

API Data Synchronization Failure or Pending in Halo Integration

The Halo integration with MSPbots shows API data synchronization has failed or is in Pending status. When this occurs, check if you have configured the correct login type for the API application. This guide shows how to set the correct login type for the API application and configure the login account, etc.

What's on this page:

- [Issue Description](#)
- [Prerequisites](#)
- [Resolution](#)
- [Related Topic](#)

Issue Description

After establishing a successful Halo Integration with MSPbots, clients encounter API data synchronization failure or experience cases where the data is in Pending status.

The error messages are as follows:

```
403: Forbidden error indicates lack of permission to access.
"/Appointment : 403:Forbidden"
"/Tickets : 403:Forbidden"
```

Halo PSA - APPOINTMENT-SYNC

API Count40

Success Count19

Fail Count13

API List

All

API	Last Sync Time	Status	Action
	0	Pending	
	10/26/2023 09:29 CST	Failed	
	10/26/2023 09:23 CST	Succeeded	
	10/26/2023 09:23 CST	Failed	
	0	Pending	
	10/26/2023 09:03 CST	Failed	
	0	Pending	
	10/26/2023 10:26 CST	Succeeded	
	10/26/2023 09:13 CST	Succeeded	

Sync Frequency86400 Seconds

Last successful data acquisition10/26/2023 09:23 CST

API - DatasetHalo Appointment

Sync Total3

Success Count0

Fail Count3

Sync History

2023-10-26 - 2023-10-26

All

Client Name:

Start Time	Sec	Status
10/26/2023 09:23 CST	1164	Failed
ID: 1173 "/Appointment : 403:Forbidden"		
How To Fix: If this error was temporary, you can try resubmitting the run and the issue may have been resolved.		
10/26/2023 09:23 CST	636	Failed
ID: 1168 "/Appointment : 403:Forbidden"		
How To Fix: If this error was temporary, you can try resubmitting the run and the issue may have been resolved.		

Total 310/page1Go to1

This issue occurs because the Agent's login type is incorrectly set resulting in insufficient permissions and data synchronization failure. To resolve this, clients need to set the correct login type for the Agent.

Prerequisites

Before proceeding, ensure successful Halo integration and authorization. These steps can only be performed by admins and may only affect Halo users.

Resolution

To set up the Agent with the correct login type

1. On the Add an Application screen of Halo PSA, select Agent for the Login Type.
2. Then select Administrator for **Agent to log in as**.

← Save

Add an Application

Details Permissions Security

Application Name *

Enter the name of the Application here

☒ Active

Authentication Method *

☐ Username & Password

☐ Implicit Flow (Single Page Application)

☐ Authorisation Code (Native Application)

☒ Client ID and Secret (Services)

For backend non user-facing applications only. This method allows logging in just with a Client ID and Client Secret. A username and password is not needed.

Client ID

This is a unique identifier for your Application, and you will need this to Authenticate.

480bdaa1-584c-48bc-9f32-b2895c23c018

Client Secret

The Client Secret is used to access to the API without logging in. If stored, it should be encrypted and never shown.
The Client Secret for this application will only be shown once. If you forget it you'll need to generate a new one. Generating a new Client Secret will stop the old one from working.

cd93b7f4-f940-47ab-7ab54bc95e83-e8fc6259-747b-4ffe-910c-0aae8bdaadb5

Generate Copy

Login Type *

Agent

Agent to log in as *

Administrator

3. Set the minimum permission to **read:tickets**. Other permissions can be added according to needs. For more information, refer to the HaloPSA guide on [Setting up an API Agent](#).

Related Topic

- [Halo Integration Setup](#)
- [NextTicket Manager for Halo](#)
- [Halo Public Datasets](#)