

## ITAS Graph Service Set Up

Hivedome increased support for the ITAS Graph WebService in Trader Desktop version 8.17.0

### Overview

The ITAS Graph Service (API) was introduced in version 8.15.0 primarily, but not exclusively, to act as a gateway to Microsoft 365 services such as Mail and Teams Chat. The initial integration supported the migration of the security procedures required by ITAS DocmanServer. Version 8.17.0 introduces support for SharePoint document storage.

The steps included in this document will enable ITAS customers to configure access for ITAS DocmanServer to nominated mailboxes through their Azure Portal and configure permissions for Teams and SharePoint.

### Requirements

To ensure that the ITAS DocmanServer, Teams or SharePoint can be accessed by the Graph Service, the following actions should be taken:

1. Sites wishing to use these features will need to subscribe to the Graph Service, which will incur a monthly charge that will be applied to your regular ITAS Licence. Please contact Hivedome to discuss this upgrade. \*
2. Complete the Microsoft Azure set up and provide Hivedome with the configuration values detailed in the Configuration Values section of this document below.
3. Contact Hivedome to arrange the deployment of Trader Desktop version 8.17.0 to your server/s.

*\*Please note this does not apply to Enterprise Services subscribers as the MS Graph Service will be included in this package.*

# Microsoft Azure Set Up

## Step 1 - Register an application

- Create application in Azure Portal – see Microsoft [documentation](#)

The screenshot shows the 'Essentials' section of an application registration in the Azure Portal. It includes the following information:

- Display name: [TestAppDoc](#)
- Application (client) ID: 9ba49926-5668-4111-8282-9c0a441a1f63
- Object ID: 2dfc8afe-99bf-4969-9a8d-74ea1b5e01c9
- Directory (tenant) ID: 4acc0709-8f3c-45f3-b048-1b0e6ec2b449
- Supported account types: [My organization only](#)
- Client credentials: [Add a certificate or secret](#)
- Redirect URIs: [Add a Redirect URI](#)
- Application ID URI: [Add an Application ID URI](#)
- Managed application in L...: [TestAppDoc](#)

- Create client secret
- Add [permissions](#) to application

| Microsoft Graph |                     |  |             |               |                  |
|-----------------|---------------------|--|-------------|---------------|------------------|
| Microsoft Graph | Chat.ReadWrite      | Read and write user chat messages            | Delegated   | Admin consent | An administrator |
| Microsoft Graph | ChannelMessage.Send | Send channel messages                        | Delegated   | Admin consent | An administrator |
| Microsoft Graph | Chat.Create         | Create chats                                 | Delegated   | Admin consent | An administrator |
| Microsoft Graph | Mail.ReadWrite      | Read and write mail in all mailboxes         | Application | Admin consent | An administrator |
| Microsoft Graph | Sites.Read.All      | Read items in all site collections           | Application | Admin consent | An administrator |
| Microsoft Graph | Sites.ReadWrite.All | Read and write items in all site collections | Application | Admin consent | An administrator |
| Microsoft Graph | Files.ReadWrite.All | Read and write files in all site collections | Application | Admin consent | An administrator |
| Microsoft Graph | User.Read.All       | Read all users' full profiles                | Application | Admin consent | An administrator |
| Microsoft Graph | Files.Read.All      | Read files in all site collections           | Application | Admin consent | An administrator |

### Default (Everything)

- User.Read.All

### Teams (Notification)

- ChannelMessage.Send
- Chat.Create
- Chat.ReadWrite

### SharePoint (Document)

- Files.Read.All
- Files.ReadWrite.All
- Sites.Read.All
- Sites.ReadWrite.All

### Mail (DOCMAN)

- Mail.ReadWrite

*Note that additional permissions may be requested in future as we add more modules/functionalities to the service.*

## Step 1 - Define Application Policy

Create an [Application Policy](#) to restrict access from the application to specific shared mailboxes (e.g. Docman-Maildrops@test.com) instead of all mailboxes in the organisation.

First setup an Exchange mail group and add its members (shared mailboxes):

The screenshot shows the 'Exchange admin center' interface. On the left is a navigation pane with options like Home, Recipients, Mailboxes, Groups, Resources, Contacts, Mail flow, Roles, Migration, Reports, Insights, and Organization. The main area is titled 'Groups > Add a group'. A progress indicator shows 'Group type' (checked), 'Basics' (selected), 'Settings', and 'Finish'. The 'Basics' section is active, showing a form to 'Set up the basics'. The 'Name' field contains 'Docman-CS01-Maildrops@HDMCS.com'. The 'Description' field contains 'Graph Powershell Script App is restricted to access mailboxes in this group'.

The screenshot shows the 'Exchange admin center' 'Groups' page. The left navigation pane is the same as in the previous screenshot. The main area shows 'Groups' with tabs for 'Microsoft 365', 'Distribution list', 'Mail-enabled security', and 'Dynamic distribution list'. The 'Mail-enabled security' tab is selected. Below the tabs are action buttons: 'Add a group', 'Export', 'Refresh', 'Edit name and description', 'Edit email address', and 'Delete group'. A table lists the groups:

| Group name  | Group email                     | Sync status | Created on                | Choose columns |
|---|---------------------------------|-------------|---------------------------|----------------|
| <input checked="" type="checkbox"/> Docman-CS01-Maildrops@HDMCS.com | Docman-CS01-Maildrops@hdmcs.com |             | February 18, 2022, 3:00 I |                |

On the right, a sidebar shows details for the selected group: 'Docman-CS01-Maildrops@H...', 'Mail-enabled security group', '1 owner', '1 member'. It includes sections for 'Owners (1)' (listing Matt Hardy) and 'Members (1)' (listing Docman Test).

This policy will also need to be created on you application server/s using the below PowerShell script, ensuring the highlighted details are changed appropriately:

```
New-ApplicationAccessPolicy -AppId 60dd33c3-9eea-4bbb-922a-17b7b69bf0a4 -PolicyScopeGroupId Docman-CS01-Maildrops@hdmcs.com -AccessRight RestrictAccess -Description "Restrict this app to members of distribution group Docman-CS01-Maildrops."
```

```
RunspaceId      : f8ce9ffe-ec93-4725-9d2f-b9ade6f7485f
ScopeName       : Docman-CS01-Maildrops@HDMCS.com
ScopeIdentity   : Docman-CS01-Maildrops@HDMCS.com20220218150017
Identity        : be023abd-3c18-47e7-886f-de85b5cb1449\60dd33c3-9eea-4bbb-922a-17b7b69bf0a4:s-1-5-21-2103643036-1067027473-1901050440-54782643;abb2dca4-44f6-46d1-8aa5-5009626c20c5
AppId           : 60dd33c3-9eea-4bbb-922a-17b7b69bf0a4
ScopeIdentityRaw : s-1-5-21-2103643036-1067027473-1901050440-54782643;abb2dca4-44f6-46d1-8aa5-5009626c20c5
Description     : Restrict this app to members of distribution group Docman-CS01-Maildrops.
AccessRight     : RestrictAccess
ShardType       : All
IsValid        : True
ObjectState     : Unchanged
```

## Configuration Values

Once the Microsoft setup is complete, please supply the following configuration values to HIVEDOME for inclusion in your Trader Desktop configuration:

- I. **Application (client) ID** [see Home->App registrations]
- II. **Directory (tenant) ID** [see Home->App registrations]
- III. **Client Credentials** [Client Secret created in Step 2 of the Setup]
- IV. **Delegate credentials** (username & password). This should be an account in the same tenant as the application. It is used for delegate access type permissions e.g. the 'from' account when sending channel messages.

*For more information or assistance with this set up, please contact your ITAS representative or support team.*