Setting up Webhooks in WorkDrive using Custom Apps - help article

Enhance your organization's security, boost productivity, improve usability, and achieve much more with WorkDrive's Custom Apps!

As an admin or super admin of a WorkDrive team, you now have the ability to create and manage custom apps directly from the Admin Console. Custom apps enable you to create applications within your WorkDrive team to fulfill the distinct needs and preferences of either yourself or your organization.

Notes:

- Currently, WorkDrive utilizes custom apps to setup webhooks.
- You can create up to 10 custom apps for your WorkDrive team.

To create a custom app:

1. Sign in to your WorkDrive account as an admin or super admin.
2. Click **Admin Console** in the bottom-left corner.
   This will open the *Admin Console* window. The *Dashboard* tab will be selected by default.
3. Navigate to the **Apps** tab by clicking on it from the left pane. The *Apps* tab will appear on the right.
4. Click **+ Create a new custom app** in the top-right corner. This will open the *Create new app* window.
5. Fill in the *Create new app* form with the details such as **App name**, **Description**, and **Client-id**.

   Note: Client-ID will only be generated when you register your application with the Zoho developer console. Without client-id you can't be able to create a custom app in WorkDrive.

   Follow the below steps to register your application:

   i. Go to the Zoho API Console and click **Get Started**.

   ii. Select **Server based applications** as the client type.

   iii. Provide the required details to register your application for the client type you chose:

- **Client Name:** The name of your application you want to register with Zoho.
- **Homepage URL:** The URL of your client's home page.
- **Authorized Redirect URIs:** A valid URL of your application that Zoho Accounts redirect you to with the grant token after a successful authentication.

iv. Click **CREATE** to receive the following credentials:

- **Client ID:** The consumer key generated from the connected app.
- **Client Secret:** The consumer secret generated from the connected app. Learn more on registering your application with the Zoho developer console

6. Click **Create**. You can configure up to five webhooks for the created app.

   Note: A unique secret key will be generated upon app creation, which is used for webhooks authentication purposes.

View and manage custom apps in WorkDrive

As an admin or super admin of your WorkDrive team, you have the ability to view and manage all the custom apps associated with your team. Navigate to the **Admin Console** and access the **Apps** tab. In the **Apps** tab, you will find a list of all the custom apps that have been created for your WorkDrive team.

From here, you'll be able to perform the following actions:

- To update the app details: Click on the app of your choice. This will open the corresponding *App details* page, where you can edit the app's name and description according to your requirements.
- To delete the custom app: If you want to remove a custom app from your WorkDrive team, you can do so by clicking the **Delete app** button located at the bottom of the *App details* page for the specific app you wish to remove.

Webhooks

Enabling Webhooks in WorkDrive allows you to receive real-time notifications for file, folder, team folder, and org-based events, sent to the external app (URL you specify) whenever these events occur. This eliminates the need for continuously monitoring the

file/folder and enables you to promptly act upon the received information.

Note: You can create up to 5 webhooks for each app.

To configure webhooks:

Once the custom app is created, you can create and configure webhooks. Follow these steps to configure webhooks for your custom app:

1. Click **Admin Console** in the bottom-left corner.
   This will open the *Admin Console* window. The *Dashboard* tab will be selected by default.
2. Navigate to the **Apps** tab by clicking on it from the left pane. The *Apps* tab will appear on the right with the list of all your custom apps.

3. Choose the custom application for which you want to configure webhooks. This will open the *Custom app* window. The *App details* tab will be selected by default.
4. Switch to the **Webhooks** tab and click **Create new webhook**. This will open the *Create new webhook* window.
5. Provide the webhook name and description in the respective fields.

6. Enter the Endpoint URL to which you want to receive notifications.
   Note: Make sure the URL is active and capable of processing webhooks.

7. Select the trigger event (File, Folder, Team Folder, Org based) and specify the event's target location. Click here to learn more about the event types available in WorkDrive
8. Click **Create Webhook**. You will now receive notifications at the specified URL whenever the specified event occurs in WorkDrive.

Webhooks payload

The webhook payload refers to the response sent to the specified URL whenever the configured trigger event takes place in WorkDrive.

Below is an example of Webhooks payload response for the file creation trigger event:

```
{
  "data": [
    {
      "resource_info": {
        "parent_id": "lvwg28f94012d0a484328b6175c6da296b433",
        "resource_id": "ep19987f95a0161684d8ea1b3161f16e41e38",
        "resource_name": "Default App Migration Report.csv",
        "base_parent_id": "lvwg28f94012d0a484328b6175c6da296b433",
        "status": 1
      },
      "share_info": {
        "role": "7",
        "shared_type": "14",
        "shared_by": 5608329,
        "shared_status": 14,
        "shared_to": "111118000000038003"
      },
      "association_info": {
        "entity_value": "Guna",
        "entity_label": "record",
        "module": "Leads",
        "entity_id": "EID0000001011"
      },
      "event_id": "839687000000338003",
      "event_type": "file_create",
      "app_key": "1000.0UUMEY8E1WWRF26GF0XIHRLKDHHFNH",
      "webhook_id": "ep19987f95a0161684d8ea1b3161f16e41e38-
839687000000335005",
      "module_name": "",
      "portal_id": "638722",
      "team_id": "lvwg26329e83825ed4815b2e685e1781d6728",
      "type": "event_callback",
      "event_time": 1600422715262,
      "event_by": 61184597
    }
  ]
}
```


Webhook Authentication

To enhance security, WorkDrive employs a method called Webhook Authentication, which involves signing each Webhook request using HMAC-SHA256 (Hash-based

Message Authentication Code with SHA-256). This is a symmetric signing mechanism where both WorkDrive and your application share a secret key to generate and validate HMAC signatures.

When WorkDrive sends a Webhook request, it includes an HMAC signature in the **X-ZWDWebhook-Signature** header of the request. Your application receives this request with the Webhook payload in the request body and the signature in the request header. It then follows these steps:

- It uses the shared secret key to sign and encode the Webhook payload.
- It compares the resulting signature with the value sent in the **X-ZWDWebhook-Signature** header of the Webhook request.

If the two signatures match, the request is considered legitimate and that it hasn't been tampered with between your application and WorkDrive. This mechanism ensures the security and integrity of Webhook communications.

Creation of HMAC Signature

To create HMAC Signature, WorkDrive combines JSON WEB SIGNATURE (JWS) header and webhook payload as a UTF-8 string and then hashed the result using HMAC SHA-256 algorithm. The JWS header is as follows:

```
{
"alg": "HS256",
"typ": "JWT"
}
```

It includes the following:

- **alg:** HS256 algorithm is used to generate hashing signature.
- **typ:** The typ (type) header parameter is used to declare the type of the signed content.

Refer here for webhook Payload Format

Steps for Creation of webhook Signature

1. The JWT header and Webhook payload will be individually Base64 encoded, then joined together with a full stop “.”

2. Webhook signature is generated by hashing the Base64 encoded header and Base64 encoded Webhook Payload using SHA-256 algorithm and encode the resulting signature using Base64 encoding.
3. The three components, which are the Base64 encoded header, the Base64 encoded webhook payload, and the Base64 encoded HMAC SHA-256 signature, are concatenated together with full stops "." as separators.

WorkDrive includes this signature as a header in the HTTP POST back to the webhook request, which appears as follows:

X-ZWDWEBHOOK-SIGNATURE: <base64 header>.<base64 body>.<base64 HS256(<base64 header>.<base64 body>)

Verify the HMAC Signature

Once your app receives a Webhook request containing an HMAC Signature in the header, it should perform a verification process. This involves attempting to recreate a signature by hashing the webhook payload using a shared secret key.

Note: All webhooks configured for a custom app use the same secret key for verifying the signature.

To obtain the secret key:

1. Click **Admin Console** in the bottom-left corner.
   This will open the *Admin Console* window. The *Dashboard* tab will be selected by default.
2. Navigate to the **Apps** tab by clicking on it from the left pane. The *Apps* tab will appear on the right with the list of all your custom apps.
3. Choose the custom app for which you need to copy the secret key. This will open the *Custom app* window and *App details* tab will be selected by default.

   Info: If you're already on the webhooks page, simply click the **View secret key** link on the right. This will take you to the corresponding **App details** tab.

4. Navigate to the secret key field within the *App details* tab and copy the value. You can now use the secret key for verifying webhooks.

To verify the webhooks:

1. Extract the webhook payload from the received webhook request.
2. Compute an HMAC signature for the webhook payload using the shared secret key. This involves using the SHA-256 hashing algorithm.
3. Encode the computed HMAC signature using the Base64 encoding mechanism.
4. Extract the signature from the **X-ZWDWEBHOOK-SIGNATURE** header of the webhook request.
5. Ensure that the computed Base64 encoded SHA-256 hash of the webhook payload matches the value provided in the **X-ZWDWEBHOOK-SIGNATURE** header of the webhook request.

   If there is a mismatch, reject the webhook request.

Note: Make sure that both the creation and verification mechanisms use the same encoding mechanism to ensure consistency and accurate verification of the webhook data.

View and manage webhooks in WorkDrive

As an admin or super admin of your WorkDrive team you'll be able to view and manage webhooks for each custom app from the Admin Console.

1. Click **Admin Console** in the bottom-left corner.
   This will open the *Admin Console* window. The *Dashboard* tab will be selected by default.
2. Navigate to the **Apps** tab by clicking on it from the left pane. The *Apps* tab will appear on the right with the list of all your custom apps.
3. Choose the custom application for which you want to make changes to the webhooks. This will open the *Custom app* window. The *App details* tab will be selected by default.
4. Switch to the **Webhooks** tab to access the complete list of configured webhooks for your custom app, along with the respective manage options:
   - To enable or disable a webhook: Simply toggle the ON/OFF switch provided in the webhooks tab.
   - To modify the name and description of a webhook: Click the **More actions** icon and choose the **Edit** option.
   - To delete a webhook: Click the **More actions** icon and select **Delete**.

Confirm the deletion by clicking **Delete** again in the confirmation dialog box.