



Configuring Single Sign-On for 360iQ: OneLogin

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:

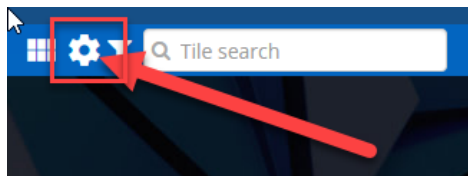
- [Configuring 360iQ Organization Wizard](#)
- [Configuring OneLogin](#)

Configuring 360iQ Organization Wizard

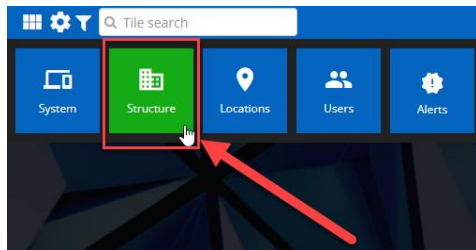
Note: To access the **Organization Wizard** in 360iQ, you must have an **SSO Admin role in 360iQ**. To update your permissions, please contact [Support](#) or your Customer Experience Manager.

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

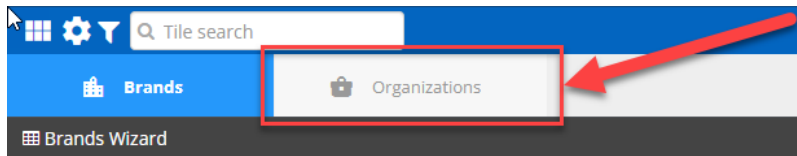
1. Log in to 360iQ.
2. Click the **Settings** (gear) icon in the top left corner of the page.



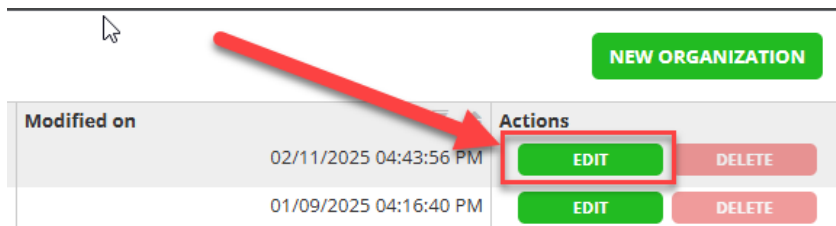
3. Click the **Structure** tile.



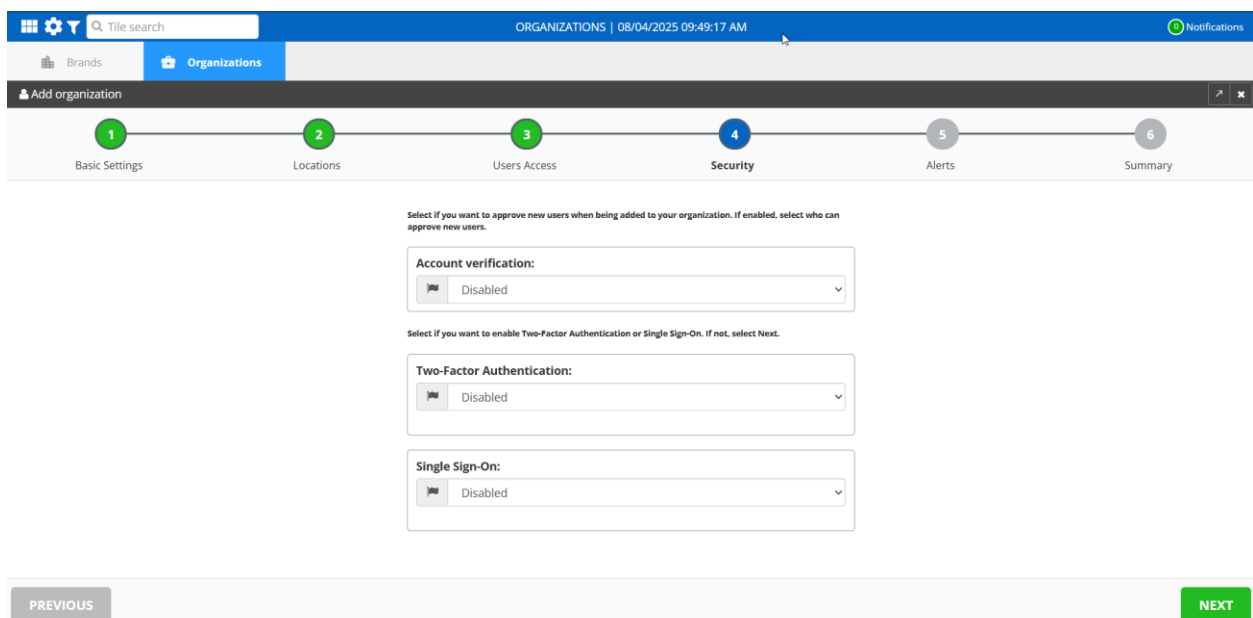
4. Click the **Organizations** tab.



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](#)

`https://id.go360iq.com/api/account/sso/callback`

[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](#)

`https://id.go360iq.com/api/account/sso/callback`

[VERIFY](#)

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

onelogin Users Applications Devices Authentication Activity Security Settings Developers Modules

Applications / OpenID Connect (OIDC) More Actions Save

Info Configuration Parameters Rules SSO Access Users Privileges Setup

Enable OpenID Connect

Client ID
16a89880-7cd2-013e-83a0-59f3f7bc4be4252215

Client Secret
Show client secret Regenerate client secret

Issuer URL
https://wdtest2.onelogin.com/oidc/2 Well-known Configuration

Application Type
Application Type
Web

Token Endpoint
Authentication Method
Basic

Token Timeout settings

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

Single Sign-On:

Enabled

CLIENT ID

AUTHORITY


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

https://id.go360iq.com/api/account/sso/callback

VERIFY

11. 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.

Single Sign-On:


 Enabled ▼

CLIENT ID ▬
ClientID from OneLogin

AUTHORITY ▬
Issuer URL from OneLogin


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


`https://id.go360iq.com/api/account/sso/callback`


 [VERIFY](#)

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

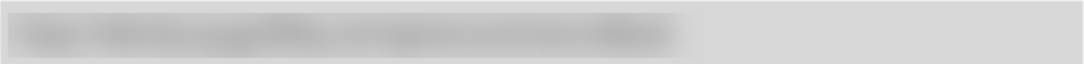
Single Sign-On:

 Enabled ▼

CLIENT ID ▬
 ▼

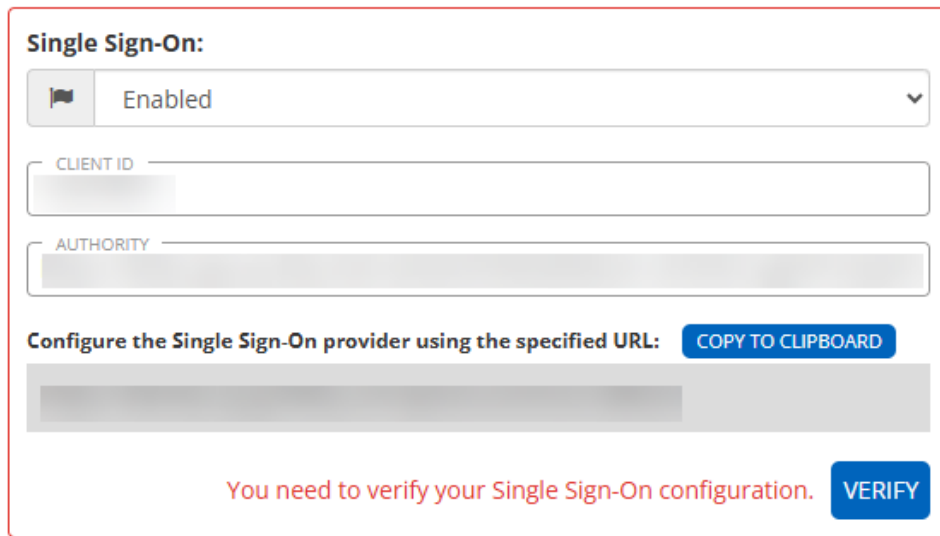
AUTHORITY ▬
 ▼

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](#)

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



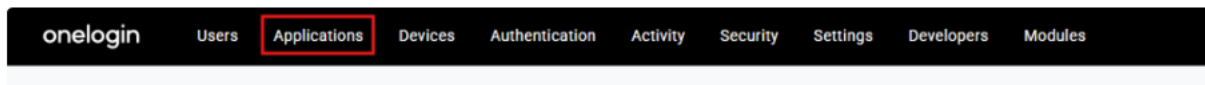
13. On the Summary page, review your details, then click **Save**.

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

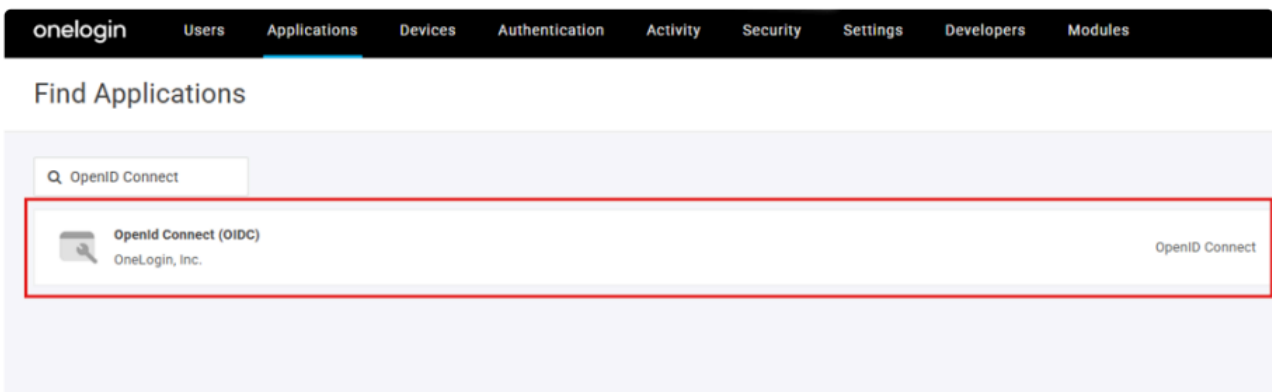
Configuring OneLogin

Take the following steps:

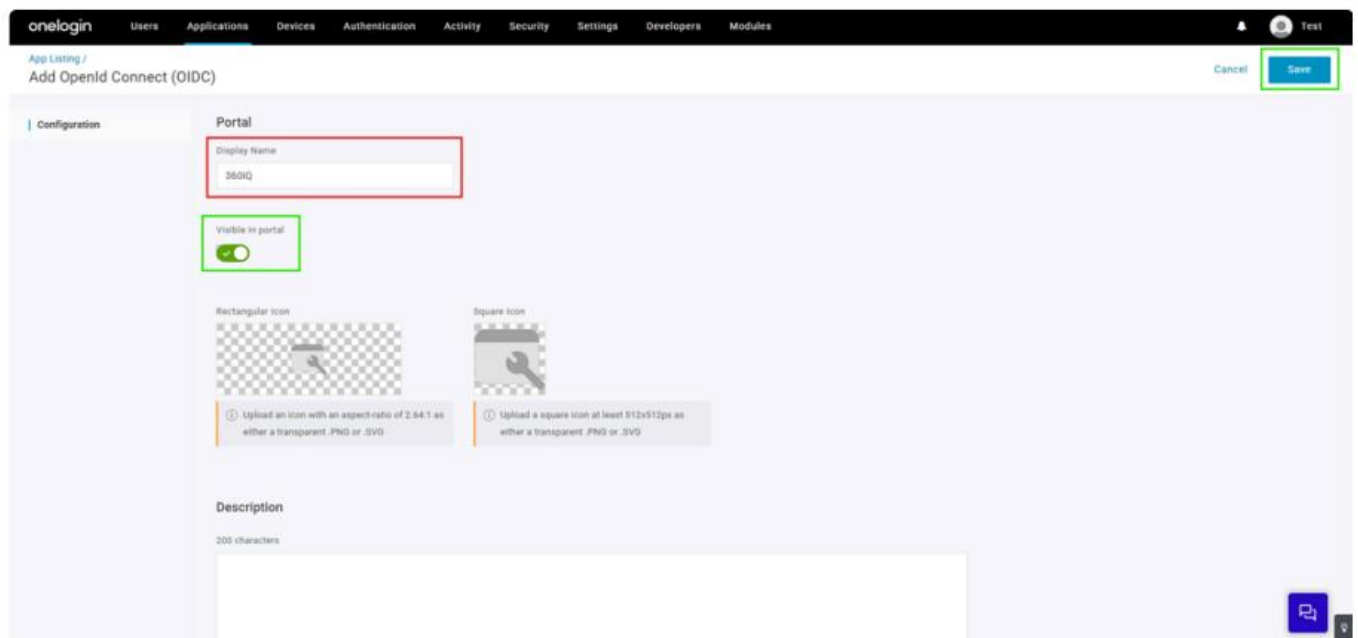
1. Navigate to your organization's **administration page** (https://{your_org}.onelogin.com/admin2). Click the **Applications** tab.



2. On the right side of the screen, click **Add App**. On the next screen, in the search bar, input “OpenID Connect” and select **Openid Connect (OIDC)** as the application type.



3. On the next page, locate the **Display Name** box and enter **360iQ**. **Note:** To allow users to log in directly via the OneLogin portal, toggle the **Visible in portal** option on. Provide application icons and description (if desired), then click **Save** in the upper-right corner.



- Once your app has been saved, click the **Configuration** tab on the left side of the screen. Set the **Redirect URI's** to <https://id.go360iq.com/api/account/sso/callback> (copied from 360iQ). **Note:** To allow users to log in directly to 360iQ via OneLogin, set **Login Url** to <https://app.go360iq.com>. Leave the **Post Logout Redirect URIs** field empty.

onelogin Users Applications Devices Authentication Activity Security Settings Developers Modules

Applications /
OpenId Connect (OIDC)

Info

Configuration

Parameters

Rules

SSO

Access

Users

Privileges

Setup

Application details

Login Uri
https://app.go360iq.com

Redirect URI's
https://id.go360iq.com/api/account/sso/callback

① After the user is authenticated we only allow redirects back to entries on this comma (or new-line) separated list of urls, and HTTPS is required.
http://localhost is permitted for development purposes only and should not be used in production.

Post Logout Redirect URIs

① After the user is logged out by OIDC we only allow redirects back to entries on this comma (or new-line) separated list of urls, and HTTPS is required.
http://localhost is permitted for development purposes only and should not be used in production.

- Next, go to your **SSO** tab. You will need to enter the **Issuer URL** and the **Client ID** in **360iQ's Organization Wizard**.

onelogin Users Applications Devices Authentication Activity Security Settings Developers Modules

Applications / OpenId Connect (OIDC)

More Actions Save

Info

Configuration

Parameters

Rules

SSO

Access

Users

Privileges

Setup

Application details

Login URL
https://app.go360iq.com

Redirect URI's
https://id.go360iq.com/api/account/sso/callback

ⓘ After the user is authenticated we only allow redirects back to entries on this comma (or new-line) separated list of urls, and HTTPS is required.
http://localhost is permitted for development purposes only and should not be used in production.

Post Logout Redirect URIs

ⓘ After the user is logged out by OIDC we only allow redirects back to entries on this comma (or new-line) separated list of urls, and HTTPS is required.
http://localhost is permitted for development purposes only and should not be used in production.

Single Sign-On:

Enabled

CLIENT ID
ClientID from OneLogin

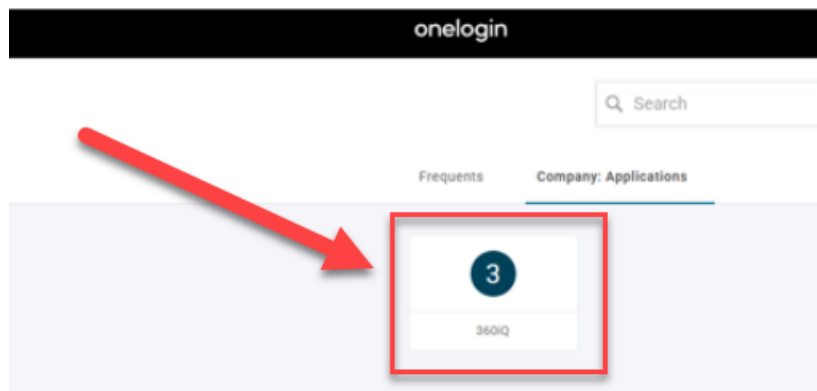
AUTHORITY
Issuer URL from OneLogin

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

https://id.go360iq.com/api/account/sso/callback

VERIFY

6. Once you have added the 360iQ application to OneLogin, you must assign it to the appropriate users or user groups in OneLogin.
7. If the application and login portal have been configured correctly, you should see the 360iQ tile in OneLogin.



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