Two Factor Authentication

Last Modified on 05/04/2026 9:45 pm IDT

This article is designated for all users.

About

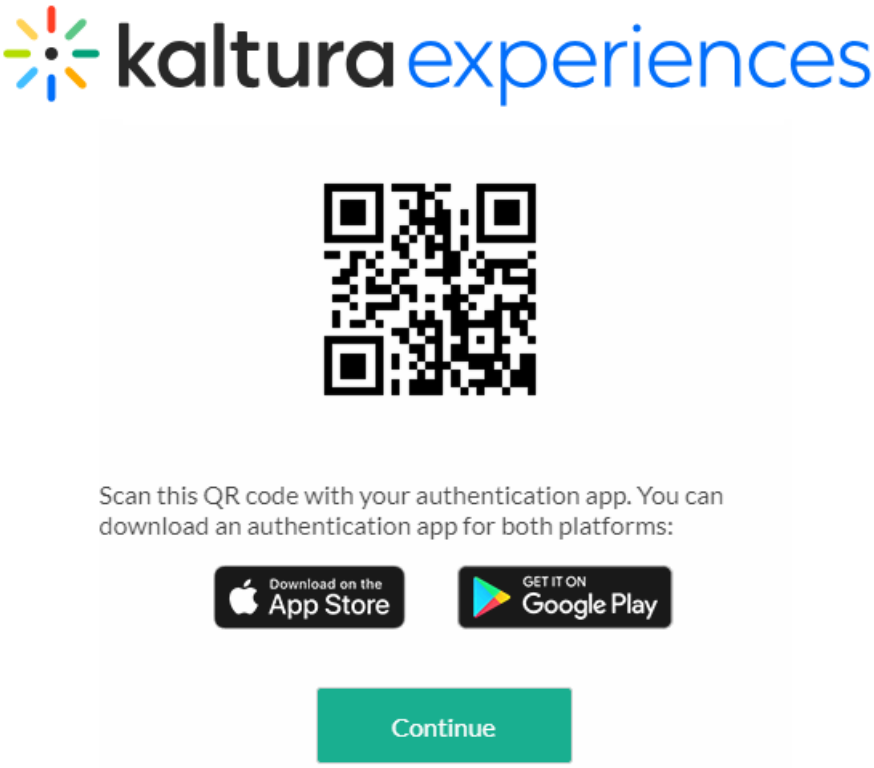
The information in this article is intended for customers that have accounts that are enabled with Two Factor Authentication (2FA). Contact your Kaltura representative to enable this feature. After 2FA is enabled on your account, an email is sent to the account owner (and all registered Kaltura experiences users of this account). The email contains a link that directs to the Kaltura experiences Authentication-QR-code Screen.

The Kaltura experiences Authentication Screen

The Kaltura experiences Authentication Screen includes a one-time-use QR code that needs to be scanned using the Google Authenticator (or any other authenticator application available on your device)

To Proceed With 2FA

1. Scan the code. By scanning the code, your Kaltura experiences credentials (email and password) will be paired with the authenticator application that supplies a re-generating code that you will need to login to Kaltura experiences. (Google Authenticator is available for both Android and iOS devices. If is not installed on your device, use the links to Google Play Store and Apple’s App Store on the Kaltura experiences Authentication Screen.)

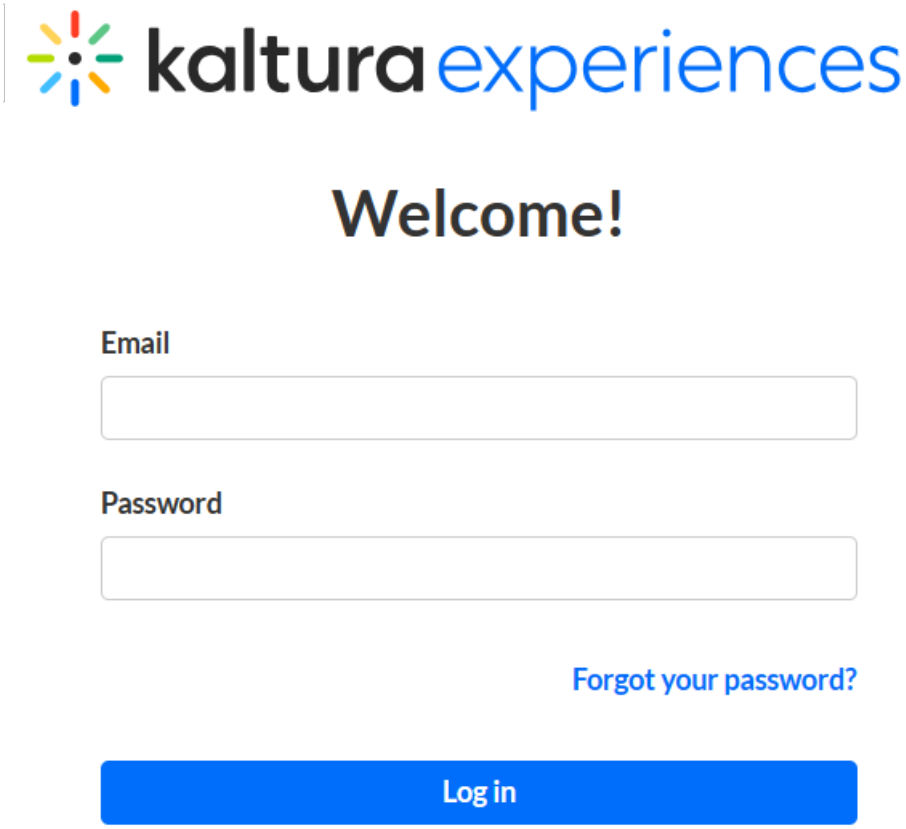


2. Click **Continue** and proceed to the Kaltura experiences Login Screen.

To login to Kaltura experiences Using 2FA

The initial login screen is the same for all accounts.

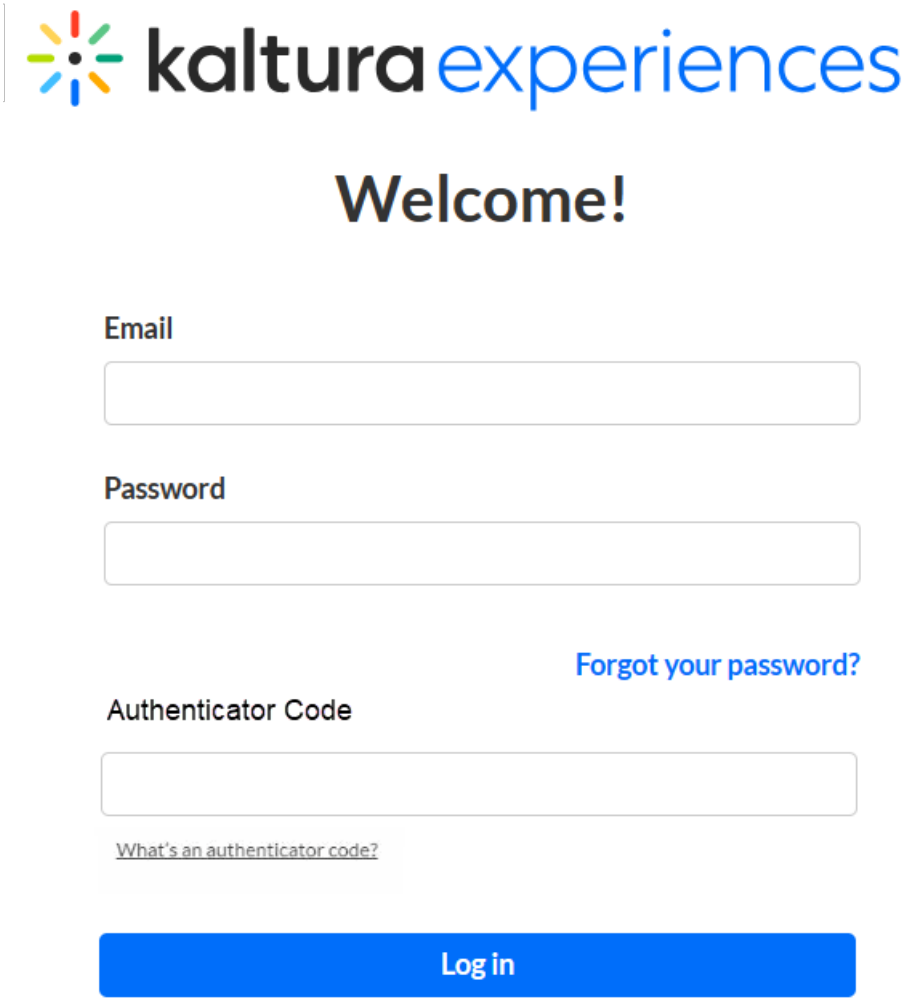
1. Enter your email and password and click Login.



When 2FA is enabled, the screen expands and includes a field for the Authenticator Code. This code will be required for every login session to this specific account.

If you scanned the QR code previously, your authenticator app is set to provide your authentication code whenever you need it to login.

2. Enter the authenticator code and click Log in.



If you reset your password, a new QR code will be provided via the reset password email that will be sent to you. You will need to perform the 2FA set up process again by scanning the new QR code.

If your credentials are used to access more than one account, when you want to switch to an account that has 2FA enabled, you will need to log out and login using the authenticator code.

Troubleshooting

When 2FA authentication is enabled for the account (for admins, Kaltura experiences users), if a user did not use the QR code that they received within 24 hours, it is no longer valid. The QR code expires after 24 hours.

The workaround is to use the Forgot Password link to produce a new QR code.

1. Go to Kaltura Events https://eventplatform.kaltura.com/login.
2. Click “Forgot Password” and enter your email address.
   The users will receive an email from Kaltura with a password reset link:
3. Use the link to set a new password. The message “Your new password has been set...” is displayed.
4. MANDATORY: Click OK.
5. The user will be prompted with a new QR code to scan by their mobile Authenticator app.

⚠
Please note that every time the password is reset a new QR code is generated, and the previous QR code becomes irrelevant.