Project2Planner Security and Trust

What the add-in connects to, what it stores and what it transmits

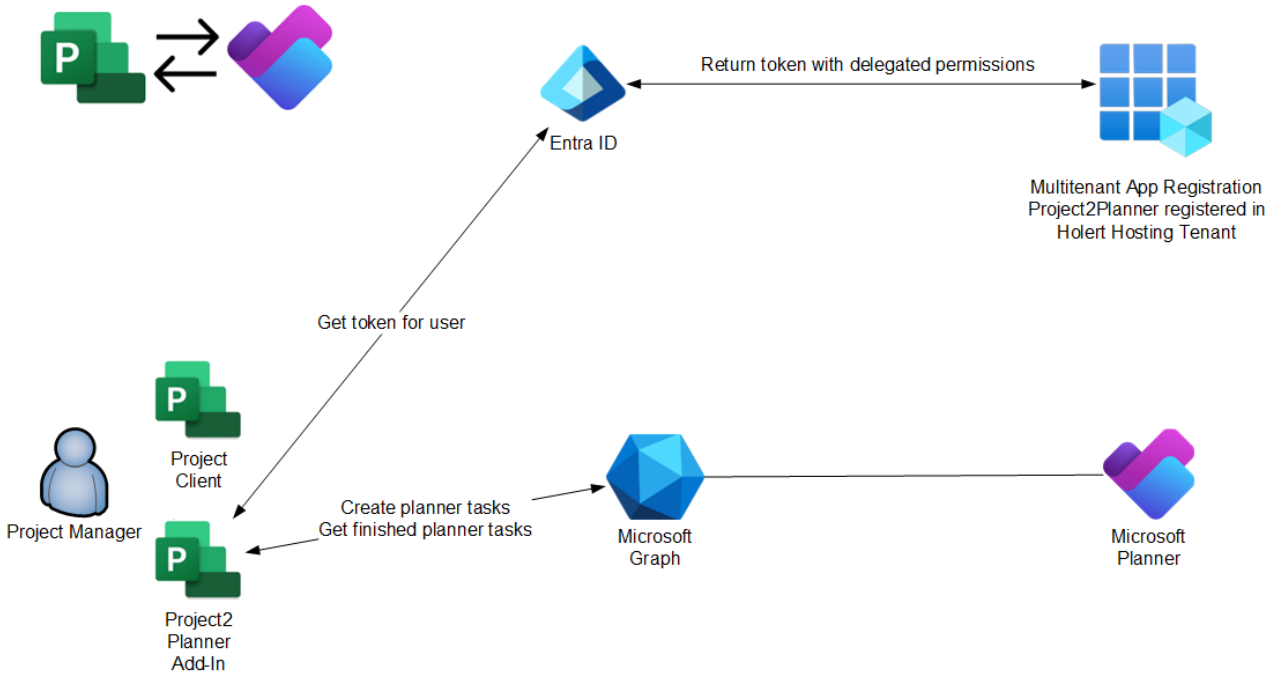
Contents

Contents 2
1. Overview 3
2. Stored data 3
2.1 On the computer of the user 3
2.2 In the Holert tenant 4
2.3 What never leaves the computer 4
3. Permissions 4
3.1 User.Read 4
3.2 User.ReadBasic.All 4
3.3 Tasks.ReadWrite 5
3.4 Consent 5
4. Network connections 5
5. Licensing 5
6. Data protection 6
Related documents 6
Contacts 6

1. Overview

Project2Planner is a VSTO add-in that runs inside Microsoft Project. It creates tasks in Microsoft Planner from the tasks a user selects in a project, and writes the progress of those Planner tasks back into the project.

The add-in signs the user in against Microsoft Entra ID and works with the access token of that user. Everything it reads or writes in Planner happens with the permissions of the signed-in user; there is no service account and no background service.



2. Stored data

2.1 On the computer of the user

The following is written to the local app data folder of the signed-in user, %localappdata%\Project2Planner\:

- **Token cache —** holds the refresh token after the sign in, so that the user does not have to sign in on every use.
- **Configuration file —** the settings of the add-in, above all the names of the fields it reads in Microsoft Project.
- **Log files —** one text file per session with runtime information, warnings and error messages. They are deleted automatically after 90 days and are not sent to Holert.

- **Licence cache —** the result of the licence check, encrypted with the Windows Data Protection API for the signed-in user. It lets the add-in keep working while the licence file is temporarily unreachable.
- **Evaluation period file —** records when a user first started the add-in without being licensed, so that the evaluation period can be counted.

2.2 In the Holert tenant

- **Telemetry —** the add-in reports runtime information to Azure Application Insights in Germany West Central. Each entry carries the Entra tenant id, the domain part of the user principal name, the add-in version and a one-way hash of the Entra object id of the user. No user principal name, display name or mail address is transmitted. Telemetry is retained for 365 days and deleted afterwards.
- **Licence files —** one file per customer with the tenant id, the customer name, the expiry date and one-way hashes of the licensed users. The files hold no mail addresses.

2.3 What never leaves the computer

No content of a project is transmitted. Task names, resource names, notes, dates, links and the name of the project file stay on the computer of the user and in Planner, where the user puts them. The synchronisation report names tasks and resources, and so does the log file, but both are local; telemetry carries only counts per outcome and per reason.

3. Permissions

Application id: bd5bd2b1-2802-4629-b5df-3f03c19bb074

The add-in asks for three delegated permissions. Delegated means that it can never do more than the signed-in user may do.

3.1 User.Read

Sign in and read the profile of the signed-in user. Needed so that the user can authenticate against Microsoft Graph, and for the user principal name the licence check compares against.

3.2 User.ReadBasic.All

Read a basic set of profile properties of other users in the organisation on behalf of the signed-in user: id, display name, user principal name, given name, surname, mail address, open extensions and photo.

Needed to resolve the resource names of a project to accounts, so that the created Planner tasks can be assigned to the right people. Without this permission, tasks are created without an assignee.

3.3 Tasks.ReadWrite

Create, read, update and delete the tasks and task lists of the signed-in user. Needed to read Planner plans and to create and update Planner tasks on behalf of the user.

3.4 Consent

Where a tenant does not let users consent to applications themselves, an administrator allows the app once with this link: https://login.microsoftonline.com/common/adminconsent?client_id=bd5bd2b1-2802-4629-b5df-3f03c19bb074&redirect_uri=https%3A%2F%2Fwww.holert.com%2Fen%2Fproject2planner%2Fadmin-consent. Nothing else must be set up in the tenant of the customer.

4. Network connections

The add-in talks to these addresses, all over HTTPS. Where a proxy is in use, it uses the proxy configured in the add-in.

Address	Purpose	When
login.microsoftonline.com	Sign in and token refresh against Microsoft Entra ID	At the first use and whenever the token expires
graph.microsoft.com	Reading plans and buckets, creating and updating Planner tasks, resolving resources to accounts	During a synchronisation
holerthosting.blob.core.windows.net	The licence file of the own tenant, and the setup and the updates of the add-in	At start up and when the add-in updates itself
germanywestcentral-1.in.applicationinsights.azure.com	Telemetry	During use

5. Licensing

Project2Planner is licensed per named user. After the sign in, the add-in retrieves the licence file of the signed-in tenant from https://holerthosting.blob.core.windows.net/project2planner/Licenses/ and compares a one-way hash of the user principal name against the list in it.

The request is a plain HTTPS GET whose address contains the tenant id. Nothing else leaves the computer for this check, and no information about the project or its tasks is involved.

The check uses only the token the user has already signed in with. It needs no additional permission, no consent by an administrator and no configuration in the customer tenant.

A user who is not licensed can work for an evaluation period of 30 days; after that, synchronisation is refused. If the licence file cannot be reached, the last retrieved result stays valid for 14 days, so a short

outage does not stop anybody from working. Working with the project itself is never affected by the licence check.

6. Data protection

- The add-in processes the content of a project only on the computer of the user and in the Microsoft 365 tenant of the customer.
- The licence files published by Holert hold one-way hashes instead of mail addresses, so a file that somebody retrieves contains no personal data.
- Telemetry identifies a user only by a one-way hash of the Entra object id, and the organisation by the tenant id and the mail domain.
- Local log files are deleted after 90 days, telemetry after 365 days.
- There is no Holert service that the add-in signs in to, and no Holert account that has access to customer data.

Related documents

- **Admin Guide —** Project2Planner Admin Guide, consent, installation and configuration
- **User Guide —** Project2Planner User Guide
- **Setup —** Download of the add-in

Contacts

- **Support —** Holert service desk, support@holert.com
- **Licensing —** sales@holert.com
- **Product owner —** Maximilian Münst, Holert GmbH