Why is it safe to use STOCKHOLM?

STOCKHOLM is the core product of ESUPS (Emergency Supply Pre-positioning Strategy), a project funded by USAID/BHA, hosted by Welthungerhilfe and led by a Steering Group consisting of key humanitarian logistics actors.

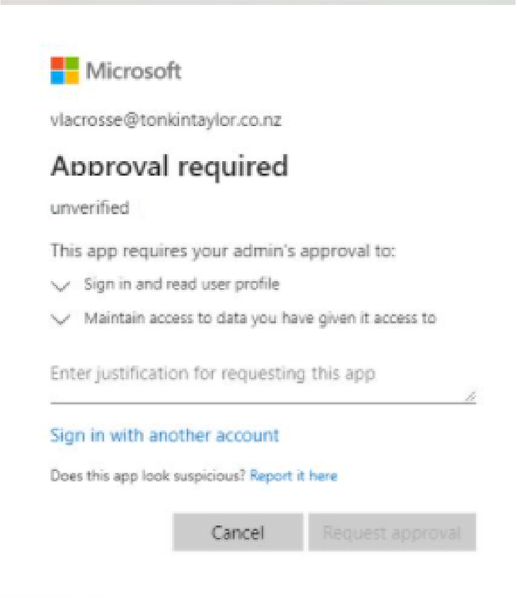
In addition:

- STOCKHOLM is managed by Welthungerhilfe (WHH) and hosted on two servers located in Europe;
- It is being developed in accordance with GDPR requirements;
- It is developed by Tonkin + Taylor, a registered company, who specialise in agile post-disaster website development.

Microsoft Azure AD Authentication

STOCKHOLM uses Microsoft Azure AD login as one of the authentication methods, which is a cloud-based identity and access management service managed by Microsoft. This app requires your internal IT administrator's approval to use it as a sign-in and to read the user profile (e.g., email and username).

Here is a screenshot of the Microsoft required approval pop-up that appears:



Microsoft

vlacrosse@tonkintaylor.co.nz

Approval required

unverified

This app requires your admin's approval to:

Sign in and read user profile

Maintain access to data you have given it access to

Enter justification for requesting this app

Sign in with another account

Does this app look suspicious? Report it here

Once tenant-wide approval has been granted by your internal IT administrator, anyone from that same agency will be able to access the STOCKHOLM website going forward. Individual approval for different users within the same agency is not required.

Providing approval to the app permission request

Steps required to approve the app permission request:

1. Sign in to the Azure portal using an Azure AD user account with one of the following roles:
   - Global Administrator or Privileged Role Administrator, for granting consent for apps requesting any permission, for any API.

- Cloud Application Administrator or Application Administrator, for granting consent for apps requesting any permission for any API, except Azure AD Graph or Microsoft Graph app roles (application permissions).
- A custom directory role that includes the permission to grant permissions to applications, for the permissions required by the application.

2. Select Azure Active Directory, and then select Enterprise applications.
3. Select the application to which you want to grant tenant-wide admin consent, and then select Permissions.
4. Carefully review the permissions that the application requires. If you agree with the permissions the application requires, select Grant admin consent.

For more information, please refer to:

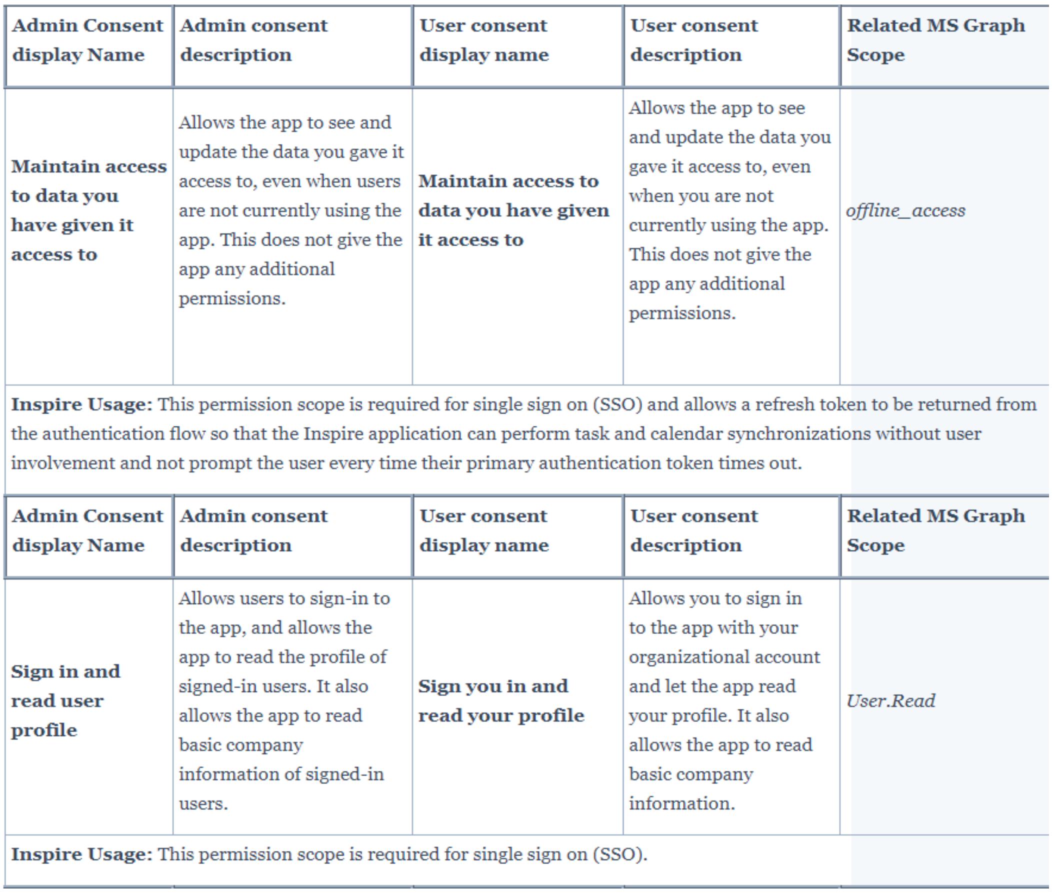
Grant tenant-wide admin consent to an application - Microsoft Entra | Microsoft Learn

More Information on what the Admin is asked to approve

The app requires the admin's approval to:

1. Sign in and read your user profile
2. Maintain access to data you have given it access to

Below is an explanation of what that entails.



Admin Consent display Name	Admin consent description	User consent display name	User consent description	Related MS Graph Scope
Maintain access to data you have given it access to	Allows the app to see and update the data you gave it access to, even when users are not currently using the app. This does not give the app any additional permissions.	**Maintain access to data you have given it access to**	Allows the app to see and update the data you gave it access to, even when you are not currently using the app. This does not give the app any additional permissions.	*offline_access*
Inspire Usage: This permission scope is required for single sign on (SSO) and allows a refresh token to be returned from the authentication flow so that the Inspire application can perform task and calendar synchronizations without user involvement and not prompt the user every time their primary authentication token times out.				

Admin Consent display Name	Admin consent description	User consent display name	User consent description	Related MS Graph Scope
Sign in and read user profile	Allows users to sign-in to the app, and allows the app to read the profile of signed-in users. It also allows the app to read basic company information of signed-in users.	**Sign you in and read your profile**	Allows you to sign in to the app with your organizational account and let the app read your profile. It also allows the app to read basic company information.	*User.Read*
Inspire Usage: This permission scope is required for single sign on (SSO).				