Teams messages: setting it up

CTW Herald 0.10.0 · for whoever administers your Microsoft 365, and for the operator

Herald can show the media account's recent **Teams chats** in its own window, say when a message has arrived, and bring an attached presentation into the library with one press. Before it can, whoever administers the church's Microsoft 365 has to **register CTW Herald once**. It is free, takes about ten minutes, and nothing is installed in Microsoft 365.

This page is for that administrator. The last section is for the operator.

> **Checked against a stand-in only.** Everything below was built and checked against a small program that plays Microsoft's sign-in service and Microsoft Graph. No real Microsoft 365 organisation has been involved, so these steps are written from Microsoft's documentation, not from doing them on your tenant. If a screen is named differently, or a step refuses, tell us what it said: section T of REHEARSAL-CHECKS.md.

What Herald will be allowed to do

Herald signs in **as the media account**, in the web browser, on Microsoft's own page. It then asks Microsoft Graph for these four **delegated** permissions, which means "what this signed-in person can already do", never more:

Permission	What Herald uses it for
`Chat.Read`	List the chats the media account is in, and read their recent messages
`Files.Read.All`	Open a file someone attached to a message. Delegated, this is "files the media account can open", not everybody's files
`offline_access`	Stay signed in between Sundays without asking again
`User.Read`	Show whose account is signed in

Herald **cannot** send, edit or delete a message, mark one as read, read channels, read anyone else's chats, or change a file. It asks for no permission that would allow it. There is **no client secret** and no password stored: Herald is a "public client" and proves itself with a one-time code each sign-in (PKCE).

Steps for the administrator

1. Open the **Microsoft Entra admin centre** (entra.microsoft.com) and sign in as an administrator.
2. Go to **Entra ID → App registrations → New registration**.
3. Fill it in:
   - **Name:** `CTW Herald`
   - **Supported account types:** *Accounts in this organizational directory only* (single tenant)
   - **Redirect URI:** choose the platform **Public client/native (mobile & desktop)** and type `http://localhost`

   Press **Register**.

4. On the registration's **Overview** page, copy two values. These are what the operator types into Herald. They are identifiers, not secrets:
   - **Application (client) ID**
   - **Directory (tenant) ID**
5. Go to **API permissions → Add a permission → Microsoft Graph → Delegated permissions**, and tick: `Chat.Read`, `Files.Read.All`, `offline_access` (and `User.Read`, which is usually there already). Press **Add permissions**.
6. Still on **API permissions**, press **Grant admin consent for (your organisation)**. If your organisation lets people approve apps for themselves this is not strictly needed, but it saves the media account being asked, and it is required if you have switched user consent off.
7. Do **not** create a client secret or a certificate. Leave **Allow public client flows** as it is (*No* is fine): Herald uses the ordinary browser sign-in.

Recommended, so that only the media account can use it:

8. Go to **Entra ID → Enterprise applications → CTW Herald → Properties**, set **Assignment required?** to **Yes**, and save. Then under **Users and groups**, add the media account.

That is all. Send the two IDs from step 4 to the media team.

If you use Conditional Access or multi-factor sign-in

Herald opens the sign-in in the computer's normal web browser, so your sign-in rules apply as they would for any web app, and the media account answers its usual second step there. Herald never sees the password or the code.

Taking it away again

- **On the media computer:** in Herald, *Media → Teams messages → Sign out*. The key that kept Herald signed in is forgotten.
- **In Microsoft 365:** delete the app registration, or remove the media account under *Enterprise applications → CTW Herald → Users and groups*. Herald notices at its next look, says the sign-in has been withdrawn, and stops asking.

Steps for the operator

1. In Herald, open **Media → Teams messages**.
2. Type the **Directory (tenant) ID** and the **Application (client) ID** from the administrator, and press **Save**. (Each is 36 characters: letters, digits and dashes.)
3. Press **Sign in to Microsoft 365**. Your web browser opens Microsoft's page. Sign in as the **media team's account**, agree to what it lists, and come back to Herald. If you close the browser without finishing, press **Cancel** in Herald and start again.
4. The panel now lists the last two weeks of messages. From here on Herald looks every 45 seconds.

What you will see afterwards:

- **Someone sends slides** (a PDF or PowerPoint file): a notice names the sender and the file, and the bottom of the window says *Teams: 1 new message*. Open the panel, press **Bring in**, then **Add to service**.
- **Someone sends a message with no slides:** in Rehearsal, a short notice; **On Air, only the count along the bottom changes**, so nothing pops up over you during a service.

- **The words of a message** are shown only in this panel on the control window. They are never sent to the projector, the stage display, the livestream, OBS, or a remote, and they are not saved to disk.

What is kept on the media computer

Only on this computer, in Herald's own settings file, and **never in a backup**:

- the two IDs;
- the name of the signed-in account;
- the key that keeps Herald signed in (a "refresh token"), **sealed by the operating system's key store** (Windows DPAPI, the macOS Keychain). If a computer has no key store, Herald says so in the panel and keeps the key unsealed: sign out on a shared computer;
- which attached files have already been brought in.

Messages themselves are held in memory while Herald is open and fetched again next time. A file fetched from Teams is kept only until it has been brought into the library, then removed.

When something goes wrong

Herald says	What it means
Those do not look like the IDs from the Microsoft Entra page	One of the two IDs is mistyped. Each is 36 characters with four dashes.
Microsoft says an administrator has to approve CTW Herald first	Step 6 (admin consent) has not been done, or the media account is not assigned (step 8).
Microsoft did not sign you in: …	Microsoft's own reason follows. Often the wrong account, or a redirect address other than `http://localhost` in step 3.
Teams: not connected along the bottom	Herald cannot reach Microsoft 365 just now. It keeps what it has, keeps trying, and nothing else in Herald is affected.
The sign-in has run out or been withdrawn. Sign in again.	The password changed, the administrator removed access, or it was unused for about three months. Press Sign in.
Herald can see the message but may not open the file	The sender's file is not shared with the media account, or `Files.Read.All` was not granted. Ask the sender to send it again, or save it from Teams by hand.

Where this comes from

- Listing chats: https://learn.microsoft.com/en-us/graph/api/chat-list
- Listing a chat's messages: https://learn.microsoft.com/en-us/graph/api/chat-list-messages
- Attachments on a message: https://learn.microsoft.com/en-us/graph/api/resources/chatmessageattachment
- Opening a shared file by its address: https://learn.microsoft.com/en-us/graph/api/shares-get
- Registering an app: https://learn.microsoft.com/en-us/entra/identity-platform/quickstart-register-app