

USER GUIDE

SECURITY

STOCKHOLM is a platform of the [Emergency Supply Prepositioning Strategy \(ESUPS\)](#).

ESUPS is hosted by [Welthungerhilfe](#) (WHH) and led by a Steering Group of key humanitarian actors.

STOCKHOLM has been developed by [Tonkin + Taylor](#), a registered company specialising in agile post-disaster website development. It is managed by WHH and hosted on two servers located in Europe.

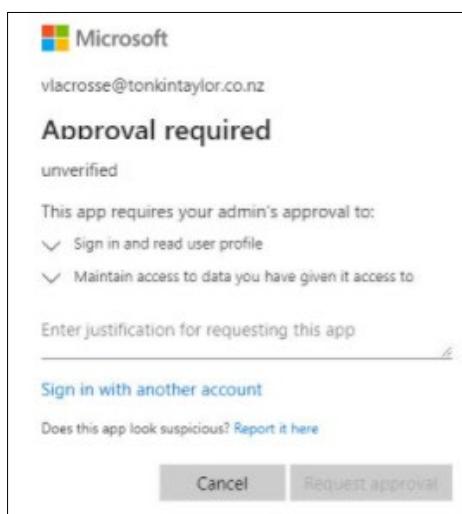
STOCKHOLM adheres to the requirements of the General Data Protection Regulation (GDPR).

MICROSOFT AZURE AD AUTHENTICATION

STOCKHOLM uses Microsoft Azure AD login as one of the authentication methods. It 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 method, and to read the user profile (e.g. email and username).

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



Once tenant-wide approval has been granted by your internal IT administrator, anyone from that same agency will be able to access STOCKHOLM.

Individual approval for different users within the same agency is not required.

The App requires the IT administrator's approval to:

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

The table below explains further.

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.	<i>offline_access</i>
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.				
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.	<i>User.Read</i>
Inspire Usage: This permission scope is required for single sign on (SSO).				

HOW TO PROVIDE APPROVAL

1. **Sign in to the Azure portal** using an Azure AD user account with one of the following roles:
 - a) Global Administrator or Privileged Role Administrator, for granting consent for apps requesting any permission, for any API.
 - b) 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).
 - c) 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.
5. If you agree with the permissions the application requires, select **Grant admin consent**.

MORE INFORMATION

[Grant tenant-wide admin consent to an application - Microsoft Entra](#)