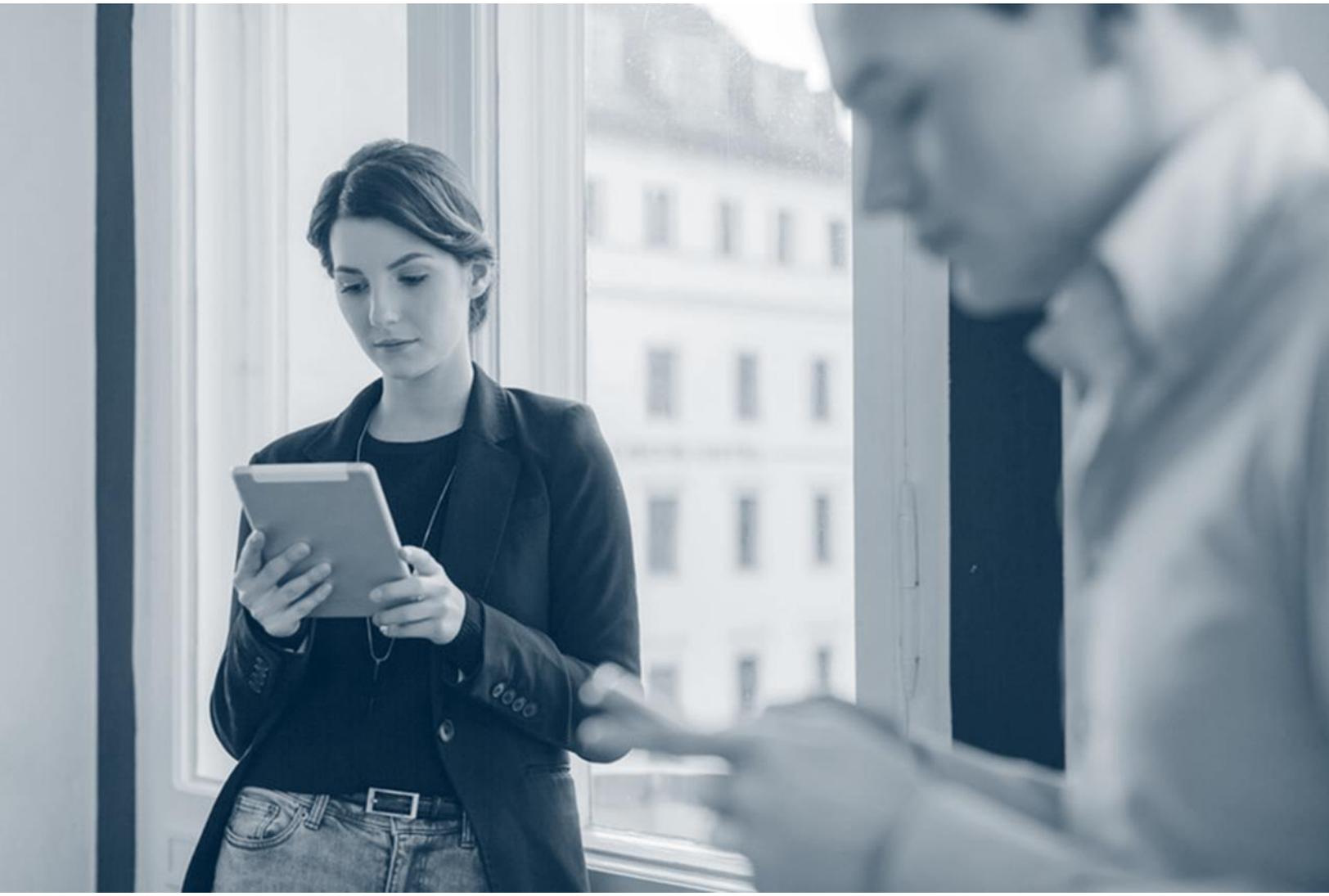




# Exchange Online Custom Configuration

Version 11 Feature Release 22

Wednesday, February 17, 2021



# Contents

Custom Configuration for Exchange Online.....	3
Modern Authentication .....	3
Registering Exchange Online with Azure .....	3
Providing Service Accounts Access to Mailboxes Exchange Online.....	6

# Custom Configuration for Exchange Online

The custom configuration method is a manual process that requires the following actions and information:

- To set up modern authentication, complete these tasks:
  - Register the Azure app with Azure.
  - Provide service accounts access to Exchange Online shell.
- Obtain the Azure application ID, secret application key value, and Azure directory ID. For instructions about locating this information in the Azure Portal, in the Microsoft documentation, see [Get tenant and app ID values for signing in](https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal#get-tenant-and-app-id-values-for-signing-in) in <https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal#get-tenant-and-app-id-values-for-signing-in>.
- Obtain the Exchange Online service account log-on credentials.

## Modern Authentication

Modern authentication is a method of identity management that offers more secure user authentication and authorization.

## Registering Exchange Online with Azure

Register the Azure app with Microsoft Azure Active Directory (AD).

When you finish registering the app, record the Application ID and Directory ID. When you finish creating the client secret, record it. You need to enter these values when you add the app to the Commvault software.

To improve performance and to minimize throttling, you can register multiple apps.

For an Exchange Online app that has 5,000 mailboxes, register 5 apps. Every time an additional 1,000 mailboxes are added, register 1 additional app.

Disclaimer: This procedure is performed using the Microsoft Azure Active Directory (Azure AD) Web application. The Azure AD application is subject to change without notice. Consult Microsoft documentation, for example "Azure Active Directory Documentation" (<https://docs.microsoft.com/en-us/azure/active-directory/> (<https://docs.microsoft.com/en-us/azure/active-directory/>)).

## Log On to the Azure Portal as the Global Administrator

1. Log on to the Azure portal (<https://portal.azure.com/>) using your global administrator account.
2. Go to Azure Active Directory.

## Register Exchange Online in the Azure Portal

1. In the navigation pane, click **App registrations**.
2. Click **New registration**.
3. In the **Name** box, enter a name for the app.
4. Under **Supported account types**, select **Accounts in this organizational directory only (<office\_365\_tenant\_prefix> - Single tenant)**.
5. **Optional:** To verify the status of the app and to authorize the app from the Command Center, under **Redirect URI**, enter the Command Center URL.

For example, enter

**`https://Command_Center_name.domainname.com/adminconsole`**.

6. Click **Register**.
7. Copy and paste the following values in a file or other document that you can access later:
  - **Application ID**
  - **Directory ID**

You will enter these values in the Commvault software when you create the Office 365 app.

## Request and Grant Permissions for Azure APIs for Azure Apps

1. In the navigation pane, click **API permissions**.
2. Click **Add a permission**.
3. Click **Microsoft Graph** and complete the following steps:
  - a. Click **Application permissions**.
  - b. Select the following permissions:
    - Directory: **Directory.Read.All**
    - Group: **Group.ReadWrite.All**
  - c. Click **Add permissions**.
4. On the app **API permissions** page, click **Add a permission**.
5. Click **APIs my organization uses** and complete the following steps:
  - a. On the search bar, type **Office 365 Exchange Online**.
  - b. Select **Office 365 Exchange Online**, and then click **Application permissions**.
  - c. Select **full\_access\_as\_app**.
  - d. Click **Add permissions**.
6. On the app **API permissions** page, click **Grant admin consent for *tenant\_name***.

## Create a Client Secret for the Office 365 App

1. In the navigation pane, click **Certificates & secrets**.
2. Click **New client secret**.
3. Enter a description, and then select **Never expire**.
4. Click **Add**.
5. Copy and paste the client secret value in a file or other document that you can access later.

You will enter this value in the Commvault software when you create the Office 365 app.

## Providing Service Accounts Access to Mailboxes Exchange Online

You must configure the Exchange Online service account to discover, archive, clean up, and restore data for user mailboxes, group mailboxes, and all public folders.

### Before You Begin

- Exchange Online service account, must meet the following requirements:
  - MFA must be disabled for the service account.

### Procedure

1. Log on to the Azure portal <https://portal.azure.com/> using your global administrator account.
2. Go to Azure Active Directory and create a user and disable MFA for the user. For more information, see [Add or delete users using Azure Active Directory](https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/add-users-azure-active-directory) <https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/add-users-azure-active-directory>.
3. Go to Office 365 Exchange Admin Center <https://outlook.office365.com/ecp>, create a custom role with the **View-Only Recipients** permission, and then add the user to this role.
4. You can convert the user into a mailbox or shared mailbox to protect Office 365 group mailboxes for which there is no valid owner or member.

©1999–2021 Commvault Systems, Inc. All rights reserved. Commvault, Commvault and logo, the "C hexagon" logo, Commvault Systems, Commvault HyperScale, ScaleProtect, Commvault OnePass, Unified Data Management, Quick Recovery, QR, CommNet, GridStor, Vault Tracker, InnerVault, Quick Snap, QSnap, IntelliSnap, Recovery Director, CommServe, CommCell, APSS, Commvault Edge, Commvault GO, Commvault Advantage, Commvault Complete, Commvault Activate, Commvault Orchestrate, Commvault Command Center, Hedvig, Universal Data Plane, the "Cube" logo, Metallic, the "M Wave" logo, and CommValue are trademarks or registered trademarks of Commvault Systems, Inc. All other third party brands, products, service names, trademarks, or registered service marks are the property of and used to identify the products or services of their respective owners. All specification are subject to change without notice.

The development release and timing of future product releases remains at Commvault's sole discretion. Commvault is providing the following information in accordance with Commvault's standard product communication policies. Any resulting features, functionality, and enhancements or timing of release of such features, functionality, and enhancements are at the sole discretion of Commvault and may be modified without notice. All product roadmap or other similar information does not represent a commitment to deliver any material, code, or functionality, and should not be relied upon in making a purchasing decision.

Visit the [Commvault Documentation](#) website for complete documentation of Commvault products.



[COMMVault.COM](https://www.commvault.com) | 888.746.3849 | [GET-INFO@COMMVault.COM](mailto:GET-INFO@COMMVault.COM)