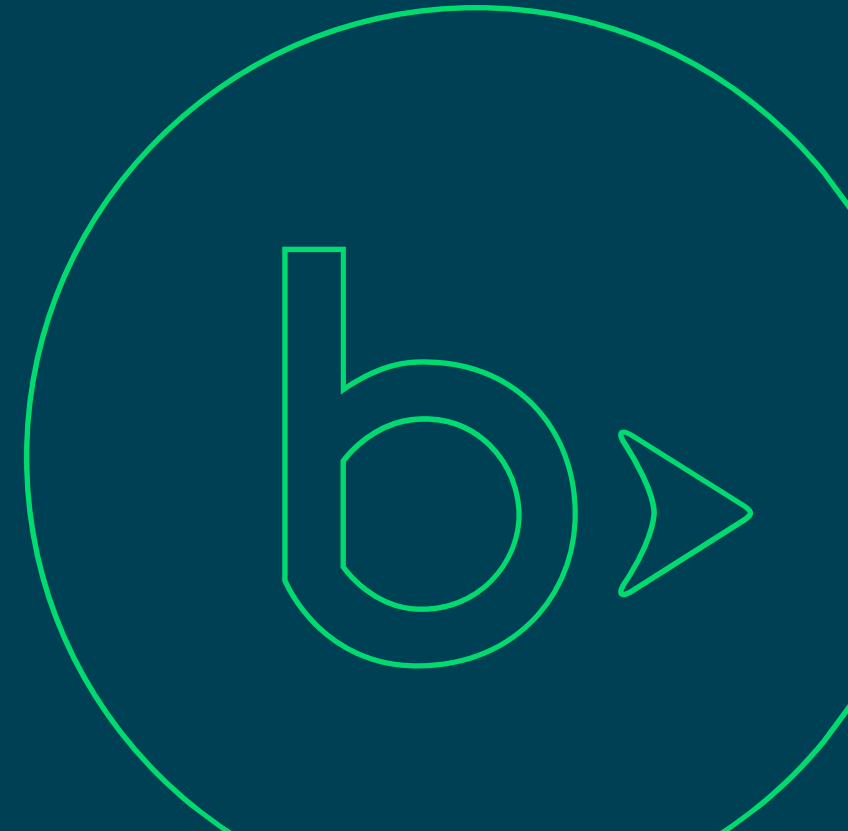


blackbaud®

Using Google as the IDP for a SSO connection with Blackbaud ID

Is your org a Google shop? Then learn how easy it is to setup Single Sign On (SSO) with Blackbaud ID using Google

John Vogel
Senior Technical Product Manager





John Vogel

Senior Technical Product Manager

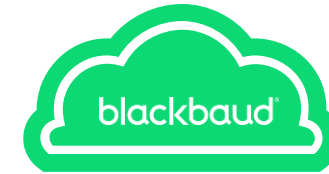
I'm the Identity and Access Management (IAM) product manager for Blackbaud SKY platform solutions.

You're here because you regularly sign in to...

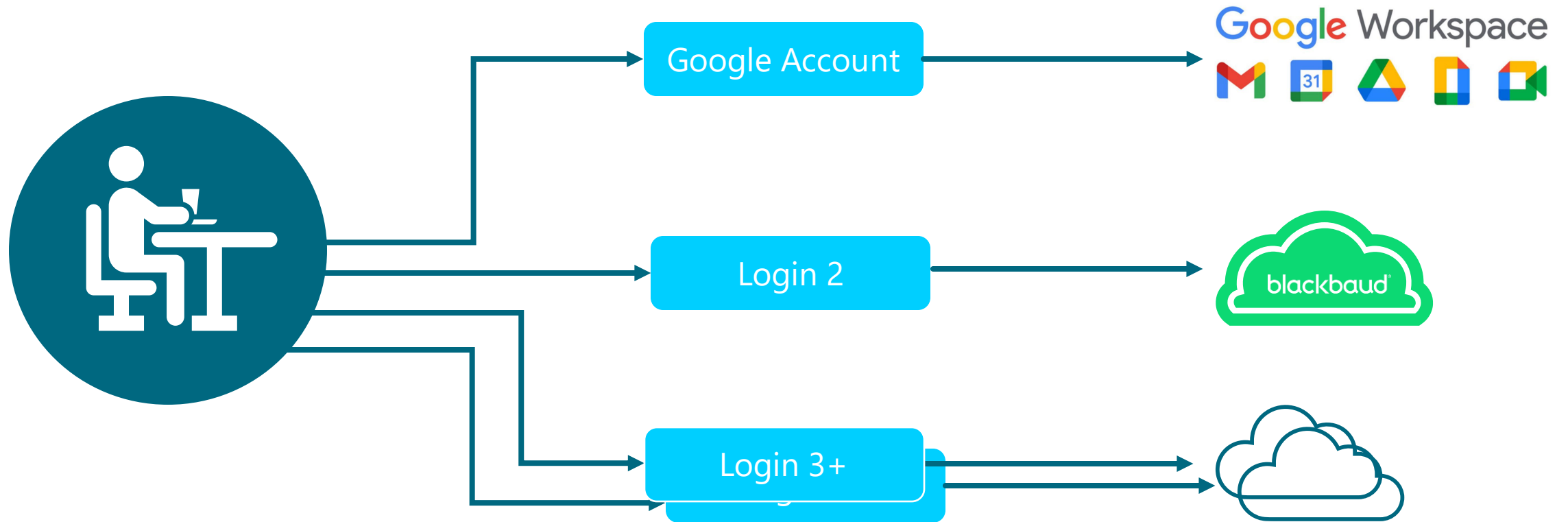
Google Workspace



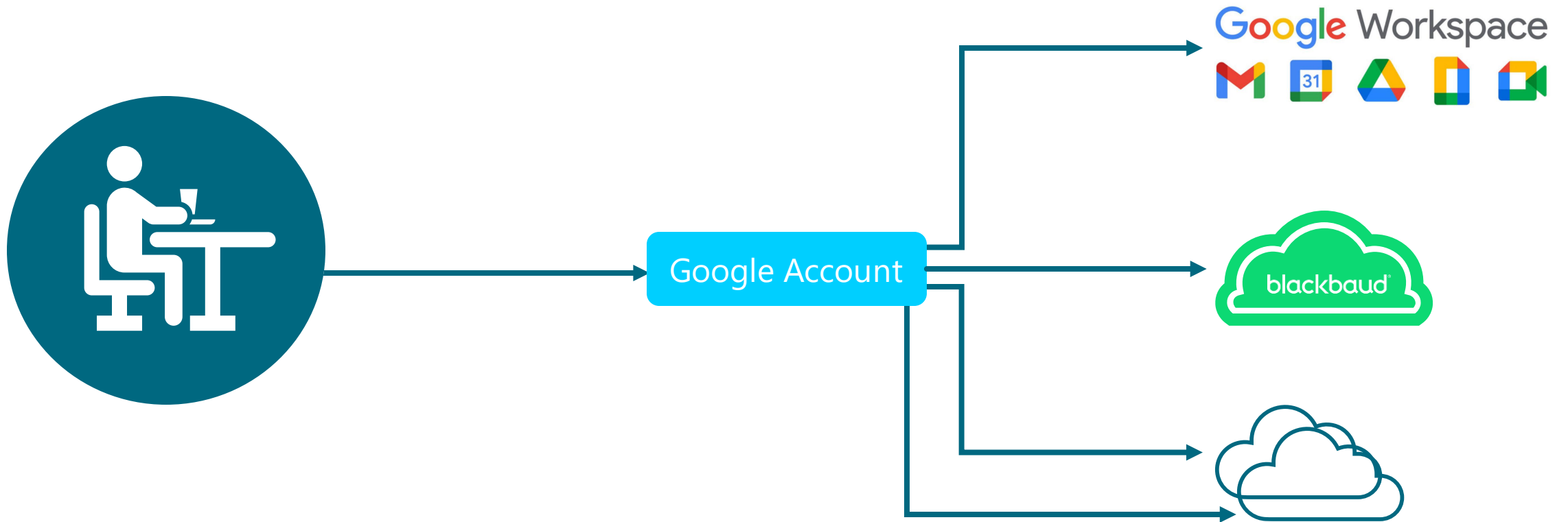
Other Business Applications



And your authentication landscape looks something like...



But you wish it was...



To complete this job you'll need access to 3 roles

- **Blackbaud Org Admin** –to configure the connection on the Blackbaud side
- **Google Admin** – to configure the connection within Google
- **DNS Admin** – to verify ownership of the domain being claimed on the connection

Pro tip: Before starting this process, consider inviting yourself as an Org Admin at an email address that will not be on the same domain you are claiming for SSO. This can help avoid accidental lockout on the account.

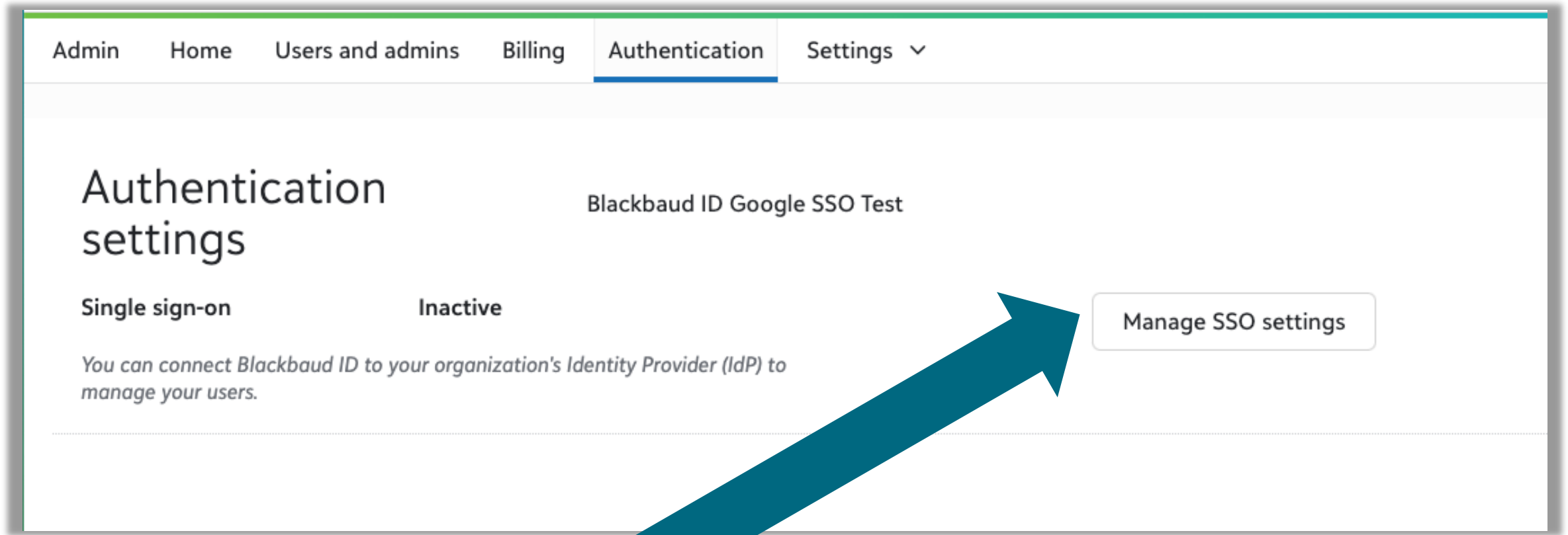
So...

Let's make it
happen!!!

The background features several decorative geometric shapes. In the top-left corner, there is a large cyan rounded square with a white outline of a diamond inside it. To its right is a smaller purple-to-cyan gradient diamond. In the bottom-left, there is a cyan rounded square and a purple diamond. In the bottom-right, there is a large cyan rounded square with a green diamond on top of it, and a white line forming a peak shape below it. The text is centered in the middle of the page.

Google SSO by Creating an Application

Navigate to Manage SSO within Blackbaud Admin



The screenshot shows the Blackbaud Admin interface. The top navigation bar includes links for Admin, Home, Users and admins, Billing, Authentication (which is currently selected and underlined), and Settings with a dropdown arrow. Below the navigation, the page title is 'Authentication settings' and the sub-section is 'Blackbaud ID Google SSO Test'. The status of 'Single sign-on' is shown as 'Inactive'. A teal arrow points from the bottom left towards a button labeled 'Manage SSO settings' on the right side of the page.

Admin Home Users and admins Billing **Authentication** Settings ▾

Authentication settings

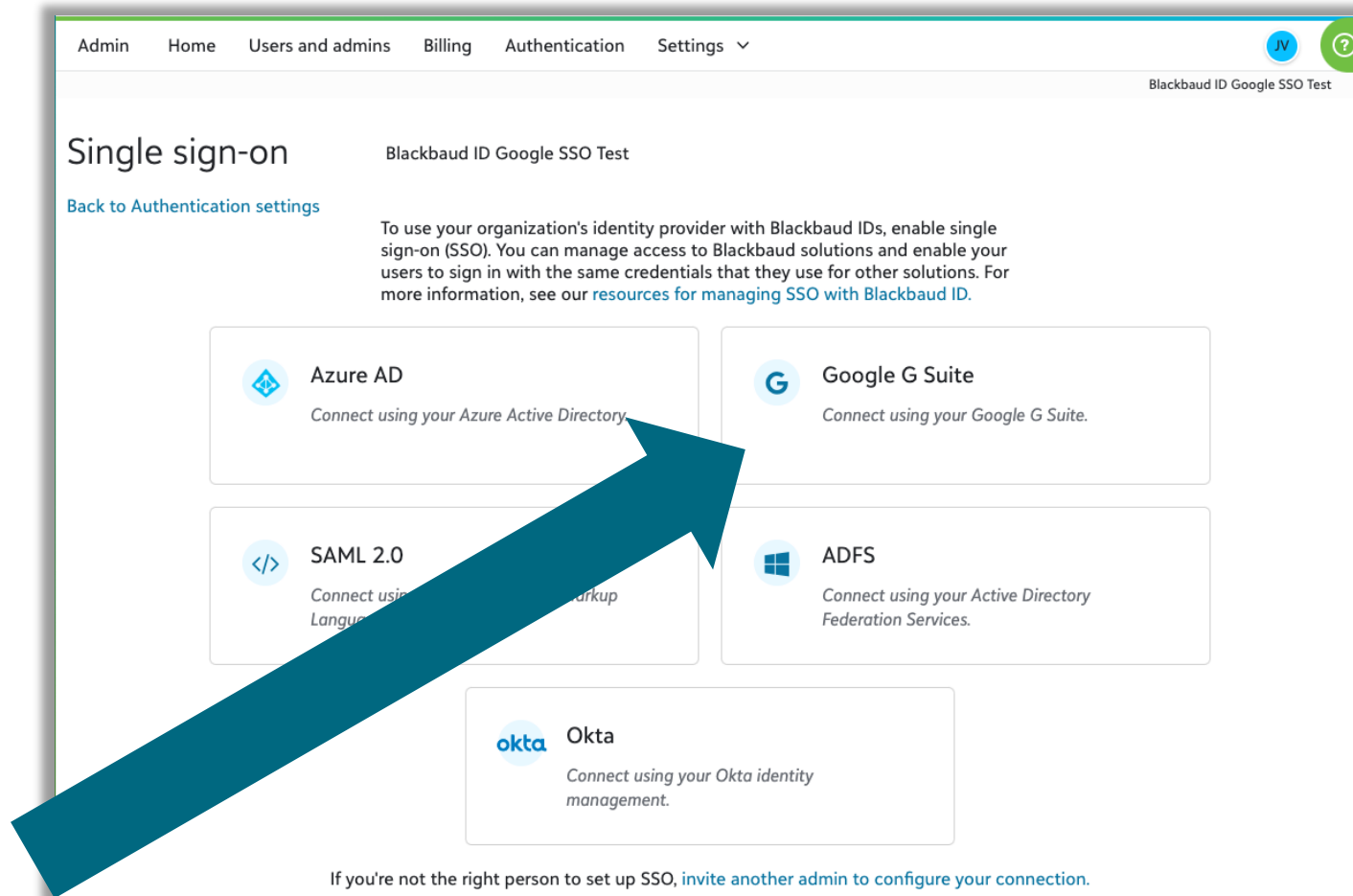
Blackbaud ID Google SSO Test

Single sign-on **Inactive**

You can connect Blackbaud ID to your organization's Identity Provider (IdP) to manage your users.

[Manage SSO settings](#)

Select Google



The screenshot shows the 'Single sign-on' configuration page for 'Blackbaud ID Google SSO Test'. The page includes a navigation bar with 'Admin', 'Home', 'Users and admins', 'Billing', 'Authentication', and 'Settings'. Below the navigation, there is a title 'Single sign-on' and a subtitle 'Blackbaud ID Google SSO Test'. A link 'Back to Authentication settings' is provided. The main content area contains a paragraph explaining SSO and a list of five identity providers: Azure AD, Google G Suite, SAML 2.0, ADFS, and Okta. A large teal arrow points to the 'Google G Suite' option.

Admin Home Users and admins Billing Authentication Settings

Blackbaud ID Google SSO Test

Single sign-on

Blackbaud ID Google SSO Test

[Back to Authentication settings](#)

To use your organization's identity provider with Blackbaud IDs, enable single sign-on (SSO). You can manage access to Blackbaud solutions and enable your users to sign in with the same credentials that they use for other solutions. For more information, see our [resources for managing SSO with Blackbaud ID](#).

- Azure AD**
Connect using your Azure Active Directory.
- Google G Suite**
Connect using your Google G Suite.
- SAML 2.0**
Connect using SAML 2.0 markup Language.
- ADFS**
Connect using your Active Directory Federation Services.
- Okta**
Connect using your Okta identity management.

If you're not the right person to set up SSO, [invite another admin to configure your connection](#).

Configure your connection

Admin Home Users and admins Billing Authentication Settings ▾

Blackbaud ID Google SSO Test

Single sign-on

Blackbaud ID Google SSO Test

[Back to Authentication settings](#)

To prevent inadvertent lockouts, complete this configuration during a maintenance window. [Learn more](#)

Google G Suite configuration

[Invite another admin to configure your connection](#)

- 1 - Configure your connection [Get started!](#)
- 2 - Claim your email domains
- 3 - Test connection
- 4 - Turn on

[Cancel](#)

Enter your primary domain

Admin Home Users and admin...

Blackbaud ID Google SSO Test

Single sign-on

[Back to Authentication settings](#)

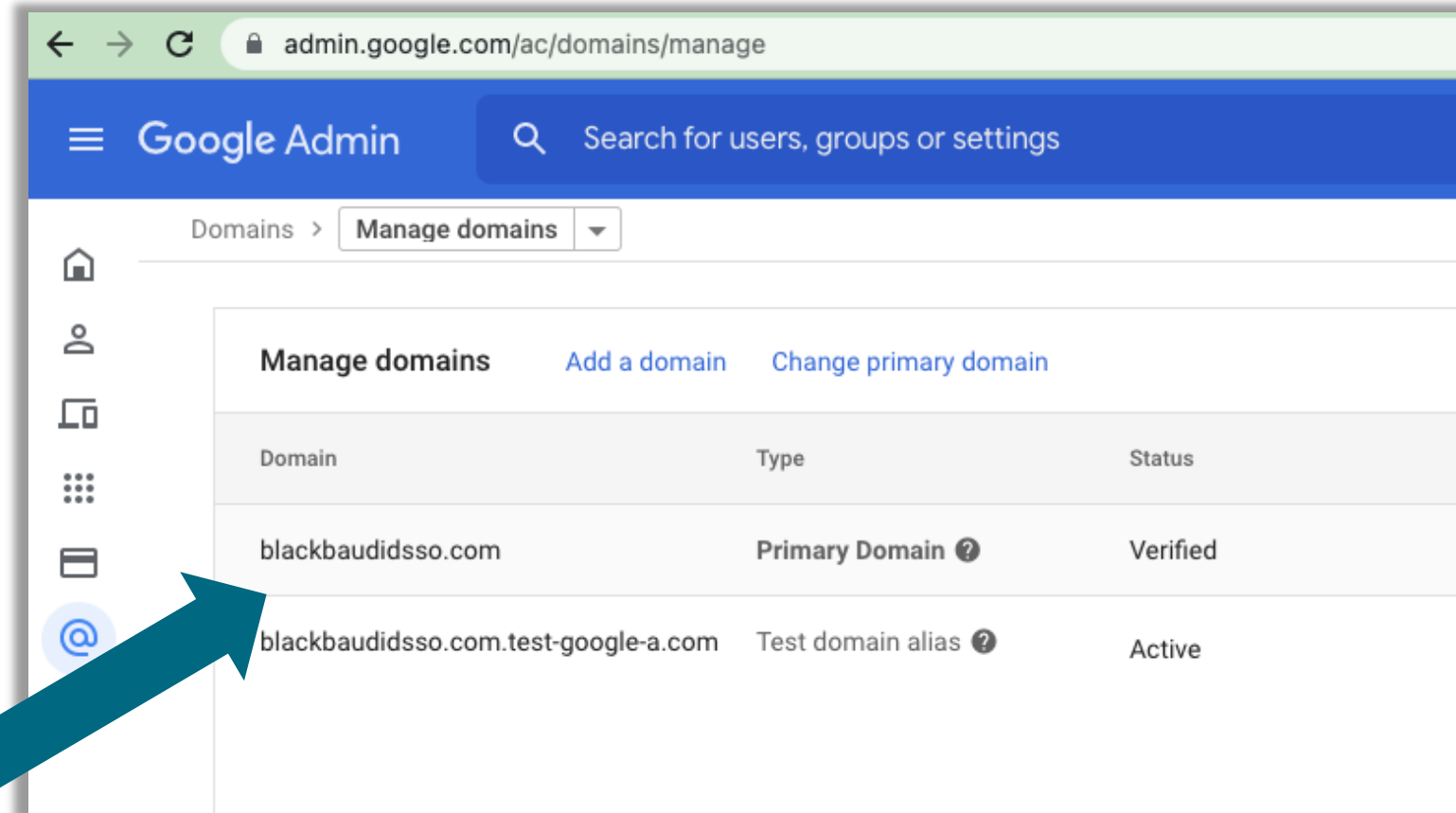
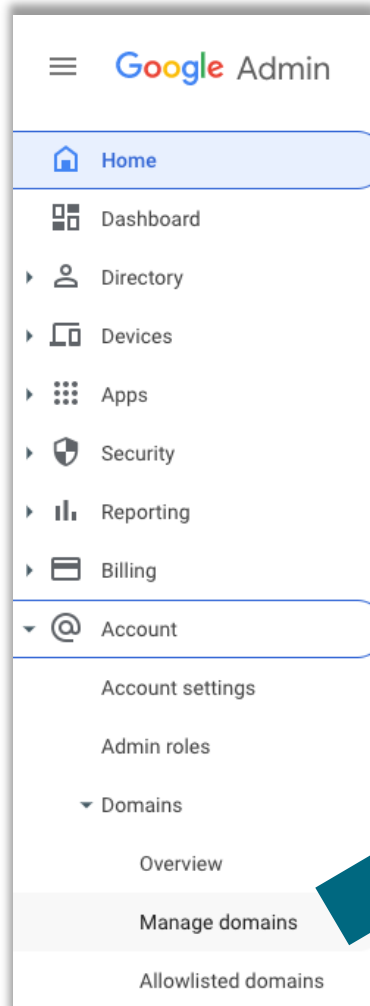
Configure G Suite connection

1. In a separate browser tab, open [your Google APIs](#).
2. Enter your G-Suite primary domain *

⚠ Enter a valid G-Suite domain
Enter the name of your SSO connection to Blackbaud ID. You can save additional email domains later.
3. To configure the Blackbaud ID connection, create a new Web Application project, or choose one on your Google domain.
4. Create new **OAuth Client ID** credentials.
5. Paste this into **Authorized domains** on your **OAuth consent screen**
 [Copy](#)
6. Paste this URL into **Authorized Javascript origins**
 [Copy](#)
7. Paste this URL into **Authorized redirect URIs**
 [Copy](#)
8. Enter your project's Client ID *
9. Enter your project's Client secret *

[Finish](#) [Cancel](#)

Here's where to confirm your domain



Follow Instructions for link to setup Google application

The screenshot shows a web interface for configuring a G Suite connection. The main page is titled "Single sign-on" and has a sidebar with "Admin", "Home", and "Users and admin". The main content area is titled "Configure G Suite connection" and contains a list of instructions. A large blue arrow points from the bottom left towards the instructions. A smaller inset window on the right shows a "Credentials" dialog box with "Select" and "Create" buttons.

Admin Home Users and admin

Single sign-on

[Back to Authentication settings](#)

Configure G Suite connection

1. In a separate browser tab, open [your Google APIs](#).
2. Enter your G-Suite primary domain *

Enter the name of your SSO connection to Blackbaud ID. You can add additional email domains later.
3. To configure the Blackbaud ID connection, create a new Application project, or choose one on your Google domain.
4. Create new **OAuth Client ID** credentials.
5. Paste this into **Authorized domain** *
6. Paste this URL into **Authorized script origins** *
7. Paste this URL into **Authorized redirect URIs** *
8. Enter your project's Client ID *
9. Enter your project's Client secret *

select **Manage SSO settings** under **Single sign-on**.

2. Under **Single sign-on**, select **G Suite**.
3. Under **Configure G Suite connection**, select **Get started** or **Edit connection**.
4. Enter the primary *Google* email domain used with single sign-on (SSO) for your members' Blackbaud IDs.
5. Sign in to [your Google API Console](#) as the administrator for your *G Suite* connection.
6. Choose whether to create a new project or use one already on the domain.

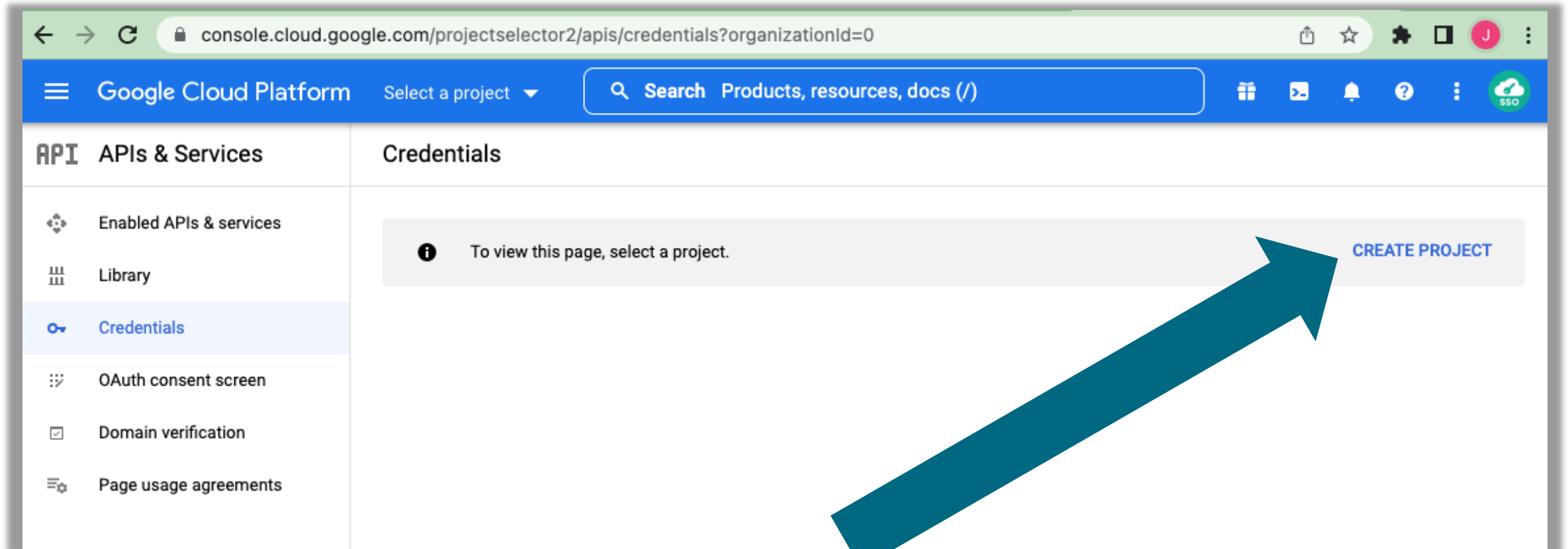
APIs & Services Credentials

To view this page, select a project.

or

- To use an existing project, select **Select**.


This is the view if your org has no existing connections




Create new project

Google Cloud Platform

New Project

 You have 12 projects remaining in your quota. Request an increase or delete projects. [Learn more](#)

[MANAGE QUOTAS](#)

Project name * 

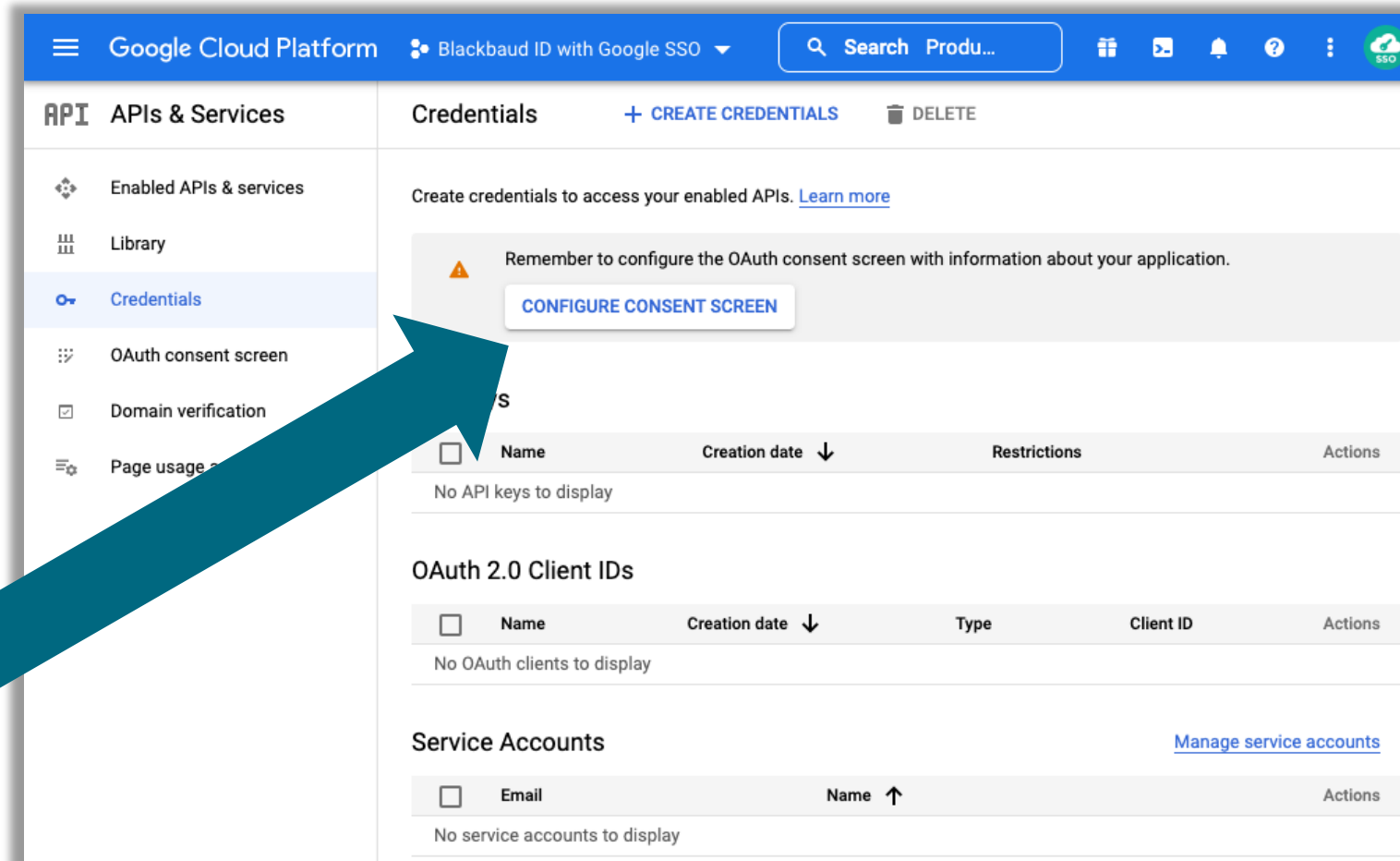
Project ID: optimistic-tree-352319. It cannot be changed later. [EDIT](#)

Location * [BROWSE](#)

Parent organization or folder

[CREATE](#) [CANCEL](#)

Configure consent screen



The screenshot displays the Google Cloud Platform console interface. The top navigation bar includes the Google Cloud Platform logo, the project name 'Blackbaud ID with Google SSO', a search bar, and various utility icons. The left sidebar shows the 'APIs & Services' menu with 'Credentials' selected. The main content area is titled 'Credentials' and features a '+ CREATE CREDENTIALS' button and a 'DELETE' icon. Below this, there is a warning message: 'Remember to configure the OAuth consent screen with information about your application.' A prominent teal arrow points to a 'CONFIGURE CONSENT SCREEN' button located within this warning box. Below the warning, there are three sections: 'API Keys', 'OAuth 2.0 Client IDs', and 'Service Accounts', each with a table header and a 'No [item] to display' message.

Google Cloud Platform | Blackbaud ID with Google SSO | Search | Products | Home | Messages | Notifications | Help | SSO

APIs & Services

- Enabled APIs & services
- Library
- Credentials**
- OAuth consent screen
- Domain verification
- Page usage

Credentials + CREATE CREDENTIALS DELETE

Create credentials to access your enabled APIs. [Learn more](#)

Warning: Remember to configure the OAuth consent screen with information about your application.

[CONFIGURE CONSENT SCREEN](#)

API Keys

<input type="checkbox"/>	Name	Creation date ↓	Restrictions	Actions
No API keys to display				

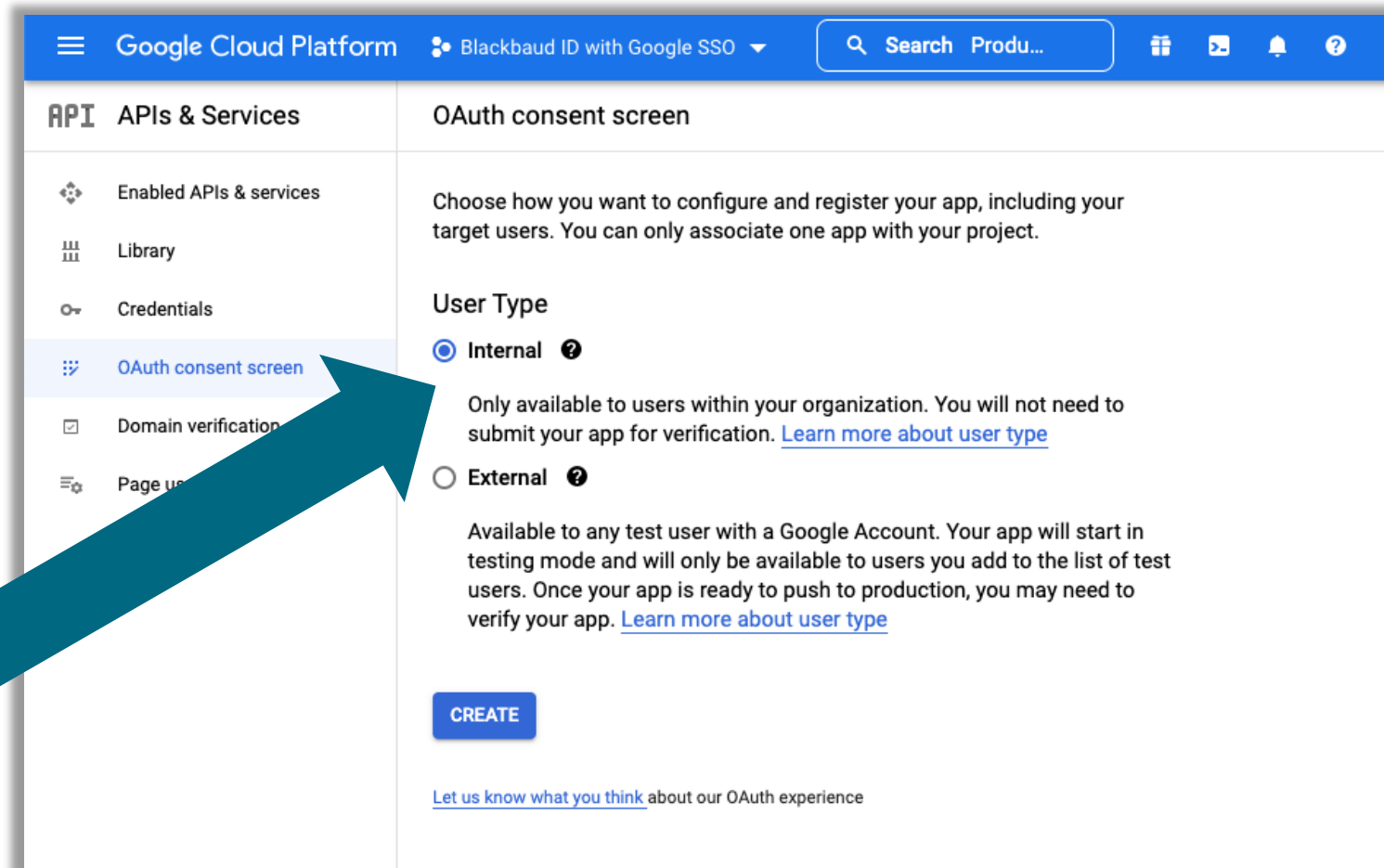
OAuth 2.0 Client IDs

<input type="checkbox"/>	Name	Creation date ↓	Type	Client ID	Actions
No OAuth clients to display					

Service Accounts [Manage service accounts](#)

<input type="checkbox"/>	Email	Name ↑	Actions
No service accounts to display			

Select Internal



The screenshot shows the Google Cloud Platform console interface. At the top, the navigation bar includes the Google Cloud Platform logo, the user account 'Blackbaud ID with Google SSO', a search bar, and utility icons. The left sidebar is titled 'API APIs & Services' and lists several options: 'Enabled APIs & services', 'Library', 'Credentials', 'OAuth consent screen' (highlighted in blue), 'Domain verification', and 'Page us...'. The main content area is titled 'OAuth consent screen' and contains the following text: 'Choose how you want to configure and register your app, including your target users. You can only associate one app with your project.' Below this is the 'User Type' section, which has two radio button options: 'Internal' (selected) and 'External'. The 'Internal' option is accompanied by a help icon and the text: 'Only available to users within your organization. You will not need to submit your app for verification. [Learn more about user type](#)'. The 'External' option is also accompanied by a help icon and the text: 'Available to any test user with a Google Account. Your app will start in testing mode and will only be available to users you add to the list of test users. Once your app is ready to push to production, you may need to verify your app. [Learn more about user type](#)'. At the bottom of the main content area, there is a blue 'CREATE' button and a link: '[Let us know what you think](#) about our OAuth experience'. A large teal arrow points from the bottom left towards the 'Internal' radio button.

Enter the App name and support email (can be a group)

The screenshot shows the Google Cloud Platform interface for editing an app registration. The left sidebar lists navigation options: Enabled APIs & services, Library, Credentials, OAuth consent screen (highlighted), Domain verification, and Page usage agreement. A large teal arrow points from the bottom left towards the 'App name' field in the 'App information' section.

Edit app registration

1 OAuth consent screen — 2 Scopes — 3 Summary

App information

This shows in the consent screen, and helps end users know who you are and contact you

App name *
Blackbaud (or provide a name contextual to your users)

The name of the app asking for consent

User support email *
john.vogel@blackbauidss.com

For users to contact you with questions about their consent

App logo [BROWSE](#)

Upload an image, not larger than 1MB on the consent screen that will help users recognize your app. Allowed image formats are JPG, PNG, and BMP. Logos should be square and 120px by 120px for the best results.

App domain

To protect you and your users, Google only allows apps using OAuth to use Authorized Domains. The following information will be shown to your users on the consent screen.

Application home page
Provide users a link to your home page

Application privacy policy link
Provide users a link to your public privacy policy

Learn

How is this info presented to users?

This is the consent screen that users see

1 [Display Name] wants access to your Google Account

2 Select what [Display Name] can access

3 Make sure you trust [Display Name]

Cancel Allow

Enter Blackbaud.com as Authorized domain

The screenshot displays the Google Cloud Platform console interface for editing an application registration. The left sidebar shows the navigation menu with 'OAuth consent screen' selected. The main content area is titled 'Edit app registration' and includes several configuration sections: 'Application home page', 'Application privacy policy link', 'Application terms of service link', 'Authorized domains', and 'Developer contact information'. In the 'Authorized domains' section, a text input field contains 'blackbaud.com'. A large teal arrow points from the bottom left towards this input field. Below the input field is a '+ ADD DOMAIN' button. To the right of the console, a preview of the OAuth consent screen is shown. It features a 'Sign in with Google' button at the top, followed by three numbered callouts: 1. '[Display Name] wants access to your Google Account', 2. 'Select what [Display Name] can access', and 3. 'Make sure you trust [Display Name]'. At the bottom of the preview are 'Cancel' and 'Allow' buttons.

No scopes needed

The screenshot shows the Google Cloud Platform interface for editing an application registration. The breadcrumb trail is: OAuth consent screen > **Scopes** > Summary. The 'Scopes' step is active. A text block explains that scopes are permissions requested from users to access private user data. Below this is a button labeled 'ADD OR REMOVE SCOPES'. Three sections follow, each with a table header: 'Your non-sensitive scopes', 'Your sensitive scopes', and 'Your restricted scopes'. Each table has columns for 'API', 'Scope', and 'User-facing description', and all three tables display 'No rows to display'. At the bottom are 'SAVE AND CONTINUE' and 'CANCEL' buttons. A large teal arrow points from the left towards the 'No rows to display' text in the 'Your restricted scopes' table.

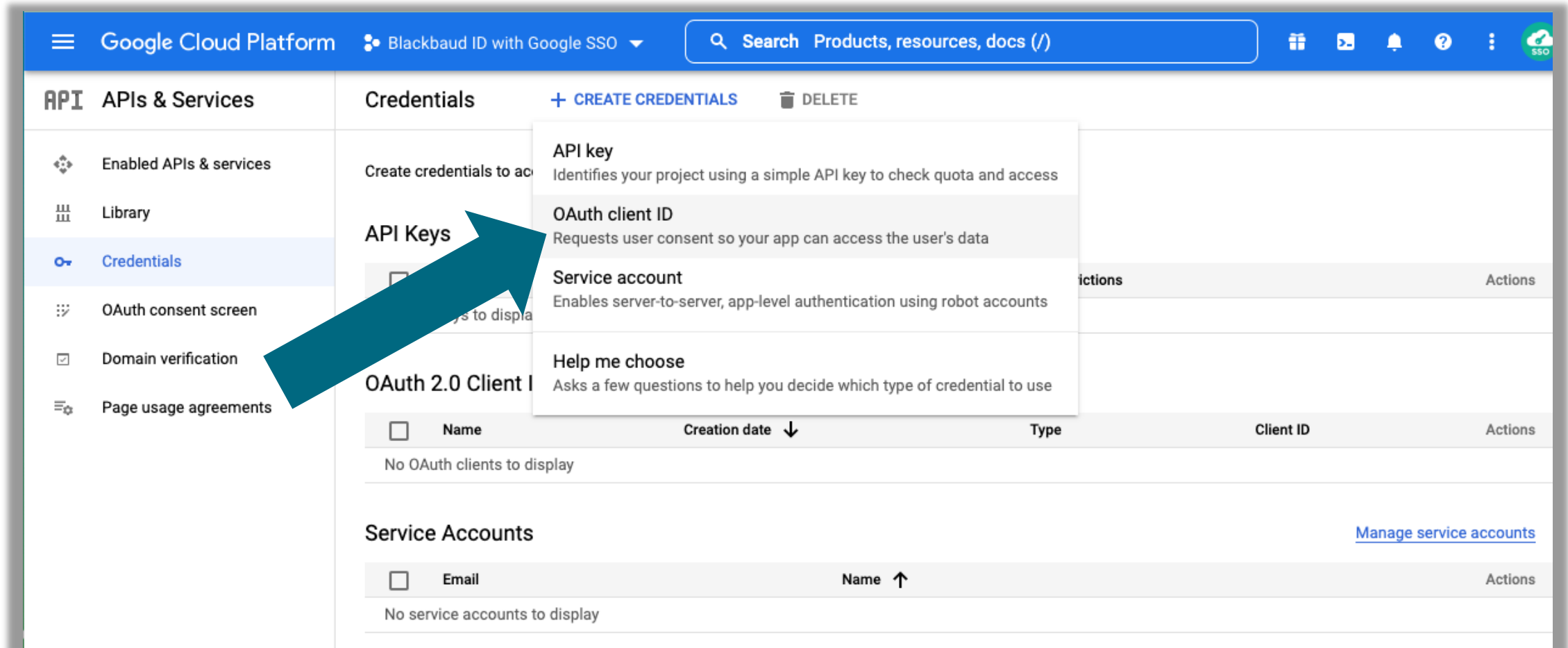
Review Summary and go back to dashboard

The screenshot shows the Google Cloud Platform interface for editing an application registration. The page title is "Edit app registration" and the breadcrumb is "APIs & Services". The left sidebar contains navigation options: "Enabled APIs & services", "Library", "Credentials", "OAuth consent screen" (highlighted), "Domain verification", and "Page usage agreements". The main content area displays the following information:

- App name:** Blackbaud (or provide a name contextual to your users)
- Support email:** john.vogel@blackbaudidsso.com
- App logo:** Not provided
- Application homepage link:** Not provided
- Application privacy policy link:** Not provided
- Application terms of service link:** Not provided
- Authorized domains:** blackbaud.com
- Contact email addresses:** john.vogel@blackbaud.com, john.vogel@blackbaudidsso.com

Below this information is a section for "Scopes" with an "EDIT" link. A table header is visible with columns for "API", "Scope", and "User-facing description", but it contains no data rows. At the bottom of the page, there is a button labeled "BACK TO DASHBOARD". A large teal arrow points from the bottom left towards this button.

Go to Credentials tab & create OAuth client ID



The screenshot shows the Google Cloud Platform interface for the 'Credentials' tab. The left sidebar contains the 'APIs & Services' menu with 'Credentials' selected. The main content area has a '+ CREATE CREDENTIALS' button and a 'DELETE' button. A dropdown menu is open from the '+ CREATE CREDENTIALS' button, listing four options: 'API key', 'OAuth client ID', 'Service account', and 'Help me choose'. A large teal arrow points from the 'Credentials' tab in the sidebar to the 'OAuth client ID' option in the dropdown. Below the dropdown, there are sections for 'API Keys', 'OAuth 2.0 Client IDs', and 'Service Accounts', each with a table header and a 'No [type] to display' message.

Google Cloud Platform Blackbaud ID with Google SSO Search Products, resources, docs (/)

APIs & Services

- Enabled APIs & services
- Library
- Credentials**
- OAuth consent screen
- Domain verification
- Page usage agreements

Credentials + CREATE CREDENTIALS DELETE

Create credentials to access your project

API Keys

- Name Creation date ↓ Type Client ID Actions

No OAuth clients to display

OAuth 2.0 Client IDs

Service Accounts [Manage service accounts](#)

- Email Name ↑ Actions

No service accounts to display

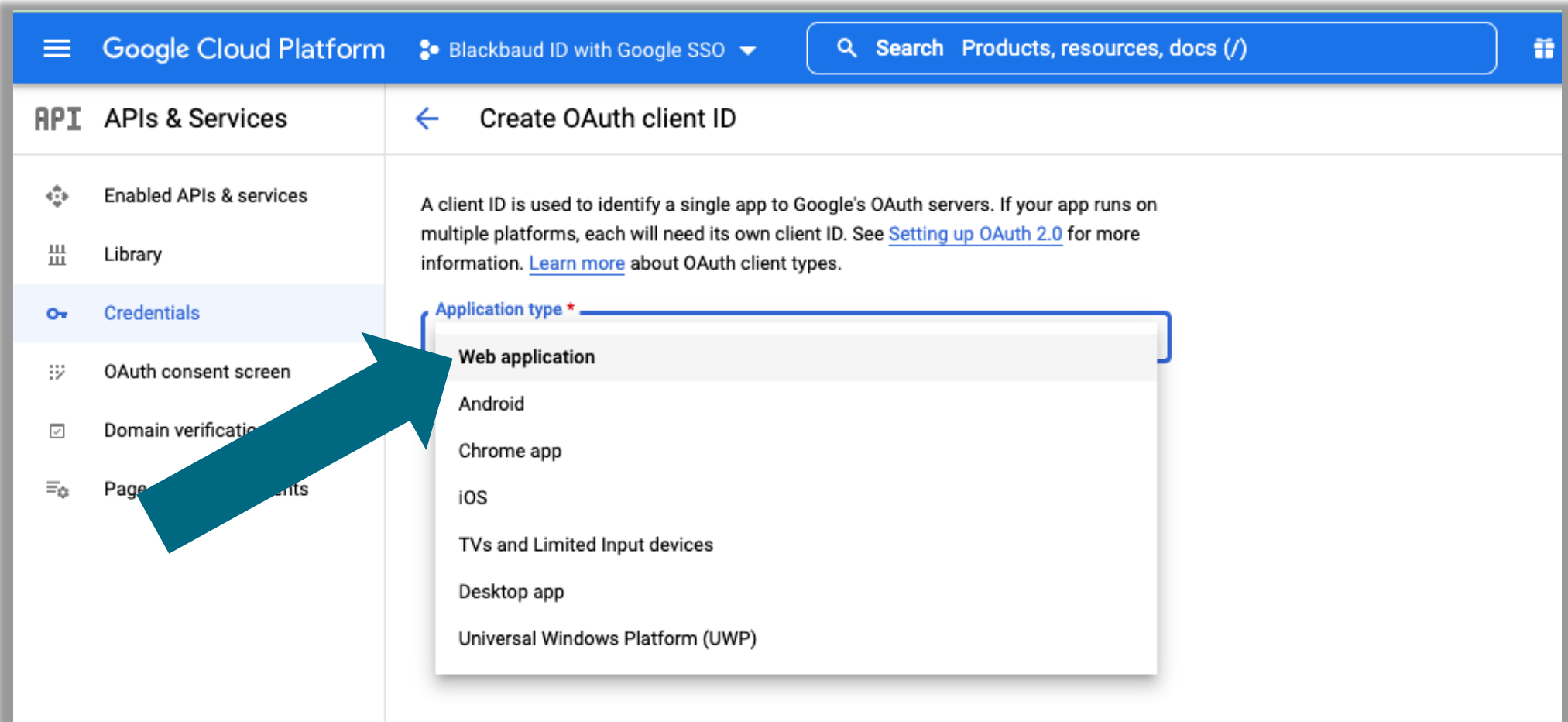
API key
Identifies your project using a simple API key to check quota and access

OAuth client ID
Requests user consent so your app can access the user's data

Service account
Enables server-to-server, app-level authentication using robot accounts

Help me choose
Asks a few questions to help you decide which type of credential to use

Select Web application



The screenshot shows the Google Cloud Platform console interface. At the top, there is a blue header with the text "Google Cloud Platform" and "Blackbaud ID with Google SSO". A search bar is visible on the right. The main content area is titled "Create OAuth client ID". On the left, there is a navigation menu with "APIs & Services" selected, and "Credentials" highlighted. The main content area contains a description of a client ID and a dropdown menu for "Application type". The dropdown menu is open, showing options: "Web application", "Android", "Chrome app", "iOS", "TVs and Limited Input devices", "Desktop app", and "Universal Windows Platform (UWP)". A teal arrow points to the "Web application" option.

Google Cloud Platform Blackbaud ID with Google SSO Search Products, resources, docs (/)

API APIs & Services

Enabled APIs & services

Library

Credentials

OAuth consent screen

Domain verification

Page

← Create OAuth client ID

A client ID is used to identify a single app to Google's OAuth servers. If your app runs on multiple platforms, each will need its own client ID. See [Setting up OAuth 2.0](#) for more information. [Learn more](#) about OAuth client types.

Application type *

- Web application**
- Android
- Chrome app
- iOS
- TVs and Limited Input devices
- Desktop app
- Universal Windows Platform (UWP)

Copy over the authorized URIs from Blackbaud

The image shows a side-by-side comparison of two Google Cloud Platform (GCP) configuration screens. On the left is the 'Configure G Suite connection' dialog, and on the right is the 'Create OAuth client ID' page. Two large blue arrows indicate the transfer of information from the left to the right.

Configure G Suite connection (Left Panel):

- Step 3: To configure the Blackbaud ID connection, create a new Web Application project, or choose one on your Google domain.
- Step 4: Create new **OAuth Client ID** credentials.
- Step 5: Paste this into **Authorized domains** on your **OAuth consent screen**
blackbaud.com
- Step 6: Paste this URL into **Authorized Javascript origins**
https://bbid.blackbaud.com
- Step 7: Paste this URL into **Authorized redirect URIs**
https://bbid.blackbaud.com/login/callback
- Step 8: Enter your project's Client ID *
- Step 9: Enter your project's Client secret *
- Step 10: Ensure the **Admin SDK** library is enabled on your project.

Create OAuth client ID (Right Panel):

- Application type: Web application
- Name: Blackbaud ID
- Authorized JavaScript origins: https://bbid.blackbaud.com
- Authorized redirect URIs: https://bbid.blackbaud.com/login/callback

Note: It may take 5 minutes to a few hours for settings to take effect.

Enter your project's Client ID & Client Secret

The image shows a composite screenshot of the Google Cloud Platform console. On the left, a 'Configure G Suite connection' dialog box contains a list of steps. Step 8, 'Enter your project's Client ID', and step 9, 'Enter your project's Client secret', are highlighted with red arrows pointing to the 'Your Client ID' and 'Your Client Secret' fields in a 'OAuth client created' dialog box on the right. The background shows the 'APIs & Services' page with 'Credentials' selected, displaying a table with one OAuth 2.0 Client ID entry. The 'Your Client ID' and 'Your Client Secret' fields in the dialog box are filled with redacted text.

Configure G Suite connection

Enter the name of your SSO connection to Blackbaud ID. You can save additional email domains later.

- To configure the Blackbaud ID connection, create a new Web Application project, or choose one on your Google domain.
- Create new **OAuth Client ID** credentials.
- Paste this into **Authorized domains** on your **OAuth consent screen**
blackbaud.com
- Paste this URL into **Authorized Javascript origins**
https://bbid.blackbaud.com
- Paste this URL into **Authorized redirect URIs**
https://bbid.blackbaud.com/login/callback
- Enter your project's Client ID *
- Enter your project's Client secret *
- Ensure the **Admin SDK** library is enabled on your project.

⚠ After you save this connection, Blackbaud IDs on your primary email domain won't be able to sign in through Google until you complete the configuration.

OAuth client created

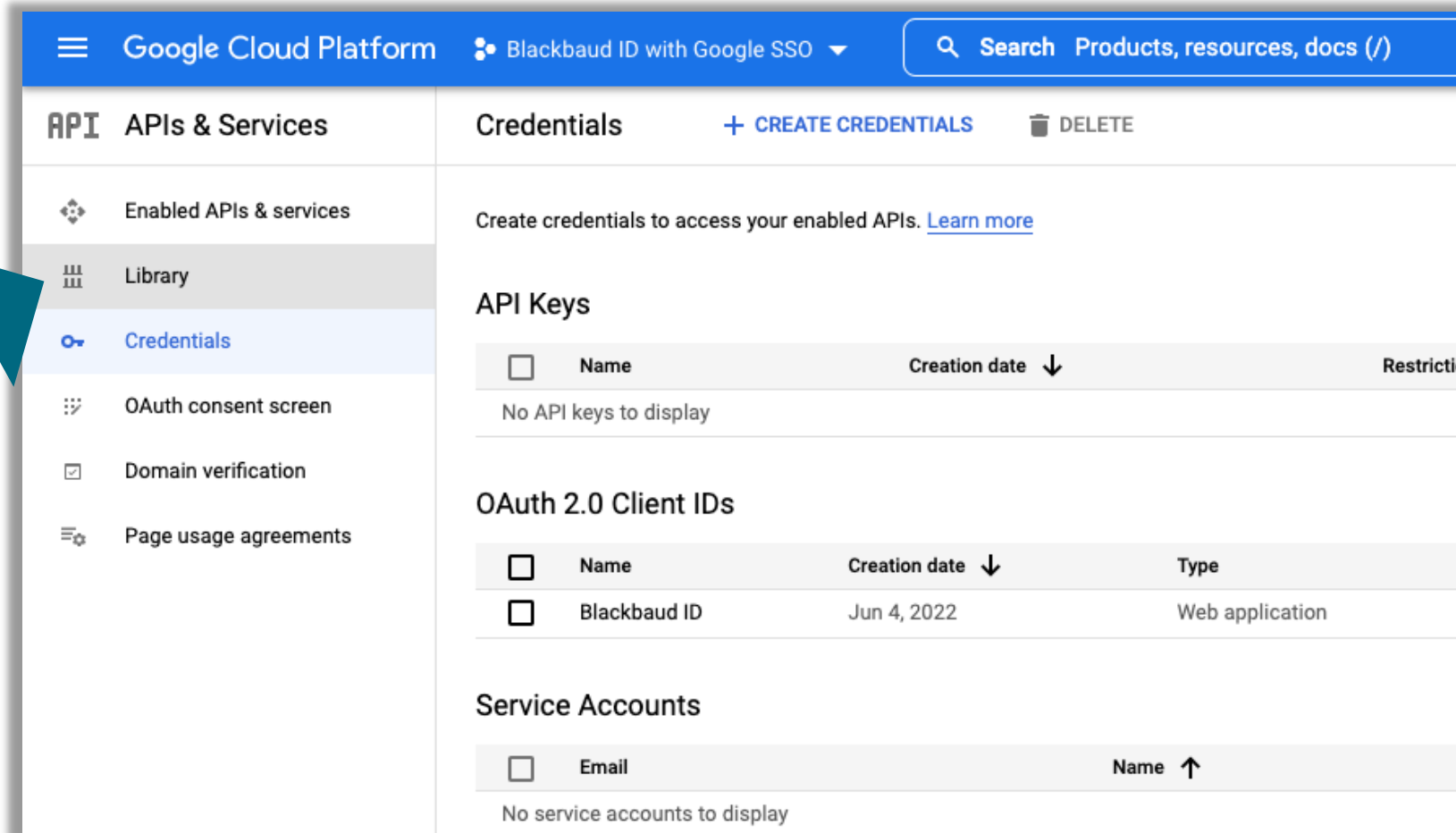
The client ID and secret can always be accessed from Credentials in APIs & Services

ⓘ OAuth access is restricted to users within your organization unless the [OAuth consent screen](#) is published and verified

Your Client ID

Your Client Secret

Go to the Library



The screenshot shows the Google Cloud Platform console interface. The top navigation bar includes the Google Cloud Platform logo, the user profile 'Blackbaud ID with Google SSO', and a search bar. The left sidebar contains a menu with the following items: 'APIs & Services', 'Library', 'Credentials', 'OAuth consent screen', 'Domain verification', and 'Page usage agreements'. A large teal arrow points to the 'Library' menu item. The main content area is titled 'Credentials' and includes a '+ CREATE CREDENTIALS' button and a 'DELETE' button. Below this, there is a section for 'API Keys' with a table that currently shows 'No API keys to display'. Another section for 'OAuth 2.0 Client IDs' contains a table with one entry: 'Blackbaud ID' created on 'Jun 4, 2022' as a 'Web application'. A final section for 'Service Accounts' shows 'No service accounts to display'.

Google Cloud Platform Blackbaud ID with Google SSO Search Products, resources, docs (/)

APIs & Services Credentials + CREATE CREDENTIALS DELETE

Enabled APIs & services

Library

Credentials

OAuth consent screen

Domain verification

Page usage agreements

Create credentials to access your enabled APIs. [Learn more](#)

API Keys

<input type="checkbox"/>	Name	Creation date ↓	Restrictio
No API keys to display			

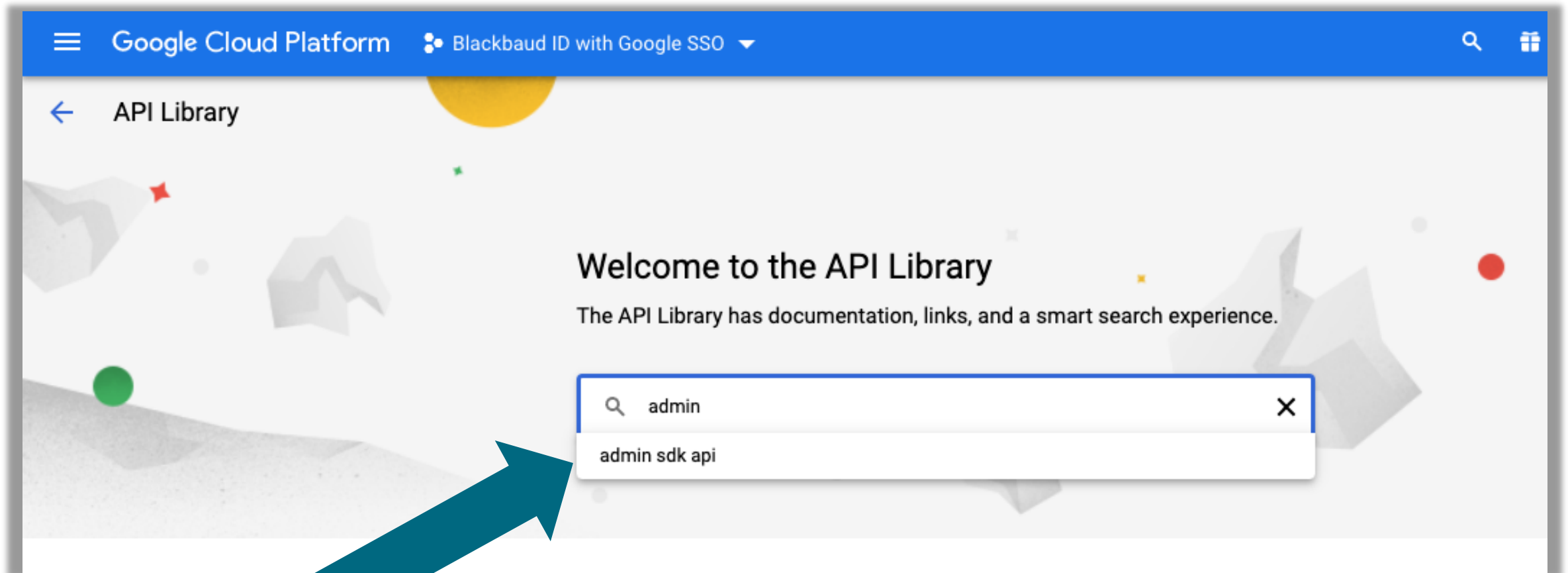
OAuth 2.0 Client IDs

<input type="checkbox"/>	Name	Creation date ↓	Type
<input type="checkbox"/>	Blackbaud ID	Jun 4, 2022	Web application

Service Accounts

<input type="checkbox"/>	Email	Name ↑
No service accounts to display		

Search for Admin SDK API



Select Admin SDK API

The screenshot shows the Google Cloud Platform API Library interface. At the top, the navigation bar includes 'Google Cloud Platform' and 'Blackbaud ID with Google SSO'. A search bar contains the text 'admin sdk api'. Below the search bar, the breadcrumb 'API Library > "admin sdk api"' is visible. A filter section on the left lists categories: 'Developer tools (1)', 'Google Enterprise APIs (2)', 'Security (1)', and 'Google Workspace'. The search results are titled '"admin sdk api"' and show '2 results'. The first result is 'Admin SDK API', a Google Enterprise API, with a description: 'Admin SDK lets administrators of enterprise domains to view and manage resources like user, groups etc. It also provides audit and usage reports of domain.' The second result is 'Cloud Identity', also a Google Enterprise API, with a description: 'Cloud Identity is the most secure platform for managing your company's users, devices and applications in the cloud. Stay secure on the same infrastructure Google uses to manage billions of enterprise and consumer identities. Backed by Google Cloud, you can scale from prototype to planet-scale without having to think about capacity. Cloud Identity features include user lifecycle management, account security, single sign-on,...

API Library

API Library > "admin sdk api"

Filter Type to filter

"admin sdk api"

2 results

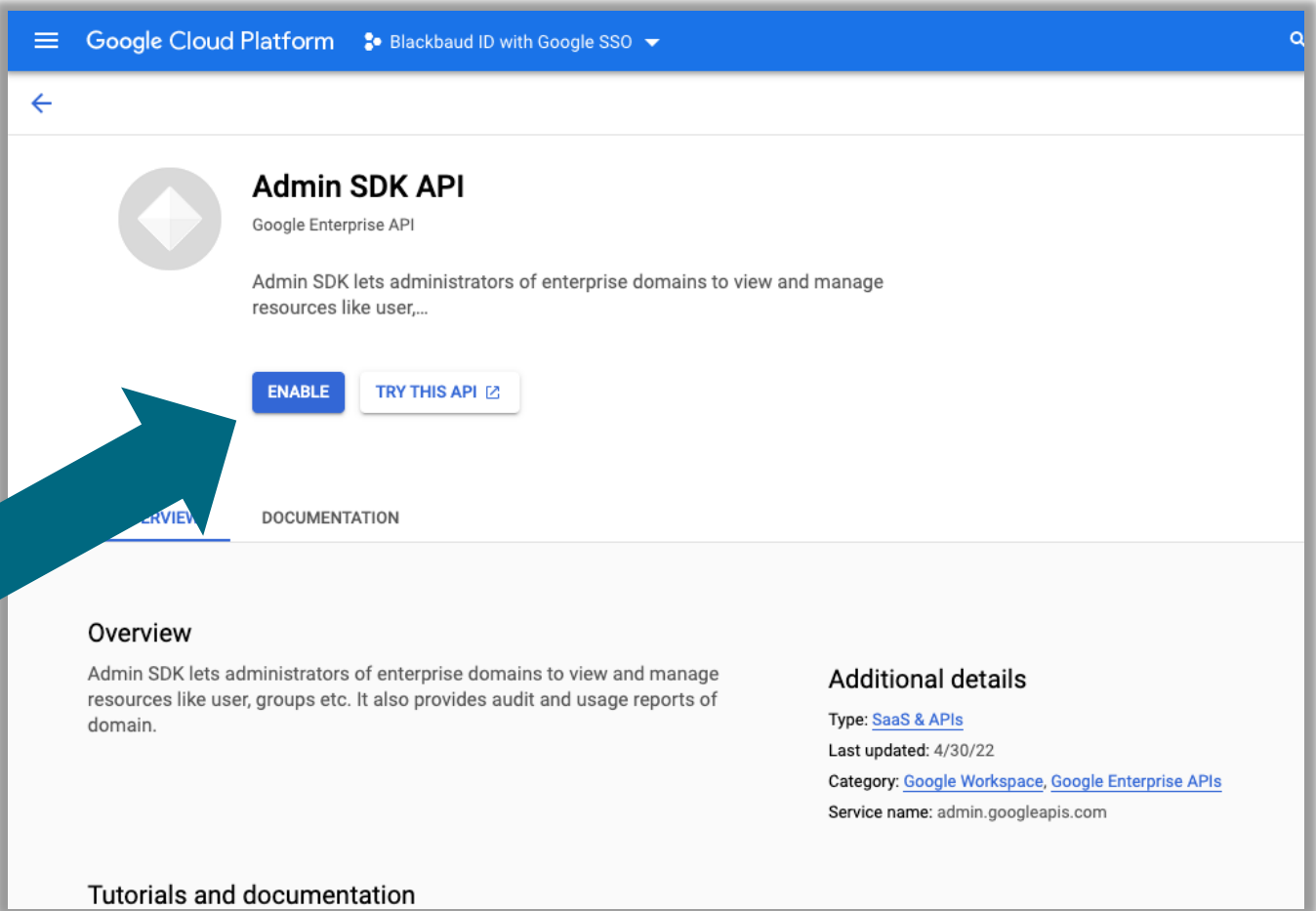
Category ^

- Developer tools (1)
- Google Enterprise APIs (2)
- Security (1)
- Google Workspace

Admin SDK API
Google Enterprise API ⓘ
Admin SDK lets administrators of enterprise domains to view and manage resources like user, groups etc. It also provides audit and usage reports of domain.

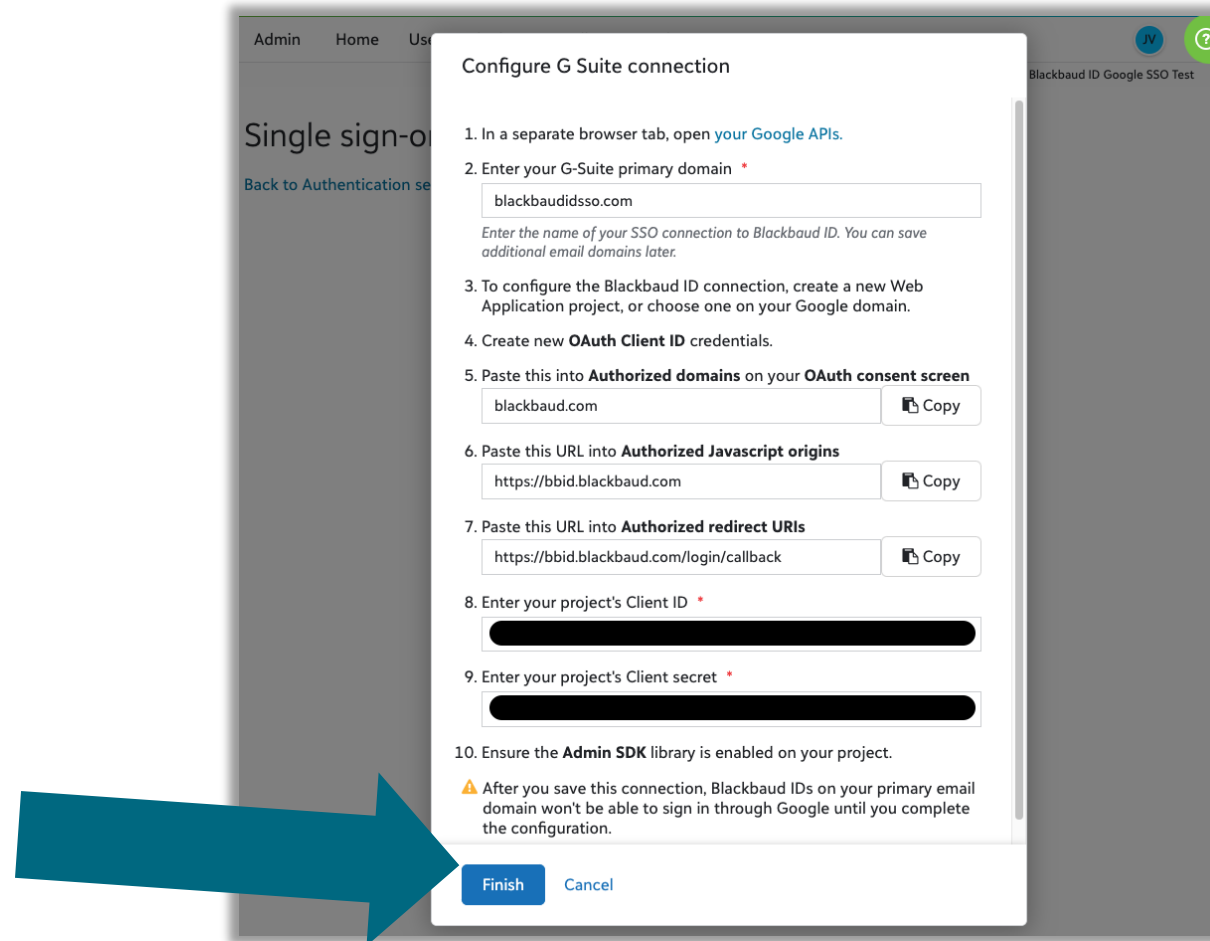
Cloud Identity
Google Enterprise API ⓘ
Cloud Identity is the most secure platform for managing your company's users, devices and applications in the cloud. Stay secure on the same infrastructure Google uses to manage billions of enterprise and consumer identities. Backed by Google Cloud, you can scale from prototype to planet-scale without having to think about capacity. Cloud Identity features include user lifecycle management, account security, single sign-on,...

Enable Admin SDK API



The screenshot shows the Google Cloud Platform interface for the Admin SDK API. At the top, the navigation bar includes 'Google Cloud Platform' and 'Blackbaud ID with Google SSO'. Below the navigation bar, the API name 'Admin SDK API' is displayed with a 'Google Enterprise API' label. A description states: 'Admin SDK lets administrators of enterprise domains to view and manage resources like user,...'. Two buttons are visible: a blue 'ENABLE' button and a white 'TRY THIS API' button with an external link icon. Below the buttons are tabs for 'OVERVIEW' and 'DOCUMENTATION'. The 'OVERVIEW' section contains the text: 'Admin SDK lets administrators of enterprise domains to view and manage resources like user, groups etc. It also provides audit and usage reports of domain.' The 'Additional details' section lists: 'Type: SaaS & APIs', 'Last updated: 4/30/22', 'Category: Google Workspace, Google Enterprise APIs', and 'Service name: admin.googleapis.com'. At the bottom, there is a section for 'Tutorials and documentation'. A large teal arrow points from the left towards the 'ENABLE' button.

Finish connection



Admin Home User

Blackbaud ID Google SSO Test

Configure G Suite connection

1. In a separate browser tab, open [your Google APIs](#).
2. Enter your G-Suite primary domain *

Enter the name of your SSO connection to Blackbaud ID. You can save additional email domains later.
3. To configure the Blackbaud ID connection, create a new Web Application project, or choose one on your Google domain.
4. Create new **OAuth Client ID** credentials.
5. Paste this into **Authorized domains** on your **OAuth consent screen**
6. Paste this URL into **Authorized Javascript origins**
7. Paste this URL into **Authorized redirect URIs**
8. Enter your project's Client ID *
9. Enter your project's Client secret *
10. Ensure the **Admin SDK** library is enabled on your project.

⚠ After you save this connection, Blackbaud IDs on your primary email domain won't be able to sign in through Google until you complete the configuration.

Claim Email Domains

Admin Home Users and admins Billing Authentication Settings

Blackbaud

Single sign-on

Blackbaud ID Google SSO Test

[Back to Authentication settings](#)

⚠ Blackbaud IDs on your email domain won't be able to sign in through Google until you complete or erase this configuration.

Google G Suite configuration

[Invite another admin to configure your connection](#)

- ✓ 1 - Configure your connection
[Edit connection](#)
- ➔ 2 - Claim your email domains
[Claim domains](#)
- 3 - Test connection
- 4 - Turn on

[Erase all single sign-on settings](#)


Enter domain and start verification

Claim email domains


Enter the domains you want to claim below [i](#)

[Start domain verification](#)

[+ Claim another domain](#)

 *You must verify your domains to begin testing your SSO connection*


[Close](#)




Record details to place on DNS

Claim email domains

Enter the domains you want to claim below [?](#)


blackbaudidsso.com Add a custom record to your DNS configuration with the following 

Name/Host/Alias	@
Record type	TXT
Time to live (TTL)	3600 (or 1 hour)
Value	<input type="text" value=""/>  Copy

Verify this domain Verifying...

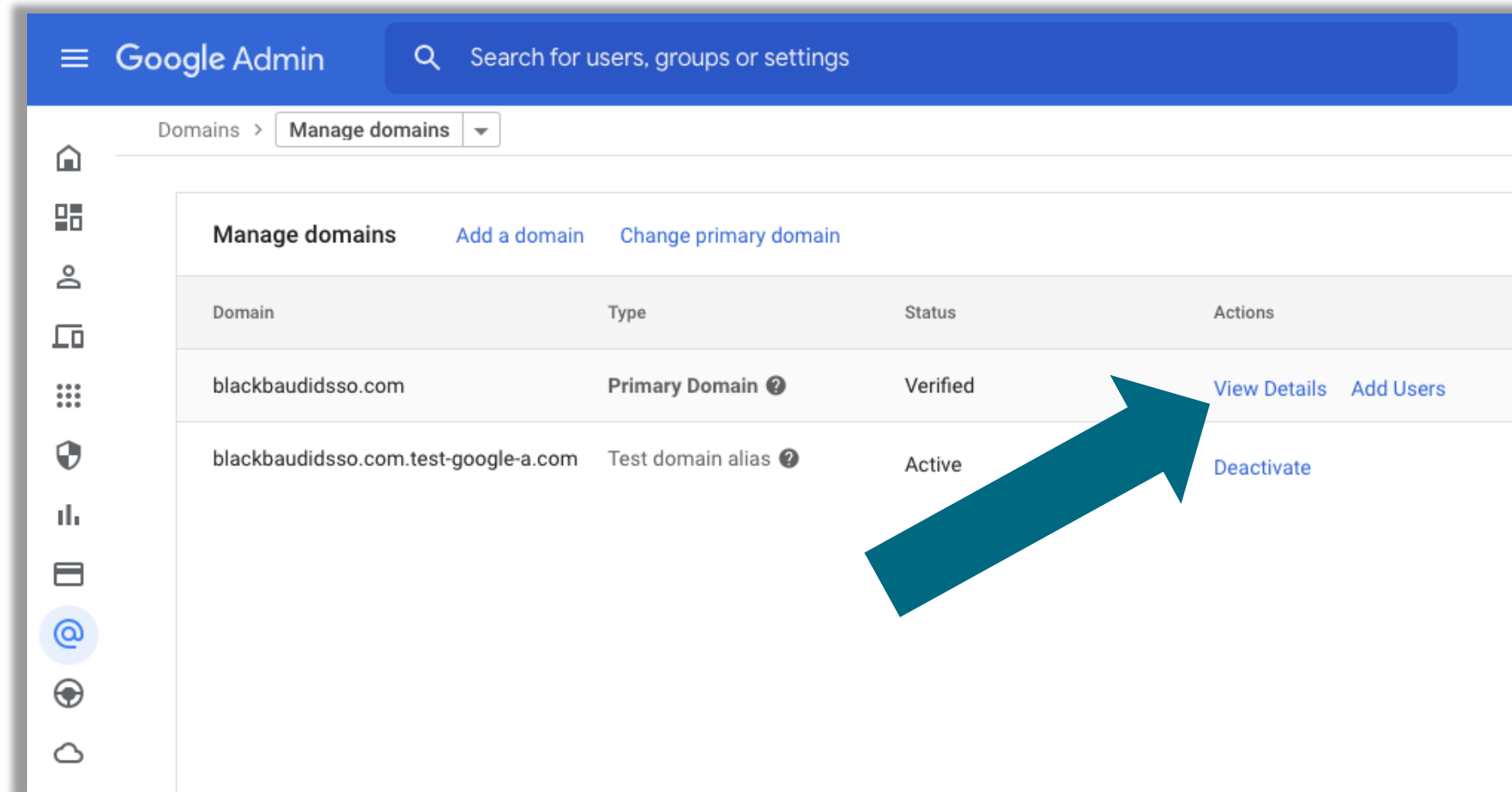
This can take a few minutes or up to 2 days, but we'll email you as soon as we verify this domain. [Troubleshoot the issue.](#)

[+ Claim another domain](#)

 You must verify your domains to begin testing your SSO connection

Close

View details of domain



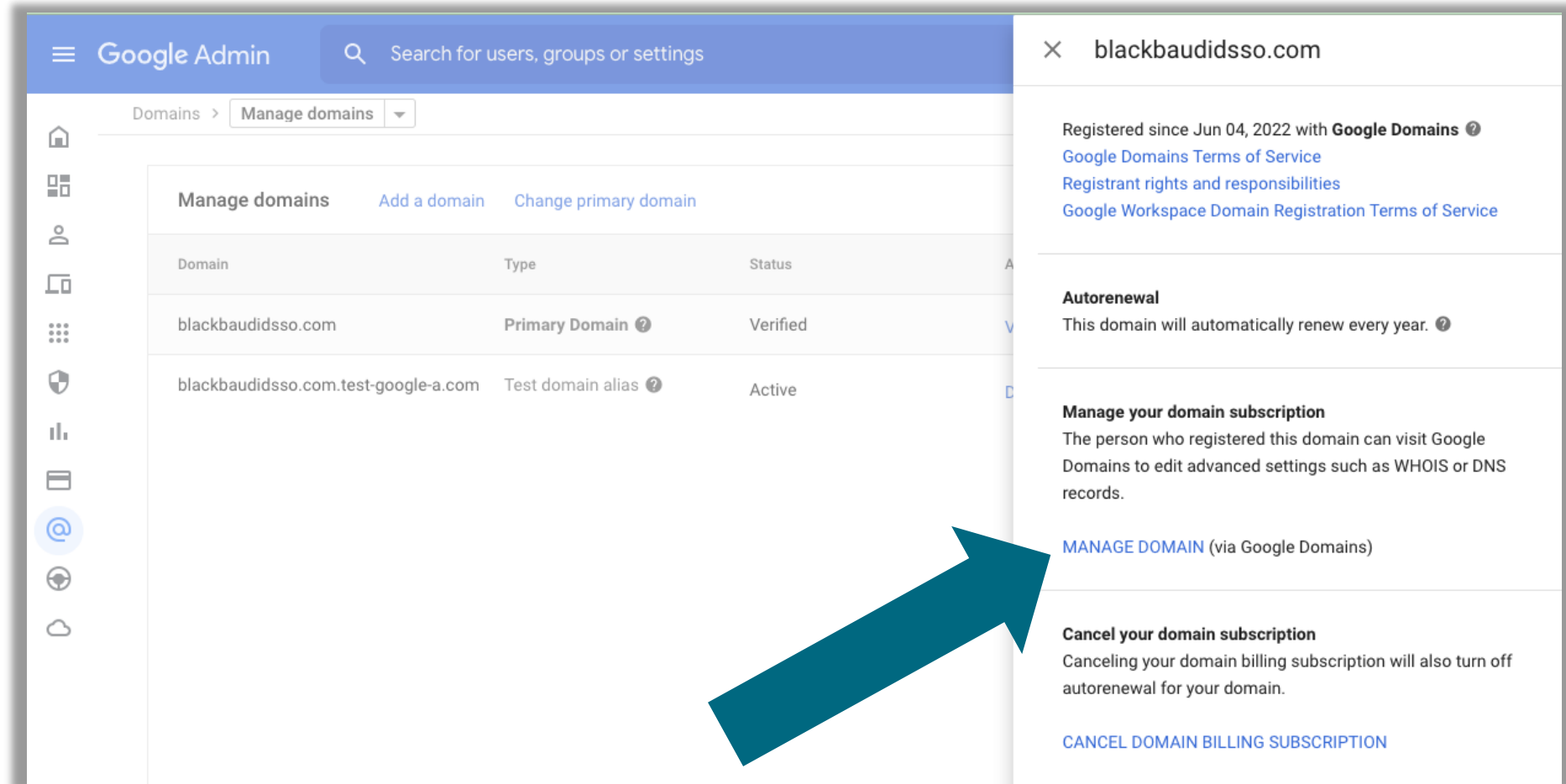
The screenshot shows the Google Admin console interface. At the top, there is a blue header with the Google Admin logo and a search bar. Below the header, the breadcrumb navigation shows 'Domains > Manage domains'. The main content area features a 'Manage domains' section with two links: 'Add a domain' and 'Change primary domain'. Below this is a table with columns for 'Domain', 'Type', 'Status', and 'Actions'. The table contains two rows: one for 'blackbaudidsso.com' (Primary Domain, Verified) and one for 'blackbaudidsso.com.test-google-a.com' (Test domain alias, Active). A large teal arrow points to the 'View Details' link in the 'Actions' column of the first row.

Domains > Manage domains

Manage domains [Add a domain](#) [Change primary domain](#)

Domain	Type	Status	Actions
blackbaudidsso.com	Primary Domain ?	Verified	View Details Add Users
blackbaudidsso.com.test-google-a.com	Test domain alias ?	Active	Deactivate

Go to Google Domains (or your domain manager)



The screenshot shows the Google Admin interface for domain management. The left sidebar contains navigation icons, and the main content area displays a table of domains. A teal arrow points from the bottom of the table to the 'MANAGE DOMAIN' link in the right-hand details panel.

Google Admin Search for users, groups or settings

Domains > Manage domains

Domain	Type	Status
blackbaudidsso.com	Primary Domain	Verified
blackbaudidsso.com.test-google-a.com	Test domain alias	Active

blackbaudidsso.com

Registered since Jun 04, 2022 with **Google Domains**

- [Google Domains Terms of Service](#)
- [Registrant rights and responsibilities](#)
- [Google Workspace Domain Registration Terms of Service](#)

Autorenewal
This domain will automatically renew every year.

Manage your domain subscription
The person who registered this domain can visit Google Domains to edit advanced settings such as WHOIS or DNS records.

[MANAGE DOMAIN](#) (via Google Domains)

Cancel your domain subscription
Canceling your domain billing subscription will also turn off autorenewal for your domain.

[CANCEL DOMAIN BILLING SUBSCRIPTION](#)

Manage domain

The screenshot shows the Google Domains interface. On the left is a navigation sidebar with options: 'Get a new domain', 'My domains' (highlighted), 'Transfer', 'Billing', 'Account', 'Send feedback', 'Help and support', and 'United States (US \$)'. The main content area is titled 'My domains' and includes a 'Show bulk tools' link. A table lists the domain 'blackbaudidsso.com' with 'Google Workspace' services and an expiration date of 'Jun 4, 2023'. A 'Manage' link is positioned to the right of the expiration date, highlighted by a teal arrow. Below the table is a '+ Get a new domain' button. At the bottom, a status message reads: 'You're signed in as john.vogel@blackbaudidsso.com. Can't find your domain? [Get help](#)'.

Name	Services [?]	Expires/renews on
blackbaudidsso.com	Google Workspace	Jun 4, 2023 Manage

[+ Get a new domain](#)

You're signed in as **john.vogel@blackbaudidsso.com**. Can't find your domain? [Get help](#)

Go to DNS



The screenshot shows the Google Domains management interface for the domain **blackbauidssso.com**. The interface is divided into a left sidebar and a main content area.

Left Sidebar:

- Domain overview (highlighted)
- Registration settings
- DNS
- Website
- Reports
- Email
- Security
- Get a new domain
- Send feedback
- Help and support
- United States (US \$)

Main Content Area:

- SERVICES:** Google Workspace
- PRIVACY PROTECTION:** On (Info is private)
- Get online with Google:** A progress bar is shown. Tasks include:
 - Get a custom email with Workspace (checked)
 - Create a website (in progress). Description: "Build your no-code website with tools from Google at no charge, or connect your domain to services like Shopify, Squarespace, Weebly, Wix and Wordpress". Buttons: "Build website", "Mark as done".
 - Set up Google Search reporting

Enter DNS record details

The image consists of two side-by-side screenshots from a web application interface, likely for managing DNS records.

Left Screenshot: Claim email domains dialog

- Title:** Claim email domains
- Instruction:** Enter the domains you want to claim below
- Domain:** blackbaudidsso.com
- Action:** Add a custom record to your DNS configuration with the following
- Record Details:**
 - Name/Host/Alias: @
 - Record type: TXT
 - Time to live (TTL): 3600 (or 1 hour)
 - Value: [Redacted]
- Buttons:** Verify this domain (highlighted with a blue arrow labeled '2'), Copy, Close
- Status:** Verifying...
- Text:** This can take a few minutes or up to 2 days, but we'll email you as soon as we verify this domain. [Troubleshoot the issue.](#)
- Footer:** Claim another domain, You must verify your domains to begin testing your SSO connection


Right Screenshot: DNS configuration page

- Page Title:** DNS
- Domain:** blackbaudidsso.com
- Settings:** Global DNS settings
- Active Status:** Default name servers (Active) | Custom name servers
- Message:** These DNS settings are active. Changes are published immediately, but may take time to propagate
- Resource records:** Export DNS records
- Custom records:** No records added
- Record Form:**
 - Host name: @
 - Type: TXT
 - TTL: 3600
 - Data: [Redacted]
- Buttons:** Add more to this record, Create new record, Cancel, Save (highlighted with a blue arrow labeled '7')
- Footer:** Google Workspace


Email domain Verified

Claim email domains

Enter the domains you want to claim below [i](#)

blackbaudidsso.com	✓ Verified	<i>You may remove the TXT record from your DNS</i>	
--------------------	------------	--	---

[+ Claim another domain](#)

 *You cannot remove a domain that has active users*

[Close](#)

Test Connection

Admin Home Users and admins Billing Authentication Settings

you complete or erase this configuration.

Google G Suite configuration

Invite another admin to configure your connection

- ✓ 1 - Configure your connection
[Edit connection](#)
- ✓ 2 - Claim your email domains
blackbaudidsso.com [View Blackbaud IDs](#)
[Edit claimed domains](#)
- ✓ 3 - Test connection
Open this Test mode URL in a private/incognito browser window
<https://signin.blackbaud.com/signin/?loginTest=true>
[Copy](#)
(0 Blackbaud IDs currently in Test mode)
- 4 - Turn on
⚠ You must have at least one successful sign in to Test mode before you can activate this connection

blackbaud

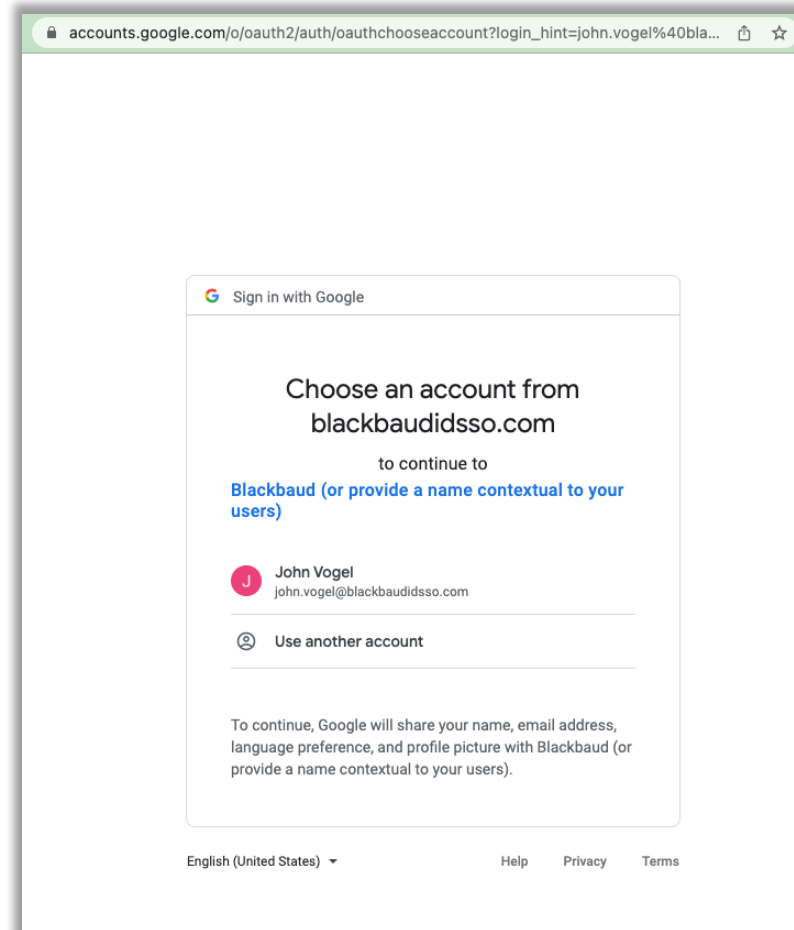
Sign in

Email address
john.vogel@blackbaudidsso.com

[Continue](#)

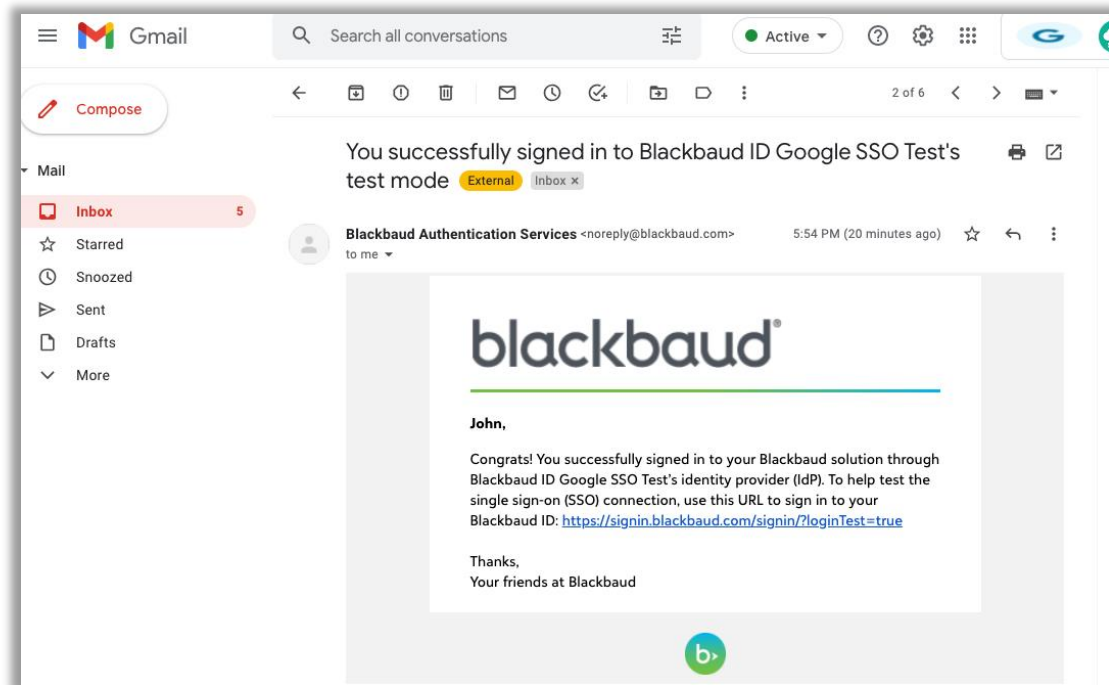
[Need help?](#)

Select and authenticate with your Google account

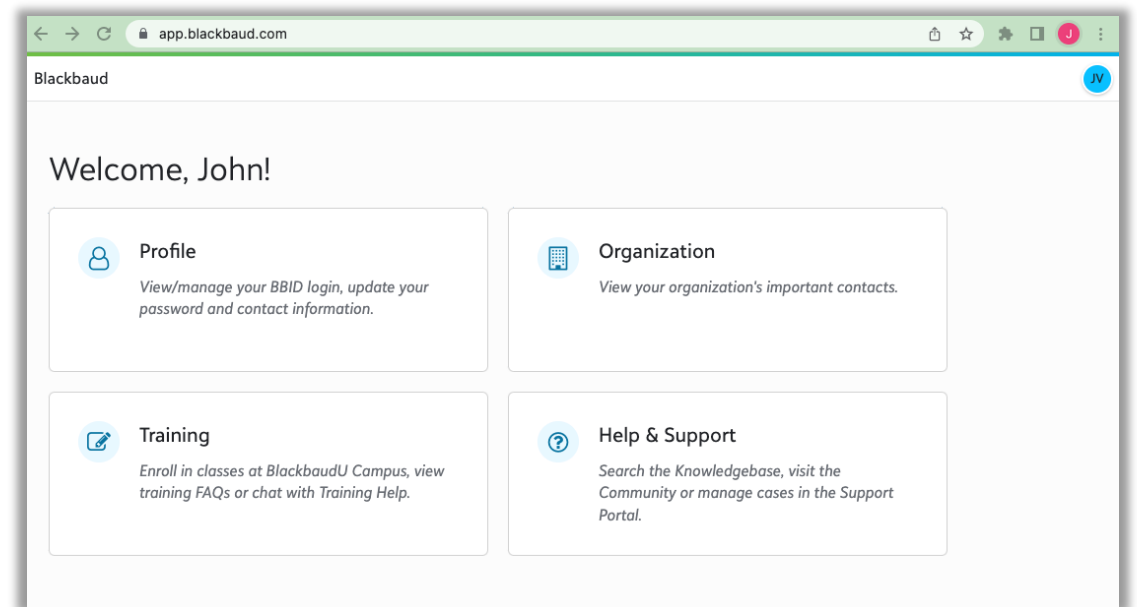


Test connection successful!

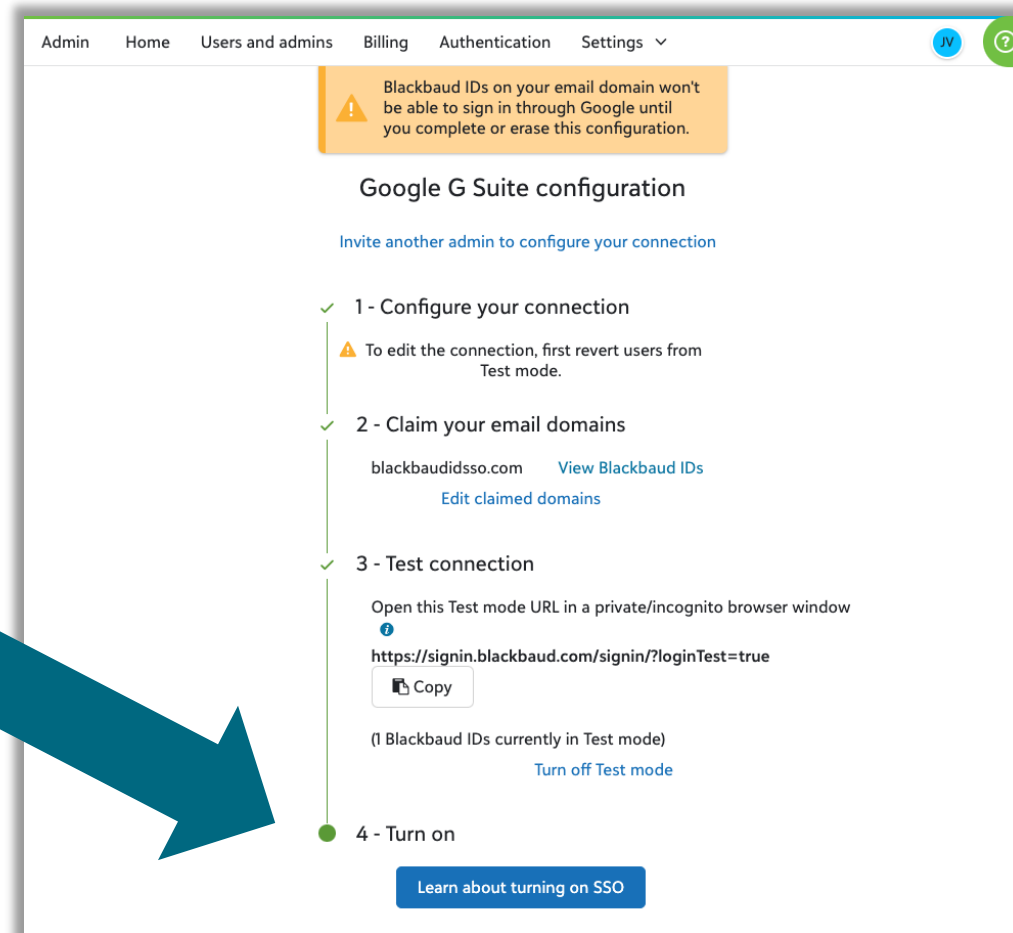
EMAIL CONFIRMING SIGN IN



WELCOME PAGE AFTER SIGNING IN



Turn on SSO



The screenshot shows the Blackbaud admin interface with a navigation bar at the top containing 'Admin', 'Home', 'Users and admins', 'Billing', 'Authentication', and 'Settings'. A warning message at the top states: 'Blackbaud IDs on your email domain won't be able to sign in through Google until you complete or erase this configuration.' The main content area is titled 'Google G Suite configuration' and includes a link to 'Invite another admin to configure your connection'. A progress indicator shows four steps: 1 - Configure your connection (completed), 2 - Claim your email domains (completed), 3 - Test connection (completed), and 4 - Turn on (in progress). Step 2 shows the domain 'blackbaudidsso.com' with links for 'View Blackbaud IDs' and 'Edit claimed domains'. Step 3 provides a test mode URL: 'https://signin.blackbaud.com/signin?!loginTest=true' with a 'Copy' button. Step 4 is currently selected, and a large blue arrow points to it from the left. A 'Learn about turning on SSO' button is located at the bottom of the configuration area.

Admin Home Users and admins Billing Authentication Settings

Blackbaud IDs on your email domain won't be able to sign in through Google until you complete or erase this configuration.

Google G Suite configuration

[Invite another admin to configure your connection](#)

- 1 - Configure your connection
 - To edit the connection, first revert users from Test mode.
- 2 - Claim your email domains
 - blackbaudidsso.com [View Blackbaud IDs](#)
 - [Edit claimed domains](#)
- 3 - Test connection
 - Open this Test mode URL in a private/incognito browser window
 - <https://signin.blackbaud.com/signin?!loginTest=true>
 - [Copy](#)
 - (1 Blackbaud IDs currently in Test mode)
 - [Turn off Test mode](#)
- 4 - Turn on

[Learn about turning on SSO](#)

Confirm any impact & Connect SSO

Connect your Google G Suite SSO



Ready to make the switch? When you connect with Google G Suite:

- Anyone who signs in with a Blackbaud ID that includes one of your verified domains will automatically redirect to your identity provider (IdP), like those currently in Test mode.
 - [View the Blackbaud IDs using @blackbaudidssso.com](#)
- When your IdP authenticates a Blackbaud ID, that ID will then use your Google G Suite connection to manage passwords, lockouts, and other security features.

- Automatically send members an email from Blackbaud informing them of the change

Connect with Google G Suite

Cancel

Blackbaud IDs

These Blackbaud IDs all signed in with your domain in their email address at some point.

Any changes to your SSO settings affect these users. To notify them of changes, you can copy and paste this list as email recipients.

(Showing up to 1,000)

Copy all to clipboard

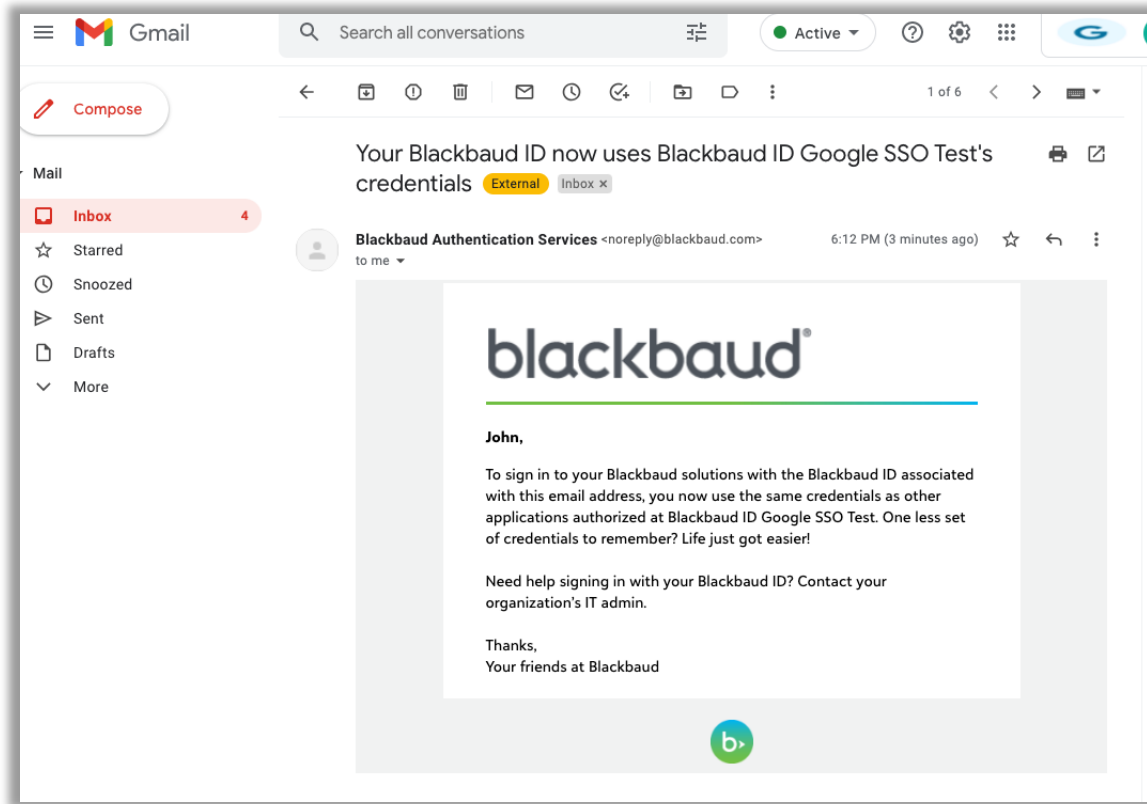
john.vogel@blackbaudidssso.com

Close

2

1

Confirmation email



Sent to users that previously had a Blackbaud ID on the claimed domain(s) used with the SSO connection

Completed connection page

The screenshot shows a web interface for configuring a single sign-on connection. The navigation bar at the top includes 'Admin', 'Home', 'Users and admins', 'Billing', 'Authentication', and 'Settings'. The main heading is 'Single sign-on with Google G Suite' for the connection 'Blackbaud ID Google SSO Test'. A green checkmark indicates the connection is active. Below this, there are links for 'Edit display name' and 'Update client secret'. A secondary section offers to 'Invite another admin to configure your connection' and provides a link to 'Learn about disconnecting SSO'. The interface is divided into three main panels: 'Connection details' showing the connection name 'blackbauidssso-com' and a redacted client ID; 'Redirect settings' with a note that links will redirect users to the sign-in URL; and 'Claimed email domains' with an 'Edit claimed domains' button and a list of domains including 'blackbauidssso.com' with a 'View Blackbaud IDs' link.

Admin Home Users and admins Billing Authentication Settings

Single sign-on with Google G Suite

Blackbaud ID Google SSO Test

[Back to Authentication settings](#)

✔ Blackbaud ID Google SSO Test
[Edit display name](#) [Update client secret](#)

[Invite another admin to configure your connection](#) [Learn about disconnecting SSO](#)

Connection details

Connection name blackbauidssso-com
Client ID [REDACTED]

Redirect settings

These links will redirect your users directly to your sign in URL.

Claimed email domains

[Edit claimed domains](#)

Users with Blackbaud IDs using these email domains will be redirected to your Google G Suite sign in

blackbauidssso.com [View Blackbaud IDs](#)

blackbaud[®]



Thank you

john.vogel@blackbaud.com





Disconnecting SSO

Disconnecting SSO

The screenshot shows the 'Single sign-on with Google G Suite' configuration page for 'Blackbaud ID Google SSO Test'. The navigation bar includes 'Admin', 'Home', 'Users and admins', 'Billing', 'Authentication', and 'Settings'. The main content area features a green checkmark next to the connection name, an 'Update client secret' link, and a callout box with the text 'Learn about disconnecting SSO'. A large teal arrow points from the bottom left towards the callout box. Below the main content are two expandable sections: 'Connection details' (showing 'blackbauidssso-com') and 'Redirect settings'.

Admin Home Users and admins Billing Authentication Settings ▾

Single sign-on with Google G Suite

Blackbaud ID Google SSO Test

[Back to Authentication settings](#)

✔ Blackbaud ID Google SSO Test
[Edit display name](#) ⓘ

[Update client secret](#)

Invite another admin to configure your connection

Learn about disconnecting SSO

Connection details

Connection name blackbauidssso-com

Redirect settings

These links will redirect your users

Disconnecting SSO

Admin Home Users and admins B

Single sign-on with Google G Suite

[Back to Authentication settings](#)

✔ Blackbaud ID Google SSO Test
[Edit display name](#) ⓘ

Invite another admin to configure your connection

Connection details

Connection name blackbauidss-co
Client ID

Disconnect Google G Suite

⚠ When you disconnect your connection, members will sign in to their Blackbaud IDs using Blackbaud's secure authentication service instead of Google G Suite.

In addition:

- Members can still connect to Google G Suite through your Test mode URL.
- Your claimed email domains remain verified.
- No members can sign in to their Blackbaud IDs through Google until you erase or reconnect the G Suite connection.

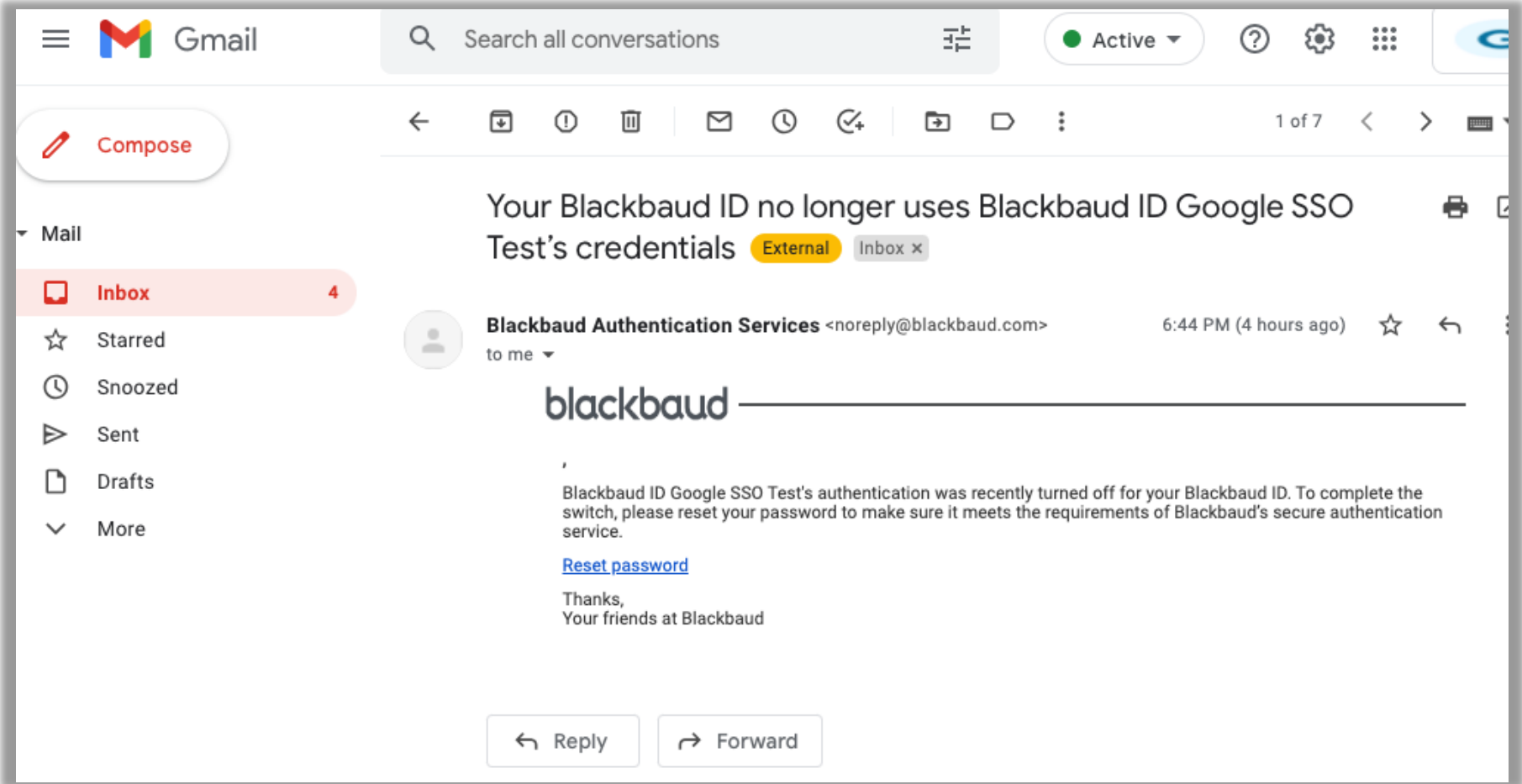
Yes, disconnect the Google G Suite connection

Automatically send members an email from Blackbaud to reset their Blackbaud ID passwords

[Disconnect Google G Suite](#) [Cancel](#)

directly to your

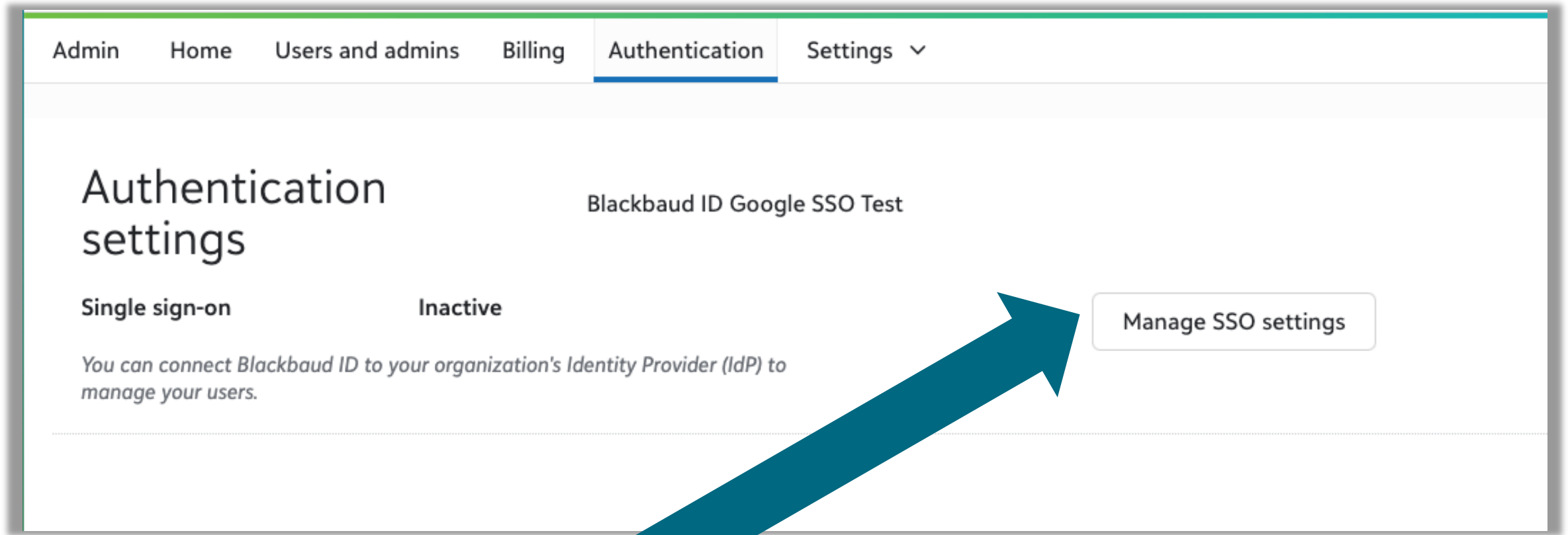
Disconnection Email to Users



The background features several decorative geometric shapes. In the top-left corner, there is a large cyan rounded square with a white outline of a diamond inside it. Below it is a smaller purple-to-cyan gradient diamond. In the bottom-left, there is a cyan rounded square and a purple-to-cyan gradient diamond. In the bottom-right, there is a large cyan rounded square with a green rounded square overlapping its top-left corner, and a white outline of a triangle pointing upwards. The text "Google SSO using SAML" is centered in white.

Google SSO using SAML

Blackbaud Admin




The screenshot shows the Blackbaud Admin interface. At the top is a navigation bar with the following items: Admin, Home, Users and admins, Billing, Authentication (which is underlined and highlighted with a blue bar), and Settings with a dropdown arrow. Below the navigation bar, the main content area is titled "Authentication settings" on the left and "Blackbaud ID Google SSO Test" on the right. Under "Authentication settings", the text "Single sign-on" is followed by "Inactive". Below this, a descriptive sentence reads: "You can connect Blackbaud ID to your organization's Identity Provider (IdP) to manage your users." On the right side of the page, there is a button labeled "Manage SSO settings". A large teal arrow points from the bottom center towards this button.

Single sign-on

Blackbaud ID Google SSO Test


[Back to Authentication settings](#)


To use your organization's identity provider with Blackbaud IDs, enable single sign-on (SSO). You can manage access to Blackbaud solutions and enable your users to sign in with the same credentials that they use for other solutions. For more information, see our [resources for managing SSO with Blackbaud ID](#).

 **Azure AD**
Connect using your Azure Active Directory.

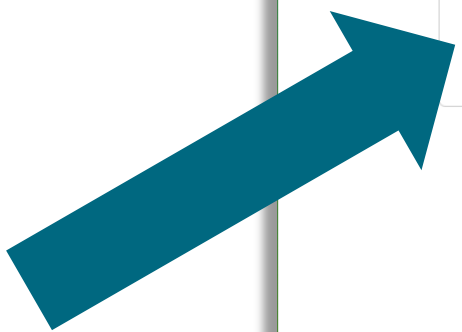
 **Google G Suite**
Connect using your Google G Suite.

 **SAML 2.0**
Connect using Security Assertion Markup Language.

 **ADFS**
Connect using your Active Directory Federation Services.

 **Okta**
Connect using your Okta identity management.

If you're not the right person to set up SSO, [invite another admin to configure your connection](#).



Configure your connection

Admin Home Users and admins Billing Authentication Settings ▾

Blackbaud ID

Single sign-on

Blackbaud ID Google SSO Test

[Back to Authentication settings](#)

SAML 2.0 configuration

[Invite another admin to configure your connection](#)

- 1 - Configure your connection
- 2 - Configure your identity provider (IdP)
- 3 - Claim your email domains
- 4 - Test connection
- 5 - Turn on

[Get started!](#)

[Cancel](#)

Enter your organization name to be used

Admin

Single

Back to Auth

Configure SAML 2.0 connection

Enter your connection details

Organization name *

Blackbaud-ID-Google-SSO-Test

Organization name must start and end with an alphanumeric character and can only contain alphanumeric characters and '-'.

SAML sign in URL *

https://yourDomain.org/idp/profile/SAML2/Redirect/SSO

IdP initiated SSO URL

https://www.blackbaud.com

JV

gle SSO

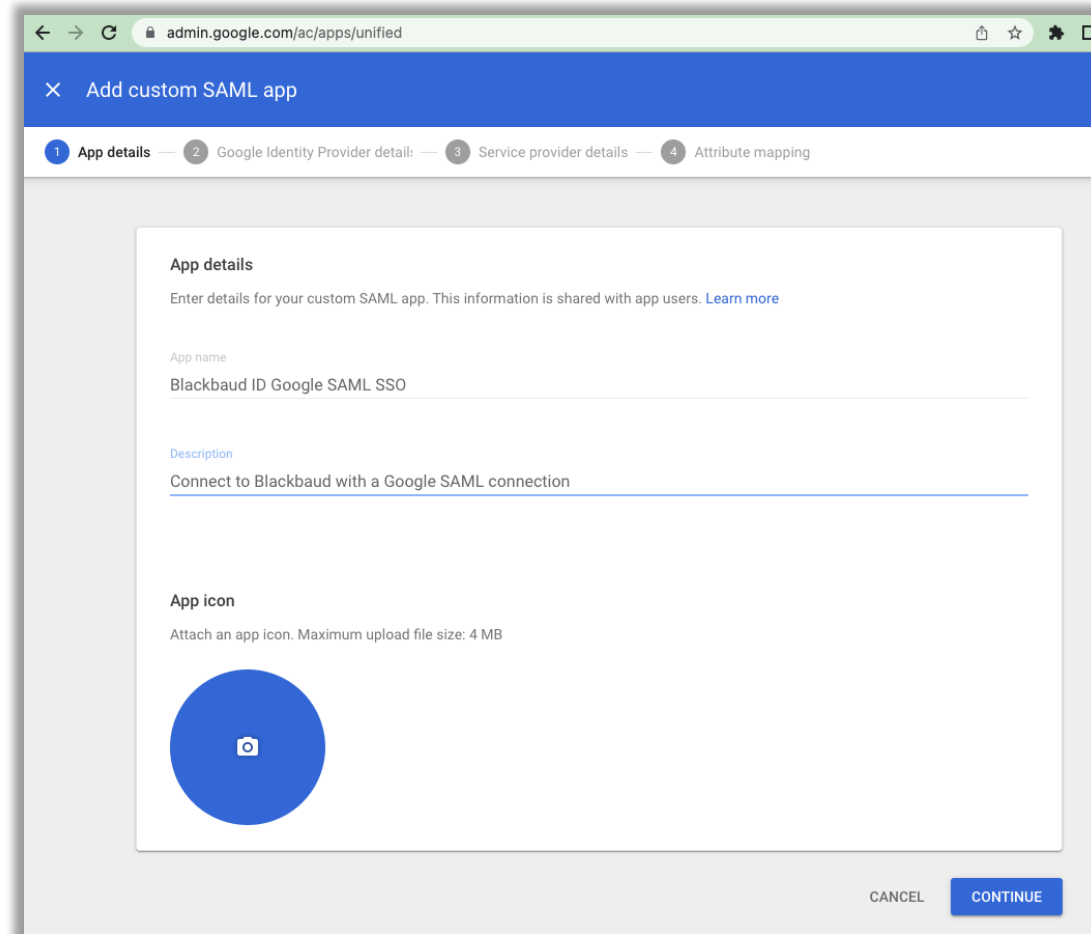
Add a custom SAML App in Google Admin

The image shows a two-step process for adding a custom SAML app in Google Admin. Step 1 is indicated by a blue arrow pointing from the 'Web and mobile apps' menu item in the left-hand navigation pane to the 'Add app' button in the main content area. Step 2 is indicated by another blue arrow pointing from the 'Add app' button to the 'Add custom SAML app' option in the dropdown menu that appears.

1

2

Enter App details



The screenshot shows a web browser window at `admin.google.com/ac/apps/unified`. The page title is "Add custom SAML app". A progress bar at the top indicates four steps: 1. App details (active), 2. Google Identity Provider detail, 3. Service provider details, and 4. Attribute mapping.

App details
Enter details for your custom SAML app. This information is shared with app users. [Learn more](#)

App name
Blackbaud ID Google SAML SSO

Description
Connect to Blackbaud with a Google SAML connection

App icon
Attach an app icon. Maximum upload file size: 4 MB

A large blue circular button with a camera icon is positioned below the icon instructions.

CANCEL CONTINUE

Copy over Sign in URL and attach certificate

The image shows two side-by-side screenshots of web interfaces for configuring SAML 2.0 connections. The left interface is titled "Configure SAML 2.0 connection" and the right is "Add custom SAML app".

Left Interface: Configure SAML 2.0 connection

- Enter your connection details**
 - Organization name: Blackbaud-ID-Google-SSO-Test
 - SAML sign in URL: `https://accounts.google.com/o/saml2/idp?idpid=` [redacted]
 - IdP initiated SSO URL: `app.blackbaud.com`
 - Signing certificate (pem or .cer file): `Google_2027-6-3-115042_SAML2_0.pem`
- Confirm how your IdP identifies the user**
 - NameID: `e.g. "NameID" or "urn:oid:2.5.52.1"`
 - Email address: `e.g. "email" or "urn:oid:2.5.52.1"`
 - First name: `e.g. "firstname" or "urn:oid:2.5.52.1"`
 - Last name: `e.g. "lastname" or "urn:oid:2.5.52.1"`

Right Interface: Add custom SAML app

- Option 1: Download IdP metadata**
 - DOWNLOAD METADATA
- Option 2: Copy and paste IdP metadata**
 - SSO URL: `https://accounts.google.com/o/saml2/idp?idpid=` [redacted]
 - Entity ID: `https://accounts.google.com/o/saml2?idpid=` [redacted]
 - Certificate: `Google_2027-6-3-115042_SAML2_0` Expires Jun 3, 2027. Includes a "BEGIN CERTIFICATE" block with redacted content.
 - SHA-256 fingerprint: [redacted]

Teal arrows indicate the following data flow:

- From the SSO URL field in Option 2 to the SAML sign in URL field in the left interface.
- From the Certificate field in Option 2 to the Signing certificate field in the left interface.
- From the Certificate field in Option 2 to the file name field in the left interface.

Enter the mappings as detailed in help

Configure SAML 2.0 connection

Organization name *
Blackbaud-ID-Google-SSO-Test
Organization name must start and end with an alphanumeric character and can only contain alphanumeric characters and '-':

SAML sign in URL *
https://accounts.google.com/o/saml2/idp?idpid=C03m0b4se

IdP initiated SSO URL
app.blackbaud.com

Signing certificate (.pem or .cer file) *
Choose file Google_2027-6-3-115042_SAML2_0.pem

Confirm how your IdP identifies the following:

NameID *
emailAddress

Email address *
emailAddress

First name
given_name

Last name
sur_name

Save Cancel

f. Under **Signing certificate**, select **Choose file**, and then browse to and select the certificate (CER) file downloaded from your *Google* IdP information.

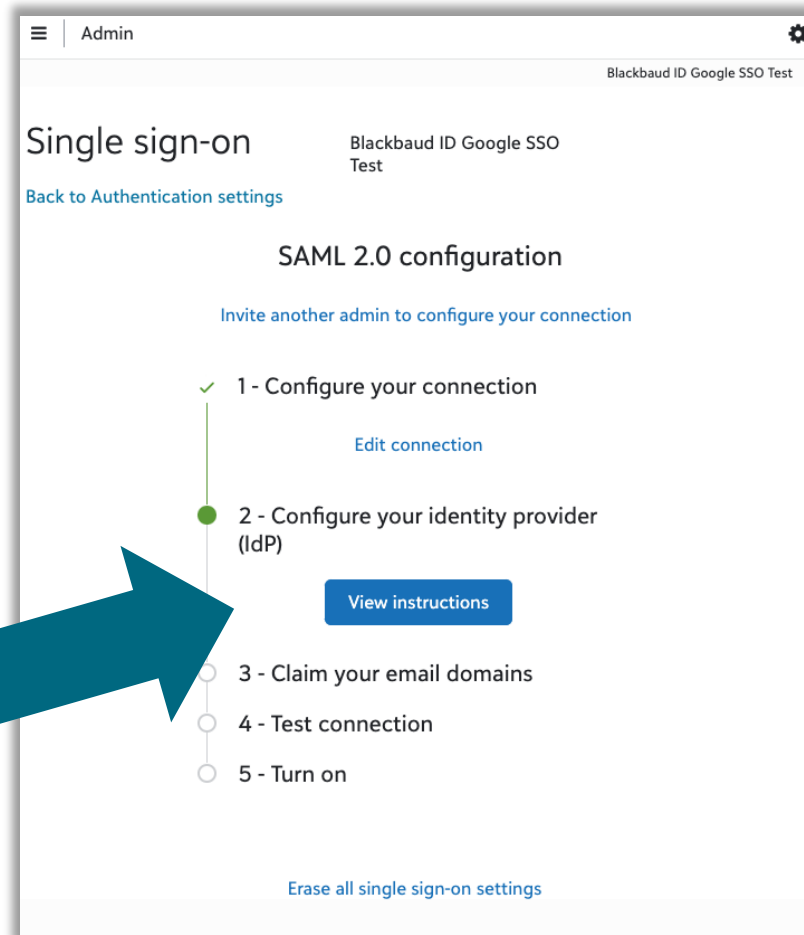
g. Enter the attributes *Google* will use to permanently identify member details:

- In the **NameID** and **Email address** fields, enter emailAddress.
- In the **First name** field, enter given_name.
- In the **Last name** field, enter sur_name.

Note: You'll create these attributes when you configure your *Google* IdP.

h. Select **Save**.

Configure IdP



The screenshot shows the 'Admin' interface for 'Blackbaud ID Google SSO Test'. The main heading is 'Single sign-on' with a sub-heading 'SAML 2.0 configuration'. A link 'Back to Authentication settings' is visible. Below the heading, there is a progress indicator with five steps: 1 - Configure your connection (completed), 2 - Configure your identity provider (IdP) (current step), 3 - Claim your email domains, 4 - Test connection, and 5 - Turn on. A large teal arrow points to step 2. A 'View instructions' button is located next to step 2. At the bottom, there is a link 'Erase all single sign-on settings'.

Admin | Blackbaud ID Google SSO Test

Single sign-on

Blackbaud ID Google SSO Test

[Back to Authentication settings](#)

SAML 2.0 configuration

[Invite another admin to configure your connection](#)

- ✓ 1 - Configure your connection
[Edit connection](#)
- 2 - Configure your identity provider (IdP)
[View instructions](#)
- 3 - Claim your email domains
- 4 - Test connection
- 5 - Turn on

[Erase all single sign-on settings](#)

Provide Blackbaud details to Google

Configure SAML 2.0 IdP

If your IdP supports metadata uploads:
Download this metadata file and upload it to your IdP
[Blackbaud SAML metadata file](#)

If your IdP requires manual configuration:
Set **Assertion Consumer Service URL** or **Application Callback URL** to
[Redacted]

If requested, set **Audience** or **Entity ID** to
[Redacted]

If requested, set **Request bindings** to
HTTP-Redirect for Authentication Requests

If requested, set **Response bindings** to
HTTP-Post for Authentication Assertions

[Erase all single sign-on settings](#)

Add custom SAML app

✓ App details — ✓ Google Identity Provider detail: — 3 Service provider details — 4 Attribute mapping

Service provider details
To configure single sign on, add service provider details such as ACS URL and entity ID. [Learn more](#)

ACS URL
[Redacted]

Entity ID
[Redacted]

Start URL (optional)

Signed response

Name ID
Defines the naming format supported by the identity provider. [Learn more](#)

Name ID format
UNSPECIFIED

Name ID
Basic Information > Primary email

Finish app setup

✕ Add custom SAML app

✓ App details — ✓ Google Identity Provider detail: — ✓ Service provider details — 4 Attribute mapping

Attributes

Add and select user fields in Google Directory, then map them to service provider attributes. Attributes marked with * are mandatory. [Learn more](#)


Google Directory attributes	App attributes
<input type="button" value="ADD MAPPING"/>	

Group membership (optional)

Group membership information can be sent in the SAML response if the user belongs to any of the groups you add here.

Google groups	App attribute
Search for a group	Groups

BACK CANCEL



Turn User access ON for everyone

The screenshot shows the Google Admin console interface. At the top, there is a blue header with the 'Google Admin' logo, a search bar, and various utility icons. The main content area is titled 'Apps > Web and mobile apps > Blackbaud ID Google SAML SSO'. On the left, there is a sidebar with navigation icons. The main content is divided into sections: 'SAML', 'Blackbaud ID Google SAML SSO', 'User access', 'Service provider details', and 'Certificate'. The 'User access' section is currently selected and shows the status 'OFF for everyone'. A large teal arrow points from this status to a modal dialog that is open. The modal dialog has a title 'Service status' and contains two radio button options: 'ON for everyone' (which is selected) and 'OFF for everyone'. Below these options is an information icon and a note: 'Most changes take effect in a few minutes. Learn more'. At the bottom of the modal, there is a footer with '1 unsaved change', 'CANCEL', and 'SAVE' buttons.

Claim email domain

The remainder of the setup is the same as the Google application setup shown earlier in this presentation. Reference Slide 32 to continue.

Single sign-on Blackbaud ID Google SSO Test

[Back to Authentication settings](#)

SAML 2.0 configuration

[Invite another admin to configure your connection](#)

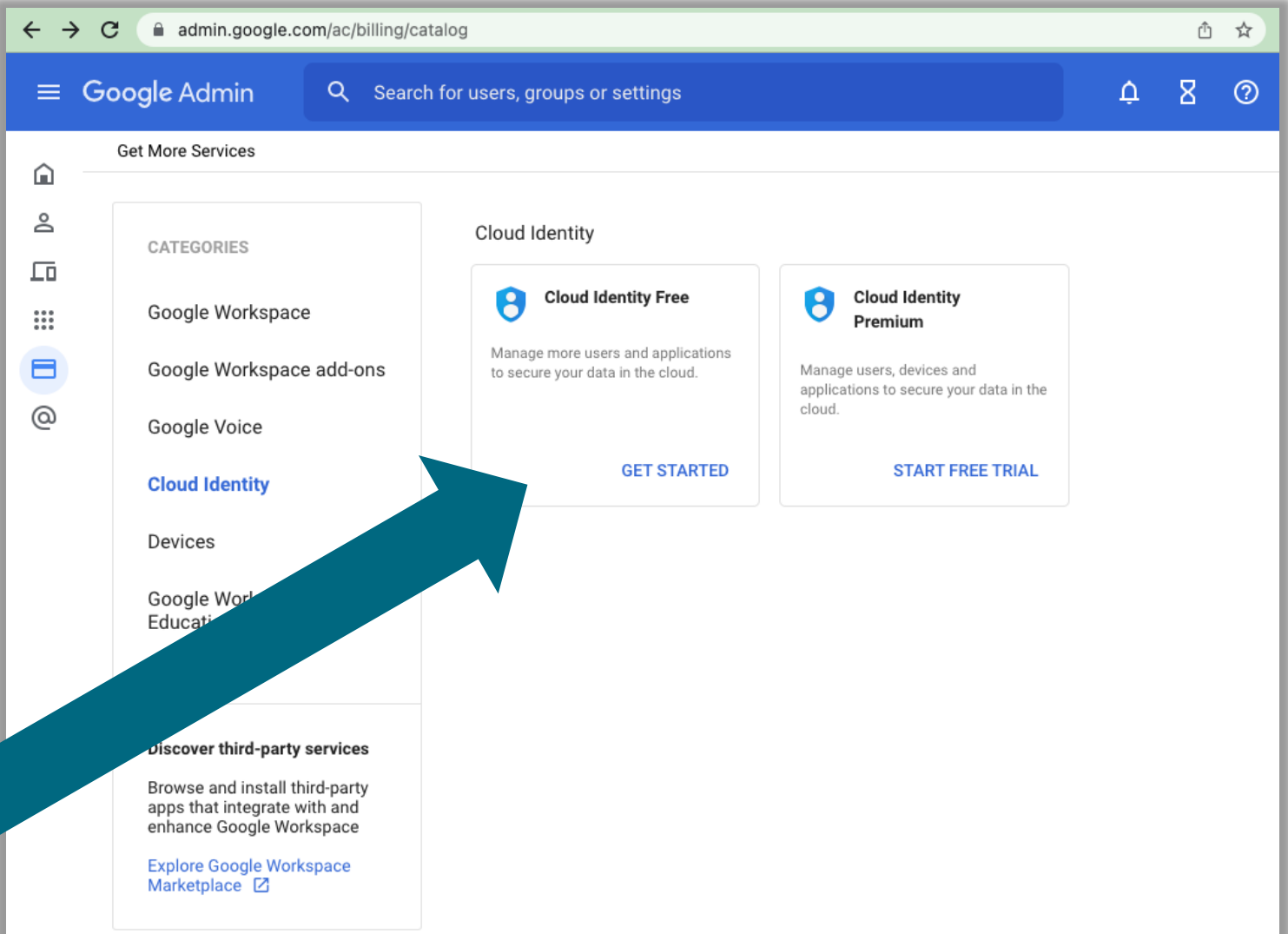
- ✓ 1 - Configure your connection [Edit connection](#)
- ➔ 2 - Claim your email domains [Claim domains](#)
- 3 - Test connection
- 4 - Turn on

[Erase all single sign-on settings](#)



Appendix

Consider Cloud Identity



The screenshot shows the Google Admin console interface. The browser address bar displays `admin.google.com/ac/billing/catalog`. The top navigation bar includes the Google Admin logo, a search bar with the placeholder text "Search for users, groups or settings", and notification, refresh, and help icons. The main content area is titled "Get More Services" and features a left-hand sidebar with a "CATEGORIES" list. The "Cloud Identity" category is highlighted in blue. The main content area displays two service cards under the heading "Cloud Identity": "Cloud Identity Free" and "Cloud Identity Premium". The "Cloud Identity Free" card includes the text "Manage more users and applications to secure your data in the cloud." and a "GET STARTED" button. The "Cloud Identity Premium" card includes the text "Manage users, devices and applications to secure your data in the cloud." and a "START FREE TRIAL" button. A large teal arrow points from the bottom-left towards the "Cloud Identity Free" card.

admin.google.com/ac/billing/catalog

Google Admin Search for users, groups or settings

Get More Services

CATEGORIES

- Google Workspace
- Google Workspace add-ons
- Google Voice
- Cloud Identity**
- Devices
- Google Work
- Educati

Discover third-party services

Browse and install third-party apps that integrate with and enhance Google Workspace

[Explore Google Workspace Marketplace](#)

Cloud Identity

- Cloud Identity Free**
Manage more users and applications to secure your data in the cloud.
[GET STARTED](#)
- Cloud Identity Premium**
Manage users, devices and applications to secure your data in the cloud.
[START FREE TRIAL](#)