



Quest® On Demand Migration for Email
1.16.0.24077 (11/18/2020)

User Guide



© 2022 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.

On Demand Migration for Email User Guide

Updated - September 15, 2022

Contents

Introduction	6
Welcome	6
System Requirements	6
Subscribing to the Service	7
Creating a Quest Account	7
Trial Subscription	8
License Subscription	8
Getting Started for New Users	9
Roles and Permissions	11
Using Azure AD Single Sign-On to Access ODME	12
Overview of The Migration Process	13
Preparing a Migration	16
Configuring and Running a Migration	16
Post Migration	16
Preparing Migrations	17
Choosing a Migration Type	17
Setting Up Mail Routing	17
Deciding How to Configure Your Shared Address Space	17
Source Email Service	17
Exchange 2007/2010/2013/2016/2019	18
G Suite	18
Microsoft 365 (Cloud Relay)	23
Zimbra	24
Sun ONE/iPlanet	25
Initial Target Mail Hosts	25
Microsoft 365	26
Exchange 2010/2013/2016/2019	27
Creating Target Mailboxes	27
Preparing Your Source Email Service for Migration	27
G Suite	27
Sun ONE/iPlanet	28
Microsoft Exchange 2007/2010/2013/2016/2019	28
Enabling Application Impersonation Rights	28
Accessing the Mail Server	29
Specifying Administrator Credentials	29
Upgrade Throttling Policies (Microsoft Exchange 2010/2013/2016/2019)	30
Microsoft 365	30
Required Permissions	30
Upgrade Throttling Policies	31

POP/Windows Live Hotmail	31
IMAP	32
Zimbra	32
Preparing Your Target Email Service for Migration	33
Microsoft 365	33
Required Permissions	33
Provisioning	34
Upgrade Throttling Policies	34
Disable In-Place Hold and Litigation Hold	34
Microsoft Exchange 2010/2013/2016/2019	35
Enabling Application Impersonation Rights	35
Accessing the Mail Server	35
Provisioning	35
Upgrade Throttling Policies	36
Disable In-Place Hold and Litigation Hold	36
Test and Pilot Migrations	38
Configuring and Running Migrations	39
Creating a Migration Plan	39
Dashboard	39
Copying Migration Plans	40
Managing Migration Templates	40
Connecting to Email Services	41
Connecting to the Source Email Service	41
G Suite	42
Sun ONE/iPlanet	43
Microsoft Exchange 2007/2010/2013/2016/2019	43
Microsoft 365	44
Windows Live Hotmail	45
POP	45
IMAP	45
Zimbra	45
Connecting to the Target Email Service	46
Microsoft 365	46
Microsoft Exchange 2010/2013/2016/2019	47
Using Self-Signed SSL Certificates	48
Validating Connections	48
G Suite	49
Sun ONE/iPlanet	50
Microsoft Exchange 2007/2010/2013/2016/2019	50
Microsoft 365	51
POP/Windows Live Hotmail	51
IMAP	51
Zimbra	52
Adding Mailboxes	52

Adding Mailboxes Manually	54
Adding Mailboxes through a TSV File	54
Selecting Migration Options	56
Selecting Items to Migrate	57
Filtering Mailbox Folders	59
Migrating Delegate Access Permissions	59
Migrating Folder Permissions	61
Migrating Rules	62
Setting Up Mail Forwarding	68
Managing Google Throttling	70
Updating Outlook Client Profiles	71
Limiting Concurrent Migrations	74
Setting User Notifications	74
Known Issues and Limitations	75
Known Limitations	75
General	75
Client Profile Updating Utility	75
Microsoft Exchange	76
Microsoft 365	77
POP/Windows Live Hotmail	79
IMAP	79
G Suite	79
Zimbra	81
Known Issues	82
Running Migration	82
Migration Concurrency	84
Re-migration	84
Post Migration	85
Viewing Migration Reports	85
Executive Summary Report	85
Migration Summary Report	85
Billing Summary Report	86
Migration Details Report	86
Per Mailbox Statistics Report	87
Notify and Train Users	87
Third Party Assessments and Certifications	88
Glossary	89
About us	91
Technical support resources	91

Introduction

Welcome

On Demand Migration for Email (ODME) securely migrates data to Microsoft 365 and on-premises Exchange or hosted Exchange email platforms without requiring organizations to install or maintain any software for the move. From a single console, you can migrate multiple mailboxes simultaneously, including data such as email, calendar, contacts, and tasks.

System Requirements

Before using ODME, ensure that your system meets the following minimum software requirements:

Table 1: System requirements

Requirement	Details
Browser	Internet Explorer 11, 10, and 9; Firefox (latest); Chrome (latest)

ODME securely migrates data to Microsoft 365 and on-premises Exchange from the following source email platforms:

Table 2: Supported source platforms

Source Platform	Supported Versions and Other Details
Microsoft Exchange Server	Microsoft Exchange Server 2019, 2016, 2013, 2010 Service Pack 1 or later, 2007 NOTE: Personal archives can be migrated only from Exchange Server 2010, 2013, 2016, and 2019.
Microsoft 365	Current version NOTE: ODME supports migration of personal archives from the source Microsoft 365 to the target Microsoft 365.
Zimbra	Zimbra 8, 7
G Suite	Current version NOTE: ODME does not migrate Tasks from G Suite.
Sun ONE/iPlanet	Sun One mail server 6, 5 NOTE: <ul style="list-style-type: none">• ODME uses IMAP to migrate messages and folders from your Sun ONE/iPlanet server.• ODME does not migrate Contacts, Calendars, and Tasks from Sun ONE/iPlanet.

Source Platform	Supported Versions and Other Details
Microsoft Hotmail	Current version NOTE: ODME uses POP3 to migrate messages and folders from Microsoft Hotmail.
Yahoo	Current version
All servers that supported the IMAP protocol	N/A
All servers that supported the POP3 protocol	N/A

For the list of migrated items and other details, please see [Selecting Items to Migrate](#).

For a complete list of items that are not migrated, see [Known Limitations](#).

Table 3: Supported target platforms

Target Platform	Supported Versions
Microsoft Exchange Server	Microsoft Exchange Server 2019, 2016, 2013, 2010 Service Pack 1 or later
Microsoft 365	Current version

Updating Outlook Client Profiles

Client Profile Updating Utility is used to switch end-user Microsoft Outlook Client Profiles from the source Exchange server or Microsoft 365 to the target Exchange server or Microsoft 365 once the user's mailbox is migrated.

Limitations and requirements:

- To enable the CPUU integration feature on the source Exchange Server 2007, you should turn on and configure the WebDAV API access for your Exchange Server 2007.

For more details, please see [Updating Outlook Client Profiles](#).

Subscribing to the Service

- [Creating a Quest Account](#)
- [Trial Subscription](#)
- [License Subscription](#)

Creating a Quest Account

Active Quest Account is required to access Quest On Demand Services.

To register a Quest Account

1. Go to the Quest On Demand Services website: <https://portal.ondemand.quest.com/>
2. Click **Try** or **Subscribe** next to the Quest On Demand Migration for Email service. The **Create a New Account** screen opens.
3. Enter the company and user information required to set up your Quest Account. Follow the on-screen instructions.
4. We create your account and send you a confirmation by email. Follow the instructions in the email to activate your email address.
5. Then use this account to register for Quest On Demand Migration for Email.

Trial Subscription

Your 30-day free trial subscription begins on the date that you activate your trial subscription to an Quest On Demand Migration for Email service. It doesn't begin on the date that you requested the trial.

To get and activate a trial subscription

1. Go to the Quest On Demand Services website: <https://portal.ondemand.quest.com/>
2. Click **Try** next to the Quest On Demand Migration for Email service. The **Create a New Account** screen opens.
3. If you already have a Quest Account, click **Sign In** and enter your user name and password. Otherwise, you have to create a [Quest Account](#).
4. On the **Try On Demand Migration for Email** screen, you have to specify the nearest data center to maximize the service performance.
5. Then, read and accept the terms and conditions of the Trial Agreement before continuing.

i **NOTE:** Your migrations are limited in the trial version of the ODME service. You can migrate only 25 messages, 5 contacts, 25 appointments, 5 tasks, 5 notes and 50 recoverable items per mailbox. Number of mailboxes is limited to 5.

6. Click **Open On Demand Migration for Email** to activate your trial subscription.

License Subscription

Use this option if you already have a license or a coupon code to access the Quest On Demand Migration for Email Service.

To access the ODME service using a license key or coupon code

1. Go to the Quest On Demand Services website: <https://portal.ondemand.quest.com/>
2. Click **Subscribe** next to the Quest On Demand Migration for Email service. The **Create a New Account** screen opens.
3. If you already have a Quest Account, click **Sign In** and enter your user name and password. Otherwise, you have to create a [Quest Account](#).

4. If you already have a license key or coupon code, select **Yes** under **Choose a Plan** and enter your key on the **Subscription Options**. Then press **Continue**.
5. On the **Activate Your Subscription** screen, specify the nearest data center to maximize the service performance.
6. Then, read and accept the terms and conditions of the Services Agreement.
7. Press **Activate Subscription**.

Getting Started for New Users

This section provides basic instructions on how to use On Demand Migration for Email.

1. Log in the [ODME Portal](#). For more details about how to get the service subscription, refer [Subscribing to the Service](#).
2. The **Dashboard** screen opens. Here you can create a migration plan. For that, press the **New Plan** button at the bottom of the screen.
You can also create a migration plan from a template if available. To do this, select a template from the drop-down list in the dialog box where you create the migration plan.
3. Once an ODME Plan is created, there are four steps: **Connections**, **Mailboxes**, **Options** and **Migrate**:
 - **Connections**
On the first step, you need to specify Source and Target details so that ODME can connect to the both endpoints. Some fields may be not editable if your plan was created from a template.

Quest | On Demand Migration for Email

Dashboard >

1 Connections ✓ 2 Mailboxes ✓ 3 Options ✓ 4 Migrate

Source Connection

System: Microsoft Office 365

☒ Use Modern Authentication ⓘ

Authorization: ODME requires permission to access resources in your organization in order to migrate mailboxes. Sign in as an administrative user who can grant consent to ODME.

Sign in with Microsoft

This user must belong to the same Office 365 tenant and have a valid Exchange Online license.

☒ Use Autodiscover ⓘ

Server Name:

[Test Connection...](#)

Target Connection

System: Microsoft Office 365

☒ Use Modern Authentication ⓘ

Authorization: ODME requires permission to access resources in your organization in order to migrate mailboxes. Sign in as an administrative user who can grant consent to ODME.

Sign in with Microsoft

This user must belong to the same Office 365 tenant and have a valid Exchange Online license.

☒ Use Autodiscover ⓘ

Server Name:

[Test Connection...](#)

- **Mailboxes**

On the second step, you need to add the list of mailboxes that you are going to migrate. This can be done manually one by one or using a TSV file.

- **Options**

On the third step, decide whether you want to migrate from a primary mailbox or personal archives. To migrate from personal archives, select the corresponding checkbox, and then select the items you want to migrate. Some fields may not be editable if your migration plan was created from a template.

NOTE: Do not forget to select items for your migration (no matter if you migrate from a primary mailbox or personal archives). Otherwise, nothing will be migrated.

- **Migrate**

Finally, you need to run the migration for all added mailboxes or select mailboxes that you want to migrate.

The screenshot shows the Quest On Demand Migration for Email interface. At the top, there's a header with the Quest logo and the title 'On Demand Migration for Email'. Below this is a progress bar with four steps: 1 Connections (checked), 2 Mailboxes (checked), 3 Options (checked), and 4 Migrate (checked). On the left, there's a 'Migration Checklist' section with three items: 'Connections' (Microsoft Office 365 to Microsoft Office 365), 'Mailboxes' (1 Mailbox), and 'Options' (Migrate Email). Below the checklist, there's a note: 'On Demand Migration for Email will be connecting from the following IPs: 65.52.72.179, 13.70.205.106.' In the center, there's a 'Migration Status' section with a table showing the status of the migration. The table has columns for Status, Source Mailbox, Errors, Processed Items, and Est. Item. The status is 'Completed' for the mailbox 'MNEAdmin@a830edad9050849NDA3020.onmicrosoft...'. At the bottom, there's a 'Migration complete' message and buttons for 'Restart Selected' and 'Start All'.

To get more detailed information on the migration process, see the following sections:

- [Preparing Migrations](#)
- [Configuring and Running Migrations](#)
- [Post Migration](#)

Roles and Permissions

On Demand Migration for Email uses a role-based approach to manage user permissions in the **Users and Roles** tab. The following table describes the migration-related permissions for the default roles **Full Administrator** and **Migration for Email Admin**:

Table 4: Roles and Permissions

Permission	Actions	Full Administrator	Migration for Email Admin
Manage Migration Plans	<ul style="list-style-type: none"> • Create a migration plan from scratch. • Edit / Delete / Rename / Copy a migration plan created from scratch. • The actions defined by the permission Read. 	✓	✓
Execute Migration Plans	<ul style="list-style-type: none"> • Start / Stop / Restart a migration plan created from scratch. 	✓	✓

	<ul style="list-style-type: none"> The actions defined by the permission Read. 		
Manage Migration Plans From Templates	<ul style="list-style-type: none"> Create a migration plan from template. Edit / Delete / Rename / Copy a migration plan created from a template. The actions defined by the permission Read. 	✓	✓
Execute Migration Plans From Templates	<ul style="list-style-type: none"> Start / Stop / Restart a migration plan created from a template. The actions defined by the permission Read. 	✓	✓
Manage Templates	<ul style="list-style-type: none"> Create / Edit / Delete a migration template. The actions defined by the permission Read. 	✓	✓
Read	<ul style="list-style-type: none"> View the existing migration plans (including those created from a template) and templates. Download and view audit logs for a migration template. Download and view all types of reports for a migration. 	✓	✓

i NOTE: Users without any permissions can still log in to ODME and will see a blank page after login, but they cannot work with the product until proper permissions assigned.

Using Azure AD Single Sign-On to Access ODME

Azure Active Directory single sign-on (Azure AD SSO) enables users to access On Demand Migration for Email based on their single organizational account in Azure Active Directory. Single sign-on enables users to authenticate to the application using their single organizational account.

To configure access to On Demand Migration for Email via Azure AD SSO:

1. First, the administrator of your organization must grant On Demand Migration for Email access to your organization's data. To do this, perform the following steps:

- a. Go to <https://portal.ondemand.quest.com/> and click **Sign In**.
- b. In the Sign In dialog, click **Sign in with Microsoft**.

Sign In

Email

Password


[Forgot your Quest Password?](#)

☐ Remember Me

Sign In

[Sign up for a new account](#)

or

 Sign in with Microsoft

- c. Enter Azure AD administrator credentials.
 - d. Click **Accept** in the dialog that opens to grant consent to the On Demand Migration for Email application.
2. After that you can assign the ODME roles to Azure AD security groups directly, so that users in these groups would automatically gain access to ODME.
- a. For that, go to **Users and Roles** tab in ODME, select the role you need and click **Users**.
 - b. Click the **Add Azure Group** button.
 - c. In the dialog that opens, you can choose the group from the drop-down list. This list is populated with Azure AD groups that the user is a member of. You can also specify the group name in the following format: <domain name>\<group name>.

Overview of The Migration Process

This chapter is designed to give new On Demand Migration for Email users an overview of each step in the migration process, which can be divided into three general stages:

1. **Preparing a Migration**— These steps are performed before logging in to On Demand Migration for Email and include preparing your source and target email services for a migration.

2. **Configuring and Running a Migration** — These steps involve connecting to your source and target email services, importing mailboxes, selecting which items to migrate, and then running a migration.
3. **Post-Migration** — These steps are optional and are performed after a migration. They include viewing reports and training users on the new mail system.

i NOTE:

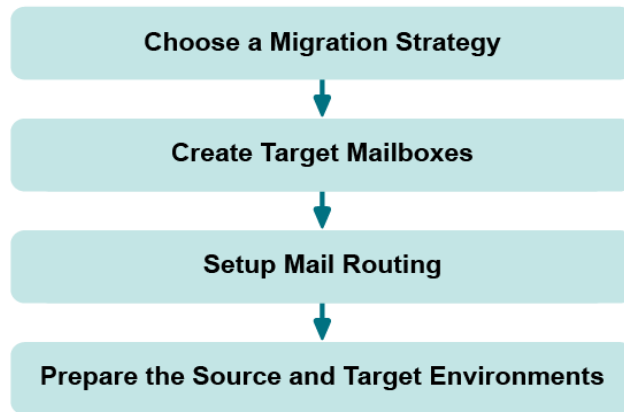
- ODME does not synchronize source changes with the target.
Sample usage scenario: If a message was migrated to the target, the customer delete it in source mailbox and then migrate it again, the migrated message is still in the target in the same folder.
- ODME does not update the Read/Unread status for email messages on the target if this status is changed on the source.

References:

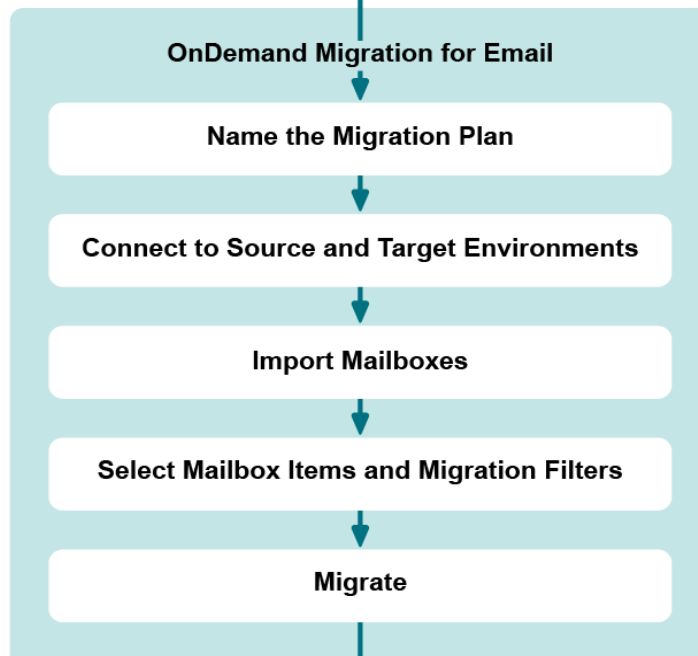
- <https://support.quest.com/on-demand-migration-for-email/kb/181739>
- <https://support.quest.com/on-demand-migration-for-email/kb/206785>

The illustration below shows the stages of the migration process and the order in which each step should be performed.

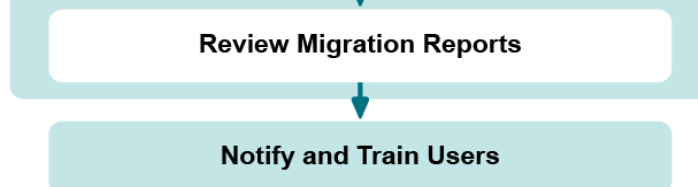
Preparing Migrations



Configuring and Running a Migration



Post Migration



Preparing a Migration

Before running a migration with On Demand Migration for Email, you should consider carefully which migration strategy best suits your needs. Then, if you haven't already done so, you should create the target mailboxes in the target email service and (optionally) implement a mail routing strategy. Lastly, you should configure your source and target email service to ensure that On Demand Migration for Email can connect to each one and execute a migration.

1. **Choose a Migration Strategy** — Depending on various factors, you can choose to perform either a one-time, “big bang” migration (cutover) or perform several staged migrations (co-existence). Choosing the right strategy will minimize migration errors and make it easier for users to transition into the new mail system.
2. **Create Target Mailboxes** — Create the target mailboxes in the target email service. On Demand Migration for Email does not create them for you.
3. **Setup Mail Routing** — Implement a mail routing strategy that will enable users to send and receive mail from both internal and external sources.
4. **Prepare the Source and Target Email Service** — Configure your source and target email services to allow On Demand Migration for Email to connect to them and run a migration.

Configuring and Running a Migration

After you have performed all the necessary preparatory steps, you are ready to login to On Demand Migration for Email and setup and run your migration.

1. **Name the Migration Plan** — Assign a name to the migrations plan under which you will configure and run the migration.
2. **Connect to the Source and Target Email Service** — Specify server locations and the administrator account credentials for both your source and target email services.
3. **Add Mailboxes** — Identify the mailboxes you want to migrate, either by entering each mailbox manually or by uploading a list.
4. **Select Mailbox Items and Migration Filters** — Specify which mailbox items you want to migrate and (optionally) any filter parameters.
5. **Migrate** — Initiate your migration and monitor it in the cloud.

Post Migration

After you run a migration, there remain additional activities you may perform.

1. **Review Migration Reports** — Review and correct any errors identified in the migration reports and re-migrate as needed.
2. **Notify and Train Users** — Notify users of the migration and provide information on how to access the new mail system. This step may include training users on the new system as needed.

Preparing Migrations

Choosing a Migration Type

To ensure your migration runs as smoothly as possible, you should first decide which type of migration most suits your needs. You can perform either a one-time, “big bang” migration (cutover) OR several staged groups (co-existence). You may choose a cutover approach if you have a small number of users and you want to move everyone all at once to reduce the amount of administrative overhead. This is also a good option if your users are experienced and won't require a lot of training on the new target domain client. Inform users that they may not have all their old email right away.

The co-existence approach is a good option if you need to train your users on the new mail system. This minimizes the number of users calling the helpdesk. It also allows you to schedule training sessions and migrations together, managing expectations for both your IT staff and your end-users.

Setting Up Mail Routing

Before migrating or creating mailboxes, you need to implement a mail routing strategy that will enable users to send and receive mail from both internal and external sources. There are different strategies to do this depending on how you want mail directed to and from the internet.

Deciding How to Configure Your Shared Address Space

During the co-existence period of on-premises mail and hosted mail, you need to decide which system will initially receive the email traffic for your organization. To make the best decision for your organization, please review the Microsoft documentation associated with your target email service:

- For Exchange 2010, see [https://technet.microsoft.com/en-us/library/bb676395\(v=exchg.141\).aspx](https://technet.microsoft.com/en-us/library/bb676395(v=exchg.141).aspx).
- For Exchange 2013, see [https://technet.microsoft.com/en-us/library/aa998825\(v=exchg.150\).aspx](https://technet.microsoft.com/en-us/library/aa998825(v=exchg.150).aspx).
- For Exchange 2016 or 2019, see [https://technet.microsoft.com/en-us/library/aa998825\(v=exchg.160\).aspx](https://technet.microsoft.com/en-us/library/aa998825(v=exchg.160).aspx).
- For Microsoft 365, see <http://social.technet.microsoft.com/wiki/contents/articles/30202.shared-address-space-office365-mail-routing.aspx>.

Source Email Service

Refer to the sections below for mail routing instructions specific to your source email service.

- [Exchange 2007/2010/2013/2016/2019](#)
- [G Suite](#)
- [Microsoft 365 \(Cloud Relay\)](#)

- Zimbra
- Sun ONE/iPlanet

i | IMPORTANT: Mail routing is not supported by POP/Hotmail and IMAP source email services.

Exchange 2007/2010/2013/2016/2019

i | NOTE: To enable the CPUU integration feature on the source Exchange Server 2007, you should turn on and configure the WebDAV API access for your Exchange Server 2007. For more details, please see [Updating Outlook Client Profiles](#).

When migrating from on-premises Exchange server to Microsoft 365, you can use the Microsoft directory synchronization solution together with ODME. For more details about how to convert mail-enabled users created by Microsoft directory synchronization tool to mailbox-enabled users, please see the following article <https://msdn.microsoft.com/en-us/library/azure/hh967617.aspx>.

Your DNS MX records will already be set to deliver mail to your Exchange server. For Exchange to forward mail, set the targetAddress for the mailboxes that now reside on your new mail system to a subdomain that exists, and configure Exchange to route to target mail system. You can do this by using the Exchange PowerShell Set-Mailbox cmdlet. In the Exchange Management Shell, use the following command:

```
Set-Mailbox -Identity SourceMailbox -TargetSmtpAddress
TargetUsername@ForwardingSubDomain
```

Where:

- SourceMailbox is the user's SMTP address in the source system.
- TargetUsername is the user's Target userid.
- ForwardingSubDomain is a secondary domain that you have set up in the Target domain.

For the forwarded mail to get sent to your target system, create a new send connector to handle the forwarding domain. By using a send connector you do not need to expose this forwarding domain in your DNS. You can create a send connector in the Exchange Management Console, or you can use PowerShell in the Exchange Management Shell. To create the send connector with PowerShell, use the New-SendConnector cmdlet. The following is a simple usage of the send connector, your target system may require TLS or authentication to forward mail. You can change the Name parameter to something that better describes your connector.

```
New-SendConnector -Name ForwardToTarget -AddressSpaces ForwardingSubDomain -
DNSRoutingEnabled $false
```

G Suite

To forward mail from G Suite to Microsoft 365, you must register your domain with both providers. You must register the domain you are using to forward mail from G Suite due to a restriction of the Google APIs used by ODME. The Google APIs will only allow forwarding addresses for registered domains or subdomains of the primary G Suite account. Adding a domain for mail destined for Microsoft 365 may seem counter to normal migration practices, but is a required step. Please note that registering a domain with G Suite does not impact mail routing for the domain.

After registering your domain, the procedure for setting up mail routing for G Suite is the same if Microsoft 365 is the target email service, but slightly different if the target is Exchange 2010.

For information about setting up mail forwarding and available forwarding actions, see [Setting Up Mail Forwarding](#).

Registering your Domain with Google Domains and Microsoft 365

To set forwarding from G Suite to Microsoft 365, you need a domain that is registered with Google Domains and with Microsoft 365. The Google APIs used by ODME require that the domain is registered with Google Domains. To receive mail for the forwarded messages from G Suite, you need email addresses with this domain for your Microsoft 365 Exchange accounts. The following procedures walk you through registering your forwarding domain with Google Domains and registering your domain with Microsoft 365.

To register your domain with Google Domains:

1. Log in to your Google Admin console (<https://www.google.com/a/example.com/>) and go to **Domains > Add/remove domains** page.
2. Click **Add a domain or a domain alias**.
3. Select the **Add another domain** option and enter the domain name.
4. Click **CONTINUE AND VERIFY DOMAIN OWNERSHIP**.

You are prompted to sign in to your domain name provider to verify your ownership of the domain. A helper app may be available, but we recommend completing the process manually by adding a TXT record.

5. Click **Add a TXT record**.
6. Complete the steps for creating a DNS record that proves to Google that you own the domain.
7. Return to the Google domain registration page and click **Verify**.

If you have entered all the information correctly you should receive a conformation message. The next step is to activate your domain.

8. Click **Continue** and go to the **Domains > Add/remove domains** page again.

You should see your domain listed with an exclamation mark,

9. Click **Skip Google MX setup** since you don't want mail to route to G Suite for this domain.
10. In the **Route mail to another server** box, click **I use another mail server**.

Next you need to register the domain with Microsoft 365.

To register your domain with Microsoft 365:

1. Go to <https://portal.microsoftonline.com/> and login as an administrator to your Microsoft 365 portal.
2. Select **Admin > Office365** and then select *Domains* on the left hand navigation tree.
3. Select **Add a domain** and add the same domain to Microsoft 365 that you added to G Suite.

This opens a wizard which prompts you to add another TXT record to verify ownership.

4. After proving the domain name in the wizard, complete the remaining steps for verifying your ownership of the domain by creating another TXT record.

When finished, you should have two TXT records in my DNS, one for G Suite and one for Microsoft 365.

5. Return to the Microsoft 365 portal and click **Done, verify now**.

If you have entered all the information correctly you should receive a conformation message.

6. Click **Finish**.

The next step offered is **Add users and assign licenses**.

7. Click **Start step 2**.
8. Since this is a subdomain for mail routing, select **I don't want to add users right now**.
9. Click **Next**.
10. Click **Start step 3**.

This opens the "how do you want to use..." page.

11. Check the **Exchange Online** option since you just want to setup this domain for Exchange Online, and then click **Next**.

This opens the "add these dns records" page.

12. Follow the instructions for adding the TXT record.
13. Add the CNAME for autodiscover.
14. Click **Done, go check**.

If you have entered all the information correctly you should receive a conformation message.

i NOTE: To add a subdomain to a domain that's set up for federated authentication, do the following:

1. Connect to Windows Azure Active Directory (Windows Azure AD) by using Windows PowerShell. Connect from ADFS Core Server.
2. Use the Connect-MSOLService cmdlet to connect to cloud with Global Administrator credential.
3. Use the New-MSOLFederatedDomain cmdlet.
4. The syntax to add a subdomain is as follows, where <subdomain> is the name of the subdomain that you want to add:

```
New-MSOLFederatedDomain -DomainName:<subdomain>"
```

Mail Routing between G Suite and Microsoft 365

To set up mail routing between G Suite and Microsoft 365, you must configure per-mailbox forwarding in conjunction with subdomain forwarding. This prevents email duplication and subdomains appearing in the Reply Address on any message, either internal or external.

To set up mail routing between G Suite and Microsoft 365:

1. Configure both G Suite and Microsoft 365 to accept mail from the same domain, for example, "example.com." For how to set up MX records for G Suite and Microsoft 365, refer to <https://support.google.com/a/answer/140034?hl=en> and [https://technet.microsoft.com/en-us/library/mt595791\(v=exchg.150\).aspx](https://technet.microsoft.com/en-us/library/mt595791(v=exchg.150).aspx).

In addition, MX records point to G Suite. Though MX can direct email at either system, it is best to have mail delivered to the server with the largest number of users. This means that at the start of the migration, MX points to G Suite, and at the halfway point of the migration, the MX records switch to point to Microsoft 365. Note that the system receiving the mail must know about all users in both systems.

```

> set type=mx
> example.com
Server: harneypeak.wingra.com
Address: 10.4.160.64

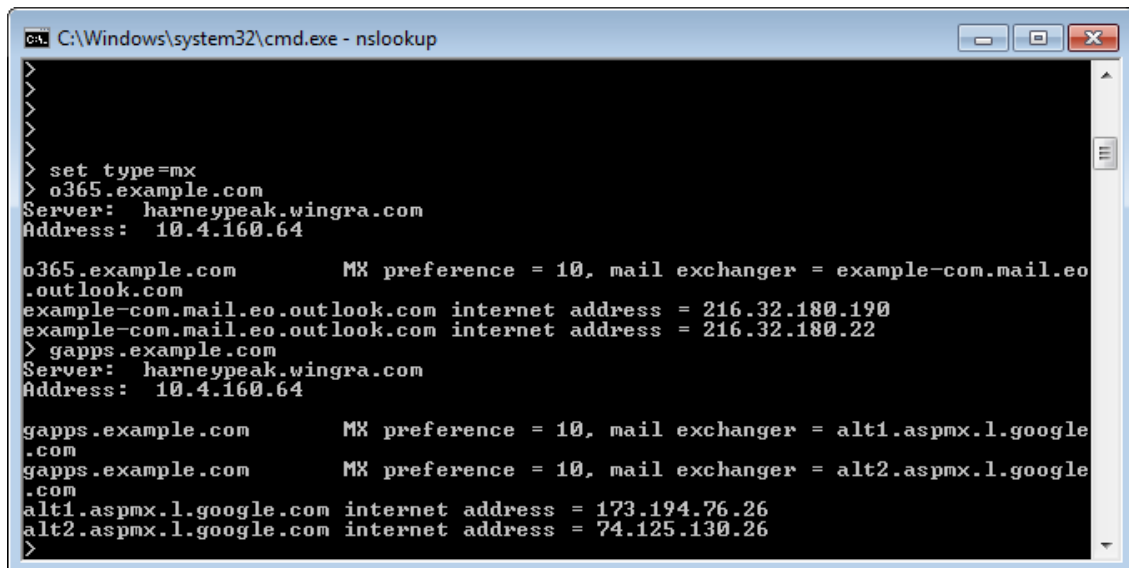
example.com      MX preference = 0, mail exchanger = aspmx.l.google.com
example.com      MX preference = 0, mail exchanger = alt1.aspmx.l.google.com
example.com      MX preference = 0, mail exchanger = alt2.aspmx.l.google.com
example.com      MX preference = 0, mail exchanger = aspmx2.googlemail.com
example.com      MX preference = 0, mail exchanger = aspmx3.googlemail.com

```

The first step is to create two subdomains used for routing.

2. Create an MX record for each domain, which allows each system to send mail to the other.

For example, the domain "O365.example.com" directs mail to Microsoft 365, while the domain "gapps.example.com" directs mail to G Suite.



```

C:\Windows\system32\cmd.exe - nslookup
>
>
>
> set type=mx
> o365.example.com
Server: harneypeak.wingra.com
Address: 10.4.160.64

o365.example.com      MX preference = 10, mail exchanger = example-com.mail.eo
                        .outlook.com
example-com.mail.eo.outlook.com internet address = 216.32.180.190
example-com.mail.eo.outlook.com internet address = 216.32.180.22
> gapps.example.com
Server: harneypeak.wingra.com
Address: 10.4.160.64

gapps.example.com      MX preference = 10, mail exchanger = alt1.aspmx.l.google
                        .com
gapps.example.com      MX preference = 10, mail exchanger = alt2.aspmx.l.google
                        .com
alt1.aspmx.l.google.com internet address = 173.194.76.26
alt2.aspmx.l.google.com internet address = 74.125.130.26
>

```

3. After you create the MX records, set up each system to accept mail for the new subdomains.

In Microsoft 365, you add this domain as a new Accepted Domain. In G Suite, you add this as a new Domain Alias.

By default, all users on G Suite will have aliases for this subdomain. However, with Microsoft 365, you must configure each user with the routing domain, either manually or via a powershell script.

4. Create representative mailboxes in Microsoft 365 for each user that is presently in G Suite.

This allows users who are migrated to Microsoft 365 to see a GAL that is populated with all the users, as well as facilitate message forwarding for users still homed in G Suite.

5. After all the users have mailboxes in Microsoft 365, set forwarding on them that will remain until the user is migrated.

The setting of forwarding can be done with the ODME per-user mail forwarding feature, as described in the section [Setting Up Mail Forwarding](#).

6. When migrating users, flip forwarding so that new mail is delivered to the Microsoft 365 mailbox, and not the G Suite mailbox.

With the ODME per-user mail forwarding option, you now need to select to remove forwarding from the target as well as setting forwarding in the source. It is important to remove the target forwarding to prevent the creation of a mail loop.

Mail Routing between G Suite and Exchange 2010

To set up mail routing between G Suite and Exchange 2010, you must configure per-mailbox forwarding in conjunction with subdomain forwarding. This prevents email duplication and subdomains appearing in the Reply Address on any message, either internal or external.

To set up mail routing between G Suite and Exchange 2010:

1. Configure both G Suite and Exchange 2010 to accept mail from the same domain, for example, "example.com."

In addition, MX records point to G Suite. Though MX can direct email at either system, it is best to have mail delivered to the server with the largest number of users. This means that at the start of the migration, MX points to G Suite, and at the halfway point of the migration, the MX records switch to point to Exchange 2010. Note that the system receiving the mail must know about all users in both systems.

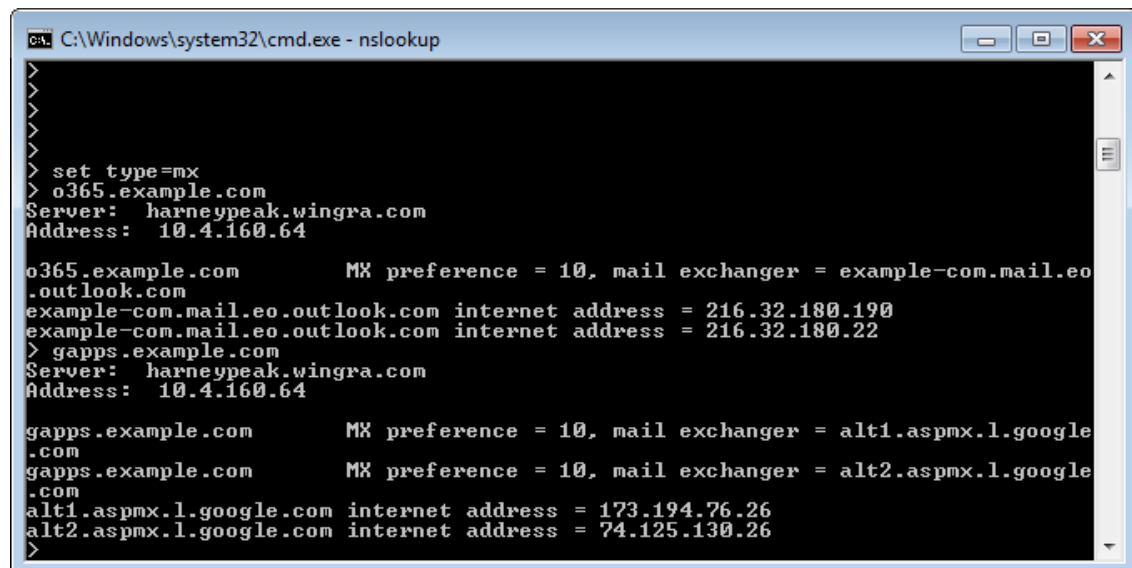
```
> set type=mx
> example.com
Server: harneypeak.wingra.com
Address: 10.4.160.64

example.com      MX preference = 0, mail exchanger = aspmx.l.google.com
example.com      MX preference = 0, mail exchanger = alt1.aspmx.l.google.com
example.com      MX preference = 0, mail exchanger = alt2.aspmx.l.google.com
example.com      MX preference = 0, mail exchanger = aspmx2.googlemail.com
example.com      MX preference = 0, mail exchanger = aspmx3.googlemail.com
```

The first step is to create two subdomains used for routing.

2. Create an MX record for each domain, which allows each system to send mail to the other.

For example, the domain "ex2010.example.com" directs mail to Exchange 2010, while the domain "gapps.example.com" directs mail to G Suite.



```
C:\Windows\system32\cmd.exe - nslookup

>
>
>
> set type=mx
> o365.example.com
Server: harneypeak.wingra.com
Address: 10.4.160.64

o365.example.com      MX preference = 10, mail exchanger = example-com.mail.eo
.outlook.com
example-com.mail.eo.outlook.com internet address = 216.32.180.190
example-com.mail.eo.outlook.com internet address = 216.32.180.22
> gapps.example.com
Server: harneypeak.wingra.com
Address: 10.4.160.64

gapps.example.com      MX preference = 10, mail exchanger = alt1.aspmx.l.google
.com
gapps.example.com      MX preference = 10, mail exchanger = alt2.aspmx.l.google
.com
alt1.aspmx.l.google.com internet address = 173.194.76.26
alt2.aspmx.l.google.com internet address = 74.125.130.26
>
```

3. After you create the MX records, set up each system to accept mail for the new subdomains.

In Exchange 2010, you add this domain as a new Accepted Domain. In G Suite, you add this as a new Domain Alias.

By default, all users on G Suite will have aliases for this subdomain. However, with Exchange 2010, you must go to the Exchange Management Console and configure the recipient policy to include this domain for all the users.

4. Create representative mailboxes in Exchange 2010 for each user that is presently in G Suite.

This allows users who are migrated to Exchange 2010 to see a GAL that is populated with all the users, as well as facilitate message forwarding for users still homed in G Suite.

5. After all the users have mailboxes in Exchange 2010, set forwarding on them that will remain until the user is migrated.

The setting of forwarding can be done with the ODME per-user mail forwarding feature, as described in the section [Setting Up Mail Forwarding](#).

At this point, mail routing is configured and operational between Exchange 2010 and G Suite.

6. When migrating users, flip forwarding so that new mail is delivered to the Exchange 2010 mailbox, and not the G Suite mailbox.

With the ODME per-user mail forwarding option, you now need to select to remove forwarding from the target as well as setting forwarding in the source. It is important to remove the target forwarding to prevent the creation of a mail loop.

Microsoft 365 (Cloud Relay)

CAUTION: The scenario described in this topic isn't supported in Microsoft 365 Beta for enterprises.

According to the current Microsoft documentation:

Update your MX record so that all mail destined for your domain will be routed to your new mail server. The instructions from Microsoft found [here](#) (login required) talk about how to route mail to the cloud. You will need to just update the MX records to redirect SMTP traffic to your Edge transport server. You can learn more about the edge transport server on <https://technet.microsoft.com/en-us/library/bb124701.aspx>

The Microsoft 365 mail routing page also provides instructions for different DNS providers.

Since you have decided to route all mail to your new domain first, you also need to make sure your Primary domain is a "Shared Domain." This will let any email addressed to mailboxes deleted from your Microsoft 365 server to be routed to your new mail server.

To forward any new mail to your new mail system that is routed to Microsoft 365, use the ODME per-user mail forwarding feature as described in the section [Setting Up Mail Forwarding](#). To use the mail forwarding feature, the administrator account must be assigned the "Recipient Management" role, for example:

```
Add-RoleGroupMember "Recipient Manager" -Member migadmin@example.com
```

NOTE: When you configure mail forwarding for Microsoft 365 in ODME, the settings will be accessible in the O365 user account page, but not in the Exchange Admin Center.

Zimbra

Mail Routing between Zimbra and Microsoft 365

To set up mail routing between Zimbra and Microsoft 365, you must configure per-mailbox forwarding in conjunction with subdomain forwarding. This prevents email duplication and subdomains appearing in the Reply Address on any message, either internal or external.

To set up mail routing between Zimbra and Microsoft 365:

1. Configure both Zimbra and Microsoft 365 to accept mail from the same domain, for example, "example.com".

In addition, MX records point to Zimbra. Though MX can direct email at either system, it is best to have mail delivered to the server with the largest number of users. This means that at the start of the migration, MX points to Zimbra, and at the halfway point of the migration, the MX records switch to point to Microsoft 365. Note that the system receiving the mail must know about all users in both systems.

The first step is to create two subdomains used for routing.

2. Create an MX record for each domain, which allows each system to send mail to the other.

For example, the domain "O365.example.com" directs mail to Microsoft 365, while the domain "zimbra.example.com" directs mail to Zimbra.

3. After you create the MX records, set up each system to accept mail for the new subdomains.

For Microsoft 365, you add this domain as a new Accepted Domain. In Zimbra, you add this as a new Domain.

For Zimbra, you must create aliases for this new subdomain under the Aliases section of Manage Accounts. For Microsoft 365, you must configure each user with the routing domain, either manually or via a powershell script.

4. Create representative mailboxes in Microsoft 365 for each user that is presently in Zimbra.

This allows users who are migrated to Microsoft 365 to see a GAL that is populated with all the users, as well as facilitate message forwarding for users still homed in Zimbra.

5. After all the users have mailboxes in Microsoft 365, set forwarding on them that will remain until the user is migrated.

The setting of forwarding can be done with the ODME per-user mail forwarding feature, as described in the section [Setting Up Mail Forwarding](#).

6. When migrating users, flip forwarding so that new mail is delivered to the Microsoft 365 mailbox, and not the Zimbra mailbox.

With the ODME per-user mail forwarding option, you now need to select to remove forwarding from the target as well as setting forwarding in the source. It is important to remove the target forwarding to prevent the creation of a mail loop

Mail Routing between Zimbra and Exchange 2010

To set up mail routing between Zimbra and Exchange 2010, you must configure per-mailbox forwarding in conjunction with subdomain forwarding. This prevents email duplication and subdomains appearing in the Reply Address on any message, either internal or external.

To set up mail routing between Zimbra and Exchange 2010:

1. Configure both Zimbra and Exchange 2010 to accept mail from the same domain, for example, *“example.com”*.

In addition, MX records point to Zimbra. Though MX can direct email at either system, it is best to have mail delivered to the server with the largest number of users. This means that at the start of the migration, MX points to Zimbra, and at the halfway point of the migration, the MX records switch to point to Exchange 2010. Note that the system receiving the mail must know about all users in both systems.

The first step is to create two subdomains used for routing.

2. Create an MX record for each domain, which allows each system to send mail to the other.

For example, the domain *“ex2010.example.com”* directs mail to Exchange 2010, while the domain *“zimbra.example.com”* directs mail to Zimbra.

3. After you create the MX records, set up each system to accept mail for the new subdomains.

For Exchange 2010, you add this domain as a new Accepted Domain. In Zimbra, you add this as a new Domain Alias.

For Zimbra, you must create aliases for this new subdomain under the Aliases section of Manage Accounts.

For Microsoft 365, you must configure each user with the routing domain, either manually or via a powershell script.

4. Create representative mailboxes in Exchange 2010 for each user that is presently in Zimbra.

This allows users who are migrated to Exchange 2010 to see a GAL that is populated with all the users, as well as facilitate message forwarding for users still homed in Zimbra.

5. After all the users have mailboxes in Exchange 2010, set forwarding on them that will remain until the user is migrated.

The setting of forwarding can be done with the ODME per-user mail forwarding feature, as described in the section [Setting Up Mail Forwarding](#).

At this point, mail routing is configured and operational between Exchange 2010 and Zimbra.

6. When migrating users, flip forwarding so that new mail is delivered to the Exchange 2010 mailbox, and not the Zimbra mailbox.

With the ODME per-user mail forwarding option, you now need to remove forwarding from the target as well as setting forwarding in the source. It is important to remove the target forwarding to prevent the creation of a mail loop.

Sun ONE/iPlanet

Refer to the documentation provided by Sun ONE/iPlanet for information on setting up mail routing.

Initial Target Mail Hosts

Refer to the sections below for mail routing instructions specific to your target email service.

- [Microsoft 365](#)
- [Exchange 2010/2013/2016/2019](#)

Microsoft 365

Required Permissions

NOTE: If you use end-user credentials for migration, you do not need to create an administrator account.

If you do not use the **Use Modern Authentication** option, your administrator account must have an Enterprise Microsoft 365 license and must be assigned to a Role-Based Access Control group that has Application Impersonation rights. By default, the ApplicationImpersonation role is not assigned to this group, which means the first step is to sign in as an organization administrator to the Microsoft 365 portal (<http://portal.microsoftonline.com>) and add this role to either an existing role group or to a new role group that you create. See Exchange Online documentation for more information on creating role groups and assigning rights.

It is recommended that you create a new role group named "Migration Impersonation" and assign the ApplicationImpersonation role to it.

Role groups are created in the **Role Groups** page of the Microsoft 365 portal. After logging in, go to the **Options** menu, select **See All Options....** Then from the Options: **Manage Myself** menu, select **My Organization**. Lastly, select the **Roles & Auditing** item and click **New**.

You can use Modern Authentication to connect to Microsoft 365. The **Use Modern Authentication** option lets you grant consent to ODME instead of providing Administrative credentials with Application Impersonation rights. When the **Use Modern Authentication** option is enabled, the **Forwarding** section in a plan's **Options** page contains additional fields where you need to specify the credentials of the account which has the permissions to modify forwarding settings. The **Use Modern Authentication** option is enabled for any newly created plan by default.

NOTE: The **Use Modern Authentication** option is supported for connections to the Microsoft 365 Worldwide. The option is not supported for connections to the Microsoft 365 hosted in the Germany, China or US Government environments (Microsoft 365 GCC High).

When connecting to your Microsoft 365 server in the **Migration Settings** screen, it is recommended you select the auto-discovery option, which uses your login credentials to automatically obtain the server name during a migration. You can also enter the name of your Microsoft 365 server manually as it appears in the address bar when you log in as an administrator to your account.

NOTE: If using the auto-discovery option, you need to have the proper DNS settings in place. See [Exchange Online](#) documentation for more information.

To perform mail forwarding, the administrator account must be assigned the "Recipient Management" role. See the section [Setting Up Mail Routing](#) for more information.

Upgrade Throttling Policies

In order to minimize Microsoft 365 throttling impact to migration and to raise the overall migration throughput, we highly recommend to upgrade your Microsoft 365 tenant throttling policies. Please contact Microsoft support with the request to raise the limits for the following throttling parameters to 'Unlimited':

- EwsMaxBurst
- EwsRechargeRate
- EwsCutoffBalance

The upgrade can be done for the time of your migration only.

Exchange 2010/2013/2016/2019

For a local Exchange 2010/2013/2016/2019 On-Premises Relay system, please review the information on <https://technet.microsoft.com/en-us/library/aa998825.aspx>.

Creating Target Mailboxes

The next task in migrating mailboxes from a source email service is to create the target mailboxes they will be migrated to in the target email service. On Demand Migration for Email does not create them for you. The procedure for creating mailboxes varies between email systems, and you should refer to the documentation provided with your system for particular instructions.

Preparing Your Source Email Service for Migration

Quest On Demand Migration for Email currently supports migrating content from the following email services:

- [G Suite](#)
- [Sun ONE/iPlanet](#)
- [Microsoft Exchange 2007/2010/2013/2016/2019](#)
- [Microsoft 365](#)
- [POP/Windows Live Hotmail](#)
- [IMAP](#)
- [Zimbra](#)

G Suite

i **NOTE:** Make sure that there is no limit on the number of messages in an IMAP folder. For that, in **Google Settings**, click the **Forwarding and POP/IMAP** tab and check that the **Do not limit the number of messages in an IMAP folder (default)** option is selected. Otherwise, not all mail items will be migrated.

Connecting to a G Suite source email service from ODME is a two-stage process based on the OAuth 2 protocol. First, users sign in to G Suite directly from ODME with an super administrator account. Once this account has been verified, users then configure API settings in the Google Admin Console to grant ODME web client application access.

For detailed instructions, see [G Suite](#).

Sun ONE/iPlanet

Quest On Demand Migration for Email uses IMAP to migrate messages and folders from your Sun ONE/iPlanet server to an Microsoft 365 server. The migration engine connects to your on-premises or hosted Sun ONE/iPlanet server as the user you provide that can impersonate all the users in your organization using proxy authentication. To do this, the administrator account needs to be a member of the Domain Administrators group.

Sun ONE/iPlanet uses an LDAP directory to hold the user information for the messaging server. Typically, the users for your domain are located in an organizational unit (OU) labeled People and Groups which should be a peer to the People OU. The Domain Administrators group should exist in the Groups OU. Verify that the user that you want to use is listed in the **uniqueMember** attribute. The value in this attribute will be the distinguished name of the user.

Only email is migrated by On Demand Migration for Email from the Sun ONE/iPlanet Messaging Server. Folder structures are maintained including empty folders. Read and Unread flags for messages are maintained for the migration of each user. Because of throttling of Microsoft 365, only 27 mailboxes can be migrated at a time per each administrative account configured for the Microsoft 365 servers.



NOTE: The Sun ONE mail server has undergone several brand name changes. It may also be known as the following:

- iPlanet Messaging Server
- Sun ONE Messaging Server
- Sun Java System Messaging Server
- Oracle Communications Messaging Exchange Server

Microsoft Exchange 2007/2010/2013/2016/2019



NOTE: To enable the CPUU integration feature on the source Exchange Server 2007, you should turn on and configure the WebDAV API access for your Exchange Server 2007. For more details, please see [Updating Outlook Client Profiles](#).

Enabling Application Impersonation Rights

To migrate data from Exchange 2007/2010/2013/2016/2019 you need to enable Application Impersonation for the migration administrator account. This allows the migration administrator to impersonate all users on all your client access servers.

There are two separate procedures for enabling Application Impersonation rights. For Exchange 2007, do the following:

1. Open the Exchange Management Console.
2. Run the Add-ADPermission cmdlet to add the impersonation permissions on the server for the identified user.

The following example shows you how to set the impersonation permissions on all Client Access servers in an Exchange organization.

```
Get-ExchangeServer | where {$_.IsClientAccessServer -eq $TRUE} | ForEach-Object {Add-ADPermission -Identity $_.distinguishedname -User (Get-User -Identity User1 | select-object).identity -extendedRight ms-Exch-EPI-Impersonation}
```



NOTE: For more information, refer to the instructions provided by Microsoft on [https://msdn.microsoft.com/en-us/library/bb204095\(v=exchg.80\).aspx](https://msdn.microsoft.com/en-us/library/bb204095(v=exchg.80).aspx).

For Exchange 2010/2013/2016/2019, you will use role based access controls, and create a role group that has Application Impersonation rights.

The instructions for Exchange 2010 can be found on [https://msdn.microsoft.com/en-us/library/bb204095\(v=exchg.140\).aspx](https://msdn.microsoft.com/en-us/library/bb204095(v=exchg.140).aspx). For more details about how to configure impersonation in versions of Exchange starting from Exchange 2013, see [https://msdn.microsoft.com/en-us/library/office/dn722376\(v=exchg.150\).aspx](https://msdn.microsoft.com/en-us/library/office/dn722376(v=exchg.150).aspx).

To create a role group for impersonation, use the PowerShell cmdlets from the articles above. The following is a step by step guide for creating the impersonation role and assigning a user to that role.

1. Logon to your Exchange server, or to a machine that has the Exchange Administration tools installed on it as an Exchange administrator.
2. Run Exchange Management Shell.
3. Run the cmdlet to create the management role group and assign the **ApplicationImpersonation** role to that group, and then assign the user you want to use as a migration administrator.

In the following example, we are using the user *migAdmin@example.com*.

```
New-RoleGroup -Name MigrationImpersonation -Roles ApplicationImpersonation -Members migAdmin@example.com
```

You can add multiple users using commas to separate each user.

Accessing the Mail Server

To migrate data from Exchange 2007/2010/2013/2016/2019, make sure that Outlook Web Access (OWA) is accessible from the internet. Quest On Demand Migration for Email uses Exchange Web Services (EWS) to access your mail server from the internet. The OWA server name can be used for accessing your Exchange server with EWS. If you are not using HTTPS for OWA, you will need to enter the full URL for your EWS service which follows the format `http://servername/EWS/Exchange.asmx`.

You can find the URL for your EWS server using PowerShell. From the Exchange Management Shell, execute the following command:

```
Get-WebServicesVirtualDirectory | Select name, *url* | fl
```

The EWS server URL will be returned in the `ExternalUrl` value. To access the mailboxes slated for migration, the migrator needs to have an account with the ApplicationImpersonation role.

Specifying Administrator Credentials

When specifying the administrator credentials in the Migration settings screen, the Admin value is the account's UPN or Windows domain login (`domain\samAccountName`). Click [https://technet.microsoft.com/en-us/library/cc756018\(WS.10\).aspx](https://technet.microsoft.com/en-us/library/cc756018(WS.10).aspx) for more information about adding additional domains for UPNs.

It is recommended that you use auto-discovery to obtain the server URL. During a migration, this option uses the specified UPN and password to retrieve the server URL that hosts EWS for the given mailbox. You can also enter the server URL manually.

i **NOTE:** Your Exchange 2007/2010/2013/2016/2019 server must be configured to support auto-discovery before you can use it to obtain the server URL. Click [https://technet.microsoft.com/en-us/library/bb201695\(EXCHG.80\).aspx](https://technet.microsoft.com/en-us/library/bb201695(EXCHG.80).aspx) for more information on the autodiscover service in Exchange 2007. Click <https://technet.microsoft.com/en-us/library/bb201695.aspx> for information on Exchange 2010 or [https://technet.microsoft.com/en-us/library/bb124251\(v=exchg.150\).aspx](https://technet.microsoft.com/en-us/library/bb124251(v=exchg.150).aspx) for information on Exchange 2013, 2016, and 2019.

If entering the server URL manually, enter the name of your Exchange 2007/2010/2013/2016/2019 server in SSL format (e.g., *exchange.example.com*). If your server does not support SSL, enter the fully qualified URL for Exchange Web Services (e.g., <http://exchange.example.com/EWS/Exchange.asmx>).

i **NOTE:** If your server does not support SSL, all mailbox data will be transmitted non-encrypted. Use SSL connections if possible to secure your data. ODME supports self-signed SSL certificates. For information on generating a properly formatted self-signed SSL certificate, see [Using Self-Signed SSL Certificates](#).

Upgrade Throttling Policies (Microsoft Exchange 2010/2013/2016/2019)

In order to minimize Exchange throttling impact to migration and to raise the overall migration throughput, we highly recommend to upgrade your throttling policies. Please raise the limits for the following throttling parameters to 'Unlimited':

Microsoft Exchange 2013/2016/2019

- EwsMaxConcurrency
- EwsMaxBurst
- EwsRechargeRate
- EwsCutoffBalance

Microsoft Exchange 2010

- EWSPercentTimeInMailboxRPC
- EWSPercentTimeInCAS
- EWSPercentTimeInAD

We recommend to create a custom throttling policy and assign it to all the admin accounts used for your migration. The upgrade can be done for the time of your migration only.

Microsoft 365

Required Permissions

i **NOTE:** If you use end-user credentials for migration, you do not need to create an administrator account.

If you do not use the **Use Modern Authentication** option, your administrator account must have an Enterprise Microsoft 365 license and must be assigned to a Role-Based Access Control group that has Application Impersonation rights. By default, the ApplicationImpersonation role is not assigned to this group, which means the first step is to sign in as an organization administrator to the Microsoft 365 portal (<http://portal.microsoftonline.com>)

and add this role to either an existing role group or to a new role group that you create. See Exchange Online documentation for more information on creating role groups and assigning rights.

It is recommended that you create a new role group named "Migration Impersonation" and assign the ApplicationImpersonation role to it.

Role groups are created in the **Role Groups** page of the Microsoft 365 portal. After logging in, go to the **Options** menu, select **See All Options**.... Then from the Options: **Manage Myself** menu, select **My Organization**. Lastly, select the **Roles & Auditing** item and click **New**.

You can use Modern Authentication to connect to Microsoft 365. The **Use Modern Authentication** option lets you grant consent to ODME instead of providing Administrative credentials with Application Impersonation rights. When the **Use Modern Authentication** option is enabled, the **Forwarding** section in a plan's **Options** page contains additional fields where you need to specify the credentials of the account which has the permissions to modify forwarding settings. The **Use Modern Authentication** option is enabled for any newly created plan by default.

i **NOTE:** The **Use Modern Authentication** option is supported for connections to the Microsoft 365 Worldwide. The option is not supported for connections to the Microsoft 365 hosted in the Germany, China or US Government environments (Microsoft 365 GCC High).

When connecting to your Microsoft 365 server in the **Migration Settings** screen, it is recommended you select the auto-discovery option, which uses your login credentials to automatically obtain the server name during a migration. You can also enter the name of your Microsoft 365 server manually as it appears in the address bar when you log in as an administrator to your account.

i **NOTE:** If using the auto-discovery option, you need to have the proper DNS settings in place. See [Exchange Online](#) documentation for more information.

To perform mail forwarding, the administrator account must be assigned the "Recipient Management" role. See the section [Setting Up Mail Routing](#) for more information.

Upgrade Throttling Policies

In order to minimize Microsoft 365 throttling impact to migration and to raise the overall migration throughput, we highly recommend to upgrade your Microsoft 365 tenant throttling policies. Please contact Microsoft support with the request to raise the limits for the following throttling parameters to 'Unlimited':

- EwsMaxBurst
- EwsRechargeRate
- EwsCutoffBalance

The upgrade can be done for the time of your migration only.

POP/Windows Live Hotmail

Ensure that the keep mail on the server option is set. On Windows Live Hotmail, go to Managing your account settings, **select POP and deleting downloaded messages** and then select the option **Don't let another program delete messages from Hotmail**. (If your other program is set to **delete messages from the server**, messages are moved to a special POP folder. They are not deleted.

IMAP

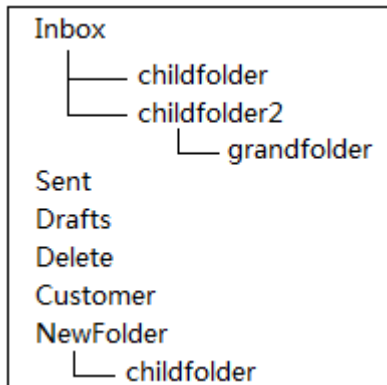
Ensure IMAP support is enabled in mail server.

Dovecot Mail Server

To exclude a specific folder from migration, you should specify the full path to this folder (mail location).

By default Dovecot uses the Maildir++ directory layout. This means that all mailboxes are stored in a single directory and prefixed with a dot.

Example:



The full path to **grandfolder** is "Inbox.childfolder2.grandfolder"

If the file system (fs) layout is enabled in the server, the full path to **grandfolder** looks like "Inbox/childfolder2/grandfolder".

To enable the file system layout, use the following string: `mail_location = maildir:~/Maildir:LAYOUT=fs`

For more details about the mail location, please see <http://wiki2.dovecot.org/MailLocation/Maildir>.

Zimbra

For Zimbra 7, 8 source systems, make sure that the following configuration settings are enabled at the server level as well as for each user account:

Major Features

- Mail
- Address Book
- Calendar
- Tasks

Mail Features

- IMAP Access
- External IMAP Access

ODME uses a combination of IMAP and Zimbra's SOAP API to migrate data. Generally, IMAP is enabled for every user by default, but if not it must be enabled. The default IMAP ports are same as any IMAP-based server (143 and 993 using SSL). The default ports for Zimbra are port 7071 for the admin connection and port 80 for the normal connection. The admin connection is only used to configure impersonation for the mailbox being migrated. Once the mailbox is successfully impersonated, ODME uses a regular SOAP connection on port 80 for the rest of the SOAP calls. You can change port numbers if needed. You can also enable SSL on each connection.

Preparing Your Target Email Service for Migration

Before you do any migrations, you need to configure your target email service.

On Demand Migration for Email currently supports migrating content to the following target email services:

- [Microsoft 365](#)
- [Microsoft Exchange 2010/2013/2016/2019](#)

Microsoft 365

Required Permissions

i | **NOTE:** If you use end-user credentials for migration, you do not need to create an administrator account.

If you do not use the **Use Modern Authentication** option, your administrator account must have an Enterprise Microsoft 365 license and must be assigned to a Role-Based Access Control group that has Application Impersonation rights. By default, the ApplicationImpersonation role is not assigned to this group, which means the first step is to sign in as an organization administrator to the Microsoft 365 portal (<http://portal.microsoftonline.com>) and add this role to either an existing role group or to a new role group that you create. See Exchange Online documentation for more information on creating role groups and assigning rights.

It is recommended that you create a new role group named "Migration Impersonation" and assign the ApplicationImpersonation role to it.

Role groups are created in the **Role Groups** page of the Microsoft 365 portal. After logging in, go to the Options menu, select **See All Options....** Then from the Options: **Manage Myself** menu, select **My Organization**. Lastly, select the **Roles & Auditing** item and click **New**.

You can use Modern Authentication to connect to Microsoft 365. The **Use Modern Authentication** option lets you grant consent to ODME instead of providing Administrative credentials with Application Impersonation rights. When the **Use Modern Authentication** option is enabled, the **Forwarding** section in a plan's **Options** page contains additional fields where you need to specify the credentials of the account which has the permissions to modify forwarding settings. The **Use Modern Authentication** option is enabled for any newly created plan by default.

i | **NOTE:** The **Use Modern Authentication** option is supported for connections to the Microsoft 365 Worldwide. The option is not supported for connections to the Microsoft 365 hosted in the Germany, China or US Government environments (Microsoft 365 GCC High).

When connecting to your Microsoft 365 server in the **Migration Settings** screen, it is recommended you select the auto-discovery option, which uses your login credentials to automatically obtain the server name during a migration.

You can also enter the name of your Microsoft 365 server manually as it appears in the address bar when you log in as an administrator to your account.

i | **NOTE:** If using the auto-discovery option, you need to have the proper DNS settings in place. See [Exchange Online](#) documentation for more information.

To perform mail forwarding, the administrator account must be assigned the "Recipient Management" role. See the section [Setting Up Mail Routing](#) for more information.

Provisioning

Before creating new user accounts on your Microsoft 365 server, consider how these new accounts should be managed in the future and what implications this will have on mail routing. Mail routing is discussed in the Mail Routing section of the help.

Account that is used to migrate Microsoft 365 F1 users must have Application Impersonation rights. If you have only end-user credentials, Migration of Microsoft 365 F1 users is not supported.

If you are migrating from on-premises Exchange server, you should consider using the directory synchronization tools that will push your local Active Directory users over to the Microsoft 365 server. For more details about how to convert mail-enabled users created by Microsoft directory synchronization tool to mailbox-enabled users, please see the following article <https://msdn.microsoft.com/en-us/library/azure/hh967617.aspx>.

If you are migrating from G Suite, you will need to create users manually using the bulk import in the Administrator control panel or use PowerShell cmdlets, for more help with PowerShell, See [Exchange Online](#) documentation.

Upgrade Throttling Policies

In order to minimize Microsoft 365 throttling impact to migration and to raise the overall migration throughput, we highly recommend to upgrade your Microsoft 365 tenant throttling policies. Please contact Microsoft support with the request to raise the limits for the following throttling parameters to 'Unlimited':

- EwsMaxBurst
- EwsRechargeRate
- EwsCutoffBalance

The upgrade can be done for the time of your migration only.

Disable In-Place Hold and Litigation Hold

In order to prevent the excessive growth of **Recoverable Items** folder which can lead to its size quota exceeding and consequent migration stop, we highly recommend to turn off In-Place Hold and Litigation Hold for every migrated mailbox for the time of migration.

Why do I need to do it?

If a user who is placed on In-Place Hold or Litigation Hold modifies specific properties of a mailbox item, a copy of the original mailbox item is created before the changed item is written. The original copy is saved in the **Recoverable Items** folder. This process is known as "copy-on-write" page protection. The "copy-on-write" page protection applies to items residing in any mailbox folder.

Due to supported mail systems heterogeneity, ODME creates messages in a staged manner to ensure content fidelity. In case of a message with several attachments, the number of stages is not less than a number of attachments. First, the empty message is created, then the attachments are uploaded one by one. For each of this stage or action, the copy of a message is put into the **Recoverable Items** folder. It leads to excessive growth of the

Recoverable Items folder as the automatic purging of this folder is disabled when a mailbox is in the In-Place Hold and Litigation Hold state.

Please refer to Microsoft KB article for details: <https://technet.microsoft.com/en-us/library/ee364755.aspx#hold>.

Microsoft Exchange 2010/2013/2016/2019

Enabling Application Impersonation Rights

To migrate data to Exchange 2010/2013/2016/2019, your administrator accounts must have Application Impersonation rights, which means that the accounts must be assigned to a Role-Based Access Control group that has Application Impersonation rights. Because no groups have Application Impersonation rights by default, you need to add Application Impersonation rights to an existing group or create a new group. You have to do this using the Exchange Management Shell with PowerShell cmdlets. The cmdlets to run can be found at [https://msdn.microsoft.com/en-us/library/bb204095\(v=exchg.140\).aspx](https://msdn.microsoft.com/en-us/library/bb204095(v=exchg.140).aspx).

To create a role group for impersonation, use the PowerShell cmdlets from the article above. To create the Impersonation role and assigning a user to that role, use the following procedure.

1. Logon to your Exchange server, or to a machine that has the Exchange Administration tools installed on it as an Exchange administrator.
2. Run Exchange Management Shell.
3. Run the cmdlet to create the management role group and assign the ApplicationImpersonation role to that group, and then assign the user you want to use as a migration administrator.

In the following example, we are using the user migAdmin@example.com.

```
New-RoleGroup -Name MigrationImpersonation -Roles ApplicationImpersonation -Members migAdmin@example.com
```

You can add multiple users using commas to separate each user.

Accessing the Mail Server

Make sure that Outlook Web Access (OWA) is accessible from the internet. Quest On Demand Migration for Email uses Exchange Web Services (EWS) to access your mail server from the internet. The OWA server name can be used for accessing your Exchange server with EWS. If you are not using HTTPS for OWA, you will need to enter the full URL for your EWS service which follows the format `http://servername/EWS/Exchange.asmx`.

You can find the URL for your EWS server using PowerShell. From the Exchange Management Shell, execute the following command:

```
Get-WebServicesVirtualDirectory | Select name, *url* | fl
```

The EWS server URL will be returned in the ExternalUrl value. To access the mailboxes slated for migration, the migrator needs to have an account with the ApplicationImpersonation role.

Provisioning

Before creating new user accounts on your on-premises Exchange 2010/2013/2016/2019 server, consider how these new accounts should be managed in the future and what implications this will have on mail routing. Mail routing is discussed in the Mail Routing section of the help.

If you are migrating from an on-premises Exchange server, go to the Microsoft TechNet library located on <https://technet.microsoft.com/en-us/library/aa995902.aspx> and follow the upgrade instructions specific your version of Exchange under the "Planning and Deployment" section.

If you are migrating from G Suite, you must create users manually either by using the bulk import in the Exchange Management Console or by using PowerShell cmdlets. For more help with bulk account creation, see the instructions for importing CSV files on <https://technet.microsoft.com/en-us/library/dd347665.aspx>, and how to add mailboxes on <https://technet.microsoft.com/en-us/library/aa997663.aspx>. To see how PowerShell cmdlets work together, go to <https://social.technet.microsoft.com/Forums/exchange/en-US/480078a8-e017-44d1-8ce5-13c87e0a660b/exchange-2010-importcsv-to-create-new-users-and-include-their-passwords?forum=exchange2010>.

Upgrade Throttling Policies

In order to minimize Exchange throttling impact to migration and to raise the overall migration throughput, we highly recommend to upgrade your throttling policies. Please raise the limits for the following throttling parameters to 'Unlimited' or to the highest possible values:

Microsoft Exchange 2013/2016/2019

- EwsMaxConcurrency
- EwsMaxBurst
- EwsRechargeRate
- EwsCutoffBalance

Microsoft Exchange 2010

- EWSPercentTimeInMailboxRPC
- EWSPercentTimeInCAS
- EWSPercentTimeInAD

We recommend to create a custom throttling policy and assign it to all the administrator accounts used for your migration.

The upgrade can be done for the time of your migration only.

Disable In-Place Hold and Litigation Hold

In order to prevent the excessive growth of **Recoverable Items** folder which can lead to its size quota exceeding and consequent migration stop, we highly recommend to turn off In-Place Hold (not applicable to Exchange 2010) and Litigation Hold for every migrated mailbox for the time of migration.

Why do I need to do it?

If a user who is placed on In-Place Hold or Litigation Hold modifies specific properties of a mailbox item, a copy of the original mailbox item is created before the changed item is written. The original copy is saved in the **Recoverable Items** folder. This process is known as "copy-on-write" page protection. The "copy-on-write" page protection applies to items residing in any mailbox folder.

Due to heterogeneity of mail systems, ODME creates messages in a staged manner to ensure content fidelity. In case of a message with several attachments, the number of stages is not less than a number of attachments. First, the empty message is created, then the attachments are uploaded one by one. For each of this stage or action, the copy of a message is put into the **Recoverable Items** folder. It leads to the excessive growth of the **Recoverable Items** folder as the automatic purging of this folder is disabled when a mailbox is in the In-Place Hold and Litigation Hold state.

Please refer to the following Microsoft KB articles:

- For Exchange 2019 or 2016: <https://technet.microsoft.com/en-us/library/ee364755.aspx#hold>
- For Exchange 2013: [https://technet.microsoft.com/en-us/library/ee364755\(v=exchg.150\).aspx#hold](https://technet.microsoft.com/en-us/library/ee364755(v=exchg.150).aspx#hold)
- For Exchange 2010: [https://technet.microsoft.com/en-us/library/ee364755\(v=exchg.141\).aspx](https://technet.microsoft.com/en-us/library/ee364755(v=exchg.141).aspx)

Test and Pilot Migrations

Any full scale migration should be preceded by test and pilot migrations, to confirm that your migration processes and procedures will accommodate the organization requirements.

- A **test migration** uses real users and real data in a segregated test environment, or dummy users and dummy data in your live production environment.
- A **pilot migration** uses a small portion of real users and real data in the live production environment.

In either case - a test or pilot migration - the data to be migrated should be a representative sample of the production data, and the test or pilot migration should be run with the Quest applications set for the same configuration and process options that you intend to use for the production migration. It is recommended to select test or pilot users whose usage and data types make them representative of the total user population. Then run the migration for those users, just as you have defined the process in your migration planning. When the migration is completed, review application log file for errors and warnings, if any. See [Viewing Migration Reports](#) section for more information.

Quest recommends that you use both test and pilot migrations:

1. Perform one or more test migrations in a separate test environment, migrating test copies of real users and their real data. The separate test environment ensures that no test process will affect the data or configurations of your production environment. If a test exposes any problems under migration, you can make amendments and then repeat the test by simply dumping the test environment and recreating it from scratch.
2. When you are confident that your test migrations have sufficiently refined your planned migration, perform a pilot migration for 20 or 30 users to verify if your planned migration is satisfactory for your "real world."

Configuring and Running Migrations

Creating a Migration Plan

A migration plan saves in a reusable format all the configuration details of a migration, including its connection properties, source and target mailboxes, and optional parameters. When you first log in to On Demand Migration for Email, you are prompted to specify a name for your first migration plan.

Instead of creating the migration plan from scratch, you can also create it from a template that specifies the connection properties and optional parameters for the migration. Once a migration plan is created from a template, you only need to add the mailboxes you want to migrate (you can also edit the target connection and the date filter, if necessary).

For a step by step procedure to create a migration plan from scratch or using a template, see [Getting Started for New Users](#). For more information about the migration template, see [Managing Migration Templates](#).

You can copy migration plans and then edit those copies to create other migration plans. This spares you the task of specifying the same set of values if you want to run multiple migrations that share certain configuration details and mailboxes. For example:

- If certain mailboxes fail to migrate when you first run a migration, you can quickly create a new migration plan which only includes the mailboxes that failed to migrate the first time.
- If you are planning to migrate a large number of mailboxes, you can divide the workload into more manageable segments or among different migrators.
- If you want to migrate more than 100 mailboxes concurrently, you can create multiple migration plans with different administrator accounts and run them simultaneously. For more information, review information in [Connecting to Email Services](#).

Dashboard

Migration plans are viewed and managed in the **Dashboard**, which you open by clicking the **Dashboard** link in the breadcrumb bar.

The **Dashboard** displays the configuration settings of each migration plan and includes links pointing to the **Connections**, **Mailboxes**, **Options**, and **Migrate** tabs. To edit a migration plan, click the appropriate link to open the tab you want, make your changes, and then save the migration plan.

Migration plans that were created from a template, or copied from a plan that was previously created using a template, have a subtitle "*Created from [template_name]*" on the **Dashboard** page. To view the template details, click the template name. If the template has been deleted, you will see an alert dialog box.

Copying Migration Plans

To copy a migration plan:

1. Do one of the following:

- Open the Dashboard and click **Copy**.
- Open the Migrate tab and click **Copy Migration Plan**.

2. Specify a name for the copied migration plan.

By default, all the configuration details and mailboxes of the original migration plan are selected to be copied.

3. De-select the configuration details you do not want to copy and de-select the migration status of any mailbox you do not want to include in the new migration plan.

For example, if you want to create a migration plan that only includes mailboxes that failed to migrate in the original migration plan, you would keep the same connection properties and options and de-select all the mailbox statuses except Failed.

If the source migration plan was created using a template, all the **Connections** and **Options** fields will be selected to copy by default and grayed out.

4. Click **Copy**.

5. Edit the new migration plan as needed.

If the source migration plan was created using a template, the new plan will keep the connection properties and optional parameters specified by the template, as well as the same read only fields with the source plan.

Managing Migration Templates

The migration template facilitates the creation of migration plan by specifying the connection properties and optional parameters for the migration.

The migration template can be only created from an existing migration plan:

1. On the **Dashboard** page, select a migration plan from which you want to create a template, and click **Save as Template**.
2. In the **Save as Template** dialog box, specify a name for the template.
3. **(Optional)** To copy the connections and options from the migration plan, select the corresponding check boxes.
4. Click **Save**.

To view all of your existing templates and manage them, click **Manage Templates** in the **Dashboard** page to open the **Manage Templates** page where you can edit, delete or create a plan from a template.

On Demand Migration for Email provides an audit trail of these activities on the templates with audit logs:

- Creating, editing, deleting a template
- Creating a migration plan from a template

To view the audit log, click **Download Audit Logs** on the page to save it as a .csv file.

i **NOTE:** You must have the "Manage Templates" permissions to create, edit, delete a template and download audit logs. Without these rights, you can only view the template or create a plan from it.

For existing customers: "Manage Templates" permission is not set by default. Use ODME administrative account to create a new role and assign this permission to users in the On Demand portal. Then you need to log out and log in again to apply the new permission.

Editing or deleting a template will not affect any migration plans that were created from that template.

Changes to the template affect only those migration plans that are created subsequent to the changes.

Connecting to Email Services

To set up a migration, you must specify the connection properties for your source email service and target email service. This is done in the **Connections** tab.

When connecting to email services, be aware of the following:

- For all email services except G Suite and Sun ONE/iPlanet, you can connect to an email service either by specifying the login credentials of an administrator account, or you can select the option to migrate using the **end-user credentials** of each mailbox (source or target or both). If you select the **Use end-user credentials** option, you must specify the password for each mailbox when you add them to the migration plan, as described in the section, [Adding Mailboxes](#).
For Microsoft 365, you can also use Modern Authentication. The **Use Modern Authentication** option lets you grant consent to ODME instead of providing Administrative credentials with Application Impersonation rights. The **Use Modern Authentication** option is enabled for any newly created plan by default.

i **NOTE:** Connecting to POP and IMAP email services is always done through end-user credentials.

- Each mailbox in a source email service can be migrated successfully a total of 10 times with a maximum extraction limit of 500 GB across all migrations. This includes mailboxes that have 10 different date filters. This limit applies even if the 10 migrations do not migrate the same message more than once.
- For each Microsoft-based email service, a total number of mailboxes that can be migrated concurrently is limited per administrator (G Suite and Sun ONE/iPlanet have no such limitation). For details, see topic below.

Connecting to the Source Email Service

Refer to the sections below for instructions specific to your source email service.

[G Suite](#)

[Sun ONE/iPlanet](#)

[Microsoft Exchange 2007/2010/2013/2016/2019](#)

[Microsoft 365](#)

[Windows Live Hotmail](#)

[POP](#)

[IMAP](#)

[Zimbra](#)

G Suite

Connecting to a G Suite source email service from ODME is a two-stage process based on the OAuth 2 protocol: First, sign in with a super admin account so that ODME can verify your access.

Once this account has been verified, configure API settings in the Google Admin Console to grant access to ODME's service account.

i **IMPORTANT:** Be aware of the following:

- The OAuth 2 protocol used to connect to a G Suite email service replaces the OAuth Consumer Key and Consumer Secret method used in previous versions of ODME. Any connections to G Suite in migration plans created prior to ODME version 1.7 must be updated with the OAuth 2 connection procedure described below.
- IMAP must be enabled at the Organization level for ODME to connect to G Suite and run migrations.

Signing In

To sign in to G Suite:

1. In the **System** field, select **Google G Suite**.

i **NOTE:** If running a migration plan created prior to ODME 1.7, the **System** Field displays **Google G Suite (deprecated)**, meaning the connection properties used to connect to G Suite in previous versions of ODME no longer apply. Click **Upgrade** to update the connection properties.

2. Click **Sign in to Google**.

This opens the standard Google sign in UI.

3. Follow the Google prompts to sign in as a user with super admin rights and to grant ODME access permissions.

After completing the G Suite sign in process, ODME verifies that the user is a super admin (You will see a green success message once the sign-in process is complete). At this point you are redirected back to the ODME Connections tab, which now displays your super admin's username.

i **NOTE:** The Change User link allows the user to sign in as a different super admin and migrate from another G Suite account.

Configuring API Access

ODME connects to Google's APIs using an OAuth 2.0 service account. This account is identified by a client name shown on the Connections screen after you sign into G Suite. Below the client name is a set of URLs (called scopes) that represent the APIs ODME will access. You need to add the client name and scopes to the Google admin console to allow ODME to retrieve data using these APIs.

To Configure API Access:

1. In the Connections tab, use the **Copy to Clipboard** links to copy the values in the **Client Name** and **API Scopes** fields.
2. Click **Manage Google API Client Access**.

This opens the page in the Google Admin console.

NOTE: If the proper page is not displayed, from the admin console home page, go to the Security section (If not shown, its icon may be in the More Controls drawer at the bottom of the screen.) Click the **Show More** link and then select **Advanced Settings**. Finally, click the **Manage API Client Access** link.

Paste the text copied from the Client Name and API Scopes fields in the Connections tab to their respective fields in the Google Admin console. Then click Authorize.

CAUTION: You may receive connection validation and migration errors if API scopes are not granted correctly and if certain mail item API are turned off at the domain level or for particular mailboxes. To resolve this, make sure that all the scopes have been granted and enable all mail item migrations for all mailboxes. However, if you want to turn off migrations for particular mail items, such as Calendars or Contacts, uncheck the mail item in its migration types, and ODME will no longer validate that API connection or migrate the item. If a mail item is turned off, you have several choices:

- Leave the mail item turned off (item will not migrate)
- If the mail item is disabled at the domain level, enable it for the entire domain
- If the mail item is disabled for particular users:
 - Enable the item for those users
 - Move those users into a new plan that has item turned off.

Sun ONE/iPlanet

IMPORTANT: You cannot use end-user credentials to connect to a Sun ONE/iPlanet email service.

Specify the following values to connect to your Source ONE/iPlanet source email service:

- **Server Name**— Enter the location of the Sun ONE/iPlanet server as appears in the address bar when you log in as an administrator to your account.
- **Port** — Enter the Sun ONE/iPlanet server port number.
- **Use SSL** — If your server does not support SSL, all mailbox data will be transmitted non-encrypted. Use SSL connections if possible to secure your data. ODME supports self-signed SSL certificates.

NOTE: For information on generating a properly formatted self-signed SSL certificate, see [Using Self-Signed SSL Certificates](#).

- **Use end-user credentials** — Select this option if you want to connect to the email service using the passwords for each mailbox instead of the credentials of the administrator account. If selected, you must specify the password for each source mailbox. For more information, see [Adding Mailboxes](#).
- **Admin User Name and Password** — The name and password of the administrator account.

To migrate data from Sun ONE/iPlanet, your administrator account must have FullAccess rights to all mailboxes.

Microsoft Exchange 2007/2010/2013/2016/2019

Specify the following values to connect to your Exchange 2007/2010/2013/2016/2019 source email service:

- **Server URL**— You can enter the URL of the Exchange 2007/2010/2013/2016/2019 server manually, or you can use the auto-discovery option.

If you are not using HTTPS for Outlook Web Access (OWA), enter the full URL for your EWS service, e.g., <http://servername/EWS/Service.ASMX>.

i **NOTE:** For Exchange Server 2007 only: To enable the CPUU integration feature on the source Exchange Server 2007, you should turn on and configure WebDAV API access on your source Exchange Server 2007. For more details, see [Updating Outlook Client Profiles](#).

If you are using SSL, enter the name of your Exchange 2007/2010/2013/2016/2019 server manually (e.g., exchange.example.com).

i **NOTE:** If your server does not support SSL, all mailbox data will be transmitted non-encrypted. Use SSL connections if possible to secure your data. ODME supports self-signed SSL certificates. For information on generating a properly formatted self-signed SSL certificate, see [Using Self-Signed SSL Certificates](#).

- **Use auto-discovery** — Use auto-discovery to obtain the server URL. During a migration, this option uses the specified user name and password to retrieve the server URL that hosts your Exchange Web Services (EWS) server for the given mailbox.

If you are having problems with auto-discovery, you can test your external connectivity using a free tool from Microsoft. The following website can be used to validate if your services are working properly. Please go to <https://www.testexchangeconnectivity.com> to test your Exchange connectivity.

- **Use end-user credentials** — Select this option if you want to connect to the email service using the passwords for each mailbox instead of the credentials of the administrator account. If selected, you must specify the password for each source mailbox. For more information, see [Adding Mailboxes](#).
- **Admin User Name and Password** — The name and password of the administrator account.

The **Admin User Name** value is the account's UPN or domain credentials (e.g., [domain\username](#)). For more information about UPNs and how to determine which domain you are using for your users, please see [Active Directory naming](#) on the Microsoft Technet site.

Microsoft 365

Specify the following values to connect to the Microsoft 365 source email service:

- **Server Name** — You can enter the name of the Microsoft 365 server as it appears in the address bar when you log in as an administrator to your account, or you can use the auto-discovery option.
- **Use Modern Authentication** — You can use Modern Authentication to connect to Microsoft 365. The **Use Modern Authentication** option lets you grant consent to ODME instead of providing Administrative credentials with Application Impersonation rights. The **Use Modern Authentication** option is enabled for any newly created plan by default.

When the **Use Modern Authentication** option is enabled, the **Forwarding** section in a plan's **Options** page contains additional fields where you need to specify the credentials of the account which has the permissions to modify forwarding settings.

i **NOTE:** The **Use Modern Authentication** option is supported for connections to the Microsoft 365 Worldwide. The option is not supported for connections to the Microsoft 365 hosted in the Germany, China or US Government environments (Microsoft 365 GCC High).

- **Use auto-discovery** — It is recommended that you use auto-discovery to obtain the name of your Microsoft 365 server.

Auto-discovery uses your login credentials to automatically obtain the server name during a migration. With auto-discovery, On Demand Migration for Email connects directly to the Microsoft 365 auto-discovery endpoints, meaning that you don't have to configure your DNS to take advantage of auto-discovery. You do need to make sure that all your mailboxes exist in Microsoft 365 before migrating data into them.

- **Use end-user credentials** — Select this option if you want to connect to the email service using the passwords for each mailbox instead of the credentials of the administrator account. If selected, you must specify the password for each source mailbox. For more information, see [Adding Mailboxes](#).
- **Admin User Name and Password** — The name and password of the administrator account.

To migrate data to Microsoft 365, your administrator account must have Application Impersonation rights, which means the account must be assigned to a Role-Based Access Control group that has Application Impersonation rights. For more information, see [Preparing Your Source Email Service for Migration](#).

Windows Live Hotmail

The values used to connect to the Windows Live Hotmail source email service are configured automatically by ODME.

POP

Specify the following values to connect to the POP source email service:

- **Server Name** — Enter the location of the POP server.
- **Port** — Enter the POP server port number
- **Use SSL** — If your server does not support SSL, all mailbox data will be transmitted non-encrypted. Use SSL connections if possible to secure your data. ODME supports self-signed SSL certificates.

i | **NOTE:** For information on generating a properly formatted self-signed SSL certificate, see [Using Self-Signed SSL Certificates](#).

IMAP

Specify the following values to connect to the IMAP source email service:

- **Server Name** — Enter the location of the IMAP server.
- **Port** — Enter the IMAP server port number
- **Use SSL** — If your server does not support SSL, all mailbox data will be transmitted non-encrypted. Use SSL connections if possible to secure your data. ODME supports self-signed SSL certificates.

i | **NOTE:** For information on generating a properly formatted self-signed SSL certificate, see [Using Self-Signed SSL Certificates](#).

Zimbra

ODME uses a combination of IMAP and Zimbra's SOAP API to migrate data. Specify the following values to connect to your Zimbra source email service.

IMAP Settings

- **Server Name** — Enter the location of the IMAP server. Depending on your configuration, this may be the same location as the SOAP API server but with different port numbers.
- **Port** — Enter the IMAP server port number. The default is 143 (993 using SSL).
- **Use SSL** — If your server does not support SSL, all mailbox data will be transmitted non-encrypted. Use SSL connections if possible to secure your data. ODME supports self-signed SSL certificates.

i | **NOTE:** For information on generating a properly formatted self-signed SSL certificate, see [Using Self-Signed SSL Certificates](#).

- **Use end-user credentials** — Select this option if you want to connect to the email service using the passwords for each mailbox instead of the credentials of the administrator account. If selected, you must specify the password for each source mailbox. For more information, see [Adding Mailboxes](#).
- **Admin User Name and Password** — The name and password of the administrator account.

SOAP API Settings

- **Server Name** — Enter the location of the SOAP API server. Depending on your configuration, this may be the same location as the IMAP server but with different port numbers.
- **Admin Port** — Enter the port number for the admin connection to the SOAP API server. The admin connection is used for impersonation only. The default is 7071.
- **Port** — Enter the SOAP API server port number. The SOAP connection is used for all non-IMAP migrations. The default is 80.
- **Use SSL** — If your server does not support SSL, all mailbox data will be transmitted non-encrypted. Use SSL for both your admin connection and normal connection if possible to secure your data. ODME supports self-signed SSL certificates.

i | **NOTE:** For information on generating a properly formatted self-signed SSL certificate, see [Using Self-Signed SSL Certificates](#).

- **Admin User Name and Password** — The name and password of the administrator account.

Connecting to the Target Email Service

Refer to the sections below for instructions specific to your target server.

- [Microsoft 365](#)
- [Microsoft Exchange 2010/2013/2016/2019](#)
- [Using Self-Signed SSL Certificates](#)

Microsoft 365

Specify the following values to connect to the Microsoft 365 target email service:

- **Server Name** — You can enter the name of the Microsoft 365 server as it appears in the address bar when you log in as an administrator to your account, or you can use the auto-discovery option.

- **Use Modern Authentication** — You can use Modern Authentication to connect to Microsoft 365. The **Use Modern Authentication** option lets you grant consent to ODME instead of providing Administrative credentials with Application Impersonation rights. This option is enabled for any newly created plan by default.

When the **Use Modern Authentication** option is enabled, the **Forwarding** section in a plan's **Options** page contains additional fields where you need to specify the credentials of the account which has the permissions to modify forwarding settings.

i **NOTE:** The **Use Modern Authentication** option is supported for connections to the Microsoft 365 Worldwide. The option is not supported for connections to the Microsoft 365 hosted in the Germany, China or US Government environments (Microsoft 365 GCC High).

- **Use auto-discovery** — It is recommended that you use auto-discovery to obtain the name of your Microsoft 365 server.

Auto-discovery uses your login credentials to automatically obtain the server name during a migration. With auto-discovery, On Demand Migration for Email connects directly to the Microsoft 365 auto-discovery endpoints, meaning that you don't have to configure your DNS to take advantage of auto-discovery. You do need to make sure that all your mailboxes exist in Microsoft 365 before migrating data into them.

- **Use end-user credentials** — Select this option if you want to connect to the email service using the passwords for each mailbox instead of the credentials of the administrator account. If selected, you must specify the password for each target mailbox. For more information, see [Adding Mailboxes](#).
- **Admin User Name and Password** — The name and password of the administrator account.

To migrate data to Microsoft 365, your administrator account must have Application Impersonation rights, which means the account must be assigned to a Role-Based Access Control group that has Application Impersonation rights. For more information, see [Preparing Your Target Email Service for Migration](#).

Microsoft Exchange 2010/2013/2016/2019

Specify the following values to connect to your Exchange 2010/2013/2016/2019 target email service:

- **Server URL**— You can enter the URL of the Exchange 2010/2013/2016/2019 server manually, or you can use the auto-discovery option.

If you are not using HTTPS for Outlook Web Access (OWA), enter the full URL for your EWS service, e.g., <http://servername/EWS/Service.ASMX>.

If you are using SSL, enter the name of your Exchange 2010/2013/2016/2019 server manually (e.g., exchange.example.com).

i **NOTE:** If your server does not support SSL, all mailbox data will be transmitted non-encrypted. Use SSL connections if possible to secure your data. ODME supports self-signed SSL certificates. For information on generating a properly formatted self-signed SSL certificate, see [Using Self-Signed SSL Certificates](#).

- **Use auto-discovery** — Use auto-discovery to obtain the server URL. During a migration, this option uses the specified user name and password to retrieve the server URL that hosts your Exchange Web Services (EWS) server for the given mailbox.

If you are having problems with auto-discovery, you can test your external connectivity using a free tool from Microsoft. The following website can be used to validate if your services are working properly. Please go to <https://www.testexchangeconnectivity.com> to test your Exchange connectivity.

- **Use end-user credentials** — Select this option if you want to connect to the email service using the passwords for each mailbox instead of the credentials of the administrator account. If selected, you must specify the password for each target mailbox. For more information, see [Adding Mailboxes](#).
- **Admin User Name and Password** — The name and password of the administrator account.

The **Admin User Name** value is the account's UPN or domain credentials (e.g., domain\username). For more information about UPNs and how to determine which domain you are using for your users, please see [Active Directory naming](#) on the Microsoft Technet site.

Using Self-Signed SSL Certificates

When using self-signed SSL certificates to connect to an email service provider, the Issued By and Subject fields must match.

Windows-Based Systems

To generate a properly formatted certificate for Windows-based systems, use the SelfSSL utility packaged with the IIS 6.0 Resource Kit (available for download on <http://www.microsoft.com/en-us/download/details.aspx?id=17275>) and execute a command with the following syntax:

```
selfssl.exe /n:CN=autodiscover.domain.com /v:9999
```

Where /n: defines the Subject (which needs to match the issuer) and /v: is the number of days for which the cert is valid.

Linux-Based Systems

To generate a properly formatted certificate for Linux-based systems, use the OpenSSL utility (available for download on <http://www.openssl.org/>) and execute the following commands:

```
KEY + REQUEST
```

```
openssl req -out domain.com.csr -new -newkey rsa:2048 -keyout domain.com.key
```

```
CERT
```

```
openssl x509 -req -days 2000 -text -in domain.com.csr -signkey domain.com.key -out domain.com.crt
```

```
CONVERT CRT KEY TO PFX
```

```
openssl pkcs12 -export -out domain.com.pfx -inkey domain.com.key -in domain.com.crt
```

Validating Connections

After entering the connection properties of a source or target email service, enter the name of a source or target mailbox (and corresponding password if you selected the User end-user credentials option). Then click Test Connection. On Demand Migration for Email uses the login credentials you specified to connect to that mailbox. Depending on your type of source and target email service, different connection errors may be reported.



NOTE: You need to configure your firewalls to accept the WebRole IP addresses that ODME uses to validate connections. To obtain the current IP addresses, open the About box from the ODME home page:

- North America: <https://migration.ondemand.quest.com>
- EU: <https://migrationeu.ondemand.quest.com>
- APJ: <https://migrationapj.ondemand.quest.com>

Refer to the sections below for validation errors specific to your email platform:

G Suite
Sun ONE/iPlanet
Microsoft Exchange 2007/2010/2013/2016/2019
Microsoft 365
POP/Windows Live Hotmail
IMAP
Zimbra

G Suite

On Demand Migration for Email connects to the URL <http://www.google.com/a/example.com> (example.com is from the Google Domain setting above). If that page exists as a Google domain, the next step is to connect to the G Suite server using the OAuth 2 protocol.

Error	Description/Resolution
Any message saying an exception occurred because of an “invalid grant”, “invalid request”, or “400 bad request error”.	<p>Each scope URL gives ODME access to a different type of data. ODME checks that each scope has been granted when validating the connection. Note: All scopes need to be added for validation to succeed, even if the options to migrate certain item types are disabled.</p> <p>Make sure that the test mailbox used for validation exists. Confirm that the client name and API scopes have been set correctly in the Google Admin console. (The Connections screen shows instructions on doing this after you have signed into G Suite with a super admin account.)</p>
Unable to connect to the Google Contacts API.	<p>The test mailbox does not exist, the API scopes are not set correctly, or network issues are preventing ODME from reaching G Suite.</p> <p>Make sure that the test mailbox used for validation exists. Confirm that the client name and API scopes have been set correctly in the Google Admin console. (The Connections screen shows instructions on doing this after you have signed into G Suite with a super admin account.)</p>
Unable to connect to the Google Calendar API.	<p>The test mailbox does not exist, the API scopes are not set correctly, or network issues are preventing ODME from reaching GSuite. Make sure that the test mailbox used for validation exists. Confirm that the client name and API scopes have been set correctly in the Google Admin console. (The Connections screen shows instructions on doing this after you have signed into G Suite with a super admin account.)</p>
Invalid Mailbox (Unable to retrieve folders)	<p>The test mailbox does not exist or does not have IMAP access enabled, the API scopes are not set correctly, or network issues are preventing ODME from reaching G Suite.</p> <p>Make sure that the test mailbox used for validation exists and has IMAP access</p>

Error	Description/Resolution
	enabled. Confirm that the client name and API scopes have been set correctly in the Google Admin console.

Sun ONE/iPlanet

Error	Description/Resolution
The test mailbox doesn't exist.	You may see the following error when you test the connection: There was a problem testing your connection. Please try again. Verify that the mailbox name does exist in SunONE/iPlanet and that you have spelled the name correctly.
Server name is incorrect, or firewall is blocking access.	<p>You may see the following error when you test the connection:</p> <pre>Failed to connect sunone.example.com IMAP server.</pre> <p>Check that your server name is spelled correctly and that your firewall is open to the On Demand Email Migration for Email IP addresses to port 7191. To obtain the current IP addresses, open the About box from the ODME home page:</p> <ul style="list-style-type: none"> • North America: https://migration.ondemand.quest.com • EU: https://migrationeu.ondemand.quest.com • APJ: https://migrationapj.ondemand.quest.com

Microsoft Exchange 2007/2010/2013/2016/2019

On Demand Migration for Email uses Exchange Web Services (EWS) to connect to your on premises server from the cloud. To validate your server settings, the application connects to your Exchange server using port 443 (https) or port 80 (http) and the administrator credentials you provided in the server configuration.

If you enter a Server URL value that does contain http:// or https://, https:// will be prepended to the URL. It is recommended that you use the servername, but if you require http:// access, you should enter http://servername as the value for Server URL.

After the validation routine has connected to your Exchange server it opens the mailbox that you specified.

Problem	Description/Resolution
Firewall blocking access	<p>Your firewall is blocking the On Demand Migration for Email application. To ensure your data can be migrated, open the appropriate port for the On Demand Migration for Email application to connect to your server. To obtain the current IP addresses, open the About box from the ODME home page:</p> <ul style="list-style-type: none"> • North America: https://migration.ondemand.quest.com • EU: https://migrationeu.ondemand.quest.com • APJ: https://migrationapj.ondemand.quest.com
Migration administrator account doesn't have sufficient rights, or test mailbox doesn't exist	<p>You may see one of the following errors when you test the connection:</p> <pre>Invalid Mailbox (Unable to retrieve folders).</pre>

Problem	Description/Resolution
	<p>Invalid Mailbox (Unable to retrieve folders). The Autodiscover service returned an error.</p> <p>When this happens make sure your administrator account has been configured as described in the section, Microsoft Exchange 2007/2010/2013/2016/2019. Also verify that your test mailbox exists, and your spelling is correct.</p>
WebDAV API access is not configured on the source Exchange Server 2007	<p>In this case, you may get the following error:</p> <p>Cannot create a CPUU switch message. Reason: Cannot connect to the mailbox <mailbox name> using the Web Distributed Authoring and Versioning (WebDAV) protocol. Verify that WebDAV is configured and enabled on Exchange server.</p> <p>If this error occurs, make sure that the WebDAV API access is turned on and properly configured on your source Exchange Server 2007. For more details, please refer the Updating Outlook Client Profiles section.</p>

Microsoft 365

When entering connection properties for Microsoft 365, it is recommended that you select the Use auto-discovery option for your server. Entering the Server Name manually may cause errors when migrating many mailboxes.

Error	Description/Resolution
Migration administrator account doesn't have sufficient rights, or test mailbox doesn't exist	<p>You may see one of the following errors when you test the connection:</p> <p>Invalid Mailbox (Unable to retrieve folders).</p> <p>Invalid Mailbox (Unable to retrieve folders). The Autodiscover service returned an error.</p> <p>When this happens make sure your administrator account has been configured as described in the section, Microsoft 365. Also verify that your test mailbox exists, and your spelling is correct.</p>

POP/Windows Live Hotmail

Error	Description/Resolution
Invalid mailbox (Unable to retrieve folders): authentication failed.	Either the test mailbox you entered does not exist or you typed an incorrect password.
Invalid Mailbox (Unable to retrieve folders): The requested name is valid, but no data of the requested type was found.	The Server name and/or port number are incorrect.

IMAP

i | **NOTE:** Error messages may vary depending on the IMAP server you are connecting to.

Error	Description/Resolution
LOGIN Failure	Invalid password
Invalid login or password	Invalid login or password
A connection attempt failed because the connected party did not properly respond after a period of time, or established connection failed because connected host has failed to respond.	Invalid Port Number
No Such Host	Invalid server address

Zimbra

Error	Description/Resolution
Invalid Mailbox (Unable to retrieve folders): A connection attempt failed because the connected party did not properly respond after a period of time, or established connection failed because connected host has failed to respond <IP address>:<port number>.	Incorrect IMAP address/port
Invalid Mailbox (Unable to retrieve folders): AUTHENTICATE failed	Incorrect IMAP admin username/password
Invalid Mailbox (Unable to retrieve folders): Failed to connect to server <IP address> on admin port <port number> as user root. Unable to connect to the remote server	Incorrect SOAP address/admin port
Invalid Mailbox (Unable to retrieve folders): Unable to connect to the remote server	Incorrect SOAP port
Invalid Mailbox (Unable to retrieve folders): Failed to connect to server <IP address> on admin port <port number> as user root2. Exception of type 'Zimbra.Client.ZimbraException' was thrown.	Incorrect SOAP username/password
Invalid Mailbox (Unable to retrieve folders): Failed to connect to server <IP address> on admin port <port number> as user root. The underlying connection was closed: An unexpected error occurred on a receive	Incorrect SOAP Admin or Port SSL setting
Invalid Mailbox (Unable to retrieve folders): Tried to read a line. Only " received.	Incorrect IMAP SSL setting

Adding Mailboxes

After connecting to your source and target email service, the next step is to list the mailboxes you want to migrate. This is done in the **Mailboxes** tab.

i NOTE: If you haven't already done so, set up the mailbox accounts in the target email service. On Demand Migration for Email does not create target mailboxes during a migration. Also, you cannot add mailboxes until you have successfully connected to your source and target email service.

You can add the mailboxes you want to migrate manually, or in the case of a large migration, you can import a TSV file which lists each mailbox. If you selected the option Use end-user credentials when connecting to either the source or target email service, you must specify the passwords for each mailbox.

Be aware that if you import TSV file, this will overwrite any mailboxes that have already been added, whether manually or through a previously imported TSV file.

Supported mailbox types

This table lists mailbox types migrated by On Demand Migration for Email.

Source	User mailbox	Shared mailbox	Resource mailbox*	Group mailbox
G Suite	✓			
Exchange 2007/2010/2013/2016/2019	✓	✓	✓ *Migration from Exchange 2010, 2013, 2016, and 2019	
Microsoft 365	✓	✓	✓	
Sun ONE/iPlanet	✓			
Zimbra	✓			
IMAP	✓			
POP/Hotmail	✓			

Resource mailboxes for Exchange and Microsoft 365 are used for reserving and coordinating rooms and equipment.

Dealing with large mailboxes

Mailboxes that added to a migration plan are migrated in parallel as described in [Connecting to Email Services](#). However, contents of each individual mailbox are migrated subsequently, item by item. That may cause decreased migration performance for large mailboxes.

To make the migration faster for a large mailbox, you can split the mailbox's contents into several parts by time when message is created or received and then migrate each part in a separate migration plan.

To do that, take the following steps:

1. Approximately estimate the time period of messages within the mailbox by finding the oldest message and the newest.
2. Split the estimated time period into several shorter time intervals. Note that each time interval must have a one-day overlap with the neighbor time intervals to avoid data loss.
3. For each time interval create a separate migration plan. Note that each migration plan should use its own pair of source and target administrative accounts.
4. Add the mailbox to all of these migration plans.
5. On the **Options** page of each migration plan under **Date Range** select **Choose Date Range** and specify the corresponding time interval.

i **IMPORTANT:** In case of migration to Microsoft 365, it is not recommended to have more than 4 migration plans processing the same mailbox in parallel due to Microsoft 365 throttling limitations. Otherwise, the *The server cannot service this request right now. Try again later. Waiting 5.00 minutes before resuming* errors may repeatedly occur decreasing an overall migration speed.

Adding Mailboxes Manually

If you are migrating a relatively small number of mailboxes, you can add the mailboxes manually. If you selected the option **Use end-user credentials** when connecting to the source or target email service, you must also specify the password for each mailbox.

For the source IMAP servers that support Simple Authentication and Security Layer (SASL), like the Dovecot IMAP server, ODME can use the Administrator credentials of the IMAP server to access the user accounts. To add a user mailbox in this scenario, enter [user account name]*[administrator account name] in the **Source Mailbox** field, and provide the Administrator account password in the **Source Password** field.

To add mailboxes manually:

1. In the **Source Mailbox** field, enter the name of the source mailbox.
2. If you selected the option **Use end-user credentials** when connecting to the source email service, click in the **Source Password** field and enter the password for the source mailbox.
3. In the **Target Mailbox** field, enter the name of the target mailbox.
4. If you selected the option **Use end-user credentials** when connecting to the target email service, click in the **Target Password** field and enter the password for the target mailbox.
5. Click the Checkmark icon to add the mailbox.
6. Click **Add Mailbox** to activate a new row.
7. Repeat steps 1 through 6 for each mailbox you want to add.
8. When finished, click **Save** to stay on the **Mailboxes** tab, or click **Save and Continue** to move to the **Options** tab.

i | **NOTE:** If for any reason you want to undo the changes you made since the last time you saved, click **Discard Changes**.

Adding Mailboxes through a TSV File

Be aware that if you import TSV file, this will overwrite any mailboxes that have already been added, whether manually or through a previously imported TSV file.

To add mailboxes through a TSV file:

1. Create a text file which lists each mailbox to be migrated on a separate line beneath a "Source Mailbox" header.

For example:

Source Mailbox

psmith@example.com

bjones@example.com

bill.jones@example.com

i | **NOTE:** For G Suite, the full primary email address for each G Suite mailbox is required.

If a source mailbox is being migrated to a target mailbox with a different name, add a second header named “Target Mailbox” and list each target mailbox that is named different than its corresponding source mailbox

Source Mailbox	Target Mailbox
psmith@example.com	Patrick_Smith
# Paula_Smith source mailbox will be migrated to Paula_Smith on the target	
Paula_Smith@example.com	
bjones@example.com	Bill_Jones
Bill_Jones@example.com	

The format of each entry varies depending on the source or target server type, as shown in the following examples:

Exchange 2007/2010/2013/2016/2019 and Microsoft 365 Source and Target

The import file entry for an Exchange 2007/2010/2013/2016/2019 and Microsoft 365 source and target mailboxes should be the full SMTP address. If, however, the domain name for the SMTP address matches the domain name on the admin credential, then it can be omitted.

Source Mailbox	Target Mailbox
psmith@example.com	
bjones@example.com	Bill.Jones@example.com

IMAP source and Microsoft 365 Target

If the MAP server supports the Simple Authentication and Security Layer (SASL), user can provide a single Administrator credentials with user mailboxes in a TSV file. ODME will use the Administrator credentials to migrate user mailboxes, if you select the Use end-user credential option in the target.

Source Mailbox	Source Password	Target Mailbox	Target Password
psmnith@example.com*Admin user name	Admin Password1	psmith@office365.com	Password1
bjones@example.com*Admin user name	Admin Password2	bjones@office365.com	Password2

Specifying Mailbox Passwords

If you selected the option Use end-user credentials when connecting to the source email service, you must specify the password for each mailbox beneath a header named “Source Password.”

Source Mailbox	Target Password
psmnith@hotmail.com	Password1
bjones@hotmail.com	Password2

Likewise, if you selected the option Use end-user credentials when connecting to the target email service, you must specify the password for each mailbox beneath a header named "Target Password." In this case, your TSV file might look like this (be sure to specify any target mailboxes with different names under the "Target Mailbox" header):

Source Mailbox	Source Password	Target Mailbox	Target Password
psmnith@hotmail.com	Password1		Password1
bjones@hotmail.com	Password2		Password2
Bill.Jones@hotmail.com	Password3	bjones@example.com	Password3

2. Click the **Mailboxes** tab.
3. Click **Import TSV**.
4. In the dialog box, click **Select TSV File**. Then find and select the TSV file you want to upload.
5. Click **Import**.

On Demand Migration for Email imports the file and displays the list of source and target mailboxes. If any entries are improperly formatted, the file will not be imported and you must correct any errors identified. If you need to modify your migration plan, edit your source text file and then re-import. The entire list will be updated to the contents of your text file.

CAUTION: If you plan on running two different migration plans simultaneously to the same target email service, migrating the same mailbox can result in duplicated data on the target.

6. When finished, click **Save** to stay on the **Mailboxes** tab, or click **Save and Continue** to move to the **Options** tab.

If for any reason you want to undo the changes you made since the last time you saved, click **Discard Changes**.

Selecting Migration Options

In the **Options** tab, you can configure the following:

- The mailbox items you want to exclude from the migration
- For migrations from Exchange server and Microsoft 365, the option to migrate delegate access permissions and folder permissions.
- For G Suite and Microsoft 365, the mail forwarding settings between the source and target email service on a per-user basis

- For G Suite only, the maximum amount of data, in megabytes, that ODME should extract before pausing for a 24-hour period to avoid Google throttling the connection and preventing user access to the mailbox.
- For migrations from a source Exchange server to a target Exchange server, the option of downloading and installing Quest's Client Profile Update Utility and using it to update users' Client Profiles on the target server.
- The option to limit the maximum number of concurrent migrations for a plan.
- Email notifications about successfully completed migrations.

Selecting Items to Migrate

In the **Options** tab, you can specify which mailbox items (email, contacts, calendar appointments, recoverable items and tasks) you want to exclude from the migration. Also, you can exclude email that was not sent or received before, after, or within a specified date range. You can also opt to exclude email in the Junk, Deleted and Sent folders as well as folders you specify.

Primary mailbox and personal archive content must be migrated separately. If you wish to migrate content from both, your migration plan should be run two times, as follows:

1. Perform migration of primary content (default scenario)
In this case, the **Migrate from personal archives** option is disabled on the source and on the target.
2. Migrate personal archives according to your migration scenario:

NOTE: Personal archives can be migrated only from Exchange Server 2010, 2013, 2016, 2019, and Microsoft 365. Migration of personal archives is not supported for other source Email services.

Migration Scenario	Source option: Migrate from personal archives	Target option: Migrate to personal archives
archive to primary	enabled	disabled
archive to archive	enabled	enabled
primary to archive	disabled	enabled

NOTE: The primary mailboxes and personal archives can be migrated in any order, but two migration passes are required to migrate content from both.

Migration of Recoverable Items (optional):

- To enable this feature, select the **Recoverable Items** check box on the **Options** tab
- Migration of recoverable Items is supported in any combination of source / target mailbox type: from primary / archive mailbox to primary / archive mailbox.
- ODME migrates data from the **Recoverable Items** folder and its subfolders.
- ODME cannot filter or limit the scope of recoverable items
- Recoverable items of all types supported by ODME can be migrated. List of message classes and item types cannot be changed.

On Demand Migration for Email migrates all email and most supported mailbox items to Exchange 2010/2013/2016/2019 and Microsoft 365 target environments, as shown in the table below. However, ODME does not support migrating certain items, including but not limited to the following:

- Tasks / Notes from G Suite
- Contacts, calendars, and tasks from Sun ONE/iPlanet

For a complete list of items that are not migrated, see [Known Issues and Limitations](#).

Source	Email	Calendar	Contacts	Tasks / Notes	Rules	Groups / Personal Distribution Lists	Recoverable Items
G Suite	✓	✓	✓			✓	
Exchange 2007/2010/2013/2016/2019	✓	✓	✓	✓	✓ Except Exchange 2007	✓	✓ Except Exchange 2007
Microsoft 365	✓	✓	✓	✓	✓	✓	✓
Sun ONE/iPlanet	✓						
Zimbra	✓	✓	✓	✓		✓	
IMAP	✓						
POP/Hotmail*							

* POP Migrations only move items from the Inbox

To select items to migrate:

1. Click the **Options** tab.
2. In the Select Items to Migrate section, de-select any type of mailbox item you want to exclude from the migration, including Email, Contacts, Calendar, or Tasks/Notes.

For G Suite, you can also opt to exclude contacts that are contained in the “Other Contacts” folder.

3. For users migrating email from G Suite only, specify how you want ODME to migrate labeled messages:

There are two options:

- ODME creates a folder on the target for each label and copies messages into the corresponding folders.

By default, messages with multiple labels are copied into multiple target folders. However, you can configure ODME to migrate messages labeled Inbox, Sent, or Draft only to the corresponding target folders and ignore any other labels these messages may have. You can also configure ODME to ignore the Important label, in which case messages labeled Important are migrated either to the Archive folder if no other labels have been applied, or to target folders corresponding to any other labels the messages may have.

- ODME converts labels to categories on the target and assigns migrated messages to each corresponding category.

Labels corresponding to system folders (Inbox, Sent, Deleted, Junk, etc.) are migrated to their matching folders on the target and categories are not assigned.

4. If you want to exclude email that was not sent or received before, after, or within specific dates, select the option(s) and use the Calendar tool to select the dates you want.

Filtering Mailbox Folders

ODME supports filtering mailbox folders to narrow down the migration scope when you migrate emails.

CAUTION: Migrating Deleted Items and Junk Email could significantly increase migration time. Also, non-mail items are not migrated from the Deleted Items folder.

To filter folders for email migration:

1. Click the **Options** tab.
2. In the **Folders** section, select an option from the following:
 - **Migrate All:** Migrates all folders in the mailbox.
 - **Exclude:** Excludes the folders you select or specify (and sub-folders if any) from migration.
 - **Migrate Only:** Only migrates the folders that you select or specify (and sub-folders if any).
 - **Migrate content to a custom folder** - select this option to migrate a Google mailbox to a custom folder.
 - **Custom folder name** - specify the name of the custom folder. If a custom name is not provided, the default name will be used.

TIP: When you specify folders in the textbox, type one fully qualified path per line, for example, *Accounting/Notice*. Press **Enter** to add more paths.

The folders **Inbox**, **Drafts** and **Conversation History** in the **Exclude** list, and the option **Migrate Only** are only available when you migrate from Exchange or Microsoft 365, to Exchange or Microsoft 365.

If your folders are localized to another language, you can still select the corresponding checkboxes in English to filter them. However, when you specify folders in the textbox, type the localized folder names for the path.

Migrating Delegate Access Permissions

ODME supports migration of delegate access permissions from Exchange server and Microsoft 365.

To set up delegates migration:

1. Click the **Options** tab.
2. Open the **Migrate Permissions** portion of the screen.
3. Select the **Delegates** option.

Matching information for source and target users is taken from the migration plan. During the migration of the delegate list for the mailbox, ODME checks for the presence of a delegate in the mailbox list of the plan. If the delegate is not in the list, it will not be migrated.

We recommend the following migration approach:

- To migrate delegates, create one or several separate plans in which:
 - Only the **Delegates** option is selected. Items from the **Select Items to Migrate** partition are not selected.
 - A list of mailboxes contains all mailboxes that planned to be migrated by ODME and groups that can potentially participate as delegates in migrated mailboxes. These groups will not be migrated, they will be used only for the matching operation.



NOTE: The following statuses will be displayed for the groups:

- **Completed** status when **Use end-user credentials** option is not selected.
- **Interrupted** status when **Use end-user credentials** option is selected.
- **Interrupted** status when the admin user account that is used to grant the consent to ODME does not have a valid Exchange Online license.

The statuses do not mean that something goes wrong.

- You can run these plans as many times as necessary to synchronize the delegate permissions.



NOTE: After migration, the migration status of groups will show as **Interrupted** instead of **Completed** when end-user credentials are used for migration. No negative effects are found besides the status.

In case target delegate does not exist, delegate access permissions are migrated by ODME as is. If the target delegate exists, a maximal value of the source and target access permissions will be set .

In case a set of permissions was customized the following exceptions of this rule are applicable, see the tables below and the [Known Limitations](#) section for details:

Source	Target (in case matched delegate does not exist in target)	
Delegate access permission on source	Delegate access permission on target before migration	Delegate access permission on target after migration
None	N/A	None
Reviewer	N/A	Reviewer
Author	N/A	Author
Editor	N/A	Editor
Customized set (except None, Reviewer, Author, Editor)	N/A	None

Source	Target (in case matched delegate exist in target)	
Delegate access permission on source	Delegate access permission on target before migration	Delegate access permission on target after migration
None or customized set (except None, Reviewer, Author, Editor)	None or customized set (except None, Reviewer, Author, Editor)	None

Source	Target (in case matched delegate exist in target)	
Delegate access permission on source	Delegate access permission on target before migration	Delegate access permission on target after migration
Customized set (except None, Reviewer, Author, Editor)	Reviewer or Author or Editor	Reviewer or Author or Editor (value from target)
Reviewer or Author or Editor	Customized set (except None, Reviewer, Author, Editor)	Reviewer or Author or Editor (value from source)
Reviewer or Author or Editor	Reviewer or Author or Editor	Maximal value of the source and target access permissions. Possible values - Reviewer or Author or Editor

Migrating Folder Permissions

ODME supports migration of folder permissions from Exchange server and Microsoft 365.

i | **NOTE:** Migration of folder permissions for Recoverable Items is not supported.

To set up migration of folder permissions:

1. Click the **Options** tab.
2. Open the **Migrate Permissions** portion of the screen.
3. Select the **Folder Permissions** option.

Matching information for source and target users is taken from the current migration plan.

We recommend the following migration approach:

- To migrate folder permissions, create one or several separate plans in which:
 - Only the **Folder Permissions** option is selected. Items from the **Select Items to Migrate** partition are not selected.
 - A list of mailboxes contains all mailboxes that planned to be migrated by ODME and groups that can potentially participate as grantees in migrated mailboxes folder permissions. These groups will not be migrated, they will be used only for the matching operation.



NOTE: The following statuses will be displayed for the groups:

- **Completed** status when **Use end-user credentials** option is not selected.
- **Interrupted** status when **Use end-user credentials** option is selected.
- **Interrupted** status when the admin user account that is used to grant the consent to ODME does not have a valid Exchange Online license.

The statuses do not mean that something goes wrong.

You can run these plans as many times as necessary to synchronize the folder permissions.

- For the content migration, use migration plans as usual and do not check the **Folder Permissions** option in these plans.

In case the target permission does not exist, permissions are migrated by ODME as is. If the target permission exists, a maximal value of the source and target access permissions will be set .

Source	Target (in case matched folder permission does not exist in target)	
Folder permission on the source	Folder permission on the target before migration	Folder permission on the target after migration
None	N/A	None
Owner	N/A	Owner
Publishing Editor	N/A	Publishing Editor
Editor	N/A	Editor
Publishing Author	N/A	Publishing Author
Author	N/A	Author
Nonediting Author	N/A	Nonediting Author
Reviewer	N/A	Reviewer
Contributor	N/A	Contributor
Custom	N/A	Custom

Migrating Rules

ODME supports rules migration from Microsoft 365, Exchange 2019, 2016, 2013, and 2010. This includes OWA (Outlook Web App) Inbox rules, and the rules created in an Outlook client version 2019, 2016, 2013, 2010, or Outlook for Microsoft 365.



NOTE: Migration of rules created in Outlook from Exchange 2010 is not supported yet.

To migrate rules

- Create a separate plan in which:
 1. Only the **Rules** option is selected. Other items from the **Select Items to Migrate** partition are not selected.
 2. A list of mailboxes contains all mailboxes that planned to be migrated by ODME and groups that can potentially participate in the rules to be migrated. These groups will not be migrated, they will be used only for the matching operation.

NOTE: The following statuses will be displayed for the groups:

- **Completed** status when **Use end-user credentials** option is not selected.
- **Interrupted** status when **Use end-user credentials** option is selected.

The statuses do not mean that something goes wrong.

- To migrate other content (such as messages, contacts), use migration plans as usual and do not check the **Rules** option in these plans.

Matching information for source and target users is taken from the migration plan. When the source email address is an Active Directory user or group, you must specify the email address with its primary domain name in the target, or rules may not work properly after migration. During the migration of the rules for the mailbox, ODME checks for the presence of a user or group in the mailbox list of the plan. If the user or group is not in the list, rules will not be migrated.

CAUTION: Every time you run the migration plan to migrate rules, ODME removes all the existing rules from your target first (including previously-migrated rules, and the rules you created in the target), and then migrates all the rules on the source to your target.

CAUTION: If the rules in a user's target Outlook do not match the rules on the server, the following message appears when the user opens the target mailbox in Outlook after migration:

The rules on this computer do not match the rules on Microsoft Exchange. Only one set of rules can be kept. You will usually want to keep the rules on the server. Which rules do you want to keep?

In this case, the user has to select "Server" to avoid data loss.

Rules that contain unsupported conditions or actions will not be migrated, or will not work after migration. So, you will need to set them up manually on the target. For other known limitations to migration of rules, see the *Rules* section in [Microsoft Exchange](#) or [Microsoft 365](#)

The following tables list the supported conditions and actions for rules created from Outlook:

Outlook Condition	Outlook 2019	Outlook 2016	Outlook 2013	Outlook 2010	Outlook for Microsoft 365
from people or public group	Yes	Yes	Yes	Yes	Yes
with specific words in subject	Yes	Yes	Yes	Yes	Yes
through the specified account	No	No	No	No	No
sent only to me	Yes	Yes	Yes	Yes	Yes
where my name is in the To box	Yes	Yes	Yes	Yes	Yes

Outlook Condition	Outlook 2019	Outlook 2016	Outlook 2013	Outlook 2010	Outlook for Microsoft 365
marked as importance	Yes	Yes	Yes	Yes	Yes
marked as sensitivity	Yes	Yes	Yes	Yes	Yes
flag for action	Yes	Yes	Yes	Yes	Yes
where my name is in the Cc box	Yes	Yes	Yes	Yes	Yes
where my name is in the To or Cc box	Yes	Yes	Yes	Yes	Yes
where my name is not in the To box	Yes	Yes	Yes	Yes	Yes
sent to people or public group	Yes	Yes	Yes	Yes	Yes
with specific words in the body	Yes	Yes	Yes	Yes	Yes
with specific words in the subject or body	Yes	Yes	Yes	Yes	Yes
with specific words in the message header	Yes	Yes	Yes	Yes	Yes
with specific words in the recipient's address	Yes	Yes	Yes	Yes	Yes
with specific words in the sender's address	Yes	Yes	Yes	Yes	Yes
assigned to specific category	Yes	Yes	Yes	Yes	Yes
assigned to any category	Yes	Yes	Yes	Yes	Yes
which is an automatic reply	Yes	Yes	Yes	Yes	Yes
which has an attachment	Yes	Yes	Yes	Yes	Yes
with a size in a specific range	Yes	Yes	Yes	Yes	Yes
received in a specific date span	Yes	Yes	Yes	Yes	Yes
uses the specific form	Yes	Yes	Yes	Yes	Yes
sender is in specific Address Book	No	No	No	No	No
with selected properties of documents or forms	Yes	Yes	Yes	Yes	Yes
which is a meeting invitation or update	Yes	Yes	Yes	Yes	Yes
from RSS feeds with specified text in the title	Yes	Yes	Yes	Yes	Yes
from any RSS feed	Yes	Yes	Yes	Yes	Yes
of the specific form type	Yes	Yes	Yes	Yes	Yes
on this computer only	Yes	Yes	Yes	Yes	Yes

Outlook Action	Outlook 2019	Outlook 2016	Outlook 2013	Outlook 2010	Outlook for Microsoft 365
move it to the specified folder	Yes	Yes	Yes	Yes	Yes
move a copy to the specified folder	Yes	Yes	Yes	Yes	Yes
assign it to the specific category	Yes	Yes	Yes	Yes	Yes
delete it	Yes	Yes	Yes	Yes	Yes
permanently delete it	Yes	Yes	Yes	Yes	Yes
forward it to people or public group	Yes	Yes	Yes	Yes	Yes
forward it to people or distribution list as an attachment	Yes	Yes	Yes	Yes	Yes
redirect it to people or distribution list	Yes	Yes	Yes	Yes	Yes
have server reply using a specific message	No	No	No	No	No
reply using a specific template	Yes	Yes	Yes	Yes	Yes
flag message for action in a number of days	Yes	Yes	Yes	Yes	Yes
clear the Message Flag	Yes	Yes	Yes	Yes	Yes
clear message's categories	Yes	Yes	Yes	Yes	Yes
mark it as importance	Yes	Yes	Yes	Yes	Yes
print it	Yes	Yes	Yes	Yes	Yes
play a sound	Yes	Yes	Yes	Yes	Yes
start application	N/A	No	No	No	N/A
mark it as read	Yes	Yes	Yes	Yes	Yes
run a script	N/A	No	No	No	N/A
perform a custom action	N/A	N/A	N/A	No	N/A
display a specific message in the New Item Alert window	Yes	Yes	Yes	Yes	Yes
display a Desktop Alert	Yes	Yes	Yes	Yes	Yes
apply retention policy	No	No	No	No	No
stop processing more rules	Yes	Yes	Yes	Yes	Yes

The following tables list the supported conditions and actions for OWA Inbox rules:

OWA Condition for Exchange	Exchange 2019	Exchange 2016	Exchange 2013	Exchange 2010
Message was received from the specified users or groups in GAL	Yes	Yes	Yes	Yes
Message was sent to the specified users or groups	Yes	Yes	Yes	Yes

OWA Condition for Exchange		Exchange 2019	Exchange 2016	Exchange 2013	Exchange 2010
in GAL					
Message contains the specified words	in the subject	Yes	Yes	Yes	Yes
	in the subject or body	Yes	Yes	Yes	Yes
	in the sender's address	Yes	Yes	Yes	Yes
	in the body	Yes	Yes	Yes	Yes
	in the recipient's address	Yes	Yes	Yes	Yes
	in the message header	Yes	Yes	Yes	Yes
My name is	in the To or Cc box	Yes	Yes	Yes	Yes
	the only recipient listed	Yes	Yes	Yes	Yes
	in the To box	Yes	Yes	Yes	Yes
	in the Cc box	Yes	Yes	Yes	Yes
	not in the To box	Yes	Yes	Yes	Yes
Message is marked with	Importance	Yes	Yes	Yes	Yes
	Sensitivity	Yes	Yes	Yes	Yes
Message is	accompanied by an attachment	Yes	Yes	Yes	Yes
	of the type...	Yes	Yes	Yes	Yes
	flagged as...	Yes	Yes	Yes	Yes
	classified as...	No	No	No	No
Message size is within a specified range		Yes	Yes	Yes	Yes
Message was received within a specified date span		Yes	Yes	Yes	Yes
Apply to all messages		Yes	Yes	Yes	Yes

OWA Condition for Microsoft 365

Microsoft 365

People	From	Yes
	To	Yes

OWA Condition for Microsoft 365		Microsoft 365
My name is	I'm on the To line	Yes
	I'm on the Cc line	Yes
	I'm on the To or Cc line	Yes
	I'm not on the To line	Yes
	I'm the only recipient	Yes
Subject	Subject includes	Yes
	Subject or body includes	Yes
Keywords	Message body includes	Yes
	Sender address includes	Yes
	Recipient address includes	Yes
	Message header includes	Yes
Marked with	Importance	Yes
	Sensitivity	Yes
	Classification	Yes
Message includes	Flag	Yes
	Type	Yes
	Has attachment	Yes
Message size	At least	Yes
	At most	Yes
Received	Before	Yes
	After	Yes
All messages	Apply to all messages	Yes

OWA Action for Exchange		Exchange 2019	Exchange 2016	Exchange 2013	Exchange 2010
Move message to folder		Yes	Yes	Yes	Yes
Copy message to folder		Yes	Yes	Yes	Yes
Delete message		Yes	Yes	Yes	Yes
Pin message		Yes	Yes	N/A	N/A
Mark message	as read	Yes	Yes	Yes	Yes
	as junk	Yes	Yes	N/A	N/A
	with importance	Yes	Yes	Yes	Yes
	with a category	Yes	Yes	Yes	Yes

OWA Action for Exchange	Exchange 2019	Exchange 2016	Exchange 2013	Exchange 2010
Forward message to...	Yes	Yes	Yes	Yes
Forward message as an attachment to...	Yes	Yes	Yes	Yes
Redirect message to...	Yes	Yes	Yes	Yes
Send a text message to... [*]	Yes	Yes	Yes	Yes
Stop processing more rules	Yes	Yes	Yes	Yes

[*] This action will not work after migrated to Microsoft 365 because Microsoft 365 does not support it.

OWA Action for Microsoft 365	Microsoft 365
Organize	Move to
	Copy to
	Delete
	Pin to top
Mark message	Mark as read
	Mark as Junk
	Mark with importance
	Categorize
Route	Forward to
	Forward as attachment
	Redirect to
Stop processing more rules	Yes

Setting Up Mail Forwarding

ODME supports automated mail forwarding on a per-user basis for these email services: G Suite, Microsoft 365 and Zimbra. After configuring your email service to interface with the ODME mail forwarding feature (as described in the section [Setting Up Mail Routing](#)), specify the required forwarding parameters in the **Options** tab.

To set up mail forwarding:

1. Click the **Options** tab.
2. Open the **Forwarding (Optional)** portion of the screen.
3. Select the type of mail forwarding operation you want ODME to execute.

Options include:

- **Forward new items as they arrive** — Mail is forwarded to a mailbox in a specified source or target email service and domain. When you select this option, you are prompted to select the source or target email service in the migration plan that you want to set forwarding on as well as the domain that mail is to be forwarded to.
- **Turn off existing forwarding** — Existing mail forwarding settings are removed from a mailbox in a specified source or target email service and domain.

These options are enabled only if mail forwarding is supported for the source or target email service in the migration plan. If mail forwarding is supported for only one email service in the migration plan (source or target), then you can only select one of the two options.

If mail forwarding is supported for both the source and target, then both options are enabled. In this case, when you select one option, the other option is automatically selected as well. This is designed to prevent messages from looping perpetually between two mailboxes in the event that mail forwarding is inadvertently set on both the source and the target email service. However, if you want to set or remove mail forwarding on only one of the two email services in the migration plan, you can de-select one of the automatically selected options.

4. If you selected the **Forward new items as they arrive** option, do the following:

- a. In the **Set forwarding address on:** field, select the source or target email service that you want to set forwarding on.

The source email service specified in the migration plan is selected by default. Select the target email service if you want to set forwarding on that instead.

When G Suite is selected as the source email service, these **Forwarding Actions** are available for you to decide what you want ODME to do when new mail items arrive:

- **KEEP:** When new mail items arrive, new item is delivered to source mailbox and kept in the Inbox as well as forwarded to target mailbox.
- **DELETE:**
 - For G Suite: When new mail items arrive, new item is delivered to source mailbox and moved to the Trash folder as well as forwarded to target mailbox.
- **MARK AS READ:** When new mail items arrive, new item is delivered to source mailbox and marked as read in the Inbox as well as forwarded to target mailbox.
- **ARCHIVE (for G Suite only):** When new mail items arrive, new item is delivered to source mailbox and archived (not visible in the Inbox) as well as forwarded to target mailbox.

i NOTE: If mail forwarding is supported for both the source and target email services, when you set mail forwarding on one service (source or target), the option to turn off existing forwarding defaults to the other service automatically.

- b. In the **Forward to:** field, enter the domain that mail is to be forwarded to.

Improperly formatted domain names result in an error message.

The domain name part of the forwarding email address (<local_part>@<domain>) is specified by the domain you enter in the **Forward to** field. The local part depends on which email service you selected in step a: When the source email service is selected, the local part of the target email address will be used; And when the target email service is selected, the local part of the source email service will be applied.

- c. For Microsoft 365, when the **Use Modern Authentication** option is enabled, the **Forwarding** section in a plan's **Options** page contains additional fields where you need to specify the credentials of the account which has the permissions to modify forwarding settings.
- d. For G Suite only, enter the name and password of the administrator account used for mail forwarding.
- d. Click **Test**.

This validates that the proper administrator credentials have been provided to perform mail forwarding. For Microsoft 365, the administrator account must be assigned the "Recipient Management" role. See the section [Setting Up Mail Routing](#) for more information.

5. If you selected the **Turn off existing forwarding** option, do the following:

- a. In the **Remove forwarding address from:** field, select the source or target email service that you want to remove existing forwarding settings from.

i **NOTE:** If mail forwarding is supported for both the source and target email service and you already set mail forwarding on one email service, this field defaults to the other service.

- b. In the **Forwarding to:** field, enter the domain to which mail is currently forwarded.

Improperly formatted domain names result in an error message.

- c. For Microsoft 365, when the **Use Modern Authentication** option is enabled, the **Forwarding** section in a plan's **Options** page contains additional fields where you need to specify the credentials of the account which has the permissions to modify forwarding settings.
- d. For G Suite only, enter the name and password of the administrator account used for the mail forwarding settings you want to remove.
- d. Click **Test**.

This validates that the proper administrator credentials have been provided to perform mail forwarding. For Microsoft 365, the administrator account must be assigned the "Recipient Management" role. See the section [Setting Up Mail Routing](#) for more information.

Managing Google Throttling

Google traffic throttling imposes a daily limit on the amount of data you can extract from your G Suite source within 24 hours. When this limit is reached during a migration, G Suite throttles all connections to the affected mailboxes up to 24 hours, during this period users cannot access the mailboxes via web or mobile devices.

You can control how much data On Demand Migration for Email will extract during this period to avoid the risk of Google mailbox throttling.

i **NOTE:** ODME currently does not coordinate data extraction from a mailbox across multiple migration plans or migrations within the same plan. For example, if two migration plans are migrating the same mailbox, ODME does not take into consideration the data downloaded from all the plans when determining when to pause a migration. Likewise, if a plan was migrated and finished, and then migrated again, the quota consumed from the first migration is taken into consideration when determining when to pause a migration. Additionally, if you stop and restart a plan, the quota consumed is not factored. Google, however, DOES record this information and could result in throttling taking effect.

To manage Google Throttling:

1. Click the **Options** tab.

If you migrating from a G Suite source, the **Manage Data Extraction** portion of the tab is displayed.

2. Specify the amount of data, in megabytes, that ODME will extract from Google before pausing for 24 hours.

Updating Outlook Client Profiles

During a migration, ODME moves mailboxes from the source Microsoft Exchange server to the target Microsoft Exchange server. Before users can start using their installation of Outlook with their new target mailboxes, their Microsoft Outlook Client Profiles must also be updated.

Quest Client Profile Updating Utility (CPUU) allows these profiles to be updated automatically and transparently. The utility is used to switch end-user Microsoft Outlook Client Profiles from the source to the target Exchange server once the user's mailbox is migrated. The utility can also be used to roll back Client Profiles to their original setting. The Client Profile Updating Utility can be downloaded from <https://support.quest.com/on-demand-migration-for-email/current/download-new-releases>.

The Client Profile Updating Utility looks for a special hidden message in a user's mailbox to determine if it should do a switch or rollback. These special hidden messages can be created by ODME during a migration.

Some of the CPUU features are not supported or partially supported by ODME. For details about limitations and compatibility issues during profile update, see below. For the full list of CPUU features, refer to <https://support.quest.com/technical-documents/client-profile-updating-utility/>.

i **NOTE:** Migration from Exchange/Microsoft 365: ODME needs that the target Autodiscover service is functioning correctly in order to put the hidden "switch message" for CPUU. The requirement is actual regardless of whether the **Use Autodiscover** option is enabled or not on the plan's **Connections** page.

Migrating from one Microsoft 365 tenant to another with domain name transfer scenario

CPUU supports Microsoft 365 tenant to tenant migration including scenario with domain name transfer starting from the version 5.7.1. For more details, see the *Tenant to tenant migration scenario with domain name transfer* section in [Client Profile Updating Utility Administrator Guide](#).

i **NOTE:** In this scenario, CPUU does not switch a profile and does not support any additional features, it just deletes some dynamic data from the profile and this allows Outlook to switch the profile successfully when a user opens it after the domain name transfer.

If a user opens a profile after the domain name transfer but before starting CPUU - everything will work fine if the user starts CPUU later.

Supported CPUU Features

- Switch Outlook profiles from the source to the target Exchange server (Existing Offline folders (OST files) are not preserved)
- Update Send/Receive Settings
- Rules

In order CPUU to process recipients in mailbox rules, you need to assign X500 address to all the target recipients which can potentially participate in rules conditions/actions and set a LegacyExchangeDN of a corresponding source recipient as its value. You can populate X500 address manually or use the other Quest solutions: Migration Manager for Active Directory for "Exchange to Microsoft 365" scenarios and On Demand Migration for "Microsoft 365 to Microsoft 365" scenarios.

Partially Supported CPUU Features

CPUU Feature	Limitations of using CPUU with ODME
Microsoft Outlook Bar Shortcuts	CPUU does not process shortcuts for folder in other user mailboxes and Public Folders due to the following reasons: <ul style="list-style-type: none">Public Folder migration is not supported.There is no matching information for source and target users.
Move to Folder Shortcuts	
Outlook Wunder bar	
Microsoft Outlook Address Book	CPUU does not process Contact folders in Public Folders because the migration of Public Folders is not supported.
Profile Properties and Logon Network settings	CPUU does not process address books in other user mailboxes because there is no matching information for source and target users.
User-Defined Folder Names	CPUU does not update names of Public Folders because the migration of Public Folders is not supported.
Folder Views	CPUU does not process Folder Views which have filtering by the From and Sent To attributes because there is no matching information for source and target users.
Search Folders	CPUU does not process Search Folders which have filtering by the From and Sent To attributes because there is no matching information for source and target users.

Not Supported CPUU Features

CPUU Feature	Limitations of using CPUU with ODME
Other User's Folder Shortcuts	These features are not supported because there is no matching information for source and target users.
Delegates	
Additional Mailboxes	
Distribution Lists	
Contact Nicknames	
Group Schedules	This feature is not supported due to the following reasons: <ul style="list-style-type: none">There is no matching information for source and target users.Associated content is not migrated.There is no matching information for messages.
Preserve Offline folders (OST files)	This feature is not supported. Offline folders are recreated after the mailbox switch.

How to deal with non-supported and partially supported CPUU features:

- **Option 1: Disable non-supported and partially supported CPUU features to increase the speed of profile processing**
You can disable CPUU features on the **Features** step of the Quest Client Profile Updating Utility Configuration wizard. To do this, select the features you need (multiselect is allowed), click **Change** and then select the **Skip** option in the **Select Processing Option** dialog. If this option is chosen, the user should manually configure Microsoft Outlook features after profile processing.
- **Option 2: Keep CPUU features and make some adjustments after profile processing**
If something does not work in the profile after processing, you should repair it manually. For example, you can change incorrect links in Microsoft Outlook rules. For that, open the **File** tab in Microsoft Outlook, select **Info** and then press **Manage Rules & Alerts**. Links can be changed in the **Rule description** section of the **Rules and Alerts** dialog.
- **Option 3: Configure matching between source and target users before processing Microsoft Outlook profiles**
This will allow you to fully support CPUU features that require matching information for source and target users. To configure user matching, add the **legacyExchangeDN** attribute value of the target user to the **proxyAddress** attribute of the source user as x500 address.

To configure ODME to work together with CPUU

1. Click the **Options** tab.
2. Click the **Outlook Profile** tab.
3. Select the option you want.

Options include:

- **Do Not Modify Outlook Profiles**
- **Enable Outlook Profile Update**
- **Enable Outlook Profile Rollback**



NOTE: Switching Exchange Server 2007 profiles

To enable the CPUU integration feature on the source Exchange Server 2007, you should turn on and configure the WebDAV API access for your Exchange Server 2007.

Configuration Requirements for WebDAV

- WebDAV must be available on the same Exchange server as the EWS service (link to the EWS service is specified on the ODME **Connections** page) and reside in the default **Exchange** virtual directory in Internet Information Services (IIS).
For example, if the specified source **Server URL** is *https://<Exchange server name>/EWS/Exchange.asmx*, WebDAV must be available at the following link: *https://<Exchange server name>/Exchange*.
- **Basic Authentication, Forms Based Authentication** or both authentication methods must be enabled for the **Exchange** virtual directory in Internet Information Services (IIS) Manager.
- It is recommended to enable the **Require SSL** option on the **SSL Settings** page for the **Exchange** virtual directory in Internet Information Services (IIS) Manager.

To update Microsoft Outlook profiles with CPUU

1. Download and install Client Profile Updating Utility.
2. Run the **Quest Client Profile Updating Utility Configuration** wizard. While running the wizard, change the following options:
 - On the **Credentials** step, select the **Use the following user account** option and specify two user accounts to log on to the source and target mailboxes. It is recommended to use the same accounts that were specified as **Source Connection** and **Target Connection** administrative accounts in the **Migration Plan**.
 - On the **Network** step, deselect the **Check availability of Exchange servers with ping command** option.
3. Go to the Client Profile Updating Utility installation folder and copy its content to any folder on a machine where Outlook profiles need to be processed.
4. Run the **CPUU_Update.bat** file and wait until the utility finishes updating the Outlook profiles. To roll back the changes made by CPUU, run **CPUU_Rollback.bat**.

If you need to process Outlook profiles on multiple machines, you should run Client Profile Updating Utility from Logon Script.

For detailed instructions, including recommended usage and deployment options, see Client Profile Updating Utility Administration Guide: <https://support.quest.com/technical-documents/client-profile-updating-utility/>.

Limiting Concurrent Migrations

In order to protect source and target mail systems from heavy loads from On Demand Migration for Email, you can use this option to limit the maximum number of mailboxes migrated simultaneously.

To limit concurrent migrations:

1. Click the **Options** tab.
2. Click the **Advanced** tab.
3. Specify the number of concurrent migrations for the migration plan or select the **Unlimited** option.

Setting User Notifications

You can configure email notification settings to send notifications after the migration session is completed successfully to source or target user, or both. These settings are disabled by default.

To configure email notification settings:

1. Click the **Options** tab.
2. Click the **Notification** tab.
3. You can configure email notifications for source and target users separately. Select the **Send notification to source mailbox** option and /or **Send notification to target mailbox** option.
The following fields can be configured:

- From display name
- From e-mail address
- Subject
- Message body

Known Issues and Limitations

On Demand Migration for Email is designed to provide a robust migration experience for a variety of source and target platforms. However, certain issues and limitations have been identified. Issues are items which are slated to be resolved in future releases of ODME. Limitations, on the other hand, are the result of inherent discrepancies between email service platforms and cannot be fixed.

Known Limitations

General

- Recurring meetings within non-Exchange source platforms are typically generated and stored using very different methodologies than the recurrence rules leveraged by Microsoft platforms. On Demand Migration for Email uses advanced technology in attempt to map recurring meetings to equivalent recurrence rules in Exchange. However, depending on the source environment and specific data, some dates of meeting invitations may be incorrectly represented in Outlook after migration
- Each mailbox in a source email service can be migrated successfully a total of 10 times and each migration cannot exceed 500 GB. These limits are in place to control the costs of migration. If an exception is required to facilitate your migration plan, please contact the Support Portal at <https://support.quest.com/>.

Client Profile Updating Utility

Consider the following limitations when using ODME together with Client Profile Updating Utility (CPUU):

- Migration from Exchange/Microsoft 365: ODME needs that the target Autodiscover service is functioning correctly in order to put the hidden "switch message" for CPUU. The requirement is actual regardless of whether the **Use Autodiscover** option is enabled or not on the plan's **Connections** page.
- CPUU does not process shortcuts for folder in other user mailboxes and Public Folders due to the following reasons:
 - Public Folder migration is not supported.
 - There is no matching information for source and target users.
- CPUU does not process Contact folders in Public Folders because the migration of Public Folders is not supported.
- CPUU does not process address books in other user mailboxes because there is no matching information for source and target users.

- CPUU does not process recipients, folders in other mailboxes and Public Folders, and links to reply templates due to the following reasons:
 - There is no matching information for source and target users.
 - Associated content is not migrated.
 - Public Folder migration is not supported.
- CPUU does not update names of Public Folders because the migration of Public Folders is not supported.
- CPUU does not process Folder Views which have filtering by the From and Sent To attributes because there is no matching information for source and target users.
- CPUU does not process Search Folders which have filtering by the From and Sent To attributes because there is no matching information for source and target users.
- These following CPUU features are not supported because there is no matching information for source and target users: "Other User's Folder Shortcuts", "Delegates", "Additional Mailboxes", "Distribution Lists", "Contact Nicknames".
- This "Group Schedules" feature is not supported due to the following reasons:
 - There is no matching information for source and target users.
 - Associated content is not migrated.
 - There is no matching information for messages.
- The "Preserve Offline folders (OST files)" feature is not supported. Offline folders are recreated after the mailbox switch.
- To enable the CPUU integration feature on the source Exchange Server 2007, you should turn on and configure the WebDAV API access for your Exchange Server 2007.

To configure ODME to work together with CPUU, please see <http://documents.quest.com/on-demand-migration-for-email/user-guide/configuring-and-running-migrations/selecting-migration-options/updating-outlook-client-profiles>.

For the full list of CPUU features, refer to <http://support.quest.com/technical-documents/client-profile-updating-utility/5.7.4/administration-guide/>.

Microsoft Exchange

General

- When viewing migrated data in OWA, there may be slight differences in the received time of emails when comparing the source to the time recorded in the target. This affects all Exchange source environments and Exchange 2013/2016/2019 target email services.
- When migrating from an Exchange server, any email addresses associated with existing users will be converted to SMTP addresses based on the source system. This means that X500 addresses will not be migrated for items, and the SMTP address on the migrated items will not be updated to the new SMTP address. In order to get Exchange to update to the new address the primary SMTP address on the source system should be an alias on the target system.

- For appointments migrated from Exchange 2007 to Microsoft 365, the acceptance date on the target will be the date/time of the migration. Also, appointment owners will see “invitation not sent” for appointments with multiple attendees.
- For Exchange-based targets, Groups are treated as Distribution Lists and cannot contain a contact with no email address. Because of this, any group members that do not have an email address on the source will not be migrated as a member of that group on an Exchange/O365 target. The contact will still migrate, it just cannot be a member of a group without an email address.
- InfoPath items are not migrated from Microsoft 365 and Exchange server.

Rules

For information about the supported types of rule's condition or action, see [Migrating Rules](#).

- For the source Exchange 2010, ODME migrates OWA Inbox rules only to the target, and:
 - Rules with the action "Delete message" will have the option **Stop processing more rules** selected on the target after migration.
- Autodiscover must be enabled on your target for successful rules migration.
- During the migration, the name of a group participating in a source rule will be converted to an SMTP email address. The address is retrieved from the mailbox list of the migration plan, and will be used in the corresponding target rule.
- Migration of rules from or to personal archives is not supported.

Delegates

- Migration of security groups as delegates is not supported for Exchange 2013 or earlier.
- For migrations from Exchange server and Microsoft 365, migration of customized set of delegate permissions is currently not supported:
 - Custom folder permissions are migrated as None (lack of any permissions) when the target delegate does not exist.
 - In case when the target delegate exists, source and target delegate permissions are merged and the predefined Roles (Editor, Author, Reviewer and None) take precedence over any Custom permission set.
 - In case when the target delegate exists and both source and target permissions are set to Custom, the target permissions will be set to None.

See [Migrating Delegate Access Permissions](#) for details.

Folder Permissions

- Migration of folder permissions for Recoverable Items is not supported.
- Migration of folder permissions from personal archive and to personal archive is not supported.

Microsoft 365

General

- If a user's Calendar is shared with people outside the organization, On Demand Migration for Email migrates shared Calendar permissions only for internal users and ignores users outside the organization.

- The **Use Modern Authentication** option is supported for connections to the Microsoft 365 Worldwide. The option is not supported for connections to the Microsoft 365 hosted in the Germany, China or US Government environments (Microsoft 365 GCC High).
- For Microsoft 365/Exchange 2010, or Microsoft 365/Exchange 2013, or Microsoft 365/Exchange 2016, or Microsoft 365/Exchange 2019 hybrid deployments, if your Microsoft 365 configuration utilizes a shared domain configuration, On Demand Migration for Email will not be able to locate your mailboxes.
- InfoPath items are not migrated from Microsoft 365 and Exchange server.
- ODME does not migrate retention policies and retention tags from one Microsoft 365 tenant to another Microsoft 365 tenant.
- ODME does not migrate some Contact fields from G Suite to Microsoft 365.
Fields that are currently supported:
 - Name
 - Job title, Company
 - Phone Numbers
 - Picture
 - Notes
 - Email Address
 - IM
 - Birthday
 - Relationship

Custom G Suite fields that cannot be migrated from G Suite to Microsoft 365:

- Phonetic Last
- Phonetic First
- URL
- Internet Call
- Custom Fields

Rules

See the **Rules** section of [Microsoft Exchange](#).

Delegates

- Migration of security groups as delegates is not supported for Exchange 2013 or earlier.
- For migrations from Exchange server and Microsoft 365, migration of customized set of delegate permissions is currently not supported:
 - Custom folder permissions are migrated as None (lack of any permissions) when the target delegate does not exist.
 - In case when the target delegate exists, source and target delegate permissions are merged and the predefined Roles (Editor, Author, Reviewer and None) take precedence over any Custom permission set.
 - In case when the target delegate exists and both source and target permissions are set to Custom, the target permissions will be set to None.

See [Migrating Delegate Access Permissions](#) for details.

Folder Permissions

- Migration of folder permissions for Recoverable Items is not supported.
- Migration of folder permissions from personal archive and to personal archive is not supported.

POP/Windows Live Hotmail

- Only content located in the source inbox is accessible and migrated.

IMAP

- Non-delivery reports migrated to exchange will not be as complete as if they were sent from exchange based client. For instance, a non-delivery report migrated from IMAP server cannot be resent by opening it and selecting Resend in Outlook.
- If an IMAP source has sent mail in a folder other than “sent items,” the target will have mail migrated to a folder of an identical name and not to the “sent items” folder in Exchange/Microsoft 365. The user can move the mail from one folder to another after migration.
- The Follow Up flag is not migrated.

G Suite



IMPORTANT: It is not required to enable IMAP for migrations from G Suite on the organization level unless you need 'Important' and 'Starred' target folders to have the same non-English localized names as the corresponding Gmail labels on the source.

- Tasks are not migrated.
- Cannot currently migrate attachments on Google Events.
- Currently, when migrating to Microsoft 365, Google Labels do not show up by default in the user's Categories list.

To have migrated Google Labels appear in the Microsoft 365 Categories list, in O365, open **manage categories...** from the **categorize** menu and select **add new category**. Then create a category that exactly matches a category that was applied to an O365 message during the migration. All messages marked with that category will take on the color applied (if any) and the category will remain on the user's list for future use.

This can also be achieved in Outlook 2010. From the **Home** tab, click the **Categorize** button and then select **All Categories**. You will see your labels that are missing with (Not in Master Category List) next to the name. Select the category, click **New**, select a color, and click **Save**.

- In G Suite to Exchange/Microsoft 365 migrations, attachments that appeared normally on the source may show up on the target as a 'winmail.dat' file. These files are actually winmail.dat files on the source as well, but G Suite automatically interprets them as their original file type. To view them on the target, users will need to use a winmail.dat viewer.
- The **Chats** label is no longer supported due to Google Chat was officially shut down (<https://support.google.com/chat/?hl=en>).
- Currently, if a G Suite user has "Make changes AND manage sharing" permissions on a secondary shared calendar, this shared calendar will be migrated, but no sharing connection is maintained between the two mailboxes, which means the shared calendar on the target will not be updated when the owner updates their own calendar. If this behavior is not desired, users need either to manually remove the shared calendars on the target after migration, or follow the steps below prior to migration to change the Sharing Permission Settings.



NOTE: ODME does not migrate primary shared calendars.

If you want to allow the migration of secondary shared calendars, which will become independent (orphaned) calendars in the target:

On an individual user basis:

1. Log in to the account whose calendar is being shared.
2. Go to Calendar > Settings (gear icon) > Settings > Calendars.
3. Click on sharing for the desired calendar.
4. Under "Share with specific people", change the Permission Settings for the user(s) to the "Make changes AND manage sharing" permission.
5. Save.

If you want to prevent the migration of secondary shared calendars, so that they can be setup natively as shared calendars in the target:

On an individual user basis:

1. Log in to the account whose calendar is being shared.
2. Go to Calendar > Settings (gear icon) > Settings > Calendars.
3. Click on sharing for the desired calendar.
4. Under "Share with specific people", change the Permission Settings for the user(s) with the "Make changes AND manage sharing" permission to any other option you want.
5. Save.

- ODME does not migrate some Contact fields from G Suite to Microsoft 365. Fields that are currently supported:

- Name
- Job title, Company
- Phone Numbers
- Picture
- Notes
- Email Address
- IM
- Birthday
- Relationship



NOTE: When migrating contacts, ODME explicitly validates the Email Address property. If the property does not contain the correct e-mail address, it will not be migrated.

Custom G Suite fields that cannot be migrated from G Suite to Microsoft 365:

- Phonetic Last
 - Phonetic First
 - URL
 - Internet Call
 - Custom Fields
- ODME does not migrate contacts that are shared from other G Suite users. For example, the user A shares some contacts with the user B. These shared contacts will not be migrated when you migrate the user B to the target, and they will not be automatically shared to the user B even if you migrate the user A to the target as well.

Zimbra

- For Zimbra 8: ODME cannot migrate Zimbra contact group members which contain an email address only.
- Migration of mailboxes from Zimbra 6 is not supported.
- Shared and search folders are not migrated
- Only the first IM address is migrated for each Zimbra contact. Additional IM addresses, if any, are not migrated.
- The "other" URL for Zimbra contacts is not migrated.
- Items contained Zimbra Briefcases are not migrated.
- ODME does not correctly map contact File-As field "Company (First Last)".
- Tags applied to mail, contacts, and tasks are not migrated.

- Certain mail items that can be defined in the Zimbra Outlook connector are not supported in the Zimbra UI and as a result cannot be migrated. These mail items include, but are not limited to, the recurrence information for tasks and completed date fields.
- ODME cannot migrate Zimbra item fields that do not exist on the target. For example, when migrating to O365, the location field on tasks will not migrate as there is no comparable field for tasks in O365.
- ODME support migrating a total of 3 email addresses per contact to an Exchange target mailbox. Zimbra has fields for 5 addresses per contact.
- ODME cannot migrate to an Exchange target group members in Zimbra that do not have contacts with defined email addresses. This is because Exchange requires each member of a distribution list to have an email address, while group members in Zimbra are not required to have an email address.
- ODME does not migrate message tags.
- ODME does not support migration of excluded dates in recurring meetings. For example, if a meeting is scheduled for "every Friday, except 2015-05-01", then it will be migrated as recurring "every Friday" - the excluded date will not be migrated to the target server.

Known Issues

For the list of known issues, please refer <http://documents.quest.com/on-demand-migration-for-email/release-notes/known-issues>.

Running Migration

After you have connected to your source and target email services, imported the mailboxes you want to migrate, and optionally, selected what mailbox items to exclude from the migration, you are ready to run the migration.

CAUTION: Before starting a migration, be aware of the following:

Each mailbox in a source email service can be migrated successfully a total of 10 times with a maximum extraction limit of 500 GB across all migrations. This includes mailboxes that have 10 different date filters. This limit applies even if the 10 migrations do not migrate the same message more than once.

NOTE: Migration from Microsoft 365 to Microsoft 365

If you switch your source domain and MX record to the target domain before the migration is completed, ODME cannot connect to the source mailboxes using old SMTP addresses, and so you need to add mailbox pairs with the new source SMTP addresses to the migration plan. In this case, an additional ODME license is consumed for each newly added mailbox pair except the following scenario:

1. Migration session N: **user@company.com** --> user@target.onmicrosoft.com or any other user's target SMTP address
2. "**company.com**" domain name is transferred to the target.
3. Migration session N+1: user@source.onmicrosoft.com or any other user's source SMTP address --> **user@company.com**

In this scenario, an extra-license will not be consumed on the step 3 despite the change of the source user SMTP address.

To run a migration:

1. Open the **Dashboard** and select the migration plan you want to run.
2. Open the **Migrate** tab.

The **Migrate** tab lists all the mailboxes that have been imported (up to 5000).

3. Optionally, make any changes to the migration settings as summarized in the in **Dashboard** or in the Migration Checklist of the **Migrate** tab.

The migration plans in the **Dashboard** and the Migration Checklist in the **Migrate** tab display links pointing to the **Connections**, **Mailboxes** and **Options** tabs. Click a link to return to the tab and make the changes you want.

i NOTE: The Migration Checklist displays the IP addresses of the ODME web services used to run the migration (which are distinct from the web services used to validate connections to the source and target email services). The system administrator should verify that no firewall rules exist that will prevent the ODME web services identified by the IP addresses from running a migration.

4. Click **Start Migration**.

During the migration, each mailbox displays what percentage of the mailbox has been migrated. At the bottom a colored progress bar indicates the overall status of the migration.

When the migration is complete, the number of mailboxes that were successfully migrated and the number that were interrupted or failed to migrate are displayed in the Migration Status section

For each mailbox, ODME also displays:

- The number of errors encountered during the migration

i NOTE: The number of errors reported for a mailbox's migration displayed in the Migrate tab may be lower than the number of error messages reported in the mailbox's migration logs. This is because certain errors counted in a mailbox's migration may be the result of several related errors reported in the migration logs. For example, ODME may fail to migrate a mailbox item for a combination of reasons, each one resulting in a separate error reported in the migration log. For the mailbox's migration, however, this failure is counted as one error.

- The estimated number of items (messages, contacts, distribution lists, appointments, and tasks) the mailbox contains
- The total number of mailbox items that were successfully migrated as well as the percentage (a successful migration is where 90% or more of the items migrated)

i NOTE: For migrations from a G Suite source, the Migration Status section indicates whether ODME has paused data extraction from Google due to hitting the data extraction limit or because Google throttled the connections. The Mailbox column shows when the migration will be restarted. There is also a tooltip to the right of the 'auto-resume' message explaining why the migration has been paused and that it will resume after 24 hours.

5. Optionally, to view migration log entries for a single mailbox, click the **View Log** link for that mailbox.

i NOTE: For migrations from a G Suite source, log messages indicate whether ODME paused its data download from Google. The messages indicate why ODME is pausing, how many items (contacts, calendar and email) ODME has migrated so far, and when ODME will re-start the migration. The messages also indicate if ODME paused due to hitting the data extraction limit or because Google throttled the connections.

6. If some issues or unexpected errors occurred during the mailbox migration, the mailbox will be marked as "Interrupted" or "Failed". To restart the migration process for one or several "Interrupted" or "Failed" mailboxes, you can select the checkbox next to the mailbox and click the Restart Selected button.

Migration Concurrency

Though the number of mailboxes that can be migrated by the product concurrently is virtually unlimited, during migration process you can encounter some limitations outside the product.

In some cases, your source or target environment may not be able to keep up too many mailboxes being migrated simultaneously while still being responsive and available to their users. To avoid this problem you can limit the number of mailboxes migrated concurrently in a migration plan. Please see [Limiting Concurrent Migrations](#) for details.

Another limit you can hit is the maximum number of PowerShell connections. The product uses PowerShell to configure the forwarding options (**Forwarding new items as they arrive** and **Turn off existing forwarding**) for Exchange / Microsoft 365. If a migration plan has one or more of these options enabled for Exchange / Microsoft 365, when it starts, it opens a PowerShell connection to configure the enabled options. If you have too many plans configured under the same administrative account and they start approximately at the same time, you can hit the 'PowerShellMaxConcurrency' throttling limit for this account. In this case, the plan hit that limit will be rescheduled to start later, when a PowerShell connection is available, and the corresponding message will be displayed in the plan. Please consider to specify a different administrative account for paused plans if you need them to start immediately. Note that the connections under the same account may be done outside the product.

Re-migration

If you rerun a migration from Exchange 2010, 2013, 2016, 2019 or Microsoft 365, On Demand Migration for Email re-migrates mail, calendar, contact, task, and sticky note items that have changed in the source mailbox to the target mailbox. Also, calendar items that have been removed from the source mailbox will be removed from the target mailbox.


Post Migration

Viewing Migration Reports

On Demand Migration for Email provides the following reports:

- An Executive Summary report which shows migration statistics both at the organization level and mailbox level.
- A general Migration Summary report
- A Billing Summary report which shows the number of billable mailbox migrations in a particular date range
- A Migration Details report which includes the event log for each migration
- A Per Mailbox Statistics report which shows a list of executed migration plans and their statuses

These reports are accessed by clicking **Reports** in the lower right corner of the **Dashboard**.

 **NOTE:** For all types of reports, the value of "Tasks/Notes" shows the sum of migrated Task and Note items.

You can download the following migration reports in the CSV format directly from the **Dashboard**:

- A Per Plan Migration report which shows the same data as the **Migrate** tab. To generate this report, click **Get Report** next to the plan on the **Dashboard**.
- A Per Company Migration report aggregates the information from all the plans for the current company. To generate this report, click the **All Plans Report** button in the lower-right corner of the **Dashboard**.

Executive Summary Report

The Executive Summary report shows migration statistics both at the migration plan level and the mailbox level. You can generate the report for individual migration plans or for all migration plans at once.

The **Overview** tab shows a pie chart representing the migration status percentages for all the mailboxes in the selected plan or plans. The total number of mailboxes in each status is displayed beneath the chart.

The **Mailbox Details** tab shows bar graphs representing the migration status of individual mailboxes. For each mailbox, the total number of successfully migrated items is coded green, while the total number of items that failed to migrate is coded red. By default, the **Mailbox Details** tab shows all the mailboxes in the selected plan or plans. To filter the results, select only the migration status options you want and click **Filter**.

Migration statuses include:

- Migrated
- Migrated with Errors
- Pending
- In Process

Migration Summary Report

The Migration Summary report displays the following information:

- The date of the first successful migration
- The total number of successfully migrated mailboxes
- The total amount of migrated data in MB
- The total number of migrated mailbox items (messages, contacts, distribution lists, appointments, and tasks/notes)

Billing Summary Report

The Billing Summary report shows information regarding all the billable mailbox migrations in a particular date range (the last 30 days shown by default). Use the calendar controls to change the date range.

The Billing Summary report includes the total number of billable migrations, and of these, the number billed to a “pay-as-you-go” plan (deprecated) and the number billed using pre-paid licenses (if any).

i **NOTE:** If you purchased any pre-paid licenses, the total number of pre-paid licenses in use is shown in the top right corner of the report window, as well as the number of licenses remaining. If you have zero licenses remaining, click the **Buy More** link to purchase additional licenses.

For each billable migration, the Billing Summary shows:

- The migration plan
- The source mailbox
- The migration status
- Payment type: Pay-As-You-Go (deprecated) or Pre-Paid
- Completion time

i **NOTE:** The payment type “Unknown” is shown for migrations that were completed prior to ODME 1.6.2.

To download the report to a CSV file that can be opened in Excel, click **Download CSV File** in the bottom right corner.

Migration Details Report

The Migration Details report displays information about each migration that completed during a particular month, including the completion date and time, the source and target mailbox, and the result (a successful migration is where 90% or more of the items migrated successfully).

To run a Migration Details report:

1. Select the **Migration Details** option.
2. Select the month in which the migrations you want to view completed.

For each migration, Migration Details reports also include a link to download the migration audit log entry to a text file.

3. Optionally, click the **Download** link for a particular migration to view the audit log.

Additional information about each migration in a Migration Details report is available as a downloadable csv file.

4. Optionally, click **Download Additional Details** to view additional information about each migration.

Per Mailbox Statistics Report

The Per Mailbox Statistics report shows a list of migration plans that had been executed at least once and their final migration statuses:

- Stopped
- Stopped With Errors
- Completed
- Completed With Errors

Notify and Train Users

After successfully migrating mailboxes, you should notify users of the migration and provide information on how to access the new mail system. This step is performed outside of On Demand Migration for Email and may include training users on the new system as needed.

Third Party Assessments and Certifications

ODME has obtained the following certifications:

- ISO/IEC 27001 Information technology — Security techniques — Information security management systems — Requirements : **C710-ISMS222-07-19**, valid until **2022-07-29**.
- ISO/IEC 27017 Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services: **C711-ITCS2-07-19**, valid until **2022-07-29**.
- ISO/IEC 27018 Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors: **C712-ITPII2-07-19**, valid until **2022-07-29**.

Glossary

This glossary provides definitions of many of the terms commonly used in On Demand Migration for Email.

Admin Credentials

The login information (username/password) of an account that has the required rights to access all mailbox data. The rights assigned to this account will vary based on the **Source Email Service** or **Target Email Service** configured for the migration.

Email Service

Collection of settings that define a mailbox store. This may include host name, port and protocol information, but in some cases it is only necessary to define the type of service (i.e. G Suite).

Alternatives: Environment, Connection, Service, Migration Path

Item

An object within a mailbox that may be migrated. This is typically one of an Email, Contact, Appointment, Distribution List.

Migration

A single pass through a Source Mailbox moving all the Items selected to migrate to the Target Mailbox.

Migration Job

Mapping between a **Source Mailbox** and a **Target Mailbox**.

Migration Options

Collection of settings that define the data to be migrated. This includes item type (Email, Contacts, Calendar, Tasks), filters (migrate items received before or after specified date, exclude folders, etc.), and may be extended to cover additional settings like custom properties on mail items.

Alternatives: Migration Items, Filters

Migration Plan

A configuration, and collection of users, defining a migration.

Source Email Service

The email service platform from which mailbox items are migrated.

Source Mailbox

Mailbox that has been selected to migrate to the **Target Email Service**.

Successful Migration

Any Migration where 90% or more of the items are migrated successfully.

Target Email Service

The future location for mailboxes after they are migrated, either Microsoft 365 or Exchange 2010.

Target Mailbox

Mailbox that exists on the **Target Email Service** and will hold all of the data from the **Source Mailbox** after the migration is complete.

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 Microsoft 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