Maintmaster® Single Sign-On (SSO) White Paper

Introduction

This white paper describes Maintmaster's Single Sign-On (SSO) solution with Microsoft Entra ID (formerly Azure Active Directory). Maintmaster provides a built-in SSO capability that enables customers to use their existing identity provider for all Maintmaster logins.

Enabling and Disabling SSO

To enable Maintmaster SSO with Microsoft Entra ID, a global Entra administrator must grant Maintmaster permission to authenticate through the organization's domain. The process begins when the administrator contacts Maintmaster Support and signs in to the Maintmaster portal to complete the authorization.

During authorization, the administrator establishes a connection between their Maintmaster user and the organization's Entra ID tenant. The tenant must be hosted in Azure or synchronized with Azure. After the global administrator has enabled the integration, they must also sign in via the Maintmaster launcher to activate SSO for the system.

For testing without affecting your production environment, you may create a dedicated <name>.onmicrosoft.com domain or an equivalent test tenant.

To disable the Entra connection, the customer's solution administrator should contact Maintmaster Support. Support will remove the Entra configuration. When SSO is disabled, users revert to Maintmaster's standard login credentials. Users who previously logged in before SSO was activated can use those credentials again. Users who only used SSO must set a password using the password-recovery option on the Maintmaster launcher ("Forgot password").

Authentication Flow

When a user signs in successfully, the SSO service issues a token containing authentication and authorization details. Maintmaster verifies the token's authenticity and grants access based on the claims it contains. If the user is authenticated and authorized, access to the system is granted.

Maintmaster manages user sessions, maintaining authentication across interactions until the user logs out or the session expires.

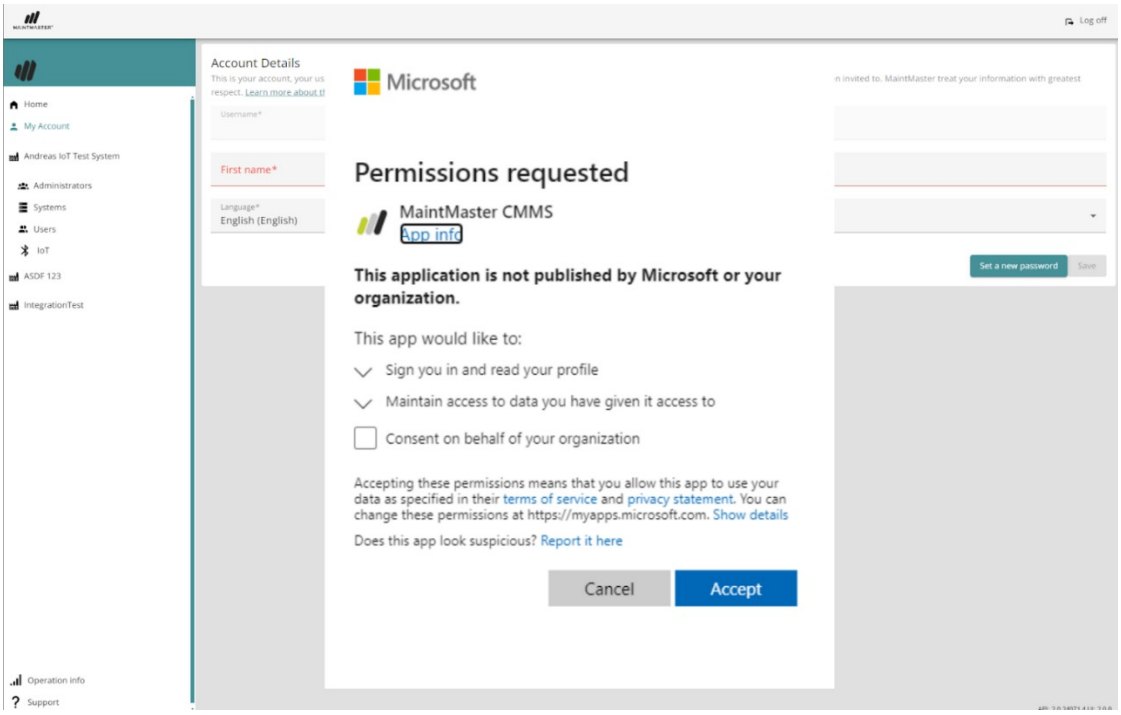
Implementing SSO in Your Maintmaster Environment

To begin the SSO integration, contact Maintmaster Support. When Support replies to enable SSO, the organization's solution administrator accepts the SSO integration in the Maintmaster portal (a feature available only to solution administrators). Domain verification may take additional time.

After the domain is added, Maintmaster users who belong to that domain and have the Solution Administrator role will see a My Account action in the Maintmaster portal labeled "Connect

your Entra ID tenant." The user who starts this process must have permission to approve the application on behalf of the entire Entra tenant (typically a global administrator in Microsoft Entra ID).

Starting the connection opens a Microsoft sign-in screen. After sign-in, the user is redirected to a consent screen requesting access to basic profile information—display name, first and last name, email address, open extensions, and photos.



Once consent is granted, all existing Maintmaster users in the organization can use their Entra ID credentials at sign-in. Newly invited users within the verified domain are required to use their Entra ID credentials when signing up to Maintmaster.

This is the information that Maintmaster gains access to with this consent:

- Profile – Reads basic user info like name, tenant ID, and other standard account details.
- Openid – Used to sign users in with Entra ID.
- Offline_access – Lets the app stay signed in using refresh tokens.
- Email – Allows access to the user's email address.

Scope and Limitations

Maintmaster's SSO solution is not a "True SSO" implementation; users are not automatically logged in across different services. A new login session requires entering credentials.

Key advantages include:

- SSO applies to all Maintmaster services and links access to the user's Entra ID.
- No need to remember a separate Maintmaster password.
- Customers control password complexity, Multi-Factor Authentication (MFA), and biometric options via Entra ID policies.

The SSO solution does not include:

- Automatic sign-in across different services.
- Password configuration management—this is controlled by the customer's Entra administrators.
- Direct user provisioning in Entra ID; users must be invited as Maintmaster users from your Maintmaster system.