Google Drive Integration Troubleshooting

Last Modified on 10/28/2026 4:42 pm CDT

This tool is available with Campus Learning Suite.

This article provides instructions for troubleshooting Google Drive integrations. See the Google Drive Configuration article for instructions on configuring a new connection.

Many issues with Google Drive integration are due to minor misconfigurations during the initial setup of a district's Google project in the Google Development Console. If you're experiencing issues with your Google Drive integration, review the configuration steps below as a starting point.

First, Access the Correct Google Project

To successfully troubleshoot an integration, make sure you're using the correct admin account and Google project.

Navigate to console.developers.google.com and log in using the same Google Admin account that was originally used to set up the integration with Infinite Campus. Verify at the top of the screen that the Google project initially created for your district's Infinite Campus/Google Drive integration is selected.

If your district no longer has access to this Google project, such as if the Google admin who initially set up the Google Drive integration is no longer in that role and no longer has a Google account, you may need to recreate the Google project from scratch instead. Google Workspace Support may be able to give guidance on how to proceed in that scenario.

Common Configuration Issues

Check the API Key

1. Select **Credentials**.
2. Under *API Keys*, you should see one record. Select the **Name** (ex. "API key 1") to open the Edit API Key screen.
3. Under *Application restrictions*, ensure **Websites** is selected.
4. Under *Website restrictions* (not API restrictions), you should see at least one entry. (If you do not, select **Add**.) Ensure this Website Restriction value is correct. Please check this value carefully. It must be 100% correct. If it is even one character off, your integration will not behave correctly.

All of the following must be true:
- It must be the first part (domain name) of your Infinite Campus URL
- It **must** start with **https://**
- It must **not** include anything after the top-level domain (.com, .org, .edu) of your Infinite Campus URL.
- It must **not** have an extra space before or after the value
- It must **not** have a **/** (slash) at the end of the value

For example: if your full Infinite Campus URL is https://example.infinitecampus.org/campus/mydistrict.jsp, this value must be just https://example.infinitecampus.org **NOT** https://example.infinitecampus.org/campus/mydistrict.jsp

5. If the value is not correct, edit it and Save.

Check the OAuth 2.0 Client ID

1. Navigate back to the **Credentials** screen
2. Under **OAuth 2.0 Client IDs**, locate the record with a type of *Web application* and select the **Name** (ex. "Web client 1") to view the Client ID for Web Application screen.
3. There should be at least one entry under *Authorized Javascript Origins*. (If not, select **Add URI**.) Ensure this value is correct. Please check this value carefully. It must be 100% correct. If it is even one character off, your integration will not behave correctly.

   All of the following must be true:
   - It should be the same value as discussed in the Check API Key section above.
   - It must be the first part (domain name) of your Infinite Campus URL.
   - It **must** start with **https://**
   - It must **not** include anything after the top-level domain (.com, .org, .edu) of your Infinite Campus URL.
   - It must **not** have an extra space before or after the value
   - It must **not** have a **/** (slash) at the end of the value

   For example: if your full Infinite Campus URL is https://example.infinitecampus.org/campus/mydistrict.jsp, this value must be just https://example.infinitecampus.org **NOT** https://example.infinitecampus.org/campus/mydistrict.jsp
4. If the value is not correct, edit it and Save.

Check the Consent Screen

1. Navigate back to console.developers.google.com and log in as described in the Access section above.
2. Select **OAuth Consent Screen**.
3. Select **Branding**. Scroll down to *Authorized Domains* and ensure that the Authorized domain value is correct. The domain field, such as **Authorized domain 1**, should be the top-level domain of your Infinite Campus site

All of the following must be true
- It must be the first part (domain name) of your Infinite Campus URL.
- It must **not** include **https://**
- It must **not** include the subdomain at the beginning or anything after the top-level domain (such as .com, .org, .edu) from your Infinite Campus URL.
- It must **not** have an extra space before or after the value
- It must **not** have a **/** (slash) at the end of the value

For example: if your full Infinite Campus URL is https://example.infinitecampus.org/campus/mydistrict.jsp, this value must be just infinitecampus.org **NOT** example.infinitecampus.org

4. If the value is not correct, edit it and Save.
5. Also check the *Audience*. Ensure the User Type is set to **Internal**. If it is not, select **Make Internal** and Confirm.

Check the Service Account

1. Navigate back to the **Credentials** screen.
2. There should be one entry under *Service Accounts.* Select the **Email** to view the Service Account Details screen.
3. Under *Unique ID*, copy the numerical value. This value should be all numbers and ~21 characters long.

   When this project was initially created, this Unique ID value should have been allow-listed via admin.google.com. The following steps confirm that the value was allow-listed correctly.

4. Navigate to admin.google.com
5. Click **Security.**
6. Scroll down to **API controls**. This option may be under Security > Access and Data Controls > API Controls if navigating with the sidebar.
7. Select **Manage Domain Wide Delegation**
8. Confirm that the 21-digit value you copied to your clipboard earlier shows on this screen in the list of Client IDs. To filter your view to only that Client ID, click **Add a filter**, select Client ID, paste in the Unique ID in the Client ID field and click **Apply**.
9. For that specific Client ID, confirm the scope is correct. Select **Edit**. The OAuth Scopes field must say https://www.googleapis.com/auth/drive.
   If you cannot find a record for that Unique ID on this screen, add it: **Add New** > Under Client ID, paste in the 21-digit Unique ID > under OAuth Scopes, enter **https://www.googleapis.com/auth/drive** and **Authorize**.

Less Common Configuration Issues

Check the Account Service Client Email

1. Navigate back to console.developers.google.com and log in as described in the Access section

above.
2. Select **Credentials**.
3. Under *Service Accounts*, note the **Email** value.
4. In Infinite Campus, navigate to Google Drive Configuration and check the **Service Account Email**. Ensure the value you see here is an exact match to the **Email** value on the Credentials screen of console.developers.google.com. If it not, correct it and Save.

Check the Enabled APIs

1. Navigate back to console.developers.google.com and log in as described in the Access section above.
2. Select **Enabled APIs and Services**.
3. Ensure these 2 APIs show in the table along the bottom of the screen:
   - Google Drive API
   - Google Picker API
4. If others are listed, they're not necessary. If these 2 are not listed, add them via Enable APIs and Services.

Known Symptoms of Misconfiguration

Students are unable to submit Google Drive submissions

"The file is not owned by you and cannot be attached"

Students try to submit Google Drive submissions through the Campus Student Portal but get the error "The file is not owned by you and cannot be attached".

Known cause
On the **Google Drive Configuration** screen within your Infinite Campus site, a typoed or incorrect value has been entered into the **Service Account Email** field.

To confirm this is the issue, navigate to **Google Drive Configuration**, select **Validate**, and work through the validation process. At the end of the process, you'll see an error like this one: "*Error getting access token for service account: 401 Unauthorized POST https://oauth2.googleapis.com/token, iss: [Service Account Email]*" at the end of the process, that confirms this is the issue.

Resolution
Follow the steps in Check the Account Service Client Email.