

Notice to introduce ITAS Graph Service

Hivedome will be introducing support for the new ITAS Graph Webservice, included in Trader Desktop version 8.15.0

Background

Following the announcement by Microsoft in 2021 that support for access to Exchange Web Services (EWS) using Basic Authentication would be terminated in October 2022, we sent Notification in May this year that this would lead to changes with the ITAS DocmanServer Service.

'ITAS DocmanServer (Windows Service) is used by a number of customers to monitor Exchange mailboxes that receive emails containing attachments that need to be processed and brought into the ITAS Document Management library.

It was initially developed as a free add-on service and provided as a simple mechanism for monitoring 1 or 2 mailboxes. Customers adopted it for various reasons but primarily to allow their counterparts to send documents which could be automatically extracted and stored, and then manually indexed through DOCMAN.

Over time it has taken on other responsibilities and the number of mailboxes being 'monitored' has vastly increased.

Following the above announcement, we have had to make a decision about the viability of the service itself.

Investment is required to adopt "Modern authentication" in order for the service to continue to be developed and supported.

Over the last few years, we have invested heavily in Microsoft Graph to enable developers to access the rich data available in Microsoft 365. Microsoft Graph, along with OAuth 2.0, provides increased security and seamless integration with other Microsoft cloud services.

In August 2018, we announced that we were no longer going to actively invest in Exchange Web Services (EWS) APIs for Exchange Online. We also gave

Research undertaken last year demonstrated that as well as providing a more secure method for accessing Exchange Online, Microsoft Graph offers other opportunities to tap into the M365 technology stack.'

Overview

The ITAS Graph Service (API) has been developed primarily, but not exclusively, to act as a gateway to Microsoft 365 services such as Mail and Teams Chat. The initial integration supports the migration of the security procedures required by ITAS DocmanServer, further capabilities will be introduced in a future release.

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

Requirements

To ensure that the ITAS DocmanServer can continue to work as expected prior to Microsoft deprecating Basic Authentication (BA), the following actions should be taken immediately:

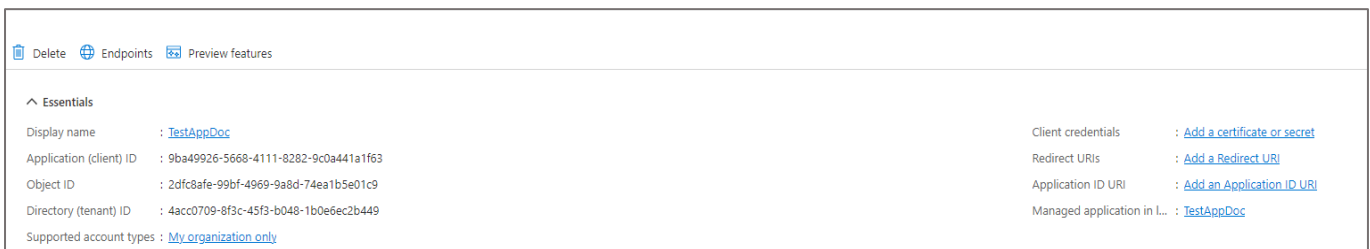
1. As suggested in our previous communication, sites using DocmanServer will need to subscribe to the new MS Graph Service which will incur a monthly charge that will be applied to your regular ITAS Licence. Please contact Hivedome to discuss this upgrade. *
2. Complete the Microsoft Azure set up and 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 8.15.0 to your server/s.

**Please note this does not apply to Enterprise Services subscribers as the MS Graph Adapter 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 details:

- 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 I...: TestAppDoc

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

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (5)				
ChannelMessage.Send	Delegated	Send channel messages	No	✔ Granted for HIVEDOME LTD
Chat.Create	Delegated	Create chats	No	✔ Granted for HIVEDOME LTD
Chat.ReadWrite	Delegated	Read and write user chat messages	No	✔ Granted for HIVEDOME LTD
Mail.ReadWrite	Application	Read and write mail in all mailboxes	Yes	✔ Granted for HIVEDOME LTD
User.Read.All	Application	Read all users' full profiles	Yes	✔ Granted for HIVEDOME LTD

- a) Application Type
 - I. Mail.ReadWrite
 - II. User.Read.All
- b) Delegated Type
 - I. ChannelMessage.Send
 - II. Chat.Create
 - III. Chat.ReadWrite

- Grant admin consent to permissions

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 'Set up the basics' section contains a 'Name *' field with the value 'Docman-CS01-Maildrops@HDMCS.com' and a 'Description' field with the text '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'. 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 for the selected group 'Docman-CS01-Maildrops@H...' shows it is a 'Mail-enabled security group' with 1 owner and 1 member. The 'Members' tab is active, listing 'Matt Hardy' (owner) and 'Docman Test' (member).

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 install, please contact your ITAS representative or support team.