Multi-factor authentication

To reduce the chances of unauthorized access, Redis Enterprise Cloud allows users to enable multi-factor authentication (MFA).

When MFA is enabled, users must enter their username, password, and an authentication code when logging in. MFA requires a mobile device that can receive these authentication codes over text messaging. In addition, you may use an authenticator app such as Google Authenticator as one of your factors.

To further increase the security of the account, the account owner can require MFA enforcement for all users.

Enabling MFA for a user account

Each user can enable and configure MFA for their account. The default MFA configuration sends an authentication code by text message that users must enter when they log in.

To configure MFA for your user account:

1. Log in to your account.
2. From the Redis Enterprise Cloud menu, click on your name to enter the User Profile view.
3. Under your user profile, click Multi-Factor Authentication.
4. From the Multi-Factor Authentication view, click Activate Now.
5. Enter your mobile phone number.
6. You will receive a confirmation code sent by text message. Enter the code and click Verify.

Your account is now configured for MFA.

Note: We recommend that you also configure MFA for an authenticator app as an additional factor.

If you cannot log in to your account because of MFA, please contact support.

If your mobile phone is lost or stolen, make sure that you update the MFA configuration to prevent unauthorized logins.

Changing your MFA phone number

To change the mobile phone number used for MFA:

1. Navigate to the Multi-Factor Authentication view.
2. Click Configure.
3. Enter the new mobile phone number, and complete the verification process as described above.

Configuring MFA for an authenticator app

After you configure MFA for text messages, you can also configure MFA to work with a Time-based One-Time Password (TOTP) app such as Google Authenticator.

When you log in to the Redis Cloud Admin Console, you can select either an authentication code sent by text message or an authentication code shown in your authenticator app.

To configure MFA for an authenticator app:
1. Install an authenticator app on your mobile phone.

2. Add Redis Cloud to the app:
   1. From the User Profile view in your Redis Cloud account, click Multi-Factor Authentication.
   2. Click Configure for the authenticator app. A QR code will appear on screen requesting verification.
   3. Scan the QR code using your phone’s authenticator app.
   4. Enter the code generated by your authenticator app to verify the setup.

You can now use either a text message code or an authenticator app code as your second factor when logging in.

### Deactivating MFA

You can deactivate MFA for your user account. To deactivate MFA, go to your profile, click Multi-Factor Authentication, and click Deactivate.

### Enforcing MFA for all user accounts

Account owner users can enable MFA enforcement for all users in their account. After MFA is enforced for the account, all users who do not have MFA enabled will be required to configure MFA the next time they log in to the Redis Cloud Admin Console.

To enable MFA enforcement for all user accounts:

1. Log in as an account owner.
2. Go to Settings > Account.
3. Under MFA enforcement, click the toggle.

- When you enable MFA enforcement, users cannot disable MFA for their account.
- When you disable MFA enforcement, users can disable MFA for their account.

Tip - We recommend that you notify all of your Redis Cloud Admin Console users before enabling MFA enforcement.

**Updated:** January 12, 2022