Configure two-factor authentication (2FA) with SALESmanago

Contents

1. What is 2FA and why is it crucial for security?

Two-factor authentication (2FA) is a security mechanism whereby a user is required to follow a two-step verification process to access their account:

- Step 1 is the provision of conventional login credentials (login/email and password).
- Step 2 is the provision of a short-lived code delivered to the user's mobile device.

2FA adds an extra layer of defense against unauthorized access to your data and operations, which could result in malicious activities.

In a world where cyber threats are increasingly sophisticated, relying solely on passwords for account protection is no longer sufficient, making 2FA indispensable if you want to ensure maximum security for your digital resources. This two-stage process not only minimizes the risks associated with common threats, such as password theft and phishing attacks, but also makes it significantly harder for attackers to compromise accounts through brute-force methods.

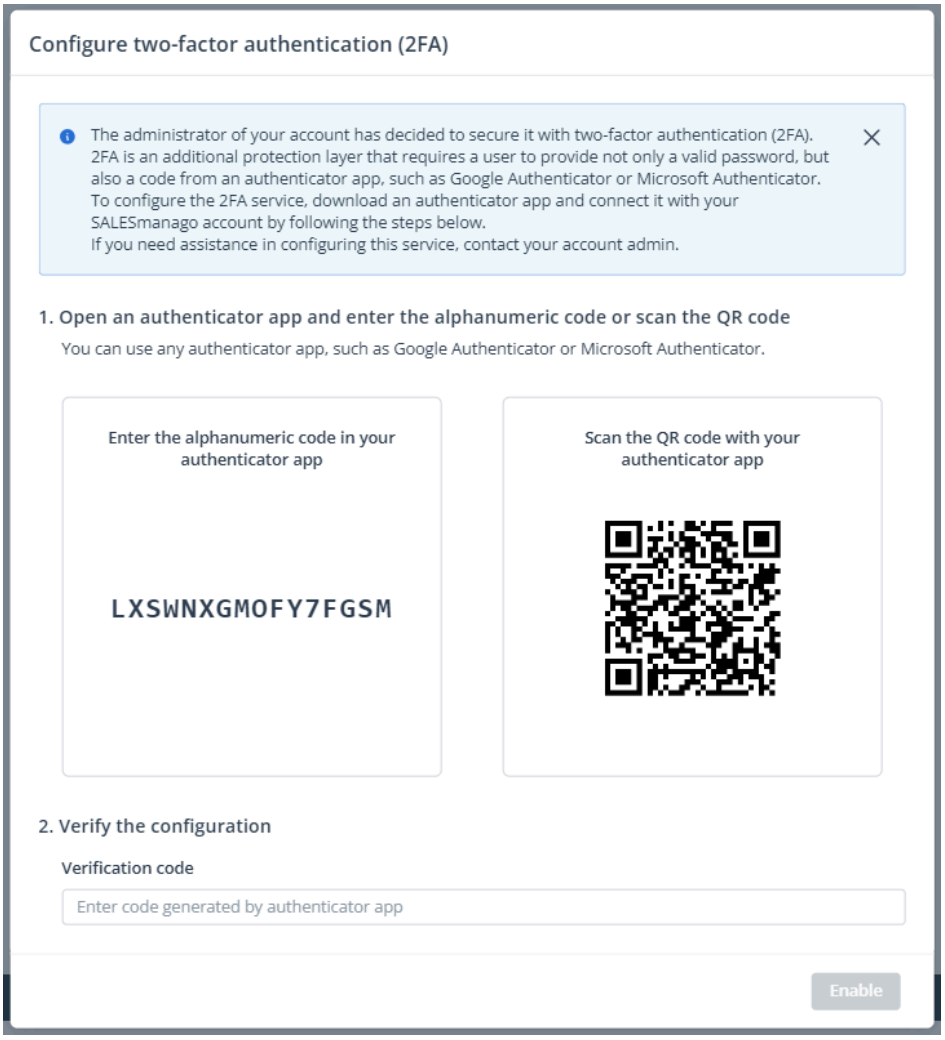
With 2FA, even if one authentication factor (the password) is compromised, the additional layer of verification (the code delivered to your mobile device by SMS or via an authenticator app) ensures that unauthorized access remains a big challenge.

By implementing 2FA, you increase the overall security of your account, safeguarding sensitive information from potential breaches and ensuring peace of mind for you, your team, and your entire company.

2. Configuring 2FA

Two-factor authentication is easy to set up—you only need your SALESmanago credentials and your smartphone.

If the administrator of your SALESmanago account has activated two-factor authentication for you, you will see the following message, asking you to configure the second step of the authentication process:



This can happen either during your ongoing SALESmanago session or the next time you try to log in.

The message provides step-by-step instructions, which are described in more detail on the following pages of this document.

Step 1. Connect your SALESmanago account with an authenticator app

To configure 2FA for your account, you need to download an authenticator application onto your smartphone and link it to your SALESmanago account.

> An **authenticator app** is a type of software that enables you to implement and use two-factor authentication (2FA). It generates a time-sensitive, usually six-digit code, known as a Time-based One-Time Password (TOTP), which must be entered during the login process in addition to the conventional login details.

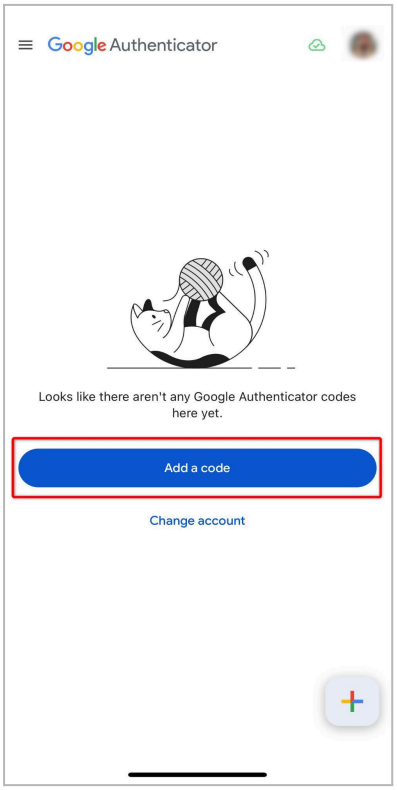
Your Organization will probably instruct you as to which app you should download. The authenticator apps recommended by SALESmanago are Google Authenticator and Microsoft Authenticator. Below, you will find a detailed guide for both.

A. Instructions for Google Authenticator

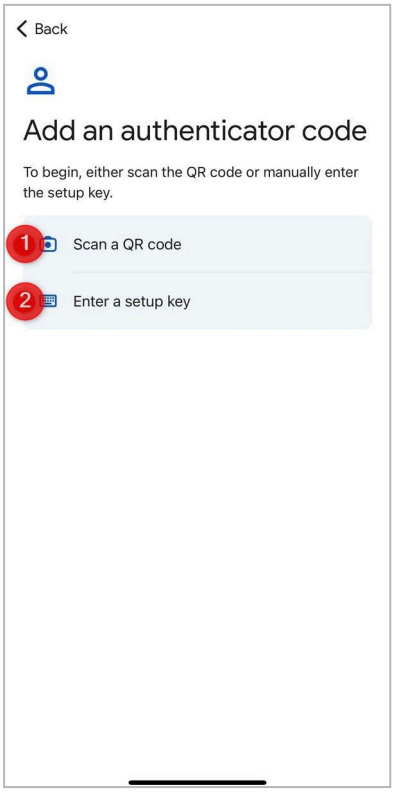
On your smartphone, go to the Apple Store or Google Play Store and download the Google Authenticator app.

Open the app and click **Get started**. You will see the following screen:

Depending on the instructions from your Organization, either select your Google Workspace account from the list and click **Continue as... [1]**, or click **Use Authenticator without an account [2]**.



If you are using the application for the first time, you will have no codes on the list. Click **Add a code** to connect Google Authenticator with your SALESmanago account and start generating TOTP codes required for your login process.



You can link Google Authenticator to your SALESmanago account in two ways:

- by **scanning your individual QR code [1]** or
- by **entering your individual setup key [2]**.

Both the QR code and the setup key (“alphanumeric code”) are provided in the message displayed on the SALESmanago platform, prompting you to configure 2FA (see page 3 above).

IMPORTANT: Never save the QR code or the alphanumeric code in any form, in particular:

- Do not take photos or screenshots of the codes
- Do not print the codes
- Do not write down the alphanumeric code
- Do not scan the codes with any app other than the authenticator app

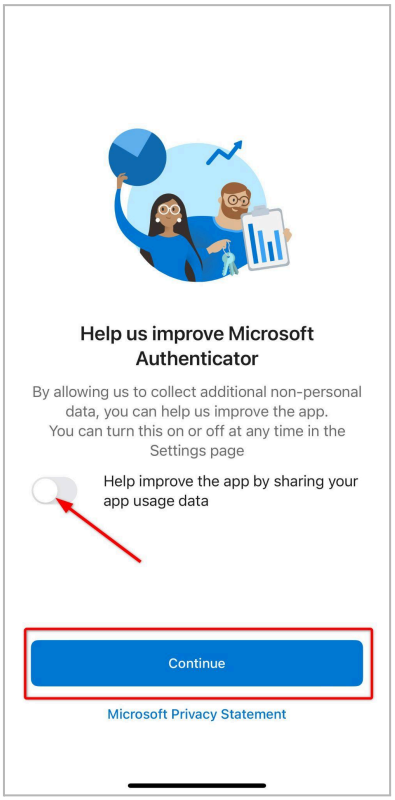
All of the abovementioned actions are considered a breach of security.

Whichever method you choose, the app will return a **verification code** that must be entered in SALESmanago. To complete the configuration, **proceed to Step 2** (page 12 below).

B. Instructions for Microsoft Authenticator

On your smartphone, go to the Apple Store or Google Play Store and download the Microsoft Authenticator app.

Open the app and click **Accept** to confirm the terms and conditions. Next, make sure that the toggle for sharing your app usage data is turned off.

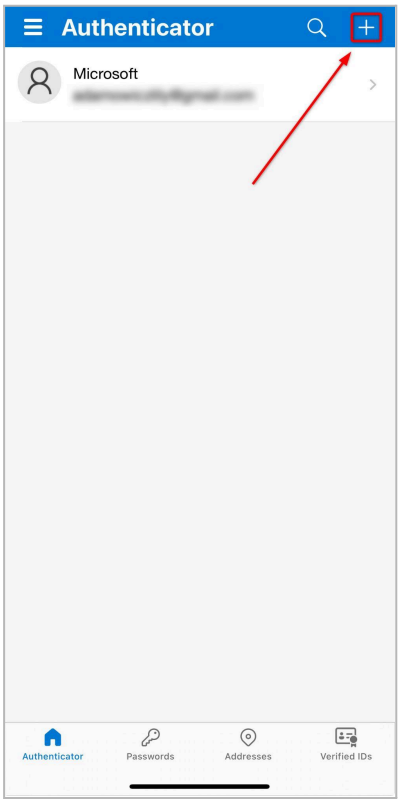


Click **Continue**.

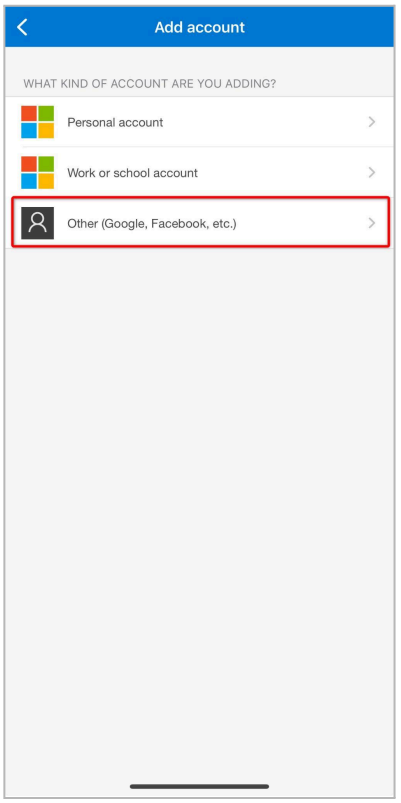
Next, click **Scan a QR code** [**1**].

You will be asked if you allow the app to take pictures and record videos. Click **Allow** to be able to scan the QR code.

NOTE: If you already have another service connected with Microsoft Authenticator, you will see a slightly different screen. In this case:

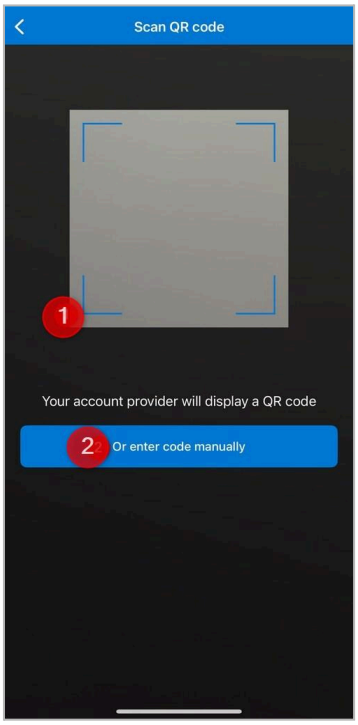


[1] Click the **plus icon** to connect Microsoft Authenticator with your SALESmanago account and start generating TOTP codes required for your login process.



[2] Select the account type: **Other (Google, Facebook, etc.)**.

At this stage, you will see the following screen:



Scan your individual QR code [1] or **manually enter your individual alphanumeric code [2]** to link Microsoft Authenticator to your SALESmanago account.

Both the QR code and the alphanumeric code are provided in the message displayed on the SALESmanago platform, prompting you to configure 2FA (see page 3 above).

IMPORTANT: Never save the QR code or the alphanumeric code in any form, in particular:

- Do not take photos or screenshots of the codes
- Do not print the codes
- Do not write down the alphanumeric code
- Do not scan the codes with any app other than the authenticator app

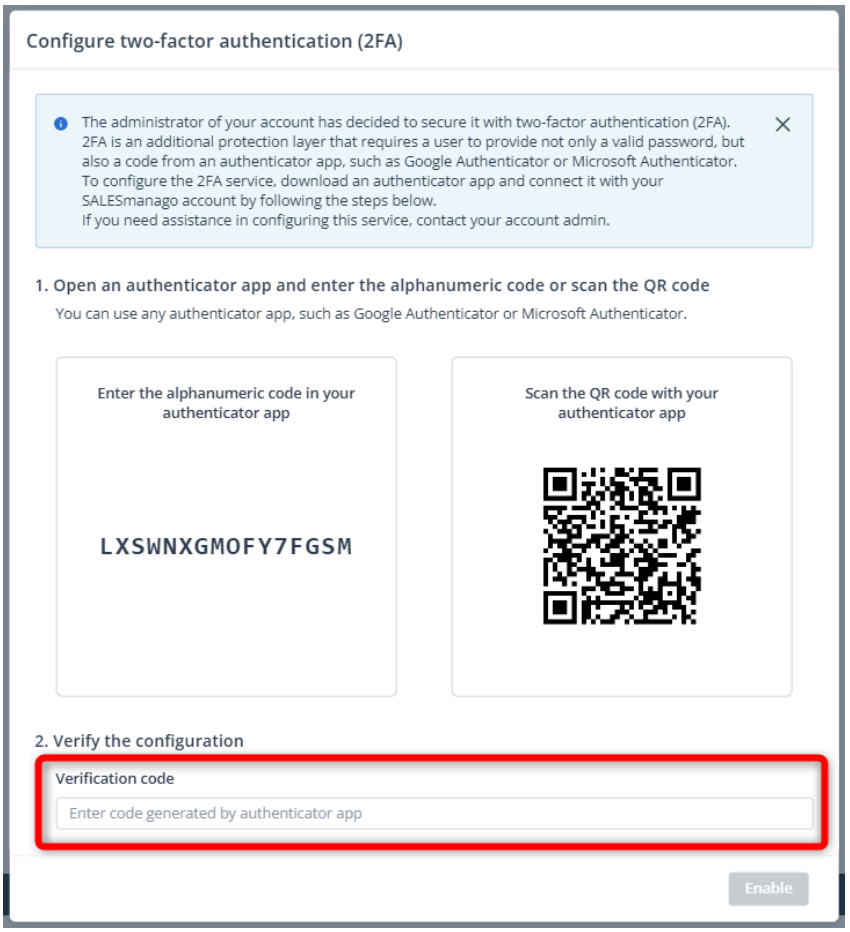
All of the abovementioned actions are considered a breach of security.

Whichever method you choose, the app will return a **verification code** that must be entered in SALESmanago. To complete the configuration, **proceed to Step 2** (page 13 below).

Step 2. Generate the first code for your SALESmanago account

At this stage, confirm the configuration performed in the authenticator app and complete the connection between the app and your SALESmanago account.

When you scanned the QR code or manually entered the alphanumeric code in the authenticator app, the app returned a verification code. This code must now be entered on the SALESmanago platform, in the following field:

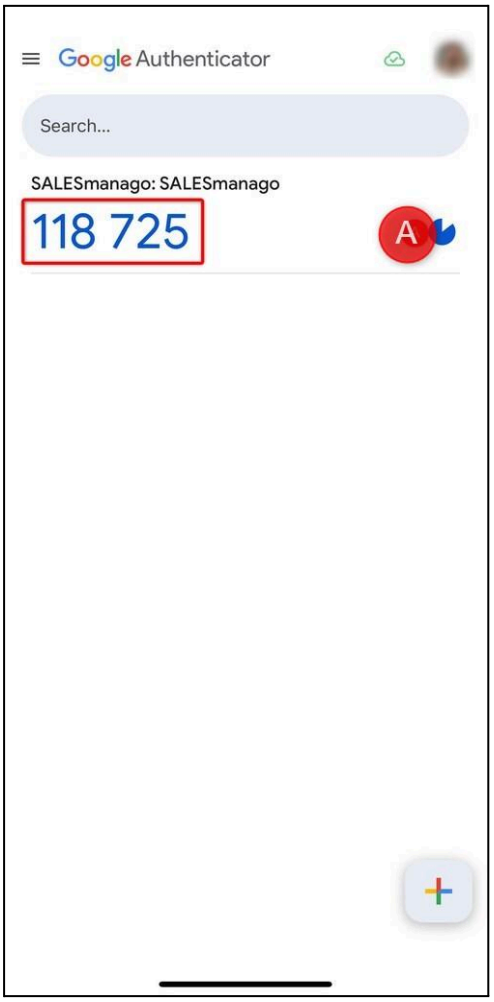


After entering the verification code displayed in your authenticator app in this field, click **Enable.**

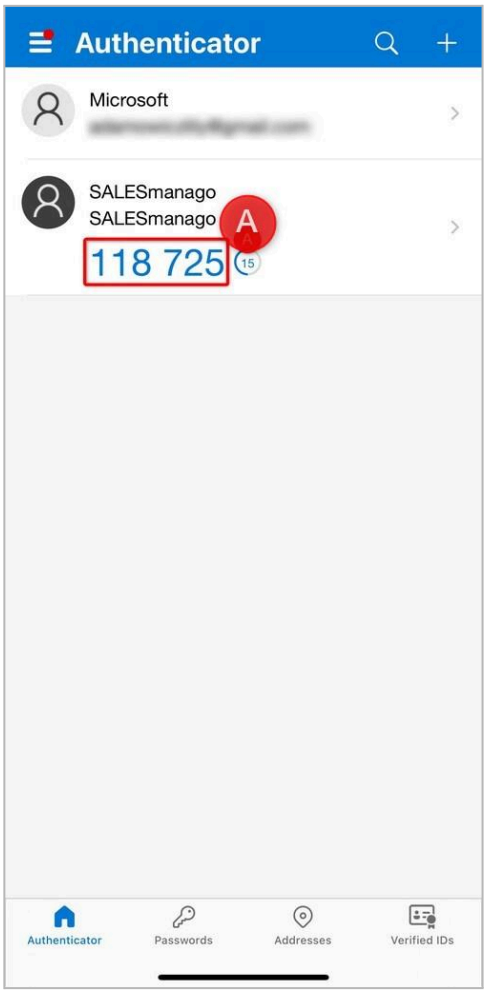
Your SALESmanago account is now successfully connected with the authenticator app. Now, **proceed to the login process** (see Step 3 below).

Step 3. Log into your SALESmanago account

Following the configuration performed in Steps 1 and 2 above, the authenticator app will start displaying short-lived codes, as demonstrated in the screenshots below.



Code displayed in Google Authenticator



Code displayed in Microsoft Authenticator

Note that the code will be accompanied by an icon showing how much time remains until the code expires [**A**]. Make sure to use the currently displayed code during the login process. If you see that the code will remain valid for a few seconds only, consider waiting for the next one.

When logging in to your SALESmanago account, you will see the following screen:

Enter the currently displayed code in field **[1]** and click **Log in [2]**—and that's it! You have successfully accessed your account.

You will be asked for a code each time you log into your SALESmanago account.

3. Q&A

What should I do if I lose my smartphone?

Contact the SALESmanago account administrator within your Organization.

Can I opt out of 2FA on my account?

The decision to activate or deactivate 2FA (either for individual users or all users) is made by the SALESmango account administrator within your Organization.

Can I disable 2FA on my account?

2FA can only be disabled by the SALESmango account administrator within your Organization.

Can I use other apps for 2FA?

Yes, this is possible, however, Google Authenticator or Microsoft Authenticator are highly recommended.

Do all team members need to use the same authenticator app?

This depends on the policy of your Organization. If you haven't received any instructions, we recommend installing either Google Authenticator or Microsoft Authenticator.

Does the Authenticator app work offline?

Yes, there is no need for internet or GSM connection.

Can I see the QR code again to set up 2FA for another device?

No, this is not possible. To configure 2FA again on a different device, contact the SALESmanago account administrator within your Organization.

If you have any questions or doubts concerning

the configuration of 2FA, please contact us at:

support@salesmanago.com