

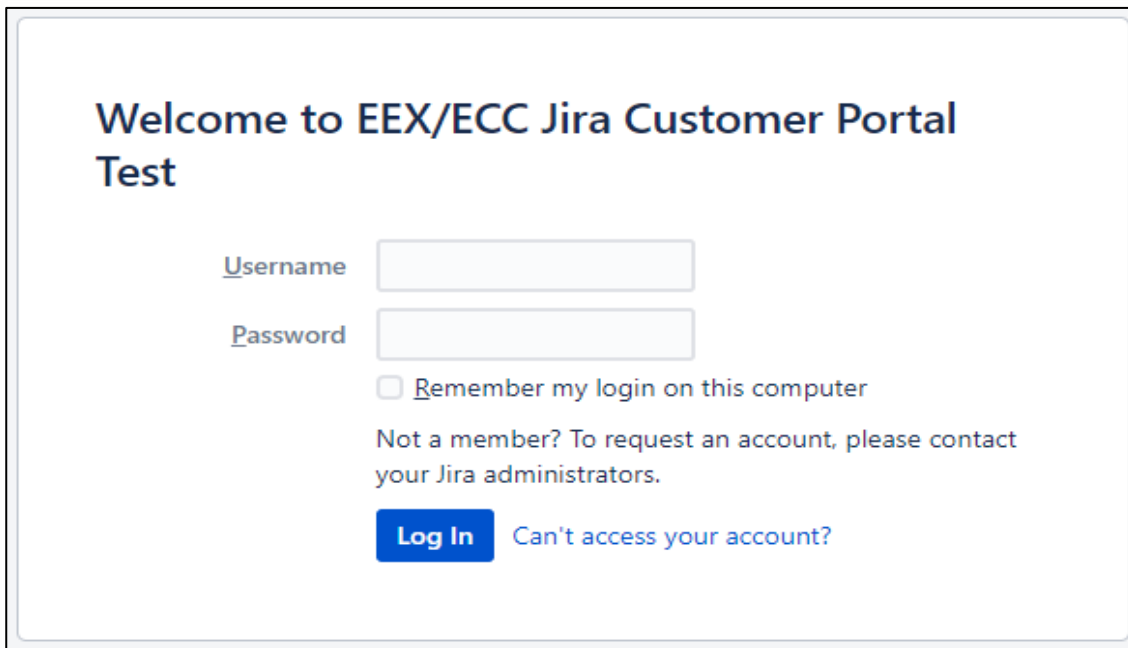
User guide for accessing Jira Customer Portal

EEX Group
07.11.2025
Leipzig

To access your customer portal account, please visit <https://customerportal.eex.com/> and follow the steps described below.

1.	Login with Jira Customer Portal login credentials	3
2.	Configure the 2-Factor Authentication	5
2.1	Mobile Authenticator app	6
2.2	Web Authentication as a 2FA method	6
2.3	Authentication by OTP via e-mail	8

1. Login with Jira Customer Portal login credentials



Welcome to EEX/ECC Jira Customer Portal
Test

Username

Password

Remember my login on this computer

Not a member? To request an account, please contact your Jira administrators.

[Can't access your account?](#)

1. Visit the following link: <https://customerportal.eex.com/>
2. Your username is derived from your first name and last name in the format: **firstname.lastname**
3. To access your password, please click on “**Can't access your account?**”
4. Afterwards, please enter your username in the Username field as shown in the example below and click **OK**. You will then receive a password reset link at the email address associated with your user account.

Can't access your account?

i If you can't access Jira, fill in this form and an email will be sent to you with the details to access your account again.

Which did you forget Password Username

Username*

Note: Please do not enter your email address in the **Username** field.

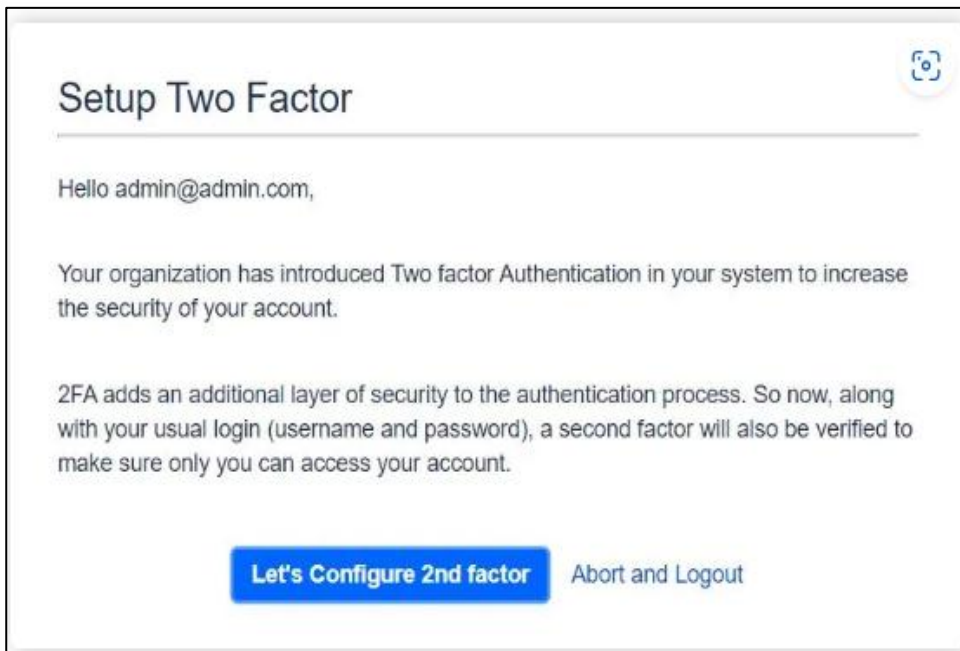
Once your password has been successfully reset, configure the second factor authentication. The procedure for setting up 2FA is described in the following paragraph.

If the password reset fails, please contact us at: exg_ts_customer_portal@eex.com .

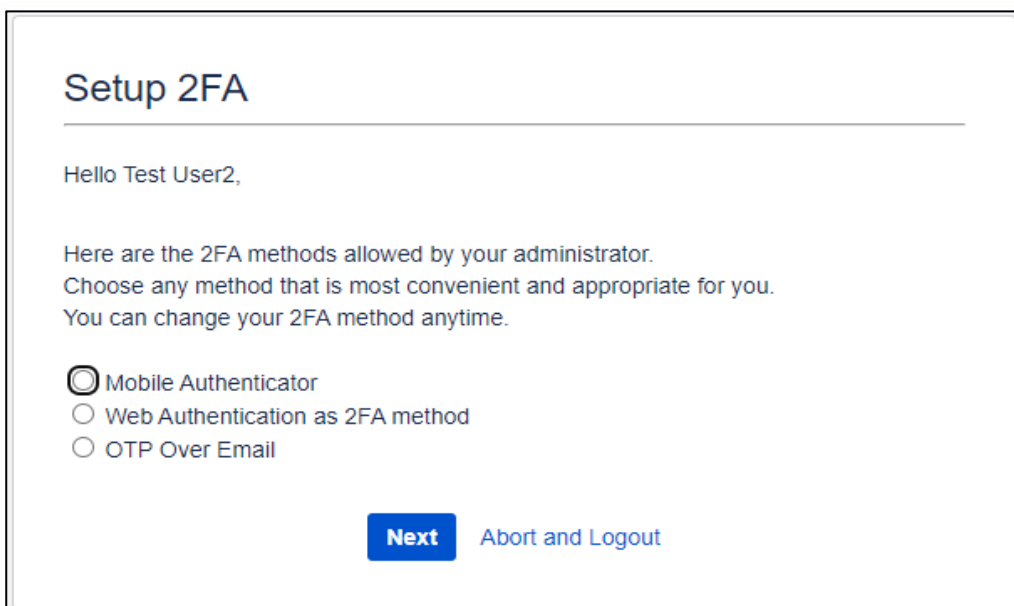
We will then provide you with your initial login information via Brainloop.

2. Configure the 2-Factor Authentication

The following screen explains how to configure Two-Factor authentication methods.

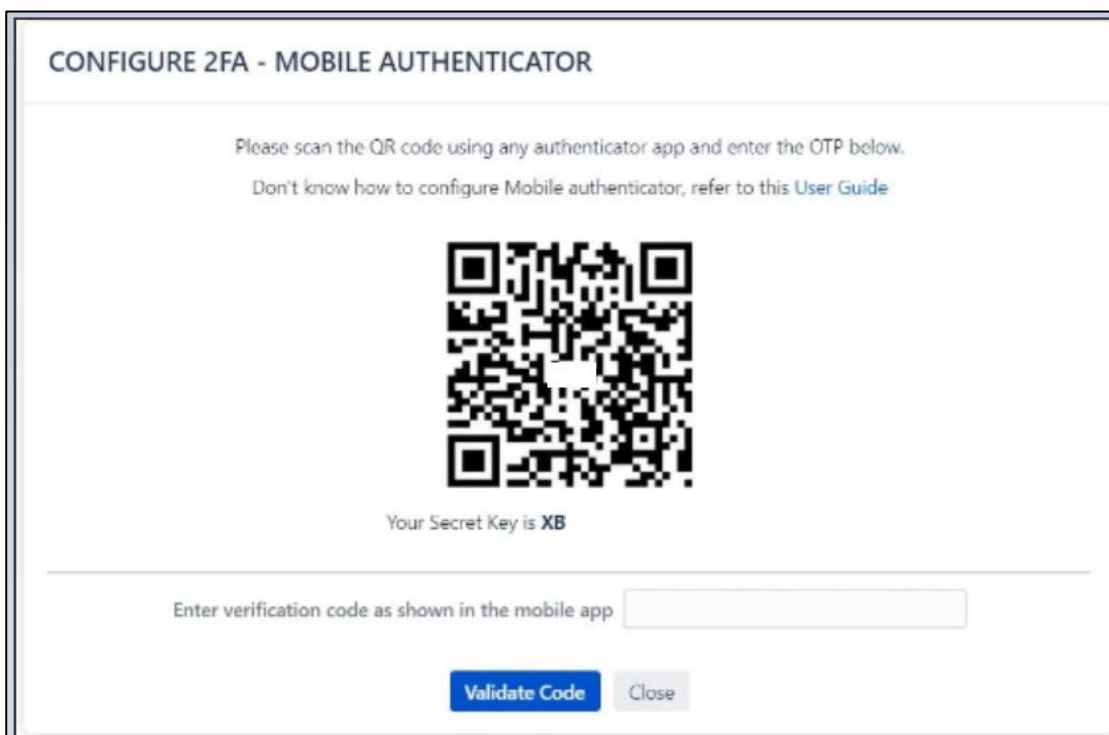


After selecting Let's Configure 2nd factor, you need to choose between the 3 available two-factor methods.



2.1 Mobile Authenticator app

The screen below will appear when configuring Mobile Authenticator as a two-factor method. You need to scan the QR code or use the Secret Key and then enter the 6-digit one-time password generated on mobile app. To scan the QR code, please install the **Mobile Authenticator app** on your phone.

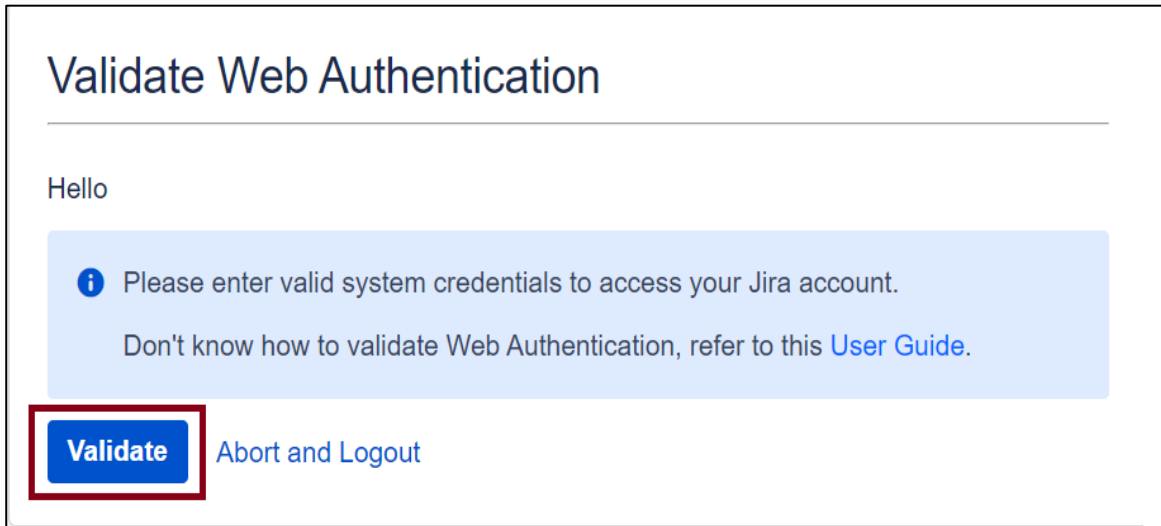


2.2 Web Authentication as a 2FA method

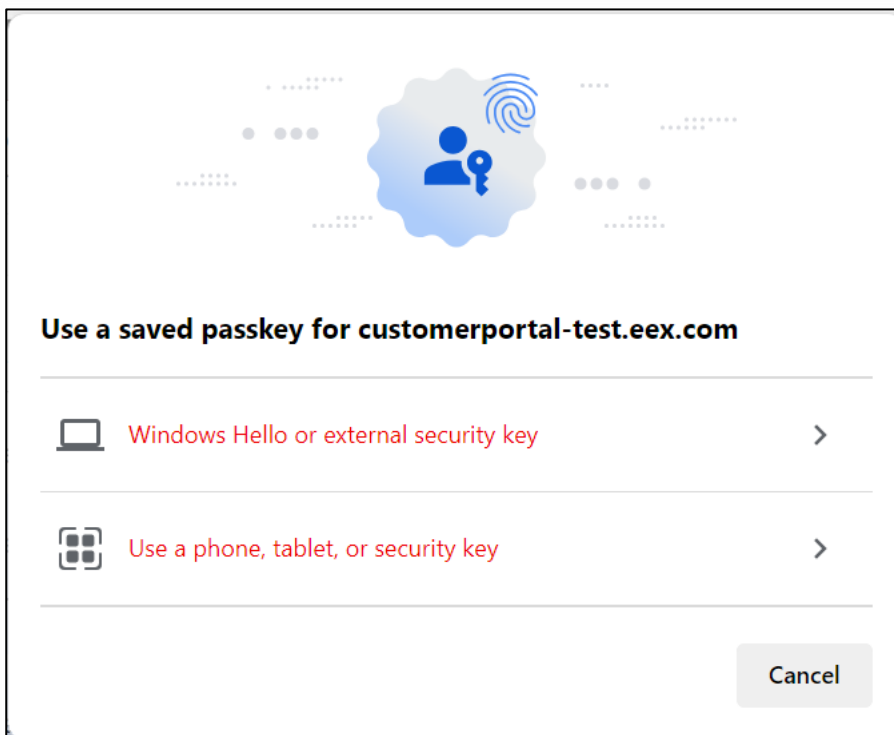
Configuring Web Authentication as a two-factor method allows you to use a system's built-in authenticators like Window's Hello PIN, Apple's Touch ID, Face ID or any other biometric authenticators as a second factor to login into your Jira Customer Portal account.

You need to register the system authenticator you use, like Window's Hello PIN, Apple's Touch ID or other biometric authenticators that support your use of the customer portal.

This allows the authenticator to be used for validation of the two-factor authentication.



The screen below shows the two-factor system authenticators that are available.



For example, after clicking on Windows Hello, you will be prompted to enter the Hello Pin.

2.3 Authentication by OTP via e-mail

After selecting this option, you will receive an authentication pin by e-mail. This must be entered into the OTP field and validated as displayed below.

Configure OTP Over Email

Hello

An OTP(one time pass-code) has been sent to your registered email address.
Enter the OTP in the text box given below to verify your identity.

If you haven't received the OTP yet, please click on Resend OTP link.

Enter OTP received on email Resend OTP

Abort and Logout

If the above steps have been carried out correctly, access to the Jira Customer Portal will be successful.

We have tested the accessibility from the Internet intensively and ensured the function. If you face connection issues, please check with your local IT in your organization the following points:

- Antivirus
- Firewall/Proxy Settings
- Whitelisting of the URL/IP address