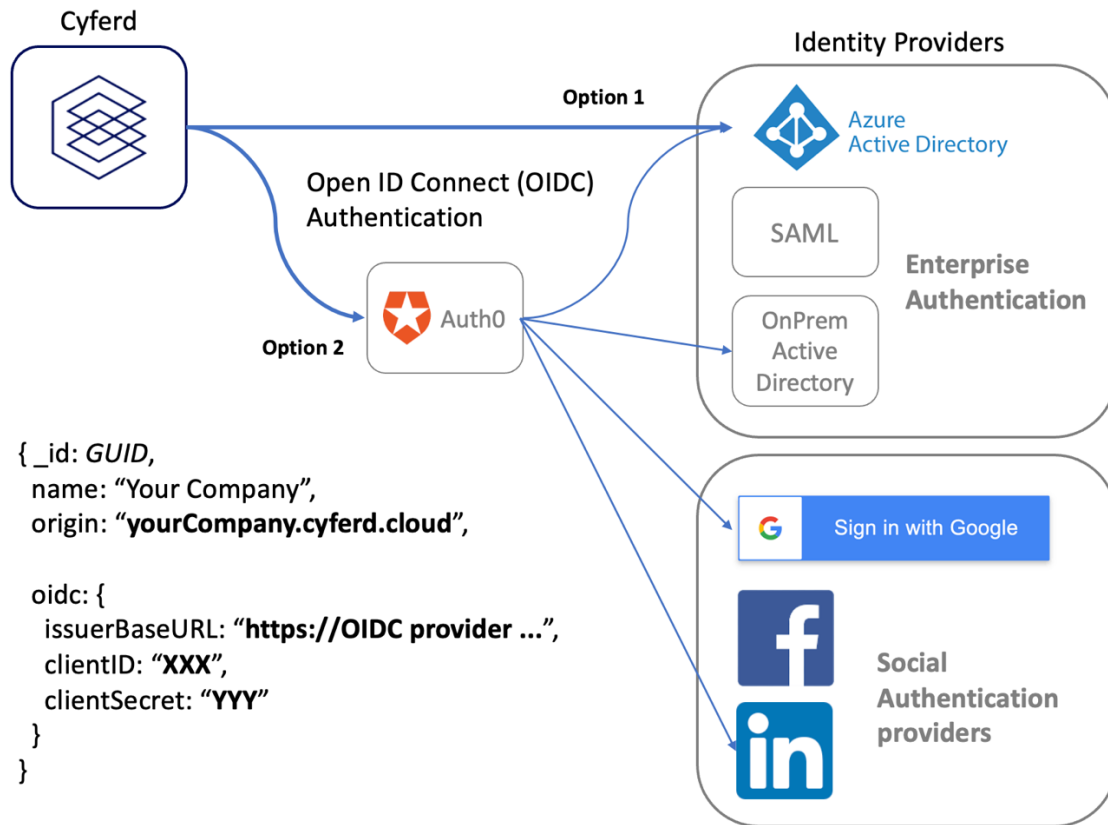


User Authentication

Cyferd supports Open ID Connect (OIDC) authentication for end users.



The OIDC authentication provider configuration details must be supplied to the Cyferd tenancy, and the OIDC provider is used to connect to the Tenant’s choice of Identity Provider(s).

Regardless of which Identity Provider(s) are enabled for authentication into Cyferd, access to data and capabilities within Cyferd is authorized to authenticated users by a Security Administrator within the Cyferd tenancy.

Many Enterprises have adopted Office 365, MS Exchange, and other Microsoft products so they consequently already have Microsoft Azure Active Directory, which can be directly supported as an OIDC Authentication Provider. The integration may be configured to permit authentication by only members of that directory, or also users from other Azure Active Directory instances. Microsoft documentation indicates that appropriately licensed Azure Active Directory instances can also federate authentication to some other Identity Providers.

In the Cyferd development environment, Auth0 is being used to provide an abstraction between Cyferd and the Identity Providers, enabling us to validate many Enterprise & Social Identity Providers for authentication into Cyferd for our development tenancies. This also allows more granular enablement of 3rd-Party Identity Providers than Azure’s all-or-nothing approach.

When available, Cyferd recommends direct adoption of Azure Active Directory for User Authentication, configured to permit *Accounts in any organizational directory* to authenticate.

After successful authentication from the browser into the selected Identity Provider, the OIDC protocol delivers an encrypted Java **Web Token** (JWT) to the user, and their browser forwards that to Cyferd. Cyferd will decrypt the contents of the Token using configuration details that have been supplied to it by the Tenant Administrator, and determines the authenticated User's identity from the **email** property.

An example of the profile information supplied from Azure Active Directory authentication is shown:

```
{
  "given_name":      "Michael",
  "family_name":     "Robertshaw",
  "nickname":        "Michael.Robertshaw",
  "name":             "Michael Robertshaw",
  "picture":          "https://s.gravatar.com/avatar/1cda654d507b4db8b2c2ad543a140353?s=480&r=pg&d=https%3A%2F%2Fcdn.auth0.com%2Favatars%2Fmr.png",
  "updated_at":      "2021-12-13T10:49:45.182Z",
  "email":            "michael.robertshaw@cyferd.com",
  "email_verified":  true,
  "sub":              "waad|dTVpuR2JaGhzpaExLFgnu017VHvXvNW_p48"
}
```

Other Identity Providers will deliver similar information but may provide more or fewer properties (called "Claims").

Configuration

Cyferd requires:

- the **URL** (maybe called Domain) of the OIDC Authentication provider
- the **Client ID** (maybe called Application) identifier, which indicates which collection of Identity Providers is to be used
- a **Secret** used for decrypting the JWT

The OIDC Authentication Provider needs:

- Allowed **Callback URLs**, which are based on the Cyferd Tenancy URL and may be simply https://*.cyferd.cloud/api/callback
- Allowed **Logout URLs**, which are based on the Cyferd Tenancy URL and may be simply https://*.cyferd.cloud/
- Allowed **Origin (CORS)**, which whitelists which URLs may request authentication via this Client ID or Application, and may be https://*.cyferd.cloud
- Allowed **Web Origins**, which (similar to Origin above) whitelists which URLs or Mobile applications may request authentication via this Client ID or Application, and may be simply https://*.cyferd.cloud

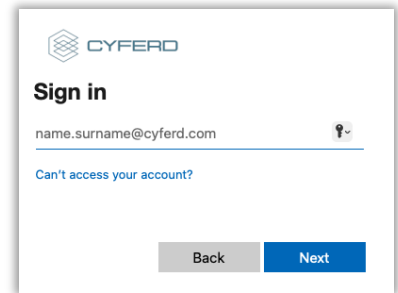
OPTION 1: Enabling Cyferd to connect directly to Azure Active Directory

Microsoft Azure

The Azure Administrator needs to know these details from Cyferd

- The Tenant URL, e.g., <https://yourCompany.cyferd.cloud>

See also <https://docs.microsoft.com/en-us/powerapps/maker/portals/configure/configure-openid-settings>



In the Azure Portal, navigate to **Azure Active Directory** > **App registrations**

1. Click **New registration**
 - a. Provide a meaningful **Name** that is easy to locate later, e.g., “Cyferd OIDC”.
 - b. Within **Supported account types**, choose who can use this application.
 - c. In **Redirect URI**, append “/api/callback” to the Cyferd Tenant URL as the **Web** URI, e.g., <https://yourCompany.cyferd.cloud/api/callback>
 - d. Click Register.
2. Click **Overview** at the top of the navigation tree on left.
 - a. Note the **Directory (tenant) ID** and concatenate this to <https://login.microsoftonline.com/> to form the OIDC Base URL that you will have to provide to Cyferd to configure your tenancy.
 - b. Note the **Application (client) ID**, as you will have to provide this to Cyferd to configure your tenancy.
3. *Optionally* Click on **Branding** in the navigation tree on left.
 - a. Upload a 215x215px image of the Cyferd logo as the **new logo**, e.g., <https://cyferd.cloud/static/Cyferd-Logo-Icon-Only-Blue-transparent.png>
 - b. Record your Cyferd tenancy <https://yourCompany.cyferd.cloud/> as the **Home Page URL**
 - c. Click **Save**
4. *Important:* Click **Authentication** in the navigation tree on left
 - a. Within the **Web** section, confirm that <https://yourCompany.cyferd.cloud/api/callback> is recorded as a Redirect URI.
 - b. Within **Front-channel logout URL**, record <https://yourCompany.cyferd.cloud/api/logout>
 - c. Scroll down to **Implicit grant and hybrid flows**.
 - d. Enable **ID tokens**.
 - e. Scroll further to **Supported account types** and choose whether you want to allow only your own staff (Accounts in this organizational directory only) or also Cyferd staff and other 3rd-parties (Accounts in any organizational directory) to be able to login to <https://yourCompany.cyferd.cloud/>
 - f. Click **Save** (at bottom)
5. Click **Certificates & secrets** in the navigation tree on left.
 - a. Click on **New client secret**.
 - b. Enter a **Description**, e.g., “Cyferd secret”
 - c. Adjust **Expires** to 12 months.
 - d. Click **Add** (at bottom)
 - e. The **Value** of the new secret is now shown. Copy this to the clipboard NOW. This is the only opportunity to capture the secret, and if you don’t then you must create a new secret. You will have to provide this secret to Cyferd to configure your tenancy.
6. Click **Token configuration** in the navigation tree on left.
 - a. Click **Add optional claim**.
 - i. Select **ID Token** type.

- ii. Ensure that **email, family_name, given_name, verified_primary_email** have been selected. These user attributes will be supplied to Cyferd after successful user authentication and will then be visible in the *Users* admin tool.
 - iii. Click **Add** (at bottom)
 - iv. You may be asked to Turn on the Microsoft Graph email, profile permission. Enable this and click **Add**.
 - b. *Optionally* Click **Add groups claim**. This will deliver the user's Group membership to Cyferd after successful user authentication.
 - v. Select **All groups**.
 - vi. Expand **ID**
 - vii. Select **sAMAccountName** to deliver the Group Names in a human-readable form.
 - viii. Click **Add**
7. Click **API permissions** in the navigation tree on left.
 - a. Locate **Configured permissions**.
 - b. Click on **Grant admin consent**.
 - c. Confirm Grant admin consent by clicking **Yes**.

Cyferd

Cyferd now requires these values for configuration of your Tenancy:

- **Domain** (from step 2a, or "common" if allowing 3rd parties at step 4e)
e.g., <https://login.microsoftonline.com/9317a7cf-3098-4f77-bf6c-73419d05b82e>

You can validate this value by replacing the Azure Tenant ID in the URL below <https://login.microsoftonline.com/9317a7cf-3098-4f77-bf6c-73419d05b82e/v2.0/.well-known/openid-configuration> and accessing it using a browser. You should get a reasonable JSON response.

- **Client ID** (from step 2b)
e.g. `4edaf090-2190-4c8a-8ca6-e9e1d7d30323`
- **Secret** (from step 5e)
e.g. `Q4G7Q~wlcP55jQXAlhnZFpY8sV_3wsyqBYDP3`

Within Azure Portal, under *Enterprise Applications* you can restrict which Users or Group members are permitted access to the configured App Registration.

You can also make your Tenancy directly navigable from <https://myapps.microsoft.com/>

OPTION 2: Enabling Auth0 to connect to Azure Active Directory

Microsoft Azure

The Azure Administrator needs to know these details from the Auth0 Administrator

- Auth0 Domain URL (see Auth0 > Settings > Custom Domains)
e.g., <https://yourCompany.eu.auth0.com>
or <https://cyferd.us.auth0.com> if this capability is being provided by Cyferd

See also <https://docs.microsoft.com/en-us/powerapps/maker/portals/configure/configure-openid-settings>

In the Azure Portal, navigate to **Azure Active Directory > Custom domain names**

2. Note the domain name that is associated with the Azure Active Directory, as you will need to provide this to the Auth0 Administrator, e.g. "yourCompany.com".

This is used by Auth0 to construct the Azure v2 OIDC configuration URL

<https://login.microsoftonline.com/yourCompany.com/.well-known/openid-configuration> which should return a meaningful JSON response.

In the Azure Portal, navigate to **Azure Active Directory > App registrations**

3. Click New registration
4. Provide a meaningful **Name** that is easy to locate later, e.g., "Auth0 OIDC"
5. Within **Supported account types**, choose who can use this application
6. In **Redirect URI**, append "/login/callback" to the Auth0 Domain URL to form a **Web URI**, e.g., <https://yourCompany.eu.auth0.com/login/callback>
7. Click Register
8. Click **Overview** at the top of the navigation tree on left
 - a. Note the **Application (client) ID**, as you will have to provide this to the Auth0 Administrator
9. *Optionally* Click on **Branding** in the navigation tree on left
 - a. Upload a 215x215px image of the Auth0 logo as the **new logo**
 - b. Record <https://manage.auth0.com/dashboard> as the **Home Page URL**
 - c. Click **Save**
10. Click **Certificates & secrets** in the navigation tree on left
 - a. Click on New client secret
 - b. Enter a **Description**, e.g., "Auth0 secret"
 - c. Leave **Expires** at the Recommended 6 months
 - d. Click **Add** (at bottom)
 - e. The **Value** of the new secret is now shown. Copy this to the clipboard NOW. This is the only opportunity to capture the secret, and if you don't then you must create a new secret. You will have to provide this secret to the Auth0 Administrator.
11. Click **Token configuration** in the navigation tree on left
 - a. Click Add optional claim
 - i. Select **ID Token** type
 - ii. Ensure that **email, family_name, given_name, verified_primary_email** have been selected. These user attributes will be supplied to Auth0 after successful user authentication.
 - iii. Click **Add** (at bottom)
 - iv. You may be asked to Turn on the Microsoft Graph email, profile permission. Enable this, and click **Add**
 - b. *Optionally* Click **Add groups claim**. This *may* deliver the user's Group membership to Auth0 after successful user authentication.

- i. Select **All groups**
 - ii. Expand **ID**
 - iii. Select **sAMAccountName** to deliver the Group Names in a human-readable form.
 - iv. Click **Add**
12. Click **API permissions** in the navigation tree on left
 - a. Locate **Configured permissions**.
 - b. Click on **Add a permission**.
 - c. Click on **Microsoft Graph**.
 - d. Click on **Delegated permissions**.
 - e. Scroll to **OpenId permissions** and expand it.
 - f. Enable
 - i. **email**
 - ii. **openid**
 - iii. **profile**
 - g. Scroll to **Directory** and expand it
 - h. Enable
 - i. **Directory.AccessAsUser.All**
 - ii. **Directory.Read.All**
 - i. Click on **Add permissions** (at bottom)
 - j. Click on **Grant admin consent**.
 - k. Confirm Grant admin consent by clicking **Yes**.

Auth0

The Auth0 Administrator requires these details from the Azure Administrator:

- Domain Name (see step 1 above), e.g., “yourCompany.com”
- Client ID (see step 7 above)
- Client Secret (see step 9e above)

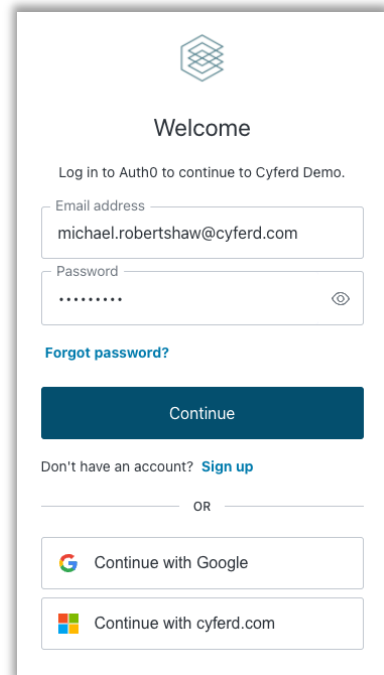
See also <https://auth0.com/docs/connections/enterprise/azure-active-directory/v2>

In the Auth0 Console, navigate to **Authentication > Enterprise > Microsoft Azure AD**

1. Click **Create Connection**
2. Enter a **Name**/label for this Connection, e.g., “yourCompany-AzureAD”
(may not contain spaces)
3. Enter the **Microsoft Azure AD Domain**, as provided by the Azure Administrator above, e.g., yourCompany.com
4. You will be asked for a **Client ID**. This is supplied by the Azure Administrator above
5. You will be asked for a **Client Secret**. This is supplied by the Azure Administrator above
6. When asked for the **Identity API**, select “Microsoft Identity Platform (v2)”
7. Basic Profile **Attributes** are required
8. **Extended Attributes** can be used to deliver more information in the JWT, and are not immediately required by Cyferd. *Optionally* enable
 - a. Extended Profile
 - b. Get user groups
 - c. Include all groups the use groups the user is a member of
9. In **Advanced**, ensure that **Email Verification** is Always set email_verified to ‘true’
10. Click **Create**
11. You’re now navigated to **Login Experience**
12. Scroll to bottom and enable **Display connection as a button**
13. Adjust the **Button display name**, and **Button logo** if you want
The Favourite Icon from your Corporate website is suitable, e.g., <https://www.yourCompany.com/favicon.ico>
otherwise this will default to the Microsoft logo
14. Click **Save**

In the Auth0 Console, navigate to **Applications > Applications**

15. Click **Create Application**
16. Provide a **Name**, e.g., “Cyferd”
17. When asked to **Choose an application type** select Regular Web Applications
18. Click **Create**
19. Ignore the Quick Start, and advance to the **Connections** tab
20. Enable the Identity Provider(s) that you wish to associate with this Application
21. Click on the **Settings** tab
22. Within **Basic Properties**, note these properties, as you must provide them to Cyferd to be configured on your tenancy:



The screenshot shows the Auth0 'Welcome' page. At the top is the Auth0 logo and the text 'Welcome'. Below that is the instruction 'Log in to Auth0 to continue to Cyferd Demo.' The login form includes an 'Email address' field with the value 'michael.robertshaw@cyferd.com' and a 'Password' field with masked characters. A 'Forgot password?' link is located below the password field. A large blue 'Continue' button is positioned below the form. Underneath the button, there is a link for 'Don't have an account? Sign up'. Below this is an 'OR' separator. At the bottom, there are two buttons: 'Continue with Google' (with the Google logo) and 'Continue with cyferd.com' (with the Cyferd logo).

- a. Domain
 - b. Client ID
 - c. Client Secret
23. Scroll down to **Application Properties**
- a. Supply the URL of a 150x150px **Application Logo** if you want, e.g. <https://cyferd.cloud/static/Cyferd-Logo-Icon-Only-Blue-transparent.png>
 - b. **Application Type** is Regular Web Application
 - c. The **Token Endpoint Authentication Method** should be Post
24. Scroll down to **Application URIs**
- a. The **Application Login URI** should be <https://cyferd.cloud/login>
 - b. **Allowed Callback URLs** should contain https://*.cyferd.cloud/api/callback
 - c. **Allowed Logout URLs** should contain https://*.cyferd.cloud
 - d. **Allowed Web Origins** should contain https://*.cyferd.cloud
 - e. **Allowed Origins (CORS)** should contain https://*.cyferd.cloud
25. Scroll to the bottom and click **Save Changes**

Cyferd

Cyferd now requires these values (from step 22 above) for configuration of your Tenancy.

- Domain
- Client ID
- Secret