

Quest® Migration Manager 8.15

Migrating to Microsoft Office 365



© 2024 Quest Software Inc. ALL RIGHTS RESERVED.

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

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

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

Quest Software Inc.

Attn: LEGAL Dept

4 Polaris Way

Aliso Viejo, CA 92656

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

Patents

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

Trademarks

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

Legend

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

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

Migration Manager Migrating to Microsoft Office 365

Updated - July 2020

Version - 8.15

Contents

Introduction	6
Migration Process Overview	6
Mail Redirection Technology Overview	10
Before You Begin	11
Checking the Requirements	11
Preparing Source Exchange Environment	12
Registering Exchange Organization as Migration Source	12
Preparing Microsoft Office 365 Environment	13
Assessing Microsoft Office 365 Deployment Readiness	13
Setting Up Company Domains in Microsoft Office 365	13
Creating Office 365 Administrative Accounts	13
Additional Configuration for the Public Folder Synchronization Account (Legacy Exchange Agents only)	16
Additional Configuration for the Public Folder Synchronization Account (MAGe only)	17
Performing Public Folder Synchronization with the Migration Agent for Exchange (MAGe)	17
Configuring Regional Settings for Office 365 Administrative Accounts	17
Disabling Calendar Repair Assistant	17
Registering Microsoft Office 365 as Migration Destination	17
Migrating Recoverable Items Subfolders	18
Migration to Microsoft Office 365	19
Provisioning User Accounts in Office 365	20
Installing Directory Migration Agent	20
Configuring Migration Pair	21
Managing User Passwords	21
Dividing Migration Scope into Collections	22
Choosing between Collection Types	22
Adding a Static Collection	23
Adding a Dynamic Collection	24
Configuring Object Matching	25
Adding a Matching Rule	25
Viewing Matched Objects	25
Performing Object Matching Explicitly	25
Breaking Object Matching	25
Configuring Attribute Mapping	26
Migrating Objects to Microsoft Office 365	26
Performing Pre-Migration Activities	27
Synchronizing Directories	28
Migrating Objects	28
Synchronizing Calendars	29

Setting Up a New Office 365 Calendar Synchronization Job	30
Step 1: Specifying Source Exchange Organization	30
Step 2: Specify Office 365 Tenant	31
Step 3: Specifying Migration Agent for Exchange Installation Settings	31
Step 4: Completing the Wizard	31
Adding a New Office 365 Calendar Collection	31
Step 1: Specifying General Options	31
Step 2: Specifying Workflow	32
Step 3: Populating the Collection	32
Step 4: Selecting Subscription Plan	33
Step 5: Configuring Office 365 Settings	33
Starting Calendar Synchronization	33
Synchronizing Public Folders	34
Public Folder Synchronization Caveats	35
Synchronizing Public Folders by Legacy Exchange Agents	37
Setting Up a New Public Folder Synchronization Job for Legacy Exchange Agents	37
Adding a Public Folder Collection	39
Starting Public Folder Synchronization by Legacy Exchange Agents	39
Synchronizing Public Folders by MAgE	40
Migrating Mailboxes	40
Setting Up a New Office 365 Mailbox Migration Job	40
Step 1: Specifying Source Exchange Organization	40
Step 2: Specify Office 365 Tenant	40
Step 3: Configuring Notification Messages	40
Step 4: Specifying Migration Agent for Exchange Installation Settings	41
Step 5: Completing the Wizard	41
Adding a New Office 365 Mailbox Collection	41
Step 1: Specifying General Options	41
Step 2: Specifying Workflow	42
Step 3: Populating the Collection	42
Step 4: Selecting Subscription Plan	42
Step 5: Configuring Mailbox Switch	42
Step 6: Configuring Office 365 Settings	43
Starting Mailbox Migration	43
Post-Migration Activities	44
Redirecting Email to Microsoft Exchange Online	44
Updating Outlook Profiles	44
Decommissioning Exchange Servers (Optional)	44
Switching to Other Directory Synchronization Tools (Optional)	45
Tracking the Migration Progress	46
Directory Migration	46
Calendar Synchronization	47
Mailbox Migration	48

Hybrid Migration Scenarios	49
Acquisition with a Hybrid	49
Establish Mail Flow to Source Exchange Organization	51
On-Premises Directory Migration	52
On-Premises Mailbox Migration	53
User Matching	53
Cloud Directory Migration	54
Cloud Mailbox Migration	55
Synchronize calendars	55
Migrate mailboxes	56
Perform mailbox switch	56
Complex Acquisition with a Hybrid	57
Establish Mail Flow to Source Exchange Organization	59
On-Premises Directory Migration	60
Synchronizing Users	60
Migrating Passwords	61
On-Premises Mailbox Migration	62
Cloud Directory Migration	63
User Matching	63
Cloud Mailbox Migration	64
Synchronize calendars	64
Migrate mailboxes	65
Perform mailbox switch	65
Reorganization or Upgrade with a Hybrid	66
Complex Reorganization or Upgrade with a Hybrid	67
Advanced Migration Topics	68
Supporting Single Sign-On (SSO) using Migration Manager	68
Interoperating with Microsoft Azure AD Connect	71
Troubleshooting Migration to Microsoft Office 365	73
Managing Migration Agent for Exchange	73
Other Problems: Checking the Logs	74
About us	75
Technical support resources	75

Introduction

Migration Manager provides tools for seamless migration to Microsoft Office 365 from on-premises Exchange environment.

We assume that you are familiar with Migration Manager concepts described in the Migration Manager Installation Guide, and that you have already installed the product, following the instructions provided in that guide. It is also recommended that you read the release notes for the current version of Migration Manager. The release notes contain information about specific product behavior, limitations, known issues, and workarounds that may be useful for planning and performing your migration.

For information which types of source Exchange environments are supported, see *Cloud Migration* subsection of [Source and Target Exchange Organizations](#).

Migration Process Overview

Migration Manager supports various scenarios of migrating your messaging infrastructure to Microsoft Office 365. This topic describes a basic migration when messaging infrastructure is completely moved to Microsoft Office 365.

i **NOTE:** Migration Manager supports various cloud migration scenarios that involves hybrid deployments. For detailed information how to implement them, see [Hybrid Migration Scenarios](#).

The basic migration to Microsoft Office 365 consists of the following main stages:

1. Preparing on-premises Exchange and Microsoft Office 365 environments for migration.
2. Synchronizing entire Active Directory with Microsoft Office 365 to provide for co-existence of Global Address List and to provision users in Microsoft Office 365.
3. Synchronizing calendars including free/busy information to Microsoft Exchange Online.
4. Synchronizing public folders with Microsoft Office 365.
5. Migrating and switching mailboxes to Microsoft Office 365.
6. Re-migrating some Active Directory objects to set specific settings for them (optional).
7. Performing post migration activities like redirecting email, updating Outlook profiles, etc.

i **TIP:** If you plan to implement Single Sign-On (SSO) for Microsoft Office 365, or you already use Microsoft Azure AD Connect to synchronize user accounts with Microsoft Office 365, review information in the [Advanced Migration Topics](#) section.

The table below describes the steps that you need to perform in each stage of migration and the results that you get after you complete those steps.

Stage	What to Do	Result	Tool to Use
1	<ol style="list-style-type: none"> 1. Check the system requirements 2. Prepare the source Exchange environment 3. Prepare the Microsoft Office 365 environment 	Both source Exchange and Microsoft Office 365 environments are ready for migration	N/A
2	<ol style="list-style-type: none"> 1. Install the Directory Migration Agent 2. Create a migration pair of Active Directory domain and Microsoft Office 365 3. Configure matching rules for migration pair if default ones do not satisfy your needs 4. Configure mapping rules for migration pair if default ones do not satisfy your need 5. Create a dynamic collection including all objects from Active Directory domain 6. Configure object matching for the dynamic collection 7. Enable coexistence for the dynamic collection 	<ul style="list-style-type: none"> • All objects from source Active Directory are created in Microsoft Office 365 and kept in sync • A unified global address list (GAL) is established between Active Directory domain and Microsoft Office 365 • Mail redirection is configured for users in Microsoft Office 365 • Emails containing password for connecting to Microsoft Office 365 are sent to users' on-premises mailboxes, so that users can sign in to Microsoft Office 365 	Migration Manager for Active Directory (Microsoft Office 365) console
3	<ol style="list-style-type: none"> 1. Set up a calendar synchronization job 2. Create calendar collections 3. Start the corresponding agents to begin calendar synchronization 	Calendars including users' free/busy information are kept in sync with Microsoft Exchange Online.	Migration Manager for Exchange console
4	<p>Refer to For synchronization by legacy Exchange Agents:</p> <ol style="list-style-type: none"> 1. Set up a public folder synchronization job 2. Add public folder collections 	Public folders are kept in sync with Microsoft Office 365.	Migration Manager for Exchange console - OR - Migration Agent For Exchange and

Stage	What to Do	Result	Tool to Use
	<p>3. Start the corresponding agents to begin public folder synchronization</p> <p>- OR-</p> <p>For one-way or two-way public folder synchronization using Migration Agent For Exchange and MMEX PowerShell Module:</p> <ul style="list-style-type: none"> Refer to Public Folder Synchronization (MAgE) document for step by step instructions on how to configure and manage public folder synchronization. 		MMEX PowerShell Module
5	<ol style="list-style-type: none"> Set up a mailbox migration job Create mailbox collections Start the corresponding agents to begin mailbox migration 	<ul style="list-style-type: none"> All desired mailboxes are being migrated to Microsoft Exchange Online Mailboxes are switched as they are successfully migrated. After mailbox switch the mail redirection is changed to opposite direction Corresponding user accounts become mailbox-enabled. This allows migrating Exchange specific attributes for them at stage 5. 	Migration Manager for Exchange console
6(optional)	<ol style="list-style-type: none"> Create static collection containing users whose mailboxes you already provisioned to Microsoft Exchange Online Configure matching rules for the collection if necessary Configure mapping rules for the collection if necessary Migrate the collection to Microsoft Office 365 	<p>The following mailbox attributes are migrated to Microsoft Office 365:</p> <ul style="list-style-type: none"> The mailbox and the Send As permissions; The linked attributes such as group membership, the Send On Behalf permission, the publicDelegates attribute, and the others. <p>NOTE: See the Mailbox Permissions Processing Considerations topic</p>	Migration Manager for Active Directory (Microsoft Office 365) console

Stage	What to Do	Result	Tool to Use
		below for more details on mailbox permission migration.	
7	<ol style="list-style-type: none"> 1. Redirect email to Microsoft Exchange Online 2. Update Outlook profiles 3. Decommission Exchange servers (optional) 4. Switch to other directory synchronization tools (optional) 	<ul style="list-style-type: none"> • Mail data is redirected to Microsoft Office 365 • Outlook profiles are updated using Client Profile Updating Utility • Exchange infrastructure is decommissioned (optional) • Directory is synced with the other synchronization tools 	Client Profile Updating Utility for updating Outlook profiles

Exchange Resource Forest Migration Considerations

If your Exchange organization is deployed in an Exchange resource forest then consider the following:

- You should [provision users](#) directly from Exchange resource forest instead of the corresponding Active Directory authentication forest.
- Despite all user accounts in the Exchange resource forest are disabled by default, Migration Manager for Active Directory creates them enabled in Microsoft Office 365.
- After you [provision users](#), you may start [synchronizing calendars](#) and [migrating mailboxes](#) from the Exchange resource to Microsoft Office 365 forest using Migration Manager for Exchange.
- If you need to [migrate](#) specific attributes that are presented only in the corresponding Active Directory authentication forest, you can do so by creating a separate [migration pair](#) of that authentication forest and Microsoft Office 365 in Migration Manager for Active Directory (Microsoft Office 365).

Mailbox Permissions Processing Considerations

Migration Manager can synchronize mailbox permissions and the **Send As** permission during synchronization and migration to Microsoft Office 365. So if a source user can send mail messages as another user account and/or manage mailboxes of other users, the corresponding target user will have the same rights.

Take into account the following:

- The **Rollback Task** cannot revert changes of the **Send As** and mailbox permissions that were made during migration or synchronization.
- If any of these permissions is removed on the source, this action will not be synchronized on the target during the next migration or synchronization session.
- If a source user has the **Deny Send As** permission, the corresponding target user will have no **Send As** permission (neither **Allow** nor **Deny**) after synchronization. If the user has the Allow Send As permission for any mailbox on the source and a membership in a group that has the Deny Send As permission for the same mailbox, this user will have the **Allow Send As** permission on the target.
- The **Send As** permissions are synchronized only for mailboxes. If a user has the **Send As** permission for a group (i.e. is able to send emails from this group), the corresponding target user will not have this permission.

- This functionality is not supported in the Exchange resource forest when permissions are granted to users or groups from the account forest.

Mail Redirection Technology Overview

For uninterrupted user collaboration during the migration to Microsoft Office 365, users in source Exchange organization and Microsoft Office 365 should see other users' mailboxes in their Global Address Lists (GALs). All mail sent to the user should arrive to the mailbox he or she is currently using, no matter which mailbox it was sent to. To achieve this, mail should be automatically forwarded to the currently-used mailbox from the other mailbox. For that, Migration Manager establishes mail redirection between source Exchange servers and Microsoft Office 365 using the Migration Manager for Active Directory redirection technology as follows:

- Before a [mailbox switch](#), all new mail is delivered to the source user mailbox and redirection is configured for the corresponding cloud user mailbox.
- After the [mailbox switch](#), all new mail is delivered to the cloud mailbox, redirection on the cloud mailbox is disabled, and redirection is configured for the source mailbox

The process of mail redirection is fully automated by Migration Manager for Active Directory; therefore no additional configuration activities are required to be performed.

Before You Begin

Before you start the migration, read the following:

- Checking the Requirements
- Preparing Source Exchange Environment

RECOMMENDATION: Subscribe to Microsoft Office 365 in Advance

If you do not already have a Microsoft Office 365 account, consider signing up at <http://office.microsoft.com> before you start migration preparations. This will help avoid delays and interruptions during migration.

Checking the Requirements

Basic Authentication in Exchange Online is now deprecated by Microsoft. Migration Manager supports modern authentication (based on OAuth 2.0) for migration to Microsoft Office 365 tenants, for all scenarios supported by MAgE. This support is available in MMEx 8.15 with the application of public update 20200813EX or later. In addition, MMAD 8.15 plus public update 20221207 or later are required for use of the MMAD Directory Migration Agent (DMA).

i **IMPORTANT:** Now that Basic Authentication is deprecated by Microsoft, public folder synchronization by legacy Exchange agents is no longer supported. Public folder synchronization should be performed by MAgE.

For details about the access privileges and software required for migration to Microsoft Office 365, refer to the following sections in the *System Requirements and Access Rights* document:

- Migration to Microsoft Office 365
- Directory Migration Agent
- Accounts Used for Migrating to Office 365

Supported Microsoft Office 365 Plans

Migration Manager ensures migrating to tenants with Microsoft Office 365 Enterprise plans (plan E1, plan E3 and plan E5) and standalone Exchange Online plans 1 and 2. For more details about Microsoft Office 365 and Exchange Online plans go to <https://products.office.com/en/business/compare-more-office-365-for-business-plans> and <https://products.office.com/en/exchange/compare-microsoft-exchange-online-plans> respectively.

Microsoft Office 365 tenants with Exchange Online Kiosk plan are not supported as a migration destination.

To support mailbox migration to Microsoft Office 365 tenants by MAgE, Microsoft Office 365 plan should have the following features:

- EWS Application support
- EWS Connectivity support

In case your used Microsoft Office 365 plan has these features, please contact Quest Support to check if this plan can be supported.

i | **NOTE:** Migration to Office 365 China tenants (operated by 21Vianet) and Office 365 Germany tenants (operated by T-Systems) is not supported.

Preparing Source Exchange Environment

The Migration Manager documentation set includes documents about preparing the different types of supported Exchange environments. Please refer to the document that deals with your particular Exchange version.

For the purposes of migration to Office 365, follow the sections in the document that describe:

1. Configuring the Exchange account
2. Configuring the source Active Directory account
3. Backing up the Exchange infrastructure (optional)
4. Setting up connection with the target Exchange organization.

Registering Exchange Organization as Migration Source

After you configured your Exchange environment you need to register your Exchange organization as migration source in Migration Manager for Exchange console. For that, right-click the **Source Exchange Organizations** node of the management tree and select **Add Source Exchange Organization**. This starts graphical wizard that guide you through the registration process.

The wizard prompts you to specify the accounts that will be used to connect to the servers where Migration Manager for Exchange components are installed. The accounts you specify should have the appropriate privileges, as detailed in the System Requirements and Access Rights document. Specified accounts are used by default with all the servers of the registered Exchange organization.

i | **NOTE:** If needed, you can modify the connection settings for each of the registered Exchange servers using the **General** page of the appropriate server **Properties** dialog box.

Preparing Microsoft Office 365 Environment

You need to perform a few steps in order to prepare you Microsoft Office 365 tenant for migration:

Assessing Microsoft Office 365 Deployment Readiness

To analyze and prepare your on-premises environment for an Office 365 deployment, use the Microsoft Office 365 Deployment Readiness Tool in accordance with the Microsoft Office 365 Deployment Guide.

To get the Microsoft Office 365 Deployment Guide for Enterprises, go to <http://community.office365.com/en-us/f/183/p/1541/5095.aspx>. The tool can be downloaded from <http://community.office365.com/en-us/f/183/p/2285/8155.aspx>.

Setting Up Company Domains in Microsoft Office 365

You need to add each email domain you want to migrate to Microsoft Office 365 as an accepted domain of your Microsoft Office 365 tenant. The migration service will then use the SMTP addresses of your on-premises mailboxes to create the corresponding email addresses for the new Office 365 mailboxes.

For information on adding company domains to Microsoft Office 365, read [Adding domains and users to Office 365](#) article.

Creating Office 365 Administrative Accounts

You need to create at least four separate administrative accounts which will be used during migration for one of the following tasks:

- [Provisioning user accounts in Office 365](#)
- [Synchronizing calendars](#)
- [Migrating mailboxes](#)
- [Synchronizing public folders](#)

Task	Requirement	More Info
Provisioning user accounts in Office 365	<ul style="list-style-type: none">• Exchange administrator user role• User Administrator user role	Refer to the Requirements for provisioning user

Task	Requirement	More Info
	<ul style="list-style-type: none"> • ApplicationImpersonation role • Mail Recipients role • Microsoft Exchange Online license • Default UPN 	accounts in Office 365
Synchronizing calendars	<ul style="list-style-type: none"> • User Administrator user role • ApplicationImpersonation role • Mail Recipients role 	Refer to the Requirements for synchronizing mailboxes, calendars and public folders in Office 365
Migrating mailboxes	<ul style="list-style-type: none"> • Microsoft Exchange Online license • Default UPN 	
Synchronizing public folders	<ul style="list-style-type: none"> • User Administrator user role • ApplicationImpersonation role • Mail Recipients role • Microsoft Exchange Online license • Default UPN • The account should be associated with the primary hierarchy public folder mailbox • The account should be granted by Owner permissions on all public folders 	Refer to the Requirements for synchronizing mailboxes, calendars and public folders in Office 365 and to the Additional Configuration for the Public Folder Synchronization Account

Requirements for provisioning user accounts in Office 365

The administrative account must have the **Exchange administrator**, **User Administrator** user roles and **ApplicationImpersonation** and **Mail Recipients** roles in the Microsoft Office 365 tenant. A Microsoft Exchange Online license must be issued for this administrative account. This account must have the default UPN suffix <tenant_name>.onmicrosoft.com. To create the administrative account you should perform the following:

- Manually grant **User Administrator**, **Exchange administrator** user roles and **ApplicationImpersonation**, **Mail Recipients** roles to the accounts that already have a Microsoft Exchange Online license

To grant existing account the User Administrator and Exchange Administrator user roles

1. Log on to any computer running Microsoft Windows 7 (x64 edition) or Microsoft Windows Server 2008 R2 operating system.
2. Install Microsoft Online Services Sign-In Assistant (64-bit version). To get installation instructions and download link, go to <http://technet.microsoft.com/en-us/library/jj151815.aspx>.

3. Grant the account **User Administrator** and **Exchange Administrator** user roles:

```
Import-Module MSOnline

$cred = Get-Credential

Connect-MsolService -Credential $cred

Add-MsolRoleMember -RoleName 'User Administrator' -RoleMemberEmailAddress
<User E-mail address>

Add-MsolRoleMember -RoleName 'Exchange Administrator' -RoleMemberEmailAddress
<User E-mail address>
```

i **NOTE:** The role object IDs can be used instead of the role name:

```
Add-MsolRoleMember -RoleObjectId 'fe930be7-5e62-47db-91af-98c3a49a38b1' -
RoleMemberEmailAddress <User E-mail address>

Add-MsolRoleMember -RoleObjectId '29232cdf-9323-42fd-ade2-1d097af3e4de' -
RoleMemberEmailAddress <User E-mail address>
```

4. Grant the account **ApplicationImpersonation** and **Mail Recipients** role as follows:

```
$proxy = New-PSSessionOption -ProxyAccessType IEConfig

$session = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri
https://ps.outlook.com/powershell/ -Credential $cred -Authentication Basic -
AllowRedirection -SessionOption $proxy

Import-PSSession $session

New-RoleGroup -Name 'QMMAD Accounts' -Roles 'ApplicationImpersonation', 'Mail
Recipients' -Members <User>

Remove-PSSession $session
```

Requirements for synchronizing mailboxes, calendars and public folders in Office 365

A Microsoft Exchange Online license must be issued to these administrative accounts. These accounts must have the default UPN suffix <tenant_name>.onmicrosoft.com. Also they must have the **User Administrator**, **Mail Recipients** and **ApplicationImpersonation** roles in the Microsoft Office 365 tenant. There are two options how to grant the required roles:

1. Manually grant **ApplicationImpersonation** and **Mail Recipients** roles to the accounts that already have a Microsoft Exchange Online license and the **User Administrator** role in Microsoft Office 365 as specified [above](#).
2. Use the PowerShell script that creates accounts in Microsoft Office 365, issues Microsoft Exchange Online licenses to these accounts and grants the accounts required roles. That script is attached to the following Migration Manager for Exchange Knowledge Base article: <https://support.quest.com/migration-manager-for-exchange/kb/255600/how-to-create-o365-service-accounts-with-required-permissions>.

i **NOTE:** For speeding up migration performance, you will need to use multiple administrative accounts for calendar synchronization and mailbox migration. Using the script allows automating account creation and role assignment.

To create administrative accounts with User Administrator user role using the `CreateQSGranularPermissionAdminAccountsInMSOLModule.ps1` script

You can create the accounts via PowerShell with the minimum required permissions acceptable.

To download `CreateQSGranularPermissionAdminAccountsInMSOLModule.ps1` script and see step-by step usage instructions refer to Migration Manager for Exchange Knowledge Base article:

<https://support.quest.com/migration-manager-for-exchange/kb/255600/how-to-create-o365-service-accounts-with-required-permissions>.

CAUTION: The user account that you specify for the `CreateQSGranularPermissionAdminAccountsInMSOL` cmdlet must have the **Global Administrator** role in **Microsoft Office 365**.

The administrative accounts specified in .CSV file will be created in Microsoft Office 365 and granted the **User Administrator**, **Mail Recipients**, and **ApplicationImpersonation** user roles.

Additional Configuration for the Public Folder Synchronization Account (Legacy Exchange Agents only)

For the account you are going to use for public folder synchronization by legacy Exchange agents, the following steps are also required:

1. Associate the account with the primary hierarchy public folder mailbox. For that, in the Office 365 Exchange admin center, do the following:
 - a. Create a new PowerShell session with Office 365:

```
$cred = Get-Credential
$proxy = New-PSSessionOption -ProxyAccessType IEConfig
$session = New-PSSession -ConfigurationName Microsoft.Exchange -
ConnectionUri https://ps.outlook.com/powershell/ -Credential $cred -
Authentication Basic -AllowRedirection -SessionOption $proxy
Import-PsSession $session
```
 - b. Associate Office 365 Administrative Account with the primary hierarchy mailbox:

```
Set-Mailbox -Identity<Office_365_Administrative_Account>-
DefaultPublicFolderMailbox<Primary_Hierarchy_Mailbox>
```
 - c. Finally, close the PowerShell session:

```
Exit-pssession
Remove-pssession $session
```
2. Grant this account **Owner** permissions on all public folders you want to synchronize.
 - a. Click **public folders**.
 - b. Select the root folder.
 - c. In the toolbar on the right, click the ellipsis icon and select **Root permissions**.
 - d. Add the necessary account and assign it the **Owner** role. Select the **Apply changes to this public folder and all its subfolders** option and save your changes.

CAUTION: At this time, the account you specify in the properties of your Office 365 target organization is used for public folder synchronization. By default, this account registers Microsoft Office 365 as the migration destination.

Additional Configuration for the Public Folder Synchronization Account (MAgE only)

For the account you are going to use for public folder synchronization by MAgE refer to [Public Folder Synchronization \(MAgE\)](#) document.

Performing Public Folder Synchronization with the Migration Agent for Exchange (MAgE)

Refer to the [Public Folder Synchronization \(MAgE\) Reference Guide](#) for instructions on how to perform public folder synchronization with the enhanced Migration Agent for Exchange (MAgE).

Configuring Regional Settings for Office 365 Administrative Accounts

You should configure regional settings for [administrative accounts](#) that you are going to use for the migration. If they remain unconfigured, this may cause error messages about an incorrect time zone during migration. To configure these settings:

1. Sign in to Microsoft Office 365 using the account that you are going to use for the migration.
2. Click the **Outlook** link at the top of the page. You will be prompted to set the time zone and language.

Disabling Calendar Repair Assistant

It is necessary to disable Calendar Repair Assistant (CRA) for all user mailboxes that will be involved in migration for the whole period of migration. To do that for each mailbox in your organization, invoke the following cmdlet:

```
Get-Mailbox -ResultSize unlimited | Set-Mailbox -CalendarRepairDisabled $true
```

Registering Microsoft Office 365 as Migration Destination

In the final step of preparing the Microsoft Office 365 environment, you need to register the new migration destination in the Migration Manager for Exchange console. For that, right-click the **Target Exchange Organizations** node of the management tree and select **Add Office 365 as Target Organization**. You are prompted to supply the following:

1. The display name that will stand for Microsoft Office 365 in the Migration Manager for Exchange console
2. The default [administrative account](#) under which to access Microsoft Office 365.

! CAUTION:

- **A Microsoft Exchange Online license must be issued to this account.**
- **This account must have Global Administrator role in Microsoft Office 365.**

i | **NOTE:** If you do not yet have a Microsoft Office 365 subscription, click the link in the dialog box.

After you click **Finish**, a node representing Microsoft Office 365 is added to the management tree. This node provides the tools you need for the migration.

Migrating Recoverable Items Subfolders

Content of the following subfolders from source Recoverable Items folders can be migrated to target:

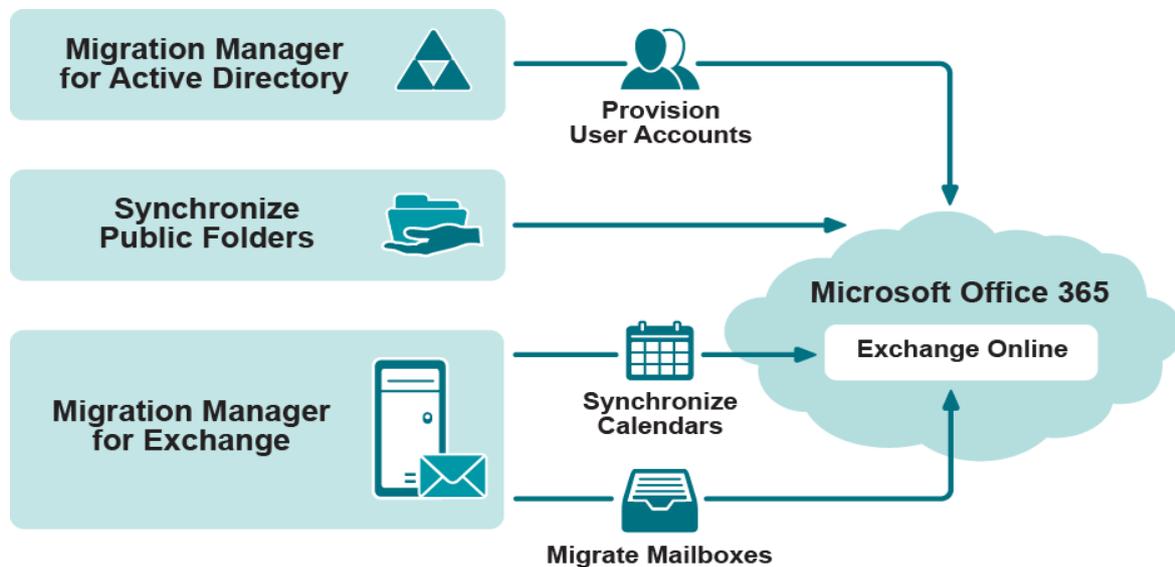
- Deletions
- Purges
- DiscoveryHolds
- Versions

Refer to [User Guide](#) for instructions on how to prepare your environment and enable this feature.

Migration to Microsoft Office 365

Migration involves migrating Active Directory objects (such as users, contacts and groups) from the source domain to Microsoft Office 365, synchronizing calendars and migrating mailboxes from on-premises Exchange organization to Microsoft Exchange Online.

While migrating to Microsoft Office 365 you will need to use both Migration Manager for Active Directory and Migration Manager for Exchange as shown in the figure below:



Migration to Office 365 Considerations:

- Migration Agent for Exchange cannot process a message that is larger than 40MB. This limitation is set by Office 365 Exchange Web Services.
- If you want to change an agent instance for a collection that is being processed, you should stop the agent, wait until the current session is finished and then specify the agent instance you need.
- If a mailbox is added to more than one collection via groups or organizational units, the Migration Agent for Exchange processes this mailbox only for the collection that is the first in the synchronization order.
- One instance of Migration Agent for Exchange cannot process collections from on-premises Exchange migration and Microsoft Office 365 migration projects at the same time. You will need separate instances of Migration Agent for Exchange to process these migration projects.
- Likewise, one set of public folder synchronization agents cannot process collections from on-premises Exchange migration and Microsoft Office 365 migration projects at the same time.

Refer to [Public Folder Synchronization Caveats](#) for public folder synchronization considerations.

Provisioning User Accounts in Office 365

In the first step of migrating to Microsoft Office 365, you need to provision user accounts in Microsoft Office 365. All steps from this section should be performed in Migration Manager for Active Directory (Office 365) console:

- [Installing Directory Migration Agent](#)
- [Configuring Migration Pair](#)
- [Dividing Migration Scope into Collections](#)
- [Matching Objects](#)
- [Configuring Attribute Mapping](#)
- [Migrating Objects to Microsoft Office 365](#)

CAUTION: Migration Manager for Active Directory always creates user accounts enabled in Microsoft Office 365 regardless of their states in Active Directory.

Installing Directory Migration Agent

Both migration and synchronization tasks are handled by the specific engine called Directory Migration Agent (abbreviated to DMA). Before you start your migration activities, be sure to install at least one DMA instance in your environment. For that, perform the following:

1. Run the Migration Manager for Active Directory (Office 365) console.
2. Select **Directory Migration** node in the management tree of the Migration Manager for Active Directory (Office 365) console.
3. Go to **Agents** tab, and in the **Action Items** pane click the **Install Agent** item to the start the **Install Agent** wizard.
4. Complete the wizard by specifying the following:
 - a. A server where DMA should be installed.
 - b. User credentials under which DMA should be installed and run.

NOTE: A server where you plan to install DMA must satisfy specific system requirements listed in the corresponding section of the *System Requirements and Access Rights* document.

Migration Manager for Active Directory (Office 365) uses Microsoft Graph API to access Azure Active Directory. Administrative consent is required in order to grant the "Quest Migration Manager for Active Directory" application access to the tenant data.

Consent can be granted at the time of adding a Migration Pair or in advance using this hyperlink https://login.microsoftonline.com/###-####-###-####/adminconsent?client_id=8edd986e-2f01-4f62-84d2-34576b05fc01 where **###-####-###-####** must be replaced with an actual tenant id (which can be obtained via the Azure Admin console).

In order to grant admin consent, the account needs one of the following roles: Global Administrator or Privileged Role Administrator.

Once the Application has been granted access, the Migration Manager service account can function with the following minimal set of roles:

- For Matching only: Exchange Administrator role
- For Migration, the following minimal set of roles: Exchange Administrator, Directory Readers, Directory Writers

Configuring Migration Pair

All migration activities are performed between pairs of Active Directory domains and Microsoft Office 365 tenants. Such pairs along with corresponding configuration settings are referred as migration pairs in the console.

The **first time** you create a migration pair, an additional step is needed to obtain and install the latest version of the Microsoft Graph API, used to communicate with Microsoft 365. Microsoft PowerShell is used for this step. Once installed, this step is not required when setting up subsequent migration pairs.

To create a new migration pair, perform the following:

1. Select the **Directory Migration** node in the management tree of the Migration Manager for Active Directory (Office 365) console.
2. From the **Home** tab, under **Action Items**, choose the **Create Migration Pair** button.
3. Alternatively, go to the **Migration Pairs** tab, and in the **Action Items** pane choose the **Create Migration Pair** item.
4. In the **Create Migration Pair** wizard specify the Active Directory domain and configuration settings to use for connecting to it. Those settings include the following:
 - Active Directory domain
 - User credentials under which to connect to Active Directory
 - SSL configuration options
 - Preferred domain controller and global catalog (optionally)
5. Specify the settings to use for connecting to a Microsoft Office 365 tenant. Those configuration settings include the following:
 - User credentials under which to connect to Microsoft Office 365
 - Proxy server and credentials, if necessary.
6. If prompted (when using MFA or using Graph app for the first time across multiple tenants), sign into the Graph API to create the necessary connection to Microsoft 365.

i | **NOTE:** You can later edit the migration pair settings or delete it using the corresponding action items on the migration pair node in the management tree.

When you specify a set of configuration settings, it is saved as a specific entity called connection. The connection is a set of configuration settings that are used to access the Active Directory domain or Microsoft Office 365 tenant. You can use connections in future migrations instead of reentering the configuration settings.

Managing User Passwords

By default, when Migration Manager creates a user in Microsoft Office 365 during migration process, it generates a temporary password for the user and then sends it by email. However, you can choose not to send passwords to users. For that, select a migration pair node in the management tree, click the **Edit Initial Password Settings** item in the **Actions** pane and select the desired option in the dialog box opened.

CAUTION: Take the following into consideration:

- If you select not to send passwords to users, the Microsoft Office 365 administrator will need to reset and send passwords manually so that users can sign in to Microsoft Office 365.
- Passwords are not generated for user accounts created in federated domain, as such users sign in to Microsoft Office 365 using their domain credentials through Single Sign-On (SSO). Moreover, the Reset Password task does not affect users from federated domain.

TIP: You will be able to reset passwords for migrated users later using the **Reset Password** action item available on the [collection](#) node level. Note that when you reset password for a user using Migration Manager for Active Directory, the generated password is sent to the user by email automatically.

Dividing Migration Scope into Collections

After you have successfully added a [migration pair](#), you need to specify objects which you plan to synchronize with or migrate to Microsoft Office 365. Migration Manager for Active Directory organizes the objects into collections. A collection is a set of objects that are migrated to Microsoft Office 365 at the same time by the same instance of Directory Migration Agent.

Considerations

When dividing migration scope into collections you should consider the way that linked attributes (such as group membership) get resolved:

- Linked attributes always get resolved in the scope of the collection. For example, if you migrate a group and its members within the same collection, the membership will get migrated.
- Linked attributes are also resolved for previously migrated objects. For example, if you first migrate users and then migrate a group, the group will be migrated with its membership.
- Backlinks (such as "member of") are not updated across collections. For example, if you first migrate a group and then in other collections migrate its members, the newly migrated accounts will not get added to the target group. If you have to migrate a group before its members, you can restore the membership by either re-migrating the group or doing full re-synchronization.

Choosing between Collection Types

Migration Manager for Active Directory has two types of collections described in the table below:

Collection Type	Used to	Populated
Static	<ul style="list-style-type: none">• Migrate a group of objects with non-default mapping or matching rules• Re-migrate groups after their members were migrated to Microsoft Office 365 to resolve group membership	Directly with objects, by executing queries or by importing objects from .CSV files

Collection Type	Used to	Populated
	<ul style="list-style-type: none"> Synchronize a group of objects to keep their attributes actual in Microsoft Office 365 Re-migrate users after their mailboxes have been created in Microsoft Office 365 for migration of the following mailbox attributes to Microsoft Office 365: <ul style="list-style-type: none"> The mailbox and the Send As permissions; The linked attributes such as group membership, the Send On Behalf permission, the publicDelegates attribute, and the others. <p>NOTE: See the Mailbox Permissions Processing Considerations for more details on mailbox permission migration.</p>	
Dynamic	Synchronize all objects from Active Directory domain with Microsoft Office 365 to maintain a unified global address list (GAL)	By specifying a particular container in Active Directory domain and a filter to apply to it Note that dynamic collections are updated automatically when content of the container is changed.

The two following sections will describe how to create and populate static collections and dynamic collections.

i **NOTE:** Dynamic collections can be involved only in directory synchronization tasks and cannot be used for migration tasks. For more information on migration and synchronization differences, see [this](#) section.

! **CAUTION:** Prior to creating any collections, review and configure if necessary [matching](#) and [mapping rules on migration pair level](#). Those rules will affect all your collections created afterwards.

Adding a Static Collection

To add a static collection, select your migration pair in the management tree, open the Collections tab and click the New Collection item in the Actions pane and then specify the following:

1. A name for the static collection
2. The instance of Directory Migration Agent that should process this collection
3. Whether [coexistence](#) should be enabled for the collection immediately after collection is created.

! **CAUTION:** Select to enable collection for coexistence only if you are sure that default [matching](#) and [mapping rules](#) for this collection satisfy your needs.

To populate the collection with objects use **Add Objects**, **Query Objects** and **Import Objects** action items from the **Home** tab according to the table below.

Action Item	Do What	Useful When
Add Objects	Adds objects and containers directly from Active Directory	You want to add objects that can be easily located in the Active Directory.
Query Objects	Filters objects from Active Directory by specific attribute values or add objects that match specified LDAP query	You want to select mailboxes based on some custom criteria: for example, mailboxes of all users that have a specific Active Directory attribute.
Import Object	Imports objects from CSV file. File should contain one column with attribute name in the first row and appropriate attribute values in the subsequent rows. For example: Name User1 User2 User3	You already have a list of objects with specific attributes which you want to add to a collection.

To verify that the static collection is populated correctly or to make any adjustments to the collection membership, go to the **Objects** tab and check the resulting list of objects.

To review and configure if necessary [matching](#) and [mapping](#) rules for the collection, go to the **Matching** or **Mapping** tabs, respectively.

Adding a Dynamic Collection

To add a dynamic collection, select your migration pair in the management tree, click the New Dynamic Collection item in the Actions pane and then specify the following:

1. A name for the dynamic collection
2. The instance of Directory Migration Agent that should process this collection
3. Whether [coexistence](#) should be enabled for the collection immediately after collection is created
4. Container to search objects in and a filter to refine results.

i | **TIP:** Click **Preview** to display a resulting list of found objects that will be added to the dynamic collection.

To verify that the dynamic collection is populated correctly, go to the **Objects** tab and check the resulting list of objects.

If you need to change container which objects should be synchronized or edit applied filter, click the **Change Scope** action item on the **Object** tab and perform necessary adjustments.

To review and configure if necessary [matching](#) and [mapping](#) rules for the collection, go to the **Matching** or **Mapping** tabs, respectively.

Configuring Object Matching

During migration of an object Directory Migration Agent automatically tries to match it with objects from Microsoft Office 365 according to the matching rules specified for the object.

All defined matching rules are located on the **Matching** tab. Matching is performed in top-down priority; therefore the topmost rule in the list of rules has the highest priority. From the Actions pane you can add, remove, or edit rules, and also change rules priority.

Migration Manager for Active Directory has a set of default matching rules that provide appropriate matching in most cases. Also, you can define your own matching rules as well as edit or delete existing ones.

Adding a Matching Rule

To add a new matching rule, select the collection in the management tree, open **Matching** tab, click **Add Matching Rule** in the **Actions** pane and specify the following:

1. Target class and its matching attribute
2. Source class and its matching attribute

i **NOTE:** You can also add matching rules for a migration pair. Such matching rules will be applied to every collection created afterwards. However, already existing collections will not be affected.

Viewing Matched Objects

To view currently matched objects, select the collection in the management tree and open the **Objects** tab. All source objects that are matched successfully with the objects in Microsoft Office 365 have **Matched** status.

Performing Object Matching Explicitly

You can match objects explicitly to ensure that objects are matched according to your needs. For instance, it may be useful if you already have objects in Microsoft Office 365 before migration and want to check that they are matched correctly.

To match objects in the collection, perform the following:

1. Select the desired collection in the management tree.
2. Open the **Objects** tab.
3. Click the **Match Objects** item in the Actions pane.
4. Specify whether current matching should be broken and start object matching.

i **NOTE:** If you made any changes to the list of matching rules and want those changes to apply for already matched objects, you need to select to break matching for the objects..

Breaking Object Matching

In some cases you may need to break matching for a pair of a source and target objects. This means that the object from the Active Directory and the corresponding object from Microsoft Office 365 are not considered as matched objects any longer in the Migration Manager for Active Directory (Microsoft Office 365) console. For instance, it is

required when you change mapping or matching rules for the collection and want them to apply onto already matched or migrated objects.

To break matching for an object, select the object on the **Objects** tab and click **Break Matching** in the **Actions** pane.

Configuring Attribute Mapping

Each attribute of the source object is **migrated** to the corresponding attribute of the Microsoft Office 365 object according to so-called mapping rules. Migration Manager for Active Directory has a default set of mapping rules which provide appropriate attribute mapping in most cases. However, if necessary you can define your own mapping rules as well as edit or delete existing ones.

You can also select from one of the predefined sets of rules by clicking **Change** near the **Schema template** field on the migration node level.

! **CAUTION:** Changing scheme template does not affect collections that already exist under the migration pair.

To define a new mapping rule for a specific collection, select the collection in the management tree, open **Mapping** tab, click **New Mapping Rule** in the **Actions** pane and specify the following:

1. Target class and its attribute that will contain source attribute after migration.
2. One of the following mapping rules that should be applied:
 - **Copy From**
Overwrites value of target attribute with value of source attribute
 - **Merge With**
Merges value of source multivalued attribute with value of target multivalued attribute
 - **Resolve To**
Resolves source linked attribute and writes the resulting value into the target attribute
 - **Set To**
Sets constant value for the target attribute
 - **Clear**
Makes target attribute value blank
3. Source class and its attribute to map.

i **TIP:** You can also add mapping rules for a **migration pair**. Such mapping rules will be applied to every collection created afterwards. However, already existing collections will not be affected.

Migrating Objects to Microsoft Office 365

You have two ways to migrate objects including their attributes from Active Directory domain to Microsoft Office 365:

- [Synchronizing Directories](#)

An on-going process of keeping the Microsoft Office 365 objects and their attributes (including group membership) in sync with their matching objects in the source domain during the coexistence period.

- [Migrating Objects](#)

A one-time operation of copying a collection of objects including their attributes from source domain to Microsoft Office 365. Only static collections are capable for migration. You can undo object migration at any time.

! **CAUTION:** Read information from the [Performing Pre-Migration Activities](#) section before starting any synchronization or migration tasks.

Performing Pre-Migration Activities

! **CAUTION:** Read information from this section very carefully.

Prior to performing any synchronization or migration tasks it is strongly recommended to review [matching](#) and [mapping](#) rules to be applied and to [match objects](#) explicitly. This is very important because if any object from Active Directory domain is matched with wrong object from Microsoft Office 365 and you migrate such object or enable coexistence for it, the attributes of the object in Microsoft Office 365 will be overwritten. Also settings and data related to the object in Microsoft Office 365 may be lost. If that happens during [migration task](#), you can roll back changes made to the object. However, if you [synchronize](#) those objects, the changes cannot be rolled back automatically, so you will need to fix the object in Microsoft Office 365 manually.

! **CAUTION:** If the object is mail- or mailbox-enabled then due to [mail redirection](#) specifics, all mail that comes to the mailbox in Microsoft Office 365 will be automatically redirected to on-premises mailbox before [mailbox switch](#) and in opposite direction after it. This may cause that user receive mail not intended for him or her.

Customizing automatic messages sent during migration

Migration Manager lets you customize the text of the automatic messages sent to users on actions performed on their accounts in Microsoft Office 365 (account creation, UPN change, password change, and their combinations).

You can do this in two ways:

1. In the Notifications subfolder of the folder where the Migration Manager for Active Directory (Office 365) console is installed, create any of the following text files:
 - `NewUser_NewPassword.custom.txt`
 - `NewUser_EnableSSO.custom.txt`
 - `NewPassword.custom.txt`
 - `ChangeUPN.custom.txt`
 - `ChangeUPN_EnableSSO.custom.txt`
 - `ChangeUPN_NewPassword.custom.txt`
 - `EnableSSO.custom.txt`

These files are templates that override the default message templates (`NewUser_NewPassword.default.txt` and so on) for particular scenarios.

Every Directory Migration Agent you install after that inherits these updated files and sends customized notifications to end users.

2. To customize the messages only for a collection of users, do the same in the Notifications subfolder of the folder where the corresponding Directory Migration Agent is installed. Only the users processed by that particular agent will get customized notifications.

If you need to disable email notifications for a scenario (for example, for Single Sign-On activation), create an empty file for it (for example, an empty EnableSSO.custom.txt).

Synchronizing Directories

! **CAUTION:** Read information from the [Performing Pre-Migration Activities](#) section before starting directory synchronization.

To synchronize objects from Active Directory with objects from Microsoft Office 365, you need to enable coexistence for the collection containing the objects. For that, select the desired collection in the management tree, click **Enable Coexistence** in the **Actions** pane and specify the following settings:

- Whether to create objects for which there are no matching objects in Microsoft Office 365
- Whether to merge not matched yet objects with their matching objects in Microsoft Office 365
- User principal names (UPN) suffix to use
- Country code to set for the users

After you complete the wizard, DMA will start synchronizing objects from the collection. If you need to stop synchronizing objects, click **Disable Synchronization** in the **Actions** pane.

You can get [track](#) the migration project on the **Statistics** tab.

Restarting Coexistence

In some case you may need to re-synchronize a collection with Microsoft Office 365. This may be necessary in the following cases:

- The collection is dynamic and its synchronization scope has been changed.
- Matching rules for the collection have been added, deleted or changed. In this case you need to explicitly [break matching](#) for the matched objects prior to re-synchronizing the collection.
- Mapping rules for the collection have been added, deleted or changed.

To re-synchronize a collection, select that collection in the management tree and click **Restart Coexistence** in the **Actions** pane.

i **NOTE:** Re-synchronizing may take a long time to complete.

Migrating Objects

! **CAUTION:** Read information from the [Performing Pre-Migration Activities](#) section before starting migration of objects.

To migrate objects to Microsoft Office 365 select the collection containing the objects in the management tree, click **Migrate Objects** in the **Actions** pane and specify the following settings:

- Whether to create objects for which there are no matching objects in Microsoft Office 365
- Whether to merge not matched yet objects with their matching objects in Microsoft Office 365

- User principal names (UPN) suffix to use
- Country code to set for the users

After you complete the wizard, DMA will create a migration task and start migrating objects from the collection. To view the migration task status and other details, go to the **Tasks** tab.

i **NOTE:** You can also migrate a part of objects from the collection. For that, select objects you plan to migrate on the **Objects** tab and click the **Migrate Objects** item in the **Actions** pane.

You can get track the migration project on the Statistics tab.

Undoing Object Migration

You can roll back the changes made to the Microsoft Office 365 tenant by each migration task independently. All the changes made to the Microsoft Office 365 tenant by the migration task will be rolled back exactly to the state before the migration task started.

To undo the results of a migration task, select the collection that was migrated in the management tree and click **Roll Back Objects** in the **Actions** pane. Complete the wizard to roll back all the changes made by that migration task to Microsoft Office 365.

! **CAUTION:** Take the following into consideration:

- **Objects are rolled back exactly to the same state as they have been before migration. All changes made to the source objects after migration will be overwritten.**
- **Rollback tasks that move accounts from a federated domain to a non-federated domain (or the other way around) complete with errors. To avoid this issue, perform an explicit migration to a non-federated (or federated, respectively) domain first, and then perform the rollback task.**

i **NOTE:** You can also undo migration for a single object. For that, select previously migrated object on the **Objects** tab and click the **Roll Back Object** item in the **Actions** pane.

Synchronizing Calendars

After you successfully migrated objects from Active Directory to Microsoft Office 365 you may start synchronizing calendars with Microsoft Exchange Online. To do that, you need to perform the following steps in the Migration Manager for Exchange console:

- [Set up a new Office 365 calendar synchronization job](#)
- [Add a new Office 365 calendar collection](#)
- [Start calendar synchronization](#)

i **TIP:** To provide co-existence of calendars between on-premises Exchange organization and Microsoft Exchange Online, calendar synchronization is performed apart from the mailbox migration by a separate instance of Migration Agent for Exchange. However, you may skip this step; in this case calendars will be migrated as a part of a [mailbox migration](#).

Resource Mailbox Synchronization Specifics

By default, Migration Manager for Exchange processes resource mailboxes such as equipment mailboxes and room mailboxes as regular user mailboxes. To convert those mailboxes to proper Microsoft Office 365 shared mailboxes you need to perform the following steps:

Exchange 2010 or higher

1. Synchronize resource mailboxes as regular calendars within a separate Office 365 calendar collection with a two-way synchronization turned on for it.
2. After those mailboxes are provisioned in Microsoft Exchange Online, you may convert each of them to appropriate type of Microsoft Office 365 shared mailbox. For that, invoke the following PowerShell cmdlet under any [Office 365 administrative account](#):

```
Set-Mailbox -Identity <MailboxIdParameter> [-Type <Regular | Room |  
Equipment | Shared>]
```

Exchange 2007

1. Synchronize resource mailboxes as regular calendars within a separate Office 365 calendar collection with a two-way synchronization turned on for it.
2. After those mailboxes are provisioned in Microsoft Exchange Online, you may convert each of them to appropriate type of Microsoft Office 365 shared mailbox. For that, invoke the following PowerShell cmdlet under any [Office 365 administrative account](#):

```
Set-Mailbox -Identity <MailboxIdParameter> [-Type <Regular | Room |  
Equipment | Shared>]
```

3. After that, go to <https://portal.microsoftonline.com> and sign in under the Office 365 administrative account.
4. In the header, click **Admin**.
5. On the **Admin** page, in the center pane, under **Outlook settings and protection**, click **Manage**.
6. In the **Exchange Control Panel**, select **Manage My Organization | Another User**.
7. Finally, open settings of each shared mailbox you converted on the step 2 and adjust necessary settings (for instance, **the Automatically process meeting request and cancellations** option). Be sure to click **Save** after modifying any settings for the shared mailbox.

i | **NOTE:** You may revoke Microsoft Exchange Online license for each migrated resource mailbox as that license is not required in Microsoft Office 365 for shared mailboxes.

Setting Up a New Office 365 Calendar Synchronization Job

To add a new Office 365 calendar synchronization migration job, right-click the Calendar Synchronization node in the management tree and after that click **Add Office 365 Calendar Synchronization Job** on the shortcut menu. This will start the **Add Office 365 Calendar Synchronization Job** wizard, which will install a Migration Agent for Exchange instance and help you to set up and configure the job.

This section guides you through each step of the wizard and explains the calendar synchronization with Office 365 options.

Step 1: Specifying Source Exchange Organization

Select the source Exchange organization, source Active Directory account and separate source Exchange account if necessary for the Office 365 calendar synchronization job.

Step 2: Specify Office 365 Tenant

Select the Microsoft Office 365 tenant to synchronize calendars with from the list of registered in Migration Manager for Exchange console ones. For information how to register new Microsoft Office 365 tenant, refer to [Registering Microsoft Office 365 as Migration Destination](#).

Step 3: Specifying Migration Agent for Exchange Installation Settings

In this step, you need to specify agent host server and path where Migration Agent for Exchange performing Office 365 calendar synchronization job should be installed. The default installation path is in the hierarchy of the **Program Files** system folder. You can customize the path, but your custom path will be used only if there are no previously installed instances of the Migration Agent for Exchange on the computer. Otherwise, the agent will be installed to the same location as the other existing instances regardless of the path you specify.

You can also override the default credentials that the agent will use. However, note that in this case you will be changing the credentials not only for the agent instance you are installing, but also for any existing agent instances on the agent host.

Step 4: Completing the Wizard

Finally you need to review the changes that will be made and apply them. When done, you can start dividing mailboxes you plan to migrate into [Office 365 calendar collections](#) in Migration Manager for Exchange console.

Adding a New Office 365 Calendar Collection

To create a new Office 365 calendar collection for an existing Office 365 calendar synchronization job, right-click the job in the management tree and click **Add Collection** on the shortcut menu.

This will start the **Add Office 365 Calendar Collection** wizard, which will help you to set up and configure a new collection for the Office 365 calendar synchronization job. Each step of the wizard is described below.

i | **NOTE:** All configuration settings that you specify for the collection during the wizard can be later changed. For that right-click the collection node in the management tree and select **Properties**.

Step 1: Specifying General Options

In the first step of the wizard, specify a name for the collection. You can optionally provide a text description for the collection. Also you can specify the Migration Agent for Exchange instance that should process the collection.

Enable the collection to force the corresponding agent to start processing the collection at scheduled time that will be specified on the next step of the wizard. Otherwise, the collection will not be involved in the migration process until you enable it.

i | **NOTE:** The corresponding Migration Agent for Exchange instance must be running to start processing the collection. To check the agent state, go to the **Agent Management** node in the management tree.

CAUTION: For regular calendar synchronization, the **Enable two-way synchronization for this collection** option should stay cleared. Select it only if your calendar collection contains shared and/or resource mailboxes which will be used by source and target users at the same time during co-existence period.

Step 2: Specifying Workflow

Set the preferred start date and other options for migrating the collection. By default, the option to start as soon as possible is selected. You can also specify a particular date and time to start synchronizing calendars from the collection.

Step 3: Populating the Collection

You can add mailboxes to the collection in the following ways:

- Explicitly add mailboxes to the collection by clicking the **Add User** button and selecting mailboxes from the list.
- Implicitly add mailboxes located in the containers by clicking the **Add Container** button and selecting the appropriate container check box. To add the mailboxes from the subcontainers as well, select the **Include subcontainers** check box. You can create and apply a LDAP filter to mailboxes of the Exchange organization using the **Advanced** tab.
- Implicitly add mailboxes listed in the groups. To add the mailboxes listed in the nested groups, select the **Expand nested distribution groups** check box.

To preview the list of mailboxes added to the collection, click the **Preview** button.

Step 4: Selecting Subscription Plan

Select the subscription plan for users whose calendars will be synchronized within the collection from ones available in the Microsoft Office 365 tenant specified as migration target for the [Office 365 calendar synchronization job](#). By default, each user that does not have Exchange Online license yet, will be assigned all licenses from the selected subscription plan when the migration starts. That will give the user access to the licensed services provided by the plan. Assigning the license will also cause provisioning a mailbox for user in Microsoft Office 365.

! **CAUTION:** Make sure the plan you selected contains Exchange Online service.

i **TIP:** You can configure Migration Agent for Exchange to assign users only Exchange Online license instead of all licenses at once. For more information how to do that, refer to the [Knowledge Article 136629](#).

i **TIP:** The information about the selected subscription plan is displayed for your information.

Step 5: Configuring Office 365 Settings

At the final wizard step, specify Microsoft Online Services ID and password of [Office 365 administrative account](#) under which Migration Agent for Exchange specified on [step 1](#) will access Microsoft Office 365.

i **NOTE:** By default all agents use the administrative account that you specified when you [register Microsoft Office 365 as migration destination](#).

Speeding Up Calendar Synchronization

It is recommended to create a separate administrative account for each collection. That speeds up calendar synchronization and prevents possible throttling limit excesses resulting in account locks.

i **NOTE:** Total number of administrative accounts should be calculated based on throttling policy limitations.

i **TIP:** You can create a bunch of administrative accounts with necessary permissions in Microsoft Office 365 at once as described in [Creating Microsoft Office 365 Administrative Accounts](#).

Starting Calendar Synchronization

To start synchronizing the calendars with Microsoft Office 365, perform the following:

1. Select the Office 365 calendar synchronization job in the management tree, and then click the **Agent Manager** toolbar button.
2. After that in the agent host pane select the agent host where the agent instance specified for the calendar collections you plan to synchronize is installed.
3. Finally, right-click the corresponding agent instance from the list of agent instances below and select **Start** from the shortcut menu.

i **NOTE:** You can temporarily disable any collection so that it will not be involved in the synchronization process until you enable it. For that, select **Disable** in the collection context menu.

You can get track the calendar synchronization migration using the Statistics dashboard. For information on how to do that, refer to the [corresponding section](#) of this document.

Synchronizing Public Folders

After you successfully synchronized calendars with Microsoft Exchange Online, you can synchronize public folders if necessary.

The following public folder synchronization methods are available

- [By legacy Exchange Agents](#)
- [By Migration Agent for Exchange \(MAgE\) with enhanced MMEX PowerShell Module](#)

Table 1: Public Folder Synchronization Method Comparison

Category	Feature	Legacy Exchange agents	MAgE with MMEX PowerShell module
Synchronization	2-way synchronization	Yes	Yes
	Migration from Exchange 2007	Yes	No
	Migration from Exchange 2010/2013/2016	Yes	Yes
	Migration from/to Exchange 2019	No/Yes	Yes
	Add, update, delete messages	Yes	Yes
	Update public folders automatically (permissions including group permissions; rename, move folder)	Yes	Yes
	Handle deleted public folders automatically	Yes	Yes
	Add new public folders	Yes	YES, BUT RERUN NEEDED
	Synchronize public folders' mail-enabled status	No	Yes
	Re-migrate public folders deleted on target	Limited Legacy agent only works in manual mode.	Yes
	Resync	Limited Legacy agent only supports the entire collection of folders.	Yes
	Synchronize permissions	Yes	Yes
	Synchronize SMTP address and advanced folder properties	No	Yes

Category	Feature	Legacy Exchange agents	MAGe with MMEX PowerShell module
Configuration	Define migration scope	Yes	Yes
	Modify migration scope	Yes	Yes
	Content filtering	Yes	Yes
	Support for existing content structure on target	Yes	Yes
	GUI	Yes, except for manual configuration of Outlook profiles on agent host	NO, MIGRATION BY MMEX POWERSHELL SCRIPTS ONLY
System Requirements	Minimal requirements	Minimum 2 hosts,6 agents, Outlook is required.	1 host, 1 agent
Performance	Overall performance	Low	High
Monitoring	Synchronization statistics	No	Yes

Before you migrate public folders to Microsoft Office 365 using agents you should take in consideration some specifics mentioned in [Public Folder Synchronization Caveats](#) subsection.

Public Folder Synchronization Caveats

- [Synchronization by legacy Exchange agents](#)
- [Synchronization by Migration Agent for Exchange with extended MMEX PowerShell module](#)

Synchronization by legacy Exchange agents

Consider the following specifics before you migrate public folders to Microsoft Office 365 by legacy Exchange agents:

- During synchronization of public folders with Microsoft Office 365 Exchange Online or Exchange 2013 or higher, Public Folder Target Agent is unable to set the message owner (creator) correctly for items in folders. The account of the corresponding administrative mailbox becomes the creator of the message instead of the actual mailbox owner.
This causes unwanted effects on the target. For example, the user cannot modify and delete their own migrated messages unless they have Owner permissions on the containing folder. This behavior is due to Exchange and Office 365 design decisions aimed at preventing security risks.
- Migration of public folders to Office 365 is significantly slow with Public Folder Synchronization Agents than with Migration Agent by Exchange. This is due to the extra time that the agent takes to match source and target recipients and process permissions.

- The administrative mailbox and account cannot be specified separately for public folder migration to Office 365. All public folder synchronization activity will reuse the account specified when the Office 365 target organization was added in the Migration Manager for Exchange console.
The account you specify will require additional configuration for public folder-related operations. For details, see [Additional Configuration for the Public Folder Synchronization Account \(Legacy Exchange Agents only\)](#). If you change the account after migration has started, this will result in full resynchronization from target to source. In addition, you have to manually perform the **Reapply Agents Configuration** operation for the public folder synchronization job in the Migration Manager for Exchange console.
- Only one Public Folder Target Agent instance performs all migration to Office 365. This means the choice of agent host must be made carefully. This should be a dedicated host rather than the same host as for the source Exchange server; otherwise, public folder synchronization performance will degrade.
Also note that if you change the agent host after migration has started, you have to manually install all the required agents on the new host and perform the Reapply Agents Configuration operation for the public folder synchronization job in the Migration Manager for Exchange console.
To avoid data loss and source-bound data duplication, initiate full resynchronization from the source to the target. This is needed because some PUB files may be left behind on the old agent host (causing loss of the data contained in them) or, in the case of two-way synchronization, the new agent host does not have information about which folders have been restored and don't need to be copied to the source (causing data duplication).
- The administrative account used for public folder synchronization with Office 365 requires the Owner client permission on all target public folders. Notify your users that they should expect to see this account as the owner of their public folders. Consider setting an informative display name for this account.
- Before you begin migration to Microsoft Office 365, you need to provision user accounts in it. For that, use the Migration Manager for Active Directory (Office 365) console. The information about user matching is stored in the corresponding migration project. It is important that you use the same migration project in the Migration Manager for Exchange console when you configure public folder synchronization.
- Mail-enabled folders are synchronized as non-mail-enabled with Office 365. As a workaround, after migration use native tools to make the folders mail-enabled.
- During public folder migration to Office 365 involving Migration Manager for Exchange Public Folder Synchronization Agents, make sure there are no batch public folder migrations being performed with native Microsoft tools in the source or in the target.

Synchronization by Migration Agent for Exchange with extended MMEX PowerShell module

Consider the following specifics before you migrate public folders to Microsoft Office 365 by Migration Agent for Exchange with extended MMEX PowerShell module:

- During synchronization of public folders with Microsoft Office 365 Exchange Online, MAgE is unable to set the message owner (creator) correctly for items in folders. The administrative account becomes the creator of the message instead of the actual mailbox owner. This causes unwanted effects on the target. For example, the user cannot modify and delete their own migrated messages unless they have **Owner** permissions on the containing folder. This behavior is a result of Exchange and Office 365 architecture aimed at preventing security risks.
- A single MAgE instance performs all migration to Office 365.
- The migrated public folders always inherit the client permissions from this root folder. To avoid granting unnecessary privileges, make sure that the client permissions for the target root folder are granted to the administrative account only before starting the migration.
- Synchronization should be rerun in case new public folders are added.

Synchronizing Public Folders by Legacy Exchange Agents

To synchronize public folders take the following steps in the Migration Manager for Exchange console:

1. [Set up a new public folder synchronization job.](#)
2. [Add a public folder collection.](#)
3. [Start public folder synchronization.](#)

It is recommended that you synchronize public folders before you migrate mailboxes. Before the users are migrated to the new environment, you need to copy the contents of the public folders to the new servers. This will ensure that the first migrated user will have access to up-to-date public folder information.

i **NOTE:** If public folder content in source organization is larger than storage limits per public folder mailbox, which is 50GB in Office 365, review the information provided in the [Migrating Large Public Folders to Exchange 2013 \(or Higher\) and Office 365](#).

Setting Up a New Public Folder Synchronization Job for Legacy Exchange Agents

Before you begin, open the properties of the target Office 365 organization, go to the **Default Agent Host** page and specify the computer where to install the necessary agents for synchronizing public folders with Exchange Online.

To create a new public folder synchronization job, right-click the **Public Folders Synchronization** node of the console management tree and select the **Add Public Folders Synchronization Job** option from the shortcut menu.

This will start the Add Public Folders Synchronization Job Wizard that will help you to install the public folder synchronization agents and configure the job.

This section guides you through each step of the wizard and explains the available public folder synchronization options. For more details, see the related topics.

Step 1. Select Exchange Servers

The public folder synchronization job is set up between the source Exchange server and Microsoft Office 365. Select your Office 365 tenant as the target organization; the choice of target server is disabled, because it becomes irrelevant.

For the source server, specify a mailbox that will be used by the public folder synchronization agents.

On the Office 365 end, the synchronization uses the Office 365 credentials and mailbox specified in the properties of your Office 365 organization.

The account under which the public folder synchronization agents are running must have full access to the administrator mailboxes so that they can get administrative access to the synchronized folders.

i **NOTE:** To learn how to configure public folder migration administrator mailboxes, refer to the dedicated Exchange environment preparation documents.

! **CAUTION:** Changing the agent's administrator mailbox after the public folder synchronization has been started is not recommended. This will lead to resynchronization of public folder contents.

Migration Manager will retrieve the public folder hierarchy using the mailboxes you specify. If you are logged on under an account that does not have access to these mailboxes, click Advanced to use an alternate NT account to retrieve the hierarchy.

The wizard will also create the first collection for the job. This first step prompts you for the collection name.

Step 2. Select Public Folders

The next step allows you to configure the public folder synchronization collection. Select the root folders to be synchronized. If you don't want to change the folder hierarchy, the easiest way is to select All Public Folders on both the source and target servers as the synchronization root. Simply select Public Folders in both the Source server box and the Target server box. The wizard will ask if you want to create a Public Folders folder on the target server and synchronize all the source public folders to this folder. Select **Yes** or **No** as appropriate.

Alternatively, you can select an existing Exchange folder as a target root folder. If the target root folder does not exist, you can create it by selecting the Add New Folder option from the shortcut menu as shown below.

i **NOTE:** Migration Manager for Exchange does not actually create the public folders. The public folder root will be created by the Public Folder Target Agent when the first PUB file comes from the corresponding source or target public folder.

To add a pair of folders to the collection, select the folders in both lists, set the synchronization direction, and click Add. The folders and all their subfolders will be marked as included to the collection.

You can also select the synchronization direction. Click the <-> button to change the initial source-to-target direction of synchronization if necessary.

! **CAUTION:** Once you start the public folder synchronization process, do not change the synchronization roots for any jobs or collections. Changing the selected folder pairs after the synchronization has started might result in duplicate folders in one of the environments.

To exclude a folder from synchronization, right-click the folder in the tree and click Exclude. The public folder synchronization agents will not synchronize the content of the folder, but will create it on the corresponding server and synchronize its subfolders, if any.

Click **Exclude PF with subfolders** to exclude from synchronization the folder itself and all its subfolders.

Step 3. Specify Agent Installation Path

The wizard will install the public folder synchronization agents on the Exchange servers or the corresponding default agent host. If no Migration Manager for Exchange component has been yet installed on these servers, you will be able to specify the installation path for the agents. As soon as the agents are installed, the QMME\$ServerName\$ shared folder will be created in the path you specified. All the agents or components you install later will be installed in the same location. However, if by the time you install the public folder agents, any other agents or components have already been installed, you will not be allowed to specify the installation path for the agents, and they will be installed in the location where the QMME\$ServerName\$ shared folder has been created.

By default the shared folder is created in the %SystemRoot%\System32 folder. For 64-bit Microsoft Exchange the default shared folder is created in the %SystemRoot%\SysWOW64 folder.

Step 4. Complete the Wizard

After the agents are installed, the wizard will inform you that you can start the public folder synchronization job. It is strongly recommended that you verify all the agents and collection settings before starting the public folder synchronization.

Step 5. Commit Changes

After a new job is created, it is marked with an exclamation mark. This means that you need to update the public folder synchronization agents' databases before starting the job. Right-click the job in the management tree and click **Commit Changes** on the shortcut menu to update the agents' task lists on the remote servers.

You can also commit changes for all the public folder synchronization jobs you have created. To do that, right-click the **Public Folder Synchronization** node in the management tree and select **Commit All Public Folder Jobs** from the shortcut menu.

Adding a Public Folder Collection

To create a new collection for an existing public folder synchronization job, right-click the job in the management tree and select **Add Collection** from the shortcut menu.

This will start the Add Public Folder Collection Wizard, which will help you to set up and configure a new collection for the job. Each of the wizard's steps is described in the related topics.

Step 1. General Options

Specify a name for the collection and set its priority. Optionally, you can provide a text description for the collection. You can temporarily disable the collection and it will not be involved in the synchronization process until you enable it.

Step 2. Workflow

Set the preferred date to start migrating the collection. By default, the option to **Start as soon as possible** is selected.

Step 3. Select Public Folders

Populate the collection with public folder pairs. Note that folders that are already synchronized within other collections of the job are marked in the folder lists and cannot be included in the collection.

! CAUTION: Once you start the public folder synchronization process, do not change the synchronization roots for any jobs or collections. Changing the selected folder pairs after the synchronization has started might result in duplicate folders in one of the environments.

Step 4. Complete the Wizard and Commit Changes

After the new collection is created, the job is marked with an exclamation mark that means that you need to update the public folder synchronization agents' databases. Right-click the job in the management tree and click **Commit Changes** on the shortcut menu to update the agents' task lists on the remote servers.

Starting Public Folder Synchronization by Legacy Exchange Agents

The public folder synchronization job should be started after all the target mailboxes already exist and have been matched to the source mailboxes. The matching step is critical for synchronization of public folder permissions.

To start the public folder synchronization agents, perform the following:

1. Select the public folder synchronization job in the navigation tree, and then click the **Agent Manager** toolbar button.
2. After that in the agent host pane select all necessary agent hosts.
3. Finally, in the **Actions** pane click **Start Agents**.

Synchronizing Public Folders by MAgE

In case you prefer alternative method of public folders synchronization for migration scenarios from Microsoft Exchange 2010/2013/2016/2019 by enhanced Migration Agent for Exchange (MAgE) combined with extended MMEEx PowerShell module refer to [Public Folder Synchronization \(MAgE\)](#) document. This synchronization method does not currently have an appropriate user interface and is intended for advanced PowerShell users only. To select optimal synchronization method refer to [Synchronizing Public Folders](#).

Migrating Mailboxes

After you successfully migrated objects from Active Directory to Microsoft Office, you may start migrating mailboxes to Microsoft Exchange Online. To do that, you need to perform the following steps in the Migration Manager for Exchange console:

1. [Set up a new Office 365 mailbox migration job](#)
2. [Add a New Office 365 mailbox collection](#)
3. [Start mailbox migration](#)

Setting Up a New Office 365 Mailbox Migration Job

To add a new Office 365 mailbox migration job, right-click the **Mailbox Synchronization** node in the management tree and click **Add Office 365 Mailbox Migration Job** on the shortcut menu. This will start the **Add Office 365 Mailbox Migration Job** wizard, which will install a Migration Agent for Exchange instance and help you to set up and configure the job.

This section guides you through each step of the wizard and explains the options for migration to Office 365.

Step 1: Specifying Source Exchange Organization

Select the source Exchange organization, the source Active Directory account and the separate source Exchange account (if necessary) for the Office 365 mailbox migration job.

Step 2: Specify Office 365 Tenant

Select the Microsoft Office 365 tenant to migrate mailboxes to from the list of registered in Migration Manager for Exchange console ones. For information how to register new Microsoft Office 365 tenant, refer to [Registering Microsoft Office 365 as Migration Destination](#).

Step 3: Configuring Notification Messages

After a mailbox has been migrated and [switched](#) to Microsoft Office 365, Migration Manager for Exchange sends notification email messages to the old on-premises and new cloud mailboxes to inform user that that user's new mailbox has been provisioned and all new mail goes into that new mailbox. Also notification messages may contain additional instructions how to configure mail client to use Microsoft Office 365 mailbox, etc.

You can use predefined notifications or write your own based on the default message templates, for the source and target mailboxes separately.

Step 4: Specifying Migration Agent for Exchange Installation Settings

In this step, you need to specify agent host server and path where Migration Agent for Exchange performing Office 365 mailbox migration job should be installed. The default installation path is in the hierarchy of the **Program Files** system folder. You can customize the path, but your custom path will be used only if there are no previously installed instances of the Migration Agent for Exchange on the computer. Otherwise, the agent will be installed to the same location as the other existing instances regardless of the path you specify.

You can also override the default credentials that the agent will use. However, note that in this case you will be changing the credentials not only for the agent instance you are installing, but also for any existing agent instances on the agent host.

Step 5: Completing the Wizard

Finally, you need to review the changes that will be made and apply them. When done, you can start dividing mailboxes you plan to migrate into [Office 365 mailbox collections](#) in Migration Manager for Exchange console.

Adding a New Office 365 Mailbox Collection

To create a new Office 365 mailbox collection for an existing Office 365 mailbox migration job, right-click the job in the management tree and click **Add Collection** on the shortcut menu.

This will start the **Add Office 365 Mailbox Collection** wizard, which will help you to set up and configure a new collection for the Office 365 mailbox migration job. Each step of the wizard is described below.

i | **NOTE:** All configuration settings that you specify for the collection during the wizard can be later changed. For that right-click the collection node in the management tree and select **Properties**.

Step 1: Specifying General Options

In the first step of the wizard, specify a name for the collection. You can optionally provide a text description for the collection. Also you can specify the Migration Agent for Exchange instance that should process the collection.

Enable the collection to force the corresponding agent to start processing the collection at scheduled time that will be specified on the next step of the wizard. Otherwise, the collection will not be involved in the migration process until you enable it.

! | **CAUTION:** The corresponding Migration Agent for Exchange instance must be running to start processing the collection. To check the agent state, go to the **Agent Management** node in the management tree.

i | **NOTE:** You may enable the collection anytime later by clearing **Disable** option in the collection context menu or by selecting **Enable** collection in the collection properties.

Step 2: Specifying Workflow

Set the preferred start date and other options for migrating the collection. By default, the option to start as soon as possible is selected. You can also specify a particular date and time to start migrating mailboxes from the collection.

Step 3: Populating the Collection

You can add mailboxes to the collection in the following ways:

- Explicitly add mailboxes to the collection by clicking the **Add User** button and selecting mailboxes from the list.
- Implicitly add mailboxes located in the containers by clicking the **Add Container** button and selecting the appropriate container check box. To add the mailboxes from the subcontainers as well, select the **Include subcontainers** check box. You can create and apply a LDAP filter to mailboxes of the Exchange organization using the **Advanced** tab.
- Implicitly add mailboxes listed in the groups. To add the mailboxes listed in the nested groups, select the **Expand nested distribution groups** check box.

To preview the list of mailboxes added to the collection, click **Preview**.

Step 4: Selecting Subscription Plan

Select the subscription plan for users whose mailboxes will be migrated within the collection from ones available in the Microsoft Office 365 tenant specified as migration target for the [Office 365 mailbox migration job](#). By default, each user that does not have Exchange Online license yet, will be assigned all licenses from the selected subscription plan when the migration starts. That will give the user access to the licensed services provided by the plan. Assigning the license will also provision a mailbox for user in Microsoft Office 365.

! **CAUTION:** Make sure the plan you selected contains Exchange Online service.

i **NOTE:** You can configure Migration Agent for Exchange to assign users only Exchange Online license instead of all licenses at once. For more information how to do that, refer to the [Knowledge Article 136629](#).

i **TIP:** The information about the selected subscription plan is displayed for your information.

Step 5: Configuring Mailbox Switch

After you selected a subscription plan, you need configure mailbox switch options. If you prefer to switch mailboxes manually using the Migration Manager for Exchange console, select the **Mailboxes will be switched manually** option. Otherwise, you can schedule when to start a mailbox switch.

You can optionally select whether a mailbox should be switched even if no more than specified number of errors occurred during synchronization.

Manually Switching Mailboxes and Undoing Mailbox Switch

1. Select the node of the mailbox collection you need.
2. In the right pane, go to the **Statistics** tab.
3. Select the mailboxes you need in the table at the bottom

4. The Actions pane shows either the **Switch** or the **Undo Switch** action item, depending on the state of the mailboxes. Click the action item to perform the required operation.

Step 6: Configuring Office 365 Settings

At the final wizard step, specify Microsoft Online Services ID and password of [Office 365 administrative account](#) under which Migration Agent for Exchange specified on [step 1](#) will access Microsoft Office 365.

i | **NOTE:** By default all agents use the administrative account that you specified when you [register Microsoft Office 365 as migration destination](#).

Speeding Up Calendar Synchronization

It is recommended to create a separate administrative account for each collection. That speeds up calendar synchronization and prevents possible throttling limit excesses resulting in account locks.

i | **NOTE:** Total number of administrative accounts should be calculated based on throttling policy limitations.

i | **TIP:** You can create a bunch of administrative accounts with necessary permissions in Microsoft Office 365 at once as described in [Creating Microsoft Office 365 Administrative Accounts..](#)

Starting Mailbox Migration

To start migrating mailboxes to Microsoft Office 365, perform the following:

1. Select the Office 365 mailbox migration job in the management tree, and then click the **Agent Manager** toolbar button.
2. After that in the agent host pane select the agent host where the agent instance [specified](#) for the mailbox collection you plan to migrate is installed.
3. Finally, right-click the corresponding agent instance from the list of agent instances below and select **Start** from the shortcut menu.

i | **NOTE:** You can temporarily disable any collection so that it will not be involved in the migration process until you enable it. For that, select **Disable** in the collection context menu.

You can get track the mailbox migration using the Statistics dashboard. For information on how to do that, refer to the [corresponding section](#) of this document.

Post-Migration Activities

Redirecting Email to Microsoft Exchange Online

After you finished [migrating](#) mailboxes to Microsoft Exchange Online, you may need to update the Mail Exchange (MX) records in your DNS so that all mail is redirected to the cloud. This step can only be performed after all on-premises mailboxes are migrated to Microsoft Exchange Online. Note that this step is mandatory only if you plan to completely [decommission](#) your on-premises Exchange infrastructure.

For information on how to do that, go to <http://onlinehelp.microsoft.com/en-us/office365-enterprises/ff637598.aspx>.

Updating Outlook Profiles

During migration, Migration Manager for Exchange switches mailboxes from the source Exchange server to Microsoft Office 365. Before users can start working with their new cloud mailboxes, their Microsoft Outlook profiles must also be updated. To update Outlook profiles you may use Client Profile Updating Utility (abbreviated to CPUU) shipped with Migration Manager. The utility allows you to update Outlook profiles automatically and transparently.

! CAUTION: You have to provide all users with their Microsoft Office 365 passwords before CPUU switches Outlook profiles. Otherwise, the user cannot log on to his or her mailbox and get an access to his/her emails after the switch.

For information on how to update Outlook profiles using CPUU, see the *Client Profile Updating Utility Administrator Guide* included in the Migration Manager documentation set.

Decommissioning Exchange Servers (Optional)

After you successfully migrated all mailboxes from on-premises Exchange organization to Microsoft Office 365, ensured that all users can connect to their cloud mailboxes, and mail flow is established properly, you may start decommissioning your on-premises Exchange servers. Refer to Microsoft documentation for information on how to do that.

For information on how to decommission existing Exchange servers, go to [http://technet.microsoft.com/en-us/library/cc463439\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc463439(v=ws.10).aspx).

Switching to Other Directory Synchronization Tools (Optional)

Establishing co-existence of objects between Active Directory domain and Microsoft Office 365 using Migration Manager for Active Directory is supported only during calendar synchronization and mailbox migration. To continue synchronizing objects after you finished migrating mailboxes, consider using Microsoft Azure AD Connect ([link](#)).

Tracking the Migration Progress

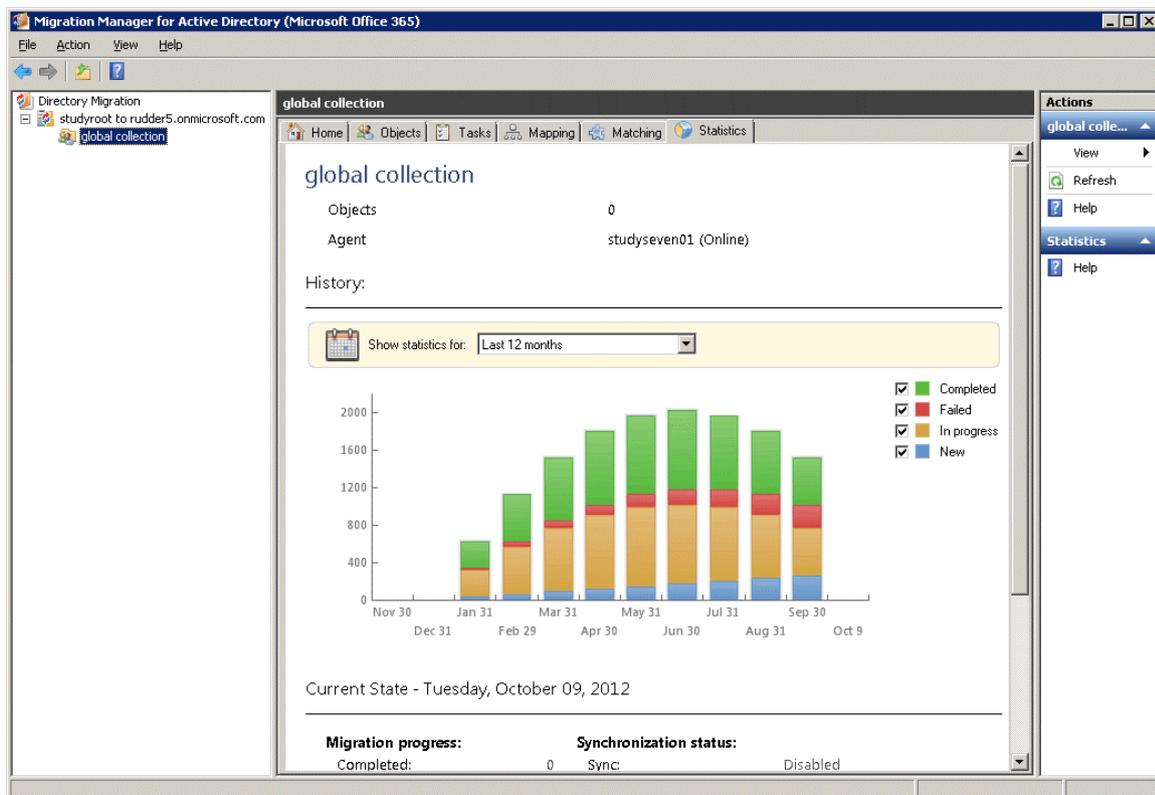
You can track the progress of the operations on the **Statistics** tab in the Migration Manager for Active Directory (Office 365) console.

NOTE: Tracking of public folder synchronization is not supported at this time.

- [Directory Migration](#)
- [Calendar Synchronization](#)
- [Mailbox Migration](#)

Directory Migration

To view the directory migration progress, open the Migration Manager for Active Directory (Office 365) console and see the statistics view on the **Home** tab in the center pane. Statistics are available at the migration and collection levels. More detailed statistics information is displayed on the **Statistics** tab.



To view the current statuses of specific objects in a collection, go to the **Objects** tab.

The objects involved in the migration can have the following statuses:

Migration Progress

- **Completed**

A mailbox of already migrated user is successfully **switched** using Migration Manager for Exchange.

- **Failed**

Some errors occurred during object synchronization.

- **In Progress**

Directory Migration Agent is processing the object at this moment. The object might be

- **Migrated** – The object is successfully **migrated** to Microsoft Office 365.
- **Matched** – The object is **matched** with the corresponding one in Microsoft Office 365.
- **Not matched** – The object has no matching objects in Microsoft Office 365 according to actual **matching rules**.

- **New**

A mailbox was added to a collection and was not processed by Directory Migration Agent yet.

Synchronization Status

- **Never synced**

The object has not been involved in the synchronization process yet.

- **In sync**

The object is being synchronized by Directory Migration Agent at this moment.

- **Not intended to be synced**

The object has not been matched yet and **synchronization settings** do not allow creating or merging not matched objects.

- **Failed**

The object failed to be synchronized due to error. To view the error description, go to the **Objects** tab.

For more information about logging and dealing with possible migration problems, see [Troubleshooting Migration to Office 365](#).

Calendar Synchronization

To view the calendar synchronization progress, you can use the Statistics dashboard in the Migration Manager for Exchange console. The dashboard is available at the calendar synchronization job level and at the calendar collection level.

Select a node related to calendar synchronization in the navigation tree and click the **Statistics** toolbar button to see the statistics for a particular collection.

i **TIP:** For details on information provided in the **Statistics** pane, refer to [Tracking the Migration Progress](#). Note that you can also obtain synchronization statistics using PowerShell cmdlets. For details, see [Configuring Migration Using PowerShell](#).

For more information about logging and dealing with possible migration problems, see [Troubleshooting Migration to Office 365](#).

Mailbox Migration

To view the mailbox migration progress, you can use the Statistics dashboard in the Migration Manager for Exchange console. The dashboard is available at the mailbox synchronization job level and at the mailbox collection level.

Select a node related to mailbox migration in the navigation tree and click the **Statistics** toolbar button to see the overall statistics or the statistics for a particular collection.

i **TIP:** For details on information provided in the **Statistics** pane, refer to [Tracking the Migration Progress](#). Note that you can also obtain synchronization statistics using PowerShell cmdlets. For details, see [Configuring Migration Project Using PowerShell](#).

For more information about logging and dealing with possible migration problems, see [Troubleshooting Migration to Office 365](#).

Hybrid Migration Scenarios

This topic contains a collection of supported by Migration Manager migration scenarios that involve hybrid deployments. For guidance on the choice of scenario, examine the descriptions to find the route that is most appropriate for you.

Currently, Migration Manager supports the following hybrid migration scenarios:

- [Acquisition with a Hybrid](#)
- [Complex Acquisition with a Hybrid](#)
- [Reorganization or Upgrade with a Hybrid](#)
- [Complex Reorganization or Upgrade with a Hybrid](#)

! **CAUTION:** Microsoft Office 365 now supports a hybrid deployment where multiple Active Directory forests can share a single tenant. Migration Manager does not support migrating into this type of deployment. The target hybrid deployment must be a single forest with a single tenant. Migration Manager can migrate one or more source forests into this single forest hybrid target.

! **CAUTION:** Prior to implementing any migration scenario, check the system requirements and prepare Exchange organizations as well as Microsoft Office 365 tenant according to the corresponding topics in [Before You Begin](#).

Keeping existing domain name

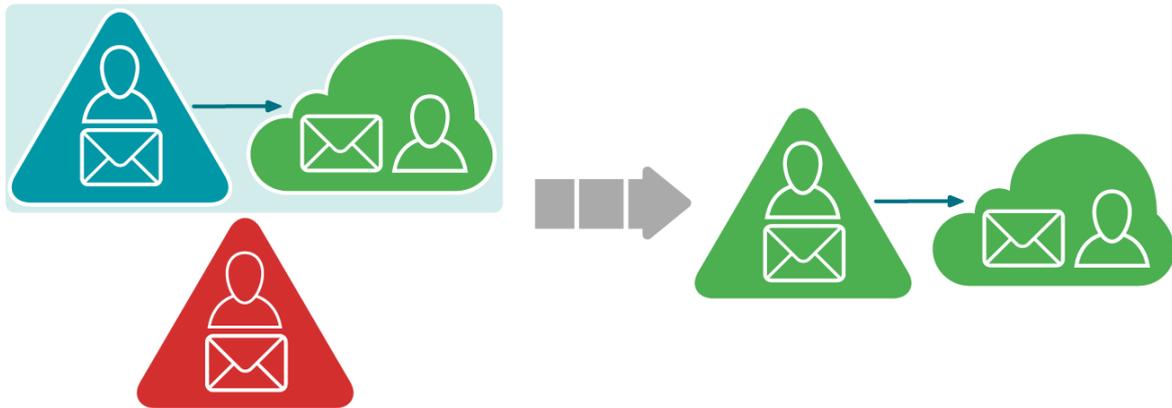
1. All described migration scenarios imply that the domain name for the migrated objects will be changed during migration. However if you want to keep the existing domain name, take the following steps:
2. Migrate objects from the original domain to a temporary domain using Migration Manager for Active Directory. The name of the temporary domain must differ from the name of the original domain.
3. After that perform another migration according to the chosen hybrid migration scenario. Be sure to have the destination domain name the same as the original domain name.

After performing such two-hop migration, you will implement the desired migration scenario and the migrated objects will have the same domain name as the corresponding source objects.

Acquisition with a Hybrid

The goal of this migration is to merge objects from the source environment into the target hybrid environment. This also entails a change of domain name for the objects that are migrated. The primary SMTP addresses for the objects from the source environment are to be changed to match the target ones.

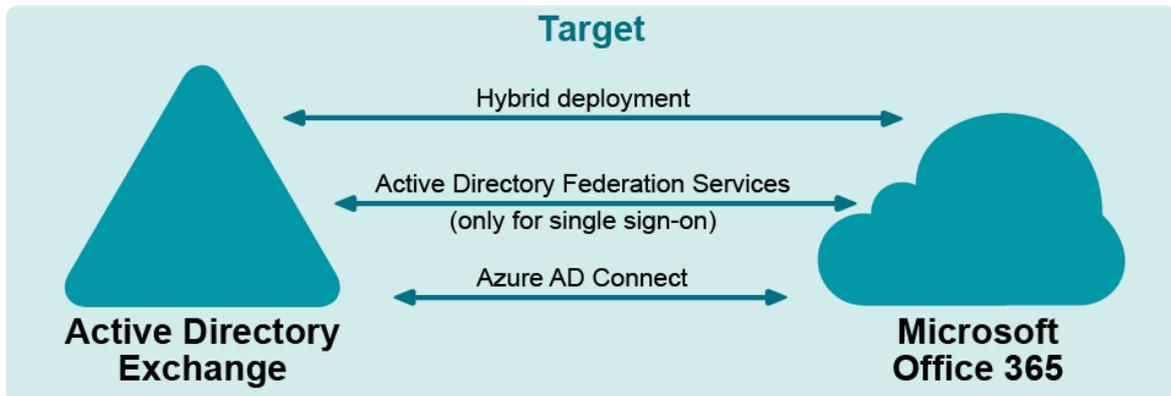
The typical use case for this scenario is when one company buys another, and the newly-acquired company needs to merge in its directory and mail system.



Migration Manager provides an ability to migrate users' mailboxes from the acquired company directly to Microsoft Office 365 without the need to firstly migrate mailboxes to on-premises Exchange organization.

Prerequisites

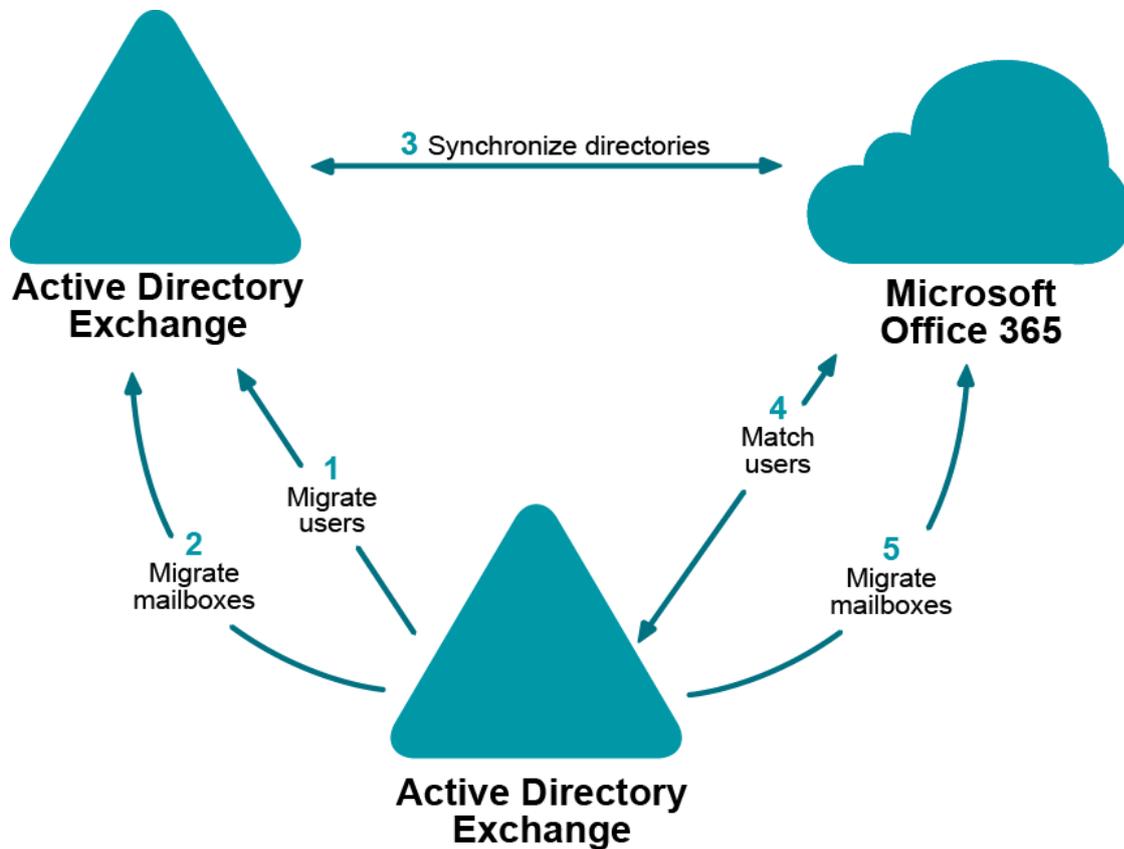
- The source environment is a regular Active Directory domain with an Exchange organization.
- The target environment is an Exchange hybrid deployment.



Procedure

Pre-migration task: Establish Mail Flow to Source Exchange Organization

1. On-Premises Directory Migration
2. On-Premises Mailbox Migration
3. Cloud Directory Migration
4. User Matching
5. Cloud Mailbox Migration



Establish Mail Flow to Source Exchange Organization

Since additional domains (for instance, source.local) will be used for mail redirection purposes, the corresponding Exchange connectors should be set up to establish proper mail flow.

Mail redirection from target to source on-premises organization

In order to enable mail redirection from the target to the source on-premises organization using @source.local namespace, add a new send connector on the target on-premises Exchange server with the following settings:

- Specify the mail delivery options depending on your organization specifics and Exchange Server version. For details, please refer to Microsoft documentation available [here](#).
- Add a SMTP address space with the source.local domain.

Mail redirection from Microsoft Office 365 to source organization

Enabling mail redirection from Microsoft Office 365 to the source organization depends on the domain suffix that will be used for the cloud-related mail redirection purposes. If the domain name is publicly available (MX records are registered in public DNS and point to source Exchange server) no additional connectors are required.

In case the domain suffix is not publicly available, the corresponding connector in Microsoft Office 365 should be created to relay mail to the on-premises target Exchange server which, in its turn, should relay mail to the source Exchange server.

On-Premises Directory Migration

Migrate users from the source Active Directory domain to the target Active Directory domain (the one that is synchronized with Microsoft Office 365).

What will you achieve

- Mail-enabled users that have the **targetAddress** attribute pointing to source mailboxes will be created.
- Mail sent to the newly created mail-enabled users using on-premises Global Access List (GAL) will be delivered to the corresponding source mailboxes

How do you do that

Configure directory synchronization from the source Active Directory domain to the target Active Directory domain so that the target GAL is populated with the objects from the source domain.

For that, take the following steps:

1. Open the Migration Manager for Active Directory console.

i | **NOTE:** Ensure that the current open project is not the one that is intended for migration to Microsoft Office 365.

2. Install a new Directory Synchronization Agent instance if none installed already. For details, see the *Agent Manager* topic of the *Migration Manager for Active Directory User Guide*.
3. Create a domain pair of the source Active Directory domain and the target Active Directory domain. For information on how to do that, see the *Domain Pairs* section in the *Migration Manager for Active Directory User Guide*.
4. Configure a new synchronization job for the domain pair according to the *Configuring the Synchronization Job* topic of the *Migration Manager for Active Directory User Guide*. Set the following specific options for the synchronization job:
 - **Specify Source Scope:** The **Disable target accounts** option must be cleared so that migrated accounts will be able to access target Active Directory domain as well as Microsoft Office 365 with the same password through SSO.
 - **Set Security Settings:**
 - The **Synchronize passwords** option must be selected.
 - Under **User Principal Name handling**, set the domain suffix of the UPNs to the appropriate domain matching federated domain used in hybrid.

- **Advanced Options:** Select **Use custom add-in** and specify add-in located at `<Migration Manager installation folder>\Active Directory\COPYTargetAddress.xml`.
- **Specify Exchange Options:**
 - Select the **Mail-enabled users** option
 - Specify the target SMTP address template (e.g. **target.local**)
 - Specify the source SMTP address template (e.g. **source.local**)

i **NOTE:** Since the *source.local* redirection domain will be also used in Microsoft Office 365, it should be publicly available, or the corresponding connectors should be created in Microsoft Office 365 to establish mail flow.

5. Start the configured directory synchronization job as described in *Starting and Stopping Directory Synchronization* topic of the *Migration Manager for Active Directory User Guide*, and wait until initial synchronization completes.

How do you verify that step worked

1. Create a test mailbox in the target on-premises organization.
2. Using GAL, send a test message to any mail-enabled user that was migrated by Directory Synchronization Agent (DSA).
3. Open the source user's mailbox and check that the message is delivered successfully.
4. Reply that message and ensure that it arrived to the target mailbox.
5. Repeat the above steps using any mailbox outside your organization to check that original and reply messages are delivered successfully.

Additional information

For details, see the following topics in the *Migration Manager for Active Directory User Guide*:

- Pre-Migration Activities
- Directory Synchronization

On-Premises Mailbox Migration

If you need to migrate some of mailboxes to the on-premises part of the target hybrid, you can do that now. For detailed information on how to do that, refer to *Migration Manager for Exchange User Guide*.

i **NOTE:** Before performing on-premises mailbox migration in Migration Manager for Exchange console, ensure that the current open project is not the one that is intended for migration to Microsoft Office 365.

User Matching

Match users in the source Active Directory domain with users in the target Microsoft Office 365 tenant.

What will you achieve

- Mailboxes from the source Active Directory domain will be matched with the corresponding Microsoft Office 365 mail users.
- The Location property will be populated for the Microsoft Office 365 users.

How do you do that

Configure a new migration from the source Active Directory domain to Microsoft Office 365 in Migration Manager for Active Directory (Microsoft Office 365) console to match accounts.

Set up a new migration as follows:

1. [Install](#) a Directory Migration Agent instance if none installed already.
2. [Configure migration pair](#) of source Active Directory domain and target Microsoft Office 365 tenant.
3. Specify the mail redirection domain for the migration pair. When choosing mail redirection domain, take the following into account:
 - This domain must be accepted in on-premises domain only
 - The domain must not be accepted in Microsoft Office 365.

i **NOTE:** The `source.local` domain used for Directory Synchronization can be used as redirection domain if it is publicly available or corresponding connectors exist in Microsoft Office 365 tenant. If centralized mail transport is enabled in your hybrid deployment, you can use the existing on-premises connector for this purpose.

4. Select the [Empty Active Directory to Microsoft Office 365 mapping template](#) for the migration pair.
5. [Create a static collection](#) including all objects from the source Active Directory domain.
6. [Start a new migration task](#) with the following options:
 - The **Create new objects on target** option cleared
 - The **Merge into existing objects** on target option selected
 - The UPN suffix set to the corresponding federated domain in Microsoft Office 365

How do you verify that step worked

To ensure that the above procedure succeeded, check that the Location property is populated for the Microsoft Office 365 users.

Additional information

For details, see the [Provisioning User Accounts in Office 365](#) section.

Cloud Directory Migration

Provision source users that were previously created in the target domain to Microsoft Office 365.

What will you achieve

- Accounts from source Active Directory domain will be listed in the Microsoft Office 365 Global Access List (GAL)

- Mail sent by cloud users to mailboxes from the source Exchange organization will be delivered successfully.
- Mail users will be created in Microsoft Office 365 and their **ExternalEmailAddress** property will point to corresponding mailboxes in the source organization.

How do you do that

This step is performed automatically by Microsoft Azure AD Connect as soon as mail-enabled users have been created in the target Active Directory domain by Directory Synchronization Agent.

i | **NOTE:** Note that the new users created in target Active Directory domain are not immediately processed by Microsoft Azure AD Connect. Therefore, wait until Microsoft Azure AD Connect completes synchronizing directories before proceeding.

How do you verify that step worked

1. Sign in to Microsoft Office 365 under any licensed user, open address book, select any user from the source organization and send a test message to that user.
2. Open the source user's mailbox, check that the message arrived successfully, and reply to it.
3. Make sure that reply message is delivered to the cloud recipient.
4. Repeat the above steps using any mailbox outside your organization to check that original and reply messages are delivered successfully.

Cloud Mailbox Migration

Once all accounts are provisioned to Microsoft Office 365 tenant and mail flow is established, migrate mailboxes from the source organization to the Microsoft Office 365 tenant and synchronize the calendars using Migration Manager for Exchange. After that perform a mailbox switch so that incoming mail start going to the Microsoft Office 365.

i | **NOTE:** Before performing any migration tasks, ensure that the current open project in Migration Manager for Exchange console is the same as you used previously in Migration Manager for Active Directory (Microsoft Office 365) console for matching users with Microsoft Office 365.

- [Synchronize calendars](#)
- [Migrate mailboxes](#)
- [Perform mailbox switch](#)

Synchronize calendars

What will you achieve

- Cloud mail users will be converted to mailboxes with valid licenses assigned (if not already converted).
- Users from the source organization and users from Microsoft Office 365 will be able to view each other's free/busy information and schedule meetings.

How to do that

Synchronize calendars using Migration Manager for Exchange as described step-by-step in [Synchronizing Calendars](#).

How do you verify that step worked

1. Sign in to Microsoft Office 365 under any licensed user and create a test meeting.
2. Open any source mailbox and verify that the cloud user under which you created the meeting is busy at the time of the meeting.
3. Then create another test meeting in that source mailbox.
4. From Microsoft Office 365, ensure that the source user is busy at the time of the new meeting.

Migrate mailboxes

What will you achieve

- Cloud mail users will be converted to mailboxes with valid licenses assigned (if not already converted).
- Users from the source organization will be able to sign in to the cloud through SSO and access mailbox data migrated from their mailboxes.

How to do that

Migrate mailboxes using Migration Manager for Exchange as described step-by-step in [Migrating Mailboxes](#).

How do you verify that step worked

1. Sign in to Microsoft Office 365 under any licensed user, open address book, select any user from source organization and send a test message to that user.
2. Open the source user's mailbox, check that the message arrived successfully, and reply to it.
3. Make sure that reply message is delivered to the cloud recipient.
4. Repeat the above steps using any mailbox outside your organization to check original and reply messages are delivered successfully.

Perform mailbox switch

Once calendars are synchronized and mailboxes are migrated to Microsoft Office 365, mailboxes can be switched using Migration Manager for Exchange. Mailbox switch allows all the Migration Manager for Exchange components to recognize the mailbox as switched and ensures that all new mail now arrives in the user's cloud mailbox.

What will you achieve

All incoming mail will be delivered to Microsoft Office 365 mailboxes instead of on-premises mailboxes.

How to do that

[Mailbox switch](#) can be done either manually from the console or automatically by the Migration Agent for Exchange. This is configured through options in the collection that the mailbox is in. If you choose automatic switching, you can either schedule the mailbox switch operation for a specified time or have the agent switch each mailbox as soon as it is synchronized.

How do you verify that step worked

1. Sign in to Microsoft Office 365 under any licensed user, open address book, select user from source organization that has been switched and send a test message to that user.
2. Open any source user mailbox, open address book; select the same user as on step 1 and send another test message to that user.
3. Sign in to Microsoft Office 365 under the user to whom you sent messages on the above steps, ensure that messages arrived successfully and reply to them.
4. Ensure that reply messages are successfully delivered to recipients.

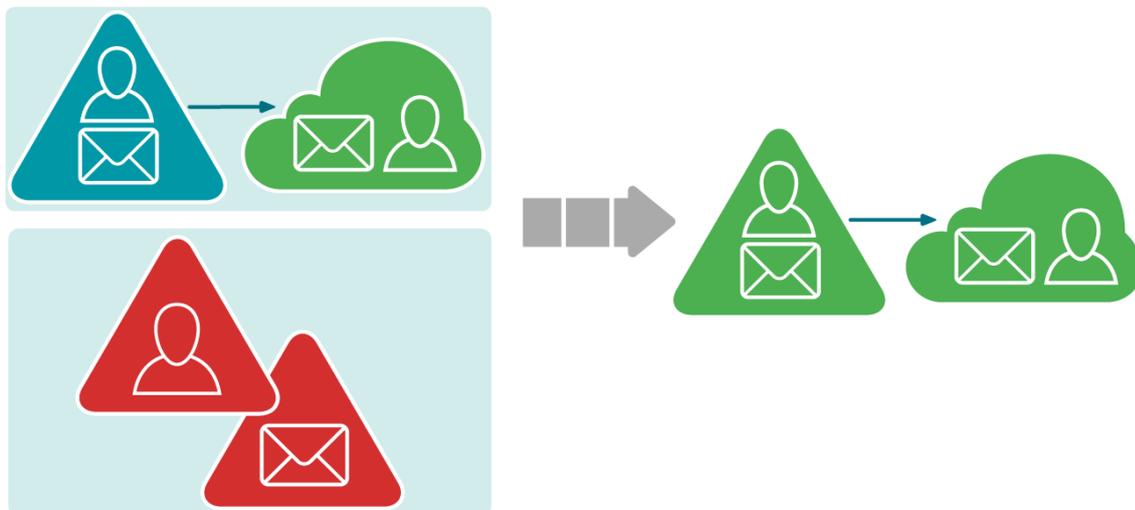
Additional information

For detailed information on mailbox switch, see the Mailbox Switch topic under the Mailbox Migration Process section in the Migration Manager for Exchange User Guide.

Complex Acquisition with a Hybrid

The goal of this migration is to merge objects from the source environment with dedicated Exchange forest into the target hybrid environment. This also entails a change of domain name for the objects that are migrated. The primary SMTP addresses for the objects from source environment are to be changed to match the target ones.

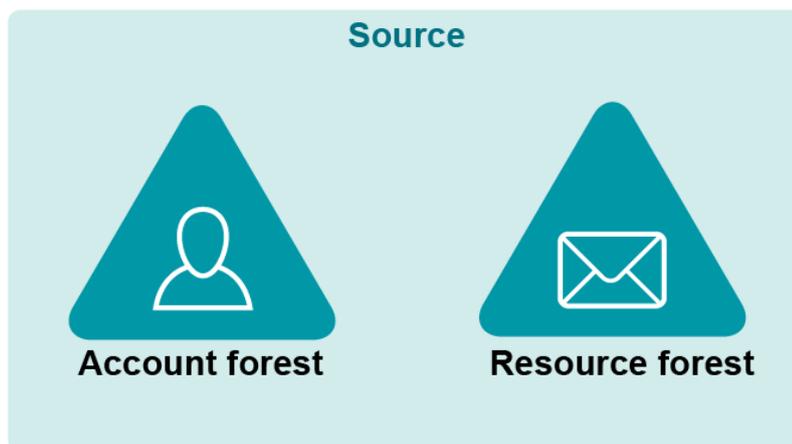
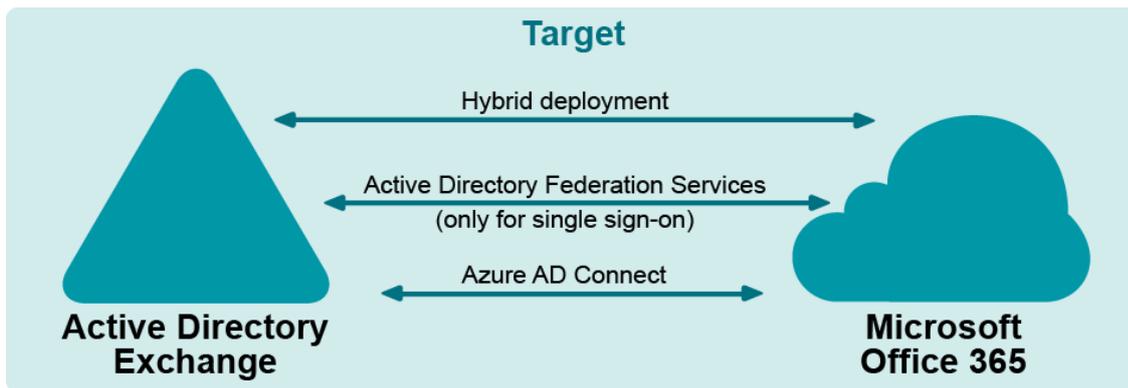
The typical use case for this scenario is when one company buys another, and the newly-acquired company needs to merge in its directory and mail system.



Migration Manager provides an ability to migrate users' mailboxes from the acquired company directly to Microsoft Office 365 without the need to firstly migrate them to on-premises Exchange organization.

Prerequisites

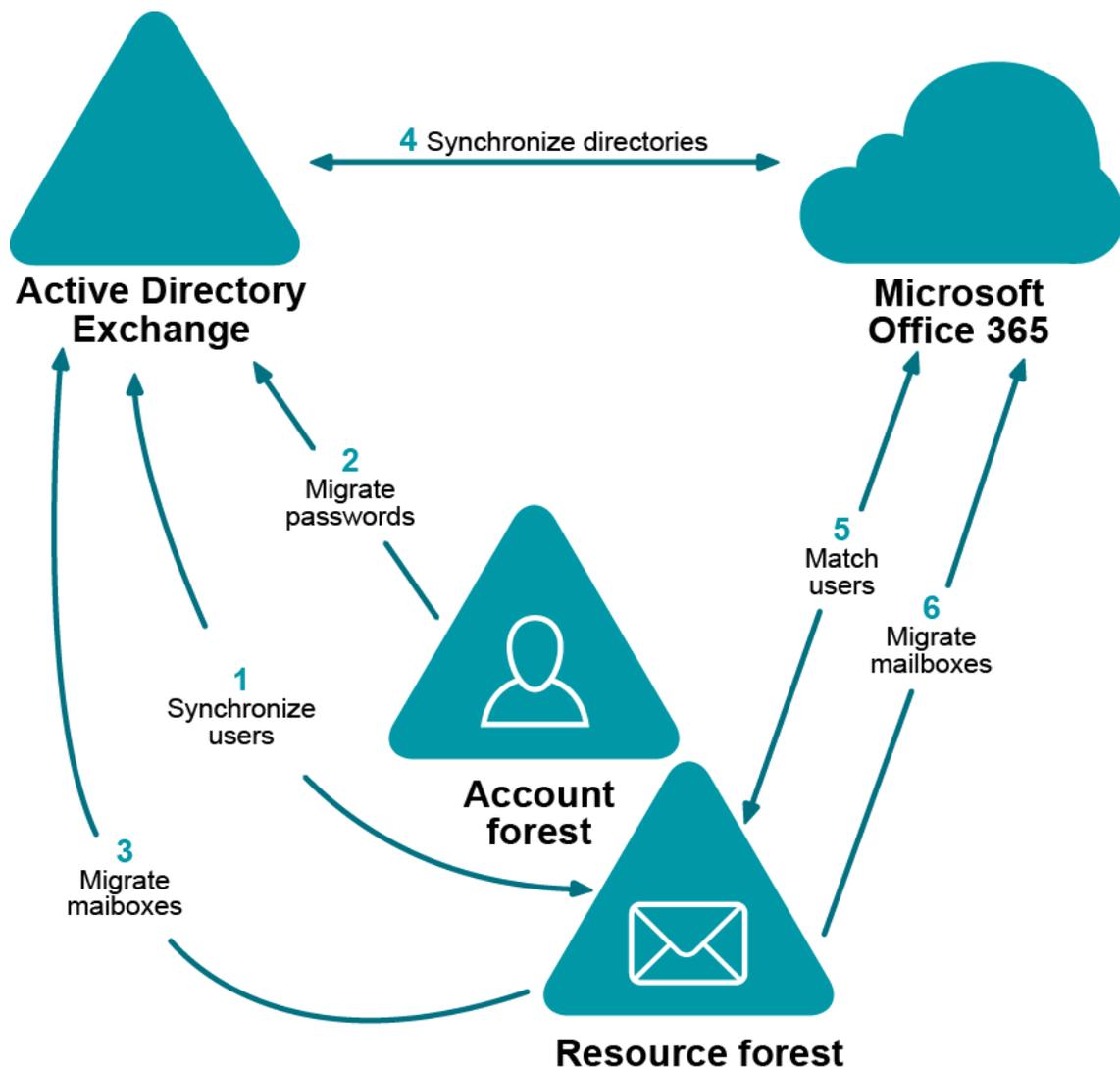
- The source environment uses a separate Exchange resource domain in addition to an account domain.
- The target environment is an Exchange hybrid deployment.



Procedure

Pre-migration task: Establish Mail Flow to Source Exchange Organization

1. On-Premises Directory Migration: Synchronizing Users
2. On-Premises Directory Migration: Migrating Passwords
3. On-Premises Mailbox Migration
4. Cloud Directory Migration
5. User Matching
6. Cloud Mailbox Migration



Establish Mail Flow to Source Exchange Organization

Since additional domains (for instance, source.local) will be used for mail redirection purposes, the corresponding Exchange connectors should be set up to establish proper mail flow.

Mail redirection from target to source on-premises organization

In order to enable mail redirection from the target to the source on-premises organization using @source.local namespace, add a new send connector on the target on-premises Exchange server with the following settings:

- Specify the mail delivery options depending on your organization specifics and Exchange Server version. For details, please refer to Microsoft documentation available [here](#).
- Add a SMTP address space with the source.local domain.

Mail redirection from Microsoft Office 365 to source organization

Enabling mail redirection from Microsoft Office 365 to the source organization depends on the domain suffix that will be used for the cloud-related mail redirection purposes. If the domain name is publicly available (MX records are registered in public DNS and point to source Exchange server) no additional connectors are required.

In case the domain suffix is not publicly available, the corresponding connector in Microsoft Office 365 should be created to relay mail to the on-premises target Exchange server which, in its turn, should relay mail to the source Exchange server.

On-Premises Directory Migration

On-Premises directory migration consists of two major steps:

1. [Synchronizing Users](#)
2. [Migrating Passwords](#)

Synchronizing Users

Migrate users from the source resource domain to the target Active Directory domain (the one that is synchronized with Microsoft Office 365).

What will you achieve

- Mail-enabled users that have the **targetAddress** attribute pointing to source mailboxes will be created.
- Mail sent to newly created mail-enabled users using on-premises Global Access List (GAL) will be delivered to the corresponding source mailboxes

How do you do that

Configure directory synchronization from the source resource domain to the target Active Directory domain so that the target GAL is populated with the objects from the source domain.

For that, take the following steps:

1. Open Migration Manager for Active Directory Console.

i | **NOTE:** Ensure that the current open project is not the one that is intended for migration to Microsoft Office 365.

2. Install a new Directory Synchronization Agent instance if none installed already. For details, see the *Agent Manager* topic of the *Migration Manager for Active Directory User Guide*.
3. Create a domain pair of the source resource domain and the target Active Directory domain. For information on how to do that, see the *Domain Pairs* section in the *Migration Manager for Active Directory User Guide*.
4. Configure a new synchronization job for the domain pair according to the Configuring the *Synchronization Job* topic of the *Migration Manager for Active Directory User Guide*. Set the following specific options for the synchronization job:
 - **Set Security Settings:**

- The Synchronize passwords option must be cleared.
- Under User Principal Name handling, set the domain suffix of the UPNs to the appropriate domain matching federated domain used in hybrid.
- **Advanced Options:**
 - Select **Use custom add-in** and specify add-in located at `<Migration Manager installation folder>\Active Directory\CopyTargetAddress.xml`.
 - Click **Attributes to Skip** and select to skip all attributes that should not be migrated from resource domain to avoid overwriting attributes during migration.
- **Specify Exchange Options:**
 - Select the **Mail-enabled users** option
 - Specify the target SMTP address template (e.g. **target.local**)
 - Specify the source SMTP address template (e.g. **source.local**)

i **NOTE:** Since the source.local redirection domain will be also used in Microsoft Office 365, it should be publicly available, or the corresponding connectors should be created in Microsoft Office 365 to establish mail flow.

5. Start the configured directory synchronization job as described in Starting and Stopping Directory Synchronization topic of the Migration Manager for Active Directory User Guide, and wait until initial synchronization completes.

How do you verify that step worked

1. Create a test mailbox in the target on-premises organization.
2. Using GAL, send a test message to any mail-enabled user created by Directory Synchronization Agent (DSA).
3. Open the source user's mailbox and check that the message is delivered successfully.
4. Reply that message and ensure that it arrived to the target mailbox.
5. Repeat the above steps using any mailbox outside your organization to check that original and reply messages are delivered successfully.

Additional information

For details, see the following topics in the Migration Manager for Active Directory User Guide:

- Pre-Migration Activities
- Directory Synchronization

Migrating Passwords

Migrate passwords for the users from the source account domain to the target Active Directory domain.

What will you achieve

Users will be able to log on to the target on-premises domain with their source account passwords.

How do you do that

Configure a new migration session from the account domain to target Active Directory domain so that users' passwords become in sync.

For that, take the following steps:

1. In Migration Manager for Active Directory select service attributes different from ones used in user synchronization for the domain pair that consists of the source account domain and the target Active Directory domain. For information on how to do that, see the *Domain Pairs* section in the *Migration Manager for Active Directory User Guide*.
2. Create a new migration session according to the *Creating a Migration Session* topic of the *Migration Manager for Active Directory User Guide*. Set the following specific options for the migration session:
 - **Select Source Objects:** Click **Import** and provide a plain-text file that contains pairs of **distinguishedName** attributes from the source account domain and the corresponding mail attributes from the target on-premises domain for each user, one per line.
 - **Set Security Settings:**
 - Under **User Principal Name handling**, set the domain suffix of the UPNs to the appropriate domain matching federated domain used in hybrid.
 - Set **Password handling** to **Copy account password** so that source account password will be copied to the target Active Directory domain. That is required to enable access to Microsoft Office 365 with the same password through SSO.
 - **Object Processing:**
 - Select the **Enable target accounts** option so that migrated accounts will be able to access target Active Directory domain as well as Microsoft Office 365 with the same password through SSO.
 - Click **Attributes to Skip** and select to skip **displayName** attribute as well as other attributes that should not be migrated from account domain to avoid overwriting attributes during migration.

3 Complete the wizard to start the migration session.

How do you verify that step worked

Once migration session completes, log on to any migrated user account using the same password as the user has in the source organization.

Additional information

For details, see the following topics in the Migration Manager for Active Directory User Guide:

- Pre-Migration Activities
- Account Migration

On-Premises Mailbox Migration

If you need to migrate some of mailboxes to the on-premises part of the target hybrid, you can do that now. For detailed information on how to do that, refer to *Migration Manager for Exchange User Guide*.

i **NOTE:** Before performing on-premises mailbox migration in Migration Manager for Exchange console, ensure that the current open project is not the one that is intended for migration to Microsoft Office 365.

Cloud Directory Migration

Provision users from the source resource domain that were previously created in the target Active Directory domain to Microsoft Office 365.

What will you achieve

- Accounts from source domain will be listed in the Microsoft Office 365 Global Access List (GAL)
- Mail sent by cloud users to mailboxes from the source resource domain will be delivered successfully.
- Mail users will be created in Microsoft Office 365 and their **ExternalEmailAddress** property will point to corresponding mailboxes in the source resource domain.

How do you do that

This step is performed automatically by Microsoft Azure AD Connect as soon as mail-enabled users have been created in the target Active Directory domain by Directory Synchronization Agent.

i **NOTE:** Note that the new users created in target Active Directory domain are not immediately processed by Microsoft Azure AD Connect. Therefore, wait until Microsoft Azure AD Connect completes synchronizing directories before proceeding.

How do you verify that step worked

1. Sign in to Microsoft Office 365 under any licensed user, open address book, select any user from source organization and send a test message to that user.
2. Open the source user's mailbox, check that the message arrived successfully, and reply to it.
3. Make sure that reply message is delivered to cloud recipient.
4. Repeat the above steps using any mailbox outside your organization to check original and reply messages are delivered successfully.

User Matching

Match users in the source Active Directory domain with users in the target Microsoft Office 365 tenant.

What will you achieve

- Mailboxes from the source Active Directory domain will be matched with the corresponding Microsoft Office 365 mail users.
- The Location property will be populated for the Microsoft Office 365 users.

How do you do that

Configure new migration from source resource domain to Microsoft Office 365 in Migration Manager for Active Directory (Microsoft Office 365) console to match accounts.

Set up a new migration as follows:

1. [Install](#) a Directory Migration Agent instance if none installed already.
2. [Configure migration pair](#) of source Active Directory domain and target Microsoft Office 365 tenant.

3. Specify the mail redirection domain for the migration pair. When choosing mail redirection domain, take the following into account:
 - This domain must be accepted in on-premises domain only
 - The domain must not be accepted in Microsoft Office 365.

i **NOTE:** The `source.local` domain used for Directory Synchronization can be used as redirection domain if it is publicly available or corresponding connectors exist in Office 365 tenant. If centralized mail transport is enabled in your hybrid deployment, you can use the existing on-premises connector for this purpose.

4. Select the **Empty Active Directory to Microsoft Office 365 mapping template** for the migration pair.
5. **Create a static collection** including all objects from the source Active Directory domain.
6. **Start a new migration task** with the following options:
 - The **Create new objects on target** option cleared
 - The **Merge into existing objects** on target option selected
 - The UPN suffix set to the corresponding federated domain in Microsoft Office 365

How do you verify that step worked

To ensure that the above procedure succeeded, check that the Location property is populated for the Microsoft Office 365 users.

Additional information

For details, see the [Provisioning User Accounts in Office 365](#) section.

Cloud Mailbox Migration

Once all accounts are provisioned to Microsoft Office 365 tenant and mail flow is established, migrate mailboxes from the source resource domain to the Microsoft Office 365 tenant and synchronize the calendars using Migration Manager for Exchange. After that perform a mailbox switch so that incoming mail start going to the Microsoft Office 365.

i **NOTE:** Before performing any migration tasks, ensure that the current open project in Migration Manager for Exchange console is the same as you used in Migration Manager for Active Directory (Microsoft Office 365) Console for matching users with Microsoft Office 365.

- [Synchronize calendars](#)
- [Migrate mailboxes](#)
- [Perform mailbox switch](#)

Synchronize calendars

What will you achieve

- Cloud mail users will be converted to mailboxes with valid licenses assigned (if not already converted).
- Users from the source organization and users from Microsoft Office 365 will be able to view each other's free/busy information and schedule meetings.

How to do that

Synchronize calendars using Migration Manager for Exchange as described step-by-step in [Synchronizing Calendars](#).

How do you verify that step worked

1. Sign in to Microsoft Office 365 under any licensed user and create a test meeting.
2. Open any source mailbox and verify that the cloud user under which you created the meeting is busy at the time of the meeting.
3. Then create another test meeting in that source mailbox.
4. From Microsoft Office 365, ensure that the source user is busy at the time of the new meeting.

Migrate mailboxes

What will you achieve

- Cloud mail users will be converted to mailboxes with valid licenses assigned (if not already converted).
- Users from the source organization can sign in to the cloud through SSO and access mailbox data migrated from their mailboxes.

How to do that

Migrate mailboxes using Migration Manager for Exchange as described step-by-step in [Migrating Mailboxes](#).

How do you verify that step worked

1. Sign in to Microsoft Office 365 under any licensed user, open address book, select any user from source organization and send a test message to that user.
2. Open the source user's mailbox, check that the message arrived successfully, and reply to it.
3. Make sure that reply message is delivered to cloud recipient.
4. Repeat the above steps using any mailbox outside your organization to check original and reply messages are delivered successfully.

Perform mailbox switch

Once calendars are synchronized and mailboxes are migrated to Microsoft Office 365, mailboxes can be switched using Migration Manager for Exchange. Mailbox switch allows all the Migration Manager for Exchange components to recognize the mailbox as switched and ensures that all new mail now arrives in the user's cloud mailbox.

What will you achieve

All incoming mail is delivered to Microsoft Office 365 mailboxes instead of on-premises mailboxes.

How to do that

[Mailbox switch](#) can be done either manually from the console or automatically by the Migration Agent for Exchange. This is configured through options in the collection that the mailbox is in. If you choose automatic switching, you can either schedule the mailbox switch operation for a specified time or have the agent switch each mailbox as soon as it is synchronized.

How do you verify that step worked

1. Sign in to Microsoft Office 365 under any licensed user, open address book, select user from source organization that has been switched and send a test message to that user.
2. Open any source user mailbox, open address book; select the same user as on step 1 and send another test message to that user.
3. Sign in to Microsoft Office 365 under the user to whom you sent messages on the above steps, ensure that messages arrived successfully and reply to them.
4. Ensure that reply messages are successfully delivered to recipients.

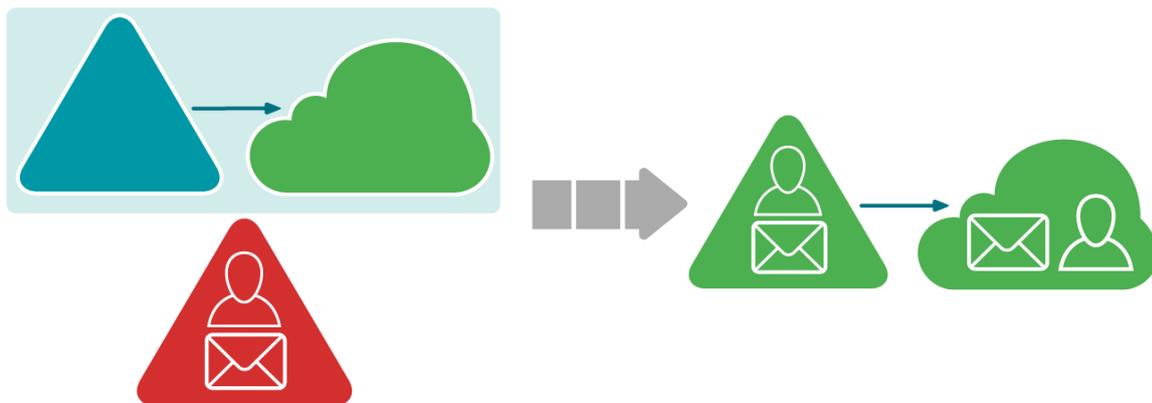
Additional information

For detailed information on mailbox switch, see the *Mailbox Switch* topic under the *Mailbox Migration Process* section in the *Migration Manager for Exchange User Guide*.

Reorganization or Upgrade with a Hybrid

The migration involves moving existing on-premises environment to a “greenfield” hybrid deployment. This entails a change of domain name for the objects that are migrated. In general, primary SMTP addresses of existing objects are not changed in course of migration.

The typical use case for this scenario is when a company optimizes its directory and mail operations, and one or more forests are merged into a single clean hybrid.



Prerequisites

- The source environment is a regular Active Directory forest with an Exchange organization.
- The target is a specifically pre-configured domain with a hybrid deployment.

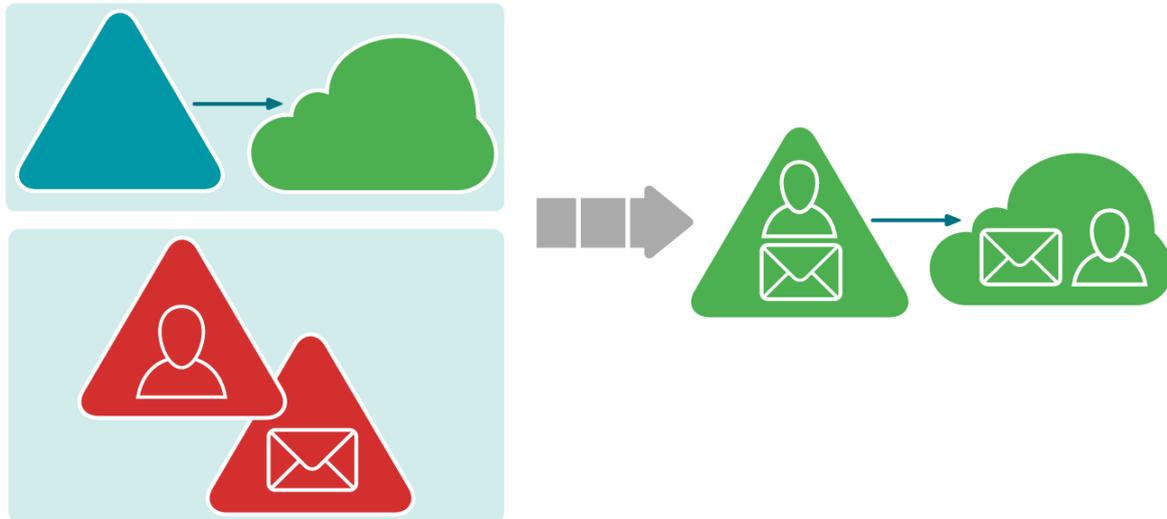
Procedure

The procedure is the same as for the *Acquisition with a Hybrid* scenario. Therefore to implement this scenario, follow the steps described [here](#).

Complex Reorganization or Upgrade with a Hybrid

The migration involves moving existing on-premises environment with dedicated Exchange forest to a “greenfield” hybrid deployment. This entails a change of domain name for the objects that are migrated. In general, primary SMTP addresses of existing objects are not changed in course of migration.

The typical use case for this scenario is when a company optimizes its directory and mail operations, and one or more forests are merged into a single clean hybrid.



Prerequisites

- The source environment uses a separate Exchange resource domain in addition to an account domain.
- The target is a specifically pre-configured forest with a hybrid deployment.

Procedure

The procedure is the same as for the *Complex Acquisition with a Hybrid* scenario. Therefore to implement this scenario, follow the steps described [here](#).

Advanced Migration Topics

This topic contains information, how to support Single Sign-On (SSO) using Migration Manager, and how to benefit from Migration Manager if you already use Microsoft Azure AD Connect to synchronize user accounts with Microsoft Office 365.

- [Supporting Single Sign-On \(SSO\) using Migration Manager](#)
- [Interoperating with Microsoft Azure AD Connect](#)

Supporting Single Sign-On (SSO) using Migration Manager

Single Sign-On (SSO) technology provides users an ability to login to trusted Active Directory domain or Microsoft Office 365 under the same credentials that they use in Active Directory where they reside. If you already have Active Directory Federation Services (AD FS) deployed in your organization and plan to migrate your Exchange environment to Office 365, you can implement SSO for Microsoft Office 365. Migration Manager for Active Directory is capable to ease the process of configuring SSO during migration to Microsoft Office 365. It can create users in federated domain or move existing users to federated domain within Microsoft Office 365 subscription; such users are capable of logging in through Single Sign-On as soon as they get a Microsoft Office 365 account.

Implementing SSO by means of Migration Manager for Active Directory allows getting the following benefits for mailbox migration over common scenario that includes using Microsoft Azure AD Connect:

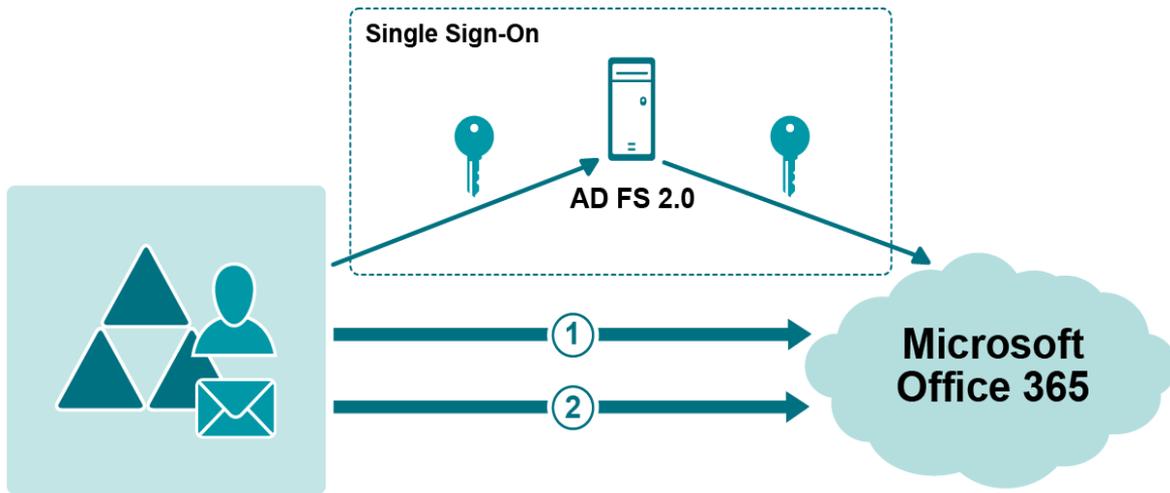
- Mail migration from multiple Exchange organizations
- Online migration from Exchange 2003
- Item-by-item migration with ability to safely rollback changes

CAUTION: Rollback tasks that move accounts from a federated domain to a non-federated domain (or the other way around) complete with errors. To avoid this issue, perform an explicit migration to a non-federated (or federated, respectively) domain first, and then perform the rollback task.

If you plan to implement SSO using Migration Manager for Active Directory, note that Active Directory Federation Services (AD FS) 2.0 must be deployed in your organization.

NOTE: If Microsoft Azure AD Connect already provisioned user accounts in Microsoft Office 365 or is managing them, then you can still support SSO and take advantage of using Migration Manager for mail migration in some environment configurations. For more information, refer to the [Interoperating with Microsoft Azure AD Connect](#) section.

The following figure denotes overall environment configuration with SSO implemented using Migration Manager:



- ① Provision user accounts using Migration Manager for Active Directory
- ② Synchronize calendars and migrate mailboxes using Migration Manager for Exchange

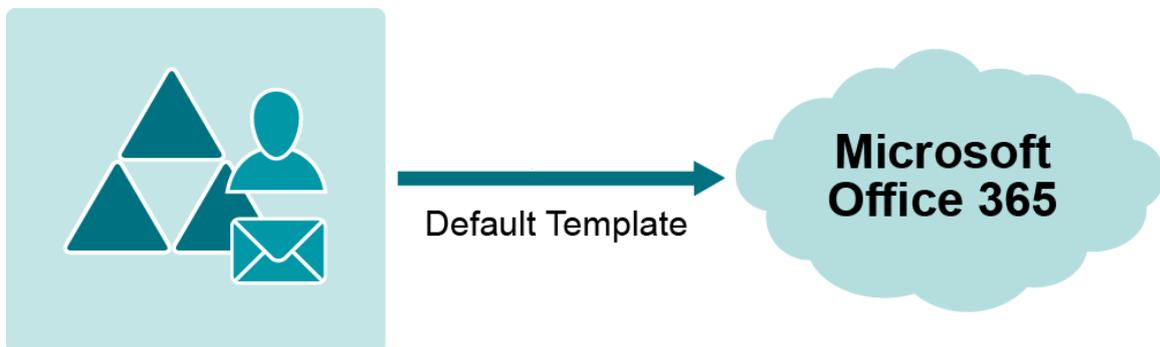
Migration Manager for Active Directory supports basic environment configuration where Active Directory and Exchange organization are located in the same forest as well as more sophisticated environment configuration with separate authentication and Exchange resource forests.

Specific for each environment configuration steps that should be taken to migrate to Microsoft Office 365 while taking advantage of Single Sign-On are described below.

Basic Migration Scenario

If your Active Directory and Exchange organization reside in the same forest, then to migrate to Microsoft Office 365 with support of Single Sign-On you need to perform the following steps:

1. Ensure that AD FS 2.0 is deployed in your environment. Do not start directory synchronization using Microsoft Azure AD Connect. If synchronization is already started make sure that the tool does not manage user accounts planned to be migrated using Migration Manager.
2. [Provision user accounts](#) in Microsoft Office 365 using Migration Manager for Active Directory (Microsoft Office 365) console. Directory Migration Agent will set up SSO support automatically. Note that you need to use the default [mapping template](#).



3. [Synchronize calendars](#) and [migrate mailboxes](#) using Migration Manager for Exchange.

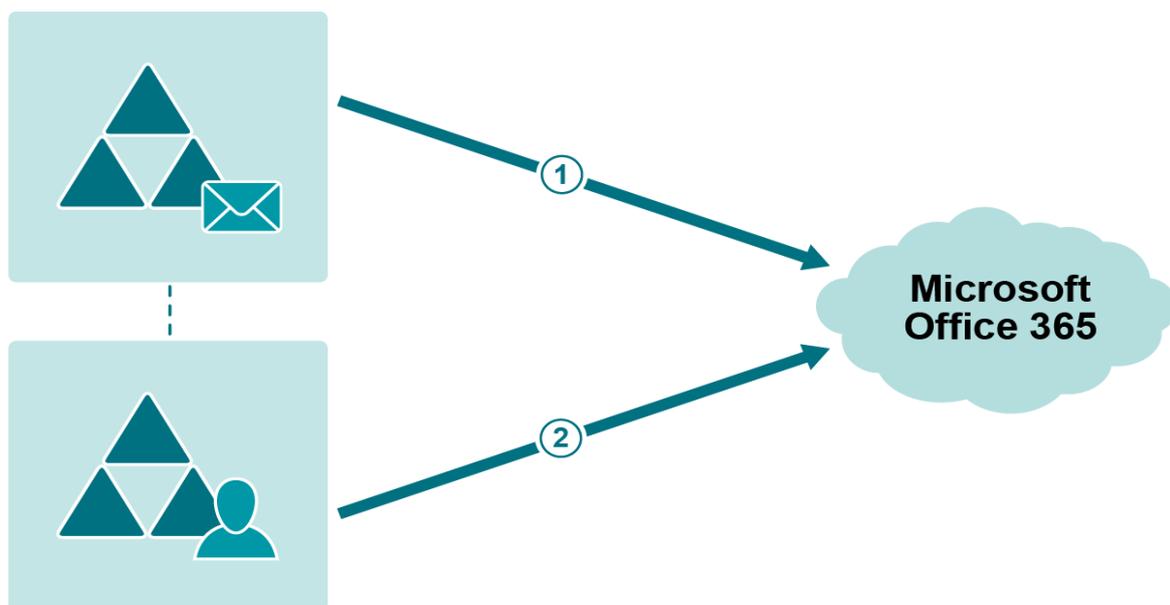
Users can log in through Single Sign-On as soon as they get a Microsoft Office 365 account.

After mail data is migrated and mailboxes are switched, you can enable Microsoft Azure AD Connect to keep user accounts synchronized.

ERF Migration Scenario

With Migration Manager you can migrate from an environment with separate authentication and Exchange resource forests (ERF) to Microsoft Office 365 to Microsoft Office 365 while taking advantage of Single Sign-On. Migration Manager for Active Directory features special migration templates for that. To migrate to Microsoft Office 365 with support of Single Sign-On you need to perform the following steps:

1. Ensure that AD FS 2.0 is deployed in your environment. Do not start directory synchronization using Microsoft Azure AD Connect.
2. **Provision user accounts** in Microsoft Office 365 using Migration Manager for Active Directory (Microsoft Office 365) console. Note that you need to **migrate** accounts twice:
 - a. First, you should synchronize or migrate users from Exchange resource forest using the **ERF mapping template**. That lets you populate the Office 365 Global Address List (GAL) from the Exchange resource forest.
 - b. Second, you need to migrate (or synchronize) users from Active Directory authentication forest using the **Activate SSO mapping template**. That template enables federation between the authentication forest and the Office 365 subscription.



① ERF Template

② Activate SSO Template

i **NOTE:** Using the ERF template, you make sure that federation with the separate authentication forest is not broken by ongoing GAL coexistence between the Exchange resource forest and the Microsoft Office 365 subscription.

3. **Synchronize calendars** and **migrate mailboxes** using Migration Manager for Exchange.

Users can log in through Single Sign-On as soon as they get a Microsoft Office 365 account.

After mail data is migrated and mailboxes are switched, you can enable Microsoft Azure AD Connect to keep user accounts synchronized.

Interoperating with Microsoft Azure AD Connect

If Microsoft Azure AD Connect is already synchronizing user accounts with Microsoft Office 365 in your organization, you can still take an advantage of using Migration Manager for mail migration in certain environment configurations.

i **NOTE:** Windows Azure Active Directory Sync (DirSync) and Azure AD Sync Azure AD Connect are also supported for this scenario. However, these tools are now deprecated by Microsoft and will reach end of support on April 13, 2017. So if still you use one of them, it is recommended to upgrade to Azure AD Connect.

Using Migration Manager along with Microsoft Azure AD Connect allows getting the following benefits for mail migration:

1. Migrate mailboxes using Migration Manager for Exchange:
 - Ability to avoid excess steps in certain migration scenarios
 - Mail migration from multiple Exchange organizations
 - Online migration from Exchange 2003
 - Item-by-item migration with ability to safely rollback changes
2. Process the *Send on behalf*, *Send as*, and *Full Mailbox Access* permissions.
3. Support Single Sign-On (SSO) by means of Microsoft Azure AD Connect right from the beginning of migration.

Migration Manager is able to work with objects created and managed by Microsoft Azure AD Connect. However as majority of mail-related object attributes are already synced by the Microsoft Azure AD Connect, they are not meant to be synced by Migration Manager. The goal of Migration Manager in this case is to establish proper matching of objects, and also set location attributes and mail redirection settings for the objects so that mail migration using Migration Manager for Exchange could be performed.

The following restrictions apply in such configuration:

- The Active Directory object that Microsoft Azure AD Connect treats as the source should be mail-enabled. This is typical for environments with a consolidated Active Directory forest or for environments with separate authentication and Exchange resource forests.
- It is strongly recommended to use only the **Empty Active Directory to Microsoft Office 365** mapping template during migrating objects and synchronizing directories. If you need to process specific permissions such as Send on behalf, add the corresponding mapping rules to the template.
- If you experienced that X.400 addresses from the EmailAddresses attribute are not synced by Microsoft Azure AD Connect, then do not try to sync them using Migration Manager. They will not be synced properly even if you add the corresponding mapping rules to the mapping template.

- If ongoing directory synchronization is established between forest where mailboxes reside and authentication Active Directory forest using Migration Manager for Active Directory or any other third-party synchronization tool, then it should be turned off while migrating to Microsoft Office 365. Otherwise, an additional domain should be set up in the Exchange organization for mail redirection using the **Edit Mail Redirection Domain** action item for the corresponding migration pair in Migration Manager for Active Directory (Microsoft Office 365) console.

! **CAUTION:** The mailboxes to be migrated with Migration Manager reside in the domain you specify. The domain must be accessible from the Internet for mail delivery and must not be listed as an accepted domain for the Microsoft Office 365 tenant.

i **NOTE:** Setting up the mail redirection domain ensures that mail can be successfully redirected from Microsoft Office 365 to the source Exchange organization.

Troubleshooting Migration to Microsoft Office 365

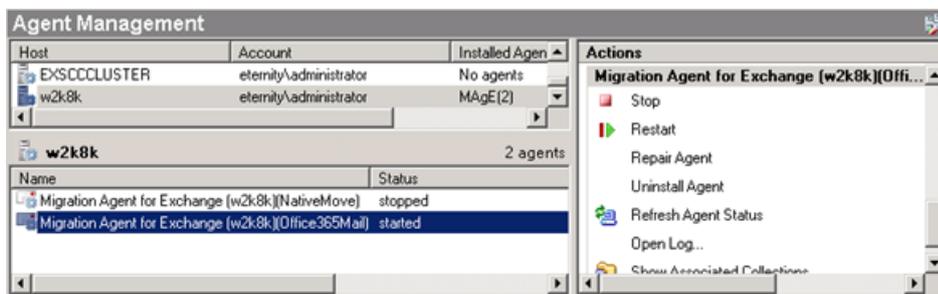
During the migration, a variety of issues may occur. This section describes some common problems and how to solve them, as follows:

- [Managing Migration Agent for Exchange](#)
- [Other Problems: Checking the Logs](#)

Managing Migration Agent for Exchange

Migration Agent for Exchange is the central component in the Office 365 migration workflow. To manage the Migration Agent for Exchange, perform the following:

1. In **Agent Management** of Migration Manager for Exchange, select the agent host where Migration Agent for Exchange (abbreviated to MAgE) is installed.
2. Select the **Migration Agent for Exchange** entry in the agent list below.



3. Use the commands in the Migration Agent for Exchange section of the Actions pane to control the agent and view its log.

CAUTION: If the agent consistently fails to start, try reinstalling it. For that use the **Repair Agent** action item.

Other Problems: Checking the Logs

If an unknown error occurs, you should refer to the logs written by the Migration Manager. The logs for the console and the agent are stored on the corresponding computers in the following locations:

Migration Manager for Active Directory (Microsoft Office 365)

Console log:

On any supported operating system Migration Manager for Active Directory (Office 365) console log is located at the following path: **%PROGRAMDATA%\Quest Software\Migration Manager for Active Directory\Directory Migration\QsDirectoryMigrationEngine.log**.

Agent log:

On any supported operating system Directory Migration Agent log is located at the following path: **%PROGRAMDATA%\Quest Software\Migration Manager for Active Directory\Directory Migration\QsDirectoryMigrationAgent.log**.

Migration Manager for Exchange

Console log:

On any supported operating system Migration Manager for Exchange console log is located at the following path: *%ProgramFiles%\Quest Software\Migration Manager\Exchange Data\EMWMigration.log*.

Agent log:

To view Migration Agent for Exchange log, use the **Open Log** action item as described in the [Managing Migration Agent for Exchange](#) section.

Public folder synchronization agents logs:

Log files are located at the installation path for the agents.

By default the shared QMMEx\$ServerName\$ folder is created in the **%SystemRoot%\System32** folder. On 64-bit Microsoft Exchange, the default shared folder is created in the **%SystemRoot%\SysWOW64** folder.

About us

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

Technical support resources

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

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

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