Two-factor authentication (2FA)

Vodafone Business Surveillance Knowledge Base Article

The future is exciting. Ready?
Contents

1.1 Introduction 3
1.2 Setting Up Two-factor authentication (2FA) on the server 3
1.3 Server Login 3
1.4 Setting up Two-factor authentication (2FA) on Mobile Client 4
1.5 Mobile Login 4
1.6 Setting up Two-factor authentication (2FA) on Desktop Client 5
1.7 Desktop Login 5
1.1 Introduction

Two-factor authentication (2FA) is a second layer of security to protect an account or system. Users must go through two layers of security before being granted access to an account or system.

2FA is enabled as a mandatory authentication option for all user accounts. For the first-time login process, user account needs to linked to a TOTP (Time-based One-time Passwords) generator app. Google Authenticator is suitable for iOS/Android/windows and is a recommended authenticator app, but most standard 2FA apps can be used. Below sections explains step by step process setting up 2FA on the server and clients.

Please note that the journeys may slightly differ depending on how your administrator has set up your account.

1.2 Setting Up Two-factor authentication (2FA) on the server

1.3 Server Login
1.4 Setting up Two-factor authentication (2FA) on Mobile Client

1. Click "add system" and enter the server address.
2. Log in using credentials provided by your administration.
3. Verify the server key and click continue.
4. Change your password by entering current and a new password twice.
5. Click yes to begin setting up 2FA.
6. You can use many authentication apps with Vodafone Business Surveillance. If you are not currently one, we recommend installing Google Authenticator, MaxiSafe, or Yubikey.
7. If you do not wish to use a new method, you can use your Google Authenticator app.
8. Log in using your credentials.
9. Either scan or select manual entry and then enter the OTP that your application provides.
10. Note these single use backup codes.
11. Return to the mobile client to continue to log in.

1.5 Mobile Login

TIP: You can use your device's multitasking feature to flick between apps.

Log in using your credentials.

Open your authenticator app and check the latest OTP listed. Type this passcode in here and click next.

Your are now successfully logged in.
1.6 Setting up Two-factor authentication (2FA) on Desktop Client

1. Click “add system” and enter the server address.
2. Log in using credentials provided by your administrator.
3. Verify the server key and click continue.
4. Change your password by entering your current and a new password twice.
5. Click to open the link in a web browser.

7. Either scan the QR code or enter the OTP that your application provides.
8. Either scan the QR code or enter the OTP that your application provides.
9. Either scan the QR code or enter the OTP that your application provides.
10. Note these single use backup codes.
11. Return to the desktop client to continue to log in.

1.7 Desktop Login

Log in using your credentials.
Open your authenticator app on your mobile and check the latest OTP listed, type this password in here and click next.
If you can not do this, you can use one of your single use backup codes by clicking on back up code.
Your are now successfully logged in.