INTRODUCTION

In September 2022 Microsoft announced that they would be retiring Microsoft Azure Directory Graph any time after 30 June 2023.

Microsoft is replacing the 'Azure Active Directory (Azure AD) Graph API' with a product with a similar name - 'Microsoft Graph API'. Further information from Microsoft can be found here:

https://learn.microsoft.com/en-us/graph/migrate-azure-ad-graph-overview (https://learn.microsoft.com/en-us/graph/migrate-azure-ad-graph-overview)

Vivantio has two pieces of functionality that use the retiring Azure AD Graph API:

- Single Sign On (SSO) authentication method for the technician's portal and to any self-service portals
- Windows Azure Directory Sync

Using the Microsoft Graph authentication has the advantage of removing the need for your users to provide login credentials and make accessing and updating information a more streamlined process. You can register multiple tenants for your Clients or even use different sign on methods tailored to different Clients (for example, username and password for some Clients, Single Sign On for others).

NEXT STEPS

If you use Azure AD Single Sign On (SSO) for the Vivantio Main Application or your Vivantio Self Service Portal (SSP) then you will be required to enable and register Microsoft Graph tenant. Please follow the configuration guidance below.

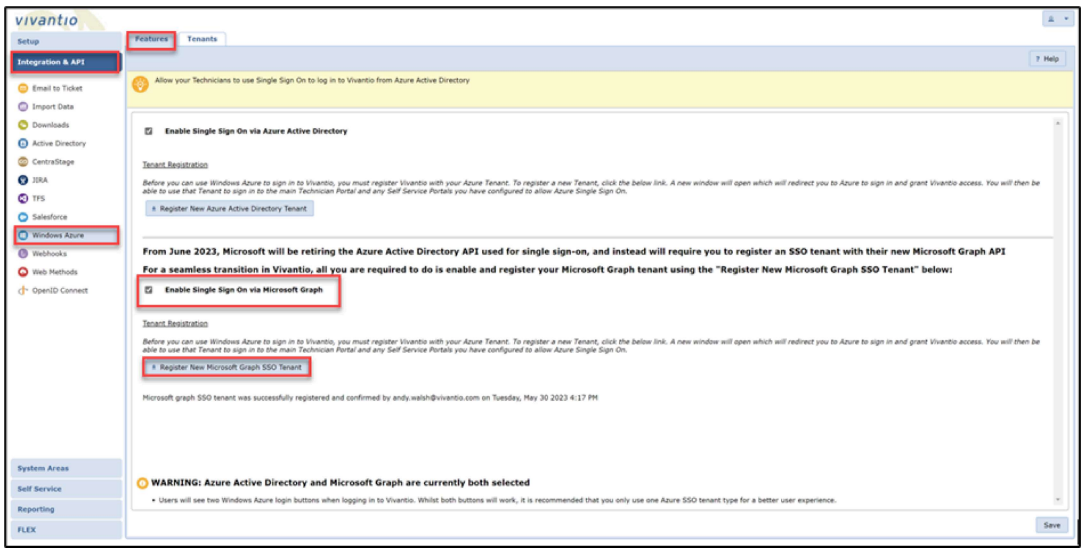
If you currently use Windows Azure Directory Sync please refer to the following article for further guidance:

Azure Sync to FlexBridge (https://support.vivantio.com/Article/Detail/2240)

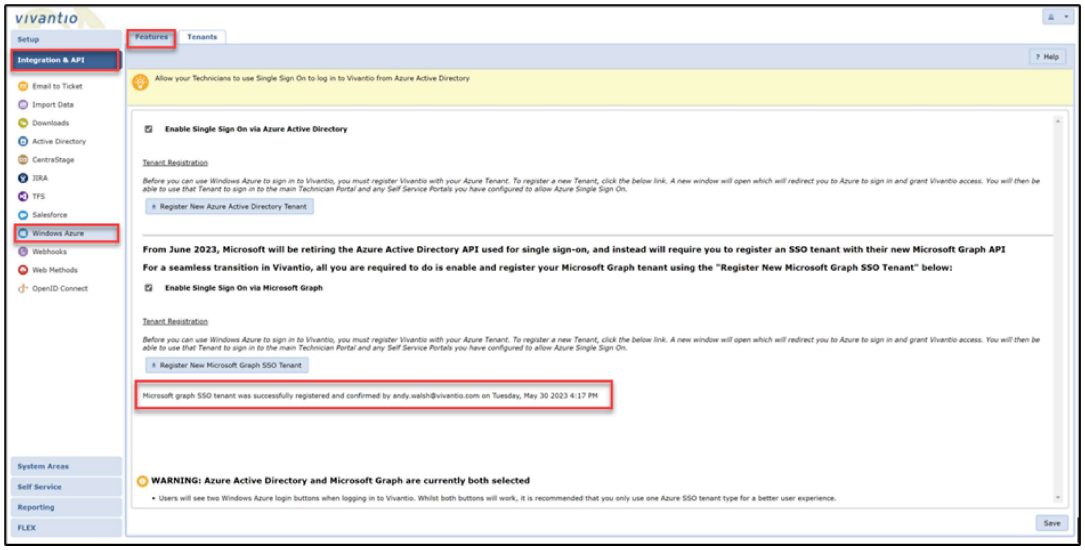
VIVANTIO TECHNICIAN'S PORTAL - SSO

For a seemless transition in Vivantio please navigate to the Vivantio Admin Area > Integration & API > Windows Azure > Features and enable the **Enable Single Sign On via Microsoft Graph** option.

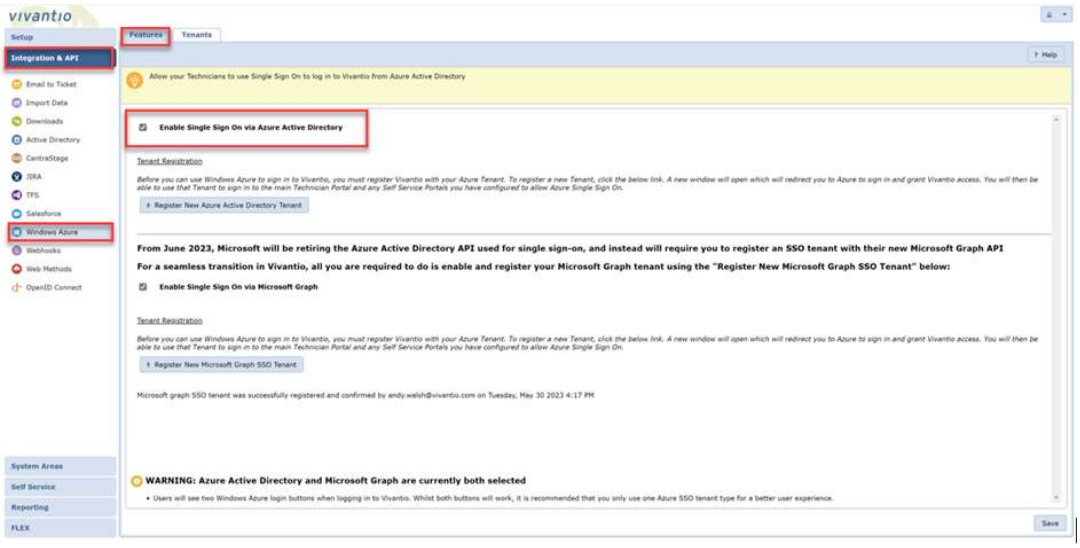
A user with Azure AD Administrator access will then need to click the **Register New Microsoft Graph SSO Tenant** button and enter their credentials.



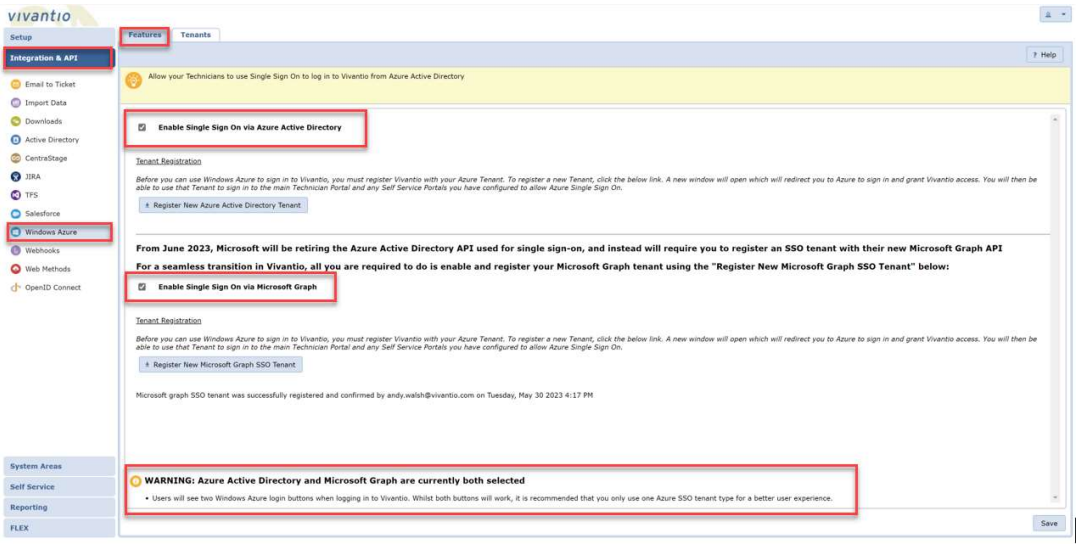
Once the tenant has been successfully registered there will be a message, as highlighted in the below screenshot



You will then be able to disable the Single Sign on via Azure Active Directory, as highlighted in the below screenshot



If you do **not** disable this option and leave both Single Sign On options enabled, you will receive a warning message, as per screenshot below

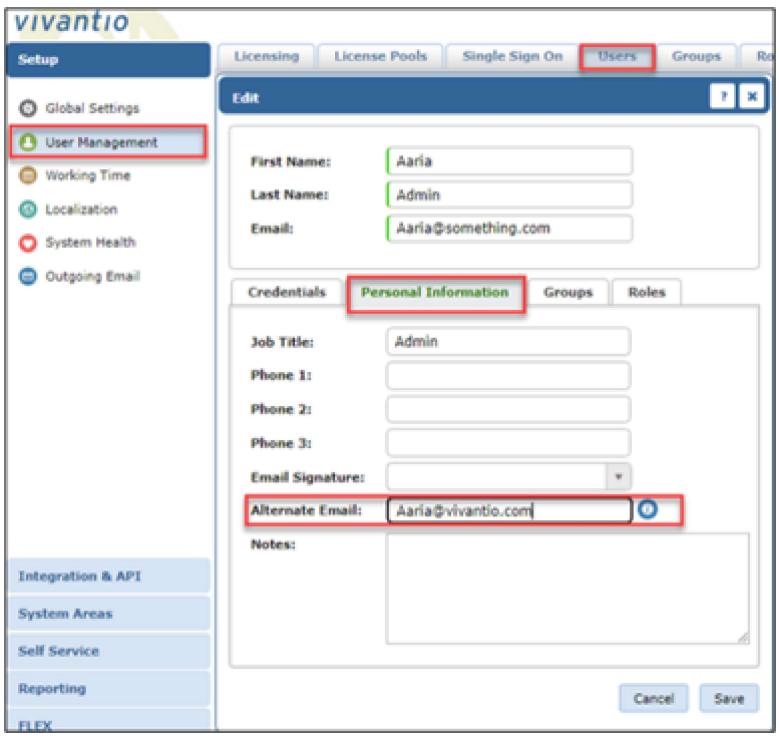


Your Users will also be presented with 2 Single Sign on login buttons upon logging into Vivantio

When they hover over the buttons, the text will show whether this is a login via Azure AD or Azure Microsoft Graph

Please Note: If the users login name is different to their email address, to be able to log into Vivantio the users Microsoft Graph login needs to go into the user email field and their email address needs to go into the 'Alternate Email' address field:

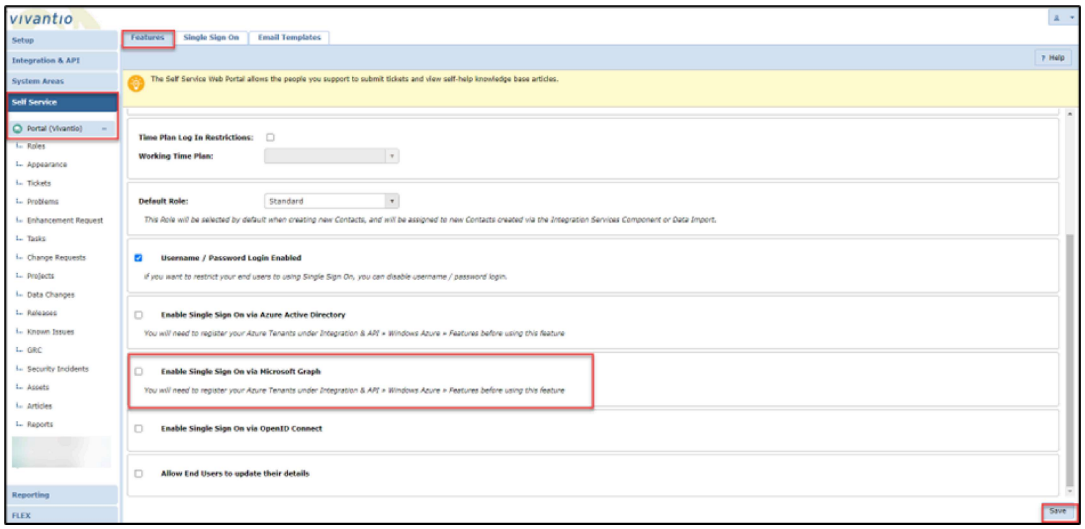
Alternate Email Field: If you specify an email address here, all emails to this user will be sent to this address instead of their primary email. Use this if your SSO provider doesn't return your user email addresses in the login name field



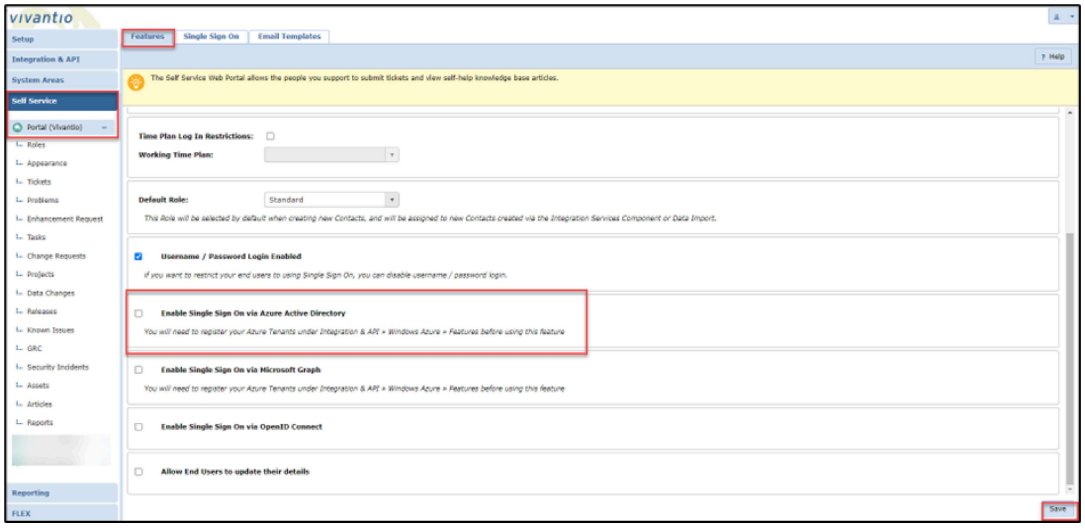
VIVANTIO SELF SERVICE PORTAL - SSO

As you will have already registered your tenant when enabling SSO on the main Vivantio application (as above) please navigate to the Vivantio Admin Area > Self Service > Portal > Features > Enable **'Enable Single Sign On via Microsoft Graph** > Save

Please Note: You will need to register your Azure Tenants under Integration & API > Windows Zure > Features before enabling this feature if you have not already done so *(as explained above)*



You will then need to disable the **'Enable Single Sign On via Azure Active Directory**



REGISTERING TENANTS FROM AN EXTERNAL CUSTOMER/CLIENT

If you are registering an external clients Microsoft Graphs instance so that they can access the self service portal via single sign on, you will either need administrative access to their tentant or you will need to co-ordinate registering the tenant with your

client via a screen share, the client representative will need to be able to provide the credentials to login and grant access.

Created: *07 June 2023*