Accessing Microsoft 365 from PMA

Proventeq Migration Accelerator

Version: 1.0

29 March 2021

Authored by: Proventeq

Status: Released

Proventeq Ltd, Reading Enterprise Centre, Earley Gate, Whiteknights Road ,Reading RG6 6BU, United Kingdom

: www.proventeq.com | : +44 118 907 9296 | : info@proventeq.com

Table of Contents

1. BACKGROUND

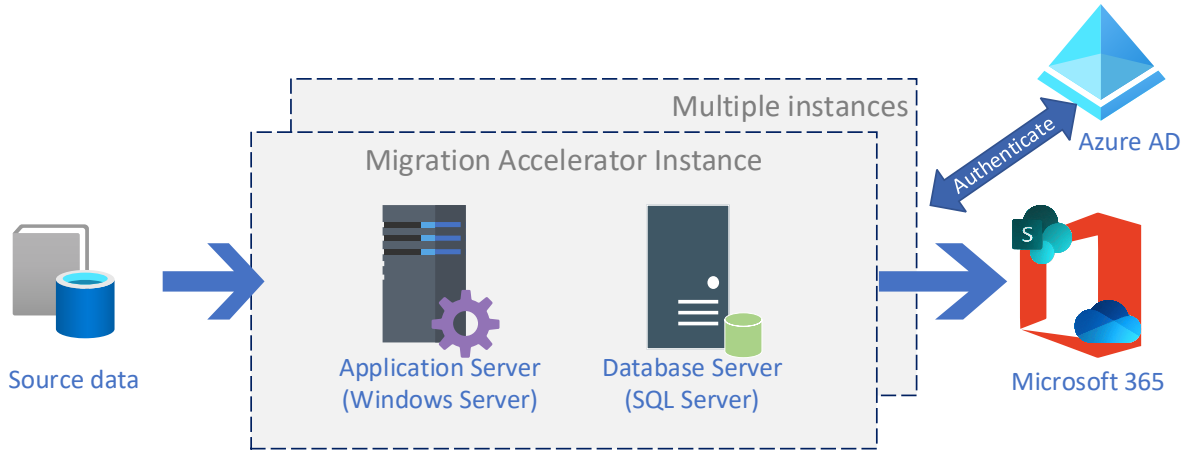
Proventeq Migration Accelerator (PMA) requires access to Microsoft 365 (M365), especially SharePoint Online, to perform any migration activity. Since access to Microsoft 365 is managed by Azure AD (AAD) with PAM Key Vault, PMA requires a mechanism to authenticate and gain authorised access to the sites and libraries to migrate content into.

Authentication

Authentication is the process of proving that you are who you say you are. It's sometimes shortened to AuthN. The Microsoft identity platform uses the OpenID Connect protocol for handling authentication.

Authorization

Authorization is the act of granting an authenticated party permission to do something. It specifies what data you are allowed to access and what you can do with that data. Authorization is sometimes shortened to AuthZ. The Microsoft identity platform uses the OAuth 2.0 protocol for handling authorization.



In addition to the above, there could be additional security such as conditional access policies that could further restrict access to content.

2. SUPPORTED AUTHENTICATION MODES IN PMA

A user can access Microsoft 365 (SharePoint Online) using one of the following supported ways:-

1. An Azure AD user account with username and password
2. An Application
    a. Customer registered AAD Application
    b. Proventeq Multi-tenant AAD Application

2.1. An Azure AD user account

PMA will use the username and password of a user to authenticate and get authorised access to SharePoint and OneDrive. User accounts with any form of multi-factor authentication (MFA) is not supported. This method is no longer recommended as migration activity using user accounts will be throttled by Microsoft.

2.2. Application

2.2.1. SharePoint/ACS App-Only (Legacy method)

SharePoint App-Only is the older, but still very relevant, model of setting up app-principals. This model works for both SharePoint Online and SharePoint 2013/2016/2019 on-premises

This option uses the Azure Access Control (ACS), a service of Azure Active Directory (Azure AD), which has been retired on November 7, 2018. For new tenants, apps using an ACS app-only access token is disabled by default. We recommend using the Azure AD app-only model which is modern and more secure.

Navigate to a site in your tenant and then call the appregnew.aspx page.

For tenant level access: https://*<your tenant>*.sharepoint.com/_layouts/15/appregnew.aspx

For site collection level access: https://*<your tenant>*.sharepoint.com/*<managed path>*/*<site name>*/_layouts/15/appregnew.aspx

Use the Generate button to generate a client id and client secret and fill the remaining information.

Grant permission to this app via the appinv.aspx page. https://*<your tenant>*-admin.sharepoint.com/_layouts/15/appinv.aspx. The permission can be granted to allow the app to access a specific site collection or the entire tenant.

For more details refer to https://docs.microsoft.com/en-us/sharepoint/dev/solution-guidance/security-apponly-azureacs

The client id and client secret generated using this approach can be used by PMA to connect to M365.

2.2.2. Azure AD App-only

An application (app) registered on an Azure tenant can be used by PMA to access SharePoint during migration. The app receives an authorization code from the Microsoft identity platform based on a certificate or a signed-in user. The authorization code represents the app's permission to call back-end services (in some cases on behalf of the user who is signed in). The app can exchange the authorization code in the background for an OAuth 2.0 access token and a refresh token. The app can use the access token to authenticate to SharePoint in HTTP requests, and use the refresh token to get new access tokens when older access tokens expire. PMA uses this App to authenticate and gain access to Sites to migrate content.

The Microsoft identity platform supports two types of permissions:

- **Application permissions** - When using application permissions, PMA will require the Application (client) ID of the registered application and a certificate. Use of secret is currently not supported.
- **Delegated permissions** - When using delegated permission, in addition to the Application (client) ID, a user account without MFA is required. The app is delegated permission to act as the signed-in user when it makes calls to SharePoint. The effective permissions of the app are the least-privileged intersection of the delegated permissions the app has been granted (by consent) and the privileges of the currently signed-in user. Your app can never have more privileges than the signed-in user.

Using the Admin Consent endpoint, a global administrator/application administrator can grant consent for the application to act on behalf of any user in the tenant.

```
https://login.microsoftonline.com/{tenant-id}/adminconsent?client_id={app-id}
```

{tenant-id} - is your organization's tenant ID (GUID) or any verified domain name (e.g. contoso.com).

{app-id} – The application ID (client-id) of the application registered in Azure AD.

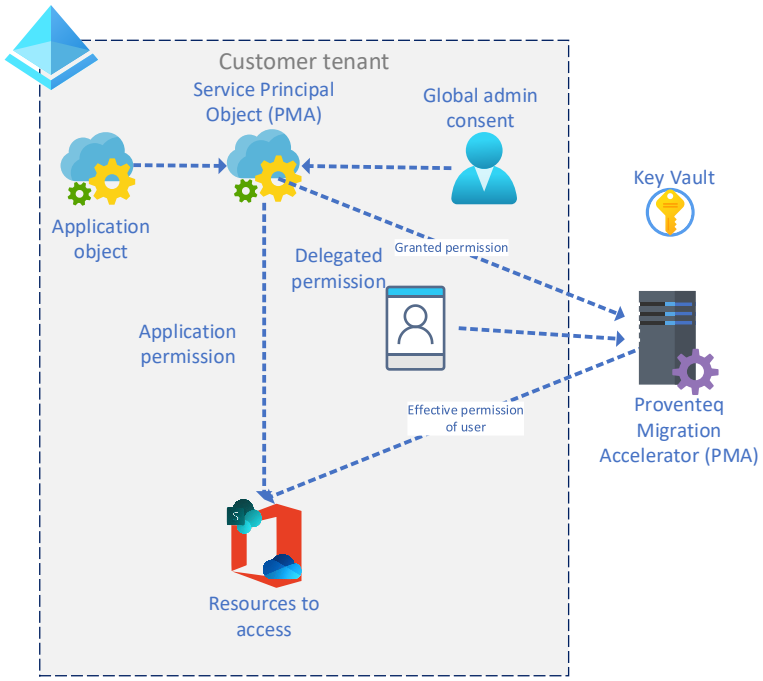
The application requires the following API permissions assigned to it.

API / Permissions name	Type	Description	Admin consent req.
Microsoft Graph (3)			
Group.Read.All	Delegated	Read all groups	Yes
Sites.FullControl.All	Delegated	Have full control of all site collections	Yes
User.Read.All	Delegated	Read all users' full profiles	Yes
SharePoint (1)			
AllSites.FullControl	Delegated	Have full control of all site collections	Yes

2.2.2.1. Customer registered AAD Application

This option is currently not supported in PMA.

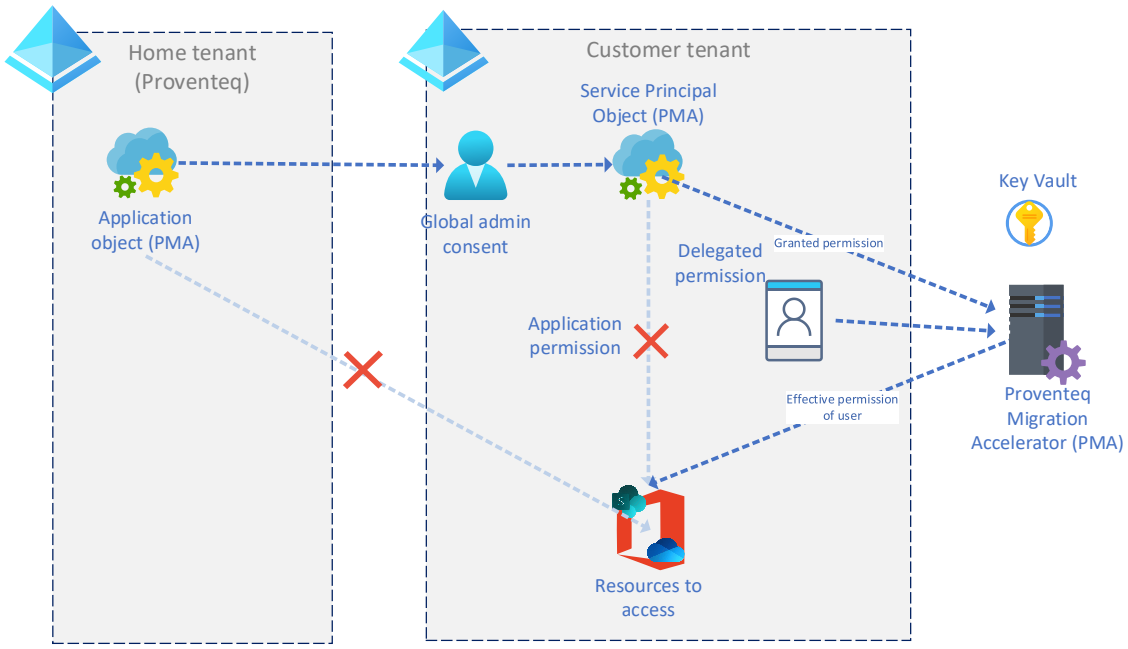
The application is registered on the customer's tenant, as a result the application object and the Service Principal Object resides in the customer's tenant.



2.2.2.2. Proventeq Multi-tenant AAD Application

This is the preferred approach to connect to M365 using PMA.

The multi-tenant application works is a similar way to the customer registered application, except the application object is registered in the Proventeq tenant, but the service principle required to access SharePoint is in the customer's tenant.



Since this application uses the delegated permission type, in addition to the application being provided admin consent on the tenant, PMA will require a user account without MFA in the customer's tenant.

The PMA application can be provided admin consent using the link below.

```
https://login.microsoftonline.com/{tenant-id}/adminconsent?client_id=d1e5e128-9660-4380-aabb-3e0061c1047c
```

{tenant-id} - is your organization's tenant ID (GUID) or any verified domain name (e.g. contoso.com).

d1e5e128-9660-4380-aabb-3e0061c1047c - is the application ID of the PMA application.

Optionally Key Vaults can be used to access the credentials while using migration orchestration using the PMA PowerShell modules.