Install Microsoft Identity Manager for User Profiles in SharePoint Server 2016

**Summary**: What changed in User Profiles in SharePoint Server 2016? Has Forefront Identity Manager been removed from SharePoint Server 2016? What is Microsoft Identity Manager (MIM) and why is it taking the place of FIM? Is MIM built-in to SharePoint Server 2016 (short answer, No), or separate? What are my options for importing User Profiles in SharePoint Server 2016?

**Applies to**: SharePoint Server 2016 | SharePoint Server 2013 using MIM technology

**Published**: Sept 2015

### Contents

* [What is Microsoft Identity Manager?](#BKMK_WhatIsMIM1)
* [Choosing MIM](#BKMK_ChooseMIM)
* [Installing Microsoft Identity Manager (MIM)](#BKMK_InstallMIM)
* [Configuration scenarios](#BKMK_ConfigScene)

**Note**:

The solutions files referenced in this article are available for download [here](https://github.com/OfficeDev/PnP/tree/master/Solutions/UserProfile.MIMSync). You will need a GitHub login to access! See the section ‘Download the solutions files that you need’ for more details.

To download a free copy of Microsoft Identity Manager for installation, please navigate to the Microsoft Volume Licensing Service Center [here](https://www.microsoft.com/Licensing/servicecenter/default.aspx), login, and search on the product name.

# What is Microsoft Identity Manager?

Previous versions of SharePoint had a built-in copy of Forefront Identity Manager (FIM) that ran inside the SharePoint Server product. That version of FIM powered the User Profile Synchronization for products like SharePoint Server 2010, and 2013. But in SharePoint Server 2016, FIM has been removed in favor of Microsoft Identity Manager, which is the successor to the FIM technology. MIM is a separate server technology (not built-in to SharePoint Server). That means, if you have MIM running in your company, more than one SharePoint Sever 2016 farm can rely upon it.

It's also important to note, here, that Active Directory Import (sometimes called Active Directory Direct Import) is also included with SharePoint Server 2016, and is a User Profile Synchronization alternative that will not need a separate server installation. This means that SharePoint Server 2016 offers two options for User Profile Sync.

Which option is right for you?

|  |  |  |
| --- | --- | --- |
|  | Microsoft Identity Management server | Active Directory Import |
| Pros | 1. Flexibility allows for customized import.  2. Can be customized for bidirectional flow.  3. Imports user profile photos automatically.  4. Supports non-Active Directory LDAP sources.  5. Multi-forest scenarios are supported. | 1. Very fast and performant.  2. Known to be reliable (used by Office 365).  3. Configurable inside of SharePoint Central Administration. (Less complex.) |
| Cons | 1. A separate MIM server is recommended for use with your SharePoint Server farm.  2. The more customized the more complex the architecture, deployment, and management. | 1. Import is unidirectional (changes go from Active Directory to SharePoint Profile).  2. Import from a single Active Directory forest only.  3. Does not import user photos automatically.  4. Supports Active Directory LDAP only.  5. Multi-forest scenarios are not supported. |

**Tip** If you need details, or you need to set up **Active Directory Import** for your SharePoint Server installation? Try [these steps](https://technet.microsoft.com/en-us/library/jj219646.aspx).

# Choosing MIM

If you choose MIM, there are some prerequisites of which you should be aware. You will need:

1. A Windows Server 2012 R2 machine or virtual machine for the installation of MIM components.
2. SQL Server 2008 or above, to be installed either on the same machine as the MIM components, or remotely.

**Note** If you have SQL Server running on a separate server from MIM, you’ll need to install SQL Server native client (either for [2008](https://msdn.microsoft.com/en-us/sqlserver/aa937733.aspx) or [2012](https://www.microsoft.com/en-us/download/details.aspx?id=29065)) where you installed MIM.

1. You'll need to create a service account in your domain to run the MIM Synchronization Service. This account should have the “Log on as a service” and “Run as a service” permissions granted to it on the machine where the MIM Synchronization Service will be installed. (These permissions will normally be assigned automatically during setup of the service.)

**Important** If SQL is on the same server as MIM, you may use a local account for this service. However, if you use a remote SQL, you must use a domain account. If the account is in another domain from the SQL server, it must be in the same forest.

1. A domain user account must be created and [permissioned properly](https://technet.microsoft.com/en-us/library/hh296982.aspx) for use in the Active Directory Connector.
2. The account running setup for MIM must be a SQL Server Admin in SQL where the MIM sync database will be hosted. The account must have local administrator permissions on the machine where the MIM Synchronization service will be installed.
3. Be sure that any accounts you maintain and use for testing/validation of the process have an email address configured in Active Directory. This will help you verify the success of your MIM configuration after import.

# Installing Microsoft Identity Manager (MIM)

During these steps, you'll actually install three different elements essential to MIM. The first install will be of the MIM software, itself. You'll also need the SharePoint Management Agent.

1. First, download and install MIM to the server where you want to install.
2. Extract the .zip file and double-click Setup.exe. (Setup.exe is usually found in the SynchronizationService folder of the MIM media.)
3. Click Next > accept the end-user license agreement, and click Next through the feature selection screen. (You don't need to change the default selection.)
4. The next screen in the wizard will ask you to supply some information about the SQL Server you want MIM to use. Choose This Computer if the SQL installation is local, or type the remote SQL server name. Indicate if your SQL uses the default instance, or type the named instance. Click Next.
5. Next, you type the credentials you want to use to run the MIM service. You won't need to configure extra permissions or policies in SQL server for this account (whether SQL is local or remote).

**Note** If you're installing to a remote SQL Server, the SQL Server Native Client must already installed on the MIM server before you install the MIM Synchronization Service.

1. Next, set up the security groups that are needed for MIM to function. You can leave these as default if you wish, but in that case your security groups will be created on the local machine were MIM is being installed. If you have more than one machine configured to run MIM, you may want to create these security groups in Active Directory (AD). Do this in the same domain as the machines where MIM is configured, and enter the group names into this page of the wizard.
2. The nest step (firewall rules) is optional. We recommend you do not check the firewall rule checkbox.
3. Click to install MIM.

**Note** You may see a Warning here (Warning 25051). Click OK to continue.

1. Next, the wizard will create a backup of the encryption key set that it has created.

**Note** You will need to backup the keys generated at this point if you are to move to another database server. Save these keys to a secure location and make certain you backup the key file along with the database backup so they're both available in a disaster recovery scenario.

1. MIM installation should complete. You should log off and back onto your server again to ensure the MIM permissions are updated.
2. Once you log on again, ensure the MIM service is running on the server by going to Services (or Start or Windows key> Run > services.msc, you can also run *Get-Service FIM\** via Windows PowerShell) and then locating the Synchronization Service Manager.

## Install the SharePoint Management Agent

SharePoint Management Agent (SPMA) is an essential if you need to connect MIM to your SharePoint installation. We'll install and configure it now.

1. You need to install the SPMA on the same server as is running MIM. Install the latest SPMA bits from [here](http://www.microsoft.com/en-us/download/details.aspx?id=41164).
2. Click 'Download' and run the installation. You won't need to make any selections during this installation process.
3. Restart the Forefront Identity Manager Synchronization Service (again, you can get to this via Start or Windows key > Run > services.msc). You can also restart this service with Windows PowerShell via *Restart-Service FIMsy\**.
4. Once the installation completes, check Programs and Features in Control Panel on your MIM server to ensure you see 'Forefront Identity Manager SharePoint Connector'.
5. Launch the 'Synchronization Service' on the server to be certain that it opens. On a Windows Server 2012 R2 server, you'll find the icon for the Synchronization Service under Apps.

The Synchronization Service Manager will open on your MIM server. At this point you must configure MIM for use with SharePoint Server.

# Configuration scenarios

There are two general categories into which SharePoint Farm Administrators may find themselves in when they choose MIM.

1. **Category 1**: The first group consists of SharePoint Farm Administrators who have decided to set up a MIM server for use by their SharePoint Server 2016 farm, and who will be doing a fresh Profile Synchronization.
2. **Category 2**: The second group is made up of SharePoint Farm Admins who would prefer to take pre-existing Profile Synchronization configurations, created in SharePoint Server 2013 (or 2010), and convert them from FIM to MIM for reuse.

For configuration steps, please see:

* **Category 1**: [Deploy a new Microsoft Identity Management (MIM) server for User Profile Sync in SharePoint 2016](https://github.com/OfficeDev/PnP-Tools/blob/master/Solutions/UserProfile.MIMSync/Documentation/Set%20up%20User%20Profile%20Sync%20in%20a%20new%20SharePoint%20Server%202016%20farm%20using%20Microsoft%20Identity%20Manager.docx?raw=true)
* **Category 2**: [Convert Forefront Identity Manager (FIM) XML files to Microsoft Identity Management (MIM) service config files for User Profile Sync](https://github.com/OfficeDev/PnP-Tools/blob/master/Solutions/UserProfile.MIMSync/Documentation/Use%20Microsoft%20Identity%20Manager%20to%20set%20up%20User%20Profile%20Sync%20in%20an%20upgraded%20SharePoint%20Server%202016%20farm%20(using%20sync%20config%20fr.docx?raw=true)