Configure TM Master to use the "OAuth2" Protocol to send e-mails.

Contents

Configure TM Master to use the "OAuth2" Protocol to send e-mails.	1
Introduction	1
How to configure the TM Master V2 mail settings to use the OAuth2 protocol	1
How to Configure TM Exchange to use the OAuth2 protocol?	3
Register your TM Master with your Azure AD	6
How to find the details required to grant TM Master access to download?	10
Find the "Tennant ID" or <oranization_id></oranization_id>	10
Find the <application_id> and the <object_id></object_id></application_id>	11
How to grant TM Master (TM Exchange) access to download emails from an account	12

Introduction

1st of October 2022 Microsoft Exchange Online stopped supporting basic authentication, and will require all connections to use more secure protocols such as the one called "OAuth2"

For more details on this please refer to : <u>https://docs.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/deprecation-of-basic-authentication-exchange-online</u>

All our clients who are using "MS Exchange Online" to send emails from TM Master and or for replication (TM Exchange) needs to update TM Master and re-configure the mail settings in TM Master and TM Exchange, to avoid replication to stop.

Please note that example data provided in this document may not always apply to your environment. We have provided details, which are excerpts of the Microsoft guide (ref link below), on how to configure Microsoft Azure side ,to enable TM Master to send and receive emails using the OAuth2 protocol. If something is found lacking in this description, please refer to the Microsoft own guides and descriptions. <u>https://docs.microsoft.com/en-us/exchange/client-developer/legacy-protocols/how-to-authenticate-an-imap-pop-smtp-application-by-using-oauth</u>

Please contact your TM Azure personnel your Office365 partner\provider for additional support, relating to your Office365/Azure environment.

How to configure the TM Master V2 mail settings to use the OAuth2 protocol. The TM Master v2 mail settings are used to send emails such as

- Request for quotations
- Order e-mails.
- Reminder e-mails

• Various "Send as E-mail" features found in HSEQ modules and the Voyage module.

Pre-requisite:

Make sure the TM Master V2 client version number is:

- For DB version 662: 2.662.8271.xxxx or higher
- For DB version 664: 2.664.8271.xxxx or higher
- For DB version 665: 2.665.8271.xxxx or higher
- 1. Click [System] \rightarrow [Settings] \rightarrow "Mail Settings" tab

2022-08 TM Master v2 (v.2.662 - 2022-08	8-24)			\square	- 🗆 ×
<u>File T</u> ools <u>H</u> elp					
🔚 Save					
e	Settings				System Settings
Ship ¥	General Mail settings Replication	Job settings Order settings Backup settings Incident setting	gs Number Formats	Documents Time sheet settings Mandatory Fields	
Inventory ¥	SMTP Settings				
Movable Assets ¥			Basic Auth OAu		
Maintenance ¥	SMTP server			Use OAuth2	
Crew ×	SMTP port		Token URL: Scope:		
Slop Chest & Accounting *	entri per	SMTP Enable SSL	User Name:		Use Address From User
			ClientID:		
Voyage ¥			Client Secret:		
Docking ¥					
Purchasing ¥	Additional Settings		SMTP Test Fund	ction	
HSEQ ¥	Domain name for user mail (restricted to):	Edit	Sender:	test@teromarine.com	
Document Handling ¥	TmMv2 system mail:		Receiver:	test@teromarine.com	
System's Place ¥	Internal mail receiver V2 errors:			Test SMTP	
Tools ¥	Users must use Outlook				
Administration ¥					
System *					
Settings					
Mark Import and export					
TM Exchange Client					
Log					
System Settings			Last service loop	p: 00:00:00 Administrator, logged on to DB - TM-CA	TO-LAP\TEROMARINE\v2.662-DEV

2. Enter the new mail server details

SMTP Settings		Basic Auth OAuth	1	
SMTP server IP	https://graph.microsoft.com/v1.0/users/example@er		Use 0Auth2	
SMTP port	0	Token URL:	https://login.microsoftonline.com/TenantID/oa	auth2/v2.0/token
SMTP Enable SSL		Scope:	https://graph.microsoft.com/.default	
		User Name:	example@email.com	Use Address From User
		ClientID:	Client ID	
		Client Secret:		

a. SMTP Server: Enter the SMTP server address

The address path may look something like this:

example https://graph.microsoft.com/v1.0/users/example@email.com/sendMail The email in the example above (<u>example@email.com</u>) should be replaced with the email address you have configured for this purpose. Alternatively, the address can be replaced with "{0}" in which case TM Master will try to use the e-mail address registered to the current user when sending e-mails. If user email is not found it will default to the e-mail address entered as "username" in the OAuth2 settings. Example: https://graph.microsoft.com/v1.0/users/{0}/sendMail

- b. SMTP Port: This can be ignored when using OAuth2
- c. SMTP Enable SSL: Tick this check box, SSL should be enabled
- 3. Click the **"OAuth2" tab** in the tab control to the left of the server details. The "Basic Auth" tab can be ignored.
- 4. Enter the following required login details.
 - a. Use OAuth2: Tick this check box
 - b. Token URL: Enter the token URL to your mail server: It may look like this: https://login.microsoftonline.com/TenantID/oauth2/v2.0/token (Replace "TenantID" with the Tenant ID from your Azure environment) For More details on how to get the token can be found here:
 - c. Scope: Enter the full scope: https://graph.microsoft.com/.default
 - d. User Name: Enter the user name (email address) for the account to be used when sending emails from the system. It will also serve as a default address in case user trying to send an email from the system does not have a registered valid address (ref: <u>SMTP Server setting</u>)
 - e. Use Address from User: Tick this if you want each user sending emails to use their own email address (the one registered on their TM Master user), when sending. (Will require the use of the variable "{0}" in the SMTP address. (ref: <u>SMTP Server</u> setting)
 - f. **Client ID:** Enter the "Application (client) ID". This should be the ID Azure assigned to TM Master when you <u>registered the application</u> with the Microsoft identity platform.
 - g. Client Secret: Enter the client secret for the client ID
- 5. Once all details are entered, it is possible to test if TM Master can send e-mails using these settings. By using the SMTP Test function. This can be done in the following manner:

Sender:	test@teromarine.com	
Receiver:	test@teromarine.com	
	_	
	Test SMTP	

- a. **Sender:** Enter an e-mail address that should be allowed to send email from the system.
- b. Receiver: Enter valid email address
- c. Click the [Test SMTP] button

How to Configure TM Exchange to use the OAuth2 protocol?

Pre-requisite:

Make sure the TM Master V2 client version number is:

- For DB version 662: 2.662.8271.xxxx or higher
- For DB version 664: 2.664.8271.xxxx or higher
- For DB version 665: 2.665.8271.xxxx or higher

Make sure the TM Master V2 Server Service version number is:

- For DB version 662: 2.662.8271.xxxx or higher
- For DB version 664: 2.664.8271.xxxxx or higher
- For DB version 665: 2.665.8271.xxxx or higher
- 1. If the client or the server service has a lower version number than the one specified above, you will need to upgrade them, to at least the ones specified above or higher.
- 2. Click [System] \rightarrow [TM Exchange Client] \rightarrow "Settings" tab

2 TM Master v2 (v.2.662 - 2022-04	18-24) — 🗆	\times
<u>F</u> ile <u>T</u> ools <u>H</u> elp		
🖹 🗙		
e	📉 TM Exchange Client	
Ship ¥	Log Rules Settings	
Inventory ¥	Save Test settings	^^
Movable Assets ¥	Default file path	
Maintenance ¥	Working area	
Crew ¥	File handling	
Slop Chest & Accounting >	lo Interval 60 minutes ◯ Time 00:00 ≑	
Voyage ¥	Automatically unpack received zip files Max filesize 0 KB (set to 0 if you do not need a file size limit)	
Docking ¥	SMTP Settings	
Purchasing ¥	Basic Auth 0Auth2	_
HSEQ ¥	Port: 25	
Document Handling ¥	Sender address Token URL:	_
System's Place ¥	Sender name	-
Tools ¥	Timeout: 100 seconds	=
Administration ¥	Use SSL/TLS Client Secret:	-
System *		
Settings	POP3 Settings Server: Basic Auth OAuth2	
0	Port: 110 Use OAuth2	
Import and export	Max messages 20 Token URL:	
TM Exchange Client	Use SSL/TLS Scope:	
Log	User Name:	
_	ClientID:	
	Client Secret:	
	Last service loop: 00:00:00	

3. SMTP Settings:

SMTP Settings	Basic Auth OAuth2
Server:	Use OAuth2 Use Same authentication for SMTP and POP3
Port: 25	
Sender address	Token URL:
Sender name	Scope:
Timeout: 100 seconds	User Name:
Use SSL/TLS	ClientID:
_	Client Secret:

a. SMTP Server: Enter the SMTP server address.

The address path may look something like this example: https://graph.microsoft.com/v1.0/users/example@email.com/sendMail
The email in the example above (example@email.com) should be replaced with the email address you have configured for replication for the particular installation.

- b. **SMTP Port:** Not used. his can be ignored for SMTP server when using OAuth2
- c. Sender Address: Enter the e-mail address for the account to be used.

- d. Senders Name: Not used. his can be ignored when using OAuth2
- e. **Timeout:** Enter the maximum time TM Exchange should wait for a response from the mail server before giving up. (100 Seconds is a reasonable value)
- f. Use SSL/TLS: Tick this check box. SSL/TLS is required for OAuth2
- g. Click the **"OAuth2"** tab in the tab control to the left of the SMTP server fields and fill in the details . (The "Basic Auth" tab can be ignored)
- h. Use OAuth2: Tick this check box
- Token URL: Enter the token URL to your mail server: It may look like this: https://login.microsoftonline.com/TenantID/oauth2/v2.0/token (Replace "TenantID" with the Tenant ID from your Azure environment) For More details on how to get the token can be found here:
- j. Scope: Enter the scope: https://graph.microsoft.com/.default
- k. **User Name:** Enter the user name (email address) for the account to be used when sending emails from the system.
- I. **Client ID:** Enter the "Application (client) ID". This should be the ID, Azure assigned to TM Master when <u>registering the application</u> with the Microsoft identity platform.
- m. Client Secret: Enter the client secret for the client ID

4. POP3 Settings

POP3 Settings -		
Server:	outlook.office365.com	Basic Auth OAuth2
Port:	995	Use OAuth2
Max messages to download	20	Token URL:
to dominodd	Use SSL/TLS	Scope:
		User Name:
		ClientID:
		Client Secret:

- a. Server: Enter the POP3 Server address (outlook.office365.com)
- b. Port: Enter the port to use for outlook.office365.com this should be 995
- c. **Max message to download:** Is not related to the authentication, so this value can be left as is. It limits the number of messages downloaded per TM Exchange service cycle.
- d. Use SSL/TLS: Tick this check box. SSL/TLS is required for OAuth2
- e. Click the **"OAuth2"** tab in the tab control to the left of the POP3 server fields and fill in the details . (The "Basic Auth" tab can be ignored)
- f. Use OAuth2: Tick this check box
- g. Token URL: Enter the token URL to your mail server: It may look like this: <u>https://login.microsoftonline.com/TenantID/oauth2/v2.0/token</u>. It will in most cases be the same as for the SMTP server.
- h. **Scope:** Enter the POP3 Server scope. For outlook.office365.com this should be: <u>https://outlook.office365.com/.default</u>
- i. User Name: Enter the e-mail address to retrieve\download e-mail from.
- j. **Client ID:** Enter the "Application (client) ID". This should be the ID, Azure assigned to TM Master when <u>registering the application</u> with the Microsoft identity platform.
- k. Client Secret: Enter the client secret for the client ID

Register your TM Master with your Azure AD

- 1. Log on to your Azure portal <u>https://portal.azure.com</u>
- 2. Click on "App registrations"

	🖕 🕂 New registration 🜐 Endpoints 🤌 Troubleshooting 🕐 Refresh 🞍 Download 🐻 Preview features 🗌 🖗 Gr	t feedback?	
Overview Preview features	All applications Owned applications Deleted applications		
X Diagnose and solve problems	P Start typing a display name or application (client) ID to filter these r		
Manage			
Lusers	1 applications found Display name ↑	Application (client) ID	Created on 1, Certificates & secret
Sroups	Test Email		-
External (dentities	-		
Roles and administrators			
Administrative units			
Enterprise applications			
Devices			
R App registrations			
Identity Governance			

3. Click [New Registration]

 * Name The user-facing display name for this application (this can be changed later). TmMaster Supported account types Who can use this application or access this API? Accounts in this organizational directory only (Tero Marine AS only - Single tenant) Accounts in any organizational directory (Any Azure AD directory - Multitenant) Accounts in any organizational directory (Any Azure AD directory - Multitenant) Accounts in any organizational directory (Any Azure AD directory - Multitenant) Personal Microsoft accounts only Help me choose Redirect URI (optional) We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.	Home > Tero Marine AS App registrations >
The user-facing display name for this application (this can be changed later). TmMaster Supported account types Who can use this application or access this API? Accounts in this organizational directory only (Tero Marine AS only - Single tenant) Accounts in any organizational directory (Any Azure AD directory - Multitenant) Accounts in any organizational directory (Any Azure AD directory - Multitenant) Personal Microsoft accounts (e.g. Skype, Xbox) Personal Microsoft accounts only Help me choose Redirect URI (optional) We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.	Register an application
The user-facing display name for this application (this can be changed later). TmMaster Supported account types Who can use this application or access this API? Accounts in this organizational directory only (Tero Marine AS only - Single tenant) Accounts in any organizational directory (Any Azure AD directory - Multitenant) Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox) Personal Microsoft accounts only Help me choose Redirect URI (optional) We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.	
TmMaster Supported account types Who can use this application or access this API? Accounts in this organizational directory only (Tero Marine AS only - Single tenant) Accounts in any organizational directory (Any Azure AD directory - Multitenant) Accounts in any organizational directory (Any Azure AD directory - Multitenant) Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox) Personal Microsoft accounts only Help me choose Redirect URI (optional) We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.	* Name
Supported account types Who can use this application or access this API? Accounts in this organizational directory only (Tero Marine AS only - Single tenant) Accounts in any organizational directory (Any Azure AD directory - Multitenant) Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox) Personal Microsoft accounts only Help me choose Redirect URI (optional) We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.	The user-facing display name for this application (this can be changed later).
Who can use this application or access this API? Accounts in this organizational directory only (Tero Marine AS only - Single tenant) Accounts in any organizational directory (Any Azure AD directory - Multitenant) Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox) Personal Microsoft accounts only Help me choose Redirect URI (optional) We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.	TmMaster 🗸
 Accounts in this organizational directory only (Tero Marine AS only - Single tenant) Accounts in any organizational directory (Any Azure AD directory - Multitenant) Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox) Personal Microsoft accounts only Help me choose Redirect URI (optional) We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios. 	Supported account types
Accounts in any organizational directory (Any Azure AD directory - Multitenant) Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox) Personal Microsoft accounts only Help me choose Redirect URI (optional) We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.	Who can use this application or access this API?
Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox) Personal Microsoft accounts only Help me choose Redirect URI (optional) We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.	 Accounts in this organizational directory only (Tero Marine AS only - Single tenant)
Personal Microsoft accounts only Help me choose Redirect URI (optional) We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.	Accounts in any organizational directory (Any Azure AD directory - Multitenant)
Help me choose Redirect URI (optional) We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.	🔘 Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
Redirect URI (optional) We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.	O Personal Microsoft accounts only
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.	Help me choose
changed later, but a value is required for most authentication scenarios.	Redirect URI (optional)
Public client/native (mobile http://localhost	We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.
rable dient/hatre (hobie in	Public client/native (mobile 🗸 http://localhost 🗸

- 4. Enter details
 - a. Name: Enter name of application: TMMaster
 - b. **Supported account types:** Select the appropriate value for your company.
 - c. Redirect URI: Enter: <u>http://localhost</u>

- 5. Make sure TM Master has the needed API permissions:
- 6. Click [+ Add a permission]
- 7. Select [Microsoft Graph]

Home > Tero Marine AS App registe	ations > Test Email			Request API permission	IS	
₋ Test Email API pe	rmissions 🖈 …					
				Select an API		
	🕐 Refresh 🛛 🗖 Got feed	dback?		Microsoft APIs APIs my organization	uses My APIs	
Overview				Commonly used Microsoft APIs		
🗳 Quickstart						
💉 Integration assistant				Microsoft-Graph		
Manage				Access Azure AD, Excel, Int	rendous amount of data in Office 365, Enterpris une, Outlook/Exchange, OneDrive, OneNote, Sh	e Mobility + Security, and Windows 10. arePoint, Planner, and more through a
Branding & properties				single endpoint.		
Authentication	/					
Certificates & secrets				_		
Token configuration	Configured permissions			P Azure Batch	Azure Communication Services	Azure DevOps
 API permissions 		call APIs when they are granted permissions by users/admins a tion needs. Learn more about permissions and consent	s part of the consent process. The list of co	Schedule large-scale parallel and HPC applications in the cloud	Rich communication experiences with the same secure CPaaS platform used	Integrate with Azure DevOps and Azure DevOps server
 Expose an API 	+ Add a permission	Grant admin consent for Tero Marine AS			by Microsoft Teams	
App roles	API / Permissions name	Type Description	Admin consent reau.			
A Owners	Microsoft Graph (10)	type beschpton	Autilit Consent requi	Azure Key Vault	Azure Rights Management	A
& Roles and administrators		· · · · · · · · · · · · · · · · · · ·		Azure Key Vault Manage your key vaults as well as the	Services Allow validated users to read and write	Azure Service Management Programmatic access to much of the
Manifest	email	Delegated View users' email address	No	keys, secrets, and certificates within	Allow validated users to read and write protected content	functionality available through
Support + Troubleshooting	Mail.Read	Application Read mail in all mailboxes	Yes	your Key Vaults		the Azure portal
support inconcontrolling	Mail.Send	Application Send mail as any user	Yes			

- 8. Click [Application Permissions]
- 9. Enter "Mail.Send" in the permission search bar
- 10. Tick the "Mail.Send"
- 11. Click the [Add Permissions] button
- 12. Close the "Request API permissions" dialog

Delegated permissions Your application needs to access the API as the signed-in men	Application permissions Your application runs as a background service or daemon without a signed-in user.
elect permissions	expand al
P Mail.Send Permission	× Admin consent required
✓ Mail (1)	
Mail.Send. ① Send mail as any user	Yes

- 13. Click the [+ Add permissions] again.
- 14. Click [APIs my organization uses]

Request API permission	าร	2	×
Select an API <u>Microsoft APIs</u> APIs my organization Commonly used Microsoft APIs	n uses My APIs		
	mendous amount of data in Office 365, Enterpris tune, Outlook/Exchange, OneDrive, OneNote, Sh		
Azure Batch Schedule large-scale parallel and HPC applications in the cloud	Azure Communication Services Rich communication experiences with the same secure CPaaS platform used by Microsoft Teams	Azure DevOps Integrate with Azure DevOps and Azure DevOps server	

- 15. Type "Office" in search bar
- 16. Select "Office 365 Exchange Online"

Request API permissions
Select an API Microsoft APIs my organization uses
Office
Nan e ONice 765 Enterprise Insights
Office 365 Exchange Online
Office 365 Information Protection
Office 365 Management APIs
Office 365 Mover

- 17. Click the [Application Permissions] link
- 18. Enter "Access" in the search bar.
- 19. Tick "IMAP.AccessAsAPP"
- 20. Tick "POP3.AccessAsAPP"
- 21. Click the [Add Permissions] button

Request API permissions	×
CAILAPIS Office 365 Exchange Online https://ps.outlook.com What type of permissions does your application require?	
Delegated permissions does your application requires Your application needs to access the API as the signed-in user.	Application permissions Your application runs as a background service or daemon without a signed-in user.
Select permissions	expand all
Permission	Admin consent required
 ✓ Other permissions full_access_as_arp ⊙ Use Exchange Web Services with full access to all mailboxes 	Yes
MAP (1)	Yes
✓ POP (1)	
POP.AccessAsApp ① POP.AccessAsApp	Yes
Add permissions	

- 22. Close the "Request API permissions" dialog
- 23. Now click "Grant admin consent for", and select the APIs just added
 - a. Mail.Send
 - b. IMAP.AccessAsApp
 - c. POP.AccessAsApp

24. The result should look like the screen shot below

₽ Search	« 🜔 Refresh 🛛 🕂 Got fe	edback?				
Overview	Configured permissions					
Quickstart	5	Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permission				
🐔 Integration assistant			ore about permissions and consent		3	
/anage	$+$ Add a permission \checkmark	Grant admin consent	t for Your domain			
Branding & properties	API / Permissions name	Туре	Description	Admin consent requ	Status	
Authentication	✓ <mark>Microsoft Graph (1)</mark>					
Certificates & secrets	Mail.Send	Application	Send mail as any user	Yes	Granted for Your doma	
Token configuration	∽ Office 365 Exchange Onlin	e <mark>(2)</mark>				
 API permissions 	IMAP.AccessAsApp	Application	IMAP.AccessAsApp	Yes	Granted for Your doma	
Expose an API	POP.AccessAsApp	Application	POP.AccessAsApp	Ves	Granted for Your doma	

- 25. Create a "Client Secret" for the application (TMMaster)
 - a. Click "Certificates & Secrets"
 - b. Click "Client secrets" taNe
 - c. Click "New Client Secret"

- i. Enter a name
- ii. Set an Expiry date
- d. A "Client Secret" will be generated
- 26. **NOTE!** Be sure to copy the "Value" before leaving the page. After leaving the page it will not be possible to retrieve the "Client secret" value. This value is needed to configure TM Master.

Manage					
 Branding & properties Authentication 	Certificates (0) Client secrets				
Certificates & secrets Token configuration	A secret string that the application of the secret string that the application of the secret	uses to prove its identity when	requesting a token. Also can be	referred to as application password.	
 API permissions 	Description	Expires	Value 🛈	Secret ID	
Expose an API App roles	tmmaster secret				D 🗊

The configuration described above applies to all TM Master installations, configured with the "Client ID" and "Client secret".

Source: <u>https://docs.microsoft.com/en-us/exchange/client-developer/legacy-protocols/how-to-authenticate-an-imap-pop-smtp-application-by-using-oauth</u>

How to find the details required to grant TM Master access to download?

Find the "Tennant ID" or <ORANIZATION_ID>

- 1. Log onto "portal.azure.com"
- 2. Enter "tenant" in the search bar

Microsoft Azure	P tenani X 🖂 🕄 (0 © Ø R
Home > Properties Asure Active Directory	All Services (4) Resources (1) Resource Groups (1) Marketplace (7) Documentation (28) Asure Active Directory (5)	
🗟 Save 🗙 Discard 🧖 Got feedback?	Services	
·····	Tenant properties Cross-tenant Synchronization	

3. A page with the "Tenant ID" will show

Name *	
Ocean Technologies Group	~
Country or region	
United Kingdom	
Location	
EU Model Clause compliant datacenters	
Notification language	
Notification language English	~
	~

4. Copy it to a notepad or similar, to use later.

NOTE! This information should be treated as "confidential information" and not freely shared.

Find the <APPLICATION_ID> and the <OBJECT_ID>

- 1. Log onto "portal.azure.com"
- 1. Go to "Enterprise applications" \rightarrow "Overview"
- 2. Search for the newly registered APP. IE: "TMMaster"
- 3. Click it to view details

Enterprise Application	ange App Overview
	4%
Overview	Properties
Deployment Plan	Name 🛈
Manage	TmMaster
III. Descention	Application ID (i)
Properties	XXXXXXXXXX
24 Owners	Object ID 💿
Roles and administrators	XXXXXXXXXX

4. Copy the **<APPLICATION_ID>** and **<OBJECT_ID>** to a notepad or similar, to use later.

TIP! The OBJECT_ID is the object ID from the overview of the Enterprise Application node (Azure Portal) for the application registration. It is not the Object ID from the Overview of the App Registration node (as shown above). Using the incorrect Object ID will cause an authentication failure

TmMaster Exchange App 🛷 …					
	📋 Delete 🜐 Endpoints 💀 Preview features				
R Overview	Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for a				
duickstart					
💉 Integration assistant	↑ Essentials				
Manage	Display name : <u>TmMaster Exchange App</u>				
Branding & properties	Application (client) ID : XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX				
Authentication	Object ID YYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYY				
📍 Certificates & secrets	Directory (tenant) ID : ZZZZZZZZ-ZZZZ-ZZZZ-ZZZZ-ZZZZZZZZZZZZ				
Token configuration					
API permissions	Starting June 30th, 2020 we will no k be upgraded to Microsoft Authentici This is not the Object ID you are looking for				
Expose an API	This is the wrong Object ID				
App roles	Get Started Documentation				
A Owners					

NOTE! This information should be treated as "confidential information" and not freely shared.

How to grant TM Master (TM Exchange) access to download emails from an account

TM Exchange needs to be able to download replication emails from the various involved email accounts. To enable TM Master to do this TM Master will need "Read" access to the mailboxes

NOTE! This is one way to do this in the Microsoft environment, your IT department may have different ways and procedures to implement this. Please make sure you are implementing this following your IT Guidelines and procedures, before proceeding.

- 1. You will need the following details from Azure (ref chapter above)
 - Application (client) ID <APPLICATION_ID>
 - Object ID <OBJECT_ID>
 - Directory (tenant) ID <ORGANIZATION_ID>
- 2. Open Exchange Online Management console
 - Open admin.microsoft.com
 - Open Azure Cloud Shell, by clicking the button to the right in the top menu bar

i.

	Microsoft 365 admin center	₽ Search	([
_				

Type AND Run "Connect-EXOPSSession" to connect to Exchange

PowerShell > 0 ? 🛞 🕞 🖆 () 🕞	- 🗆 ×
Terminal container button vud Shell.Succeeded. Connecting terminal	
MOTD: Cmdlet help is available: help <cmdlet name=""></cmdlet>	
VEENDOS: Authenticating to Azure VEENDOS: Building your Azure drive PS /home/pawel> Connect-EXUPSSession	

- Enter the commands listed in step 3 to 5 below.
- 3. Register the Azure application in Exchange (only needs to be run once)
 - New-ServicePrincipal -AppId <APPLICATION_ID> -ServiceId <OBJECT_ID> [-Organization <ORGANIZATION_ID>]
 - •
- 4. Get the Exchange ID for the Azure application using this command:
 - Get-ServicePrincipal -Organization <ORGANIZATION_ID> | fl (Service Principal ID is called "ExchangeObjectId" in the service principal list)
- 5. Use the Service Pricipal ID to grant access to the mailboxes used for replication **Note!** This command must be run once per email account
 - Add-MailboxPermission -Identity "example@email.com" -User
 <SERVICE_PRINCIPAL_ID> -AccessRights FullAccess

Example:

- APPLICATION_ID> = AAAAAA
- <OBJECT_ID> = 00000
- <ORGANIZATION_ID> = TTTTTT

a. Register the Azure application in Exchange New-ServicePrincipal -AppId AAAAAAA -ServiceId 00000 [-Organization TTTTTT]

b. Get the Exchange ID for the Azure application Get-ServicePrincipal -Organization TTTTTTT | fl

- <SERVICE PRINCIPAL_ID> = SSSSS
- Mailbox = example@email.com

c. Grant access to mailbox

Add-MailboxPermission -Identity "**example@email.com**" -User SSSSS -AccessRights FullAccess

For more details regarding this procedure:

https://docs.microsoft.com/en-us/exchange/client-developer/legacy-protocols/how-to-authenticate-an-imap-pop-smtp-application-by-using-oauth#register-service-principals-in-exchange