

Two factor authentication Guide

HR & salary online

deJong&Laan

Table of Contents

1. Explanation of Two-Factor Authentication	2
2. Installing the Visma Authenticator App	3
3. Resetting the Authenticator App	5

1 Explanation of Two-factor authentication

You do not want unauthorized parties to be able to access your data in HR & Payroll Online. Understandably so. Two-Factor Authentication (2FA) provides an additional layer of security, even if your password somehow becomes known to someone else. In this guide, we explain how to install the app, connect it to your Visma Connect account, and use it when signing in.

Install the dedicated app

With two-factor authentication, you receive either a 2FA push notification on your mobile device or a 6-digit authentication code that you can use when signing in to your account, depending on the method you choose. In section 2.1, you will find instructions for installing the Visma Authenticator app on an Android or iOS device (iPhone).

Activating two-factor authentication

After installing the app, activate two-factor authentication by adding your account to the Visma Authenticator app. Instructions for doing this can be found in section 2.2.

If you have multiple accounts in HR & Payroll Online—for example, because you work for multiple companies or have both an employee login and a manager login—please read section 2.4.

You can choose between the official Visma Authenticator app and an alternative authenticator app (such as Google Authenticator or Microsoft Authenticator). The major advantage of the Visma Authenticator app is that it allows you to approve sign-in attempts through a push notification, eliminating the need to manually enter 6-digit authentication codes.

This guide covers only the installation and setup of the Visma Authenticator app.

2 Installing the Visma Authenticator app

If you would like to install the Visma Authenticator app on your phone, follow the steps below..

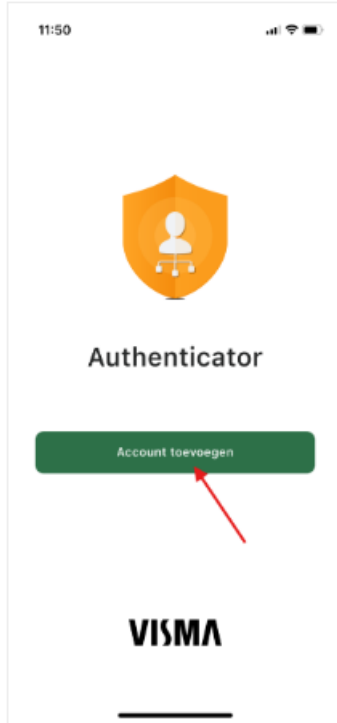
2.1 Installing the Visma Authenticator app

The Visma Authenticator app can be downloaded free of charge from the App Store (iOS) or the Google Play Store (Android). Search for "Visma Authenticator" and install the app on your phone.



2.2 Linking to Your Visma Connect account

1 Open the Visma Authenticator app on your phone and tap "Add account".



2 Choose "Sign in" and sign in with your Visma Connect account.

3 Signing in to the Visma Authenticator app automatically enables two-factor authentication (2FA) for your account.

4 Allow the Authenticator app to send notifications if you would like to use the push notification feature.

If you later prefer to enter authentication codes manually instead of receiving push notifications, you can disable notifications for the Visma Authenticator app in your phone's general settings.

The setup is now complete. Your Visma Connect account is linked to the Visma Authenticator app.

2.3 Signing in with the Visma Authenticator app

From now on, whenever you sign in to Nmbrs (via a web browser or the mobile app), you will need your phone to complete the verification step.

Follow these steps:

1. Enter your email address and password on the sign-in screen.
2. You will be prompted to provide a verification code.
3. Open the Visma Authenticator app on your phone.
4. Enter the six-digit code displayed in the app on the sign-in screen and click "Confirm".

If push notifications are enabled, you will not be asked to enter a six-digit code. Instead, you will be prompted to respond to the push notification generated by the Authenticator app.

2.4 Multiple logins with the same Email adress

You may have multiple accounts in the Visma Authenticator app. For example, you may work for multiple companies or have both a manager account and an employee account. Two-factor authentication must be configured separately for each account.

For your second account, repeat the steps described in section 2.2.

The Visma Authenticator app will now display two accounts. Each time you switch between accounts, you will need to either approve the push notification or enter the corresponding six-digit verification code.

2 Resetting the Authenticator app

2.1 No longer have access to my Authenticator app, what should I do?

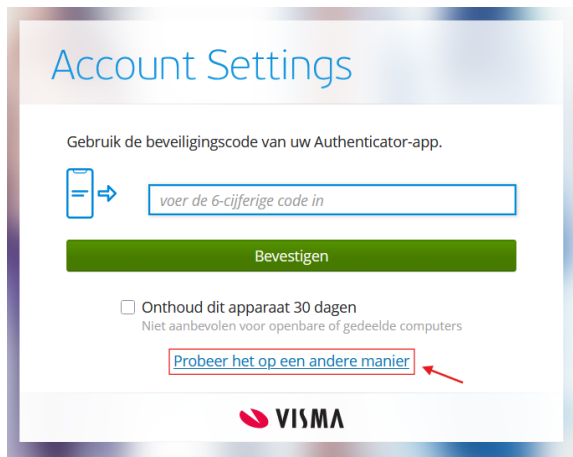
There may be situations where you no longer have access to your Authenticator app. For example, you may have started using a new phone or accidentally removed the Authenticator app from your device without having an active cloud backup.

In this case, you can request a recovery code using [this form](#). Nmbrs Support will then provide you with a backup code that allows you to sign in again and set up two-factor authentication once more.

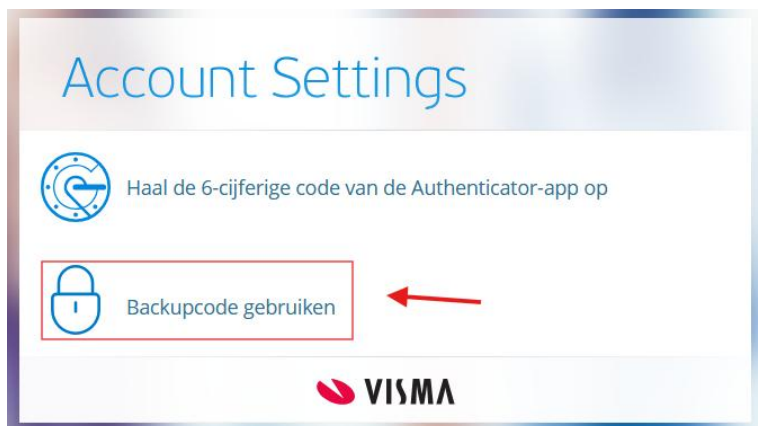
After you have received your recovery code, follow the steps described in section 2.2 "I Have Received My Recovery Code. What Should I Do Next?"

2.2 I have received my recovery code, what should I do next?

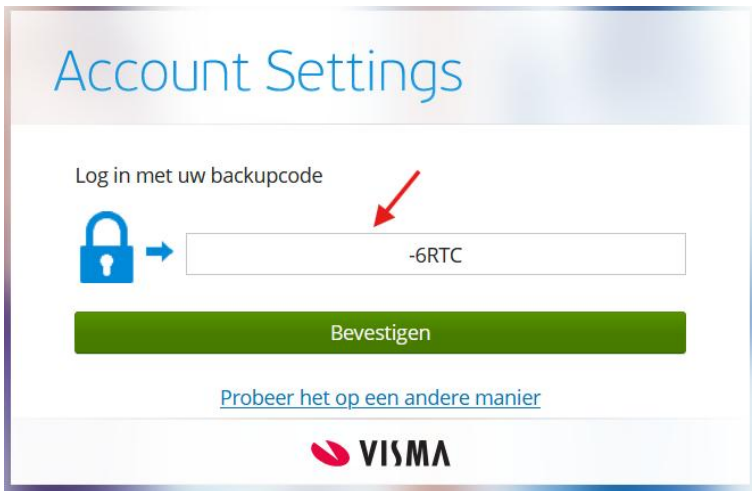
1 When signing in, you will arrive at the screen shown below. Click the "Try another way" button.



2 Then click "Use backup code".



3 Enter the backup code that you received by email.



The screenshot shows the 'Account Settings' page. At the top, it says 'Log in met uw backupcode'. Below this is a blue padlock icon with a right-pointing arrow next to it. To the right of the arrow is a text input field containing the code '-6RTC'. A red arrow points to this input field. Below the input field is a green button labeled 'Bevestigen'. Underneath the button is a link that says 'Probeer het op een andere manier'. At the bottom of the page is the VISMA logo.

4 Select the first option: "I permanently no longer have access to the Authenticator app."



The screenshot shows the 'Account Settings' page with the heading 'Kies een deblokkeeroptie voor de volgende keer wanneer u 2FA moet gebruiken'. There are two options listed, each with an icon of a smartphone. The first option is 'Ik heb permanent geen toegang tot de Authenticator-app', which is highlighted with a red rectangular box and a red arrow pointing to it. Below this option is the text 'Ik moet mijn Authenticator-app opnieuw instellen om de volgende keer 2FA te kunnen gebruiken'. The second option is 'Ik heb tijdelijk geen toegang tot de Authenticator-app', with the text 'Ik wil eenmalig inloggen om een backupcode voor accountherstel op te halen. Ik heb de volgende keer nog steeds toegang tot mijn Authenticator-app.' below it. The VISMA logo is at the bottom.

5 Click "Next" to set up two-factor authentication (2FA) again.

The process for setting up 2FA again is described in Chapter 1 of this guide..

Colofon

de Jong & Laan
Koningin Wilhelminaplein 30
1062 KR Amsterdam
085-4018718
info@jonglaan.nl
www.jonglaan.nl