Authentication and security

How to sign in to Bluecore with SSO or multi-factor authentication

When you're ready to sign in to Bluecore to create and manage campaigns, view analytics and more, go to app.bluecore.com.

Signing in with SSO

If you have single sign-on (SSO) log in enabled, follow these steps to sign in to Bluecore:

1. Enter your email address.

2. You'll be redirected to your company's IdP login page.

3. After signing in via your company's IdP, you'll be redirected back to Bluecore.

Signing in without SSO

If you do not have SSO enabled, follow these steps to sign in to Bluecore:

1. Enter your email address, then click **Next**.

2. You'll be prompted to enter your password.

  ▫

Multi-factor authentication

The first time you sign in with credentials, you'll be prompted to set up multi-factor authentication.

> ⓘ With certain configurations, multi-factor authentication may also be referred to as two-factor authentication, or 2FA.

One-time codes generated by an authenticator app must be configured by you the first time you log in to Bluecore on a new device.

Though this process will work with other authenticator apps—such as Microsoft Authenticator (free), Authy (free), Duo (paid) or 1Password (paid)—Bluecore suggests that you set up multi-factor authentication using Google Authenticator (free) as it is one of the easiest and streamlined ways of configuring.

To expedite the following process, install the app from the Apple App Store (iPhone) or Google Play Store (Android):

1. The first time you are using this device to log in to Bluecore, after you enter your email address and password, you are prompted to set up MFA. Click the **Setup** button below "Google Authenticator."

Bluecore

Set up multifactor
authentication

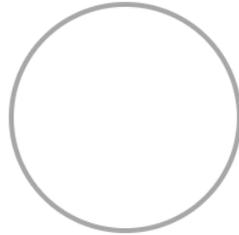◯ Okta Verify

Enter single-use code from the mobile app.

Setup

◯ Google Authenticator

Enter single-use code from the mobile app.

Setup

2. Next, select the type of device that you have, either iPhone or Android.

If you don't already have the app installed on your device, follow the onscreen instructions now to download the Google Authenticator app from the Apple App Store (iPhone) or Google Play Store (Android). Once the app is on your device, click the **Next** button.

3. The following screen has a QR code. Follow the onscreen instructions to scan the QR code from within the Google Authenticator app on your device. This allows the Google Authenticator app to generate one-time codes for you to log in to Bluecore.
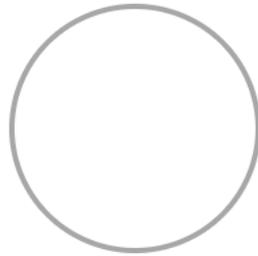
Setup Google Authenticator

Launch Google Authenticator, tap the "+" icon, then select "Scan barcode".
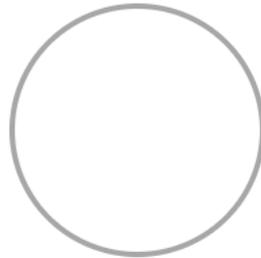
Can't scan?

Next

Back to factor list

4. After configuring your one-time code generator in the Google Authenticator app, click the **Next** button.

5. Enter the code generated by Google Authenticator in the **Enter Code** field and click the **Verify** button.

Bluecore

Setup Google Authenticator

Enter code displayed from the application

Enter Code

[   ]

[**Verify**]

Back to factor list

Multiple companies

In the rare scenario where a user has access to multiple companies, they will be prompted to provide a company name during their first sign in. For subsequent sign-ins, they will be automatically redirected to use that same company's single sign on page.

Regardless of which company single sign on page the person uses, they will be able to access any or all namespaces they have permissions to.

Once we have verified the users, they won't need to sign into a different company to access their companies' namespaces.

If you have any questions or issues signing in to your Bluecore account, reach out to the Support Team at support@bluecore.com.

Requiring company IdP to sign in to Bluecore

Bluecore can integrate with your company's identity provider (IdP) so that your users can sign in using their single sign-on (SSO) credentials.

Using single sign-on to sign in to Bluecore has a few security benefits, such as:
- Fewer points of access for user management.
- Easier deprovisioning.
- Eliminates the need for a separate Bluecore password.

> ⚠️ Does your company's IdP support Service Provider-Initiated (SP-Initiated) SAML sign-in? If not, it is not possible to set up SSO to sign in to Bluecore. Please continue to use the usual email and password credentials to sign in.
> More information on Service Provider-Initiated sign-in

Create a ticket

To use SSO to sign in to Bluecore, file a support ticket and include someone with permissions in your company's access management system. That person will need to help set up and test the SSO implementation.

Before you file the ticket, there is some information to have ready to ensure the process goes smoothly and quickly. Include the following information in the Bluecore support ticket:

1. Provide SAML Metadata XML file

    a. Ensure the XML file includes the following profile mappings, to link to Bluecore credentials:

        i. User email

        ii. First name

        iii. Last name

> ℹ️ If you have multiple namespaces, all namespaces can be set up with one XML file

Once this information is ready, submit a support ticket via support@bluecore.com. A Bluecore support representative will walk you through the testing process to make sure SSO works as expected.

Once the ticket is filed, expect the process to take up to three weeks.