Computing Requirements

Indigo assessments and courseware materials are designed to run on standard browsers, but best performance and compatibility will be ensured by using Chrome 80.0 and above on a Windows or MacOS device with at least 4GB of real memory and 1GHz processor. Components will run on less advanced configurations but must be tested and performance may be affected.

Networking Requirements

Indigo applications are multi-tier and are designed to operate on moderate bandwidth. It is suggested that applications are run over asymmetric or symmetric connections of at least sustained 30mbs downstream and 10mbs upstream throughput with low latency. Applications can be run over 4G or Wi-Fi connections.

Whitelisting

The following domains (and all subdomains) should be added to whitelisted sites and "Safe Senders" for SMTP-based email:

***.ttiadmin.com** – port 80 and 443: Administration for Teachers and Staff
***.ttisurvey.com** – port 80 and 443: Assessment link for Students, Teachers, Staff
***.auth0.com** – port 80 and 443: Authentication and Authorization Services
***.indigolearners.com** – port 80 and 443: Indigo Learners resources and materials
***.indigolaunchpad.com** – port 80 and 443: LaunchPad platform for Indigo assessments and results
***.indigoeducationcompany.com** – port 80 and 443: Websites and resources for Indigo
***.indigopathway.com** – port 80 and 443: IndigoPathway career and college readiness resources and materials
***.coloradocareeradvising.com (Colorado users only)** – port 80 and 443: Colorado Career Advising resources and materials
***.indigodashboard.com** – port 80 and 443: Students and Teacher resources for Indigo
***.vimeo.com** – port 80 and 443: Online course videos
***.youtube.com** – port 80 and 443: Online course videos
***.indigocourses.com** – port 80 and 443: Online course for Students, Teachers, Staff
***.indigoactivate.org** – port 80 and 443: Online course for Students, Teachers, Staff
***.moodle.school** – port 80 and 443: 5 Module Online course for Students, Teachers, Staff
***.moodlecloud.com** – port 80 and 443: 5 Module Online courses for Students, Teachers, Staff

Emails will be sent from **support@indigoproject.org, survey@indigopathway.com, support@indigopathway.com, support@coloradocareeradvising.com (Colorado users only), ccatool@coloradocareeradvising.com (Colorado users only), hello@coloradocareeradvising.com (Colorado users only).**

SSO Integration for Microsoft and Google Admins

To enable Single Sign-On (SSO) integration for Indigo applications using Microsoft or Google, the following permissions should be added by your organization's admin:

1. **For Google Admins**
    - Go to the Google Admin console.
    - Navigate to "Security" > "API controls" > "Manage third-party app access."
    - Go to “Configure New App” and search for Indigo Education Company and add.
    - Make sure the “Access” permissions are marked as “Trusted”.
2. **For Microsoft Admins**
    - **Log into Azure Portal**:
        1. Visit https://portal.azure.com and log in using an admin account for the school's Azure Active Directory (Azure AD).
    - **Go to App Registrations**:
        1. In the Azure Portal, click on **Azure Active Directory** from the left-hand navigation.
        2. Then, go to **App registrations** in the sub-menu. This is where the admin will manually register your app.
    - **Create a New App Registration**:
        1. Click the **New registration** button at the top of the page.
        2. Fill out the registration form with the following details:
        3. **Name**: The name of your app (e.g., “YourSurveyApp”).
        4. **Supported Account Types**: Select **Accounts in this organizational directory only**.
        5. **Redirect URI**: Select **Web** and enter the callback URL you use in Auth0 for Microsoft login https://dev-gvkzty1a1tzsknur.us.auth0.com.auth0.com/login/callback
    - **App Registration Completion**:
        1. Once the registration is completed, the app will have its **Client ID** and **Tenant ID**.
        2. These values will need to be entered into your Auth0 tenant to allow integration.
    - **Configure API Permissions**:
        1. Go to **API permissions** for the registered app.
        2. Click **Add a permission**, and then select **Microsoft Graph**.
        3. Choose the following delegated permissions:
            1. **email**
            2. **openid**
            3. **profile**
        4. After adding these permissions, click **Grant admin consent** for the organization. This step is crucial to allow students to use their Microsoft credentials without individual user consent prompts.
    - **Add Your App Details to Auth0**:
        1. Now, the admin should provide you with the **Application (client) ID**, **Directory (tenant) ID**, and **Client Secret** (which they can generate from the **Certificates & Secrets** section).
        2. Add these details to your Auth0 **Connections > Social** section for Microsoft authentication.
        3. In Auth0, go to **Connections > Social > Microsoft**.
        4. Enter the **Client ID**, **Client Secret**, and other details provided by the admin.
        5. Save the changes.
    - **Test Authentication**:
        1. The school admin can test the Microsoft login using a student email to ensure everything works.

2. Once successful, students should be able to log in using their Microsoft accounts.
3. App ID 8d00292b-22e1-4dd6-be9b-2f87e8fc9c6a
4. Tenant 8d00292b-22e1-4dd6-be9b-2f87e8fc9c6a

Security and SSL Requirements

All Indigo traffic is designed to operate over SSL. Applications will automatically redirect to SSL if the initial connection is made over port 80. However, websites and some static content may still be delivered over port 80.

Indigo applications do not require incoming connections through network firewalls; however, if remote support is desired, it is recommended that the account team is provided with details on remote connections and support options.

If additional support is required or you have questions, please contact support@indigoproject.org. Thank you!