Veeva Clinical Vault

External End User login instruction
via Microsoft Entra External ID



TABLE OF CONTENTS

Click a section title to navigate to the relevant section

First-Time Registration

Logging in to AZ VCV After Initial Registration

Frequently Asked Questions (FAQ)

First time registration

During your first sign-in through Microsoft Entra External ID, you will need to create a password and configure a second authentication factor, which is required to access the AZ VCV application. Detailed step-by-step instructions are provided.

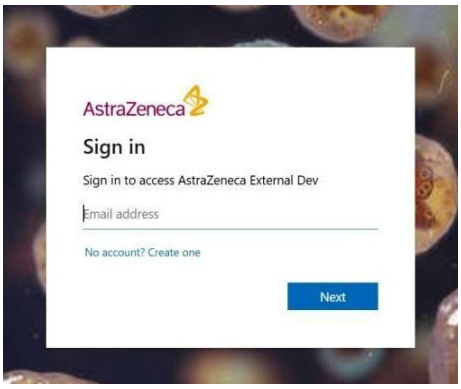
1. Open Veeva Clinical Vault using the provided URL. Then click the purple access button.



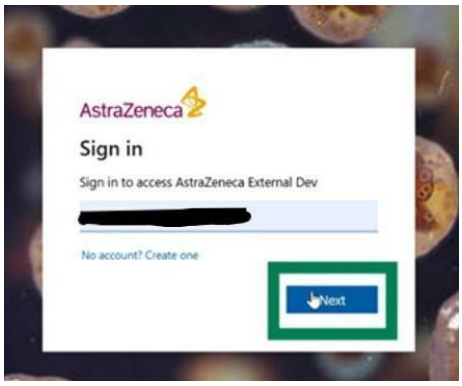
2. Click “Entra External login” button.



3. You will be redirected to the Microsoft Entra External ID sign-in page.



4. Enter your company email address used during account request, then click “Next”.



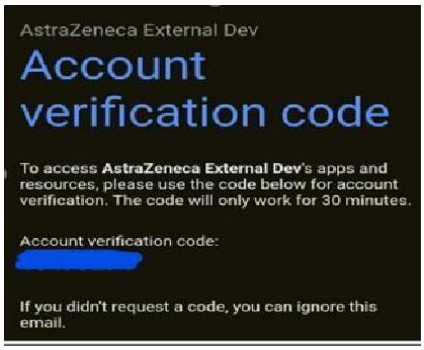
5. During your first login, you must set up password. Click “**Forget password?**” as highlighted below.



6. Click “**Email code”** button to receive a verification code at your registered email address.



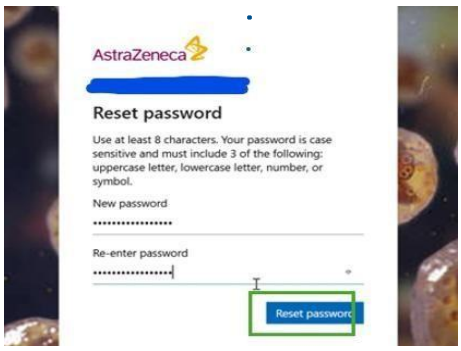
7. A verification code will be sent to your registered email address to confirm your identity.



8. Enter the verification code, then click “Verify”.



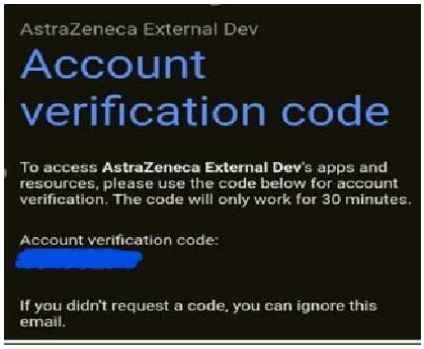
9. Set up your password by entering a new password, then re-enter it to confirm. Click “Reset Password”.



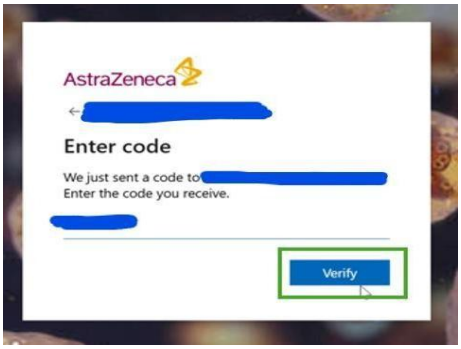
10. Click “Next” to continue.



11. A second verification code will be sent to your registered email address to enable login.



12. Enter the verification code, then click “Verify” to log in.



13. On the “Stay signed in?” prompt, select Yes or No,



14. Upon successful verification, you will be authenticated and redirected to the VCV application.

Note: Select **Yes** to keep your browser session active and reduce repeated sign-in prompts. To end the session completely, select **Sign out** or clear your browser cookies.

Logging in to AZ VCV After Initial Registration

After completing your initial registration, sign in to AstraZeneca Veeva Clinical Vault using your registered email address and password. You will also be required to complete multifactor authentication using a verification code sent to your registered email address.

1. Open Veeva Clinical Vault using the provided URL. Then click the purple access button.



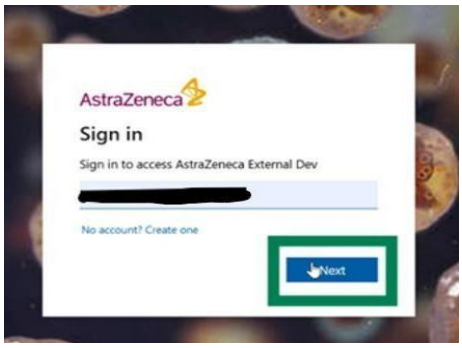
2. Click “Entra External login” button.



3. You will be redirected to the Microsoft Entra External ID sign-in page.



4. Enter your registered email address, then click “Next”.



5. Enter your password, then click “Sign in.”



6. To complete multifactor authentication, click “Email code” to receive a one-time passcode at your registered email address.



7. Enter the one-time passcode you received, then click “Verify.”



8. After successful verification, you will be authenticated and redirected to the AZ VCV application.

Frequently Asked Questions (FAQ)

Q1. I can't sign in even though my password is correct. What could be wrong?

Your account may have been disabled for one of the following reasons:

- Security concerns
- Account inactivity
- Policy or compliance requirements

To request account reinstatement, contact your application support team.

Q2. Is my account deleted if it's disabled?

No. A disabled account remains in the **Microsoft Entra External ID** platform for historical tracking and can be re-enabled upon request. Disabling an account is reversible, whereas deletion is permanent. Contact your administrator for more information.

Q3. What happens to my existing sessions if my account is disabled?

You can continue using your current session until it expires, unless an administrator immediately locks the session. Once the session expires or is locked, you will not be able to sign in.

Q4. My account shows "Your account has been temporarily locked," or I can't sign in after multiple password attempts. What should I do?

After multiple unsuccessful sign-in attempts, you may receive a temporary lockout message. Microsoft Entra External ID uses **Smart Lockout** to help protect accounts from unauthorized access and password-guessing attempts.
By default:

- Accounts are temporarily locked after **10 unsuccessful sign-in attempts**.
- Additional unsuccessful attempts may trigger another lockout period.
- The initial lockout period is typically **one minute** and may increase after subsequent failed attempts.
- The duration of subsequent lockout periods varies and is determined automatically by Microsoft security controls.

If your account is temporarily locked:

- Stop attempting to sign in with the same password.
- Select **Forgot password** on the sign-in page.
- Verify your identity using your registered email address.
- Create a new password.
- Complete MFA verification if prompted.
- Sign in again using your new password.

Note: Repeated sign-in attempts with an incorrect password may extend the lockout period. If you continue to experience issues after resetting your password, contact your application support team.

