**Single Pane of Glass (SPOG) Dynamics 365 Customer Service and Microsoft Authentication Library (MSAL) Reference Architecture**

***Applies to******:*** ***Dynamics 365 Customer Service***

This solution combines Dynamics 365 Customer Service and Microsoft Authentication Library (MSAL) via Entra ID (Azure AD), to build a Single Pane of Glass (SPOG) solution within Bank of Ireland’s (BOI) Dynamics 365 Customer Service, integrating authenticated third-party applications into Dynamics 365 via Iframes and MSAL.

## Introduction

This reference architecture describes the implementation of a **Single Pane of Glass (SPOG)** solution within **Bank of Ireland’s (BOI) Dynamics 365 Customer Service**, integrating third-party applications into Dynamics 365 via **Iframes using Microsoft Authentication Library (MSAL)**. The solution streamlines access to external applications, improving user efficiency while maintaining security and compliance standards.

**Use Cases & Industries**

* **Industry:** Finance and Banking
* **Use Cases:**
  + Centralized access to multiple applications in Dynamics 365
  + Enhanced user productivity through seamless application switching
  + Improved security via controlled access and SSO authentication

**Implementation Timing**

This reference architecture should be defined **during the early solution design phase**, ensuring integration feasibility with existing security policies and authentication mechanisms.

**Key Stakeholders**

* **Solution Architects** - Define architecture and integration strategies
* **Dynamics 365 Developers** - Implement Iframe-based logic
* **IT Security Teams** - Validate authentication mechanisms and security policies
* **End Users** - Utilize SPOG for day-to-day operational tasks

## Architecture

The following diagram illustrates the architecture for the solution.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer program

AI-generated content may be incorrect.

Download a PowerPoint file with this architecture. [graphics-reference-architecture](https://be4you-my.sharepoint.com/personal/henrique_souza_bearingpoint_com/Documents/Bearing%20Point/FastTrackSubmission/BOI-Phase1/Souza_Henrique_BearingPoint_Dynamics365CustomerEngagement/Pre%20Requisites/Reference%20Architecture/graphics-reference-architecture.pptx?web=1)

## Workflow

1. **User Opens Browser**
   1. The user opens a web browser and navigates to **Dynamics 365 Customer Service**.
   2. An **iframe within Dynamics 365** tries to load an external secure resource.
2. **Request Access to Source**
   1. The **embedded iframe inside Dynamics 365** attempts to access a **protected resource**.
   2. Since the user is not authenticated, Dynamics 365 triggers an **authentication request**.
3. **Dynamics 365 Generates a SAML Authorization Request**
   1. Dynamics 365 (acting as the **Web App Service Provider**) **generates a SAML authentication request**.
   2. The request is **redirected to Microsoft Entra ID**, the **SAML Identity Provider (IdP)**.
4. **User Authenticated in Microsoft Entra ID**
   1. Microsoft Entra ID prompts the **user to log in** if they are not already authenticated.
   2. If the user has an active session, **silent authentication occurs automatically**.
5. **Microsoft Entra ID Issues a SAML Token**
   1. Once authentication is successful, **Microsoft Entra ID generates a SAML token**.
   2. This token contains **user claims and access permissions**.
   3. The token is sent back to **Dynamics 365 Customer Service**.
6. **Dynamics 365 Redirects the Token**
   1. The **SAML token is passed back to the iframe or requesting application**.
   2. This allows the **secure session to be established**.
7. **Dynamics 365 Validates the SAML Response and Token**
   1. Dynamics 365 checks the **token signature, expiration, and claims** to ensure the user is authorized.
   2. If validation fails, authentication is rejected.
8. **Secure Page is Returned to the User**
   1. If the token is **valid**, Dynamics 365 grants access to the **requested secure resource**.
   2. The secure content is loaded inside the **iframe within Dynamics 365**.

## Components

The following components are used in the reference architecture.

* [**Dynamics 365 Customer Service**](https://www.microsoft.com/dynamics-365/products/customer-service) - Core CRM system providing centralized customer interaction management.
* [**EntraID**](https://www.microsoft.com/security/business/identity-access/microsoft-entra-id) - Identity and access management system handling authentication and security.
* [**MSAL**](https://learn.microsoft.com/entra/identity-platform/msal-overview) - Authentication library enabling seamless Single Sign-On (SSO) for third-party apps.

## Scenario details

The users required an efficient method to interact with **third-party applications** directly within Dynamics 365 without switching between multiple windows while maintaining security control within their present authentication identity provider (EntraID).

**Customer Goals**

* Provide a seamless **integrated experience** for users working in Dynamics 365
* Ensure **secure and controlled authentication** via **MSAL-based SSO** and **EntraID**

### Potential use cases

This solution was created for a **financial services organization** that required a centralized authentication system and streamlined access to compliance-related applications. It can also be applied to industries like **finance, banking, insurance, and government**. It can be used by any organization that requires **secure, single sign-on authentication and efficient tab management for multiple external applications**.

You can use this solution to:

* **Enhance security** by integrating MSAL-based SSO authentication within Dynamics 365.
* **Improve user efficiency** enabling seamless transitions between applications.
* **Ensure compliance** by maintaining centralized access logs for all third-party applications used within the CRM.

## Considerations

These considerations help implement a solution that includes Dynamics 365. Learn more at [Dynamics 365 guidance documentation](https://learn.microsoft.com/dynamics365/guidance/).

### Cost optimization

Cost optimization is about looking at ways to reduce unnecessary expenses and improve operational efficiencies. For more information, see [Overview of the cost optimization pilla](https://learn.microsoft.com/azure/architecture/framework/cost/overview)r.

The cost of running this solution depends on the **scale of deployment**, but it can be optimized by leveraging **Microsoft’s cloud-based services** efficiently.

1. **Identity Management (EntraID & MSAL)**
   * Cost is primarily driven by **user authentication requests and token exchanges**.
   * Scaling is **linear**, meaning more users lead to a predictable cost increase.
   * **Cost Optimization:** Reduce the number of authentication requests by implementing **longer session timeouts** where security policies allow.
2. **Dynamics 365 Licensing**
   * Licensing cost is tied to **active user seats** and **feature usage**.
   * The cost **scales per user**, making **proper role-based access control (RBAC)** critical.
   * **Cost Optimization:** Limit feature access based on user roles to avoid unnecessary premium licensing.

Use the [**Azure Pricing Calculator**](https://azure.microsoft.com/pricing/calculator/) to estimate costs based on specific **user count and service usage**.

## Implementing Single Pane of Glass (SPOG) Dynamics 365 Customer Service and Microsoft Authentication Library (MSAL)

This architecture enables **seamless authentication and embedded application integration** within **Dynamics 365** by leveraging **Microsoft Entra ID (Azure AD) and MSAL**. The solution ensures users can access third-party applications without needing to log in multiple times, providing a **Single Sign-On (SSO) experience**. Additionally, third-party applications are embedded using **iframing techniques**, ensuring a **unified interface** within Dynamics 365.

The user will implement:

* **Authentication setup** using Microsoft Entra ID and MSAL.
* **Application embedding** via iframes within Dynamics 365.
* **Cross-domain security configurations** to ensure smooth interaction between Dynamics 365 and external apps.
* **Token-based authentication** to securely pass user identities across embedded applications.

**Table Structure**

The section is structured into multiple **procedures**, each covering a critical part of the implementation:

1. **Authentication Procedures**
   * **Register applications in Microsoft Entra ID**: Defines how to register external applications to enable authentication via Entra ID.
   * **Enable MSAL in the client application**: Guides setting up MSAL to acquire authentication tokens for app integration.
   * **Implement Single Sign-On (SSO)**: Describes how to leverage Entra ID sessions to enable seamless logins.
   * **Configure MSAL settings**: Covers security measures like defining scopes, token storage, and login hints for a smoother authentication flow.
2. **Embedding Applications in Dynamics 365**
   * **Embed external applications using iframes**: Explains how to use Dynamics 365’s iframe functionality to integrate third-party applications.
   * **Ensure cross-domain compatibility**: Details the security policies required to allow external applications to be embedded within Dynamics 365.
   * **Handle MSAL authentication within an iframe**: Covers the authentication challenges of iframes and how to use **popup-based authentication** to bypass restrictions.
   * **Integrate multiple applications in Dynamics 365**: Outlines how to embed multiple external applications while maintaining a **Single Pane of Glass experience**.

Each procedure provides a **step-by-step approach** to implementing the required components. This structure ensures that authentication and application embedding are handled **securely and efficiently**, improving user experience within Dynamics 365.

### Procedure: Register applications in Microsoft Entra ID

Use the following steps to Register applications in Microsoft Entra ID.

1. Register each integrated application in Microsoft Entra ID to establish a unified identity platform.
2. Each app registration provides a Client (Application) ID and is associated with your Entra tenant.
3. Use a redirect URI appropriate for Dynamics 365’s domain or a custom domain. Ensure the URI is added under the SPA or Web platform settings.

### Procedure: Enable MSAL in the client application

Use the following steps to Enable MSAL in the client application.

1. Initialize the Microsoft Authentication Library (MSAL) in the embedded application’s front end (e.g., a single-page app or web page loaded in Dynamics).
2. Configure MSAL to use the OAuth 2.0 Authorization Code flow with PKCE for enhanced security.
3. This setup allows the app to obtain ID tokens (for user identity) and access tokens (for calling APIs) either silently or via interactive sign-in.

### Procedure: Implement Single Sign-On (SSO)

Use the following steps to Implement Single Sign-On (SSO).

1. Since users are already logged into Dynamics 365 via Entra ID, use MSAL’s capabilities to achieve SSO for embedded apps.
2. Use silent token acquisition (ssoSilent() or acquireTokenSilent()) to reuse the existing session.
3. If no existing session is found or consent is required, MSAL triggers an interactive authentication popup.
4. This ensures a seamless login experience across Dynamics 365 and embedded third-party applications.

### Procedure: Configure MSAL settings

Use the following steps to Configure MSAL settings.

1. Set the authority to https://login.microsoftonline.com/<tenant-id> with the known client/application IDs for audience validation.
2. Define the scopes needed for each third-party app (e.g., Microsoft Graph API scopes or custom API scopes).
3. Store the MSAL cache securely (session storage or local storage) to prevent token exposure.
4. Use login hints (user’s UPN/email) and domain hints (tenant domain) in loginPopup() or ssoSilent() to minimize unnecessary authentication prompts.

### Procedure: Embed external applications using iframes

Use the following steps to Embed external applications using iframes.

1. Use Dynamics 365’s native iframe support to embed external web applications.
2. Create a placeholder in Dynamics (e.g., dashboard iframe, navigation link, or web resource control).
3. Configure the iframe to point to the external application’s URL.

### Procedure: Ensure cross-domain compatibility

Use the following steps to Ensure cross-domain compatibility.

1. The embedded third-party application must allow framing by Dynamics 365.
2. Configure the external app’s web server to include a Content-Security-Policy (CSP) frame-ancestors directive or X-Frame-Options header that permits embedding.
3. If an application sends X-Frame-Options: DENY, update the configuration to allow framing (ALLOW-FROM <Dynamics URL>).

### Procedure: Handle MSAL authentication within an iframe

Use the following steps to Ensure cross-domain compatibility.

1. Azure AD login pages cannot be rendered inside an iframe due to security restrictions (X-FRAME-OPTIONS: DENY).
2. Configure MSAL to use popup-based authentication instead of a full-frame redirect.
3. The iframe’d app should open a small popup window to Azure AD for interactive sign-in and obtain the token before closing the popup.
4. Ensure Dynamics 365 allows popups by setting allow-popups in the iframe sandbox attributes.

### Procedure: Integrate multiple applications in Dynamics 365

Use the following steps to Ensure cross-domain compatibility.

1. Each third-party application can be embedded separately in different sections/tabs or together on a dashboard with multiple iframes.
2. MSAL handles authentication, ensuring that users do not need to re-enter credentials for each app.
3. Identity is passed via Entra ID tokens, ensuring a Single Pane of Glass experience where users seamlessly navigate between Dynamics 365 and external tools.

## //Next step

## //Related patterns

The following patterns are available to help guide your implementation of the set customer credit limits business process.

## Related resources

Review the following related architecture guides, solutions, and other guidance content:

* <https://learn.microsoft.com/en-us/entra/identity-platform/msal-overview>

## Tags

*Industries:* Finance, Insurance

*Stakeholders:* Customer services, Engineering, Finance, IT

*Products:* Dynamics 365 Customer Service

## Contributors

*This article is maintained by Microsoft. It was originally written by the following contributors.*

Principal author:

* [Henrique Silvestre](https://www.linkedin.com/in/hsilvestre/) | Solution Architect