Microsoft Graph Authentication VBO

VBO

User Guide

Document Revision 1.0

Trademarks and copyrights

Contents

Figures

1. Introduction

This document describes the VBO for generating access tokens for Microsoft's Graph API. Microsoft Graph is a RESTful web service interface that can be used to interact with Microsoft's cloud-based Office offerings such as OneNote, Excel, Sharepoint, etc. It supports using delegated and application access tokens.

You can find further details about Microsoft Graph authentication mechanism at the following link:

https://docs.microsoft.com/en-us/graph/auth/

2. Prerequisites

Before using this integration, you must create a service account credential within your Microsoft 365 environment with sufficient permission to interrogate and manage user accounts. This involves creating an **App Registration** within your Azure Active Directory. Additionally set the API permissions as necessary depending upon the API actions that you plan to use.

Creation of the App Registration will provide you with the following items you will need to configure the Microsoft Graph Teams Authentication VBO within Blue Prism:

Required Credential Information

- Client ID
- Client Secret
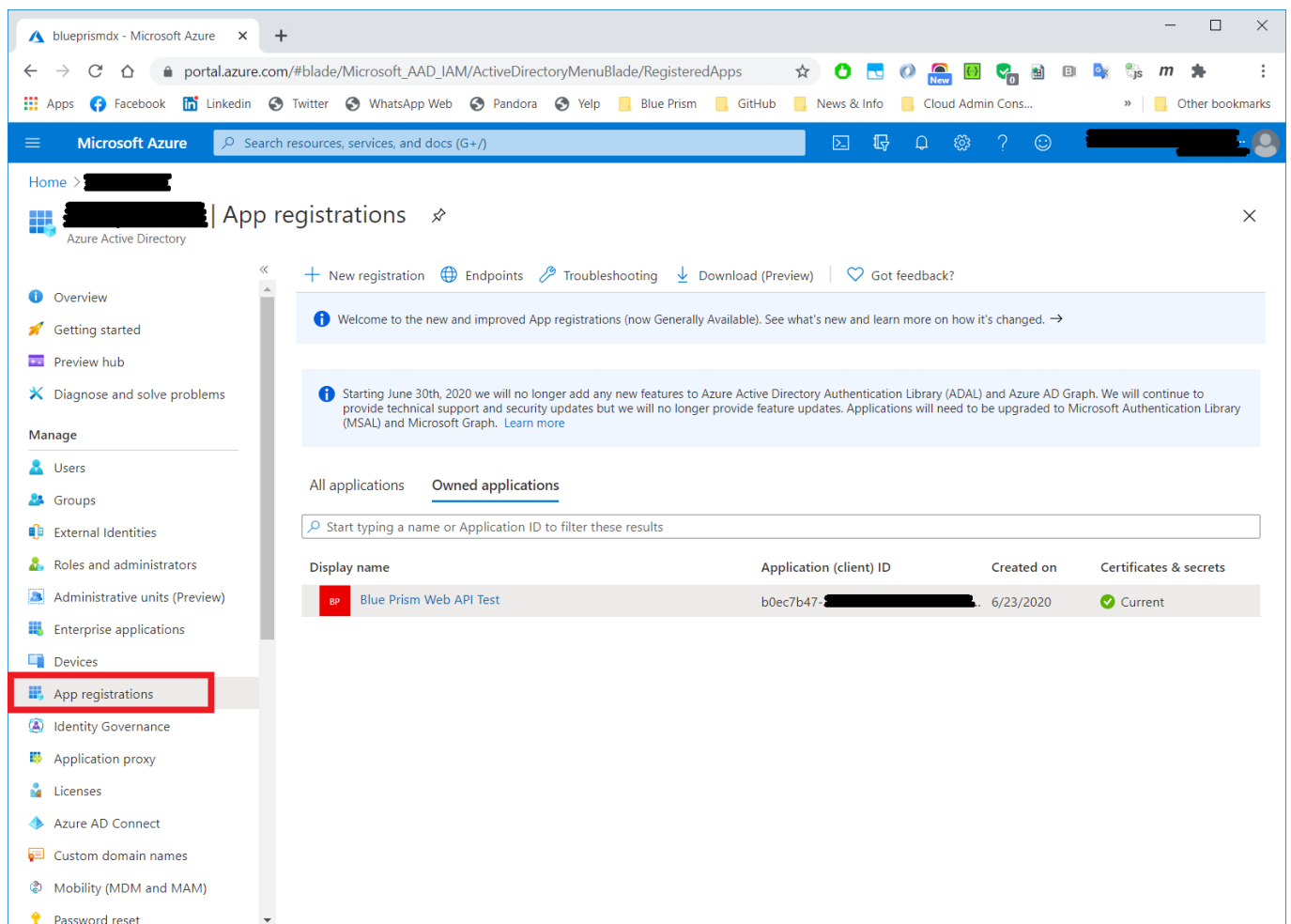
Web API Service Definition Information

- Azure Tenant ID

Figure 1 - Azure App Registration
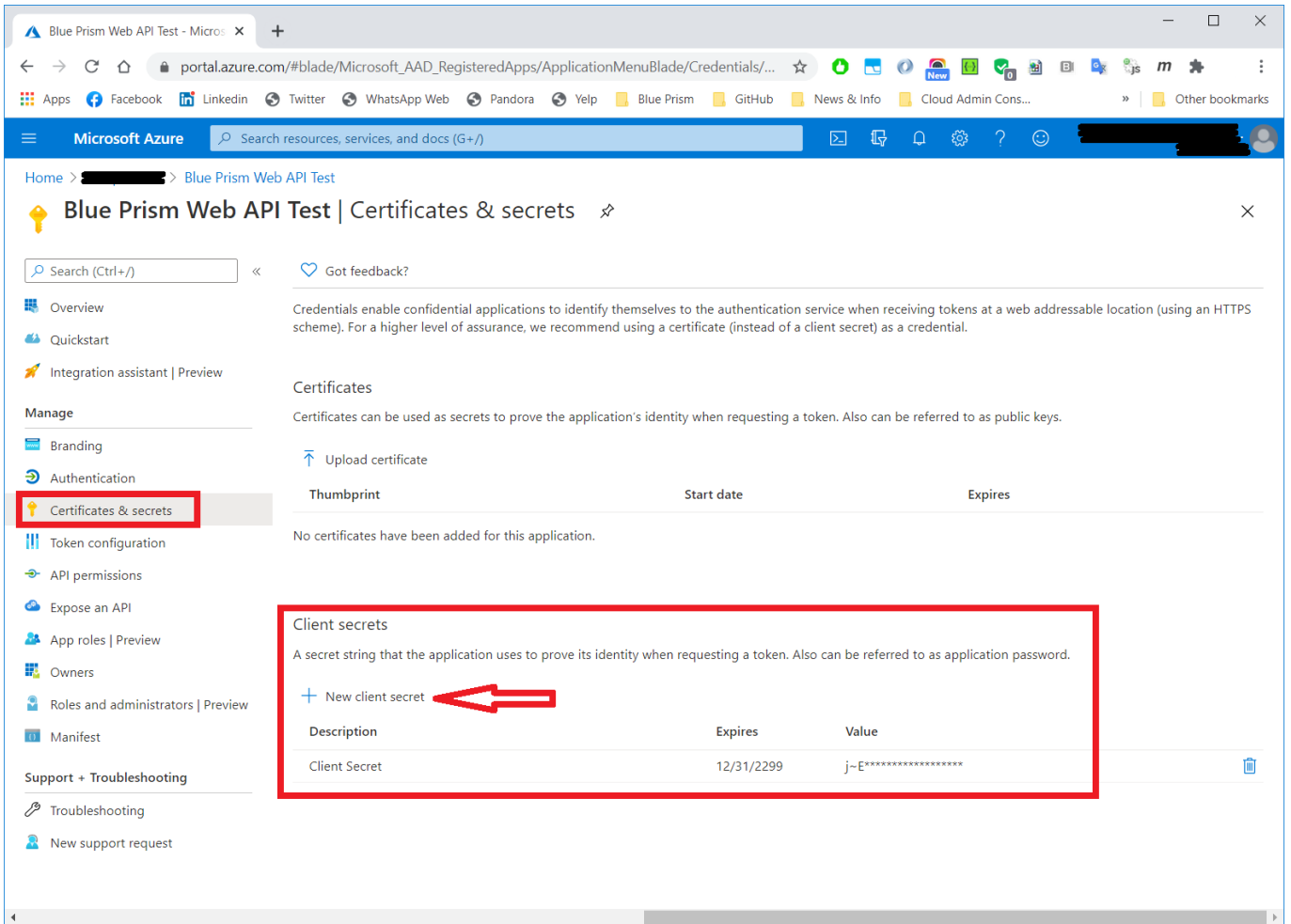
Figure 2 - App Registration Details

Figure 3 - Client Secret

Depending on the actions that you need to use, you need to grant application or delegated permissions as below -
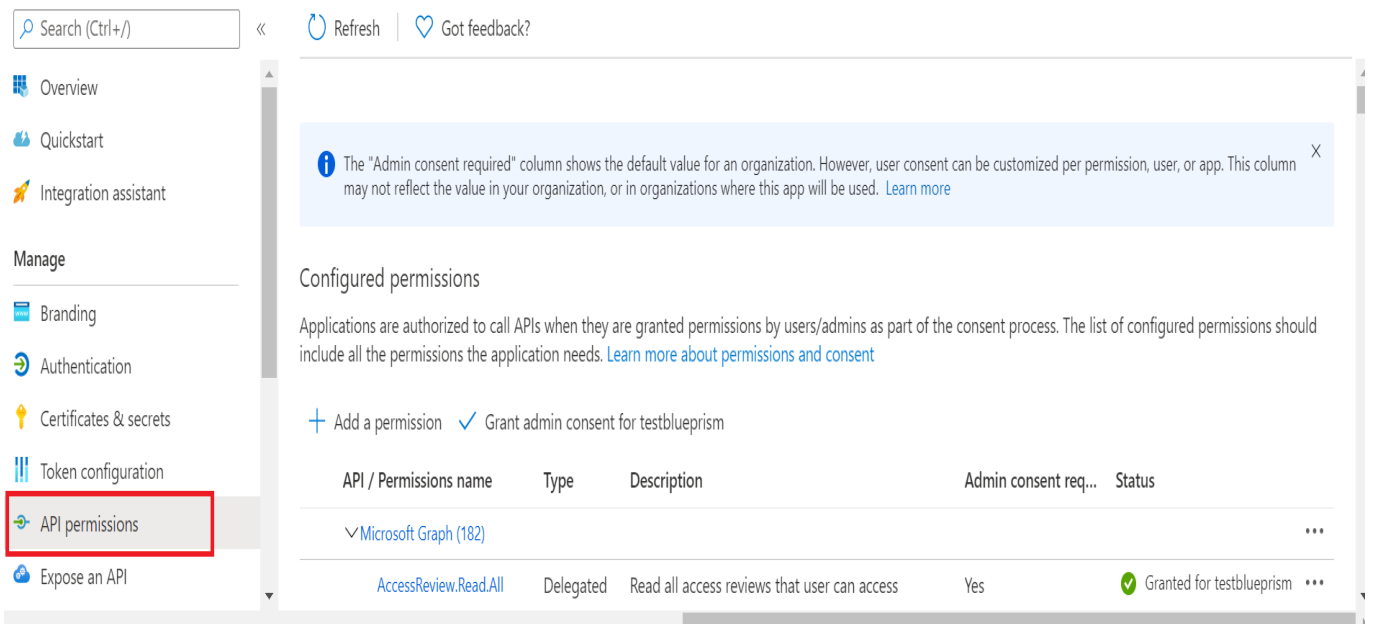
Figure 4 – API Permissions

3. Configuration

This asset has been made available as a Blue Prism release file. To use the asset you must import the .bprelease file which contains the following:

- VBO

    o   Microsoft Graph - Authentication

The Graph API actions can work using delegated permission or application permission. Both requires a token to be generated separately. Use the VBO **Microsoft Graph – Teams Authentication** to retrieve the relevant access token and pass it into the relevant Graph Web API as Bearer access token in the Authentication Header when making the call.

For retrieving Application Access Token, pass in the TenantID, ClientID and ClientSecret as input parameters.

Figure 5 – Application Access Token

For retrieving Delegated Access Token, pass in the TenantID, ClientID, ClientSecret, UserName and Password as input parameters.

Figure 6 – Delegated Access Token

4. Actions

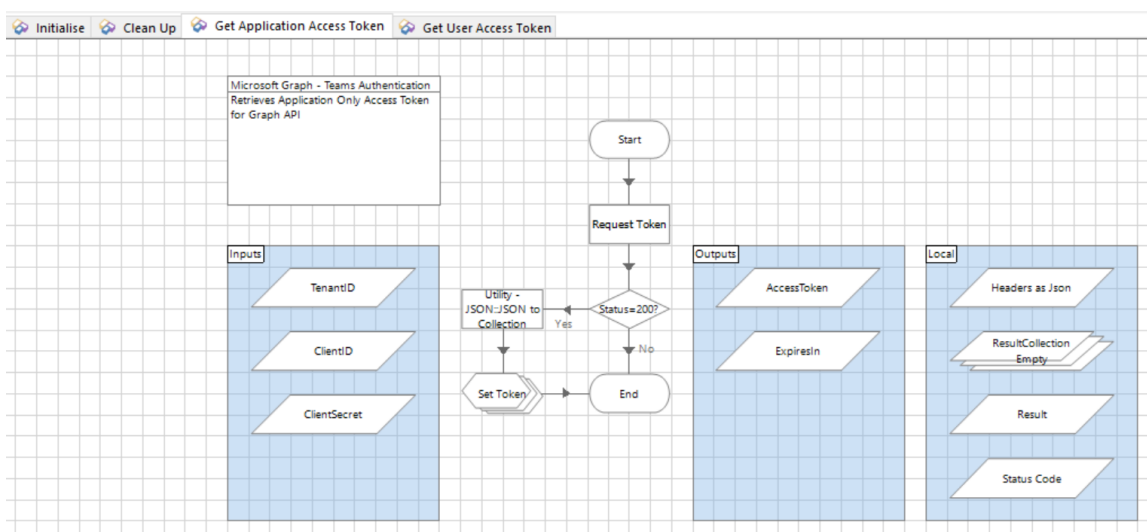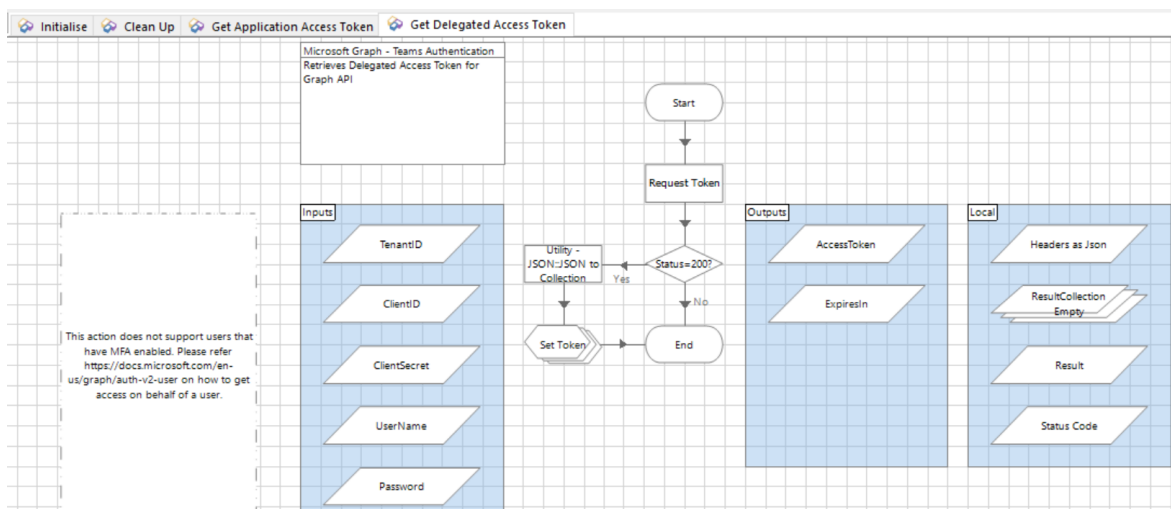## 4.1   Get Application Access Token

Retrieves Application Only Access Token for Graph API

Parameter	Direction	Data Type	Description
TenantID	In	Text	TenantID of the organization
ClientID	In	Text	Client ID of the Azure app
ClientSecret	In	Password	Secret Key for the Azure app
AccessToken	Out	Password	AccessToken for Graph API authorization
ExpiresIn	Out	Number	Token Expiration time interval

4.2   Get Delegated Access Token

Retrieves Delegated Access Token for Graph API

Type	In	Text	Set to either 'users', 'groups', or 'sites'.
TenantID	In	Text	TenantID of the organization
ClientID	In	Text	Client ID of the Azure app
ClientSecret	In	Password	Secret Key for the Azure app
UserName	In	Text	Username of the user granting access
Password	In	Password	Password of the user granting access
AccessToken	Out	Password	AccessToken for Graph API authorization
ExpiresIn	Out	Number	Token Expiration time interval

5. Support

This asset is provided free-of-charge by Blue Prism. Blue Prism does not provide formal support of this asset. Please direct any questions you have, related to this asset, to the Digital Exchange Community page:

https://community.blueprism.com/communities/community-home?CommunityKey=1e516cfe-4d1f-4de9-a9eb-58d15bf38c81