Recast

Microsoft Entra ID

Last Modified on 04.22.26

The Microsoft Entra ID (Azure AD) identity source allows you to register an application with Microsoft Entra ID (Azure AD) as a mean to authenticate against Application Workspace. This way you will leverage your Microsoft Entra ID (Azure AD) as the single point of entry. See SSO with Microsoft Entra ID (Azure AD) for configuration instructions.

You can connect Microsoft Entra ID (formerly Azure AD) to the following national clouds:

- Azure portal for US Government
- Azure portal China (operated by 21Vianet)
- Azure portal (global service).

For more details, see Microsoft Entra authentication & national clouds – Microsoft identity platform | Microsoft Learn

Create identity source dialog box

The following options are available in this dialog box:

- Microsoft Entra ID (Azure AD) environment – to connect to Azure portal (global service)
- Custom environment – to connect to Azure portal for US Government or China (operated by 21Vianet)

Detailed view of the Microsoft Entra ID (Azure AD) identity source

See below the description of each screen in the detailed view of of the Microsoft Entra ID (Azure AD) identity source, and what actions you can perform in each of them.

Overview screen

Here you can configure a few basic options for the identity source.

Name – The name of the identity source. In the case of Microsoft Entra ID (Azure AD), we recommend you use the same value as the NetBIOS name of the it.
Type – The type of identity source.
Hidden – When an identity source is hidden, it will not appear on the login screen.

> Note that the **Name** and **Type** cannot be changed once the identity source is created.

Settings screen

It is required you register a new application in the Azure Portal before you can configure the settings for your Microsoft Entra ID (Azure AD) identity source. Below you find a list of its configurable settings.

Application section
Application ID – The value of the **Application (client) ID** field in Azure Portal > **Overview** page of the Microsoft Entra ID (Azure AD) app registration.
Client secret – The Microsoft Entra ID (Azure AD) app registration secret.
Use application ID as resource – When selected, the application ID will be used to request access to the Microsoft Entra ID (Azure AD). Otherwise, the default Azure AD Graph ID will be used.
Use redirect URI – The site to which the authorization server directs the user when the app has been successfully approved

and an authorization code or access token has been issued. The redirection URL needs to be encoded to work properly.

OAuth 2 url's section

Fetch OAuth 2 url's – If you click this button, the system will prefill all the fields in this section and the**Microsoft Graph** section, based on a Microsoft Entra ID (Azure AD) tenant ID.

Authorization URI – The value of the **OAuth 2.0 authorization endpoint (v1)** field in Azure Portal > **Overview** page > **Endpoints** tab of the Microsoft Entra ID (Azure AD) app registration. For example: `https://login.microsoftonline.com/[Tennant ID]/oauth2/authorize`

Token URI – The value of the **OAuth 2.0 token endpoint (v1)** field in Azure Portal > **Overview** page > **Endpoints** tab of the Microsoft Entra ID (Azure AD) app registration. For example: `https://login.microsoftonline.com/[Tennant ID]/oauth2/token`

Logout URI – The logout URI provided by the Microsoft Entra ID (Azure AD) app registration. For example: `https://login.microsoftonline.com/[Tennant ID]/oauth2/logout?post_logout_redirect_uri=< redirection URL >` The redirection URI needs to be encoded to work properly.

JSON Web Key Set URI – The public key used to verify the signatures of JSON Web Tokens (JWTs).For more information, see Microsoft documentation.

Domain hint – You can provide Microsoft Entra ID (Azure AD) login page with a hint to which domain you want to authenticate. If the user has multiple active Microsoft Entra ID (Azure AD) sessions, and one session is matching the domain hint, then Microsoft Entra ID (Azure AD) will use that account and will not ask the user to select an account anymore. For example: `recastsoftware.com`

Microsoft Graph section

Graph endpoint – The Microsoft Graph API endpoint used to connect to the appropriate Azure environment—Global, US Government, or China—based on your organization's cloud deployment. Once prefilled by clicking the '**Fetch OAuth 2 url's** button, we do not recommend changing the endpoint manually. For more information, see Microsoft documentation.

Synchronization section

Photos – Select if photos need to be synchronized or not. This option requires*User.Read.All* permissions in Microsoft Entra ID (Azure AD). See Register an application in Azure Portal, step 9 and SSO with Azure Active Directory for more information.

Use delta synchronization – When selected, delta synchronization of the Microsoft Entra ID (Azure AD) will be enabled. This causes an initial full synchronization to be performed, after which only changes are incrementally synchronized per Application Workspace server. This reduces the time it takes to fetch all users and groups from Microsoft Entra ID (Azure AD) after the initial synchronization is completed.

Include groups that are not security enabled – Enable support for groups that are not security enabled within Microsoft Entra ID (Azure AD). Like Microsoft 365 groups. This feature requires the Access Manager license.

Modifications – What kind of modifications are allowed for Microsoft Entra ID (Azure AD). Additional permissions are needed for modifying group membership. See SSO with Microsoft Entra ID (Azure AD) for more information.

Authentication screen

Here you can configure the methods available to authenticate.

Token exchange – Allow the token exchange to be used by third party integrators. For this option you need to insert the Application ID URI which is located in Azure Portal > Microsoft Entra ID (Azure AD) > App registration > Manage > Expose an API.
For more information, see How to setup your exchange token.

Federated – Allow authentication via federation. For example: Active Directory Federation Service (AD FS).

Form Authentication – Allow the user to login via the Application Workspace login page (http/https).

Basic Authentication – Allow basic authentication.

Contacts screen

Enable contacts – If enabled, contacts from this identity source will be used.

Require Email – If enabled, all objects without an email address will be hidden.

Group – Only show members of a certain group.

Recast

Show attributes

Choose which attributes to be synchronized to Application Workspace.

Authenticator screen

Assign an authenticator to the identity source.

Authenticator – You can select one of the existing authenticators defined in Application Workspace.
Prefix – Insert a string to add before the username to form the base distinguished name (DN).
Suffix – Insert a string to add after the username to form the base distinguished name (DN).