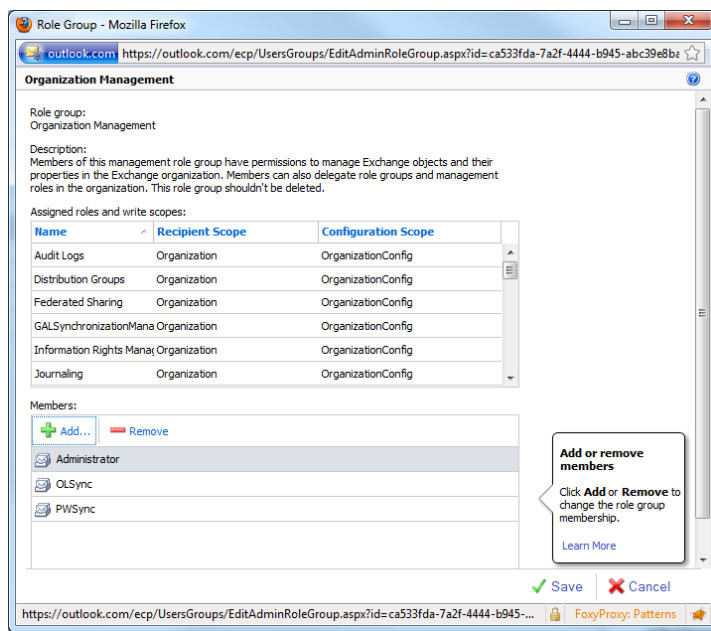
☐ Require password change on next logon

Mailbox plan: DefaultMailboxPlan

Save Cancel

Done FoxyProxy: Patterns

These accounts must be assigned the Organisation Management role:



Organization Management

Role group: Organization Management

Description: Members of this management role group have permissions to manage Exchange objects and their properties in the Exchange organization. Members can also delegate role groups and management roles in the organization. This role group shouldn't be deleted.

Assigned roles and write scopes:

Name	Recipient Scope	Configuration Scope
Audit Logs	Organization	OrganizationConfig
Distribution Groups	Organization	OrganizationConfig
Federated Sharing	Organization	OrganizationConfig
GALSynchronizationManager	Organization	OrganizationConfig
Information Rights Management	Organization	OrganizationConfig
Journaling	Organization	OrganizationConfig

Members:

Add... Remove

Administrator

OLSync

PWSync

Add or remove members

Click Add or Remove to change the role group membership.

Learn More

Save Cancel

https://outlook.com/ecp/UsersGroups/EditAdminRoleGroup.aspx?id=ca533fda-7a2f-4444-b945-abc39e8b2... FoxyProxy: Patterns

After you create the OLSync and PWSync service accounts, sign out of the Outlook Live domain, and sign in to the Outlook Live domain again with the OLSync service account using Outlook Web App (<https://www.outlook.com/owa>). You have to do this one time to accept the terms of use for that new account. If you don't sign in to Outlook Web App and accept the terms of use, you will get Access Denied errors when you try to run ILM 2007 FP1 with the service account.

Connect Windows PowerShell on your local computer to Outlook Live

- Click Start > All Programs > Accessories > Windows PowerShell > Windows PowerShell.
- ☐ Run the following command:

```
$LiveCred = Get-Credential
```

- In the Windows PowerShell Credential Request window that opens, type the Windows Live ID and password of an Outlook Live account. When you are finished, click OK.
- ☐ Run the following command:

```
$Session = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri  
https://ps.outlook.com/powershell/ -Credential $LiveCred -Authentication  
Basic -AllowRedirection
```

Note The *AllowRedirection* parameter enables Outlook Live organizations all over the world to connect Windows PowerShell to Outlook Live by using the same URL.

- ☐ Run the following command:

```
Import-PSSession $Session
```

The three commands above connect you to the Live@edu PowerShell, these are used every time you need to do anything using PowerShell.

Assign the GALSynchronizationManagement RBAC role to the OLSync service account

The **GALSynchronizationManagement** role based access control (RBAC) role lets the OLSync service account run Exchange synchronization cmdlets on your Outlook Live domain.

- In a client-side session, run the following command:

```
New-ManagementRoleAssignment -User OLSync@<tenant_domain> -Role  
GALSynchronizationManagement -Name "OLSync Svc Role"
```

Give the OLSync service account access to WinRM

The last configuration you need to make to the service account is to give the account access to Windows Remote Management (WinRM) so ILM 2007 FP1 can connect Windows PowerShell to Outlook Live. After you have run the command to enable WinRM on the OLSync service account, be sure to close the current Windows PowerShell session.

1. In a client-side session, run the following command:

```
Set-User OLSync@<tenant_domain> -RemotePowerShellEnabled $true
```

Keep the powershell window open, and proceed to the next step to test the Service Account

Test the OLSync service account

Because this OLSync service account will be used by ILM 2007 FP1 to synchronize your on-premises domain with your Outlook Live domain, the best way to test the configuration is to open a client-side session with the service account.

Using the session from the previous step, run the following cmdlets to make sure the account has the appropriate RBAC permissions:

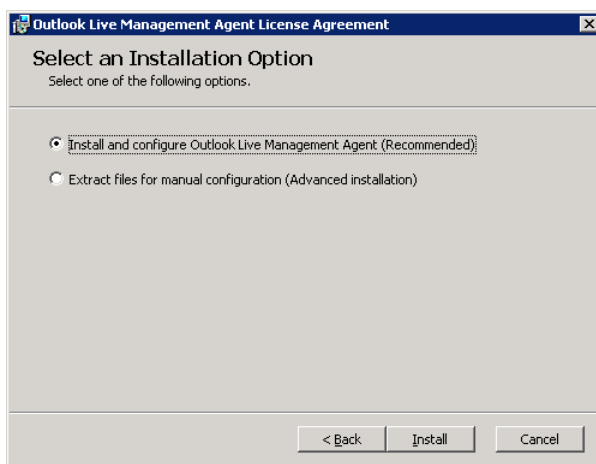
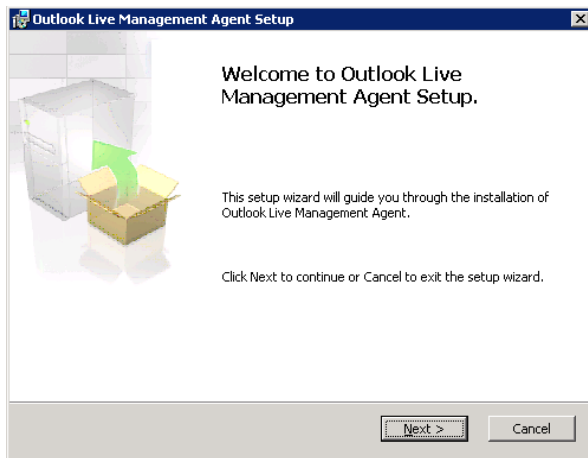
```
Get-SyncMailbox  
Get-AcceptedDomain
```

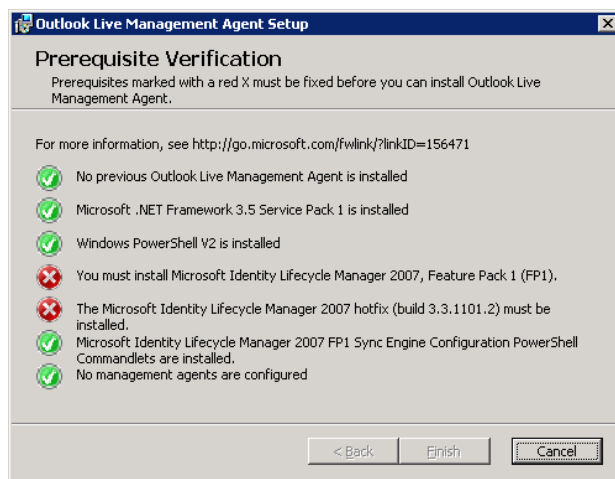
When you're finished using the Outlook Live server-side session, always disconnect Windows PowerShell from Outlook Live by running the following command:

```
Remove-PSSession $Session
```

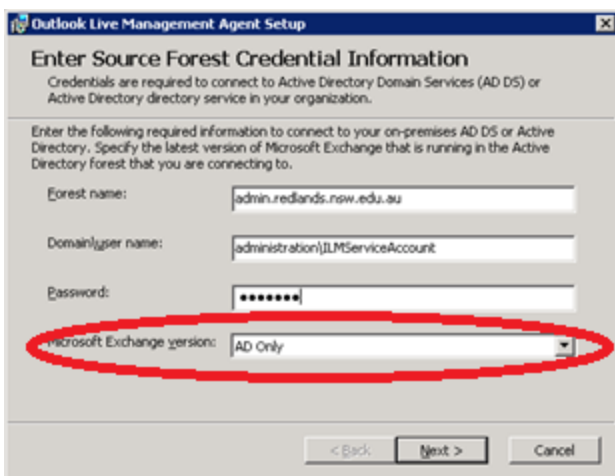
Run OLSync setup

Download and run the Galsync R4 v2.msi from the Outlook Live Site and run it. It will perform a prerequisite check to ensure the previous required components have been installed. If any of them fail, go back and ensure you have installed them all correctly.



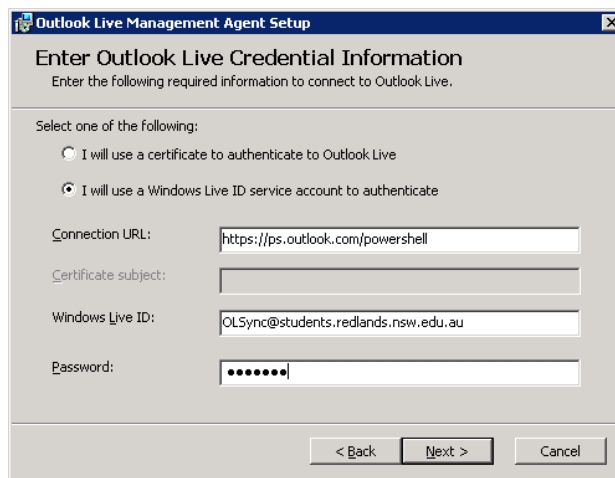


An example of the error message you might see if you haven't configured the prerequisites properly

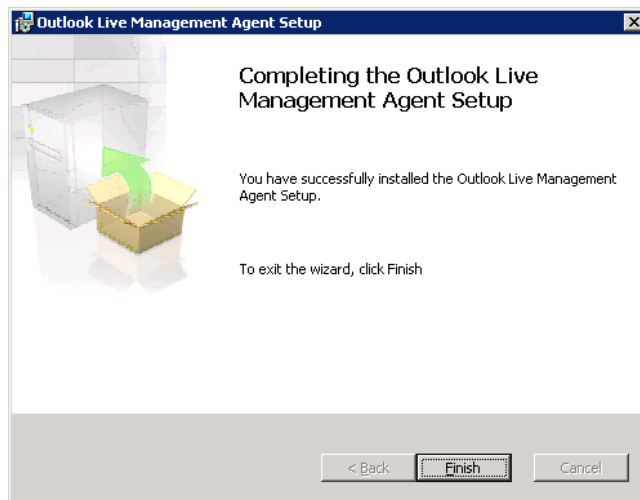


If you do not have any Exchange Server running, choose AD Only.

If you have Exchange, choose the relevant version from the drop-down



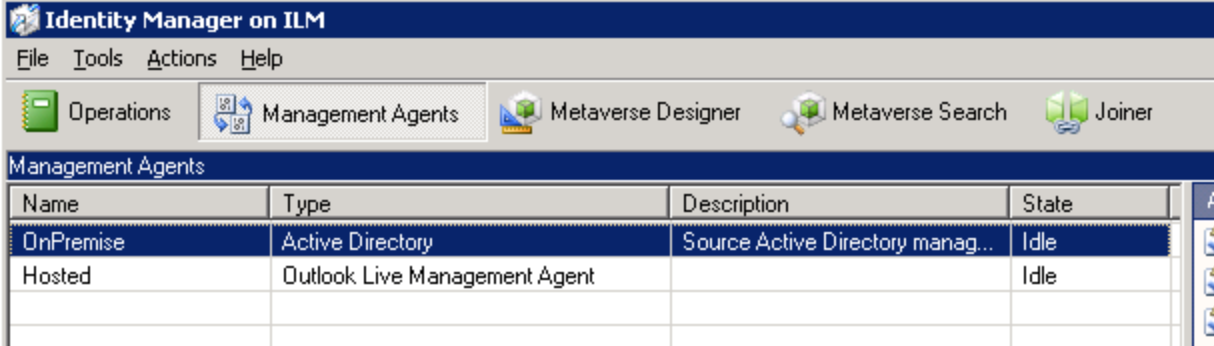
Here we specify the account and password we created in the previous step



Test the configuration to verify the import of the OLMA configuration

To verify that the import of the OLMA configuration, open the Identity Manager and make sure the Hosted and OnPremise management agents are listed.

1. Click Start > All Programs > Microsoft Identity Integration Server > Identity Manager.
2. In the Identity Manager window, click Management Agents.
3. Under Management Agents, verify that the OnPremise and Hosted management agents are listed in the Name column:



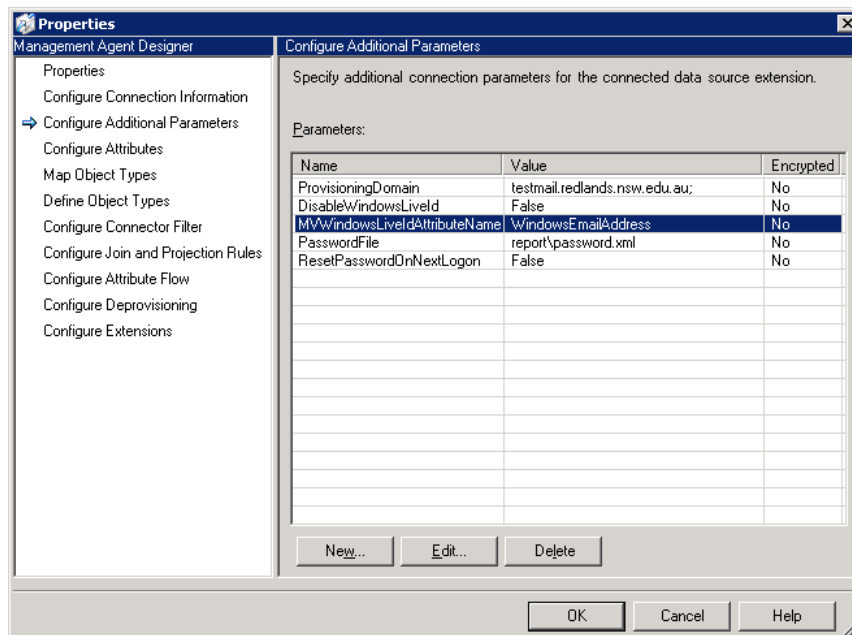
Name	Type	Description	State
OnPremise	Active Directory	Source Active Directory manag...	Idle
Hosted	Outlook Live Management Agent		Idle

Configure the OLSync Hosted management agent

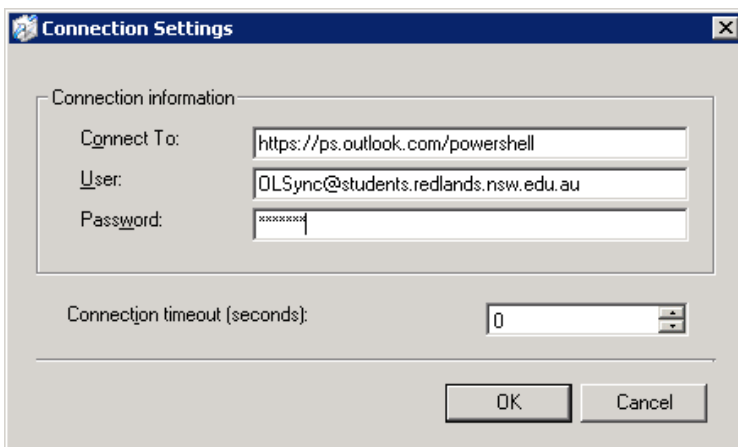
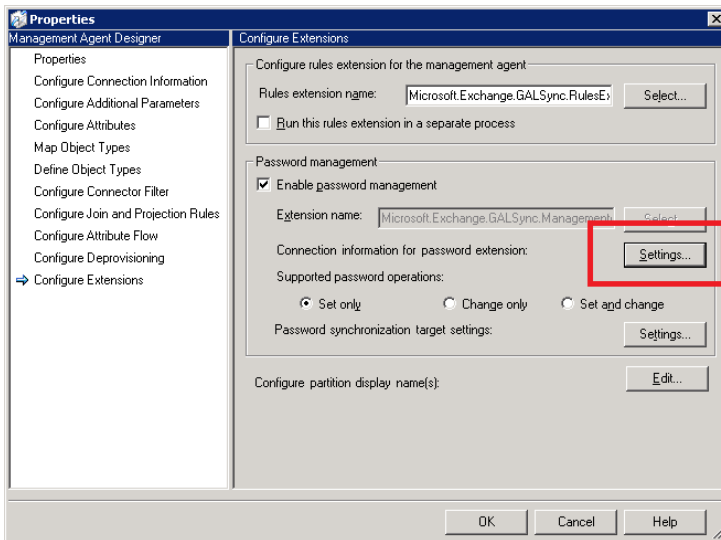
After you run Outlook Live Management Agent (OLMA) Setup, you need to configure the Hosted management agent that is included in the OLMA configuration. Specifically, you need to configure additional parameters on the Hosted management agent. This topic explains how to open the management interface and add or configure parameters.

At a minimum, you need to make sure the *ProvisioningDomain* parameter is set correctly. However, you may need to add additional parameters or change default values on existing parameters. The changes you have to make to additional parameters depend on the needs of your organization and how you have configured the recipient objects in the on-premises organization. For more information, see [Parameters for the OLSync Hosted Management Agent](#)

1. Click Start > All Programs > Microsoft Identity Integration Server > Identity Manager.
2. In the Identity Manager window, click Management Agents.
3. Under Management Agents, double-click the Hosted management agent.
4. On the Properties page, click Configure Additional Parameters, and then click New. In the Parameter and Value fields, enter the following information:
 - o **Parameter:** *ProvisioningDomain*
 - o **Value:** Enter your Outlook Live domain. By default, the *ProvisioningDomain* parameter is populated with the domain value that you entered in Setup.
5. On the Properties page, click OK.



Because we have populated the Email field in Active Directory, the *MVWindowsLiveAttributeName* needs to be set to *WindowsEmailAddress* (See Appendix for details)



Test the configuration of the Hosted management agent

You can test the configuration of the Hosted management agent by running an import operation from the Hosted management agent. Here's how:

1. Click Start > All Programs > Microsoft Identity Integration Server > Identity Manager.
2. In the Identity Manager window, click Management Agents.
3. Right-click the Hosted management agent and then click Run.
4. In the Run Management Agent dialog box, select Full Import (Stage only), and then click OK.

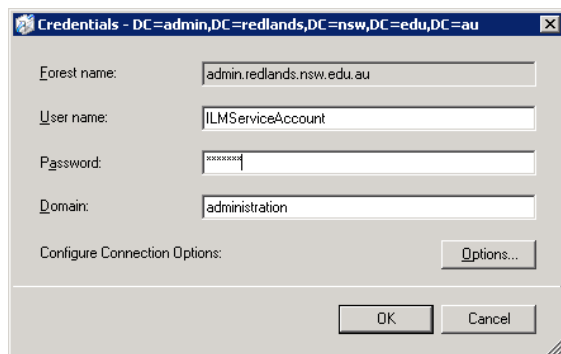
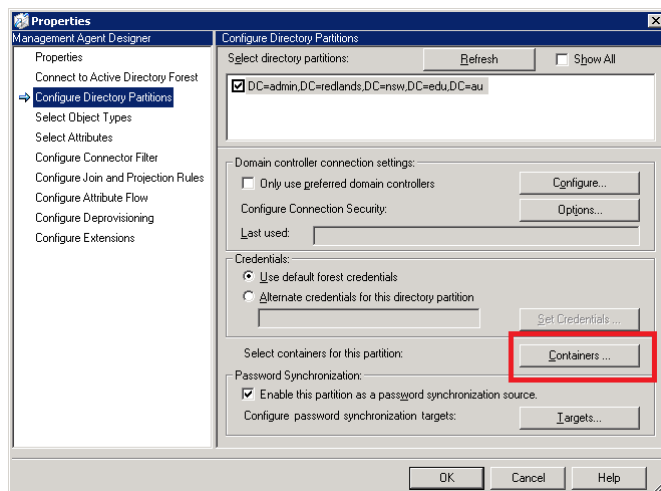
To verify that the operation was successful, in the main Identity Manager window, click Operations. The value in the Status column should say "success."

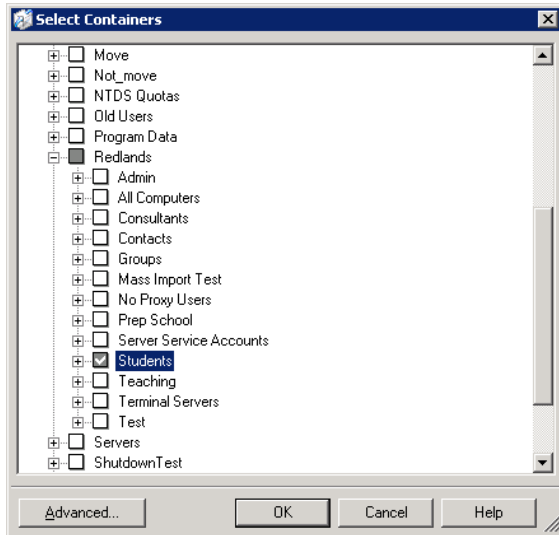
Configure the On-Premises Management Agent

Specify which on-premises organizational units you want to synchronize with Outlook Live

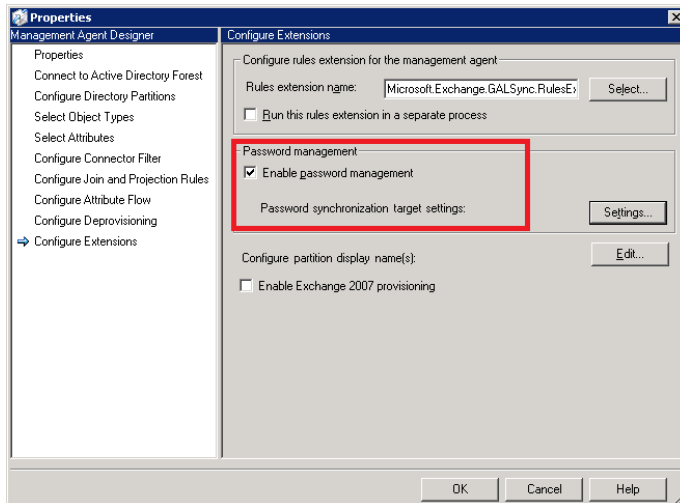
Here's how you specify which organizational units are synchronized during an OLSync synchronization.

1. Click Start > All Programs > Microsoft Identity Integration Server > Identity Manager.
2. In the Identity Manager window, click Management Agents.
3. Under Management Agents, double-click the OnPremise management agent.
4. On the Properties page, click Configure Directory Partitions. Next to Select containers for this partitions, click Containers.
5. In the Credentials dialog box, enter the user name and password for an on-premises user account, and then click OK.
6. If the credentials you entered are valid, the Select Containers dialog box is displayed. Clear the checkboxes on all containers, except for the organizational units that you want to synchronize, and then click OK.
7. On the Properties page, click OK





Enable Password Synchronisation



Perform a full data synchronization

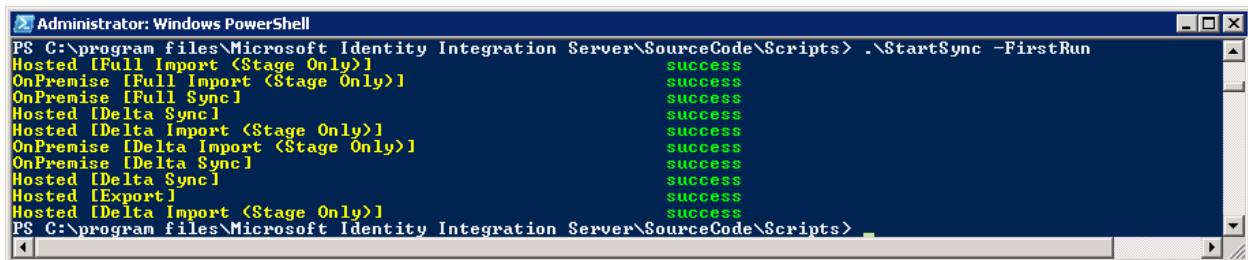
After you have installed everything, and configured the Management Agents, all that is left is to perform a set of synchronization operations to import the data into the metaverse, synchronize the data, complete "join" operations, and export data to your Outlook Live domain. You must perform a full synchronization whenever you make changes to the additional parameters.

It is advisable to use a subset of users on the initial run (about 5 -10) just to ensure everything goes to plan. Once you are sure it is working as planned, expand to the full user base.

Synchronize Using Windows PowerShell

The recommended way to perform the full synchronization is using the included Powershell script. When you run Outlook Live Directory Sync (OLSync) Setup, the script, StartSync.ps1, is copied to the following directory: *c:\Program Files\Microsoft Identity Integration Server\SourceCode\Scripts*. Use this script to automate synchronization operations with Windows PowerShell.

1. On the computer that is running ILM 2007 FP1, click Start > All Programs > Windows PowerShell V2 > Windows PowerShell V2.
2. Navigate to <system drive>:\Program Files\Microsoft Identity Integration Server\SourceCode\Scripts.
3. Run the following command: `.\StartSync -FirstRun`



```

Administrator: Windows PowerShell
PS C:\program files\Microsoft Identity Integration Server\SourceCode\Scripts> .\StartSync -FirstRun
Hosted [Full Import <Stage Only>]          SUCCESS
OnPremise [Full Import <Stage Only>]        SUCCESS
OnPremise [Full Sync]                      SUCCESS
Hosted [Delta Sync]                        SUCCESS
Hosted [Delta Import <Stage Only>]          SUCCESS
OnPremise [Delta Import <Stage Only>]        SUCCESS
OnPremise [Delta Sync]                     SUCCESS
Hosted [Delta Sync]                        SUCCESS
Hosted [Export]                            SUCCESS
Hosted [Delta Import <Stage Only>]          SUCCESS
PS C:\program files\Microsoft Identity Integration Server\SourceCode\Scripts>
  
```

Windows PowerShell will run each synchronization operation and then report on the status. All data in the Status column should say "success." If you get errors, see [Troubleshoot Outlook Live Directory Sync](#) and check the Event Viewer for any messages. I have also included some common issues and solutions in the Appendix

Verify that the on-premises accounts have been synchronized

To verify mailbox provisioning, you have to sign in to the Outlook Live domain using one of the newly-provisioned Outlook Live mailbox user accounts. Before you can sign in, you need to retrieve the password for that user.

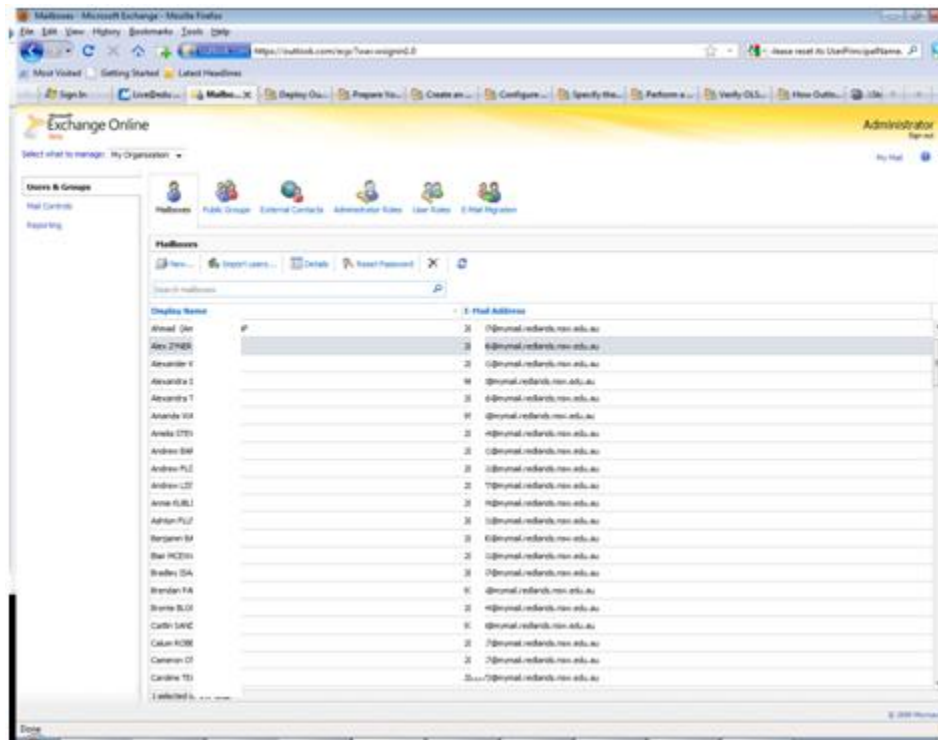
If you are using the Password Change Notification Service (PCNS) in ILM 2007, or if your on-premises organization is running in a Connected Federation environment, changing the on-premises password for the user will change the password for the corresponding Outlook Live user. After initial creation, the password will need to be changed on premise, so it is then Synced up to live@edu.

Otherwise, the password that you entered for this user when you created it in Microsoft Exchange isn't ported over to Outlook Live. Instead, a random password is generated for each user. The password file is stored on the ILM server according to the optional parameter that you set on the OLSync Hosted management agent in OLSync.

1. Retrieve the password for the test user.
2. Open a supported Web browser and sign in at <https://outlook.com/owa> using the test user credentials.

Mailbox provisioning was successful if you can sign in using the test user credentials.

Synchronization was successful if all objects that you created in the on-premises Exchange organization show up in the Outlook Live shared address book.



Perform Subsequent OLSync Data Synchronizations to Outlook Live

After you create or delete users, mail users, or contacts in your on-premises organization, you have to resynchronize Outlook Live Directory Sync (OLSync) data to keep your corresponding Outlook Live domain up-to-date.

Make sure you have performed a successful StartSync -FirstRun before completing this step.

When you run OLSync Setup, the script, StartSync.ps1, is copied to the following directory: <system drive>:\Program Files\Microsoft Identity Integration Server\SourceCode\Scripts. Use this script to automate synchronization operations with Windows PowerShell.

1. On the computer that is running ILM FP1, click Start > All Programs > Windows PowerShell V2 > Windows PowerShell V2.
2. Navigate to <system drive>:\Program Files\Microsoft Identity Integration Server\SourceCode\Scripts.
3. Run the following command:

```
.\StartSync
```

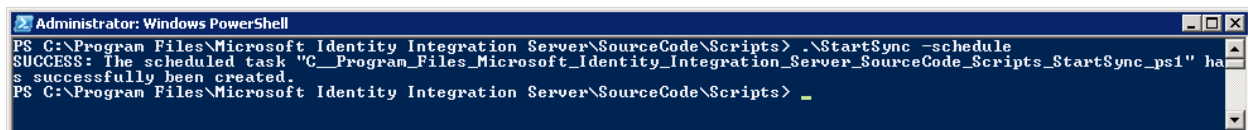
Windows PowerShell will run each synchronization operation and then report on the status. All data in the Status column should say "success." If you get errors, see [Troubleshoot Outlook Live Directory Sync](#).

To create a scheduled task that runs the StartSync.ps1 script, run the following command:

```
.\StartSync -schedule
```

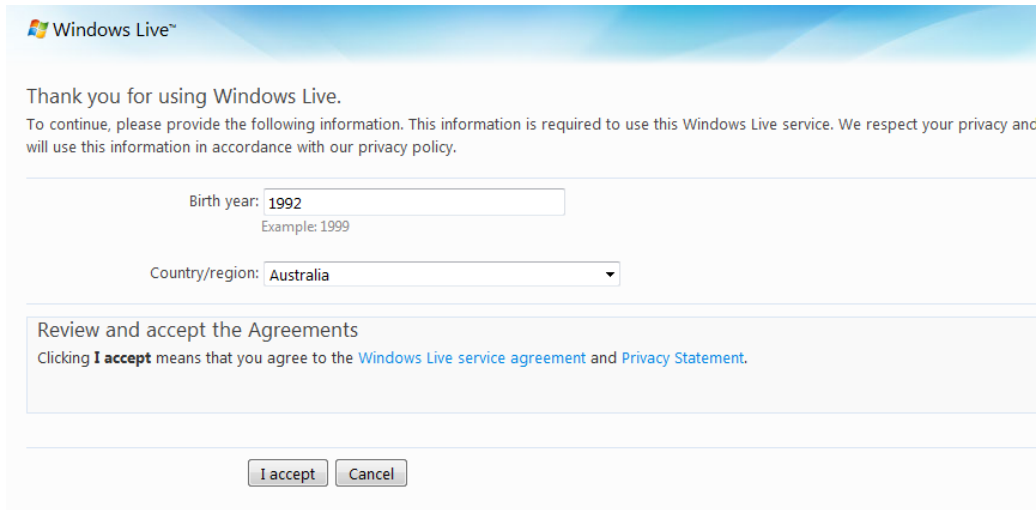
This command creates a scheduled task that runs the StartSync.ps1 script every two hours from 8 A.M. to 8 P.M. You can change the frequency on the task by opening the StartSync.ps1 script and modifying the *sc*, *mo*, *st*, and *du* parameters in the following line of code:

```
schtasks.exe /create /sc HOURLY /MO 2 /st 08:00:00 /du 0012:00 /tn
"$taskname" /tr "$PSHOME\powershell.exe -c
$(($myinvocation.mycommand.definition) "
```



Logging in to Live@edu

Need to enter their Year of birth, and their country



Windows Live™

Thank you for using Windows Live.

To continue, please provide the following information. This information is required to use this Windows Live service. We respect your privacy and will use this information in accordance with our [privacy policy](#).

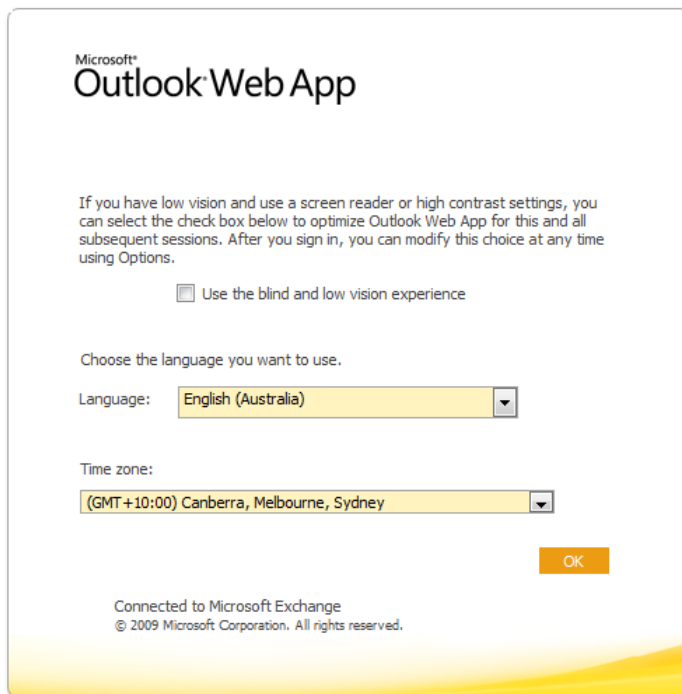
Birth year:
Example: 1999

Country/region:

Review and accept the Agreements

Clicking **I accept** means that you agree to the [Windows Live service agreement](#) and [Privacy Statement](#).

Then they need to select the Language and Timezone



Microsoft®
Outlook® Web App

If you have low vision and use a screen reader or high contrast settings, you can select the check box below to optimize Outlook Web App for this and all subsequent sessions. After you sign in, you can modify this choice at any time using Options.

☐ Use the blind and low vision experience

Choose the language you want to use.

Language:

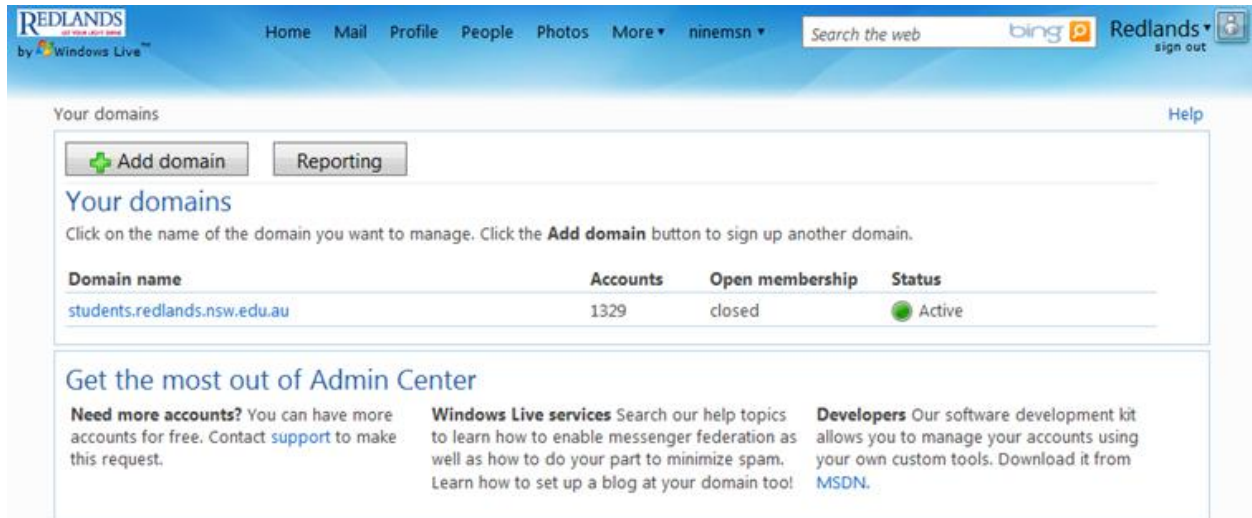
Time zone:

Connected to Microsoft Exchange
© 2009 Microsoft Corporation. All rights reserved.

Adding an Accepted Domain to Live@edu

We had the requirement to add another domain to our live@edu so that it could be used to send and receive mail to main live@edu, and also so that users from this other domain could be listed in the main live@edu Global Address list, and also have access to the Skydrive etc.

To do this, you simply login to <http://domains.live.com> and add it as an accepted domain.



REDLANDS by Windows Live™

Home Mail Profile People Photos More ▾ ninemsn ▾ Search the web bing Redlands sign out

Your domains Help

[+ Add domain](#) [Reporting](#)

Your domains

Click on the name of the domain you want to manage. Click the **Add domain** button to sign up another domain.

Domain name	Accounts	Open membership	Status
students.redlands.nsw.edu.au	1329	closed	Active

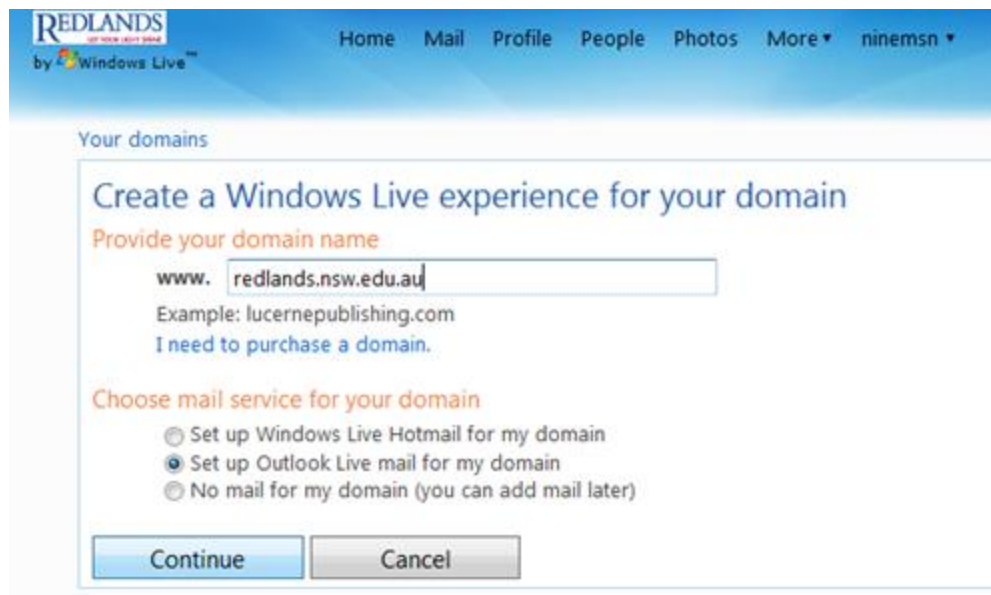
Get the most out of Admin Center

Need more accounts? You can have more accounts for free. Contact [support](#) to make this request.

Windows Live services Search our help topics to learn how to enable messenger federation as well as how to do your part to minimize spam. [Learn how to set up a blog at your domain too!](#)

Developers Our software development kit allows you to manage your accounts using your own custom tools. Download it from [MSDN](#).

We wanted to add our main domain, which the staff were using with an On-Premise Exchange mailbox



REDLANDS by Windows Live™

Home Mail Profile People Photos More ▾ ninemsn ▾

Your domains

Create a Windows Live experience for your domain

Provide your domain name

www.

Example: lucernepublishing.com

[I need to purchase a domain.](#)

Choose mail service for your domain

☐ Set up Windows Live Hotmail for my domain
☒ Set up Outlook Live mail for my domain
☐ No mail for my domain (you can add mail later)

[Continue](#) [Cancel](#)

Make sure it is set for Outlook Live and not Windows Live

REDLANDS by Windows Live™ Home Mail Profile People Photos More ▼ ninemsn ▼ Search the web bing Redlands sign out

Your domains Help

Review settings and accept agreement

 This domain will be registered as an accepted domain of students.redlands.nsw.edu.au. To make this domain a primary domain with its own Outlook Live service, you have to sign in with an account from this domain (redlands.nsw.edu.au).

Please confirm your request. You will always use this Windows Live ID to administer this domain.

Domain: redlands.nsw.edu.au
Mail service: Outlook Live
Administrator: [redacted]@students.redlands.nsw.edu.au ([Change user](#))

Clicking **I Accept** means that you agree to the terms applicable to your program.

- [Custom Domains/Admin Center](#)

The next step is to prove domain ownership by creating a CNAME entry in your external DNS. Because we are already using the domain for mail, we **DO NOT** want to add any MX records.

 You need to prove ownership of this domain by creating an [MX record](#) or a [CNAME record](#). Use the settings below.

[Cancel service](#)

Mail setup (required)

To set up mail and prove ownership of this domain, you must create an MX record through your domain registrar. Use the following settings:

- DNS record type: MX
- Host: redlands.nsw.edu.au
- MX server: [redacted].mail.outlook.com
- TTL: 3600 or 1 hour
- Priority: 10 (or High priority)

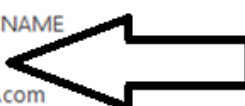
[More information](#)

Prove domain ownership (optional)

If you would like to prove the ownership of domain and create users without setting up mail, you can use a CNAME for up to 30 days. After 30 days, you will need to set up an MX record. Use the following settings:

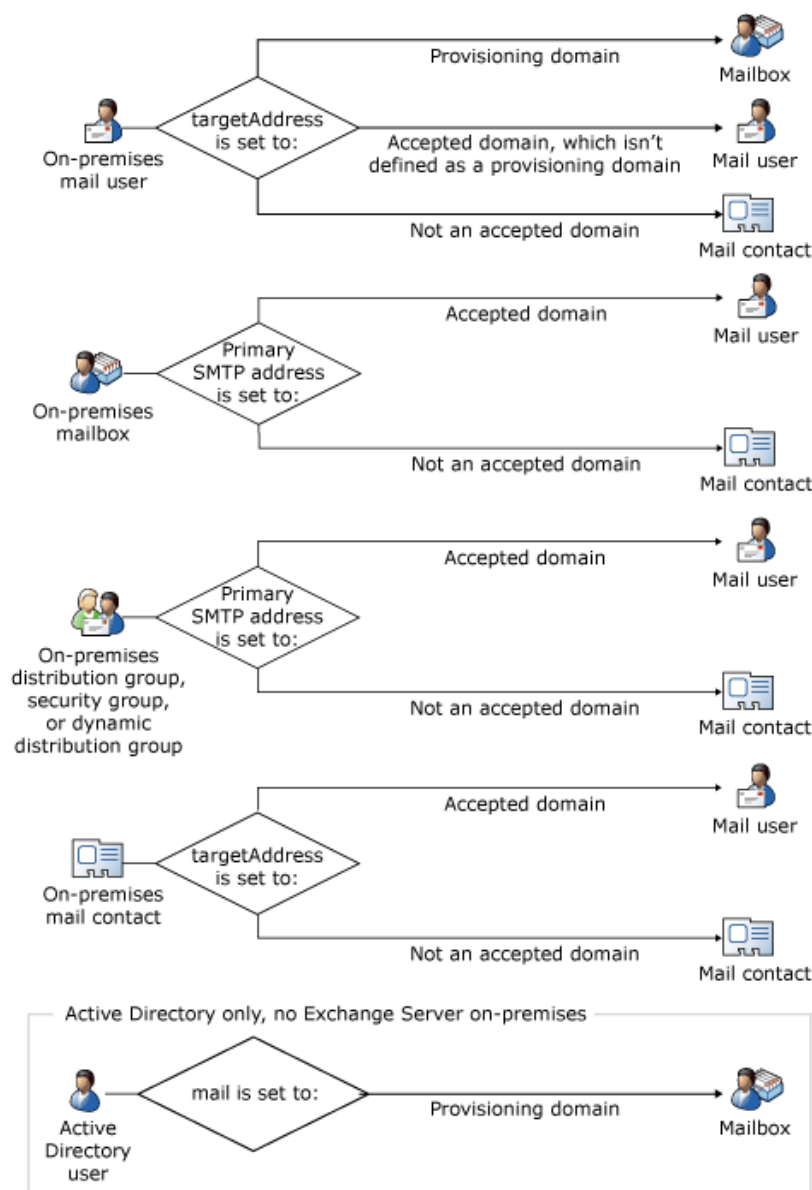
- DNS record type: CNAME
- Host: [redacted]
- Value: domains.live.com

[More information](#)



Creating Mail-Enabled Users

The following diagram shows the way that ILM and live@edu works



In our situation, we had the On-Premise Mail user, which were the students. Their targetaddress is set to the provisioning domain, so they have a mailbox created in live@edu

The staff have an on-premises mailbox, their SMTP is set to a different domain than the live@edu domain, however this has been added as an Accepted Domain. So they are created as a Mail-User in live@edu.

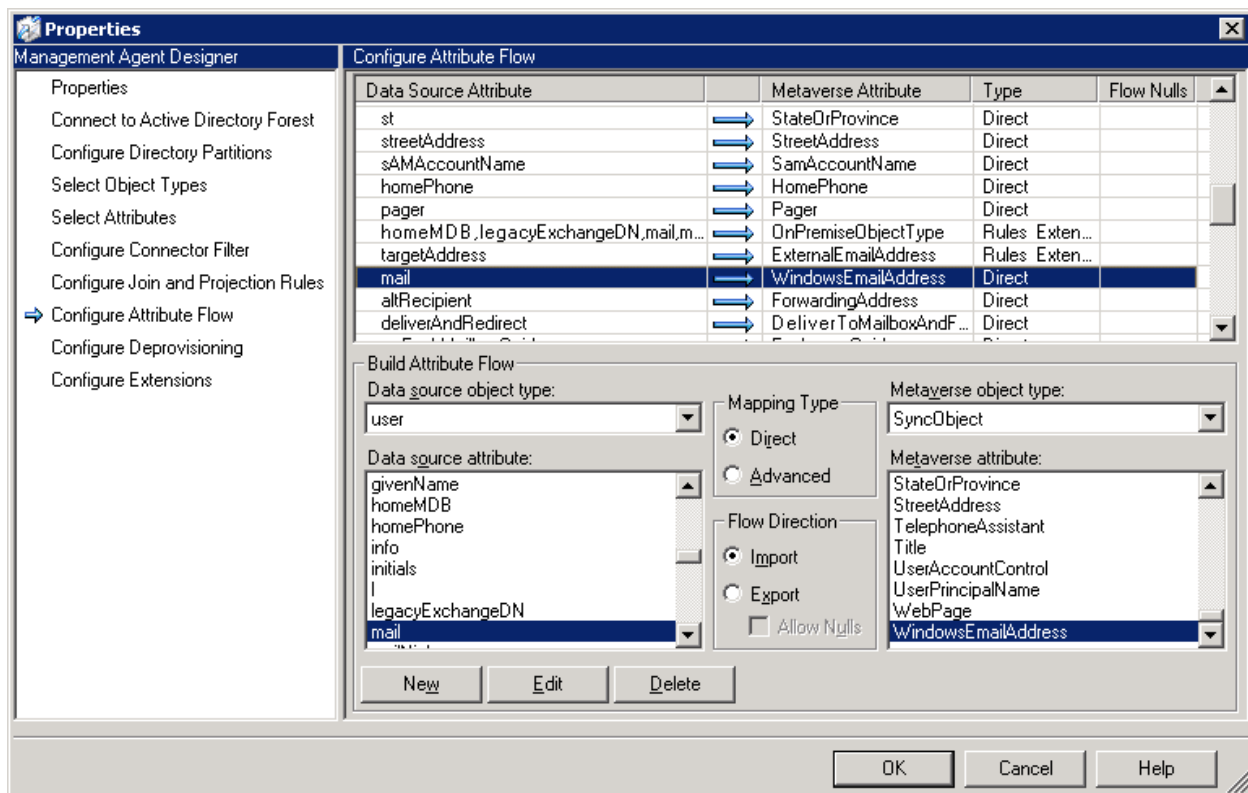
Appendix

SQL Server Issues

You can only have one ILM Installation per SQL Instance, so if you need to re-install ILM, you will need to manually remove the ILM instances from within the SQL Server Console. If you want to have more than one ILM server on premise, you should either install another SQL server, or create a separate instance on an existing SQL server.

MVWindowsLiveAttributeName

This important detail is found in the properties tab of the OnPremise Management Agent, under Configure Attribute Flow item. It shows the local attribute names and the corresponding attribute name in the ILM Metaverse.



Branding

Live@edu provides for you to create a customized 'look', in keeping with your School colours / logos / etc.

Huw Michael from Royal Holloway, University of London, has written an excellent piece about branding, which can be found at

<http://blogs.msdn.com/b/ukliveatedu/archive/2009/10/28/brand-me-happy.aspx>

Common problems

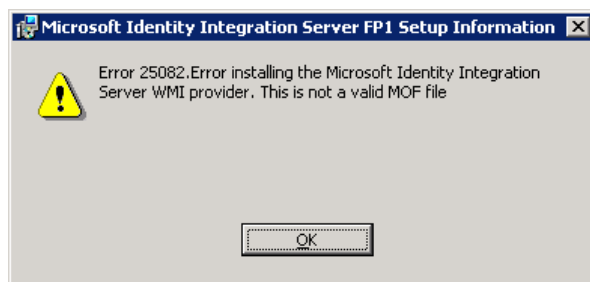
Passwords aren't syncing

In the context of the initial password, if you are running PCNS, you don't need to distribute the auto-generated passwords to your users. Instead, tell you users to change their password on their on-premises Active Directory account. PCNS will then change the password for the corresponding Outlook Live account. Users can then sign in to their Outlook Live account using the same password that they use for their on-premises Active Directory account. The Password Change Notification Service only notifies Outlook Live of Password **Changes**. When Outlook Live accounts are initially provisioned, the local user's existing password is **NOT** sent.

I see Access Denied error messages in Event Log

The most common cause of this is either the outlook live ID and password is not entered correctly in the Hosted Management Agent, or that the outlook live account has not actually been used to login to outlook live.

Error 25082



This error occurs if you attempt to install ILM onto a 64bit Server Operating System. ILM 2007 FP1 will only work on a 32 bit Server OS.

Misc

Another thing that caused me no end of grief was I had initially called named my ILM server 'ILM'. When it came to creating the service account, I named it ILM as well. This will not work.

Populating Student Email Address in Active Directory

To set the students' email field in Active Directory, you can simply select all of the accounts, right click, and select properties. You can then set the email field to %username%@<the.live.at.edu.domain> and this will change all of them at once. Eg:

