Deltek Maconomy 2.4.2

Microsoft Azure Single Sign-On (SSO) for Maconomy

July 13, 2018

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 July 2018.

Deltek’s software is also protected by copyright law and constitutes valuable confidential and proprietary information of Deltek, Inc. and its licensors. The Deltek software, and all related documentation, is provided for use only in accordance with the terms of the license agreement. Unauthorized reproduction or distribution of the program or any portion thereof could result in severe civil or criminal penalties.

Contents

Overview

This document contains details on how to configure and use Microsoft Azure Single Sign-On (SSO) for Maconomy. It walks you through the process for signing up for a Microsoft Azure SSO account, completing configuration in Azure Active Directory (AAD), and setting up user access in Maconomy.

Single Sign-On with Microsoft Azure Active Directory

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

- Complete Prerequisites
- Configure Maconomy Applications in Windows Azure Active Directory
- Register Client Applications
- Add Users to Azure Active Directory
- Configure the Coupling Service – New Configuration*
- Configure the Coupling Service – Upgrade Azure Configuration*
- Configure Users in Maconomy

*This guide contains information on both configuring the Coupling Service for the first time as well as upgrading from an existing configuration.

If you are configuring the Coupling Service for the first time, see **Configure the Coupling Service – New Configuration**.

If you are upgrading from an existing configuration, see **Configure the Coupling Service – Upgrade Azure Configuration**

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.

Configure Azure AD Connect

For more background information about Azure AD Connect, see Microsoft's Integrating your on-premises identities with Azure Active Directory. This describes what Azure AD Connect is and how it works.

Prerequisites

Review and complete the prerequisites for Azure AD Connect as outlined by Microsoft's Prerequisites for Azure Active Directory Connect (Azure AD Connect).

Hardware requirements are also listed in this article.

Deltek recommends that you do **not** install Azure AD Connect on your domain controllers.

Configuration Steps for Azure AD Connect

Complete these steps after you have signed up for a Microsoft Azure AD account.

To configure Azure AD Connect:

1. Download and install the Microsoft Online Services Sign-In Assistant for IT Professionals RTW (msoidcli_64.msi) from the following Microsoft web page:

   Microsoft Online Services Sign-In Assistant for IT Professionals RTW

   Refer to the installation instructions on the web page.

2. Click the following Microsoft link to download and install Azure Active Directory Module for Windows PowerShell for the 64-bit version (AdministrationConfig-en.msi):

   Azure Active Directory Module for Windows PowerShell (64-bit version)

3. Download and install Microsoft Azure Active Directory Connect (AdministrationConfig-en.msi) using the following Microsoft link: Azure Active Directory Connect.

   - Review the account and permissions information at the following Microsoft web page: Azure AD Connect: Accounts and Permissions.
   - You must set up the following required accounts with a username and password:
     - Windows Azure Active Directory (Global Administrator)
     - On-Premise Active Directory (Enterprise Administrator)

- For more information, see Managing Azure AD Connect.
- Depending on the size of your on-premise Active Directory, the installation of Azure AD Connect can take some time, especially if you select the option to synchronize users at the end of the installation.

4. Verify that users are synchronized with Windows Azure AD by logging into your Windows Azure portal.
5. Test a user on the Microsoft Apps portal at: https://myapps.microsoft.com.
   - No applications show but you can test authentication.
   - Use an existing user name and password for the test.

For troubleshooting information, see:
https://msdn.microsoft.com/library/azure/jj151834.aspx.

Automatic synchronization of domain users and automatic mapping of Azure users to Maconomy users is considered outside the scope of Maconomy, and must be accomplished via customizations.

Without customization, Maconomy users must therefore manually be associated with Azure users.

See the **Configure AAD with Limited Access to Maconomy** section for more information.

To login manually, users can click the Cancel button on the Azure login dialog and enter their credentials.

Configure Maconomy Applications in Windows Azure Active Directory

The following procedures prepare Maconomy applications for use with Azure Active Directory.

Create and Select an Azure Active Directory

To create and select an Azure Active Directory:

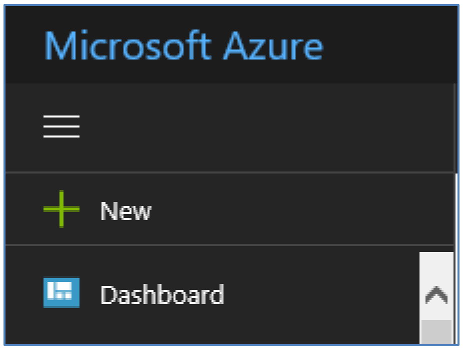
1. Log in to the new Azure portal at https://portal.azure.com/

These steps apply to the new Azure AD portal, which has replaced the classic portal.

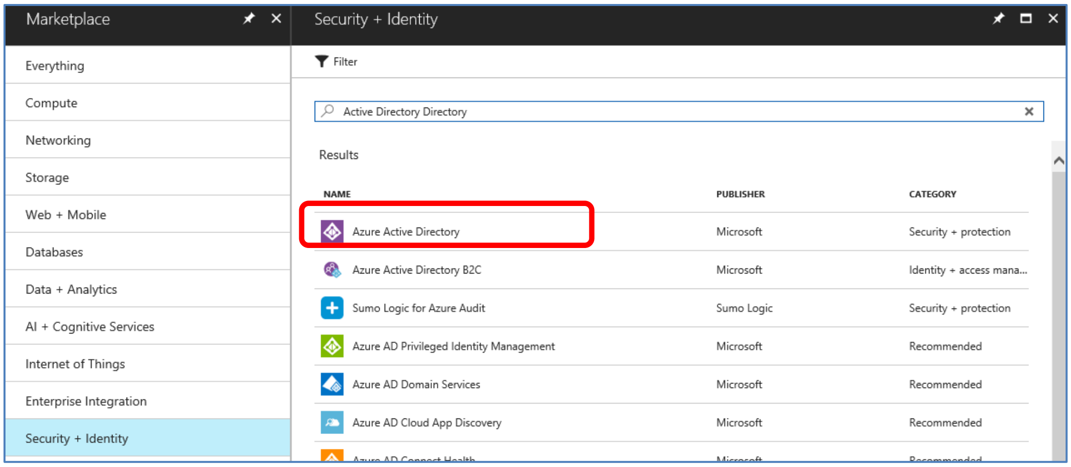
The new portal uses some new terminology:

- The portal has a ***left bar*** that you use to navigate and access resources and tools.
- When you click an item in the left bar to perform a task, the bar expands into a series of windows called ***blades*** on the right.
- The blades list the steps/options that you follow on your ***journey*** to complete a task. In this case, the journey is adding and configuring the Maconomy applications.

2. Log in to Microsoft Azure and Click **New** to create a directory.



3. In the **New** blade, type “Azure Active Directory” into the **Search the Marketplace** box and click **Enter**.
4. In the **Marketplace** blade, click **Security + Identity.**
5. In the **Security + Identity** blade select Azure Active Directory. Do not select the Azure Active Directory B2C option.

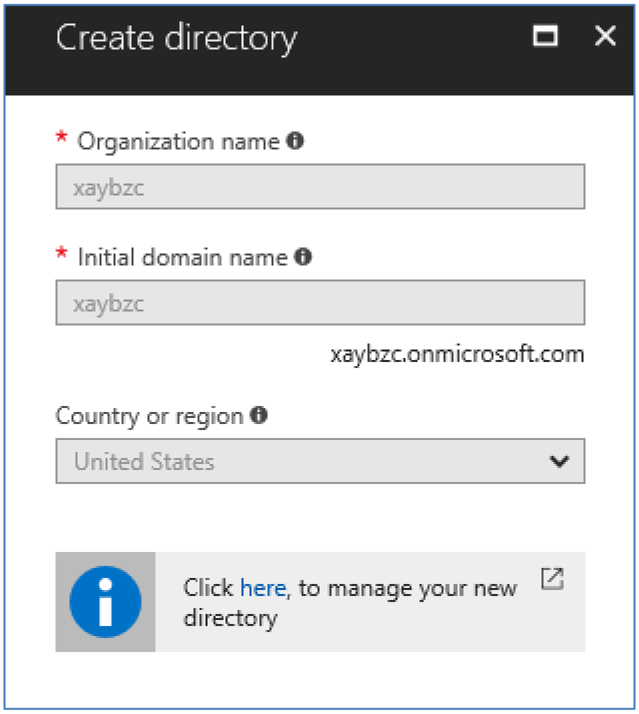


Active Directory Directory

Results

NAME	PUBLISHER	CATEGORY
Azure Active Directory	Microsoft	Security + protection
Azure Active Directory B2C	Microsoft	Identity + access mana...
Sumo Logic for Azure Audit	Sumo Logic	Security + protection
Azure AD Privileged Identity Management	Microsoft	Recommended
Azure AD Domain Services	Microsoft	Recommended
Azure AD Cloud App Discovery	Microsoft	Recommended
Azure AD Connect Health	Microsoft	Recommended

6. In the **Azure Active Directory** blade, click the **Create** button at the bottom to open the **Create directory** blade.
7. Fill out the **Create directory** form and click **Create**.


Create directory

* Organization name: xaybzc

* Initial domain name: xaybzc

xaybzc.onmicrosoft.com

Country or region: United States

Click here, to manage your new directory

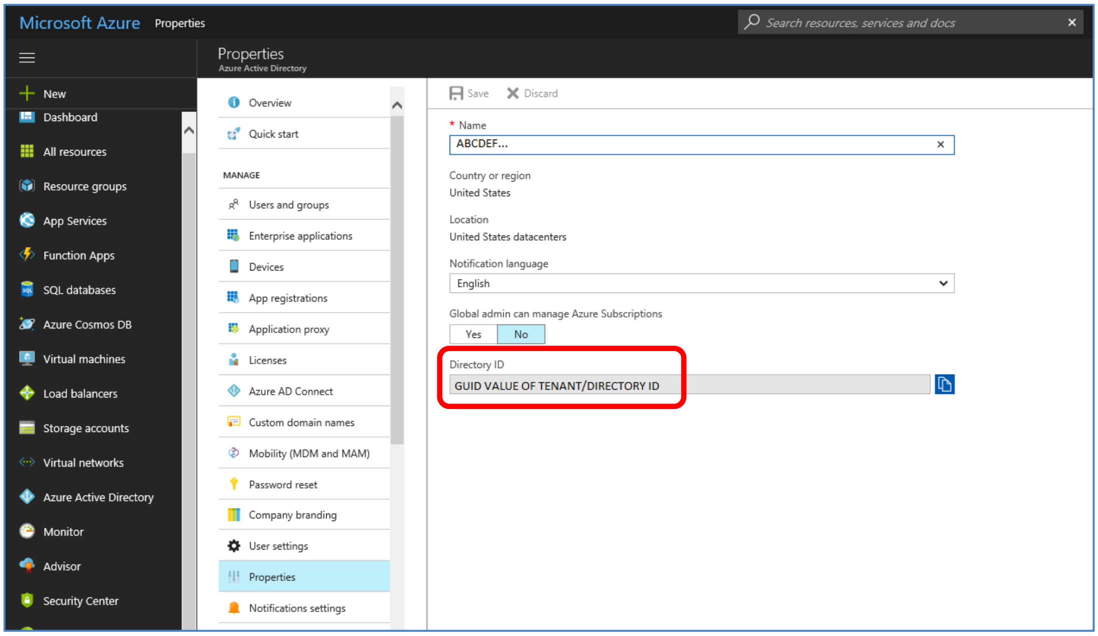
Identify your Tenant ID / Directory ID

To identify your Tenant ID:

1. Log in to the new Azure portal at https://portal.azure.com/

If you have already created a new directory or have more than one directory, click your Azure login in the top right corner, and at the bottom of the dropdown (in the Directory section), select the Directory.

2. In the **Left bar** of the Azure portal, Click **Azure Active Directory** then select **Properties** in the **Manage** section**.**
3. Click the Clipboard icon next to the **Directory ID** field to copy the value to the clipboard and save it for later.



* Name: ABCDEF...

Country or region: United States

Location: United States datacenters

Notification language: English

Global admin can manage Azure Subscriptions: Yes [✓ No]

Directory ID: GUID VALUE OF TENANT/DIRECTORY ID

Note the Tenant ID. You need this value for coupling service configuration (described in the next section).

> If you are upgrading, also note the **Client Secret** on the application. You will need this value when performing the upgrade process described in the **Configure the Coupling Service – Upgrade Azure Configuration** section in this document.

Register Maconomy Server and Coupling Service

If AAD is to provide authorization in addition to authentication, then you need to register the Coupling Service as an application, giving it a unique Azure Client ID that identifies it within the AAD. Once you have done this, you can restrict user access to Maconomy on the level of the AAD by using several mechanisms depending on the needs of the particular installation (for example, allowing access to users who belong to a certain group).

The authentication layer of the Coupling Service only grants access to users whom the AAD has verified have access to the Azure Client ID associated with Maconomy.

You can skip this step if you only intend to use the internal authorization mechanisms of Maconomy to restrict user access to resources.

To register the Maconomy server and the Coupling Service:

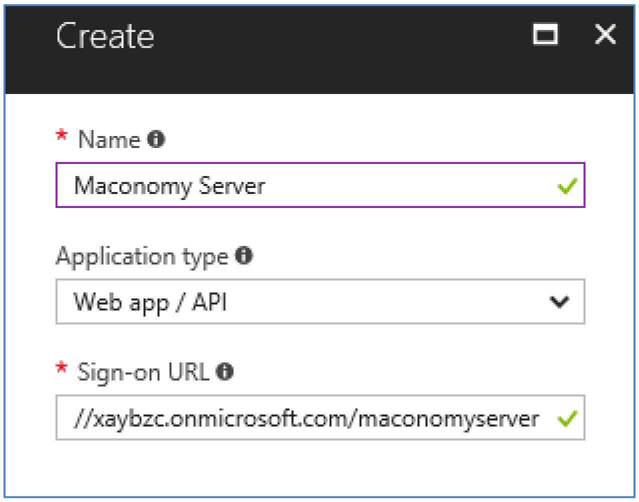
1. In the **Left bar** of the Azure portal, Click **Azure Active Directory**.
2. Click **App registrations** in the **Manage** section**.**
3. Click **New application registration** at the top of the screen.

4. On the Create dialog box:

- In the **Name** field, enter a descriptive name such as **Maconomy Server**.
- For **Application type**, select **Web App / API**.
- In the **Sign-On URL** field and the **App ID URI** fields, enter https://<directory>.onmicrosoft.com/maconomyserver.

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

  The URLs will be verified and should have a green check mark beside them.



Create

* Name

Maconomy Server ✓

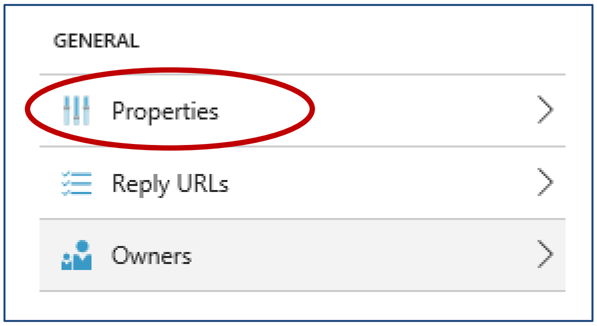
Application type

Web app / API

* Sign-on URL

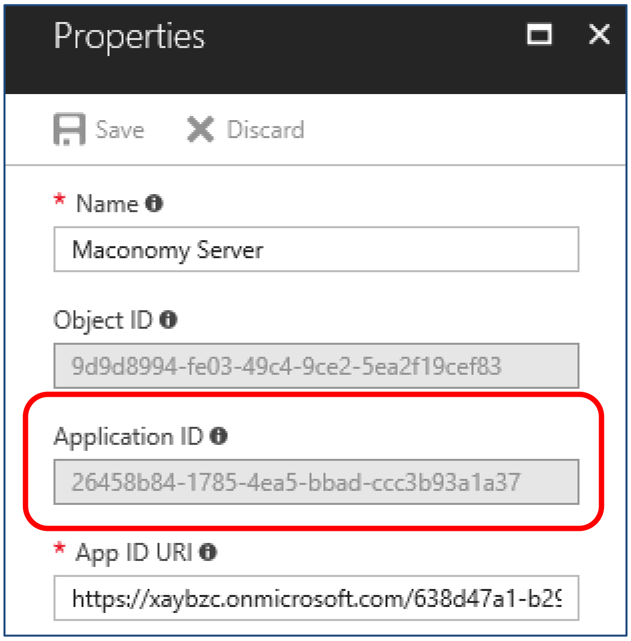
//xaybzc.onmicrosoft.com/maconomyserver ✓

5. Click the **Create** button to create and save the application.
6. Click on the **Maconomy Server** application in the list of applications to display its Settings.
7. In the General Section of the Settings blade, click on **Properties** to open the Properties blade.



8. Right-click and copy the value of the **Application ID** field in the Properties blade to use later.

- In the classic Azure AD portal, this value was labeled **Client ID**
- If the clipboard icon is not available, right-click the value in the **Application ID** field and choose **Copy** to copy the value to the clipboard and save it to use later.
- You will use this **Application ID** value as the **Client Secret** when performing the steps described in, depending on your installation, either the Configure the Coupling Service – New Configuration or the **Configure the Coupling Service – Upgrade Azure Configuration** section in this document.



Properties

Save Discard

* Name

Maconomy Server

Object ID

9d9d8994-fe03-49c4-9ce2-5ea2f19cef83

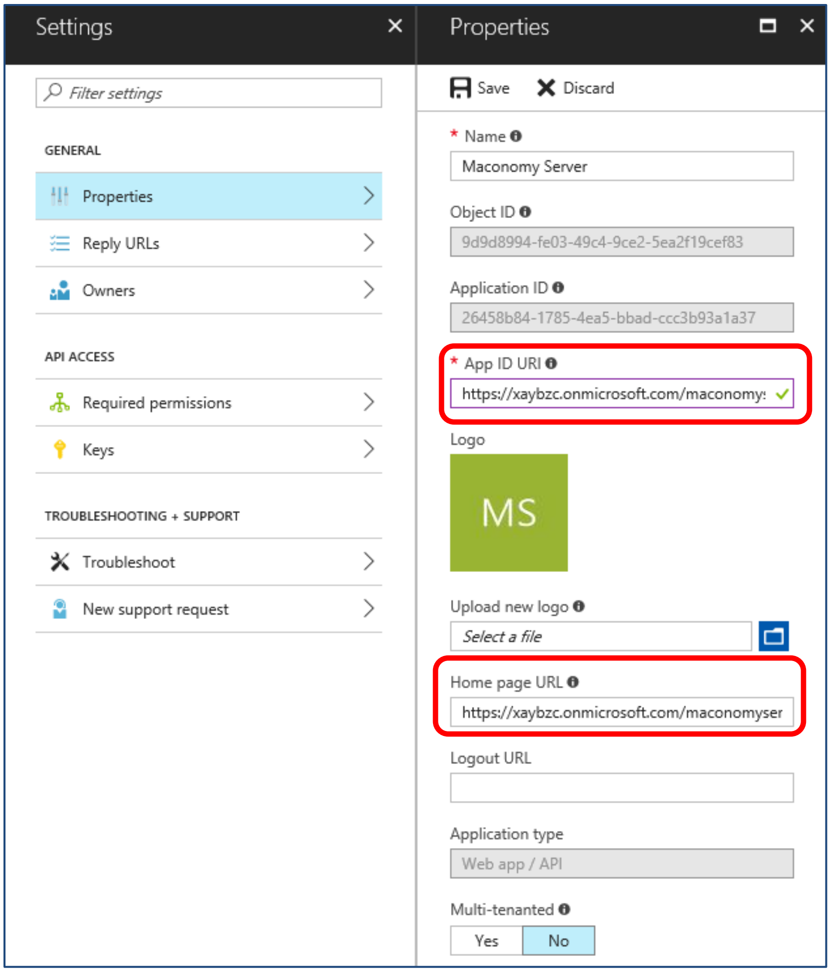
Application ID

26458b84-1785-4ea5-bbad-ccc3b93a1a37

* App ID URI

https://xaybzc.onmicrosoft.com/638d47a1-b2¢

9. On the Properties blade, enter https://<directory>.onmicrosoft.com/maconomyserver for both and APP-ID URI and the Home page URL, replacing <directory> with the name of the AAD (For example, xaybzc).



* Name: Maconomy Server

Object ID: 9d9d8994-fe03-49c4-9ce2-5ea2f19cef83

Application ID: 26458b84-1785-4ea5-bbad-ccc3b93a1a37

* App ID URI: https://xaybzc.onmicrosoft.com/maconomy: ✓

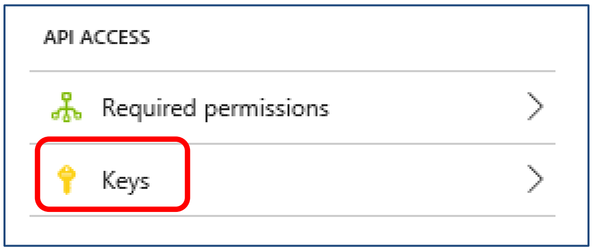
Home page URL: https://xaybzc.onmicrosoft.com/maconomyser

Logout URL:

Application type: Web app / API

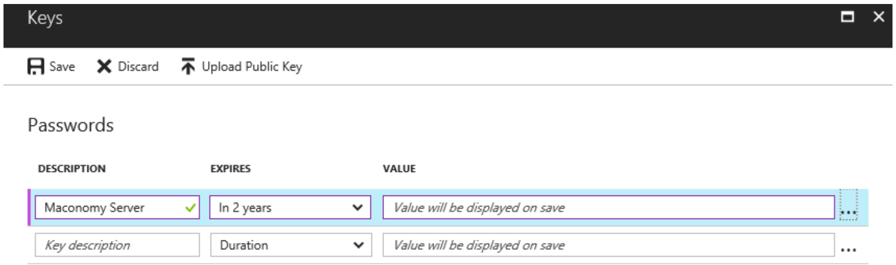
Multi-tenanted: Yes [✓ No]

9. In the API ACCESS section of the Settings blade, click **Keys** to open the Keys blade to create a Key.



10. Enter a description in the **Description** field and click the drop-down icon to select the duration of the key that you are about to generate.

    Deltek recommends that you create a two year key.



Passwords

DESCRIPTION	EXPIRES	VALUE
Maconomy Server ✓	In 2 years	*Value will be displayed on save*
Key description	Duration	*Value will be displayed on save*

11. Click **Save** to create and generate the key.

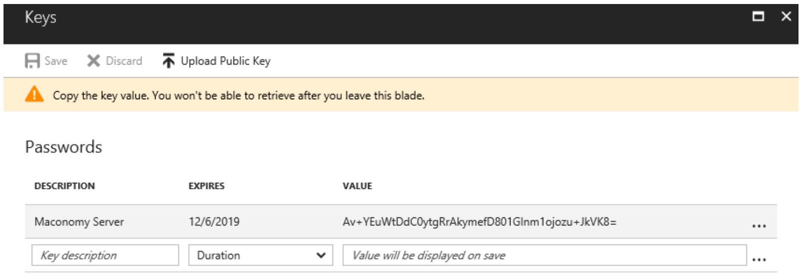
Before you leave this screen, you **must** complete the next step.

12. **Before you leave the screen that displays the key value, take note of the key value.** You must do this now because, after you leave this screen, you cannot return to the screen to see the value.

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

    You will use this **Application ID** value as the **Client Secret** when performing the steps described in, depending on your installation, either the Configure the Coupling Service – New Configuration or the Configure the Coupling Service – Upgrade Azure Configuration section in this document.

    Once you copy the value, close the Keys blade.



Copy the key value. You won't be able to retrieve after you leave this blade.

Passwords

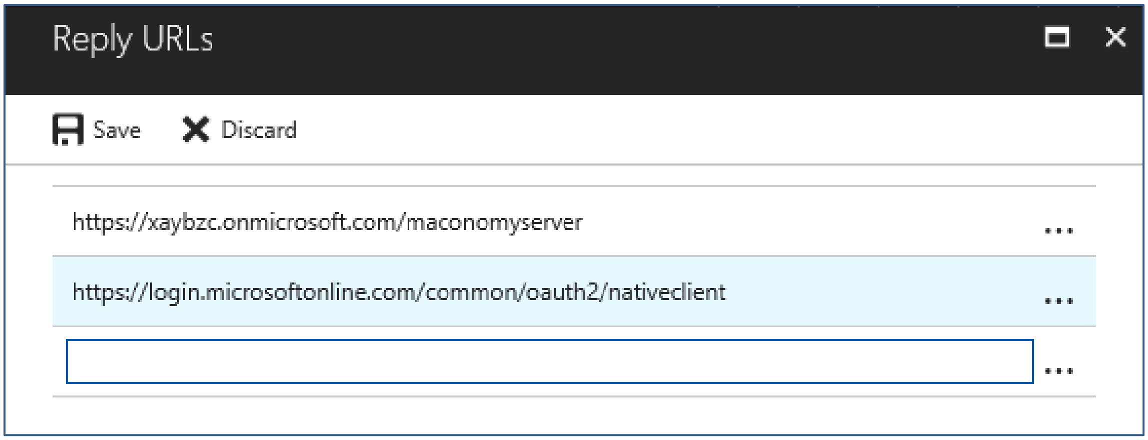
DESCRIPTION	EXPIRES	VALUE
Maconomy Server	12/6/2019	Av+YEuWtDdC0ytgRrAkymefD801Glnm1ojozu+JkVK8=
Key description	Duration	*Value will be displayed on save*

If you do not have the key value when you need to enter it in later, you must delete the key in Azure AD and recreate it.

13. Navigate to **App registrations** and select the Maconomy Server application. This will open the Settings blade.

14. In the General section of the Settings blade, click **Reply URLs**. This will open the **Reply URLs** blade.

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



https://xaybzc.onmicrosoft.com/maconomyserver

https://login.microsoftonline.com/common/oauth2/nativeclient

15. Add the following reply URLs for each of the client applications that will use Azure for authentication:
    - **Workspace Client:**

      https://login.microsoftonline.com/common/oauth2/nativeclient
    - **iAccess**: Refer to the iAccess Technical Installation Guide for the steps.
    - **Touch**: Refer to the Touch Technical Installation Guide for the steps.
    - **Portal**: TBD
16. Click **Save**.

Register Maconomy Native Client Application

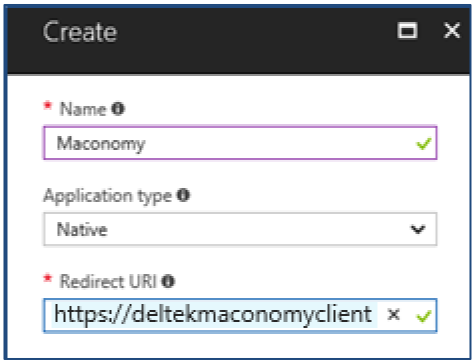
To add and configure the Maconomy Client in Azure AD:

1. On the Left bar of your Microsoft Azure AD portal, navigate to **Azure Active Directory » *<DirectoryName>***.
2. In the MANAGE section, click on **App registrations**.

> If you created applications using the classic Azure AD portal, your applications will already be listed and you do not need to re-add them.

3. Click **New application registration**.

4. On the Create dialog box:
    - In the **Name** field, enter **Maconomy**.
    - For **Type**, select **Native.**
    - On the **Redirect URI box**, enter **https://deltekmaconomylient**, then click the Tab key to exit the field and enable the **Create** button. This must be a valid URI, but not a reachable URL.

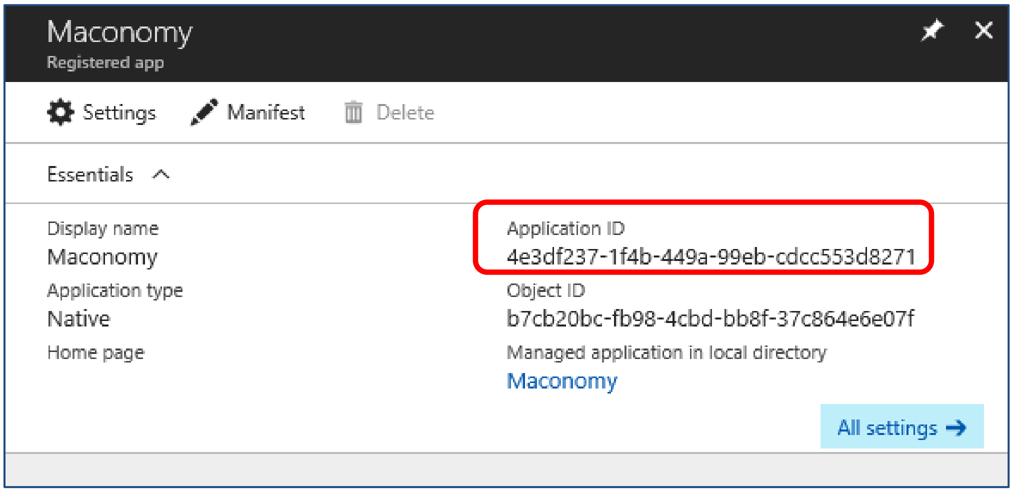

Create

* Name: Maconomy

Application type: Native

* Redirect URI: https://deltekmaconomyclient

5. Click the **Create** button to create and save the application.
6. Click on the Maconomy application in the list of applications to display the Settings blade of the Maconomy application.
7. Note the value in the **Application ID** field, to the left of the Settings blade.


Maconomy
Registered app

Display name: Maconomy

Application type: Native

Home page

Application ID: 4e3df237-1f4b-449a-99eb-cdcc553d8271

Object ID: b7cb20bc-fb98-4cbd-bb8f-37c864e6e07f

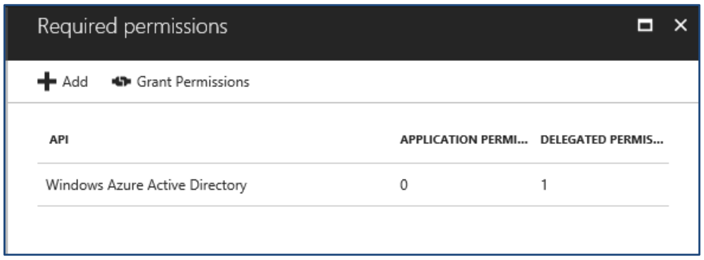
Managed application in local directory: Maconomy

- In the classic Azure AD portal, this value was labeled **Client ID**
- If the clipboard icon is not available, right-click the value in the **Application ID** field and choose **Copy** to copy the value to the clipboard and save it to use later.
- You will use this **Application ID** value as the **Client Secret** when performing the steps described in, depending on your installation, either the Configure the Coupling Service – New Configuration or the Configure the Coupling Service – Upgrade Azure Configuration section in this document.

Set Up Trust Between the Azure Maconomy (Client) Application and Maconomy Server Application

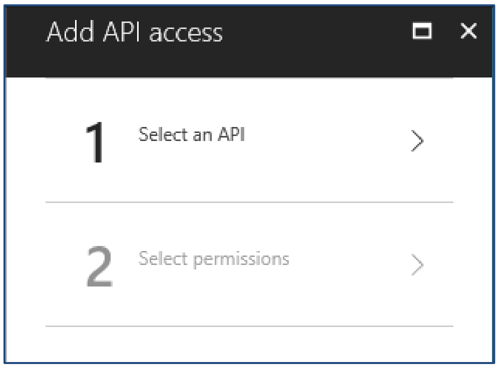
To Set Up Trust Between the Maconomy (Client) Application and Maconomy Server Application:

1. In the **Left bar** of the Azure portal, Click **Azure Active Directory**.
2. In the **Manage** section, Click **App registrations**.
3. Click the Maconomy Server Web App.
4. In the **API Access** section of the **Settings** blade, click **Required permissions**.

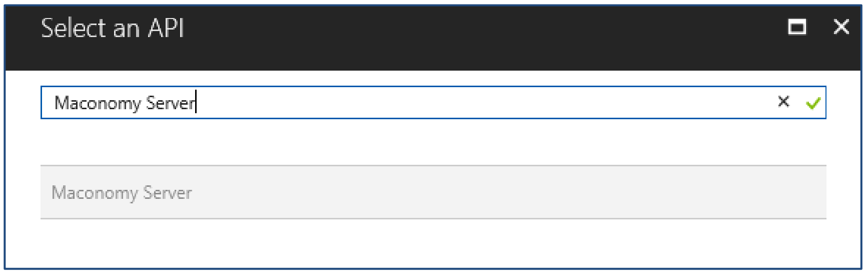


API	APPLICATION PERMI...	DELEGATED PERMIS...
Windows Azure Active Directory	0	1

5. On the **Required permissions** blade, click **Add**.



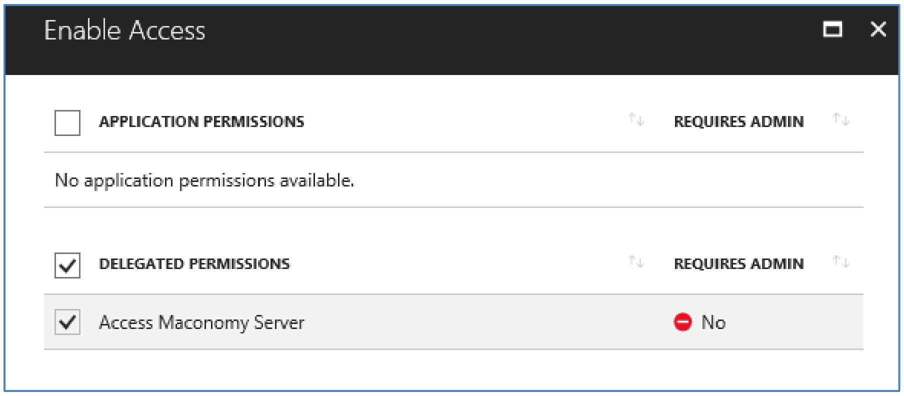
6. Click **Select an API**.
7. On the **Select an API** screen, enter **Maconomy Server** in the **Search for other applications with Service Principal name** field.



Maconomy Server

Maconomy Server

8. Click on **Maconomy Server** (in the results) and click **Select** (at the bottom of the screen).
9. On the Enable Access blade, click **Access Maconomy Server** and click **Select** (at the bottom of the screen)**.**



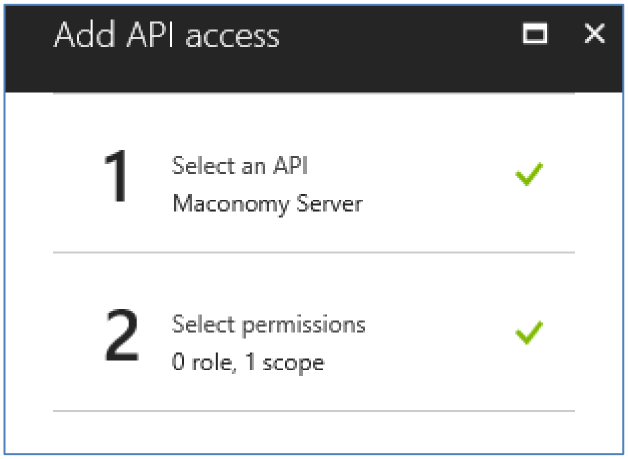
Enable Access

□ APPLICATION PERMISSIONS	REQUIRES ADMIN
No application permissions available.	

☑ DELEGATED PERMISSIONS	REQUIRES ADMIN
☑ Access Maconomy Server	⛔ No

10. Click **Select** to Save the settings.

11. On the **Add API access** blade, click **Done** to complete the permissions assignment.

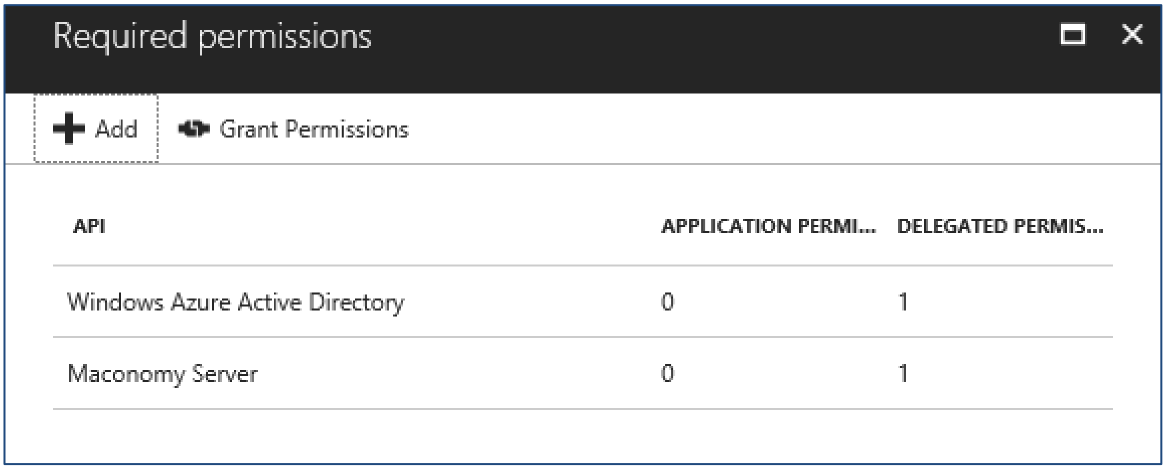


Add API access

1 Select an API
Maconomy Server ✓

2 Select permissions
0 role, 1 scope ✓

12. The Maconomy Server application will now appear in the **Required permissions** blade of the Maconomy registered application.



Required permissions

API	APPLICATION PERMI...	DELEGATED PERMIS...
Windows Azure Active Directory	0	1
Maconomy Server	0	1

Optional: Configure AAD with Limited Access to Maconomy Server

By default, the AAD allows any of its authenticated users to have access to the Maconomy application. This does not mean that any AAD user can now log in to Maconomy, however. Only AAD users specified as the network username of a corresponding Maconomy user can log in as that user, and each Maconomy user can have at most one network username defined.

The use of AAD access restriction is, therefore, optional, but might be preferred in cases where advanced access policies are required. For example, you can configure AAD to require that users of a certain group must use multi-factor authentication when accessing Maconomy (requires Premium AAD subscription).

To configure limited access to Maconomy Server:

1. In the **Left bar** of the Azure portal, Click **Azure Active Directory**.
2. In the **Manage** section, Click **Enterprise applications**.
3. Select the Maconomy Server application that was just added from the Application Gallery to open it.
   - If you don’t see the Maconomy Server application, click on **All applications** to the left, then in the search box, type **Maconomy** and hit the **Apply** button to display all the apps that begin with the word Maconomy and select **Maconomy Server.**
4. Select **Users and groups**, and then select **Add user**.
5. Configure the users that have access to Maconomy.

Note: For a standard AAD, you can only configure a list of individual users with access to a given application. Group management and multi-factor authentication are only available for Premium subscriptions.

Register Client Applications

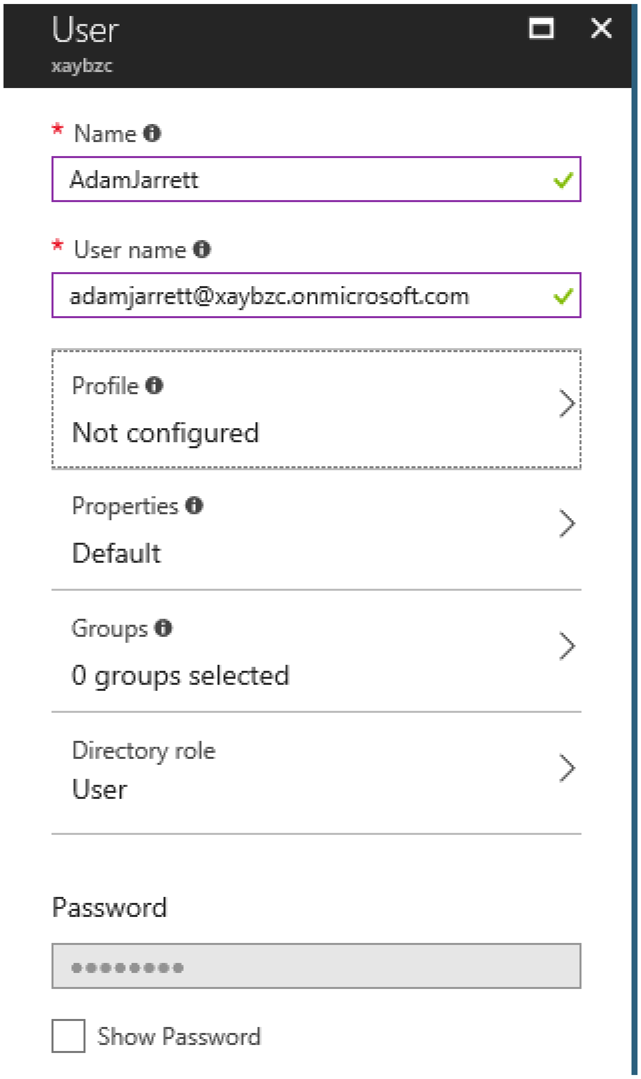
A previous version of this document contained instructions for registering a separate Azure application for each client application that was to use Azure for authentication. It is no longer necessary to register separate client applications. To migrate from a multi-application setup, add all REPLY URL entries from each client application to the Maconomy Server application.

Add Users to Azure Active Directory

You can add users directly to Azure Active Directory via the Azure Management portal.

To add users in the portal:

1. On the Left bar of your Microsoft Azure AD portal, navigate to **Azure Active Directory » *<DirectoryName>***.
2. In the Manage section, Click on **All Users**.
3. Click on the **New User** button at the top of the screen.
4. Enter user information in the dialog boxes.
5. On the last page, click **Show password** to obtain the temporary password for the user and click Save.



User
xaybzc

* Name: AdamJarrett

* User name: adamjarrett@xaybzc.onmicrosoft.com

Profile: Not configured

Properties: Default

Groups: 0 groups selected

Directory role: User

Password: ●●●●●●●●

□ Show Password

Configure the Coupling Service – New Configuration

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:

   ```
   org.eclipse.equinox.security.auth.module.ExtensionLoginModule sufficient
   extensionId=”com.maconomy.lib.coupling.MaconomyAzureADLoginModule”

   tenantId=”<Tenant ID>”

   clientId=”<Client ID>”

   clientSecret=”<Client Secret>”;
   ```

   Replace the highlighted placeholders by the appropriate values. See the previous sections for how to obtain the values of **Tenant ID**, **Client ID**, and **Client Secret**.

Configure the Coupling Service – Upgrade Azure Configuration

Complete the following steps only if you are upgrading from an existing Azure configuration. If you are configuring the Coupling Service for the first time, follow the steps in the previous section called **Configure the Coupling Service – New Configuration**.

If you are migrating the configuration from a previous version of the Coupling Service, your security configuration file will have a section in the following format:

```
org.eclipse.equinox.security.auth.module.ExtensionLoginModule sufficient
extensionId=”com.maconomy.lib.coupling.MaconomyAzureADLoginModule”

tenantId=”<Old Tenant ID>”

clientId=”<Old Client ID>”

serverId=”<Old Server ID>”;
```

To complete the migration:

1. Make a copy of the section and comment out the old version by prepending every line with two forward slashes (//).

   Modify the section as follows:

   ```
   org.eclipse.equinox.security.auth.module.ExtensionLoginModule sufficient
   extensionId=”com.maconomy.lib.coupling.MaconomyAzureOIDCLoginModule”

   tenantId=”<Old Tenant ID>”

   clientId=”<Old Server ID>”

   clientSecret=”<Client Secret>”
   ```

   Note: You must transfer the value of **Old Server ID** to the “clientId” directive, overwriting the **Old Client ID**.

   Obtain the **Client Secret** by following the instructions in the **Create and Select an Azure Active Directory** section above.

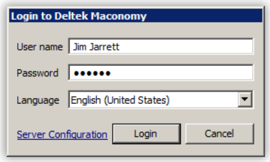
   When migrating, there is already an application registered identified by **Old Client ID**. Generate a key for that application and use it for the **Client Secret**.

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 AAD user `jimjarrett@bobedst.onmicrosoft.com` who you added to the AAD in Add Users to Azure Active Directory the “Adding Users” section above.

To configure users in Maconomy:

1. Log in to Maconomy as Administrator, or as the user who you wish to configure. You must use traditional Maconomy username/password credentials to do this—press escape if the Azure login dialog appears.



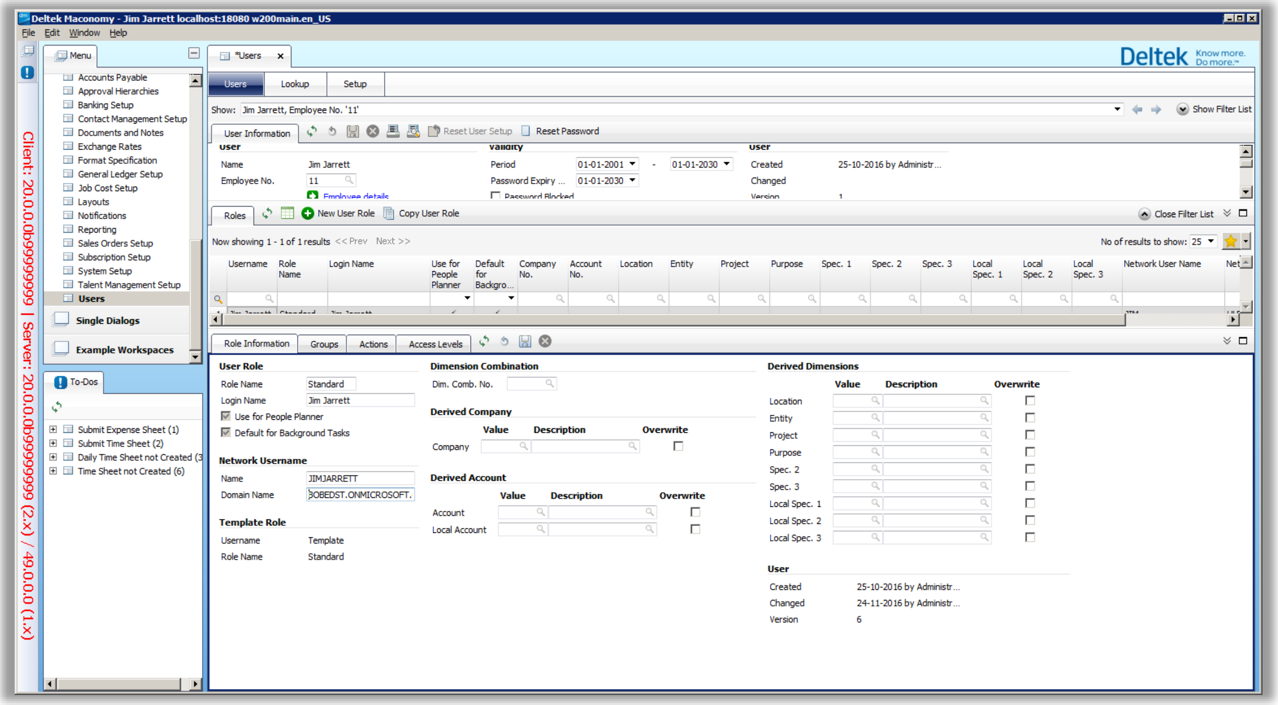
Login to Deltek Maconomy

User name: Jim Jarrett
Password: ••••••
Language: English (United States)

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.



Deltek Maconomy - Jim Jarrett localhost:18080 w200main.en_US

Show: Jim Jarrett, Employee No. '11'

User Information

User
Name: Jim Jarrett
Employee No.: 11

Validity
Period: 01-01-2001 - 01-01-2030
Password Expiry ...: 01-01-2030

User
Created: 25-10-2016 by Administr...

Now showing 1 - 1 of 1 results

Role Information

User Role
Role Name: Standard
Login Name: Jim Jarrett
☑ Use for People Planner
☑ Default for Background Tasks

Network Username
Name: JIMJARRETT
Domain Name: BOBEDST.ONMICROSOFT.

Template Role
Username: Template
Role Name: Standard

User
Created: 25-10-2016 by Administr...
Changed: 24-11-2016 by Administr...
Version: 6

5. Save the settings.
   Note: Maconomy may ask you to enter a password for the user.