



Configuring Single Sign-On for 360iQ

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

360iQ currently supports **Microsoft Entra ID**.

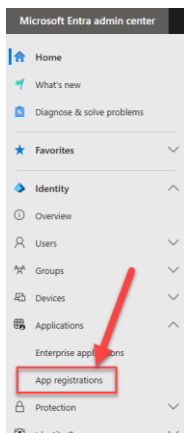
Content

In this guide, we will cover the proceeding topics:

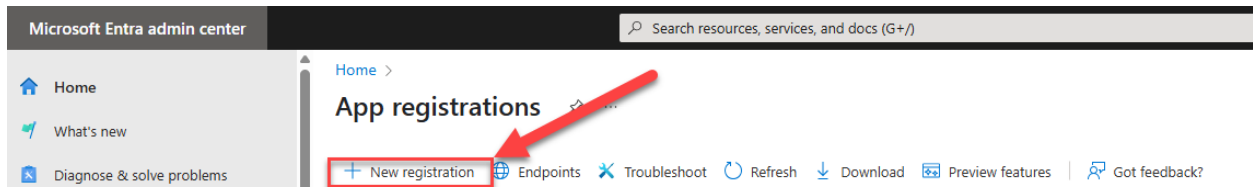
- [Configuring Microsoft Entra ID](#)
- [Configuring 360iQ Organization Wizard](#)

Configuring Microsoft Entra ID

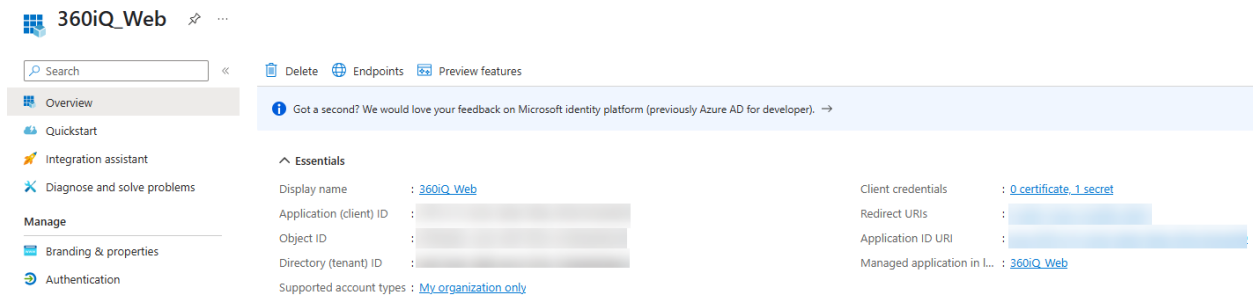
1. Sign in to Microsoft Entra.
2. Open the Microsoft Entra **admin center**, and navigate to the **Applications** tab.
3. Click the **dropdown arrow** to expand the tab, then click **App registrations**.



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



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

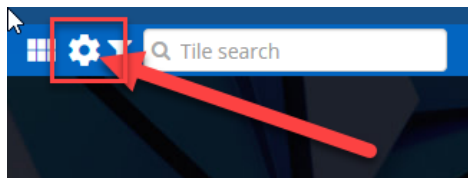


Configuring 360iQ Organization Wizard

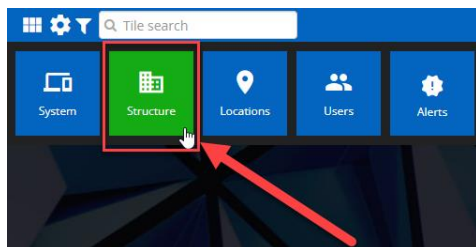
Note: To access the **Organization Wizard** in 360iQ, you must have an **SSO Admin role in 360iQ**. To update your permissions, please contact [Support](#) or your Customer Experience Manager.

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

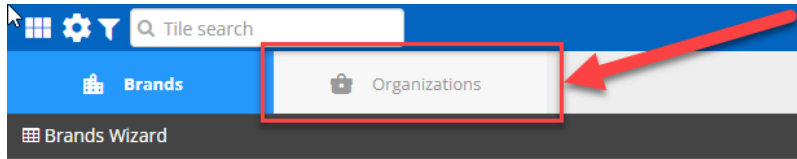
- Log in to 360iQ.
- Click the **Settings** (gear) icon in the top left corner of the page.



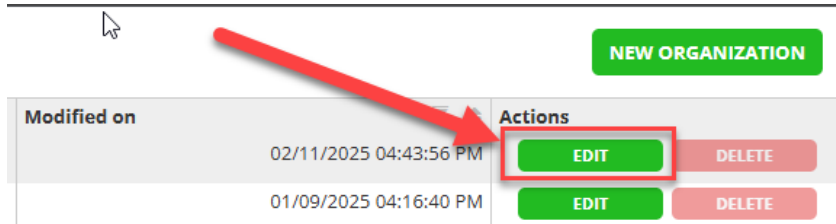
- Click the **Structure** tile.



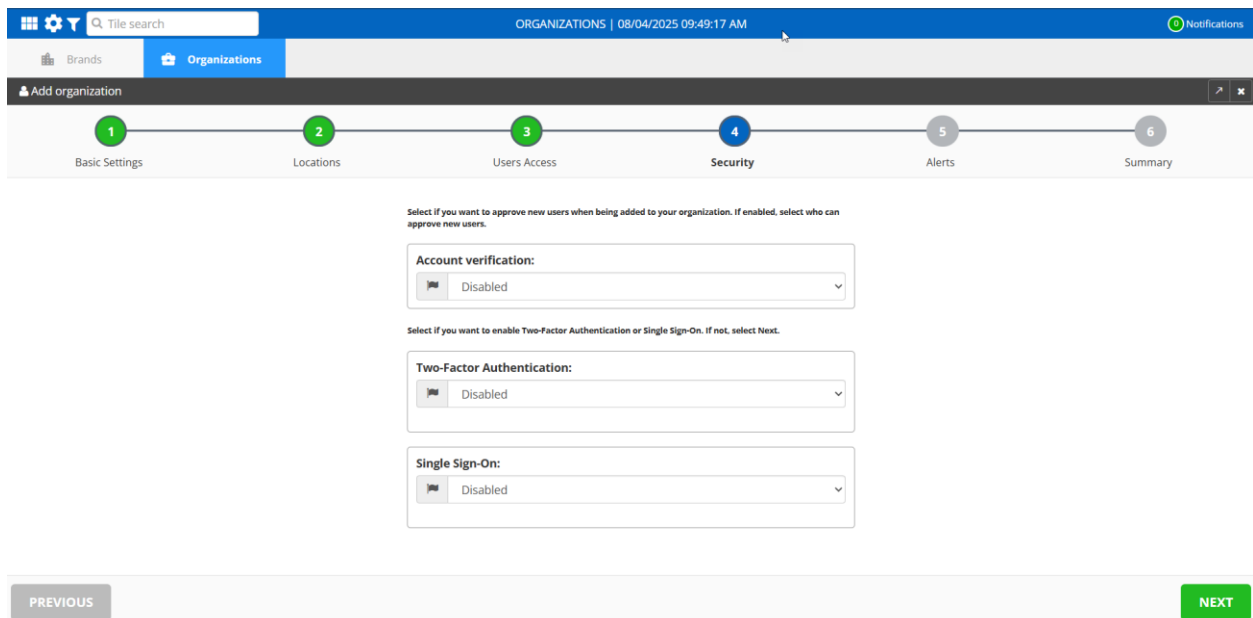
- Click the **Organizations** tab.



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 : Microsoft accounts only

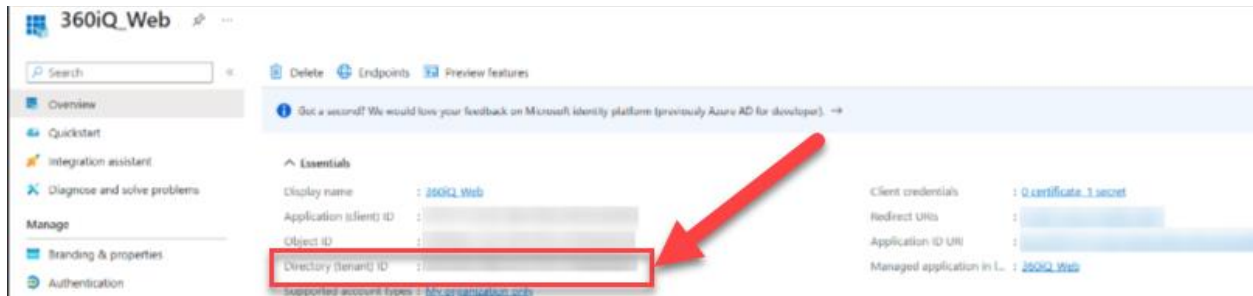
Client credentials : X.509 certificate, 1 secret

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).

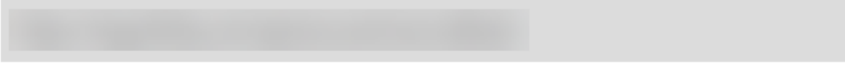
Single Sign-On:

 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.

Brands Organizations

Edit organization

1 Basic Settings 2 Locations 3 Users Access 4 Security 5 Alerts 6 Summary

Select if you want to approve new users when being added to your organization. If enabled, select who can approve new users.

Account verification: Disabled

Select if you want to enable Two-Factor Authentication or Single Sign-On. If not, select Next.

Two-Factor Authentication: Disabled

Single Sign-On: Enabled

CLIENT ID

AUTHORITY

Configure the Single Sign-On provider using the specified URL: COPY TO CLIPBOARD

VERIFY

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

Single Sign-On:

Enabled

CLIENT ID



AUTHORITY

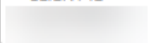
Configure the Single Sign-On provider using the specified URL: COPY TO CLIPBOARD


Verification completed VERIFY

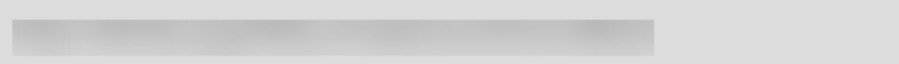
If the verification is unsuccessful, you cannot proceed and will receive this error message:

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.

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