Authenticating Users with OIDC

Published: September 20, 2024

Table of Contents

Legal Notice 3
Authenticating Users with OIDC 4
Configure an external user authentication through an OIDC IdP: 4
Configuring Amazon Cognito as an IdP 5
Configuring Microsoft Entra ID (Azure AD) 6
Prerequisites 6
Register Illumio as an application 6
Additional configuration 6
Save Configuration Parameters 6
Configure tokens 7
Custom Claims Mapping 7
Configuring Auth0 as an IdP 8
Auth0 configuration 8
Finishing configuration at Illumio Console 8

Legal Notice

The content in this documentation is provided for informational purposes only and is provided "as is," without warranty of any kind, expressed or implied of Illumio. The content in this documentation is subject to change without notice.

Resources

- Legal information
- Trademarks statements
- Patent statements
- License statements
- Open Source Licensing Disclosures

Contact Information

- Contact Illumio
- Contact Illumio Legal
- Contact Illumio Documentation

Authenticating Users with OIDC

Users with the Owner role can add external users from identity providers (IdPs) that conform to the OpenID Connect (OIDC) protocol. Although you can authenticate with any OIDC-compliant IdP, Illumio has validated the following well-known OIDC applications:

- MS Entra ID (Azure AD)
- Amazon Cognito
- AuthO
- Okta

NOTE

Integration with an OIDC-compliant application is your responsibility.

Configure an external user authentication through an OIDC IdP:

1. Go to **Access > Authentication**.
2. At the Authentication page, click the **OpenID Connect (OIDC)** tile.
3. At the OIDC page, the well-known identity providers are shown. Alternatively, you can use a different OIDC-compliant provider not listed here. Additional configuration guidelines for these IdPs are available here:
   - Configuring Microsoft Entra ID (Azure AD) [6]
   - Configuring Amazon Cognito as an IdP [5]
   - Configuring AuthO as an IdP [8]
4. Click the provider tile to see configuration information from that provider's documentation set.

   Follow the configuration steps for that provider, making sure to retain the Client ID and Issuer ID generated by the procedure.
5. After you finish the external configuration at the OIDC-compliant IdP, enter the **Client ID** and **Issuer URL** provided by the IdP during your configuration procedure.

   Some IdPs use terms that are not obvious matches to the parameters you enter at the OIDC page. The following table matches the configuration terms used by some popular IdPs with their equivalent Illumio OIDC parameter settings.

IDP Provider	Client ID Equivalent	Issuer URL Equivalent
MS Entra ID	Application (client) ID	Directory (tenant) ID, used in: `http://login.microsoftonline.com/ <tenant_id>/v2.0`
Amazon Cognito	Client ID	Token signing key URL, minus trailing `/.well-known/jwks.json`.
AuthO	Client ID	The **Domain** value prepended with "`https://`" and appended with "`.us.auth0.com`".

6. Enable IdP Logout if you want users to also be logged out of their identity provider when logging out of Illumio Console.
7. Click **Save**.

Configuring Amazon Cognito as an IdP

Follow these steps to configure Amazon Cognito as an external identity provider (IdP) in the Illumio Console's Okta instance via OIDC protocol.

1. Go to the Amazon Cognito console (`https://console.aws.amazon.com/cognito/home`). If prompted, enter your AWS credentials.
2. Create a user pool by clicking **Create user pool**. You might need to select **User Pools** from the left navigation pane to reveal this option.
3. In Configure sign-in experience, under Cognito user pool sign-in options, select **Email** only, and click **Next**.
4. In Configure security requirements:
    a. Under Multi-factor authentication, choose **No MFA**.
    b. Under User account recovery:
        i. Select **Enable self-service account recovery**.
        ii. Select **Email only** for Delivery method for user account recovery messages.
    c. Click **Next**.
5. In Configure sign-up experience, determine how a new user verifies their identity when signing up.

    Under Required attributes, confirm that **email** is specified, and from the Additional required attributes menu, select **family_name** (surname) and **given_name** (first name).
6. In Configure message delivery, choose the settings you prefer. Note the prerequisites for sending email with Amazon SES.
7. On Integrate your app:
    a. Enter a name in **user pool name**.
    b. Under Initial app client, confirm that App type is set to **Public client**.
    c. Enter a name in **App client name**.
    d. Under Client secret, you can choose whether you want to generate a client secret or not.
    e. Expand **Advanced app client settings**, and under this section set up various client app authentication flows:
        i. For Authentication flows, choose **ALLOW_USER_SRP_AUTH**.
        ii. Choose a session duration and the various token expirations as you wish.
        iii. Under the optional Advanced security configurations, we recommend **Enable token revocation** and **Prevent user existence errors**.
    f. Click **Next**.
8. At Review and Create, review your user pool details, and when satisfied click **Create user pool**.

Configuring Microsoft Entra ID (Azure AD)

Follow these steps to configure Microsoft Entra ID (formerly known as Microsoft Azure Active Directory) as an external identity provider (IdP) in the Illumio Console's Okta instance via OIDC protocol.

Prerequisites

Ensure that you have entered an email, first name, and last name in your user profile in your Azure AD instance. These fields cannot be empty.

Register Illumio as an application

1. Log into Entra ID (Azure AD).
2. In the Azure left navigation panel, click **App registrations**.
3. At the App Registrations page, click **New registration**.
4. At the Register an application page:
   a. In the Name field, enter a name for your Illumio Console instance. For example, "MyCorp on Illumio".
   b. For Supported account types, select **Accounts in this organizational directory only (Single tenant)** .
   c. Under Redirect URI, choose **Single-page application (SPA)** and enter the URI to Illumio Console: **https://console.illumio.io**.
5. Click **Register**.

Additional configuration

After you have registered your Illumio Console application as an Entra application, you can see it listed when you click **App registrations**, then **All applications**.

1. At the **App registrations** page, click your application name (for example,"MyCorp on Illumio") to see more details.
2. At your application details page, click **Authentication**.
3. Confirm that you have entered the proper Redirect URI, and correct it if needed.
4. Under **Implicit grant and hybrid flows**, you must enable the **ID tokens** setting.

Save Configuration Parameters

1. At the details page for your Illumio Console application, click **Settings**.
2. Copy the Client ID setting shown there. You will use this as the **Client ID** setting when completing your OIDC authentication in the Illumio Console.
3. Copy the **Directory (tenant) ID** shown here. This ID will be used as the basis for the **Issuer URL** setting when completing your OIDC authentication in the Illumio Console, where you will enter the URL in the form: **http://-login.microsoftonline.com/*tenant_ID*/v2.0**.

4. Click **Manifest**, and at this page use the editor to update the following JSON entries to these values:

```
"acceptMappedClaims": true
"accessTokenAcceptedVersion": 2
```

Configure tokens

1. Click **Token configuration**. At this page:
   a. Select **ID Token**.

   b. Click **Add optional claim**. Enable **email** and **upn** in the list of claims. If available, also enable the option to **Turn on Microsoft Graph email permission**.
   c. Click Add.
2. At the Token configuration page, confirm that both email and upn are listed under the Claim column, and they are Token type of ID.

3. Click **API permissions**.

   When you enabled Microsoft Graph earlier, API permissions should be turned on for email and profile.
4. Click **Microsoft Graph** under the API/Permissions name column, and enable the **openid** permission.

   The email and profile permissions should be enabled already.
5. Click **Add**.

Custom Claims Mapping

1. Go to your Entra ID Home, and click **Enterprise applications**.
2. From the list of your applications, click the name of your new Illumio Console application (for example, "MyCorp on Illumio").
3. At the details page for your Illumio Console application, click **Properties**. Ensure that the **Assignment required?** option is set to **Yes**. This setting ensures that when a user logs in, the user is assigned to the target Entra ID application.
4. Click **Single sign-on** from the left navigation. At the OIDC-based Sign-on page, under the Attributes and Claims section, click **Edit**.
5. On the Manage claim page, enter new claims for firstName and lastName:
   a. Enter the Name (for example, **firstName**).
   b. Set Source to **Attribute**.
   c. In Source attribute, choose the menu item **user.givenname** for thefirstName claim, and **user.surname** for the lastName claim.
   d. Leave all other options at default values or unspecified.
   e. Click **Save** after completing each claim.
6. The next time you log into the Illumio Console, a Microsoft window requests you grant permission. Click **Accept**.

Configuring Auth0 as an IdP

You can use Auth0 as an external Identity Provider (IdP) through the OIDC protocol support provided in Illumio Console.

Auth0 configuration

1. Log in to your Auth0 account.
2. In the left navigation pane, click **Applications > Applications**.
3. Click **Create Application**.
4. In the Create application window:
   a. Enter a **Name** for your Illumio instance.
   b. For Choose an application type, click **Single Page Web Applications**.
   c. Click **Create**.
5. At the wizard page that asks What technology are you using for your web app? click **React**.
6. At the wizard Settings tab for your new application, under the Basic Information section copy the **Client ID** and **Domain** values generated for your Illumio app. (The Domain value is the basis for your Issuer ID.)
7. Scroll down to the Application URIs section, and enter the correct callback URL in the **Allowed Callback URLs** field.
8. Click **Save** at the bottom of the page.

Finishing configuration at Illumio Console

After generating and copying the Client ID and Domain at the Auth0 website, return to the OIDC page in the Illumio Console, and complete the IdP configuration as described in Authenticating Users with OIDC [4].

1. In **Client ID**, enter (or paste) the **Client ID** generated when configuring your web app on Auth0.
2. In **Issuer URL**, enter (or paste) the **Domain** value that you also generated at Auth0, and prepend the value with "`https://`" and append the value with "`.us.auth0.com`".

   For example, a **Domain** value of `my-1a2b3c4d5e6f7g` is entered as **https://my-1a2b3c4d5e6f7g.us.auth0.com** in the **Issuer URL** field.