Blood Sector Systems

Release Notes

15 September 2024

# All Blood Sector Systems

The Blood Sector Systems have been updated on **15 September 2024.**

The following list of changes apply to all Blood Sector Systems (BloodPortal, BloodNet, BloodSTAR, ABDR, MyABDR).

## Multi Factor Authentication (MFA)

Multi Factor Authentication has been introduced for login to the Blood Sector Systems. All users are required to enter their username and password and then provide authentication by:

* Email (receive a code)
* Okta Verify App (receive a code)
* Okta Verify App (push notification)
* Phone (receive a code)

The mobile number and email used for authentication is the same as the one used for your account.

The Okta Verify Authentication App can be downloaded from the [**Google Play Store**](https://play.google.com/store/apps/details?id=com.okta.android.auth&hl=en_AU) or [**Apple Store**](https://apps.apple.com/us/app/okta-verify/id490179405). The app must be linked to your account using the QR code.

Following are some examples of the new MFA screens:









## Account access and password reset requirements

The rules for accessing Blood Sector System accounts and requirements for resetting passwords have been changed. The table below sets out the rules for when a password needs to be changed or when an account needs to be reactivated.

|  |  |
| --- | --- |
| **Account Action** | **Password reset requirements** |
| Active use | Change password every 12 months.  |
| Unused for 45 days and up to 12 months  | Reset your password on your next login. |
| After 12 months of inactivity  | Contact Blood Operations Centre on 13000 BLOOD  (1300 025 663) to have the account reactivated  |

## Password format requirements

When a new password is created or updated it will be mandatory for the password to be a minimum of 14 characters and contain lower and upper case letter. The new password requirements are shown in the screen shot below.



Updated Terms and Conditions

The Terms and Conditions for access to the Blood Sector Systems have been updated to reflect the security enhancements that have been made to the systems through this release. Users will be required to accept the Terms and Conditions on their first login after any update.

The new terms and conditions are located at <https://www.blood.gov.au/bloodportal-terms-and-conditions-use>.

Accept Terms and Conditions on each login

Users will be required to accept the new Terms and Conditions on each login to the Blood Sector Systems through the BloodPortal.



## Advice on password reset page

New advice has been added to the BloodPortal password reset page to inform users that they must use the email address linked to their account regardless of whether they have a new email. New wording as follows:

*Provide the email or username last linked to your account. If your email has changed you can update it when you are logged in. You can choose to receive a verification code by email or SMS. If you need support, please contact the Blood Operations Centre on 13 000 BLOOD (13 000 25663).*



## Updates to the error messages for duplicate account creation

When a user attempts to create a new account with a username, email or mobile number that are already associated with an account they will be shown a new message to recover their existing account rather than creating a duplicate. The new messages are:

Username Duplicate:

*This username is already registered to a BloodPortal account. If you have lost access to your account please contact support to recover this on 13 000 BLOOD (13 000 25663). Otherwise, please choose another username.*

Email Duplicate:

*This email address is already registered to a BloodPortal account. If you have lost access to your account please contact support to recover this on 13 000 BLOOD (13 000 25663).*

Mobile Number Duplicate:

*This mobile number is already registered to a BloodPortal account. If you have lost access to your account please contact support to recover this on 13 000 BLOOD (13 000 25663).*



# BloodSTAR Release 3.12

BloodSTAR version 3.12 has been released on **15 September 2024.** The following is a list of the updates to BloodSTAR.

## Auto suspension of users with AHPRA credentials changes

When a user’s AHPRA registration status changes to unregistered, the system will automatically deactivate the user’s roles. The following deactivation reason will be displayed on the access history table on the My Access Request screen:

*Deactivated due to AHPRA registration change. Contact AHPRA for further details.*



## New fields for AHPRA matching

When a user creates a New Role Access Request and enters their AHPRA number, they will be shown the following details related to that AHPRA number; *Full Name, Specialities, Date of First Registration, Place of Practice*.

The user will be required to select a checkbox under these details to confirm that the AHPRA details are correct and belong to the user.



## AHPRA name matching

AHPRA check must confirm that the name held in BloodSTAR (access request) matches exactly the name on the AHPRA registration.

When a user creates a New Role Access Request and enters their AHPRA number, they will be shown the following message if their BloodPortal name details do not match the AHPRA registration name details: **AHPRA details for <AHPRA registration number> do not match your BloodPortal account.**  Given Name, middle name and family name must match exactly. Check AHPRA number or correct your blood portal details to proceed.

The user will be required to update their name details in BloodPortal before proceeding with an access request for BloodSTAR.

NOTE: Users will still be required to confirm their AHPRA registration details as outlined above.



# MyABDR (Web and mobile app) Release <release number>

MyABDR App version <release number> has been released on **15 September 2024.** The following is a list of the updates to MyABDR App.

## Multi Factor Authentication

Multi Factor Authentication has been introduced to login to the MyABDR website and mobile application. Users are required to enter their email address and password and then provide authentication by:

* Email (receive a code)
* Okta Verify App (receive a code)
* Okta Verify App (push notification)
* Phone (receive a code)

The mobile number and email used for authentication is the same as the one used for your account.

The Okta Verify Authentication App can be downloaded from the [**Google Play Store**](https://play.google.com/store/apps/details?id=com.okta.android.auth&hl=en_AU) or [**Apple Store**](https://apps.apple.com/us/app/okta-verify/id490179405). The app must be linked to your account using the QR code.

Following are some examples of the new MFA screens for MyABDR web and MyABDR mobile app:





## Removal of login PIN

With the introduction of Multi-Factor Authentication users will no longer have the option of logging into the MyABDR mobile app with a PIN in place of their email address and password.

Users will be required to enter their email address and password along with a verification code each time they login.