

Resetting the Client Secret Expiry Date

Overview

This article describes the cause of and resolution for data retrieval errors that may appear within the Integrity Data HR portal. When this error is encountered, users are unable to view one or more of the following: Time Off Balances, Pay History, and/or W2's.

Error Message

Error Message: *There was an issue retrieving Time Off Balance data....Pay History data....W2's data..... for this employee. If problem persists, please contact an administrator.*

Root Cause

The most common cause of this error is an expired Client Secret in the Microsoft Dynamics 365 Business Central Azure App Registration. Integrity Data's HR portal authenticates with your Business Central environment using a Microsoft Entra ID (formerly Azure Active Directory) app registration. This app registration includes a Client Secret that has a defined expiration date.

When the Client Secret expires, the integration can no longer authenticate with Business Central, causing all API calls to fail silently, resulting in the error shown above.

Other Possible Causes

- Incorrect or missing Client Secret value in the integration configuration
- App registration permissions were modified or revoked in Azure
- Business Central environment URL or tenant ID has changed
- Azure subscription or tenant was migrated

Resolution: Update the Client Secret Expiry Date

Follow the steps below to generate a new Client Secret in Azure and send the updated value securely to Integrity Data Support.

⚠ Note: These changes must be completed by a user with elevated administrator permissions. Integrity Data does not have the necessary permissions to complete this on behalf of their customers.

Part 1: Locate the App Registration in Azure

1. Sign in to the Azure Portal at <https://portal.azure.com> using your administrator credentials.
2. In the Azure Portal search bar at the top, type **Microsoft Entra ID** and select it from the results (formerly called Azure Active Directory).
3. Click App registrations in the left pane.
4. Search for the app registration associated with your Integrity Data / Business Central integration. This may be named something like "Integrity Data BC Integration" or similar.
5. Click the app registration name to open its details.

The screenshot shows the 'DevFunHouse' app registration details in the Microsoft Entra ID portal. The left sidebar contains navigation links: Overview (selected), Quickstart, Integration assistant, Diagnose and solve problems, Manage, Branding & properties, Authentication (Preview), Certificates & secrets, Token configuration, API permissions, Expose an API, App roles, Owners, Roles and administrators, and Manifest. The main content area displays the 'Essentials' tab with the following information:

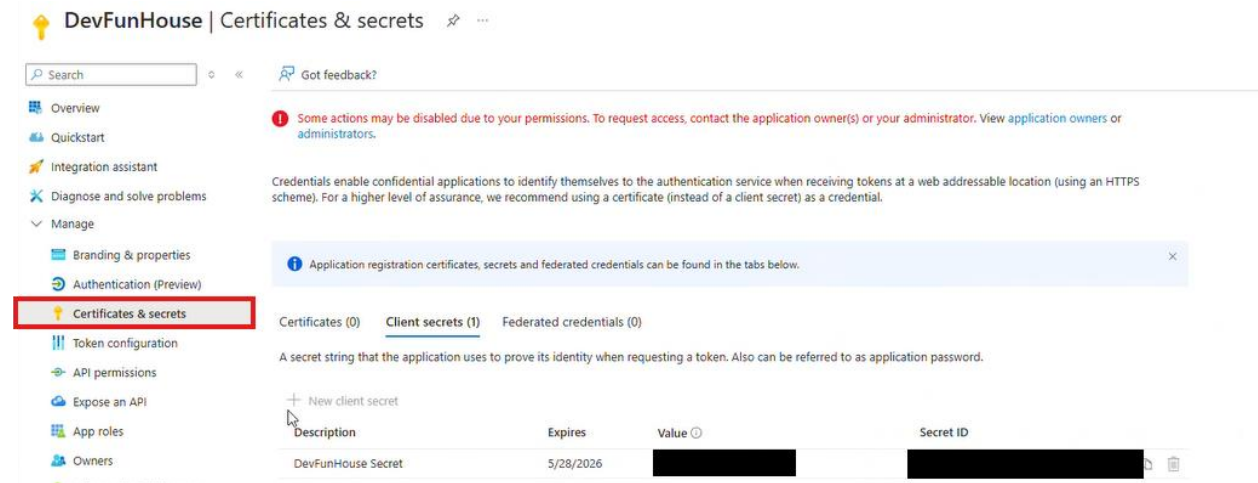
Property	Value
Display name	DevFunHouse
Application (client) ID	[Redacted]
Object ID	[Redacted]
Directory (tenant) ID	[Redacted]
Supported account types	My organization only
Client credentials	0_certificate_1_secret
Redirect URIs	1_web_0_spa_0_public_client
Application ID URI	Add an Application ID URI
Managed application in L...	DevFunHouse
State	Activated

Below the essentials, there is a message: 'Azure Active Directory Authentication Library (ADAL) and Azure AD Graph no longer receive new feature updates. We continue to provide technical support and security updates. Applications should be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)'.

The 'Get Started' tab is selected, showing a section titled 'Build your application with the Microsoft identity platform'. The text below states: 'The Microsoft identity platform is an authentication service, open-source libraries, and application management tools. You can create modern, standards-based authentication solutions, access and protect APIs, and add sign-in for your users and customers. [Learn more](#)'.

Part 2: Generate a New Client Secret

6. In the app registration, select Certificates & secrets from the left menu.



7. Under the Client secrets tab, review the list of existing secrets. Identify any that are Expired or about to expire.
8. Click + New client secret.
9. Enter a description (e.g., "Integrity Data Integration - Renewed [Month Year]").
10. Set the Expires field. It is recommended to select 24 months to reduce the frequency of renewals.
11. Click Add.
12. **IMPORTANT:** Immediately copy the new secret **Value** shown on screen. This value will only be displayed once and cannot be retrieved later.

Note: Do not delete the old secret until after Integrity Data has confirmed the new secret is working correctly in your environment.

Part 3: Version 28.51.1.30 and higher - Update the Client Secret in PayrollNow

Enter the secret value from Part 2 above into the Entra Client Credentials Window in Payroll Now

Note: This window option is only available to BC Admin users. You may need to contact your IT resources to assist with this update.

Entra Client Credentials

[Update Secret](#) | [More options](#)

Client Credentials

Client Id		Expiration Date	
Client Secret		Azure IT Contact Email	

1. Use the looking glass to search for the Entra Client Credentials window
2. Enter your company client ID. This can be located on the Payroll Now Setup Window in the Polling Parameters section:

Payroll Now Setup

Notifications: 2 [Entra credentials for the HR Integration is set to expire soon. Please update them to ensure uninterrupted service.](#) | [There are 7 polling staging entries with errors that require attention.](#)

[Start Sync](#) [Sync Log](#) [Sync Staging](#) [Polling Staging](#) [Error Messages](#) [Entra Client Credentials](#) [New Hire Reporting Setup](#) | [More options](#)

Outsource Tax Filing

Active Funds Release ☒

Data Upload

Upload Employee Data ☐

Polling Parameters

Upload Characters	42500	MW Polling Max Per Tick	0
Employee nodes	711	Refresh Authorization	☐
Employee ID nodes	107	BC Tenant Id	msft1a6720x75384000
Transaction nodes	1958	Environment Type	Sandbox
CS Account Id	{6b47a3e0-fa55-4154-8991-6a027cd95a9b}	Company DB Code	ICON_BE_Test
Upload Usage Data	☐	Azure Tenant Id	09e3207b-1181-4da2-9cf2-62d714317e47
Verify Polling Data	☐	Environment Name	Dev3
Initialize Polling job entry	☐		

3. Input the client secret obtained in Part 2 along with the new expiration date.

Part 4: Version 28.51.0.28 or lower - Send the New Client Secret to Integrity Data via Secure Email

The Client Secret is a sensitive credential. It must not be sent via standard email or shared in plain text. Use the following steps to transmit it securely.

1. Open your email client and compose a new message to Integrity Data Support at:
support@integrity-data.com
2. Use the subject line: Business Central Client Secret – [Your Company Name] – ACTION REQUIRED
3. In the email body, include the following information:
 - Your company name and Business Central environment name/URL
 - The Azure App Registration name and Application (Client) ID
 - The new Client Secret expiration date
4. Encrypt the Client Secret value before sending. Use one of the following recommended methods:

- **Preferred:** Use a secure file-sharing tool such as SharePoint, OneDrive (with password-protected sharing), or a service like 1Password Secure Share or Bitwarden Send.
 - **Alternative:** Send via Microsoft 365 encrypted email (select Encrypt before sending in Outlook).
 - **Do NOT:** Paste the raw secret directly in an unencrypted email body or in a Teams/Slack message.
5. Integrity Data Support will acknowledge receipt and update the configuration in your environment within one business day.

Verification

Once Integrity Data confirms the new secret has been applied, verify that the issue is resolved:

6. Log in to the Integrity Data HR portal.
7. Navigate to an employee record and open the Time Off section.
8. Confirm that Time Off Balance data loads successfully without error.
9. If the error persists, contact Integrity Data Support and reference this article.

Prevention: Proactive Secret Renewal

To avoid future disruptions, establish a process for monitoring Client Secret expiration dates:

- Set a calendar reminder 14 days before the Client Secret expiration date to initiate the renewal process early.
- In Azure Portal, navigate to App registrations > your app > Certificates & secrets to check expiration dates at any time.
- Consider navigating to the Microsoft Entra admin center > Entra ID > Overview > Recommendations to view and act on expiring credential alerts. This surfaces expiring secrets directly with guided remediation steps.
- When renewing, always allow 1–2 business days for Integrity Data to update the configuration before the old secret expires.

i Info: When contacting support, please reference this article number (KB-HR-0042) and include your Business Central environment details to expedite resolution.