
Installation guide for
Tenant Administrators
Version 4.0
external365

Contents

Overview

This document serves as an overview and general instruction manual on how to install the components necessary to integrate external365 with a customer Azure tenant.

External365 simplifies the management of external user accounts in Microsoft 365, making it easy to share content and users granted access to a company's SharePoint online site, but are not licensed within that organization. Please follow to Managing external users in Microsoft Office 365 to find what External365 is.

External365 is designed to operate from within the Microsoft Azure cloud and leverages Microsoft Azure specific technologies (e.g. queues, storage, app services, etc.). It cannot operate from another cloud vendor, nor can it operate from a stand-alone service platform. The external365 application is a multitenant host that can provision any number of discrete Office 365 tenants while maintaining secure separation of services between them.

The external365 application has been installed in the Azure tenant created specifically to host it. Access to that tenant is managed by administrative persons from ELEARNINGFORCE Corporation.

Deployment Prerequisites

To successfully deploy the components necessary for external365 integration, a few requirements must be met:

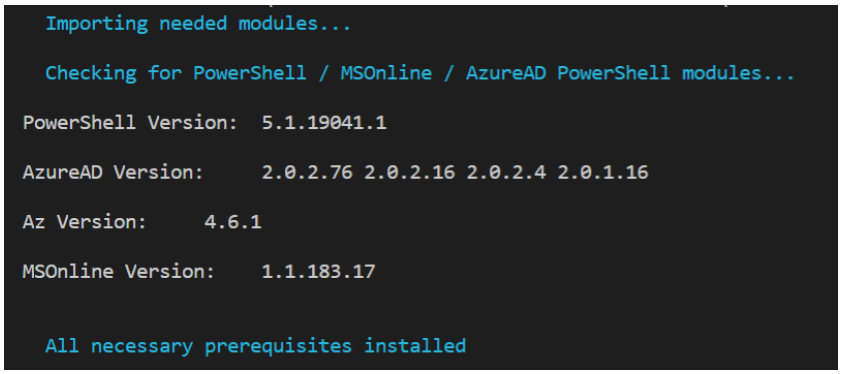
- A Global Administrator is required for application deployment as the components associated with external365 integration require elevated privileges in the Azure tenant. The components required for integration are
    - Application Registration
    - Service Principal
- A workstation with this software installed. Please note that this the required software to be able to launch the external365 Installer.
    - PowerShell 5.1 or higher
        - https://www.microsoft.com/en-us/download/details.aspx?id=50395
    - MSOnline Cmdlets (version 1.1.183.0 or higher)
        - If not available, you may launch PowerShell as an Administrator and type "**Install-Module MSOnline**". Type "Y" when prompted for consent to install.
    - AzureAD Cmdlets (Version 2.0.1.16 or higher)
        - If not available, you may launch PowerShell as an Administrator and type "**Install-Module AzureAD -AllowClobber -Force**". Type "Y" when prompted for consent to install.
    - Az Cmdlets (version 4.6.1 or higher)
        - If not available, you may launch PowerShell as an Administrator and type "**Install-Module Az -AllowClobber -Force**". Type "Y" when prompted for consent to install.
- Please note that Cmdlets detailed as required may be older versions than what is currently available. Due to compatibility differences between newer and older version, we recommend running the commands with the "**-AllowClobber -Force**" parameter to ensure that your instances of Cmdlets are compatible with the installer.
- Information pertaining to the Customer URL. This will be the URL used to access external365. Typically, the URL is constructed using the current customer domain followed by the mandatory external365.com suffix. For example, https://CustomerXYZ.external365.com/

NOTE: Instructions to download the necessary software can be found here. https://docs.microsoft.com/en-us/office365/enterprise/powershell/connect-to-office-365-powershell

Application Deployment

To **initiate deployment**, please follow these steps:

1. Extract the External365_App_Deploy.zip to a location on the workstation
2. Double click the External365_App_Deploy_v1.13_MFA
    - When initially launching the External365_App_Deploy application, a verification process is run to determine if the necessary PowerShell and Azure modules are available to proceed with the install. If any of these requirements are not met, a message is presented detailing the missing requirement. The depiction below represents all requirements met.



3. Choose option "1" to *Disconnect from all current Azure sessions*. This is to ensure that there are not any lingering sessions connected on your machine that may cause issues with the installer.
4. Choose option "2" to *Connect to Tenant*
    a. To allow for communication between External365 and a tenant, an application registration and service principal must be provisioned. Once these items are provisioned, permissions must be granted to the services manually. These tasks require elevated privileges, therefore the logged in user must be a Global Administrator.
    b. During account provisioning, the UserPrincipalName is a required field in Azure. Due to this requirement, External365 is unable to provision accounts using a federated domain or the default *.onmicrosoft.com.
    c. You will be asked to login 3 times, as the installer needs to login to each cmdlet detailed earlier. If you have multifactor authentication turned on in your tenancy, please have your authentication device ready so that you may proceed easily.

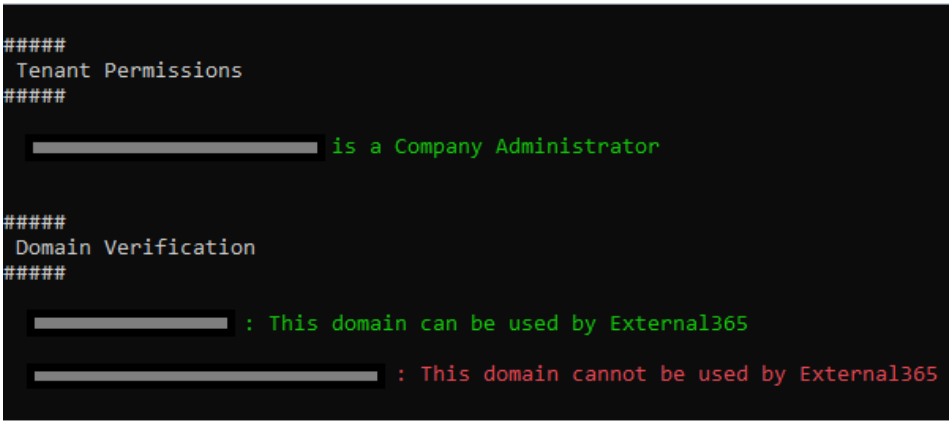
5. Choose option “3” to verify the tenant

    a. This step will be used to verify that the installer can deploy the application to your tenant as well as confirm which domains can be used with external365.

    b. We highly recommend adding an additional domain to the tenant which will be used with accounts created via External365, as this would allow you to easily identify which users were created through the application (ex. user@EXT.contoso.com).

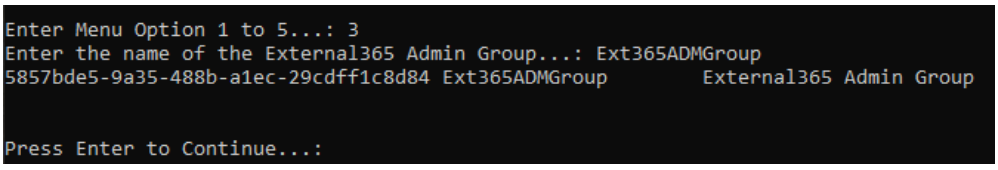
    c. You may also freely use the existing domains in your organization to use with external365, but this approach would take up a potential internal username if done.

    d. If you are intending to convert accounts made on external365 into full internal member accounts, we recommend using the main domain of your organization. For example, if you are intending to use external365 to create accounts for temp workers that you eventually want to fully license as internal members once they are hired full, you can easily convert the account from external to an internal member with this approach just by licensing the user in Microsoft 365.



6. Choose option “4” to create an External365 Admin Group

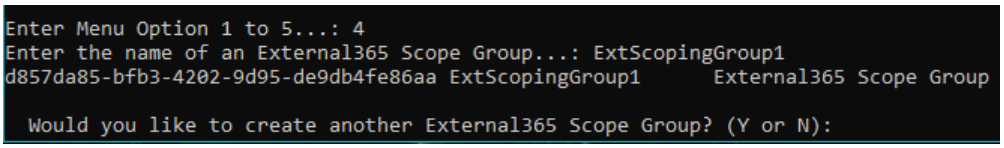
    a. To delegate access to the privileged areas of the customers instance in external365, an Azure AD security group is used. Members of this group will have access into the Control Panel and have the ability to modify items such as Tenant Configuration and Notifications along with visibility into System and Diagnostic logs. This option will create an Azure AD security group that is later added to the permissions configuration of the instance.



7. Choose option "5" to create External365 Scope Groups (can create multiple groups)

    a. To enforce delegation, External365 can leverage Azure AD security groups, known as scoping groups, to provide a level of isolation between dissimilar entities.

    b. An example use case could be, if two outside entities require account creation and/or management of accounts (ex. E365 Sales Scope Managers and E365 Marketing Scope Manager), External365 can separate these accounts into specific Scope Groups allowing visibility only to accounts managed by the respective entity. Please see Appendix A for a depiction.



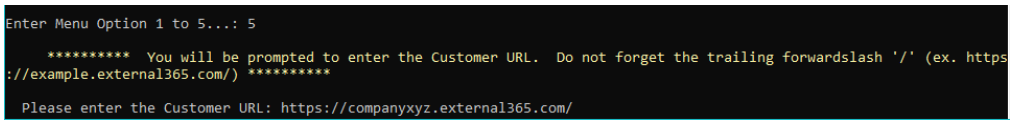
8. Choose option "6" to create an External365 Users Group.

    All External Accounts created on External365 will be placed in this group and can then be utilized by any system that leverages Azure Active Directory Groups.

9. Choose option "7" to create the App Registration.

    a. Enter the URL chosen as the endpoint for accessing external365. In typical scenarios this is **https://<tenant domain>.external365.com/** .

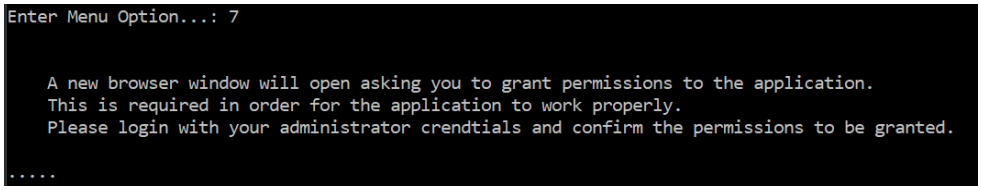
    Note: The trailing backslash is required when entering the URL.



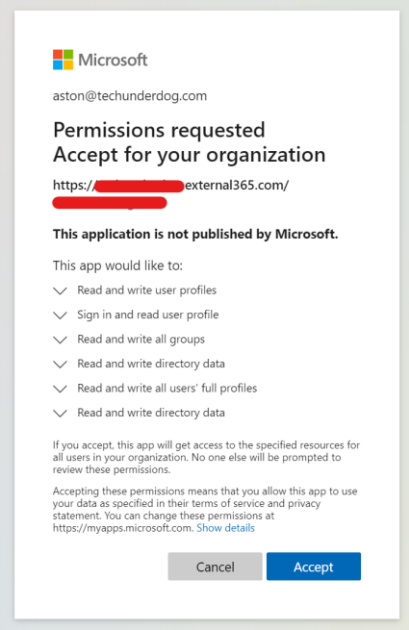
    b. The creation of the Application and Service Principal will begin. Please be patient as the process may take a few minutes.

10. Choose option "8" to grant permissions to the new application.

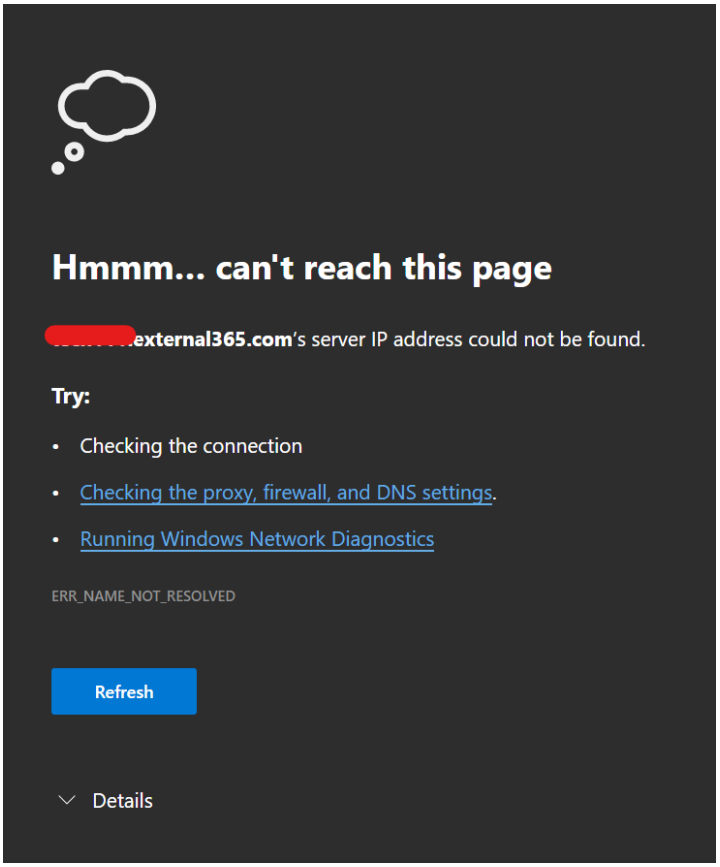
    a. A browser window will open shortly allowing to grant permissions to the application. This is required for the application to be able to access and create accounts on your Azure Active Directory. If this step is skipped, the application will not work.



b. Login with the same Global Admin account used earlier and accept the permissions detailed on the page.

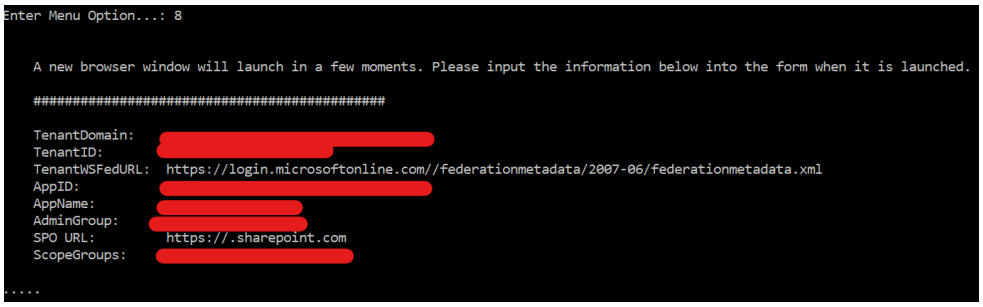


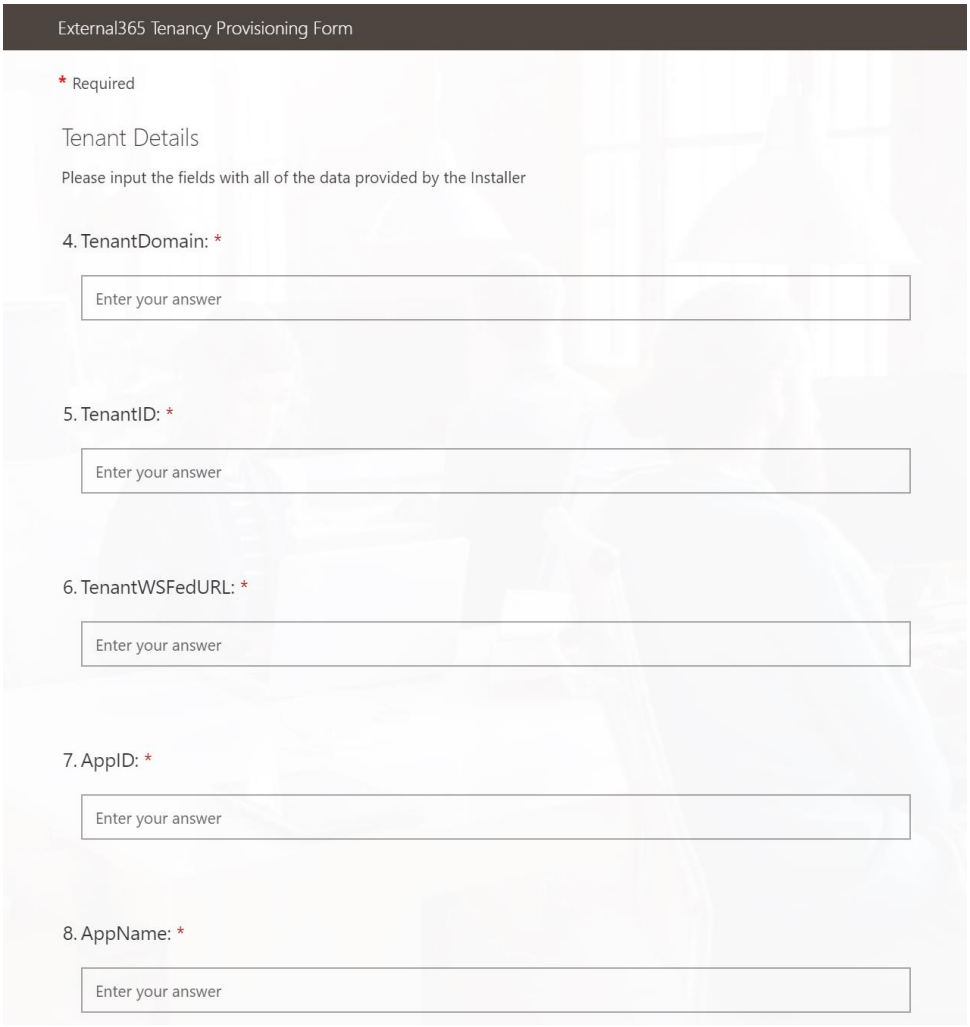
c. After accepting the permissions, you will be directed to the external365 Control Panel. However, you will likely receive an error as the tenancy is not done being provisioned yet. This will be completed in the next step.



11. Choose option “9” to complete the tenancy provisioning form.

    Details about your installation of external365 will be provided on the screen and a new browser window will open with the provisioning form that must be filled out. Please provide the details from the installer into the new form when asked.





12. Once you are done with the provisioning form, you may now exit the installer by selecting “x” from the menu.
    a. Once the form is reviewed and the provisioning in completed, you will be contacted when the application is available for use.
    b. You will be able to access your instance of External365 using the URL you provided earlier on App Registration step.
    c. To grant access to other members of your organization to be able to access external365 to create and manage external users, place these users in either the Admin Group or Scope Managers groups via Azure Active Directory. They will be able to login with their normal Microsoft 365 Credentials when accessing the URL.

Appendix A Scoped Permissions

The purpose of scoped permissions is to provide separation between the tenant operators of different groups of users. For example: given a large community of external users in a company's Azure tenant, each user is specifically associated with a company division. Each of those divisions has one or more operators who is tasked with managing the users associated with their division.

Additionally, there are several operators who are allowed to manage users associated with multiple divisions. This scenario is accommodated by enabling scoped permissions and assigning scopes to operators. This is done by creating groups with the names of the scope in Azure (or in AD if using ADFS). The operators for that scope are made members of the group. In the Tenant permissions configuration for External365, the tenant is "Enabled for Scoped Permissions" and the names for each scope are added to the scoped permissions list. In the example above, assuming three divisions. We would create three security groups in Azure (or in AD using ADFS) named "Engineering", "Sales" and "Training". Operator one would be a member of "Engineering". Operator two would be a member of "Sales" and operator three would be a member of all three groups. The effect would be that operator one would only be able to see, manage and add users to the scope "Engineering", operator two would be similarly restricted to "Sales" and operator three could manage all three user scopes.

External365 Scoping Views