MaintMaster® Single Sign-On (SSO) White Paper

This White paper covers MaintMaster's Single Sign-On (SSO) solution with Microsoft Entra. MaintMaster provides an SSO-solution for all our customers out of the box which allows customers to use their own authentication solution for all MaintMaster authentication.

How Customers Enable and Disable SSO

In order for the MaintMaster SSO to be against a Microsoft Entra (Formerly called Azure Active Directory), a global administrator of the Entra ID must grant MaintMaster permission to authenticate through your domain. This is done by the administrator contacting Maintmaster support. This authorisation process involves your administrator logging into their MaintMaster portal account. Your administrator must then fill out a form from Microsoft, including name, phone number and email to establish a connection between their user in MaintMaster and their Entra ID. The Entra ID must be either in Azure or synchronised with Azure. After it is enabled by global Azure admin, they also need to login through the MaintMaster launcher to enable it for the system.

If you would like to test it but not interfere with your production domain, you could create a <name>. onmicrosoft.com-domain or equivalent. You can find more information on how to set up a test domain here.

To disable the AD connection, the customer's solution administrator needs to contact Maintmaster support. Support will then delete the AD connections. When SSO is disabled, all users revert to MaintMaster's standard login credentials. This means that users who logged in before SSO was activated can use these login details again. Users who, only used SSO will have to create a new password by using the password recovery feature at login via "forgot password" (Old users return to their old password. New users need to accept "new terms policy" – new users and users who have forgotten their passwords must set a new password through the "forgot password link in the MaintMaster launcher").

Behind the scenes

Upon user login and successful authentication, the SSO service generates a token that contains information about the user's authentication and authorisation status. This token is then passed back to MaintMaster. MaintMaster receives the token from the SSO server, verifies its authenticity, and grants access to the user based on the information contained within the token. If the user is authenticated and authorised, they are granted access to the system.

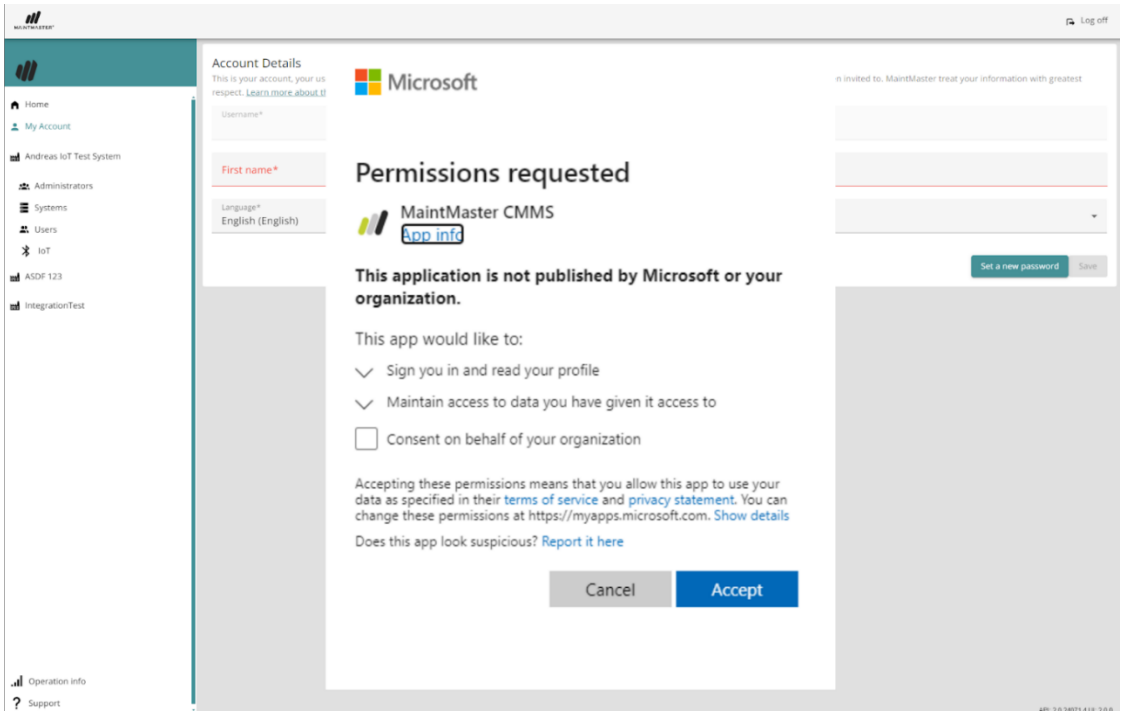
MaintMaster manages the user's session, ensuring that the user remains authenticated across multiple interactions with the system until they log out or their session expires. The session management is handled internally by MaintMaster.

Implementing SSO in your MaintMaster

To start the SSO integration process, the customer needs to contact MaintMaster's Support to start using SSO. When support replies to the request to enable SSO, the organisation's solution administrator needs to accept MaintMaster's SSO integration in the MaintMaster portal, a feature only available for your solution admin(s). This step may take some time as customers confirm their domain.

When the domain is added, users that belong to that domain and have a role of Solution Administrators within MaintMaster, have a button enabled in

MaintMaster portal under My Account called "Connect your Entra ID tenant". It is required that the user starting this process has permission to approve the application on behalf of the whole Azure tenant (most likely a global admin role within Microsoft Entra ID). When the Connect to Entra ID tenant process is started, it opens a login screen to Microsoft, so the user can login and authenticate towards Microsoft. After the login, the user is redirected to the consent screen requesting access/information about the current user logging and the basic profile of users in the customer's tenant - this includes display name, first and last name, email address, open extensions, and photos which is also shown in the picture below.



After this step is finished and consent is given, all existing MaintMaster users in the organisation have now activated the feature to use the Entra ID credentials on login. Any new users that are invited and belong to the domain, are forced to use their Entra ID credentials when signing up to MaintMaster.

Coverage of MaintMaster's SSO-implementation

MaintMaster SSO solution is NOT an implementation of "True SSO". This means that users won't be automatically logged in across different services. In other words, all new login attempts require users to enter their password-credentials.

Advantages of this SSO solution are:

- The Single Sign-On (SSO) is utilised for all MaintMaster services with integration and is linked to the user's Entra-ID.
- No need to remember multiple passwords.
- Customers have the possibility to determine the complexity of their password for authentication, as well as the tools for Multi-Factor Authentication (MFA) and Biometric Authentication.

The SSO solution does NOT include:

- Users will not be automatically logged in across different services.
- MaintMaster does NOT handle how users configure passwords. This is determined by one of your Entra Directory admins.
- There is no support for direct user provisioning in Entra. Users must still be invited as MaintMaster users from your MaintMaster system.