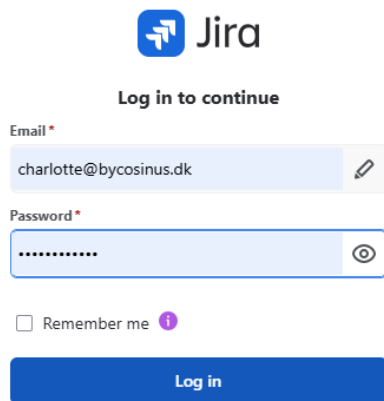


Choosing an authentication method for Atlassian Cloud

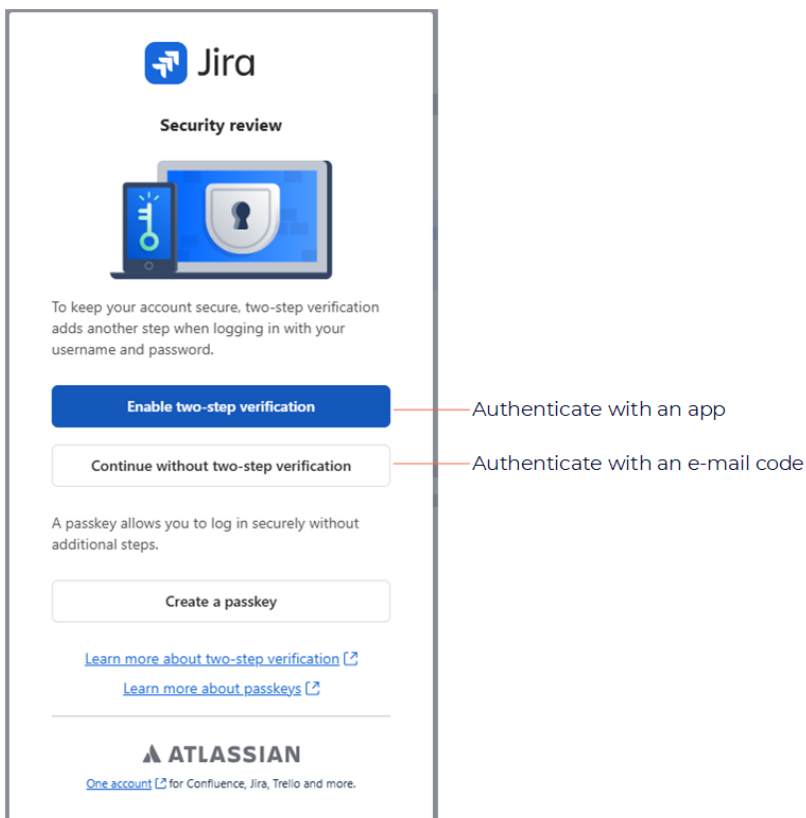
To help protect your account, Stibo DX requires an additional verification step when you sign in to Atlassian Cloud applications. The first time you sign in to an Atlassian Cloud application, you must choose an authentication method.

After entering your credentials:



The image shows the Jira login interface. At the top is the Jira logo. Below it is the text "Log in to continue". There are two input fields: "Email" with the value "charlotte@bycosinus.dk" and "Password" with masked characters. Below the password field is a checkbox labeled "Remember me" with an information icon. At the bottom is a blue "Log in" button.

You are prompted to select an authentication method for future sign-ins:



The image shows the Jira "Security review" screen. It features the Jira logo and the title "Security review". Below the title is an illustration of a smartphone and a laptop, both displaying a key icon. The text explains that two-step verification adds an extra step for security. There are three main options: "Enable two-step verification" (highlighted with a red line pointing to the text "Authenticate with an app"), "Continue without two-step verification" (highlighted with a red line pointing to the text "Authenticate with an e-mail code"), and "Create a passkey". At the bottom, there are links to "Learn more about two-step verification" and "Learn more about passkeys", followed by the Atlassian logo and a link to "One account" for Confluence, Jira, Trello, and more.

Enable two-step verification

If you click **Enable two-step verification**, you are prompted to select a two-step verification method:

Two-step verification methods

Select from one of the methods to set up your two-step verification.

**Authenticator app**
An authenticator app generates a verification code for you to complete two-step verification. →

**Security key**
A security key can be physical hardware device or software that allows you to use a fingerprint, face identity or screen lock to prove that it's really you. →

 Limited security option

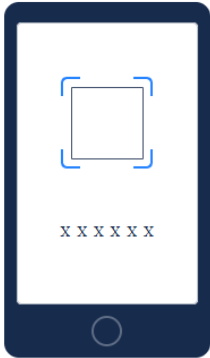
Selecting **Authenticator app** opens a page where you can configure the app and connect it to your mobile device:

 **Connect phone**

 Save recovery key

1. Scan this QR code with your verification app

Once your app reads the QR code, you'll get a 6-digit code.



 Can't scan the code?

2. Enter the 6-digit code here

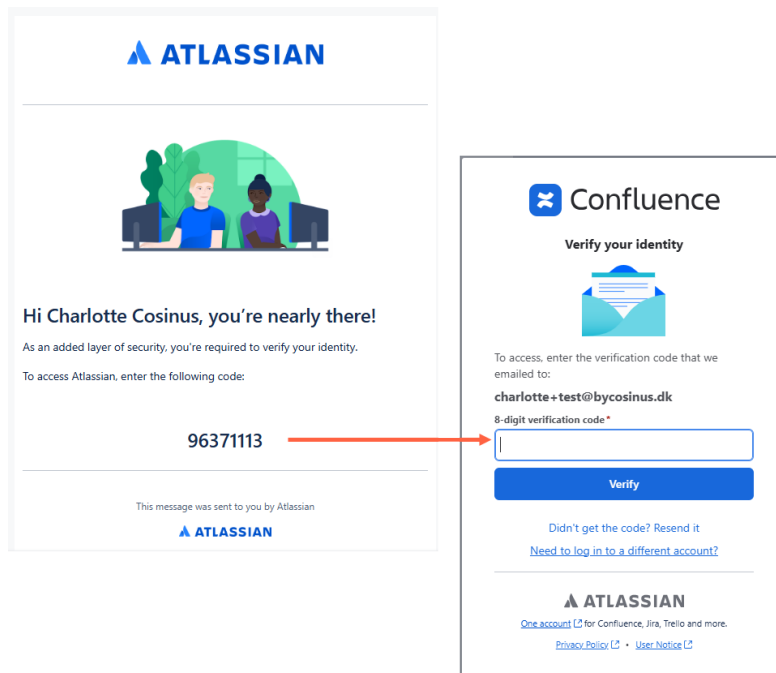
Enter the code from the app below. Once connected, we'll remember your phone so you can use it each time you log in.

6-digit code

Continue without two-step verification – Email Authentication

Because Stibo DX requires an additional verification step when signing in to Atlassian Cloud applications, you cannot continue without configuring an authentication method. Clicking **Continue without two-step verification** configures email-based verification.

Each time you sign in to an Atlassian Cloud application, you must enter a verification code that is sent to your email address:



Customers Using Single Sign-On (SSO)

If your organization **already** uses Atlassian Cloud and has configured single **sign-on (SSO)** and/or **two-factor authentication (2FA)** through a third-party identity provider such as Okta or Microsoft Entra ID, that identity provider will handle authentication when you sign in to the Stibo DX Atlassian Cloud environment.

If you experience sign-in issues or have questions about the authentication process, contact your organization's Atlassian administrator. In this scenario, authentication is managed by your organization's identity provider rather than by Stibo DX..