

BlueID5 — User Guide

Last Updated: February 2026

This guide covers the features and workflows available to you as a BlueID5 user. If anything looks different from what you see on screen, your organization may have customized certain options.

Contents

1. [Welcome & Getting Started](#)
2. [Creating Your Account \(Registration\)](#)
3. [Logging In](#)
4. [External Login Providers](#)
5. [Setting Up Two-Factor Authentication \(2FA\)](#)
6. [Setting Up Passkeys](#)
7. [Managing Your Profile](#)
8. [Changing Your Password](#)
9. [Managing External Logins](#)
10. [Managing Grants & Permissions](#)
11. [Account Recovery](#)
12. [Agreements & Privacy](#)
13. [Getting Support](#)
14. [FAQ & Troubleshooting](#)

1. Welcome & Getting Started

Welcome to **BlueID5**, your organization's identity and login system. BlueID5 is the secure gateway that protects your account and provides single sign-on access to the applications and services you

use every day.

With BlueID5 you can:

- Sign in once and access multiple applications without logging in again.
- Protect your account with strong passwords, two-factor authentication, and passkeys.
- Manage your profile information, security settings, and privacy preferences in one place.
- Control which applications have access to your account data.

How it works: When an application needs to verify your identity, it redirects you to BlueID5. You sign in (or are recognized automatically if you have an active session), and BlueID5 sends you back to the application. You will typically see the BlueID5 login page when you first access a protected application each day.

2. Creating Your Account (Registration)

If your organization allows self-registration, you can create your own BlueID5 account. Follow the steps below.

Step-by-Step Registration

Step 1 — Open the Registration Page

Navigate to the BlueID5 login page. Below the sign-in form, look for the "*Don't have an account?*" prompt and click the **Register** (or **Create Account**) link.

Step 2 — Enter Your Account Information

Fill in the required fields:

- **Username** — Choose a unique username. This is what you will use to sign in. (Some sites sign you in with your email address instead, and do not ask for a username.)
- **Email** — Provide a valid email address. A verification email will be sent to this address.
- **Password** — Create a strong password. The requirements are shown directly under the password fields.

- **Confirm Password** — Re-enter your password to make sure it matches.

Step 3 — Add Additional Information

Enter your first name, last name, company name, country, and **State / Province / Region**. Your phone number is optional. Choose your **Preferred Language**; it starts on your site's default language, and you can change it later on your account page.

Step 4 — Set Up Your Profile Photo (Optional)

BlueID5 uses **Gravatar** for profile photos. If you already have a Gravatar account linked to your email, your photo will appear automatically. You can also choose to hide your profile photo. You can always change this later.

Step 5 — Review Agreements

Before completing registration, you need to:

1. Click **Review** next to the *Privacy Notice* to read it, then return to the registration page.
2. Click **Review** next to the *Terms and Conditions*, read and accept them, then return.

Both items must show a green checkmark before you can proceed.

Step 6 — Submit and Verify Your Email

Click the **Register** button. We email you a verification code; enter it on the confirmation page that opens. **You must verify your email address before you can sign in.** If you do not see the email, check your spam or junk folder.

Password Requirements

Your password must meet the following rules:

Requirement	Details
Minimum length	At least 8 characters (your organization may require more)
Uppercase letter	At least one uppercase letter (A–Z)

Lowercase letter	At least one lowercase letter (a–z)
Number	At least one digit (0–9)
Special character	At least one special character (for example: ! @ # \$ % &)

Tip: Use a passphrase made of several unrelated words combined with numbers and symbols. For example, `Sunset7!Marble&Train` is both strong and easier to remember than a random string.

Account Approval: Some organizations require an administrator to approve new accounts before you can sign in. If this applies to you, you will see a message after registration letting you know your account is pending approval. You will receive an email once your account has been activated.

3. Logging In

BlueID5 supports several ways to sign in. The most common method is entering your username (or email) and password.

Standard Login (Username and Password)

1. Navigate to the BlueID5 login page (you may be redirected there automatically when you open an application).
2. Enter your **username or email address** in the first field.
3. Enter your **password** in the second field.
4. Optionally, check "**Remember me**" to stay signed in on this device (see note below).
5. Click **Sign In**.

Username-First Login Flow

Your organization may use a **username-first** login flow. In this case:

1. Enter your **username or email address** on the first page and click **Continue**.
2. On the next page, enter your **password** and click **Sign In**.

Why the two-step flow? This approach allows BlueID5 to detect whether your organization uses a custom identity provider (such as corporate single sign-on) and redirect you to the correct login page automatically.

Remember Me

When you check the "**Remember me**" option, your browser will keep your login session active for a longer period. This means you will not need to enter your credentials every time you visit. Avoid using this option on shared or public computers.

Your organization may still sign you out after a period of inactivity, even with "Remember me" ticked. This is a security setting your administrator controls; it does not mean anything is wrong. Simply sign in again.

Changing Your Password at First Sign-In

If your account was created for you — by an administrator, or through an invitation email — you may be asked to choose a new password the first time you sign in. This is normal. The password you were given has been sent through email and may have been seen by someone else, so it is replaced with one only you know.

You will not be able to continue until you have set your new password. It only happens once.

Account Lockout

Too many failed attempts: If you enter the wrong password several times in a row, your account will be temporarily locked to protect against unauthorized access. Wait a few minutes and try again, or use the [Account Recovery](#) options described later in this guide.

4. External Login Providers

BlueID5 may allow you to sign in using an account you already have with another service, such as:

- **Google**
- **Microsoft / Azure AD**
- **Apple**
- **GitHub**
- **LinkedIn**
- **Your organization's SSO provider** (federated login)

Signing In with an External Provider

1. On the login page, look for buttons below the password form labeled with the provider name (for example, "*GitHub*" or "*Microsoft*").
2. Click the button for the provider you want to use.
3. You will be redirected to that provider's login page. Sign in with your credentials there.
4. After successful authentication, you will be sent back to BlueID5. If this is your first time, you may be asked to confirm some details or link the external account to an existing BlueID5 account.

Signing In with Social Providers

When social login providers (such as Google, Microsoft, Apple, GitHub, or LinkedIn) are configured by your administrator, they appear as compact icon buttons on the login page.

1. On the login page, look for the row of provider icon buttons below the sign-in form.
2. Click the icon for the provider you want to use (for example, the Google icon or the Microsoft icon).
3. You will be redirected to the provider's website, where you may be asked to grant BlueID5 permission to access your basic profile information.
4. After granting permission and authenticating, you will be returned to BlueID5 and signed in. Your BlueID5 account will be linked to the social provider.

Tip: If you already have a BlueID5 account with the same email address as your social provider account, BlueID5 may automatically link them. Otherwise, you may be prompted to create a new account or link to an existing one.

Organization Sign-In

If your email domain is managed by an organization (for example, your employer), you may be redirected to your organization's own identity provider instead of using the standard BlueID5 login form.

1. On the login page, click **"Sign in with your organization"** (or enter your work email address in the username field).
2. If your email domain is recognized as belonging to a federated organization, you will be redirected to your organization's login page.
3. Authenticate using your corporate credentials on your organization's login page.
4. After successful authentication with your organization, you will be automatically signed into BlueID5 and redirected to the application you were trying to access.

Why am I being redirected? Your organization has configured BlueID5 to trust their own identity provider. This means you use your existing corporate credentials to sign in, and your organization maintains control over authentication policies. This is sometimes called "Single Sign-On" or "SSO."

Organization Single Sign-On (SSO)

If your organization has set up federated login, you may be redirected to your company's own login page after entering your username or email. This is normal. Sign in with your corporate credentials, and you will be returned to the application you were trying to access.

Linking Accounts: When you sign in with an external provider for the first time, BlueID5 may ask if you want to link that external account to your existing BlueID5 account. Linking allows you to sign in using either method in the future.

External Login Security

For additional protection, you can require two-factor authentication even when signing in through an external provider (such as Google, Microsoft, or your organization's identity provider).

1. Sign in to BlueID5 and go to your **account settings**.
2. Navigate to the **Security Preferences** section.
3. Enable the option "**Require 2FA for external logins**".

When this option is enabled, signing in through any external provider will also require you to complete a second factor (such as entering a code from your authenticator app). This provides an additional layer of security even when using trusted external providers.

Tip: If your organization's administrator has enabled this setting globally, it will apply to all users automatically. You can also enable it on your own account independently for extra protection.

5. Setting Up Two-Factor Authentication (2FA)

Two-factor authentication adds an extra layer of security to your account. Even if someone learns your password, they cannot sign in without the second factor — a time-based code from your phone.

Why this matters: Passwords alone can be guessed, stolen, or leaked. Two-factor authentication dramatically reduces the risk of unauthorized access to your account. We strongly recommend enabling it.

What You Need

You will need an **authenticator app** installed on your phone or tablet. Popular options include:

App	Available On
-----	--------------

Microsoft Authenticator	Android, iOS, Windows
Google Authenticator	Android, iOS
Authy	Android, iOS, Desktop
1Password, Bitwarden, LastPass	Various platforms

Step-by-Step Setup

Step 1 — Install an Authenticator App

If you do not already have one, download an authenticator app from your device's app store. Any app that supports TOTP (Time-Based One-Time Passwords) will work.

Step 2 — Open the 2FA Settings

Sign in to BlueID5, go to your **account settings**, and find the **Two-Factor Authentication** section. Click **Enable Authenticator** (or **Set Up 2FA**).

Step 3 — Scan the QR Code

BlueID5 will display a QR code on screen. Open your authenticator app, tap the option to add a new account, and scan the QR code with your phone's camera.

Cannot scan the code? Click the option to enter the key manually, then type the shared key shown on screen into your authenticator app.

Step 4 — Enter the Verification Code

Your authenticator app will now display a 6-digit code that changes every 30 seconds. Enter the current code into BlueID5 and click **Verify**.

Step 5 — Save Your Recovery Codes

After verification, BlueID5 will show you a set of one-time **recovery codes**. These codes allow you to sign in if you lose access to your authenticator app.

Save your recovery codes now! Write them down or store them in a secure location (such as a password manager). Each code can only be used once. If you lose both your authenticator device and your recovery codes, you may be locked out of your account.

Signing In with 2FA

After enabling two-factor authentication, signing in will work like this:

1. Enter your username and password as usual.
2. On the next screen, open your authenticator app and enter the current 6-digit code.
3. Click **Verify** to complete sign-in.

Tip: If your authenticator codes are not being accepted, make sure the date and time on your phone are set to automatic. Authenticator apps rely on accurate time to generate valid codes.

6. Setting Up Passkeys

What Are Passkeys?

Passkeys are a modern, passwordless way to sign in. Instead of typing a password, you verify your identity using something built into your device — such as your fingerprint, face recognition, or a PIN. Passkeys are faster than passwords and virtually immune to phishing attacks.

Compatible devices and methods:

- **Windows Hello** — fingerprint reader, facial recognition, or PIN on Windows devices
- **Touch ID / Face ID** — on Apple Mac, iPhone, and iPad
- **Android biometrics** — fingerprint or face unlock on Android devices
- **Security keys** — hardware devices such as YubiKey that plug into your USB port or connect via NFC

Step-by-Step Passkey Setup

Step 1 — Open Passkey Settings

Sign in to BlueID5 and go to your **account settings**. Find the **Passkeys** section and click **Add a Passkey**.

Step 2 — Name Your Passkey

Give the passkey a descriptive name so you can identify it later (for example, "*Work Laptop*", "*Phone*", or "*YubiKey*"). Click **Continue**.

Step 3 — Verify with Your Device

Your browser will prompt you to authenticate using your device's built-in method — such as scanning your fingerprint, looking at the camera for face recognition, entering your device PIN, or touching your security key. Follow the on-screen instructions from your browser or operating system.

Step 4 — Done!

Once your device confirms your identity, the passkey is saved. You will see it listed on your Passkeys page along with the date it was created.

Signing In with a Passkey

On the BlueID5 login page (especially in the username-first flow), you may see a **"Sign in with a passkey"** option or your browser may automatically suggest a saved passkey. Simply tap or click it and verify with your fingerprint, face, or PIN. No password needed.

Tip: Register passkeys on multiple devices you use regularly (for example, both your laptop and your phone). If one device is unavailable, you can still sign in with the other. You can also keep your password and 2FA as a fallback.

Managing Your Passkeys

From the Passkeys settings page you can see all your registered passkeys, including:

- The name you gave each passkey
- When it was created and last used

- Whether it is a built-in device passkey or a security key
- Whether it is synced across your devices

To remove a passkey you no longer use, click the **Remove** button next to it.

7. Managing Your Profile

Your profile page is the central place to view and update your personal information. To access it, sign in and navigate to your **account settings** (often accessible from a menu or your name/avatar in the top corner).

What You Can View and Edit

Section	Fields
Profile Photo	Powered by Gravatar. You can show or hide your photo.
Account Information	Username, email address, phone number. You can request changes to each of these (see notes below).
Personal Information	First name, last name, company name, position/title, country, region.
Address (optional)	Street address, city, postal code, PO box.
Notification Preferences	Opt out of heads-up notifications or marketing communications.
Terms & Privacy	View when you accepted the Terms of Service and Privacy Notice, and accept updates if available.

Changing Your Username

1. On the profile page, click the **Change** button next to your username.
2. Enter your new desired username.

3. Click **Save**. You may be asked to confirm the change.

Please note: Changing your username may affect how you sign in to applications. Make sure you remember your new username after the change is confirmed.

Changing Your Email Address

1. On the profile page, click the **Change** button next to your email.
2. Enter your new email address.
3. Click **Save**. A verification email will be sent to your new address.
4. Check your new email inbox, open the verification message, and click the confirmation link to complete the change.

Until you confirm the new email, your original email address remains active.

Changing Your Profile Photo

BlueID5 uses **Gravatar** (Globally Recognized Avatar) to display your profile photo. To change your photo:

1. Visit gravatar.com and sign in (or create a free account) using the same email address you use for BlueID5.
2. Upload your desired photo on Gravatar.
3. Your BlueID5 profile photo will update automatically.

If you prefer not to display a photo, toggle the "**Hide profile photo**" switch on your profile page.

8. Changing Your Password

It is good practice to update your password regularly. You can change your password at any time from your account settings.

How to Change Your Password

1. Sign in to BlueID5 and go to your **account settings**.
2. Select **Change Password**.
3. Enter your **current password** to verify your identity.
4. Enter your **new password**. Make sure it meets the [password requirements](#) listed in Section 2.
5. Enter the new password again in the **confirm password** field.
6. Click **Update Password**.

Tip: After changing your password, you may be signed out of other devices or sessions. This is a security measure to make sure only you can use the new password.

No current password? If you originally signed in only through an external provider (such as GitHub or Microsoft) and never set a BlueID5 password, you will see a **Set Password** option instead of Change Password. This lets you create a local password for your account.

9. Managing External Logins

If you have linked your BlueID5 account to external login providers (such as GitHub or Microsoft), you can manage those connections from the **External Logins** page in your account settings.

Viewing Connected Accounts

The External Logins page shows all the external providers currently linked to your BlueID5 account, along with the date each one was connected. Go to **Manage Account** → **External Logins** to see your linked accounts at a glance.

Linking External Accounts

You can link additional social or organizational accounts to your BlueID5 account for added convenience. This lets you sign in using any of your linked providers.

1. Go to **Manage Account** → **External Logins**.
2. Under the **"Add another service"** section, click the button for the provider you want to link.
3. Authenticate with the external provider when prompted.
4. The provider will now appear in your list of connected accounts.

Organization-Managed Accounts: If your account is managed by an organization, the primary provider associated with your organization cannot be removed. It will be marked as **"Required by your organization"** on the External Logins page. You can still link additional social accounts for convenience, but the organization's provider will always remain connected.

Adding a New External Login

1. On the External Logins page, look for the **"Add another service"** section.
2. Click the button for the provider you want to link (for example, *"GitHub"*).
3. You will be redirected to that provider to authenticate. Sign in there.
4. After authentication, the provider will be linked to your BlueID5 account.

Removing an External Login

1. On the External Logins page, find the provider you want to remove under **"Connected Accounts"**.
2. Click the **Remove** button next to it.

Before removing: Make sure you still have another way to sign in (such as a password or a different external provider). If you remove all login methods, you could lose access to your account.

10. Managing Grants & Permissions

When you sign in to an application through BlueID5, that application may request access to certain information about your account (such as your name, email, or profile). The **Grants** page lets you see and control which applications currently have access.

Viewing Your Grants

1. Sign in to BlueID5 and navigate to the **Grants** page.
2. You will see a list of applications that you have authorized, along with:
 - The application name (and logo, if available)
 - When the grant was created
 - When the grant expires (if applicable)
 - What types of information the application can access

Revoking Access

If you no longer want an application to access your account information:

1. Find the application in the grants list.
2. Click the **Revoke Access** button.
3. Confirm the action when prompted.

What happens after revoking: The application will no longer be able to access your information. The next time you try to use that application, it will ask you to authorize access again. Revoking access does not delete your account with that application — it only disconnects BlueID5 from it.

11. Account Recovery

Forgot Your Password

If you cannot remember your password, you can reset it using your email address.

How to Reset Your Password

1. On the BlueID5 login page, click "**Forgot your password?**"
2. Enter your **username or email address** and click **Submit**.
3. Check your email inbox for a password reset message from BlueID5.
4. Click the reset link in the email. It will take you to a page where you can set a new password.
5. Enter your new password (following the [password requirements](#)), confirm it, and click **Reset Password**.
6. You can now sign in with your new password.

Tip: Password reset links expire after a limited time for security reasons. If the link has expired, simply request a new one by repeating the steps above.

Account Lockout Recovery

If your account has been locked due to too many failed sign-in attempts:

- **Wait a few minutes** — the lockout is temporary and will lift automatically.
- **Reset your password** — if you are unsure of your current password, use the "Forgot your password?" flow to set a new one.
- **Contact support** — if the lockout persists, reach out to your administrator or use the [support page](#).

Lost Two-Factor Authentication Device

If you have lost access to your authenticator app:

1. On the 2FA verification screen during login, look for the option to **sign in with a recovery code**.

2. Enter one of the **recovery codes** you saved when you first set up 2FA.
3. Each recovery code can only be used once.
4. After signing in, go to your account settings and either re-configure 2FA with a new device or generate new recovery codes.

No recovery codes? If you have lost both your authenticator device and your recovery codes, contact your organization's administrator or use the [support page](#) for assistance. An administrator can reset your 2FA so you can set it up again.

12. Agreements & Privacy

BlueID5 requires you to review and accept certain agreements to use the service.

Terms of Service

The Terms of Service describe the rules and conditions for using BlueID5 and associated applications. You must accept them during registration. You can review the current Terms of Service at any time from your profile page.

Privacy Notice

The Privacy Notice explains what personal information is collected, how it is used, and how it is protected. You must review it during registration. You can view it again from your profile page at any time.

When Agreements Are Updated

From time to time, the Terms of Service or Privacy Notice may be updated. When this happens:

1. The next time you sign in, you will be prompted to review and accept the updated agreements before you can continue.
2. On your profile page, you will see an alert indicating that updated agreements are available.

3. Click **Review** to read the updated document, then click **Accept** to acknowledge it.

Your profile shows your agreement history: On your profile page, under the Terms & Privacy section, you can see when you accepted each agreement and which version you accepted. If a newer version is available, a notification will appear prompting you to review and accept it.

13. Getting Support

If you need help with your BlueID5 account, there are several ways to get assistance.

Support Contact Form

BlueID5 has a built-in **Support** page where you can send a message directly to the support team.

1. Click the **Support** link (usually found in the site footer or navigation menu).
2. Fill in your name, email address, and (optionally) your company name.
3. Describe your issue or question in the message field. Be as specific as possible — include what you were trying to do, any error messages you saw, and the device or browser you are using.
4. Click **Send**.

Response times: Support response times vary by organization. You will typically receive a reply via email. Check the support page for specific information about expected response times.

Self-Service Options

Before contacting support, try these self-service options:

- **Forgot password?** — Use the [password reset](#) flow on the login page.
- **Account locked?** — Wait a few minutes for the lockout to expire, or reset your password.
- **2FA issues?** — Use a [recovery code](#) to sign in.

- **Check this guide** — The [FAQ section](#) below covers the most common issues.

14. FAQ & Troubleshooting

"I didn't receive my verification email"

- **Check your spam/junk folder.** Automated emails sometimes end up there.
- **Wait a few minutes.** Email delivery can occasionally be delayed.
- **Verify the email address.** Make sure you entered the correct email during registration. A single typo will send the email to the wrong address.
- **Request a new email.** On your profile page, if your email is unverified, you will see a **"Send verification email"** button. Click it to receive a fresh verification link.
- **Check with your IT department.** Some corporate email filters may block automated messages. Ask your IT team to allow emails from BlueID5.

"I got an email about a new sign-in"

- **Why you got it.** BlueID emails you when your account is used from a device it has not seen before.
- **If it was you,** no action is needed.
- **If it was not you,** click **This wasn't me** in the email. You are asked to confirm before anything changes. **Yes, lock my account** signs out every session and requires a password reset; **No, this was me** changes nothing.

"My account is locked"

- **Wait it out.** Account lockouts are temporary (usually a few minutes). After the lockout period ends, try again.

- **Reset your password.** If you are not sure your password is correct, use the "**Forgot your password?**" link on the login page to set a new one.
- **Contact support** if the lockout does not lift after waiting.

"I lost my 2FA device"

- **Use a recovery code.** When you set up 2FA, you were given a set of one-time recovery codes. Enter one of those codes on the 2FA screen to sign in.
- **No recovery codes?** Contact your administrator or use the [support page](#). An administrator can reset your two-factor authentication so you can set it up again with a new device.
- **Prevent this in the future.** After regaining access, immediately set up 2FA on a new device and generate new recovery codes. Store them in a safe place.

"I can't log in with my external provider"

- **Check that the provider is available.** The external provider (e.g., GitHub, Microsoft) may be experiencing an outage. Try again in a few minutes.
- **Make sure the account is linked.** If you have never used that provider with BlueID5 before, you may need to link it first from the [External Logins](#) settings page.
- **Try another login method.** If you also have a BlueID5 username and password, use those to sign in and then check your external login settings.
- **Clear your browser cookies.** Stale session data can sometimes cause issues. Clear your browser's cookies and cache, then try again.

"I forgot my password"

- Click "**Forgot your password?**" on the login page.
- Enter your username or email address, and check your inbox for the reset link.
- Follow the link to create a new password.

- See the full instructions in the [Account Recovery](#) section above.

"I'm being asked to accept new terms"

- **This is expected.** When the Terms of Service or Privacy Notice are updated, all users are required to review and accept the new versions.
- **Read and accept.** Click the link to review each updated document, then click **Accept**. You will only need to do this once per update.
- **You cannot skip this step.** Accepting the current agreements is required to continue using BlueID5.

"My authenticator code isn't working"

- **Check your device's clock.** Authenticator codes are time-based. If the date and time on your phone are incorrect, the codes will not match. Go to your phone's settings and make sure **automatic date and time** is turned on.
- **Wait for a new code.** Codes change every 30 seconds. If you entered a code right as it was about to expire, wait for the next one and try again.
- **Make sure you are using the right account.** If you have multiple accounts in your authenticator app, verify that you are reading the code for your BlueID5 account.

"I want to change my username"

- Sign in and go to your **profile page**.
- Click the **Change** button next to your username.
- Enter your new username and save.
- You may need to confirm the change before it takes effect.
- Remember to use your new username the next time you sign in.

