Clearlogin - Azure Active Directory

In This Article

Overview

This article will show you how to configure Azure AD as an Identity Source with Clearlogin, which allows for authentication against user accounts in Azure AD.

> ⊘ When using Azure AD as an Identity Source for Clearlogin users will not be able to make password changes or resets via Clearlogin. Users and admins will have to perform password changes and resets via Microsoft's given methods.

Configuration Steps

Configuration: Clearlogin

- Sign into the **Clearlogin Admin Console:** https://admin.clearlogin.com
- In the left navigation bar, browse to: **Identity Sources**
- Click on the **New Identity Source** button, and then select **Azure AD**

- Display Name: Azure AD
- User Domain: yourdomain.com
- Access Tag: Azure AD
- Priority: 5
- Timeout: 10 seconds
- Click on **Create Open Identity Source**
- On the summary page, scroll down and **Copy** the **SSO Callback URL (Redirect URI)** to your clipboard.

SSO Login URL	
https://busterwolf.clearlogin.com/openid/azure/login	📋 Copy
SSO Logout URL	
https://busterwolf.clearlogin.com/logout	📋 Copy
SSO Callback URL (Redirect URI)	
https://busterwolf.clearlogin.com/openid/azure/callback	📋 Copy

- Click on **Edit.** We will come back to this page later.

Configuration: Azure AD

- Open a new tab in your browser and sign into the **Microsoft Azure AD portal** with a user account that has the **global admin** role: https://aad.portal.azure.com

- From the left navigation bar, select **Azure Active Directory**
- In the sub-nav bar, click on **App Registrations**
- Click on **+ New Registration** to create a new app registration for Clearlogin
- Name: **Clearlogin Connection**

* Name

The user-facing display name for this application (this can be changed later).

| Clearlogin Connection | ✓ |

- Supported Account Types: **Accounts in this organizational directory only...**

Supported account types

Who can use this application or access this API?

- ◉ Accounts in this organizational directory only (Single tenant)
- ○ Accounts in any organizational directory (Any Azure AD directory - Multitenant)
- ○ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

- Redirect URI (drop-down menu): **Web**
- Redirect URI (text field): **Paste in the SSO Callback URL you just copied from the Clearlogin portal.**

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

| Web ∨ | https://evolvenow.clearlogin.com/openid/azure_ad/callback | ✓ |

- Click on **Register** to create the app registration.

On the summary page, copy the **Directory (tenant) ID** to your clipboard.

🗑 Delete   🌐 Endpoints

Display name	: Clearlogin Connection
Application (client) ID	: 0e6678ca-8675-8675-8675-6050f0739ba1
Directory (tenant) ID	: 6dfd18d1-a139-a139-a139-63ad94a5fd98
Object ID	: 92b9ed9f-9d60-4412-82fa-101efef3f342

Configuration: Clearlogin

- Switch back to the **Clearlogin portal** tab in your browser
- Scroll down to the **Endpoint** text box
- **Paste** in the **Directory (tenant) ID** you just copied from the Azure AD portal, and click **Retrieve Endpoints**.

| 6dfd18d1-a139-a139-a139-63ad94a5fd98 | ☁ Retrieve Endpoints |

Enter your Microsoft Azure Tenant ID or Issuer URL.

- You should see a message that says: **Endpoints successfully Retrieved**.
- Switch back to the **Azure AD portal** tab in your browser, and **copy** the **Application (client) ID**.

🗑 Delete   🌐 Endpoints

Display name	: Clearlogin Connection
Application (client) ID	: 0e6678ca-8675-8675-8675-6050f0739ba1
Directory (tenant) ID	: 6dfd18d1-a139-a139-a139-63ad94a5fd98
Object ID	: 92b9ed9f-9d60-4412-82fa-101efef3f342

- Switch to the **Clearlogin portal** tab in your browser
- Scroll down to the **Client ID** field
- Paste in the **Application (client) ID** you just copied from the Azure AD portal.

Client ID

```
0e6678ca-8675-8675-8675-6050f0739ba1
```

The identifier for the application.

Configuration: Azure AD

- Switch back to the **Azure AD portal** tab, and click on **Manifest** in the sub-navigation bar.
- In the Manifest editor, change the **oauth2AllowIdTokenImplicitFlow** property to **true**.

```
20        "knownClientApplications": [],
21        "logoUrl": null,
22        "logoutUrl": null,
23        "name": "Clearlogin Connection",
24        "oauth2AllowIdTokenImplicitFlow": true,
25        "oauth2AllowImplicitFlow": false,
26        "oauth2Permissions": [],
27        "oauth2RequirePostResponse": false,
28        "optionalClaims": null,
29        "orgRestrictions": [],
30        "parentalControlSettings": {
```
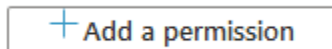
- Scroll down to the **replyUrlsWithType** property
- Add a comma after the closing curly brace under the "type": "web" line, then create a new line below the closing curly brace.
- Paste the following into the new line, and then make sure you **replace yourclearloginsubdomain** in the URL with your Clearlogin subdomain:

```
{
    "url": "https://yourclearloginsubdomain.clearlogin.com/logout",
    "type": "Web"
}
```
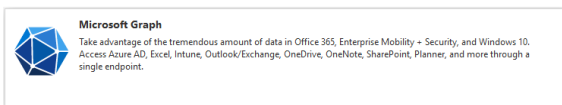
- When you are done, your changes should look similar to this screenshot (note the comma that separates the two entries for replyUrlsWithType).

```
36        "publisherDomain": "Neriiprod.onmicrosoft.com",
37        "replyUrlsWithType": [
38            {
39                "url": "https://evolvenow.clearlogin.com/openid/azure_ad/callback",
40                "type": "Web"
41            },
42            {
43                "url": "https://evolvenow.clearlogin.com/logout",
44                "type": "Web"
45            }
46        ],
47        "requiredResourceAccess": [
```

- Once you're done, click on **Save** at the top of the editor.
- Click on **API Permissions** in the sub-navigation bar.
- Click on **+ Add a Permission** to give Clearlogin the permissions to read the user accounts in Azure AD.

```
+ Add a permission
```

- In the flyout panel, click on **Microsoft Graph**

Microsoft Graph
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

- For the type of permissions, click on **Application Permissions**

Application permissions
Your application runs as a background service or daemon without a signed-in user.

- Scroll all the way down and **expand** the **User** category
- Select: **User.Read.All**

> UserNotification

> UserShiftPreferences

∨ **User (1)**

☐ User.Export.All
Export user's data ⓘ   Yes

☐ User.Invite.All
Invite guest users to the organization ⓘ   Yes

☐ User.ManageIdentities.All
Manage all users' identities ⓘ   Yes

☑ User.Read.All
Read all users' full profiles ⓘ   Yes

☐ User.ReadWrite.All
Read and write all users' full profiles ⓘ   Yes

- Click on **Add permissions** to finish the config.
- Click on the **Grant Admin Consent for...** button.

Configured permissions

Applications are authorized to call APIs when they are granted permissions b
should include all the permissions the application needs. Learn more about p

+ Add a permission | Grant admin consent for Evolve IP

- Click on the **Refresh** button to make sure that your changes properly saved, and the warning message goes away.
- Click on **Certificates & Secrets** in the sub-navigation bar.
- Click on **+ New client secret**
- Description: **Clearlogin Connection**
- Expires: **In 1 Year** (**DO NOT** select **Never** for the expiration)
- Click **Add**

Add a client secret

Description

Clearlogin Connection

Expires

⦿ In 1 year

◯ In 2 years

◯ Never

Add   Cancel

- Copy the **Value** field to the clipboard. **Do not copy the ID field.**

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	ID
Clearlogin Connection	6/25/2021	6z.bnBJNdZTtk_-1RR564~,	d-a88a-81e13f29051d

- Switch to the **Clearlogin portal** tab in your browser
- Paste the secret password into the **Client Secret** field. **Do Not click the Generate button.**

Client ID

0e6678ca-8675-8675-8675-6050f0739ba1

The identifier for the application.

Client Secret

●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●

- Scroll down and click on the **Update OpenID Identity Source** button.

This completes the steps to setup Azure AD as an identity source in Clearlogin.

Your next steps are to sign into Clearlogin using the credentials of a user account in Azure AD.

Troubleshooting

If you are experiencing issues with signing into Clearlogin using Azure AD as the identity source, check the following in Azure AD & Clearlogin.

Azure AD Manifest

- Go to: **Azure AD** > **App Registrations** > **Clearlogin Connection** > **Manifest**
- Make sure your manifest saved after making the required changes. We have experienced times when the changes we made did not save. Your manifest should look similar to these screenshots:


```
20        "knownClientApplications": [],
21        "logoUrl": null,
22        "logoutUrl": null,
23        "name": "Clearlogin Connection",
24        "oauth2AllowIdTokenImplicitFlow": true,
25        "oauth2AllowImplicitFlow": false,
26        "oauth2Permissions": [],
27        "oauth2RequirePostResponse": false,
28        "optionalClaims": null,
29        "orgRestrictions": [],
30        "parentalControlSettings": {
```

```
36        "publisherDomain": "Nelllprod.onmicrosoft.com",
37        "replyUrlsWithType": [
38            {
39                "url": "https://evolvenow.clearlogin.com/openid/azure_ad/callback",
40                "type": "Web"
41            },
42            {
43                "url": "https://evolvenow.clearlogin.com/logout",
44                "type": "Web"
45            }
46        ],
47        "requiredResourceAccess": [
```

Azure AD API Permissions

- Go to: **Azure AD** > **App Registrations** > **Clearlogin Connection** > **API Permissions**
- Make sure the status of your API permissions have green check marks and show granted for your organization. If not, click the **Grant Admin Consent...** button.

- The API Permissions should look similar to this screenshot.

Azure AD Identity Comparison

- Go to: **Azure AD** > **App Registrations** > **Clearlogin Connection** > **Overview**
- Compare the **Application (client) ID** and the **Directory (tenant) ID** with the **Clearlogin** configuration.

In Clearlogin, compare the **Endpoint** with the **Directory (tenant) ID** in Azure AD.

In Clearlogin, compare the **Client ID** with the **Application (client) ID** in Azure AD.

In Clearlogin check the **Endpoints** box, and then compare the listed endpoints with the **Director y (tenant) ID** in Azure AD.

Azure AD App Secret

- Generate a new App Secret in Azure AD
- Go to: **Azure AD** > **App Registrations** > **Clearlogin Connection** > **Certificates & Secrects**
- **Delete** the existing **Clearlogin Connection** secret

- Click on **+ New client secret**
- Description: **Clearlogin Connection**

- Expires: **In 1 Year** (**DO NOT** select **Never** for the expiration)
- Click **Add**

Add a client secret

Description

Clearlogin Connection

Expires

- ● In 1 year
- ○ In 2 years
- ○ Never

[Add] [Cancel]

- Copy the **Value** field to the clipboard. **Do not copy the ID field.**

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value		ID
Clearlogin Connection	6/25/2021	6z.bnBJNdZTtk_-1RR564~. [Copy to clipboard]		d-a88a-81e13f29051d

- Switch to the **Clearlogin portal** tab in your browser
- Paste the secret password into the **Client Secret** field. **Do Not click the Generate button.**

Client ID

0e6678ca-8675-8675-8675-6050f0739ba1

The identifier for the application.

Client Secret

●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●