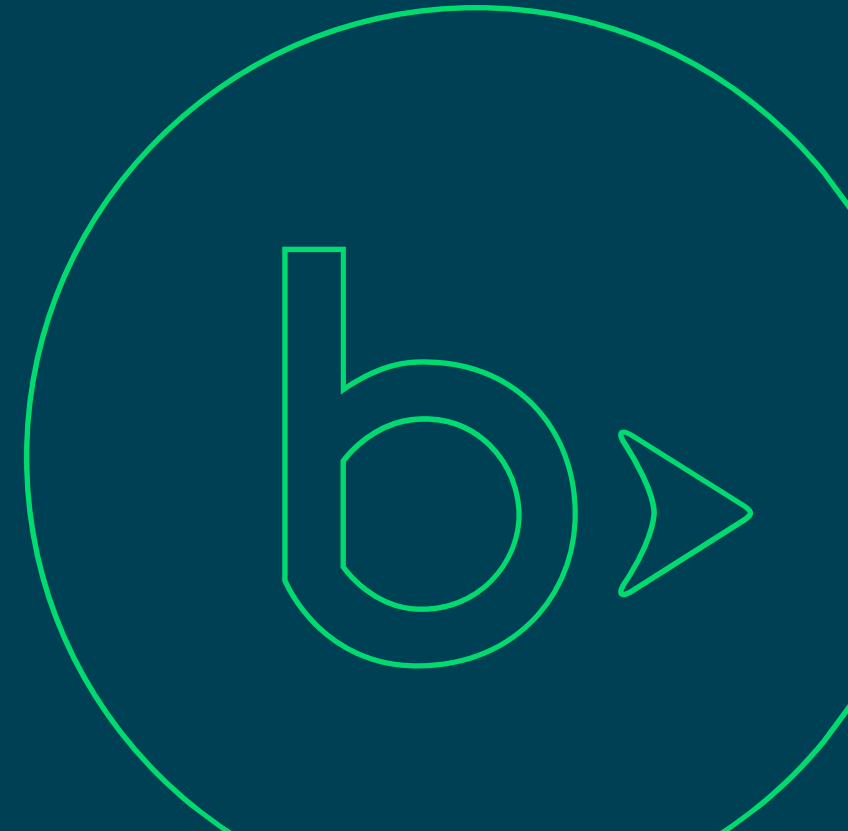


blackbaud®

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

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

John Vogel
Senior Technical Product Manager





John Vogel

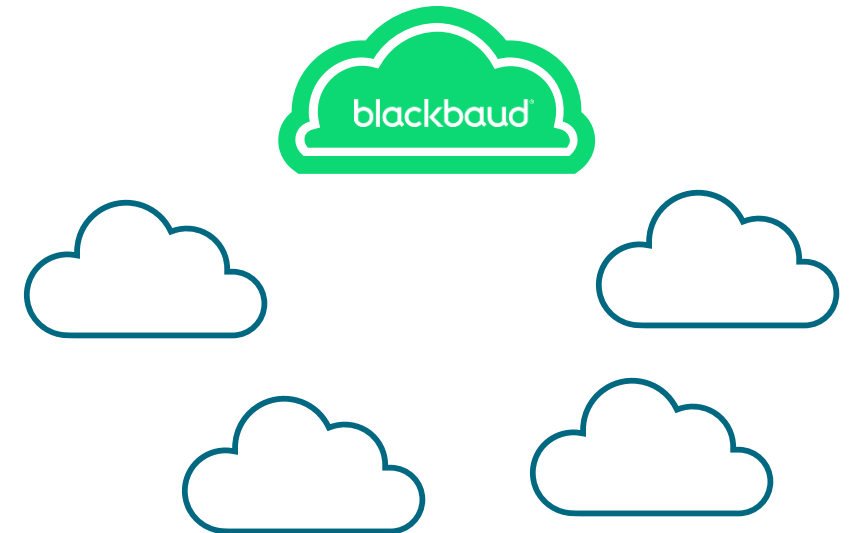
Senior Technical Product Manager

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

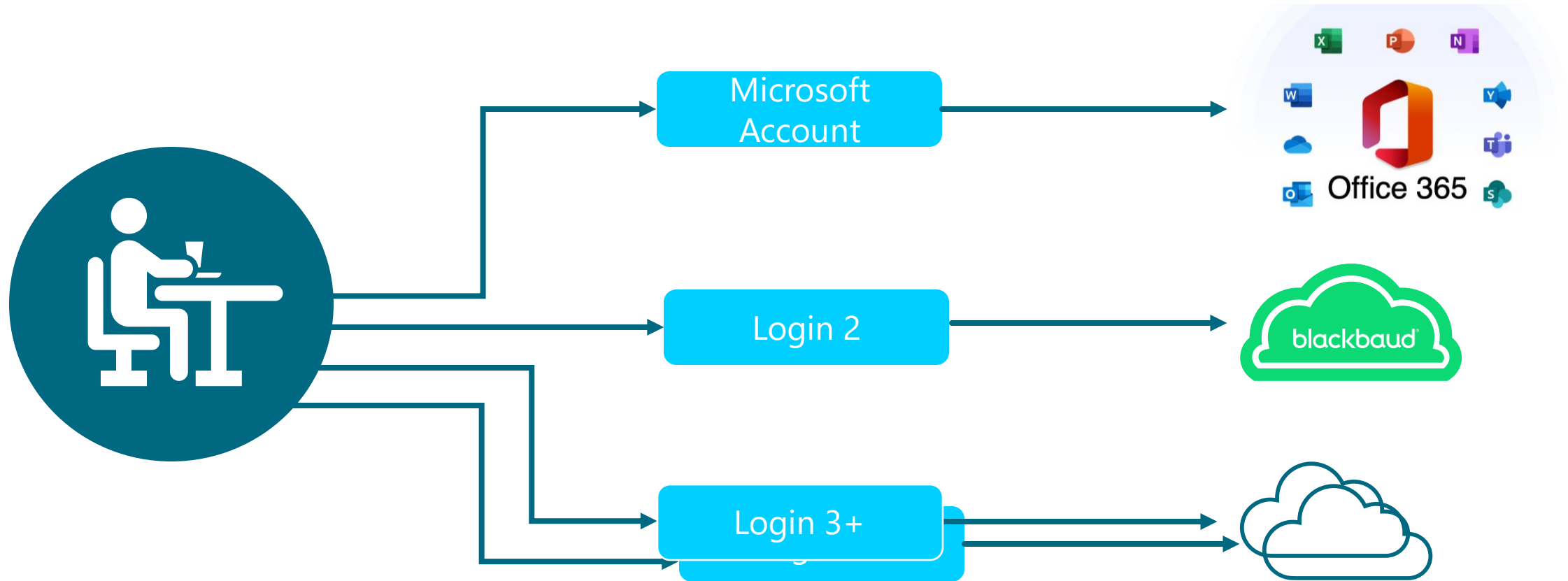
You're here because you regularly sign in to...



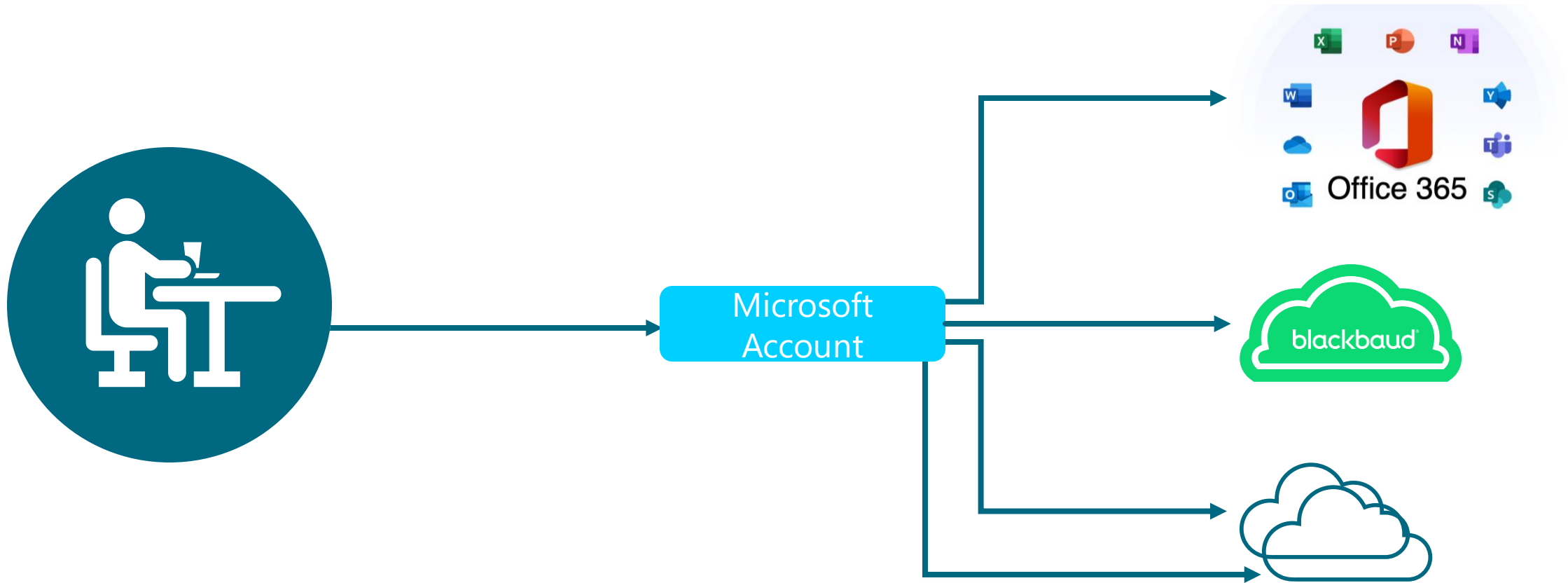
Other Business Applications



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
- **Azure Portal Admin** – to configure the connection within Azure
- **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.

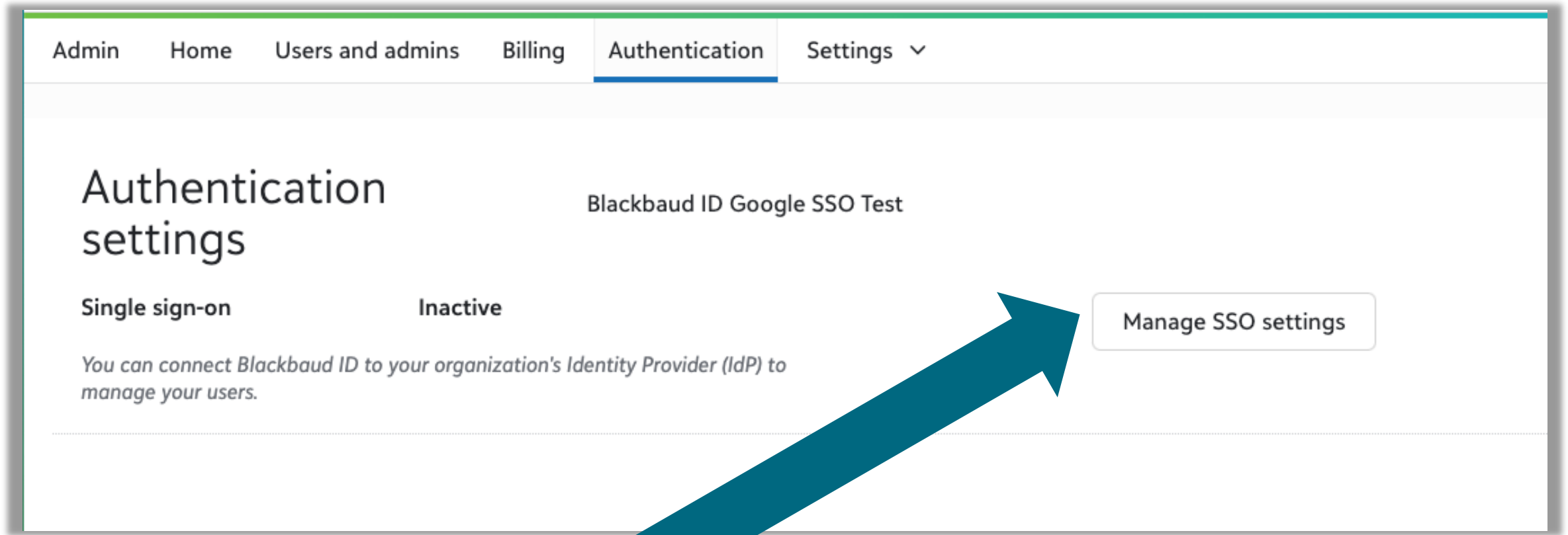
So...

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.

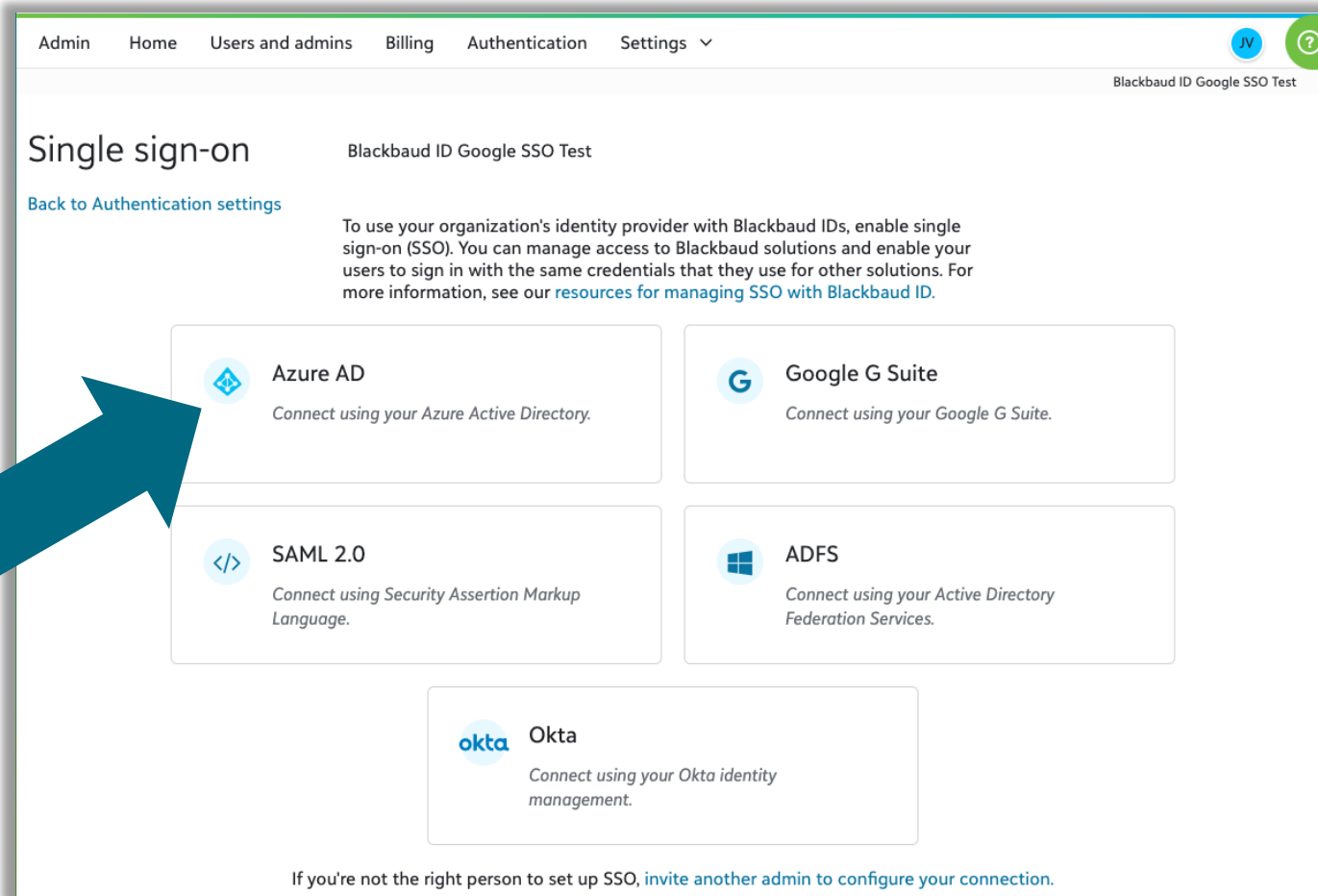
Azure SSO by Creating an Application

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 highlighted with a blue underline), and Settings with a dropdown arrow. The main content area is titled 'Authentication settings' and includes a sub-section for 'Blackbaud ID Google SSO Test'. Below this, it shows 'Single sign-on' is currently 'Inactive'. A teal arrow points from the bottom left towards a button labeled 'Manage SSO settings' on the right side of the page. Below the main heading, there is a descriptive paragraph: 'You can connect Blackbaud ID to your organization's Identity Provider (IdP) to manage your users.'

Select Azure AD



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 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

The screenshot shows the 'Single sign-on' configuration page for 'Jackie's LE'. The navigation bar at the top includes 'Admin', 'Home', 'Users and admins', 'Billing', 'Authentication', and 'Settings'. The page title is 'Single sign-on' with a sub-header 'Jackie's LE'. A link 'Back to Authentication settings' is visible. The main heading is 'Azure AD configuration', followed by the instruction 'Invite another admin to configure your connection'. A progress indicator shows four steps: '1 - Configure your connection' (active), '2 - Add your email domains', '3 - Test connection', and '4 - Turn on'. A blue 'Get started!' button is positioned next to the first step. A large teal arrow points to this button. A 'Cancel' link is located at the bottom of the page.

Admin | Home | Users and admins | Billing | Authentication | Settings

Jackie's LE

Single sign-on

Jackie's LE

[Back to Authentication settings](#)

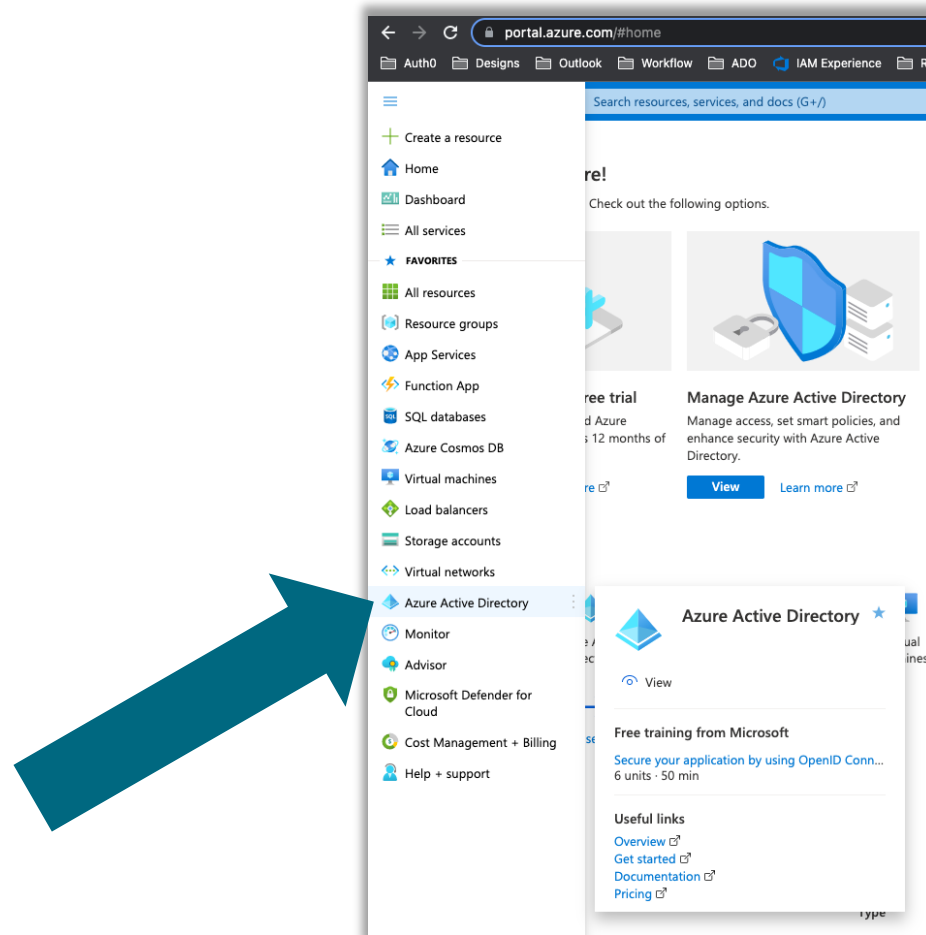
Azure AD configuration

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

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

[Cancel](#)

Sign in to Azure Portal and navigate to Azure AD



<https://portal.azure.com/#home>

Enter your primary Azure AD domain

Configure Azure AD application

- In a separate browser tab, sign in to [your Azure portal](#)
- Enter your primary Azure AD domain. *
- In the Azure portal, create an app registration with the redirect URI *
- Enter your application's ID. *
- In the Azure portal, edit the API permissions for your application to turn on the **User.Read** permission.
- In the Azure portal, create a secret key to secure your application's credentials when requesting tokens. Enter the secret key. *

blackbaudid.onmicrosoft.com

https://blackbaudinc.auth0.com/login/callback

XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX

Finish Cancel

Microsoft Azure Search resources, services, and docs (G+)

Home > Blackbaud-ID

Blackbaud-ID | Custom domain names

Azure Active Directory

+ Add custom domain Refresh Troubleshoot Columns Got feedback?

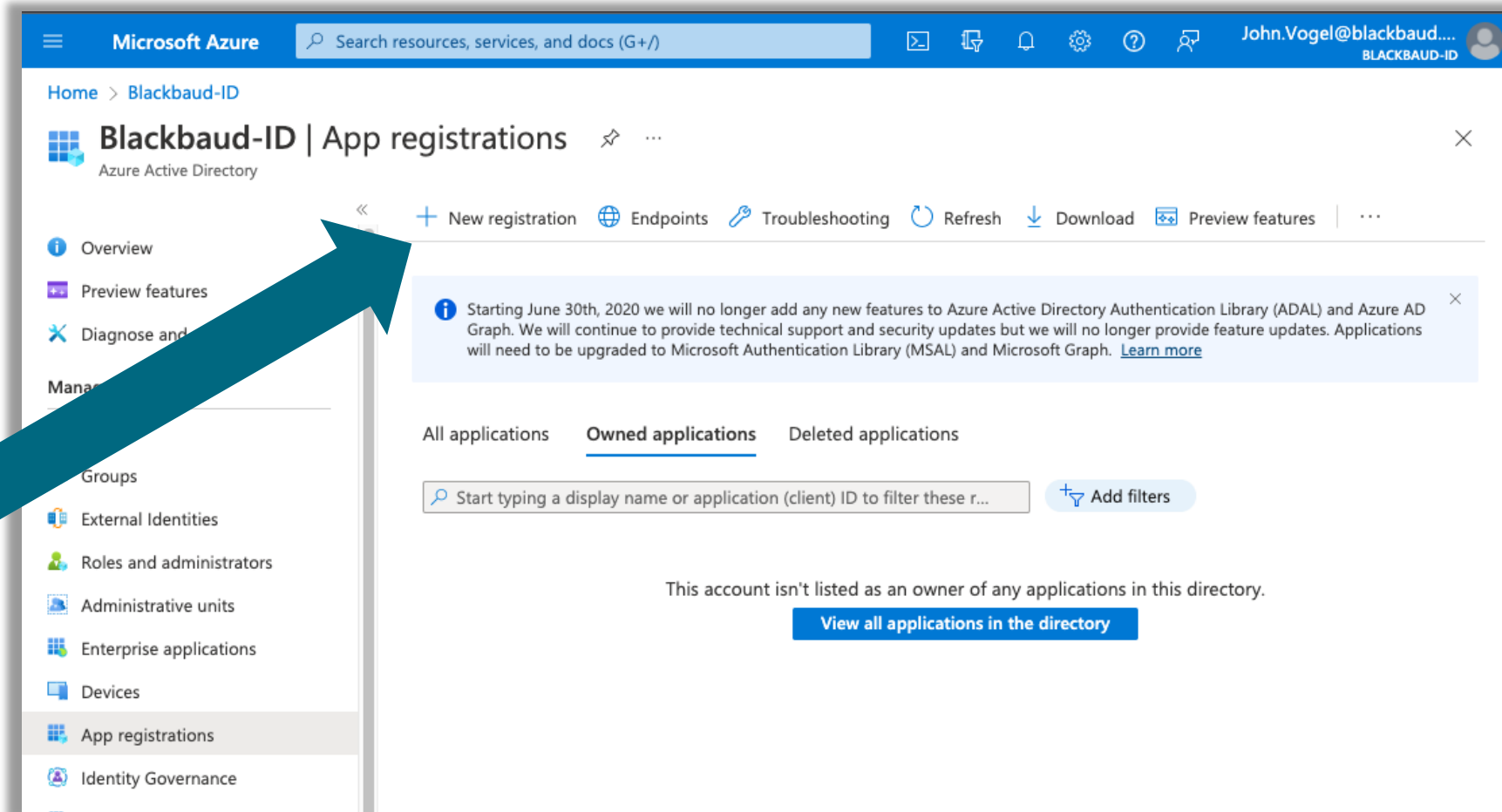
Looking to move an on-premises application to the cloud and use Azure Active Directory Domain Services?

Search domains Add filters

Name	Status	Federated	Primary
blackbaudid.com	Verified		
blackbaudid.onmicrosoft.com	Available		✓
blackbaudirest.com	Unverified		



Register new app



The screenshot displays the Microsoft Azure portal interface for the 'Blackbaud-ID' tenant. The top navigation bar includes the 'Microsoft Azure' logo, a search bar, and the user profile 'John.Vogel@blackbaud...'. The main content area is titled 'Blackbaud-ID | App registrations' and features a left-hand navigation pane with options like 'Overview', 'Preview features', and 'App registrations'. A large teal arrow points to the '+ New registration' button in the top action bar. Below this, a notification banner states that starting June 30th, 2020, new features will not be added to ADAL and Azure AD Graph. The main content area shows tabs for 'All applications', 'Owned applications', and 'Deleted applications', with a search bar and 'Add filters' button. A message at the bottom indicates that the current account is not listed as an owner of any applications, with a button to 'View all applications in the directory'.

Copy redirect URI and Register app

The image shows a screenshot of the Microsoft Azure portal. On the left, a modal dialog titled "Configure Azure AD application" is open. It contains the following steps:

1. In a separate browser tab, sign in to [your Azure portal](#)
2. Enter your primary Azure AD domain. *
3. In the Azure portal, create an app registration with the redirect URI *
 Copy
4. Enter your application's ID. *
5. In the Azure portal, edit the API permissions for your application to turn on the **User.Read** permission.
6. In the Azure portal, create a secret key to secure your application's credentials when requesting tokens. Enter the secret key. *

At the bottom of the dialog are "Finish" and "Cancel" buttons. A blue arrow points from the "Copy" button in step 3 to the "Register" button on the right page.

On the right, the "Register an application" page is visible. It includes the following fields and options:

- Name:**
- Supported account types:** Accounts in this organizational directory only (Blackbaud-ID only - Single tenant)
- Who can use this application or access this API?:** Accounts in this organizational directory only (Blackbaud-ID only - Single tenant)
- Redirect URI (optional):**
- Register:**

At the bottom of the page, there is a checkbox for "By proceeding, you agree to the Microsoft Platform Policies" and a "Register" button.

Enter App's ID

Configure Azure AD application

1. In a separate browser tab, sign in to [your Azure portal](#)
2. Enter your primary Azure AD domain. *
3. In the Azure portal, create an app registration with the redirect URI *
4. Enter your application's ID. *
5. In the Azure portal, edit the API permissions for your application to turn on the **User.Read** permission.
6. In the Azure portal, create a secret key to secure your application's credentials when requesting tokens. Enter the secret key. *

Microsoft Azure Search resources, services, and docs (G+)

Home > Blackbaud-ID >

Azure AD SSO connection for Jackie's LE with Blackbaud

Search (Cmd+/) Delete Endpoints Preview features

- Overview
- Quickstart
- Integration assistant
- Authentication
- Certificates & secrets
- Token configuration
- API permissions
- Expose an API
- App roles
- Owners
- Roles and administrators
- Manifest

Essentials

Display name
[Azure AD SSO connection for Jackie's LE with Blackbaud](#)

Application (client) ID
[REDACTED]

Object ID
[REDACTED]

Directory (tenant) ID
[REDACTED]

Supported account types
[My organization only](#)

Client credentials
[Add a certificate or secret](#)

Redirect URIs
[1 web, 0 spa, 0 public client](#)

Application ID URI
[Add an Application ID URI](#)

Managed application in local directory
[Azure AD SSO connection for Jackie's LE with Blackbaud](#)

Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? [Learn more](#)

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)

Go to API Permissions and Add a permission

The screenshot shows the Microsoft Azure portal interface. At the top, the navigation bar includes the Microsoft Azure logo, a search bar, and the user profile 'John.Vogel@blackbaud... BLACKBAUD-ID'. The breadcrumb trail is 'Home > Blackbaud-ID > Azure AD SSO connection for Jackie's LE with Blackbaud'. The main heading is 'Azure AD SSO connection for Jackie's LE with Blackbaud | API permissions'. Below the heading is a search bar and 'Refresh' and 'Got feedback?' buttons. A left-hand navigation pane lists various options, with 'API permissions' highlighted. A large blue arrow points from the left towards the 'Add a permission' button. An information box explains the 'Admin consent required' column. Below this is the 'Configured permissions' section, which currently shows 'No permissions added'. At the bottom, there is a link to 'Enterprise applications'.

Microsoft Azure Search resources, services, and docs (G+)

John.Vogel@blackbaud... BLACKBAUD-ID

Home > Blackbaud-ID > Azure AD SSO connection for Jackie's LE with Blackbaud

Azure AD SSO connection for Jackie's LE with Blackbaud | API permissions

Search (Cmd+/) Refresh Got feedback?

Overview
Quickstart
Integration assistant

Manage

- Properties
- Authentication
- Certificates & secrets
- Token configuration
- API permissions**
- Expose an API
- App roles
- Owners

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. [Learn more](#)

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ✓ Grant admin consent for Blackbaud-ID

API / Permissions n...	Type	Description	Admin consent req...	Status
No permissions added				

To view and manage permissions and user consent, try [Enterprise applications](#).

Select Microsoft Graph

The screenshot displays the Microsoft Azure portal interface. At the top, the header includes the 'Microsoft Azure' logo, a search bar, and user information for 'John.Vogel@blackbaud...'. The left-hand navigation pane shows the 'API permissions' option selected. The main content area is titled 'Request API permissions' and features tabs for 'Microsoft APIs', 'APIs my organization uses', and 'My APIs'. Under the 'Microsoft APIs' tab, a section titled 'Commonly used Microsoft APIs' lists several options. A large blue arrow points to the 'Microsoft Graph' option, which is described as providing access to data from Office 365, Enterprise Mobility + Security, and Windows 10. Other visible options include Azure DevOps, Azure Service Management, Office 365 Management APIs, Azure Batch, Azure Communication Services, and Azure Cosmos DB.

Request API permissions

Select an API

Microsoft APIs APIs my organization uses My APIs

Commonly used Microsoft APIs

Microsoft Graph
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

Azure DevOps
Integrate with Azure DevOps and Azure DevOps server

Azure Service Management
Programmatic access to much of the functionality available through the Azure portal

Office 365 Management APIs
Retrieve information about user, admin, system, and policy actions and events from Office 365 and Azure AD activity logs

More Microsoft APIs

Azure Batch
Schedule large-scale parallel and HPC

Azure Communication Services
Rich communication experiences with

Azure Cosmos DB
Fast NoSQL database with open APIs

Select delegated permissions

The screenshot shows the Microsoft Azure portal interface. At the top, there is a blue header with the Microsoft Azure logo, a search bar, and user information for John.Vogel@blackbaud.. Below the header, the breadcrumb trail reads 'Home > Blackbaud-ID > Azure AD S...'. The main content area is titled 'Request API permissions' and shows the 'Microsoft Graph' API selected. A question asks 'What type of permissions does your application require?' with two options: 'Delegated permissions' (selected by a teal arrow) and 'Application permissions'. The 'Delegated permissions' option includes the text 'Your application needs to access the API as the signed-in user.' The 'Application permissions' option includes the text 'Your application runs as a background service or daemon without a signed-in user.'

Microsoft Azure

Search resources, services, and docs (G+)

John.Vogel@blackbaud..

BLACKBAUD-I

Home > Blackbaud-ID > Azure AD S...

Azure AD SSO con

Search (Cmd+/)

- Overview
- Quickstart
- Integration assistant

Manage

- Properties
- Authentication
- Certificates & secrets
- Token configuration
- API permissions

Request API permissions

< All APIs

Microsoft Graph
<https://graph.microsoft.com/> Docs

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

Add User.Read Permission

Microsoft Azure | Search resources, services, and docs (G+)

Home > Blackbaud-ID > Azure AD > API permissions

Request API permissions

< All APIs

Microsoft Graph
https://graph.microsoft.com/ Docs

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

Select permissions [expand all](#)

user.read

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. [Learn more](#)

Permission	Admin consent required
> IdentityRiskyUser	
✓ User (1)	
<input checked="" type="checkbox"/> User.Read Sign in and read user profile	No
<input type="checkbox"/> User.Read.All Read all users' full profiles	Yes
<input type="checkbox"/> User.ReadBasic.All Read all users' basic profiles	No
<input type="checkbox"/> User.ReadWrite Read and write access to user profile	No

[Add permissions](#) [Discard](#)

Grant Admin Consent

Microsoft Azure | Search resources, services, and docs (G+)

Home > Blackbaud-ID > Azure AD SSO connection for Jackie's LE with Blackbaud

Azure AD SSO connection for Jackie's LE with Blackbaud | API permissions

Search (Cmd+)

Refresh | Got feedback?

Grant admin consent confirmation.
Do you want to grant consent for the requested permissions for all accounts in Blackbaud-ID? This will update any existing admin consent records this application already has to match what is listed below.

Configured permissions
Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

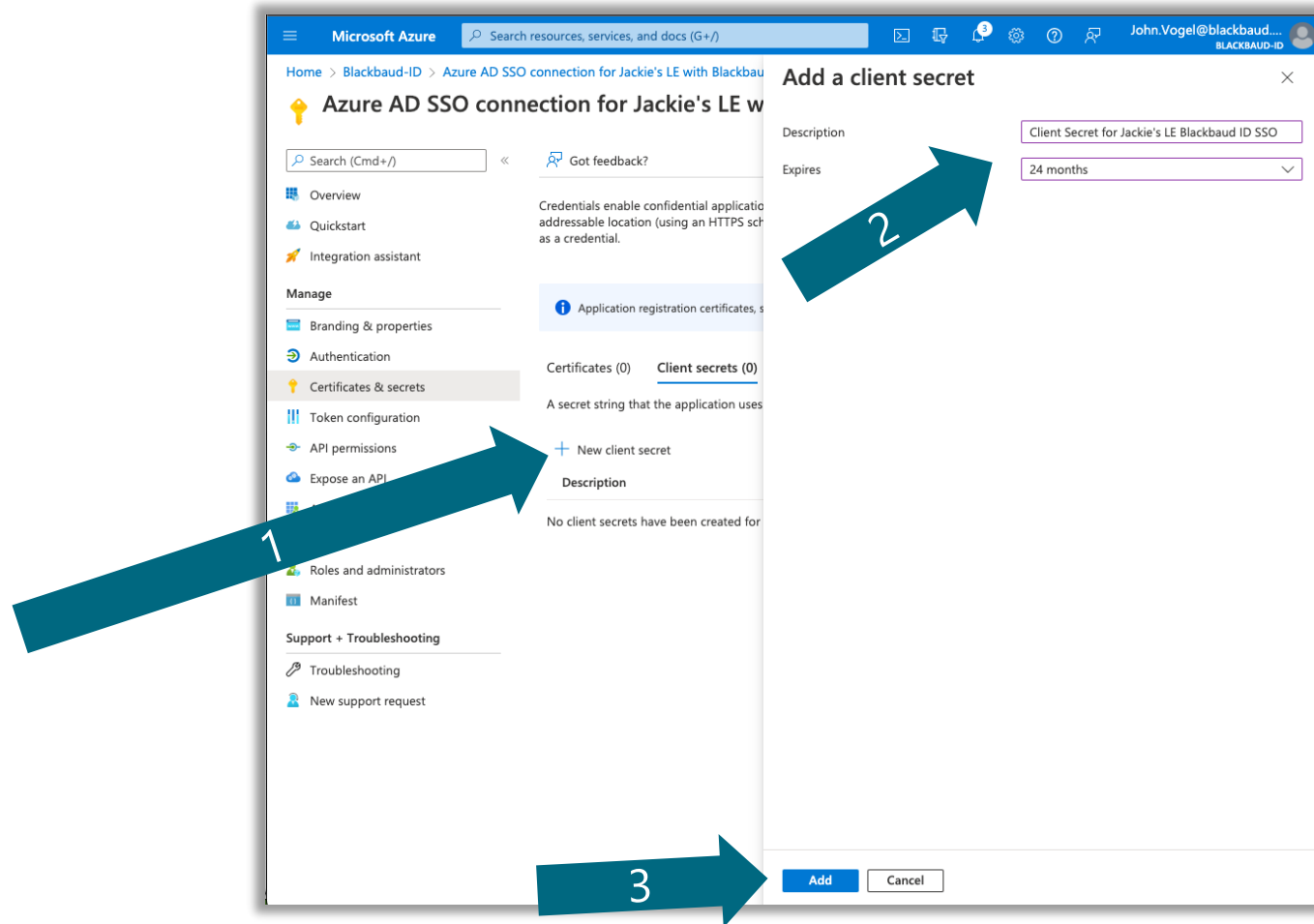
+ Add a new permission

Grant admin consent for Blackbaud-ID

Permissions (1)	Type	Description	Admin consent req...	Status
Microsoft Graph (1)				
User.Read	Delegated	Sign in and read user profile	No	

To view and manage permissions and user consent, try [Enterprise applications](#).

Go to Certificates & secrets and add new secret



Add Secret Value, expiration date and Finish configuration

The image shows two overlapping screenshots from the Microsoft Azure portal. The left screenshot is a 'Configure Azure AD application' dialog box with the following steps:

1. In a separate browser tab, sign in to your Azure portal
2. Enter your primary Azure AD domain. *
3. In the Azure portal, create an app registration with the redirect URI *
4. Enter your application's ID. *
5. In the Azure portal, edit the API permissions for your application to turn on the **User.Read** permission.
6. In the Azure portal, create a secret key to secure your application's credentials when requesting tokens. Enter the secret key. *

⚠ Enter the secret key value
7. In the Azure portal, find the "Expires" date for the secret key used in the previous step. Enter the secret key's Expires date. *

Buttons:

The right screenshot shows the 'Certificates & secrets' page for the application 'BBDevDays2023'. It features a table with the following data:

Description	Expires	Value	Secret ID
bbdevdays2023	6/4/2025	[REDACTED]	[REDACTED]

Two blue arrows point from the 'Value' and 'Expires' columns of the table to the corresponding input fields in the configuration dialog on the left.

Claim email domains

The screenshot shows the 'Single sign-on' configuration page for 'Jackie's LE'. The navigation bar at the top includes 'Admin', 'Home', 'Users and admins', 'Billing', 'Authentication', and 'Settings'. The main heading is 'Single sign-on' with a 'Back to Authentication settings' link. Below this is the 'Azure AD configuration' section, which includes an 'Invite another admin to configure your connection' link. A progress indicator shows four steps: 1 - Configure your connection (checked), 2 - Claim your email domains (highlighted with a large blue arrow), 3 - Test connection, and 4 - Turn on. A 'Claim domains' button is located next to step 2. At the bottom, there is a link to 'Erase all single sign-on settings'.

Admin Home Users and admins Billing Authentication Settings

Single sign-on

[Back to Authentication settings](#) Jackie's LE

Azure AD 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](#)



Enter DNS record details

The image shows two overlapping screenshots of the Google Domains interface. The left screenshot is a modal window titled "Claim email domains" for the domain "blackbaudidsso.com". It shows a form to add a custom DNS record with the following details: Name/Host/Alias "@", Record type "TXT", Time to live (TTL) "3600 (or 1 hour)", and a redacted "Value" field. A blue arrow with the number "2" points to the "Verify this domain" button. The right screenshot is the main "DNS" configuration page for "Google Domains DNS Example". It shows "Default name servers (Active)" and a table of "Resource records". The table has columns for "Host name", "Type", "TTL", and "Data". A record is shown with Host name "@", Type "TXT", and TTL "3600", with a redacted "Data" field. A blue arrow with the number "7" points to the "Data" field of this record. A diagonal banner across the top of the right screenshot reads "Google Domains DNS Example".

2

7

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	[Redacted]

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

DNS

Global DNS settings

Default name servers (Active) Custom name servers

These DNS settings are active. Changes are published immediately, but may take time to propagate

Resource records [Export DNS records](#)

Resource records point to the services your domain uses, including web and email services. [Learn more about resource records](#)

Custom records No records added

Host name ⓘ	Type ⓘ	TTL ⓘ	Data ⓘ
@	TXT	3600	[Redacted]

+ Add more to this record

Create new record


Cancel Save

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

The image shows two browser windows side-by-side. The left window is at `host.nxt.blackbaud.com/authenticationsettings/setup-connection?leid=t...` and displays the 'Single sign-on' configuration page for 'Jackie's LE'. It features a progress indicator with four steps: 1 - Configure your connection (checked), 2 - Claim your email domains (checked), 3 - Test connection (checked), and 4 - Turn on (not checked). Step 3 includes a 'Copy' button for the URL `https://signin.blackbaud.com/signin/?loginTest=true`. The right window is at `signin.blackbaud.com/signin/?loginTest=true` and shows a 'Sign in' form with an 'Email address' input field, a blue 'Continue' button, and a 'Need help?' link. A large teal arrow points from the 'Copy' button in the left window to the 'Continue' button in the right window.

host.nxt.blackbaud.com/authenticationsettings/setup-connection?leid=t...

Admin Home Users and admins Billing Authentication Settings

Jackie's LE

Single sign-on

Jackie's LE

[Back to Authentication settings](#)

Azure AD configuration

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

- ✓ 1 - Configure your connection
[Edit connection](#)
- ✓ 2 - Claim your email domains
blackbaudid.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

signin.blackbaud.com/signin/?loginTest=true

Sign in

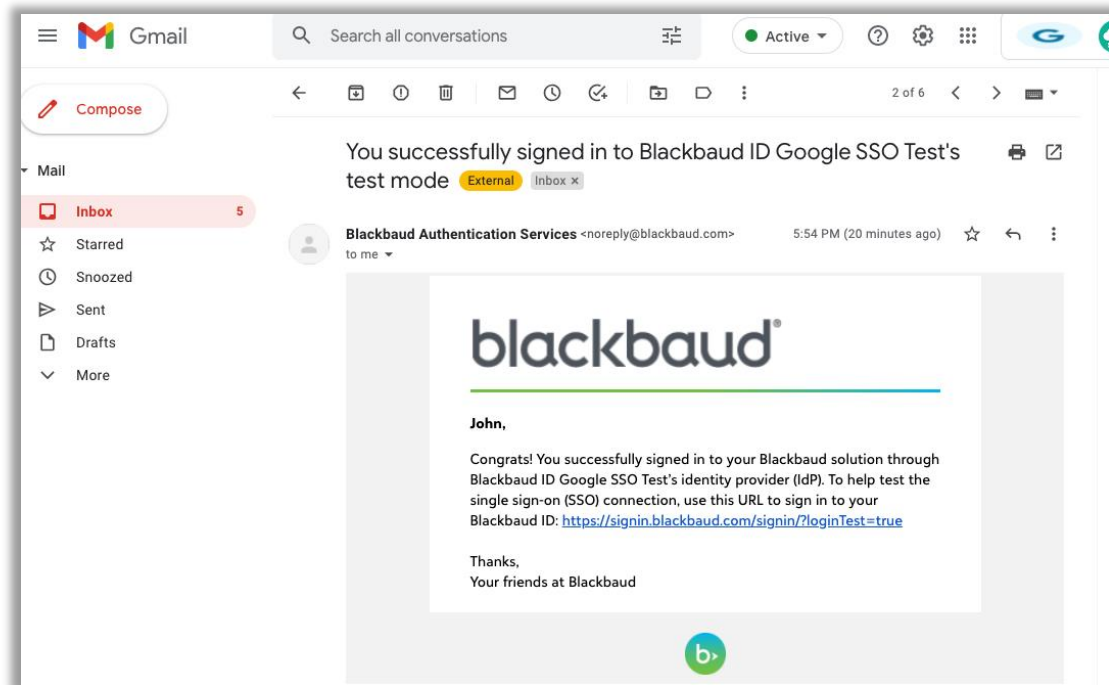
Email address

Continue

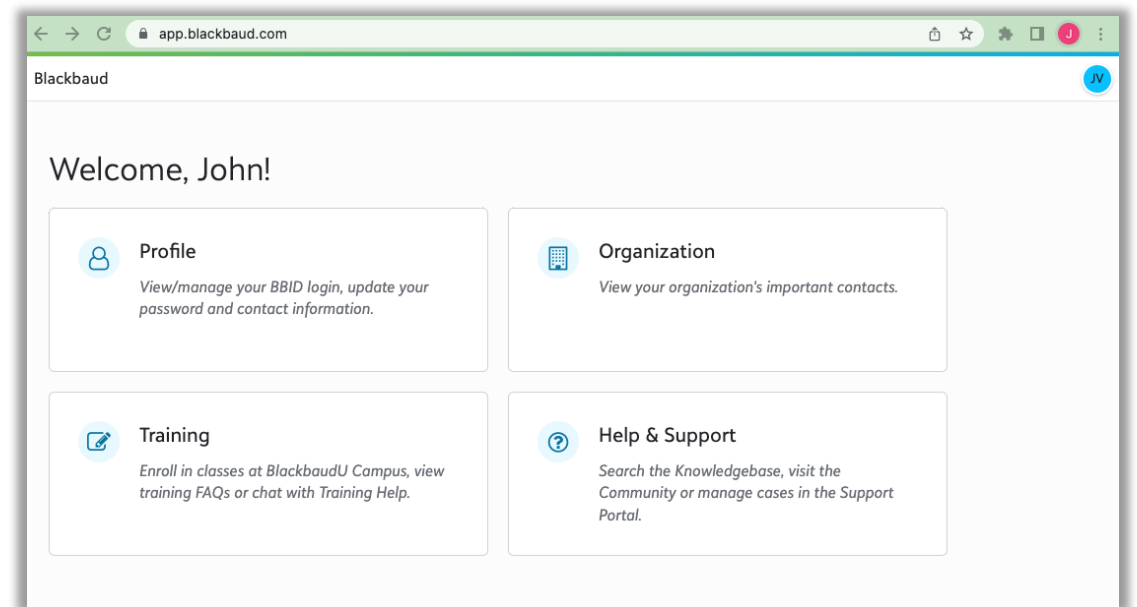
[Need help?](#)

Test connection successful!


EMAIL CONFIRMING SIGN IN



WELCOME PAGE AFTER SIGNING IN



Turn on SSO



- ✓ 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`
 -
 - (1 Blackbaud IDs currently in Test mode)
 - [Turn off Test mode](#)
- 4 - Turn on

[Learn about turning on SSO](#)

Confirm any impact & Connect SSO

The screenshot displays two overlapping dialog boxes from the Blackbaud SSO configuration interface. The background shows a navigation bar with 'Admin' and 'Home' links and a browser address bar with the URL 'https://sianin.blackbaud.com/sianin/?loginTest=true'.

Dialog 1: Connect your Azure AD SSO

- Ready to make the switch? When you connect with Azure AD:
 - 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 @blackbaudid.com](#)
 - When your IdP authenticates a Blackbaud ID, that ID will then use your Azure AD connection to manage passwords, lockouts, and other security features.
- Automatically send members an email from Blackbaud informing them of the change

Buttons: **Connect with Azure AD**, Cancel

Dialog 2: 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)

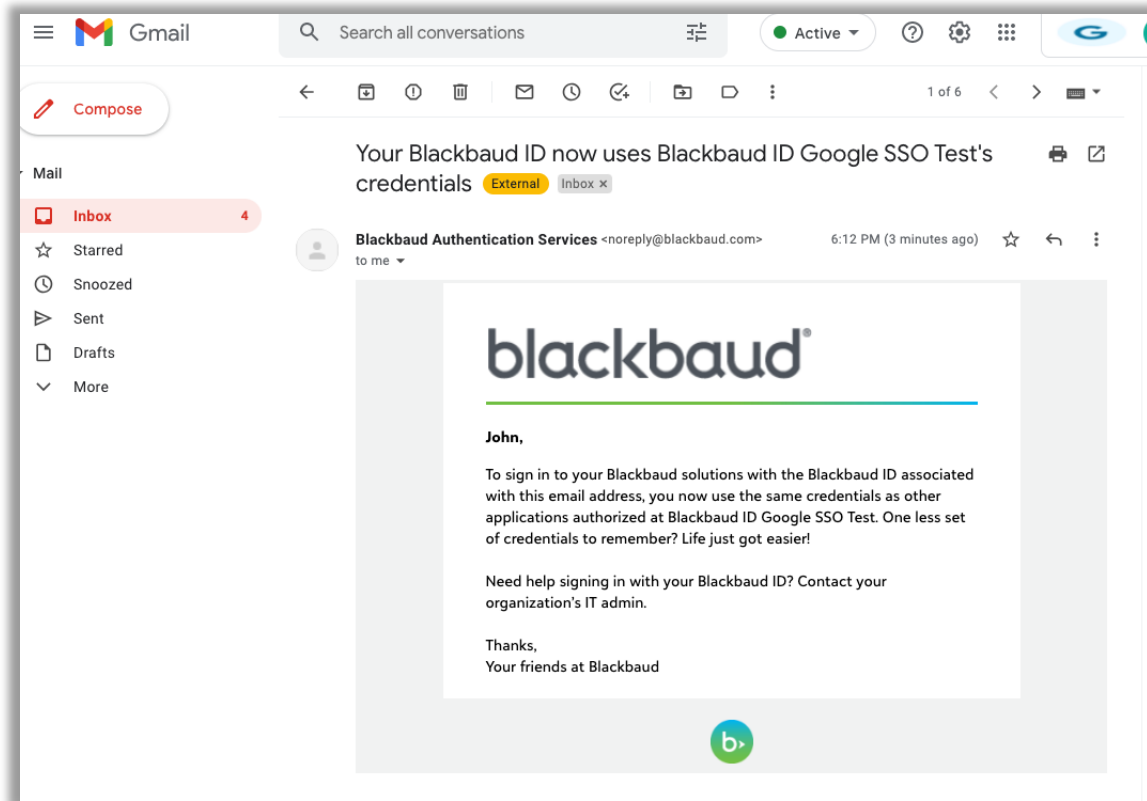
Copy all to clipboard

john.vogel@blackbaudidsso.com

Close

Teal arrows with numbers 1 and 2 indicate the flow of the process. Arrow 1 points from the link in the first dialog to the 'Copy all to clipboard' button in the second dialog. Arrow 2 points from the 'Connect with Azure AD' button in the first dialog to the left side of the image.

Confirmation email



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

Completed connection page

Admin Home Users and admins Billing Authentication Settings

JV Jackie's LE

Single sign-on with Azure AD

Jackie's LE

[Back to Authentication settings](#)

Jackie's LE
[Edit display name](#) [Update application key](#)

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

Connection details

Connection name blackbaudid-onmicrosoft-com
Application ID [REDACTED]

Redirect settings

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

Raiser's Edge NXT
`https://signin.blackbaud.com/signin?sso=blackbaudid-onmicrosoft-com&redirectUrl=https://renxt.blackbaud.com/` [Copy](#)

Claimed email domains

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 heading is 'Single sign-on with Google G Suite' with the connection name 'Blackbaud ID Google SSO Test' to its right. Below the heading is a link 'Back to Authentication settings'. A green checkmark icon is next to the connection name 'Blackbaud ID Google SSO Test', with a link 'Edit display name' and an information icon. To the right is a link 'Update client secret'. Below these is a link 'Invite another admin to configure your connection' and a button 'Learn about disconnecting SSO' which is highlighted with a teal arrow. The bottom section is divided into two panels: 'Connection details' showing 'Connection name blackbaudidssso-com' and 'Redirect settings' with the text '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 blackbauidssoco
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

