Azure AD users

Contents

How does it work?

The goal is to use **Azure Active Directory** as an identity provider for Trustelem.
It requires the creation of an "app" in Azure AD admin console for authorizing Trustelem to request Azure AD data using API.
For the synchronization, Trustelem uses the Microsoft API to list the groups and their members.
For the authentication, Trustelem sends an authentication request using Microsoft API and if it is validated, authenticates the user on Trustelem.

Prerequisites

No prerequisite, every steps of the setup are listed in the following chapter.
Note: it is not possible to authenticate users with their AzureAD password if Azure delegates the authentication to an external Identity Provider such as Trustelem.

Setup

- Create a directory Azure Active Directory on Trustelem
  - Go on the tab **Directories**
    `https://admin-mydomain.trustelem.com/app#/directories`
  - Click on **Create** and select **Azure Active Directory**.

- Define the target Azure subscription
  - In the field **Tenant ID** enter here the tenant ID of your Azure subscription, e.g. contoso.onmicrosoft.com

- Authorize Trustelem to connect to Azure
  - Connect to https://portal.azure.com with an admin account
  - Go to **Azure Active Directory** then **App registration**
  - Click on button **+Add**
    - Enter a name
    - Select **Accounts in this organizational directory only**

    - Select a platform **Web** in **Redirect URI** and enter the URL: https://mydomain.trustelem.com
  - Click on **Register**
  - In section **Expose an API**, add a permission and choose **Microsoft Graph**
    - Click on **Application permissions**
    - Select permission **Directory.Read.All - Read directory data** in section **Directory**
    - Click on button **Add permission** for applying the selected API.
  - Apply these permissions by clicking on **Grant admin consent for [Your Company]**
  - Go to **Overview**, copy the value given in Application (client) ID and paste it in the field **Client ID** on Trustelem
  - Go to **Certificates and secrets**, click on **New client secret**, give it a name and click on **Add**
  - Then copy the field **Value** and paste it in the field **Client Secret** on Trustelem
  - If needed, in section **Owner**, add an administrator for this app

- Use Azure passwords for authenticating users on Trustelem (optional)
  - On the Azure admin page of the app previously created, go to **Authentication**
  - In **Advanced Settings**, in the field **Allow public flows**, check **yes** for the option **Enable the following mobile and desktop flows**
- On Trustelem, enter the Client ID value again in the field **Client ID** (needed for compatibility with older Azure versions)

Notes:

- If you have the application Office 365 in Trustelem, that means you have federated an Azure domain.
- For a federated domain, Azure AD disable user passwords.
- If the passwords are disabled, Trustelem can't get them using API and therefore, can't use Azure passwords for authenticating users on Trustelem.

Revision #6
Created 1 July 2022 08:13:09 by WALLIX Admin
Updated 25 October 2023 07:09:49 by WALLIX Admin