Deltek

Deltek Maconomy® 2.6.2

Microsoft Azure Setup Guide

October 27, 2023

While Deltek has attempted to verify that the information in this document is accurate and complete, some typographical or technical errors may exist. The recipient of this document is solely responsible for all decisions relating to or use of the information provided herein.

The information contained in this publication is effective as of the publication date below and is subject to change without notice.

This edition published October 2023.

Contents

Overview

This document contains details on how to configure and use Microsoft Azure Single Sign-On (SSO) for Maconomy. Note that this document assumes you have an Azure AD account.

Single Sign-On with Microsoft Azure Active Directory

This document contains information about how to perform the following tasks:

- Complete Prerequisites for Azure implementation to obtain Tenant ID
- Register Maconomy applications within this tenant, and obtain Client ID
- Generate Client Secret
- Configure Users in Maconomy
- Register Touch (if needed)

Complete Prerequisites

Sign Up for a Microsoft Azure AD Account

If your firm does not already have a Microsoft Azure AD account, you can sign up for a free account at https://azure.microsoft.com/en-us/free.

Microsoft also offers an Azure AD Premium account for a cost at https://azure.microsoft.com/en-us/trial/get-started-active-directory.

The Premium edition is **not** required for using the single sign-on solution for Maconomy, unless you need to enable Azure multi-factor authentication and/or conditional access restrictions.

Add Maconomy Applications to Obtain Client IDs

The process requires the following application to be set up in Azure:

- **Maconomy** – Azure Web application for Maconomy Server, Maconomy clients (including Workspace and web clients), and Touch native and Web application

In this process, you must add Maconomy applications to Azure Active Directory and obtain Client ID.

Tip: Open Notepad and keep it handy to copy and paste IDs.

Create New Registrations

You must register Maconomy applications within the Azure Tenant ID.

To create a new registration in Azure AD:

1. Log in to the Azure portal at https://portal.azure.com/.
2. Log in to Microsoft Azure and Click **New registration**.
3. On the **Register an application** blade, in the **Name** field, enter a descriptive name such as **Maconomy Server**.
4. In the **Supported account types** field, select **Accounts in this organizational directory only – [name] Single tenant**.
5. In the **Redirect URL field**, select Web.
6. In the related URL field, enter https://<directory>.onmicrosoft.com/maconomyserver.

   Example: For XaYbZc Engineers, enter https://xaybzc.onmicrosoft.com/maconomyserver

   Verified URLs have a green check mark beside them.
7. Click **Register**.

Show the Tenant and Client IDs

Show the Directory (tenant) and Application (client) IDs, as this information is needed later in the process. These are the values that must be put into Mconfig at a later stage.

To view the tenant and client IDs:

1. On the App registrations > Maconomy blade, take note of the IDs.
2. Copy each the Application (client) ID and the Directory (tenant) ID, and paste in Notepad.

Add the Redirect URLs to the Web Platform

Add the redirect URLs to the web platform to facilitate returning authentication tokens to authenticate users. Note that if your Maconomy system is in the Deltek Cloud, the specific system URLs will have already been supplied.

To add redirect URLs:

1. On the **Authentication** blade, in the **Redirect URLs** area, click **Add URL**. A new URL line displays.
2. Add the three redirect URLs for Touch, one for Workspace, and web client.

   > **Note:** Tab after entering each URL. A green check mark will appear to confirm that the format of the URL is valid.

3. Add the following reply URLs for each of the client applications that will use Azure for authentication:

   - **Workspace Client:**

     http://localhost

     > **Note:** If you disable the external browser option, use the following URL instead:
     >
     > https://login.microsoftonline.com/common/oauth2/nativeclient .

   - **Web Client**:

     https://clientiaccess.deltekenterprise.com/oauth

   - **Touch** (link included in Touch section)
     - .../maconomyshared/backend/oauth2authorizereturn.php (for example, https://<yourdomain>.com/22_M20SP1/maconomyshared/backend/oauth2authorizereturn.php) – This is for Azure OpenID, for the Touch Web application.
     - …/maconomyshared/backend/oauth2authcodereturn.php. – This is for the Azure OpenID, for Touch native application, needed if REST_USESF = “true”
     - …/maconomyshared/backend/oauth2authcodereturn_iab.php. – This is for the Azure OpenID, for Touch native application, needed if REST_USESF = “false”

4. Click **Save**.

Generate the Client Secret

The client secret is a secret string of text that the application uses to prove its identity, like an application password.

> **Note:** Before you leave the screen that displays the client secret, you MUST take note of it and store it in a safe place.
>
> After you move past this screen, you will no longer have access to the client secret. You must do this now because, after you leave this screen, you cannot return to the screen to see the value.

To generate a client secret:

1. On the **Certificates & secrets** blade, under **Client secrets**, click **New Client Secret**.

   You can right-click the key value to copy it to the clipboard and save it.

Tip: If you input an expiration date, note that your authentication will stop working at the selected time and it will be your responsibility to generate a new client secret and provide this information to Deltek.

2. Supply to client secret to Deltek Cloud Operations.

Configuration

For cloud-based organizations, Deltek Cloud operations configures the following for the client:

- Set up MConfig

The client or a consultant configures the following:

- Configure Maconomy Users
- Configure Touch Users

For on-premises users, all of the above tasks are performed by the client or a consultant.

Set Up MConfig

To set up MConfig to support a customer's Azure implementation:

1. In MConfig, go to the OSGi products screen.
2. In the **Domain login method** field, select **Azure OpenID**.
3. In the **SSO method** field, enter namematch.
4. In the **Azure Tenant ID** field, enter the tenant ID.
5. In the **Client ID** field, enter the client ID.
6. In the **Client Secret** field, enter the client secret.

Set Up Touch

To set up Touch, make the following changes in the configuration.ini (or tenant.ini) file:

1. Set REST_USEEXTERNALCREDENTIALS to **true**. By default, it is set to **false**.
2. Set REST_EXTERNALCREDENTIALSTYPE to **Azure**. By default, it is empty.
3. Make sure **REST_USESF** has the desired value. By default, it is set to **"true"**.

Note: The **REST_USESF** refers to mechanism used to show Microsoft Azure authentication screen in the Touch app, as follows:

1. REST_USESF = "false"
   The Touch app will use InAppBrowser.
   Pro: Initial login always works.
   Con: Instead of using PIN/biometric, you might need to login using your credentials.
2. REST_USESF = "true" (this is the default and recommended value)
   The Touch app will use SafariViewController.
   Pro: After the initial login with credentials, you can use PIN/biometric for authentication.
   Con: Few Android users are not able to do the initial login, since the Microsoft Azure authentication screen is not shown.

Configure Users in Maconomy

All AAD users have to be associated with a corresponding Maconomy user to be able to log in. The following shows how to associate an existing Maconomy user with the sample AAD user `jimjarrett@bobedst.onmicrosoft.com`.

To configure users in Maconomy:

1. Log in to Maconomy as system administrator, or as the user whom you wish to configure. You must use traditional Maconomy username/password credentials to do this. Click **Escape** if the Azure login dialog appears.
2. Open the **Setup** » **Users** dialog and double-click on the user you want to configure.
3. Under the **Role Information** tab, find the **Network Username** group.
4. Complete the **Name** and **Domain Name** fields with the matching values of the AAD username, which has the format **`<Name>@<Domain Name>.`**

   > **Note: It is important to convert all values to UPPER CASE**.

   For example, if the AAD username is `jimjarrett@bobedst.onmicrosoft.com`, the values for **Name** and **Domain Name** are `JIMJARRETT` and `BOBEDST.ONMICROSOFT.COM`, respectively.
5. Save the settings.

   > **Note:** Maconomy may ask you to enter a password for the user.

Configure the Coupling Service – New Configuration

The steps below are for Deltek Cloud Ops.

Warning: Complete the following steps only if you are configuring the Coupling Service for the first time. If you are upgrading an existing configuration, see the following section called **Configure the Coupling Service – Upgrade Azure Configuration**.

To configure the coupling service for use with Azure AD:

1. Open the security configuration file at

   `<MaconomyDir>\CouplingService\configuration\maconomy.security.config`

   where <**MaconomyDir**> is the path of the Maconomy installation.

2. Under the **Maconomy** section (inside the curly braces in `Maconomy{ … };`), insert the following login module definition. Insert it before the definition of `com.maconomy.lib.coupling.MaconomyLoginModule`, but after any other login mechanisms with higher priority:

```
<<EnableAzureOIDCLogin>>org.eclipse.equinox.security.auth.module.Ext
ensionLoginModule required
<<EnableAzureOIDCLogin>>  extensionId="com.maconomy.lib.coupling.Mac
onomyAzureOIDCLoginModule"
<<EnableAzureOIDCLogin>>  tenantId="<<AzureTenantId>>"
<<EnableAzureOIDCLogin>>  clientId="<<AzureClientId>>"
<<EnableAzureOIDCLogin>>  clientSecret="<<AzureClientSecret>>"
<<EnableAzureOIDCLogin>>  externalBrowser="<<AzureExternalBrowser>>"
<<EnableAzureOIDCLogin>>  externalBrowserPortRange="<<AzureExternalB
rowserLowPortRange>>, <<AzureExternalBrowserHighPortRange>>";
```

   Replace the highlighted placeholders by the appropriate values.

   - See the previous sections for instructions on how to obtain the values of **Tenant ID**, **Client ID**, and **Client Secret**.
   - The value of **"externalBrowser"** is set to **true** by default.
   - For **"externalBrowserPortRange"**, specify the port range you want to use for the redirect link when starting a local web server in the Workspace Client.

     This is optional. If you do not specify a range, the Workspace Client will select a port using the local operating system rules.

     If you specify a range, the port numbers should preferably be in the IANA range of ephemeral port numbers. For more information, see: https://en.wikipedia.org/wiki/Ephemeral_port.

     The coupling service (CS) will allow port numbers outside this range and will only issue a warning in the CS log if port numbers outside this range are used.

Third Party (Native) Apps

Third Party (native) apps can authenticate against Azure using a flow called Client Credentials Grant Flow with Certificate, described at:

https://docs.microsoft.com/en-us/azure/active-directory/develop/v2-oauth2-client-creds-grant-flow

Previously, the OpenID Connect (OIDC) login modules (MaconomyOIDC and MaconomyAzureOIDC) were unable to consume OAuth Bearer tokens. This meant that it was not possible to use other OAuth login flows in parallel with the OIDC Client Credentials flow.

From Maconomy 2.4.7, the RESTapi accepts Bearer tokens when an OIDC login module is configured, and the OIDC login modules are able to process these tokens, if they are valid JSON Web Tokens (JWT).

For Azure, an example Curl command for obtaining a client bearer token is shown below, where the values in brackets ({…}) are system specific:

```
curl -X POST https://login.microsoftonline.com/{tenant_id}/oauth2/token
^
-F Content-Type=application/x-www-form-urlencoded ^
-F host=login.microsoftonline.com ^
-F scope=https://{sub_domain}.onmicrosoft.com/.default ^
-F client_id={client_id} ^
-F client_secret={client_secret} ^
-F grant_type=client_credentials ^
-F resource={resource_id}
```

Note: For Azure, it is important to use the ‘oauth2/token’ authorization endpoint, rather than the ‘oauth2/2.0/token’ endpoint introduced as a part of the Microsoft Identity Platform, as the ‘2.0’ endpoint is currently not compatible with Azure OIDC.

If authentication is successful, the returned JSON object has the form:

```
{"token_type":"Bearer", […], "access_token":"{access_token}"}
```

The value of ‘{access_token}’ can subsequently be used to perform a Maconomy login and obtain a session reconnect token:

```
curl -X GET http://{maconomy_host}:{port}/containers/v1/{shortname} ^
-H "Maconomy-Authentication: X-Reconnect" ^
-H "Authorization: Bearer {access_token}"
```

About Deltek

Better software means better projects. Deltek is the leading global provider of enterprise software and information solutions for project-based businesses. More than 23,000 organizations and millions of users in over 80 countries around the world rely on Deltek for superior levels of project intelligence, management and collaboration. Our industry-focused expertise powers project success by helping firms achieve performance that maximizes productivity and revenue. www.deltek.com