

OAuth - Login for Client or Connecting EM to an NVR Fails Until “Allow Public Client Flows” Is Enabled in Microsoft Entra

KB Number: 23956

Published: 23/04/2026

Overview

When configuring OAuth authentication with Microsoft Entra ID for exacqVision, OAuth authentication may partially succeed (for example, EM GUI login or user authentication), but Enterprise Manager to NVR connectivity or exacqVision Client OAuth login may fail with misleading errors.

This issue occurs when the Microsoft Entra App Registration does not have Allow public client flows enabled.

Enabling this setting resolves the issue immediately.

Symptoms

One or more of the following may be observed:

OAuth login works for Enterprise Manager GUI, but fails for:

- exacqVision Client (may stay stuck at "received discovery response" but not progress")

- EM → NVR connectivity when “Login using OAuth” is enabled

- NVRs disconnect from EM when OAuth is used, but remain connected when local credentials are used

- exacqVision Client could also displays errors such as:

 - “Login canceled by user”

 - “HTTPS request to IdP was malformed”

- Microsoft Entra sign-in logs show failures with messages such as:

The request body must contain the following parameter: client_assertion or client_secret.

Cause

Microsoft Entra treats OAuth requests differently depending on whether an application is classified as a public client or confidential client.

exacqVision uses public-client OAuth flows (PKCE) for:

- exacqVision Client authentication
- EM → NVR OAuth connectivity

If Allow public client flows is disabled in the Microsoft Entra App Registration:

- Entra interprets non-interactive OAuth requests as confidential client (service principal) requests
- Entra then requires a client_secret or client_assertion
- exacqVision does not send a client secret or assertion
- Entra rejects the request
- exacqVision reports a login or OAuth failure or doesnt progress statuses on sign in with your organization actions