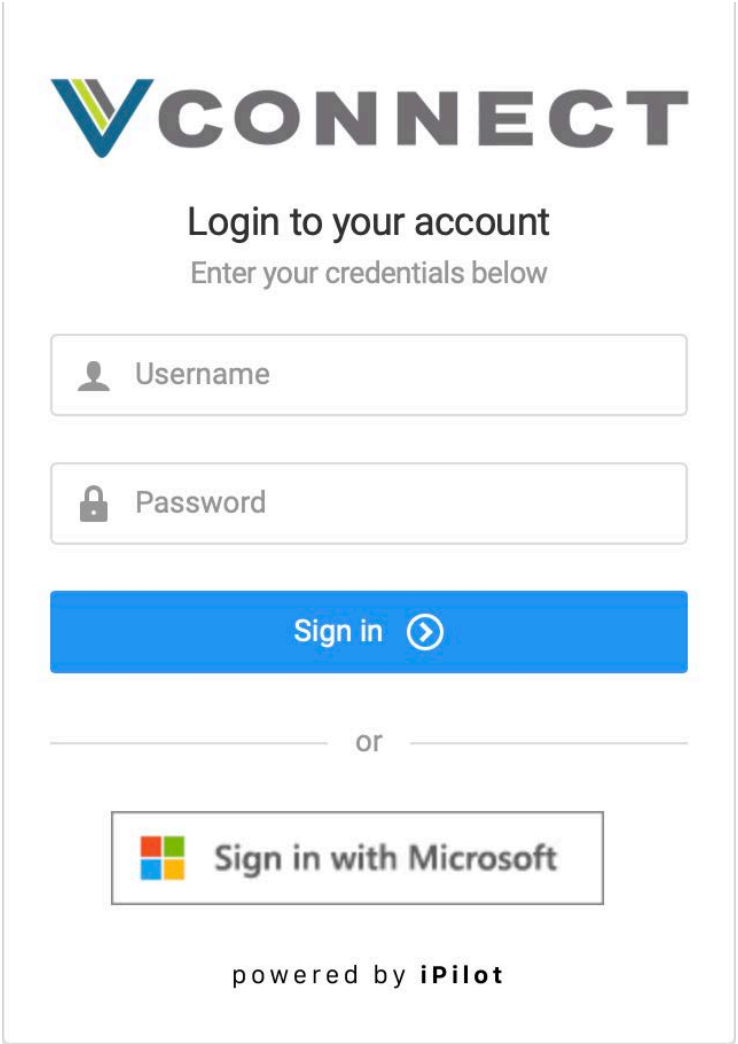
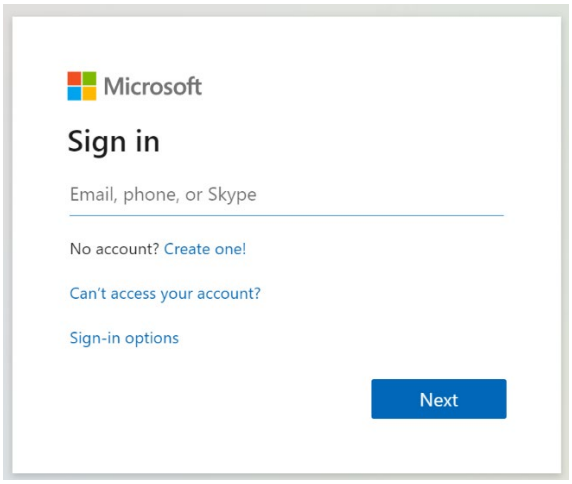
Veracity Vconnect and Microsoft SSO

Veracity Networks, Inc. Vconnect™ supports single sign on (SSO) using Microsoft work or school accounts (Azure AD) with or without AD Sync. Users manually provisioned in Vconnect use the email SAML claim to link Vconnect users to Microsoft accounts. We currently do not support auto provisioning via SCIM so the user must first be created in Vconnect with correct account permissions and correct email address.

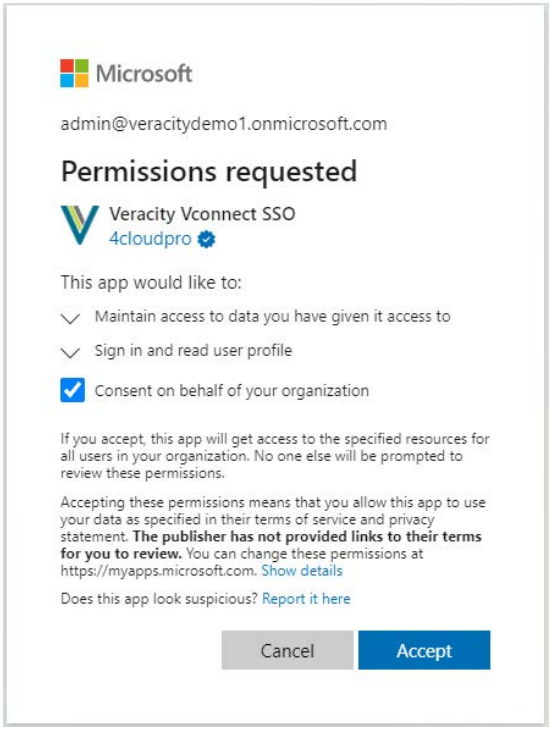
Initial Login

On the logon page to Vconnect you should see a button labeled "Sign in with Microsoft" that clicking on will redirect you to Microsoft to sign in including any multi factor authentication MFA your organization may have.





Upon first login attempt Microsoft will ask for consent:



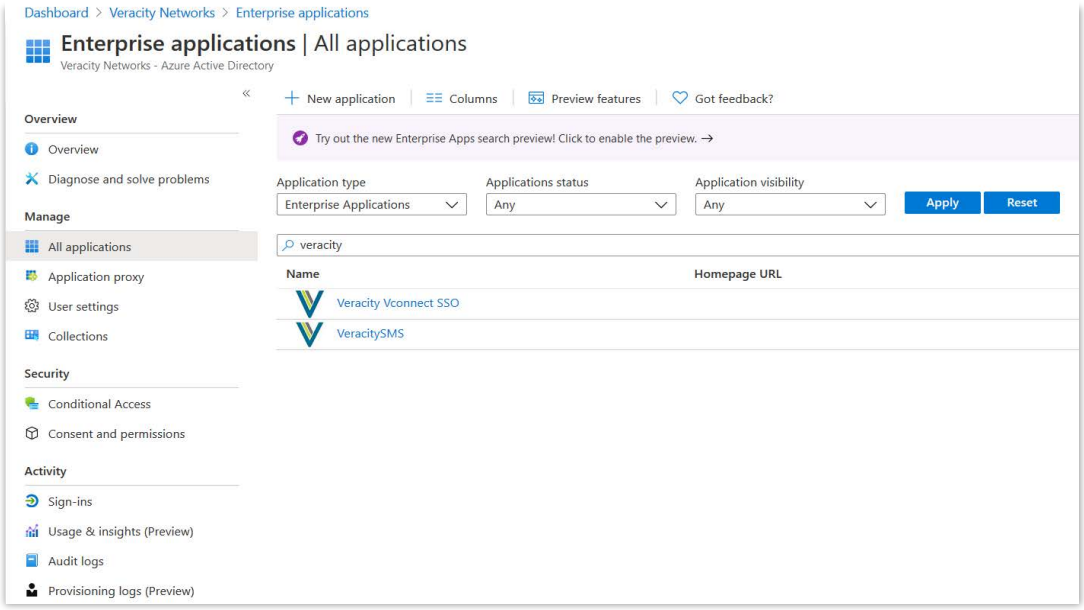
It is recommended that a Microsoft Azure AD Application Admin (at minimum) first log in so that an Admin consent is done preventing every user from having to consent. This can be managed later in the Microsoft Azure Portal as discussed later in this document.

After successful login you will be redirected and logged into Vconnect.

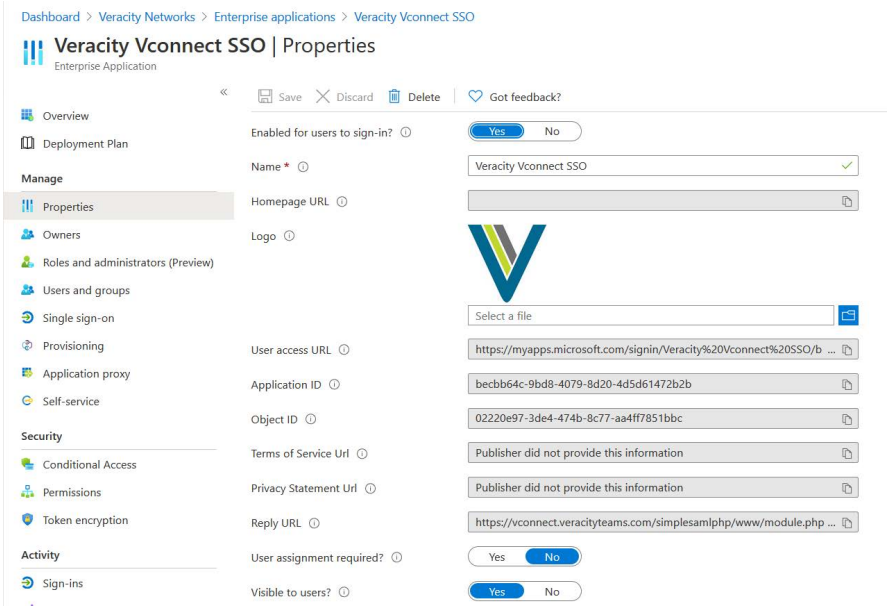
From this point on you use the Microsoft login button to sign in as the username/password has been disabled.

Administration

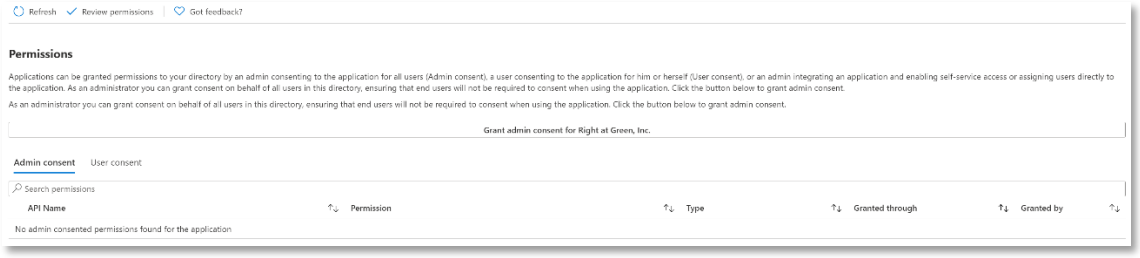
As Azure AD application administrator you can manage, consent and modify security requirements as you see fit. Once any user (or admin) has consented at least once, Microsoft will add a new Service delegate application into your portal.



If you would like to lock down which users in your organization can log into Vconnect you can enable user assignment required and then manage the users/groups manually that have access.



To enable Admin consent if not done previously on first login you can grant under permissions.



Today Vconnect does not require very many permissions as it is just being used for sign in but future releases will add more that will then need to be consented to again such as granting rights to use the Graph API for dashboards.

Additionally you can lock down access under the Conditional Access section to block if not on VPN or any other requirement your organization may have.

Previously Vconnect allowed you to create user accounts with duplicate email addresses as long as the username was unique. Going forward the system will not allow you to create a new account with a duplicate email. However, to not break existing accounts, logging in via Microsoft Azure AD is not allowed if there are duplicate emails as it is ambiguous which account to use. You can either rename the email address to be unique or open a ticket to have a Veracity employee do it.