



Configuring Single Sign-On for 360iQ: Entra ID

Single Sign-On (SSO) is an authentication method that allows users to access multiple applications using a single set of login credentials. Rather than logging in to each application separately, users can authenticate once and are then automatically granted access to the other applications within the SSO system.

Content

In this guide, we will cover the proceeding topics:

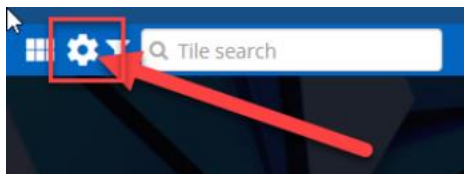
- [Configuring 360iQ Organization Wizard](#)
- [Configuring Microsoft Entra ID](#)

Configuring 360iQ Organization Wizard

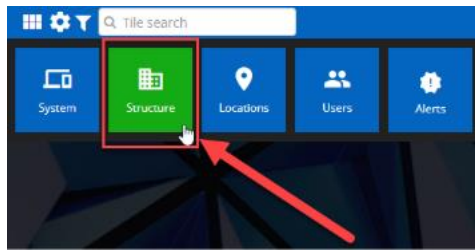
Note: To access the **Organization Wizard** in 360iQ, you must have an **SSO Admin role in 360iQ**. To update your permissions, please contact [Support](#) or your Customer Experience Manager.

Once you have added 360iQ to Microsoft Entra ID, proceed as follows:

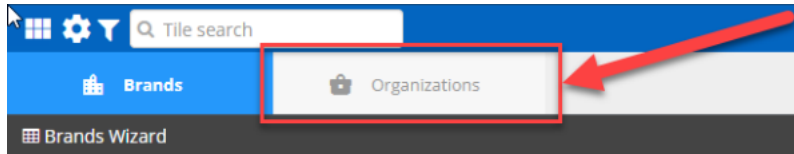
1. Log in to 360iQ.
2. Click the **Settings** (gear) icon in the top left corner of the page.



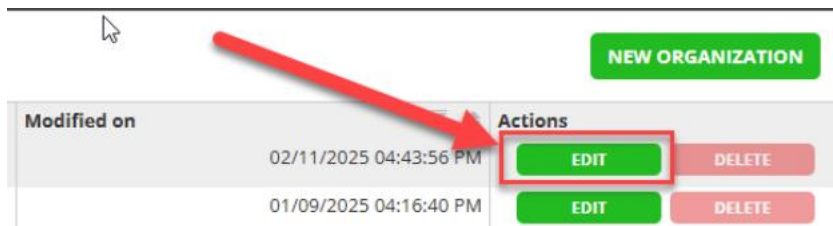
3. Click the **Structure** tile.



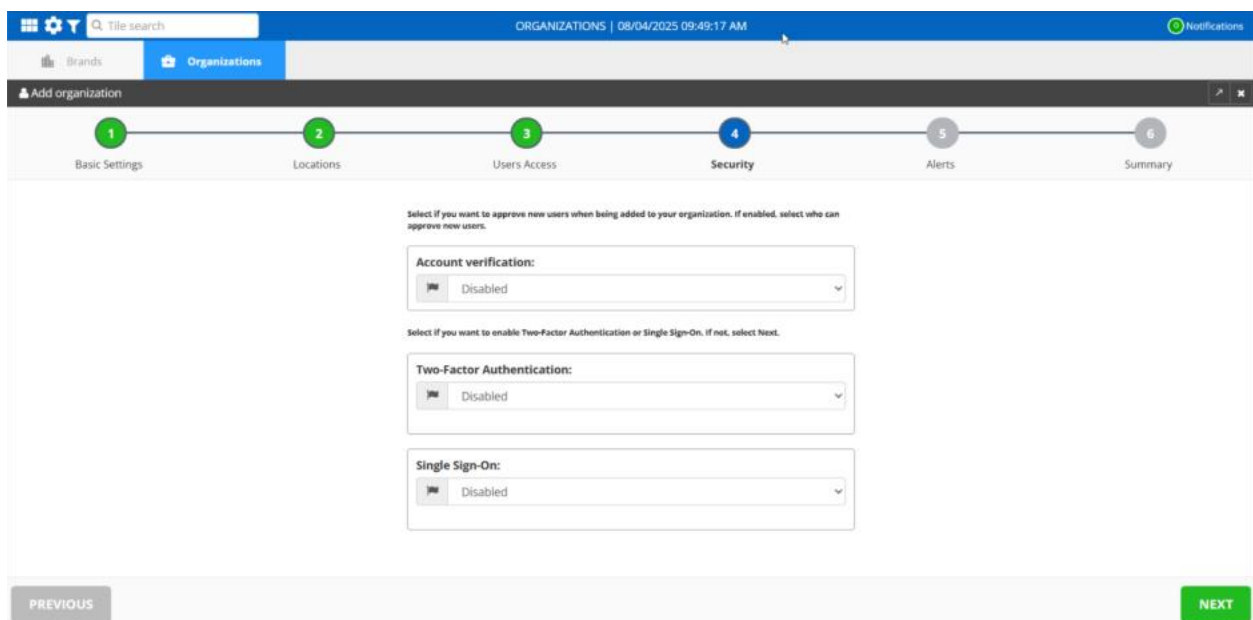
4. Click the **Organizations** tab.



5. In the **Organizations wizard**, find your organization and click the **EDIT** button in the Actions column. If there are multiple organizations, choose the one that matches your company name.



6. Click **Next** to advance the menu to the **Security** section.



7. Under **Single Sign-On**, click the **dropdown arrow** and choose **Enabled**.

Single Sign-On:

 Enabled ▼

CLIENT ID

AUTHORITY

Configure the Single Sign-On provider using the specified URL: [COPY TO CLIPBOARD](#)

[VERIFY](#)

8. More options will appear. Enter the **Client ID** and **Authority**.

Single Sign-On:

 Enabled ▼

CLIENT ID

AUTHORITY

Configure the Single Sign-On provider using the specified URL: [COPY TO CLIPBOARD](#)

[VERIFY](#)

9. Return to **Microsoft Entra ID**. Copy the **Application (client ID)** from Entra and paste it into 360iQ.

360iQ_Web

Search

[Delete](#) [Endpoints](#) [Preview features](#)

Get a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developers).

Essentials

Display name : 360iQ_Web

Application (client) ID :

Object ID :

Directory (tenant) ID :

Supported account types : [Any organization only](#)

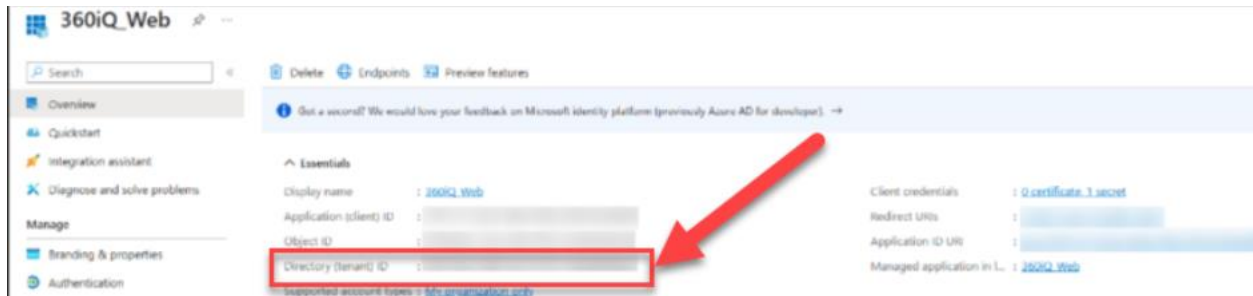
Client credentials : [Q:certificate, T:secret](#)

Redirect URIs :

Application ID URI :

Managed application in L... : [360iQ_Web](#)

10. Go back to **Microsoft Entra ID**. Find and copy the **Directory (tenant) ID**.



11. Return to 360iQ. In the **Authority** field, type “<https://login.microsoftonline.com/{Directory}/v2.0>”, where “{Directory}” is the value from the Entra page (Directory (tenant) ID).

Single Sign-On:

☐ Enabled

CLIENT ID

AUTHORITY

Configure the Single Sign-On provider using the specified URL: [COPY TO CLIPBOARD](#)

VERIFY

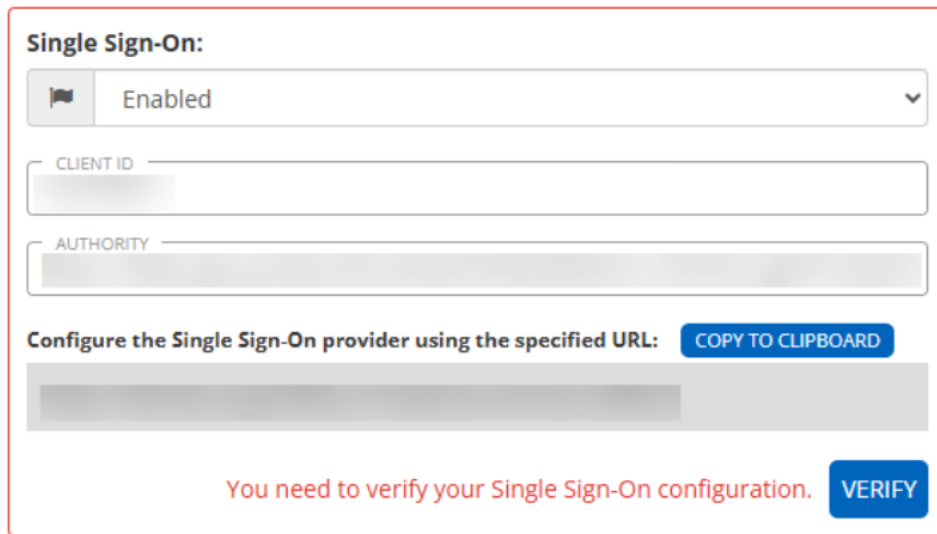
12. Once you have provided these details, you must confirm them via a verification flow. To begin verification, click the **Verify** button. You will be redirected to your SSO provider’s login page, where you need to perform a successful login.

The screenshot shows the 'Edit organization' page with the 'Security' tab selected. The page has a breadcrumb trail: Brands > Organizations > Edit organization. A progress bar at the top indicates six steps: 1. Basic Settings, 2. Locations, 3. Users Access, 4. Security (current), 5. Alerts, and 6. Summary. The main content area contains three sections: 'Account verification:' with a dropdown menu set to 'Disabled'; 'Two-Factor Authentication:' with a dropdown menu set to 'Disabled'; and 'Single Sign-On:' with a dropdown menu set to 'Enabled'. Below the 'Single Sign-On:' section, there are input fields for 'CLIENT ID' and 'AUTHORITY', both containing blurred text. A blue button labeled 'COPY TO CLIPBOARD' is next to the 'Configure the Single Sign-On provider using the specified URL:' label. Below this, there is a large text area with blurred content and a 'VERIFY' button.

If your login is successful, you will receive this message and can move on to the next steps:

This screenshot shows a detailed view of the 'Single Sign-On' configuration section. It features a dropdown menu set to 'Enabled'. Below it are input fields for 'CLIENT ID' and 'AUTHORITY', both containing blurred text. A blue button labeled 'COPY TO CLIPBOARD' is positioned next to the text 'Configure the Single Sign-On provider using the specified URL:'. Below this, there is a large text area with blurred content and a 'VERIFY' button. A green message 'Verification completed' is displayed at the bottom right of the section.

If the verification is unsuccessful, you cannot proceed and will receive this error message:



Single Sign-On:

☒ Enabled

CLIENT ID

AUTHORITY

Configure the Single Sign-On provider using the specified URL: [COPY TO CLIPBOARD](#)

You need to verify your Single Sign-On configuration. [VERIFY](#)

13. Once verification has been completed, click **Next**.

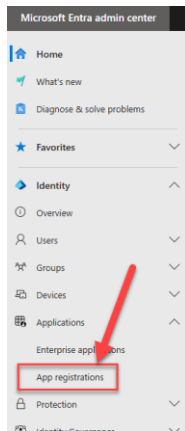


14. On the Summary page, review your details, then click **Save**.

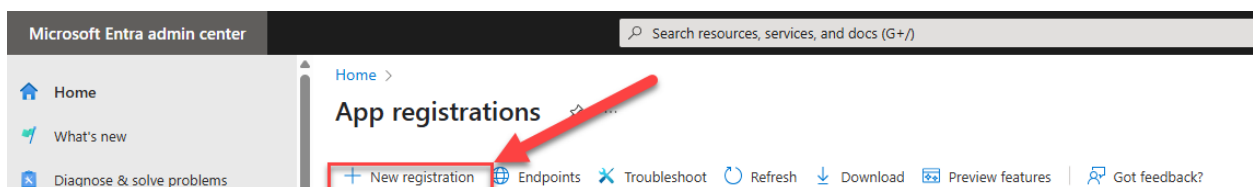
Note: Once Single Sign-On (SSO) has been configured properly, all users will be required to use SSO upon their next log in.

Configuring Microsoft Entra ID

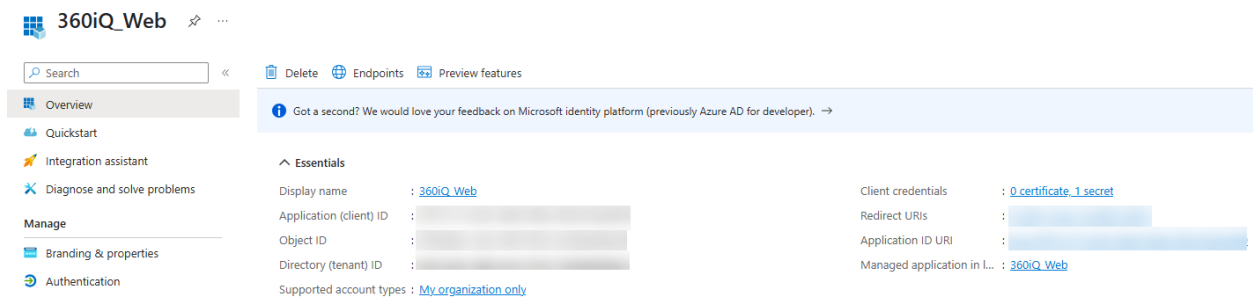
1. Sign in to Microsoft Entra.
2. Open the Microsoft Entra **admin center**, and navigate to the **Applications** tab.
3. Click the **dropdown arrow** to expand the tab, then click **App registrations**.



4. At the top of the page, click the **+ New registration** button to create a new registration option for 360iQ.



5. After creating the registration, click the **Overview** tab to configure the SSO settings.



6. Next, navigate to the **Authentication** tab.
7. Scroll down to the **Implicit grant and hybrid flows** section. You will need to enable the **ID_Token** issuance for the application.
8. Select the checkbox beside **ID tokens (used for implicit and hybrid flows)**.

Search (Ctrl+ /)

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Got feedback?

Microsoft will send a request to have the application clear the user's session data. This is required for single sign-out to work correctly.

e.g. https://example.com/logout

Implicit grant and hybrid flows

Request a token directly from the authorization endpoint. If the application has a single-page architecture (SPA) and doesn't use the authorization code flow, or if it invokes a web API via JavaScript, select both access tokens and ID tokens. For ASP.NET Core web apps and other web apps that use hybrid authentication, select only ID tokens. [Learn more about tokens.](#)

Select the tokens you would like to be issued by the authorization endpoint:

☒ Access tokens (used for implicit flows)

☒ ID tokens (used for implicit and hybrid flows)

For additional information or questions, please contact **Support** at support@dtiq.com or your **Customer Experience Team** at csr@dtiq.com.



800.933.8388 | info@dtiq.com | www.DTiQ.com