

KMC 2 Factor Authentication

This information is intended for customers that have accounts that are enabled with 2 Factor Authentication. Contact your Kaltura representative to enable this feature.

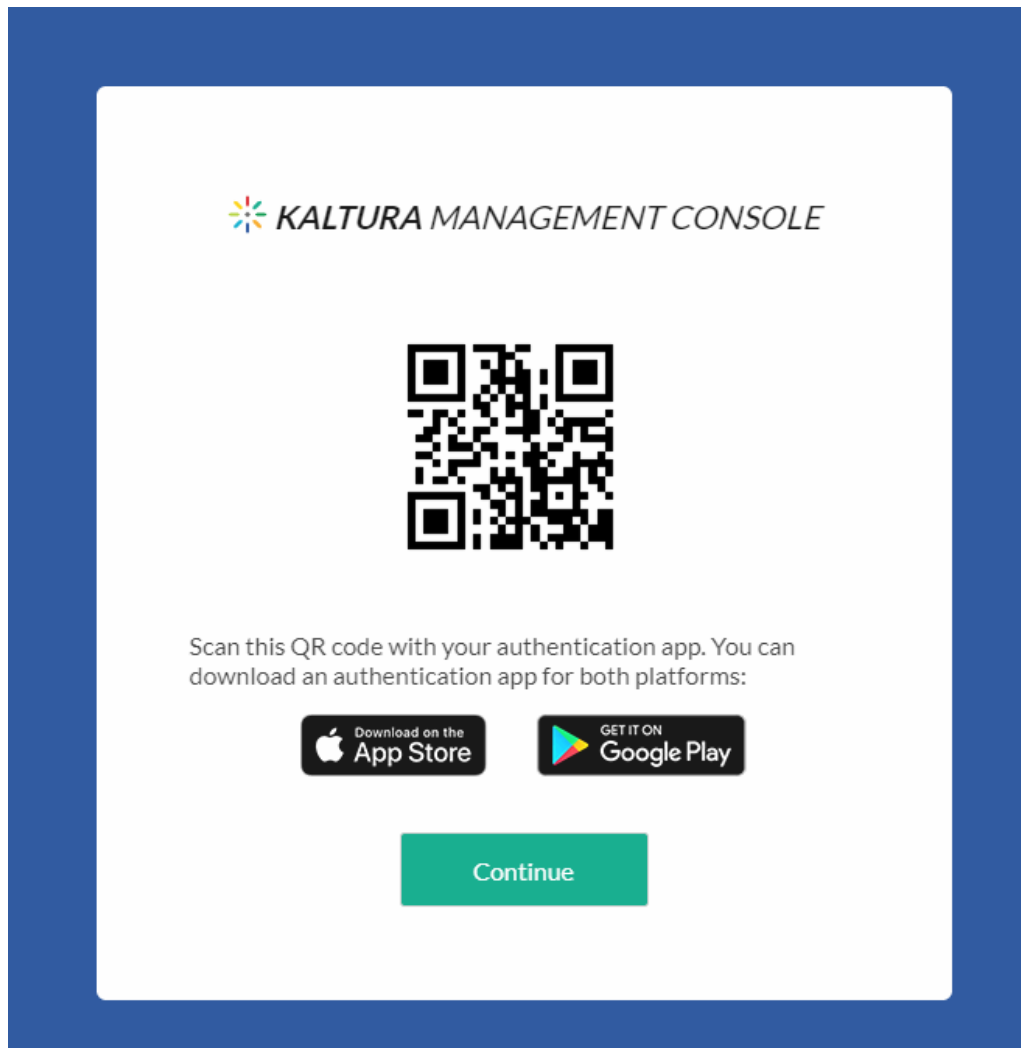
After 2 Factor Authentication (2FA) is enabled on your account, an email is sent to the account owner (and all registered KMC users of this account). The email contains a link that directs to the KMC Authentication-QR-code Screen.

The KMC Authentication Screen

The KMC 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 KMC credentials (email and password) will be paired with the authenticator application that supplies a re-generating code that you will need to login to KMC.
2. (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 KMC Authentication Screen.)

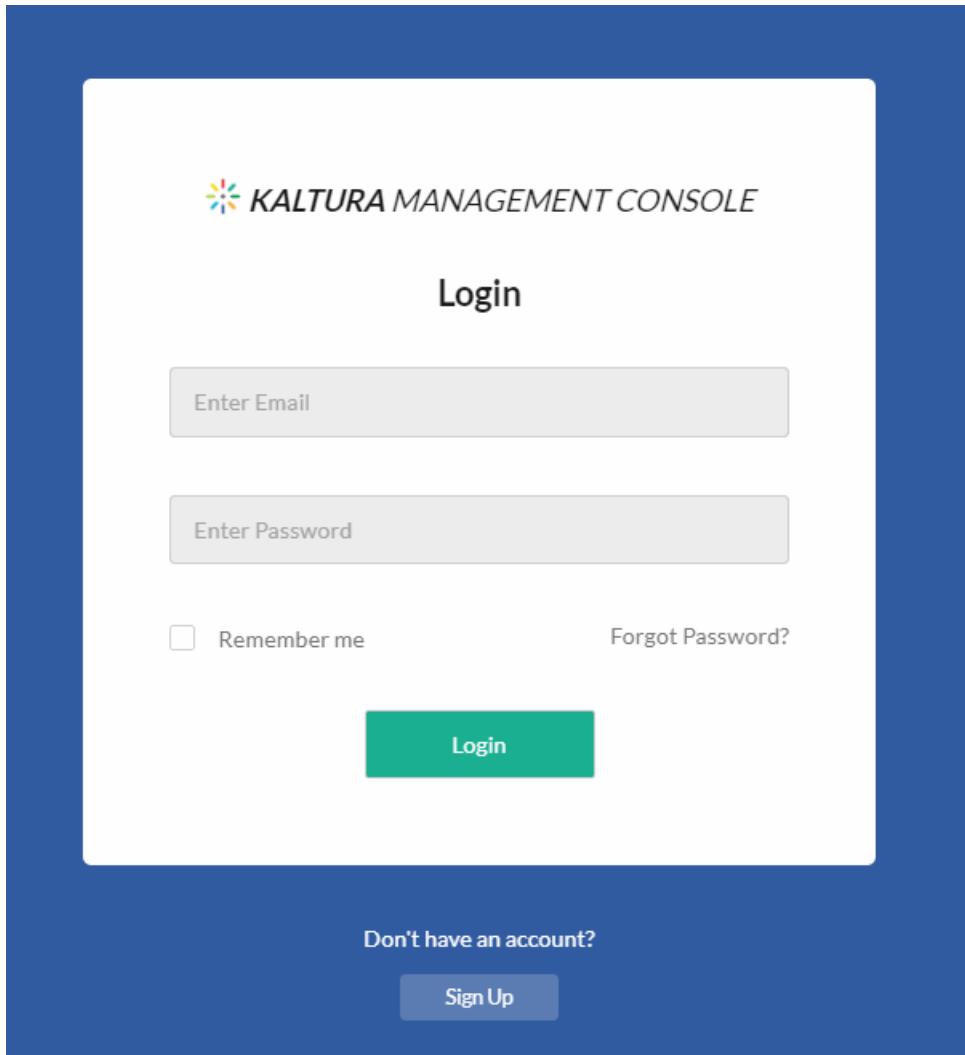


3. Click Continue and proceed to the KMC Login Screen.

To Login to the KMC Using 2 Factor Authentication

The initial login screen is the same for all accounts.

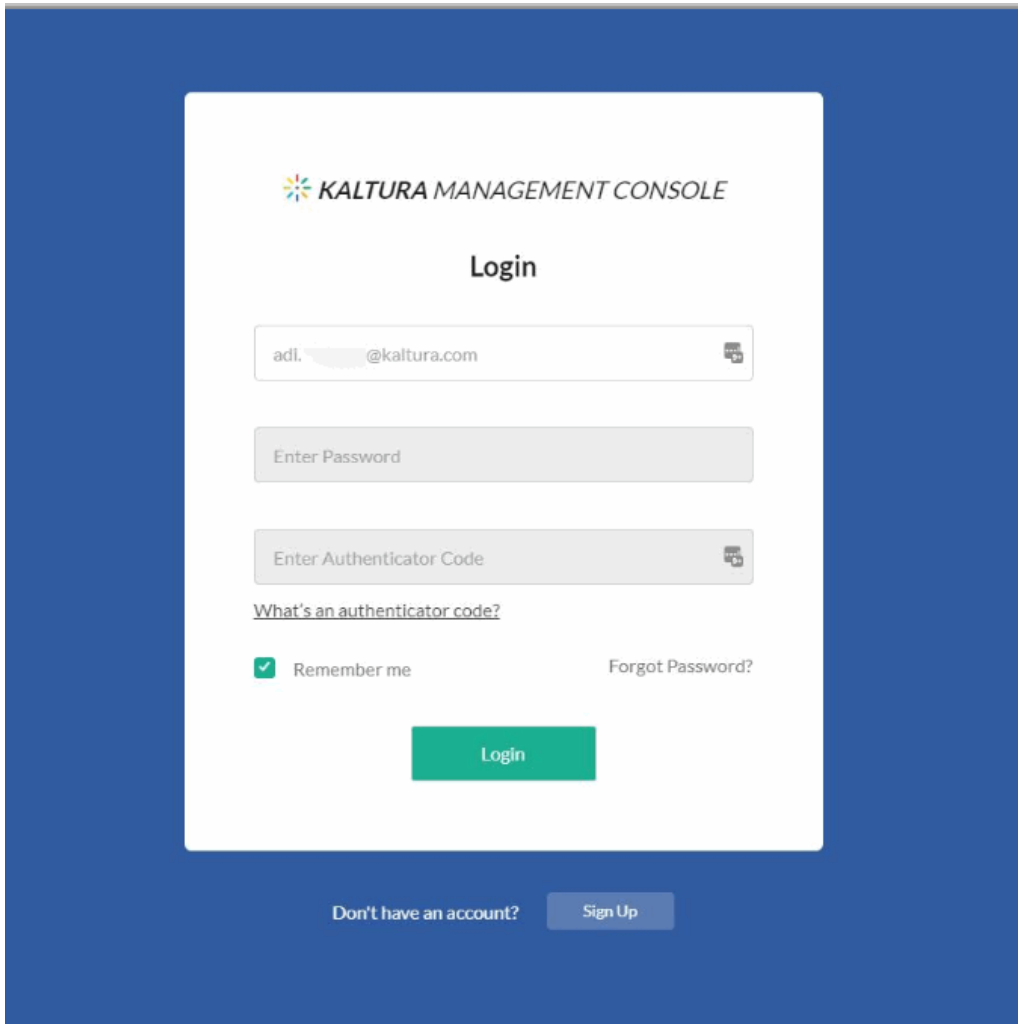
1. Enter your email and password and click Login.

The image shows a login interface for the Kaltura Management Console. It features a blue background with a white central panel. At the top of the panel is the Kaltura logo followed by the text "KALTURA MANAGEMENT CONSOLE". Below this is the word "Login" in a bold, black font. There are two input fields: "Enter Email" and "Enter Password", both with light gray borders. Below the email field is a checkbox labeled "Remember me". To the right of the password field is a link that says "Forgot Password?". A green "Login" button is centered below these elements. At the bottom of the white panel, there is a link "Don't have an account?" and a blue "Sign Up" button.

When 2 Factor Authentication 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 Login.



⚠ 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, KMC 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 KMC <https://kmc.kaltura.com/index.php/kmcng/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.

[template("cat-subscribe")]
