Journyx/PX App Registration Instructions for Microsoft Azure

Journyx/Journyx PX 12.x: Updated December 17, 2019

This document describes the process for registering a Journyx server in your Microsoft Azure® portal to grant access to Single Sign-On (SSO) or Exchange calendars and tasks for the Suggestions feature in Journyx. This process should be performed by a member of your IT staff whose has permissions to create App Registrations in your Azure portal.

Requirements

Before you begin, you need to gather the following information or requirements:

1. A license key enabling SSO/Exchange Integration. Contact your Journyx Sales Representative.
2. The Journyx server URL – referred to as YOUR_URL below.
   Important: Please note that your Journyx site should be using SSL (TLS encryption); otherwise, malicious users with access to your network can violate protocol security. That means the Journyx server URL should have the https:// prefix.
3. An administrative login on the Journyx server.
4. Access to your organizations' Azure Portal with sufficient permission to create App Registrations.
5. Decide if you want the Journyx server to use Azure Single Sign-On (SSO). Users will be signed into the Journyx server through their organization account via Microsoft Azure.
    1. **Important: Use of SSO is optional, but if you are planning to use it, you must ensure that all of your Journyx user accounts have their Username (login ID) field set to the same Azure Username (UPN) field as their accounts in your organization's Azure Portal** (or their home organizations if allowing multiple tenants). Often the Username (UPN) field is set to an email address but that is not required.
    2. If you want to use Single Sign on using your Exchange accounts and have Journyx user logins set to the user's Azure Username, you can enable the SSO at this point. For this you have to login to the server as the USER THAT INSTALLED JOURNYX and issue the following command.

       ```
       setkey AAD_USE_SSO=Yes
       ```

       - If you have a Windows server, use the Start->Journyx->Journyx Command Line Prompt to issue this command.
       - If you are using a Linux server, go to the Journyx install directory and source the setup file. Then issue this command.
       - If you are a Journyx Cloud customer, you will need to contact Journyx Support for this step.
6. Decide if you want to use the Journyx Suggestions feature. This allows entry screen users to import entries from Exchange Calendar events and Exchange Tasks.

    1. **Important: Please note that this feature only works if the Exchange Server is in the cloud (as with Office 365), or it is in a hybrid cloud/local setup. It does not work with a purely local Exchange Server or Microsoft Outlook client software locally installed.**
7. Decide if you want to allow multiple Azure tenants (organizations) access to this application (also known as multi-tenant access). For example, you administer a single Journyx server and wish to allow users from multiple Azure domains to sign in with SSO and/or retrieve Exchange Calendar events.
    1. You need to gather the GUID (tenant Directory ID) of each tenant you wish to allow access to your Journyx server.
    2. You can obtain the tenant GUID in one of two ways.
        1. Go back to the top-level Microsoft Azure Dashboard. Find the Azure Active Directory link and select it. Then select Properties. Your tenant GUID will be labeled "Directory ID".
        2. The second method, which can be accessed directly from the App Registrations area, is to look at the Endpoints panel of the App Registrations screen. The first component of each URL (after the domain) is the tenant GUID – an alphanumeric code like 83db927a-db55-44ba-82ef-25aa3e32342f
8. Decide if you need to use the Azure AD version 1 endpoint or the version 2 endpoint.
    1. The v1 endpoint is recommended at this time and these instructions mainly assume use of the v1 endpoint. The v2 endpoint is considered beta level by Microsoft at the time of this publication.
    2. Some differences in the setup process with the v2 endpoint are noted in the section at the end.

Azure Portal Registration Instructions (v1 endpoint)

1. In Azure Portal (https://portal.azure.com), go to the "App registrations" panel.
2. Click "New Registration"
    1. Give the app registration a name such as "Journyx". This name will appear on the Microsoft sign-in screen to help users identify which product/service they are signing into.
    2. Choose a "Supported account type"
        1. If you wish to allow multiple Azure tenants (organizations) access, be sure to select "Any Azure-AD directory - Multitenant"
    3. Click Register
3. Once the new App Registration has been completed, click on Overview
    1. Choose "Add new Redirect URI"
        1. Add the following WEB Redirect URI
           YOUR_URL/jtcgi/r/adlogin/token
           YOUR_URL/jtcgi/r/adlogin/sso
           YOUR_URL/jtcgi/wtlogout.pyc

Be sure to replace YOUR_URL/ with the actual URL, e.g. https://journyx.example.com/

2. Scroll down and set the Logout URL as follows: **YOUR_URL/jtcgi/wtlogout.pyc**

   Be sure to replace YOUR_URL/ with the actual URL, e.g. https://journyx.example.com/jtcgi/wtlogout.pyc
3. Under "Implicit grant", check the box for "ID Tokens"
4. **Click SAVE**

2. Sign on URL should be your basic server URL, for example: YOUR_URL = https://journyx.example.com

4. Branding
   1. If desired, you can set other properties here that will impact the end user experience. The name and logo image will be shown in sign-on screens.
5. Certificates & secrets
   1. Click "New Client Secret"
   2. Type a description, e.g. "Production Journyx Server". Then select a duration. (Note that making use of key expirations is recommended for security, but you will have to come back and generate a new key here at some point.)
   3. Click **Add**. ***A generated value will then be displayed. **Copy the value and save it somewhere** as it will not be shown again.***
6. API Permissions
   1. There should already be one permission automatically granted: **Sign in and read user profile**. If you are only using SSO and not Suggestions, this is the only permission you need. If you are not using SSO you need this **Sign in and read user profile** permission, plus the ones in the next step.
   2. If you are opting to use Exchange Calendar/Task Suggestions on Journyx entry screens, you must grant permission to read the calendar and tasks. Leave the default "Sign in" permission there and click the Add button. Choose **Microsoft Graph**, then click **Delegated permissions**.
      1. You will see a long list of Graph permissions. Select the following:
         Calendars > Calendars.Read.Shared
         Tasks > Tasks.Read.Shared
      2. Make sure those two are checked, then click the Add permissions button at the bottom.
      3. Note that if you do not wish shared tasks/calendars to be viewed through Journyx, you can opt for the version of these permissions which doesn't include shared items.
   3. Once the permissions are added, you must Grant Permissions by clicking the **Grant admin consent for ...** button
7. To complete the registration, you need to tell the Journyx server about it. Collect the following pieces of information from the "Overview" pane:
   1. **Application (client) ID**: This looks like groups of random numbers and letters (a GUID).

    2. **Directory (tenant) ID**: It will look like: add2a70c-d01e-47db-8521-739c77b1b0b2. If you are using multi-tenanted access, you need to collect the GUID of each tenant.
    3. The **Client Secret** you generated in step 5 above.
    4. The Azure Identity Provider URL, which should always be https://login.microsoftonline.com
8. Log into your Journyx site as an administrator. Then go to **Settings** → **System Settings** → **Security Settings**.
9. Scroll down to the bottom of the page and enter the 4 pieces of information from above. Then click Save.
    1. Since we used the v1 portal to register this application, make sure the Journyx option "Use the v2.0 Azure Endpoint" is **not** checked.
10. After you enter the information, there is a button to **Save Settings and Test Azure Connection**.
    1. Please note that this will only test that the provided Azure credentials are valid.
    2. In particular, it does **NOT** test whether all aspects of the Azure Portal app registration are correct, such as the Reply URLs or granted permissions.
11. If you wish to use Single Sign-On, there is a separate checkbox for that. Please contact Journyx support for additional guidance regarding Single Sign-On (SSO) before engaging this option.
12. Access to the Calendar/Task Suggestions feature must be enabled by an administrator using the checkbox on the Entry Screen Configuration. See the in-product Help for Configuration > Entry Screens for detailed information for how to grant individual users access to use Suggestions.
13. In addition, each individual user can opt in/out of Suggestions via a checkbox on their Preferences screen. See the in-product Help for Preferences > Entry screens for more information.
14. If you are not using SSO, individual users will need to link their Azure account to Journyx by using the provided "Link Account" button on either the Time Entry Screen or on the Entry Screen Preferences page. See the in-product Help for Preferences > Entry screens for more information.
15. In the event that SSO has been enabled and some situation or identity requires login using Journyx internal credentials, the site can be accessed bypassing the SSO by using a URL with the nosso=1 GET argument. E.g.

https://your_sitename.apps.journyx.com/jtcgi/wtlogin.pyc**?nosso=1**

Azure AD Endpoint v2 Support

Currently Microsoft considers the v2 Azure endpoint to be in beta status. Therefore, we recommend using the v1 endpoint as documented above. However, if you wish to use the v2 endpoint, the process is mostly the same, with some differences to note (below). You will still need to go through the v1 setup instructions above.

- The v2 endpoint supports incremental user consent to permissions.

        - For example, users might only grant basic profile permissions for an initial sign-in. If they decide to use the Suggestions/Calendar features later on, they will be prompted for consent to additional Calendar permissions at that time.
        - Under the v1 endpoint, all needed permissions must be granted up-front by the IT administrator when registering the app.
        - You can configure Journyx to require all permissions up-front even in the v2 endpoint (see below) or ask incrementally.
- The v2 endpoint is required to support personal, non-corporate Microsoft accounts, or outside accounts federated to a Microsoft account via OAuth (e.g., sign-in with Facebook or Google.)
- As with the v1 endpoint, you must designate the list of Tenants IDs (organizations) who are allowed to connect to your Journyx server.
- Application registrations for the v2 endpoint must be done at a separate portal:
    - https://apps.dev.microsoft.com/
- The registration process for this new portal is largely similar, except:
    - You must add the "Web" platform.
    - "Allow Implicit Flow" must be checked under Web platform options.
    - The following permissions should be added:
    - Calendars.Read.Shared
    - Tasks.Read.Shared
    - User.Read
    - email
    - offline_access
    - openid

profile

- Inside Journyx System Settings, the "Use v2 Endpoint" option must be checked.
    - If the Journyx site has users who have already interacted with the v1 endpoint, they will be forced to sign in again on their next access.
- There is another system setting to control whether calendar permissions are requested incrementally on the v2 endpoint or up-front. If you choose incremental permissions, users will be required to sign in again (and authorize the permissions) when accessing a calendar import feature.