How to enable Blackbaud ID for Blackbaud CRM™

Single Sign-On (SSO) with Blackbaud ID will be supported for **hosted customers only** in Blackbaud CRM™. This document will outline the steps you need to take to enable Blackbaud ID for your Blackbaud CRM environment.

Step 1: Read through this Blackbaud ID overview

Here you will find detailed information on things to consider, what you need to know before enabling, and frequently asked questions. Be sure you have taken the time to review this material before proceeding with the enablement process.

Step 2: Establish an SSO connection with Blackbaud ID

Find out who in your organization establishes SSO connections for your third-party applications. They may have already established an SSO connection with Blackbaud ID. If not, then they will need to do a few extra steps to connect Blackbaud ID to your Identity Provider for SSO. You can refer them to the section titled "Using your organization's Identify Provider with BBID" in this document. We strongly recommend you confirm completion of these steps and have verified that Blackbaud ID is connected to your SSO before proceeding.

Step 3: Ensure that you are on the latest Service Pack and hotfix

Step 4: File a ticket with Blackbaud support to enable Blackbaud ID

Provide the following information to support:

- Name and contact info. Our hosting team will be contacting you to confirm and arrange a time to perform the enablement. Ensure that users will be out of the system and no processes running, as there will be an app pool recycle. The enablement itself only takes a few minutes.
- BBCRM Environment(s) to be enabled (Staging, Test, Production). You can always choose to enable Blackbaud ID in a lower environment first, before moving to Production.
- Preferred date and time

Step 5: Blackbaud Hosting will enable Blackbaud ID

Step 6: Confirm users are presented with the Blackbaud ID login screen

Users will also see the new Omnibar at the top of the screen in the BBCRM UI.

Things to consider before utilizing Blackbaud ID

The release of Blackbaud ID for Blackbaud CRM offers several new capabilities for your organization. These features include a single sign-on for your Blackbaud Products and easy navigation between environments using the Omnibar. Before adopting Blackbaud ID, there are a few factors your organization should consider.

The largest impact will be the migration of your customizations and integrations. Integrations that connect to Blackbaud CRM in an automated fashion – such as those utilizing the API, OData, and similar endpoints – may need to be updated. The process for updating your integrations varies depending on your setup and is described in Migrating Your Integrations below.

The time required to migrate and test your integrations could vary considerably, depending on their size and complexity. Additionally, once Blackbaud releases additional enhancements, such as personal access tokens, further changes may be required. Please consider both of these factors when deciding whether or not to adopt Blackbaud ID.

Migrating your integrations

To make your integrations compatible with BBID, you will need to update those that connect to Blackbaud CRM using a username and password. These include calls to BBCRM's APIs and other endpoints. Depending on your configuration, one or more of the following will apply:

Your integrations connect using an Active Directory system account that isn't used for front-end operations

If your integrations use a system account and no users log into it through the front-end, you don't need to take any additional actions. Your integrations will continue to work normally. We have provided utilities to manage password updates and resets to these accounts with the release of BBID. Please be sure not to migrate these accounts by linking them to a BBID. They should not have an email address used by a BBID account and they should not be used to log into the application's UI.

Your integrations connect with a user account, and you will authenticate using Blackbaud's secure service

If your integrations use a user account (i.e., one that is also used to access BBCRM's UI to perform day-to-day operations) and that account will be migrated to Blackbaud ID, you will need to update the credentials of all integrations using that account to use its new Blackbaud ID credentials. It is recommended that you test each integration in a BBID-enabled test environment before enabling BBID in your production environment. Please note that this will only work if your organization does not have MFA enabled on this user account and you are not authenticating through Google or another IdP. If you are, see the next section.

Your integrations connect with a user account, and you will authenticate using Google or another IdP

If your integrations use a user account (i.e., one that is also used to access BBCRM's UI to perform day-to-day operations), that account will be migrated to Blackbaud ID, and it will be authenticated using your IdP, you have two options. You can create an AD account, or you can create a Blackbaud ID account that will use

Blackbaud's secure login service. In both cases, you will need to update your integrations to use the credentials of the newly created account. To create a Blackbaud ID account that uses Blackbaud's login service, you will need an email address from outside of the domain claimed by your organization.

Migrating from Custom SSO

If you are migrating from Blackbaud's custom SSO solution or using your own Active Directory to authenticate users, it is recommended that you take the following steps to ease migration to Blackbaud ID.

1. If you plan to authenticate your users' Blackbaud ID accounts through your organization's identity provider (IdP), see Using a Custom IdP with BBID.
2. If you set up authentication through your IdP, ensure their email addresses are from your domain.
3. Update the email on their Application User record to match their BBID account email.

These changes will allow accounts to automatically migrate once you enable Blackbaud ID in Blackbaud CRM.

Using your organization's IdP (Identity Provider) with BBID

Your organization will most likely already have in place a single-sign-on solution. If any of your users are accessing Blackbaud through our Community Forums, for example, they already are logging into that using a Blackbaud ID that they created when registering. Somebody at your organization is the Organization Administrator for your Blackbaud ID users. When that person logs into the Blackbaud.com website, they can navigate to the profile area and perform administrative functions. One of those is the ability to connect Blackbaud ID to your existing SSO. Once these steps are followed and that connection established, you can test it by having your users login to our website. They should be presented with your common SSO login.

The following information is to assist in establishing this connection between Blackbaud ID and your existing SSO. When these steps refer to the Administration section, they are referring to the Blackbaud ID administration area itself, NOT the Blackbaud CRM administration page.

Blackbaud ID supports SSO through:

- Microsoft *Azure Active Directory* (AD)
- Security Assertion Markup Language (SAML) 2.0 IdPs, such as Google G Suite, OneLogin, Shibboleth, or Central Authentication Service (CAS)
- Microsoft *Active Directory Federated Services* (*ADFS*)
- *Okta*
- Google *G Suite*

See the sections guidance below for a general overview of how to set up SSO or follow the links above for detailed instructions on a particular SSO option.

Configure the connection

To enable your organization's Blackbaud IDs to sign in to Blackbaud solutions, configure the connection to your Identity Provider (IdP). Supported providers are listed above.

Configure the IdP

For SAML and *ADFS*, you'll complete an extra step to configure your IdP to connect to Blackbaud's secure authentication service.

Claim email domains

Identify the email domains your organization uses to recognize and redirect members to your IdP when they sign in. After you claim a domain, anyone who starts to sign in to their Blackbaud ID with an email address on that domain automatically goes to your login, where they can instead sign in with their organizational credentials. To claim email domains, see Claimed Email Domains.

Test the connection

Before you turn on single sign-on, test the connection to verify your organization can use its IdP to sign in to Blackbaud solution. You'll receive an email with instructions on how to test the connection, and you'll also receive an email after you've successfully signed in to your Blackbaud solutions with your IdP. To test your connection, see Test Mode.

Turn on SSO

After you test the connection, you're ready to turn on single sign-on! When you turn on SSO, anyone who signs in to their Blackbaud ID with one of your claimed domains is redirected to your IdP. After they authenticate through your IdP, their Blackbaud ID:

- Automatically redirects to your organization’s login for future sign-ins.
- Uses your IdP for password updates, lockouts, and similar authentication management.

Redirect settings

To ease authentication, members at your organization can bypass the Blackbaud ID sign-in and instead sign in directly through your identity provider (IdP). To view the URLs your organization uses to sign in to Blackbaud solutions directly through your IdP, see Redirect Settings.

Single Sign-On With Blackbaud ID

To simplify and improve your Blackbaud log-in experience, we streamlined our system so you can use one set of credentials to access all Blackbaud resources. With the Blackbaud Omnibar and single sign-on features, you can log in to ***Blackbaud CRM***, blackbaud.com, and other Blackbaud programs using the same username and password. For example, if you use ***Blackbaud CRM*** and ***Financial Edge NXT***, when you log in to ***Blackbaud CRM*** with your Blackbaud single sign-on account, you are logged in to ***Financial Edge NXT*** automatically and you can easily navigate between the two programs in the same window.

Before you upgrade:

- Blackbaud.com site administrators: Invite all users to create a Blackbaud ID account and confirm that the email address on each user record corresponds to that user's Blackbaud ID email address. For more information about creating a Blackbaud ID, see Blackbaud ID FAQs. **Note: If your organization has connected Blackbaud ID to your Identity Provider through configuring a Single Sign-On connection, it is not necessary to invite your Blackbaud CRM users to create a Blackbaud ID account.**

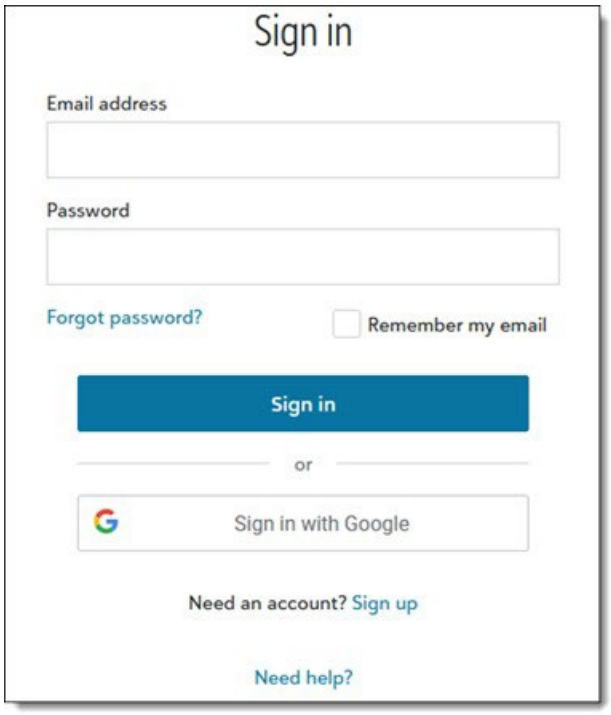
After you upgrade:

- Blackbaud CRM users: Update your OData and API connections.

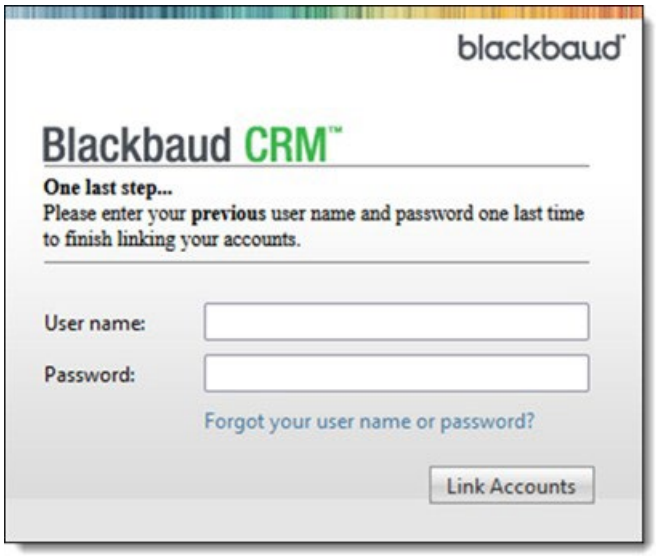
Tip: We recommend that you create a unique user account for each ***Blackbaud CRM*** user. If you must create a shared user account, make sure to use a shared email address for the login.

Initial Setup

When you first log in to ***Blackbaud CRM*** after this change, you will see a different login screen.



Enter your username and password. In the next screen, enter your previous username and password to link your existing account to the new account.



Omnibar

The omnibar at the top of the screen allows you to switch from one Blackbaud product to another, see what product you are using at the moment, as well as all the other functions like searching for features or viewing the organizational calendar.

Manage Application Users

From the Administration page, select **Application Users** under **Security** to complete these tasks:

- Send user invitations
- Link users to constituent records
- Assign system roles
- Disable user accounts

Manage Active Directory Information

Once Blackbaud ID is enabled, user active directory accounts automatically migrate to Blackbaud IDwhen users first log in to ***Blackbaud CRM***.

Under **Administration**, you can manage active directory passwords. To change a password, select **Change Active Directory Password**. To reset a password, select **Reset Active Directory Password**.

Blackbaud ID vs. Custom SSO for BBCRM

Single Sign-On (SSO) with Blackbaud ID will be supported in Blackbaud CRM™. Before this, Custom SSO has been offered for several years by Blackbaud Services as a plug-in for Blackbaud CRM. This document will compare the features of the two Single Sign-on solutions in order to help our customers understand and make the appropriate decisions.

Side-by-side feature comparison

Feature	BBID?	Custom SSO?	Notes
Supports SSO via your organization's identity provider (IdP) via SAML2.0+	Y	Y	BBID also has first class connections to these IdPs: Azure AD, Google G Suite, ADFS, Okta
Supports secure authentication directly through Blackbaud or Google	Y	N	
Supports Multi-factor Authentication through an IdP	Y	Y	
Supports Multi-factor Authentication directly	Y	N	With BBID, individual users can turn on MFA
Admins can enforce Multi-factor Authentication for all users	Thru IdP	Thru IdP	
Support and enables integrations with BBCRM through Active Directory accounts	Y	Y	For Blackbaud ID, AD accounts used for integrations cannot also be used to log in interactively
Can add new users via tasks in Blackbaud CRM administration	Y	Y	
Can add users in bulk via query	N	Y	
Supports custom branding	Y	At logout	
Separately enabled per BBCRM environment	Y	Y	You can test in a lower environment before enabling in production
Configurable session timeout setting	N	Y	BBID timeout is fixed at 90 minutes.
Can enable via a call to Support	Y	N	
Omnibar in BBCRM enables user navigation between products and environments	Y	N	

Blackbaud ID for BBCRM FAQ (Frequently asked questions)

Q: Once Blackbaud releases token-based authentication, will I need to update my integrations again?

A: In order to reduce risks from password storage and reuse, future releases may require integrations to use tokens instead of passwords. If this is the case, we will send out communications early and give you time to upgrade your integrations before disabling authentication via passwords.

Q: Will taking BBID impact any of my UI customizations, such as changes to color, size, and font?

A: Customizations to the BBCRM UI should be preserved with BBID with the exception of the menu bar and sign-in page. These have been replaced by the Blackbaud ID Omnibar and sign-in page. To see your options on customizing these areas, see Implementing a Branded Sign-in and Omnibar with BBID.

Q: How do I manage my account information like name and email?

A: Information about Application Users have been moved to the BBID account. You can edit this information by clicking on your initials in the upper right section of the Omnibar and clicking “Blackbaud ID Profile”. This will take you to your BBID profile where you can edit your name, email, password, and MFA settings. If your organization uses their own IdP, some of this information is managed by the IdP and you will need to contact your administrator to change it.

Q: How do I manage the AD accounts I use for integrations and other capabilities?

A: Just as before, AD accounts are managed through the Organizational Units section and the Application Users Page. If your organization has permitted it, you can change or reset your password by going to **Administration** and selecting **Change Active Directory password** and **Reset Active Directory password** in the **Configuration** section.

Q: How do I search for application users?

A: Each BBID account has an email address associated with it. You can either use this email address or the display name to search for application users.

Troubleshooting

Q: I’m having trouble logging in. What steps should I take?

A: First, ensure you can log into your BBID account by visiting https://signin.blackbaud.com/signin/. If you can log in successfully, confirm with your Administrator or help desk that your Application User has been linked to

your BBID account. If that does not resolve the problem or you are having a different issue logging in, please contact Blackbaud Support