LUFTHANSA GROUP

NDC PARTNER PROGRAM

Activation of Two Factor Authentication in SPRK

Status: March 28, 2025
Version: 1.2
Created by: GI/RD-S, AG/XD-G
Valid from: March 20, 2025

Austrian brussels AIRLINES Eurowings

Lufthansa SWISS

Public

CONTENT

1 TWO FACTOR AUTHENTICATION FOR SPRK AGENCY ADMINISTRATORS

Preparational work related to enabling of Two Factor Authentication in SPRK

Agency Admin checklist (please check in good time whether you are prepared):

☐ I have read below documentation

☐ All Agents in my Agency have an Authenticator app on their cell phone or PC workstation that can generate a Time-based One-Time Password (TOTP). In other words, we are prepared to go through Two Factor Authentication process in SPRK when being activated

☐ I have been informed when Two Factor Authentication will be activated for my agency

☐ I have checked that SPRK user accounts are not shared, i.e. there is no SPRK user account that is shared by several agents. If such shared SPRK user accounts do exist, I will deactivate them immediately and ensure that each agent has their own SPRK user account. This is important as each SPRK user account and the associated Second Factor may only be used by one person.

☐ Make sure that at least one SPRK user account with the role SPRK Agency Admin exists for your agency, which is based on your agency's time zone. This is important so that you receive prompt support from your SPRK Agency Admin in the event of problems.

☐ I have checked whether there are combinations of Office ID and Agent ID that exist in more than one environment. If this is the case and Two Factor Authentication (should) be activated in more than one of the affected environments, then certain things must be taken into account when setting up the second factor in Google Authenticator App, Microsoft Authenticator App or WinAuth. In this case, I familiarized myself with the content of section SETTING UP TWO FACTOR AUTHENTICATION IN MULTIPLE ENVIRONMENTS and shared it with all affected SPRK users.

In case you must reset Two Factor Authentication for a user account

Step A1: Log in to SPRK as Agency Admin

Let us assume you are SPRK Agency Admin, and your name is John Doe. When you have logged in to SPRK you will see following screen.

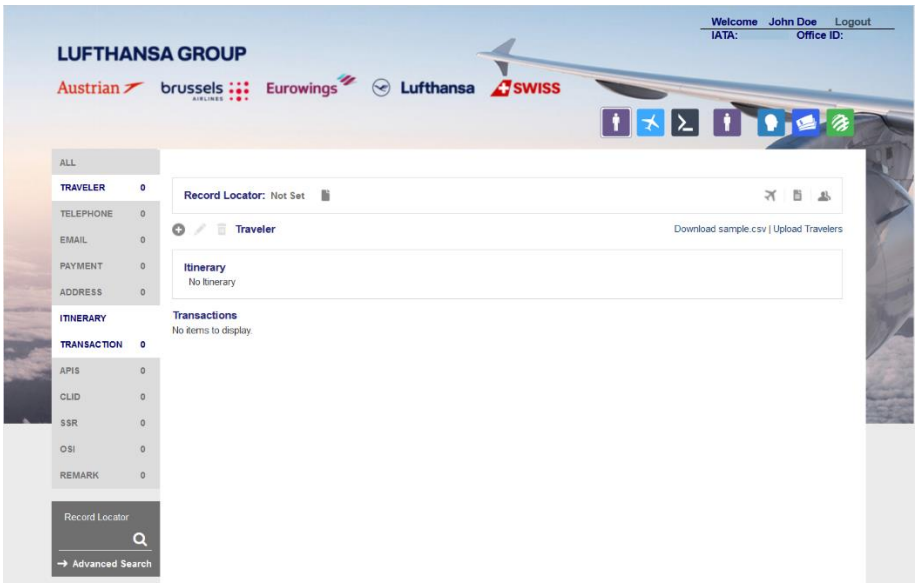


Figure 1: SPRK screen after successful login.

Step A2: Open Profile Management screen

Click on “Profile Management” icon ( ). You will then see below Profile Management screen.

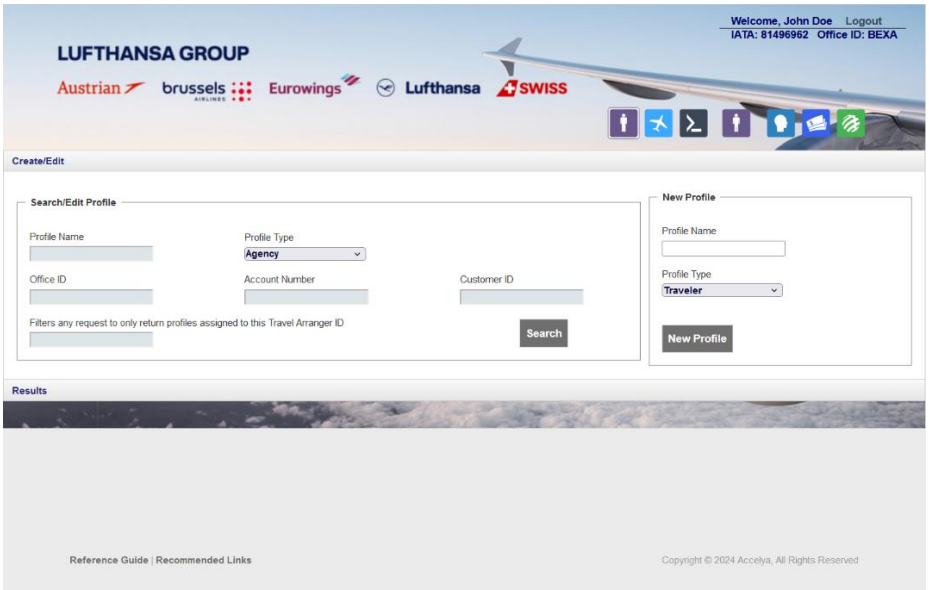


Figure 2: Profile Management screen.

Step A3: Navigate to SPRK user record in Profile Type Agency

Then select Agency from Profile Type drop-down list and click on Search button (Search).

Let us assume that you want to reset Two Factor Authentication for Paul Smith’s user Account. Enter in below dialog Paul Smith (respectively the name of a user from your agency) into field NAME and click on Refresh button (Refresh). Then the screen will look like below screenshot.

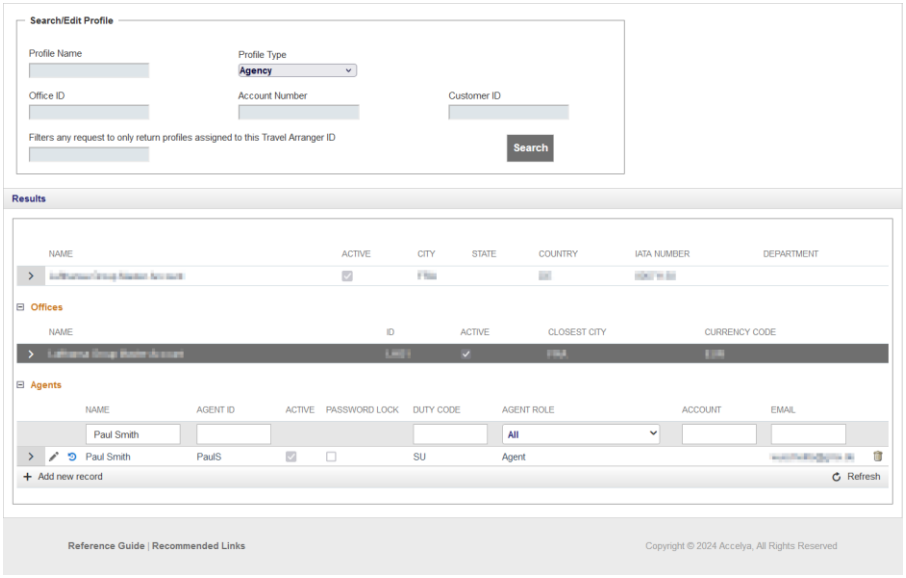


Figure 3: Profile Management screen – filtered for user with Name Paul Smith.

Step A4: Edit SPRK user account and reset Two Factor Authentication

Click on the edit icon ( ) on the lefthand side of Paul Smith's record. The record will expand, and you will see further details - similar to below screenshot.

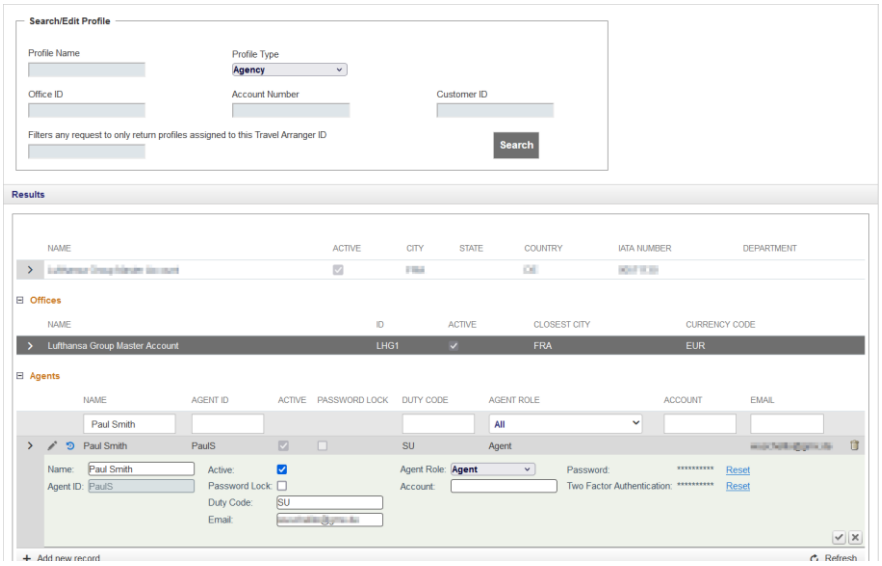


Figure 4: Profile Management screen – editing single user's record

Click on the Reset link at the right of the Two Factor Authentication entry. A pop-up dialog box will appear. Confirm by clicking on Continue.

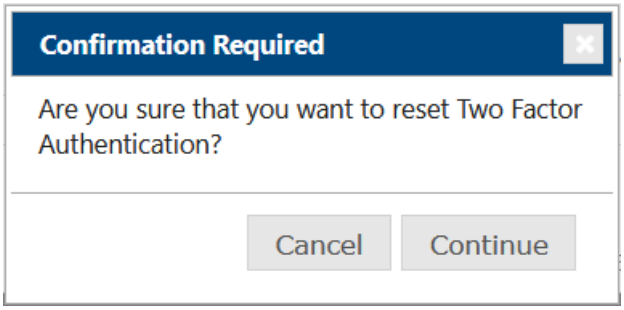


Figure 5: Two Factor Authentication reset – confirmation pop-up dialog box.

Step A4: Next time user logs in to SPRK he will have to go through Two Factor Authentication again

Two Factor Authentication for Paul Smith's SPRK user account has been reset. Next time when Paul is logging in to SPRK he will see again Setup Two Factor Authentication screen. So, Paul will have to save the new Second Factor.

☐ Check that the user has deleted their old Second Factor before creating a new Second Factor. This protects against the risk of ending up with two Second Factors that look identical (but only one of which can be valid). The user should also delete their old Secret before creating a new Second Factor after a Two Factor Authentication reset.

Figure 6: Setup Two Factor Authentication screen appearing again when Two Factor Authentication has been reset by SPRK Agency Admin.

Popular Authenticator apps

The list of Authenticator apps below does not claim to be exhaustive. Furthermore, it does not mean that the Lufthansa Group would not recommend an Authenticator app that is not mentioned.

Please check internally whether you have IT guidelines that stipulate the use of a specific Authenticator app. If this is not the case, your agency must decide for itself which Authenticator app you want to use. If you work at a workplace that has special security requirements, e.g. PCI DSS compliance, which is why it is not permitted to use cell phones to generate the Time-Based One-Time Password (TOTP) as a Second Factor, please contact your IT department to find a solution.

For iPhone and Android

You will find below Authenticator apps in both Apple App Store https://www.apple.com/app-store/ and Google Play https://play.google.com/store/apps

- 1Password Password Manager
- Bitwarden Password Manager
- Duo Mobile
- FreeOTP Authenticator
- Google Authenticator
- LastPass Password Manager
- Microsoft Authenticators
- Twilio Authy

For Windows

- WinAuth https://winauth.github.io/winauth/

Frequently asked questions

- When entering Time-based One-Time Password (TOTP) a pop-up dialog with error message “Incorrect Two Factor Code” appears.

  - Did you enter the displayed TOTP correctly? Try to enter the current code (if already expired use the one that is now displayed in your Authenticator app).
  - Is it possible that the TOTP you entered has already expired? Check if a new code is displayed in your Authenticator app and enter it.
  - If you manually set up the Second Factor by entering the Secret in your Authenticator app: did you enter the Secret correctly?

- I am SPRK Agency Admin and have lost my Second Factor. What shall I do?
  - If you are not the only SPRK Agency Admin of your agency, then please ask another SPRK Agency Admin to reset Two Factor Authentication for your SPRK user account.
  - If you are the only SPRK Agency Admin of your agency, or if no other SPRK Agency Admin is available then please contact Lufthansa Group B2B TAS (travel agency support) and ask for assistance.

- Can multiple SPRK users share the same Second Factor? No. According to Lufthansa Group IT Security regulations, user accounts must not be shared between multiple persons. Hence, each SPRK user will have his own and unique set of credentials and will have to create his own Second Factor as described below.

- I have SPRK user accounts for more than one environment, or I have SPRK user accounts where the same combination of Office ID and Agent ID is used in multiple environments. How do I differentiate between my Second Factors so that I always know which Second Factor belongs to which environment? In this case, familiarize yourself with the contents of section SETTING UP TWO FACTOR AUTHENTICATION IN MULTIPLE ENVIRONMENTS.

2 TWO FACTOR AUTHENTICATION FOR SPRK USERS

Enabling Two Factor Authentication in SPRK

Dear SPRK user,

IT security regulations of the Lufthansa Group require the introduction of Two Factor Authentication in SPRK. Your user account is affected by this. This measure will significantly increase the security of your SPRK account, i.e. significantly reduce the risk of misuse under your name. We need your cooperation to activate the Two Factor Authentication. You will find all the necessary information below.

Your checklist (please check in good time whether you are prepared):

☐ I have read below documentation

☐ I know who in my agency is the SPRK user responsible for me with the SPRK Agency Admin role. This will be my first point of contact if I have any difficulties with activating Two Factor Authentication.

☐ I have an Authenticator app on my cell phone or PC workstation that can generate a Time-based One-Time Password (TOTP). Please ask your Agency Admin for help if you do not know what an Authenticator app is and where to get it.

☐ I have been informed when Two Factor Authentication will be activated for my user account

☐ I have checked if I have SPRK user accounts for more than one environment, or if I have SPRK user accounts where the same combination of Office ID and Agent ID is used in multiple environments. In both cases, I have asked my SPRK Agency Admin for instructions on how to proceed.

Two Factor Authentication - what is that?

Two Factor Authentication in SPRK means using a Time-based One-Time Password (TOTP). This is a security method that adds an extra layer of protection to your online account. When you log in, you'll need to enter not only your regular password but also a special code generated by e.g. an app on your phone, like Google Authenticator or Authy. This code changes every 30 seconds, making it very hard for hackers to guess. Even if someone steals your password, they still can't access your account without the code from your phone. This way, your account stays much safer.

Google refers to a new entry in its Authenticator app that generates a TOTP (Time-Based One-Time Password) as a "token" or "account". Each entry corresponds to a specific account or service for which two-factor authentication has been enabled.

When you scan a QR code or manually enter a key to add a service to the app, it creates a new account entry in the app. This entry generates a TOTP every 30 seconds that you use as the Second Factor for authentication when logging in.

In this document we will not use Google's terms "token" or "account" but refer to Second Factor. Whenever we use Second Factor, we mean the corresponding configuration in your Authenticator app that generates the Time-based One-Time Password (TOTP) for your SPRK user account.

This means that Two Factor Authentication is the overall procedure and, in the context of SPRK, the Second Factor is a Time-Based One-Time Password (TOTP). They are related, but not the same. For this reason, we provide you with a definition below that clarifies this once again:

1. Two-Factor Authentication: This is a security process that requires users to provide two distinct forms of authentication to verify their identity. These two factors typically come from different categories:

    - Something you know (e.g., a password or PIN)
    - Something you have (e.g., a smartphone, security token, or app-generated code)
    - Something you are (e.g., biometric data like a fingerprint or facial recognition)

2. Second Factor: This refers to the additional form of authentication beyond the primary method (e.g., a password). In Two-Factor Authentication, the Second Factor is what you provide after entering your password. For example, receiving a code on your phone or using a biometric scan serves as the Second Factor.

In summary, Two-Factor Authentication refers to the overall process of requiring two different authentication methods, while the Second Factor is specifically the additional method used after the primary one.

Where can I get the Authenticator app?

If you are not yet using an Authenticator app, or in areas subject to special security regulations (e.g. PCI DSS[1] compliant workplaces) where the use of private cell phones is prohibited, please contact your SPRK Agency Admin. They will help you install and use an Authenticator app for your cell phone or an application for your PC workstation.

Date of activation

You should have received an email from the Lufthansa Group, which defines the exact time of the Two Factor Authentication for your agency. If you do not have this information, please contact your SPRK Agency Admin. They should be able to tell you the exact time. If you have any questions or problems during the activation of Two Factor Authentication, please also contact your SPRK Agency Admin.

You must do this for the first time after Two Factor Authentication has been activated for your agency

Step 1: Log in to SPRK as usual

Log in to the SPRK interface as usual at https://dcwebc.farelogix.com/sprk-lhg/. i.e. enter Office ID, Agent ID and your password as usual. Then click on LOGIN.

Figure 7: SPRK login screen. Log in as usual by entering your credentials.

Step 2: Setup your Second Factor in your authentication app

If Two Factor Authentication has been activated for your agency but has not yet been set up for your user account, you will see the following dialog “Setup Two Factor Authentication”.

If you have already activated Two Factor Authentication for your SPRK user account, but it has just been reset (so you are asked to set up Two Factor Authentication again - see next figure), check the following:

☐ Check that you have deleted your old Second Factor before creating a new Second Factor. This protects against the risk of ending up with two Second Factors that look identical (but only one of which can be valid). Also delete your old Secret before creating a new Second Factor after a Two Factor Authentication reset.

It contains a QR code, and below the QR code a 32-digit alphanumeric code – the so-called Secret.

Figure 8: Scan the QR code with the Authenticator app on your cell phone or make a note of the Secret displayed under the QR code

Note: Please do not scan the QR code from above figure but from your Internet browser. Please do not use the Secret shown above, but the 32-digit alphanumeric code displayed in your browser. Whether you can use the QR code or the Secret to set up your Second Factor depends on the Authenticator app you have chosen. If in doubt, please ask your SPRK Agency Admin.

Use your cell phone to scan the QR code from the "Setup Two Factor Authentication" screen or make a note of the Secret displayed under the QR code. You can then enter this manually in the Authenticator app of your choice.

Tip: If the QR code is displayed too small in your Internet browser, zoom into the page.

You can recognize that you have set up a Second Factor in your Authenticator app by the fact that it generates a different 6-digit number - the TOTP - every 30 seconds.

Now enter the TOTP currently displayed on the "Setup Two Factor Authentication" page. Click Verify.

In the event that an error message is displayed.

If a pop-up dialog with error message "Incorrect Two Factor Code" appears, check the following:

- Did you enter the displayed TOTP correctly? Try to enter the current code (if already expired use the one that is now displayed in your Authenticator app).
- Is it possible that the TOTP you entered has already expired? Check if a new code is displayed in your Authenticator app and enter it.
- If you manually set up the Second Factor by entering the Secret in your Authenticator app: did you enter the Secret correctly?

If none of the above tips help, please contact your SPRK Agency Admin. They will try to assist you and, if necessary, receive support from a Lufthansa Group B2B TAS (travel agency support).

Step 3: Agree to the End User Service Agreement

If Two Factor Authentication has been activated for your agency but has not yet been set up for your user account, you will see the following dialog “Setup Two Factor Authentication”.

Figure 9: Please confirm your agreement to the EUSA by checking the "Agree" option and then clicking SUBMIT.

Finally, we would like to ask you to read the End User Service Agreement (EUSA). Please confirm your agreement by checking the "Agree" option and then clicking SUBMIT.

After clicking SUBMIT you will then see the normal SPRK screen of your agency.

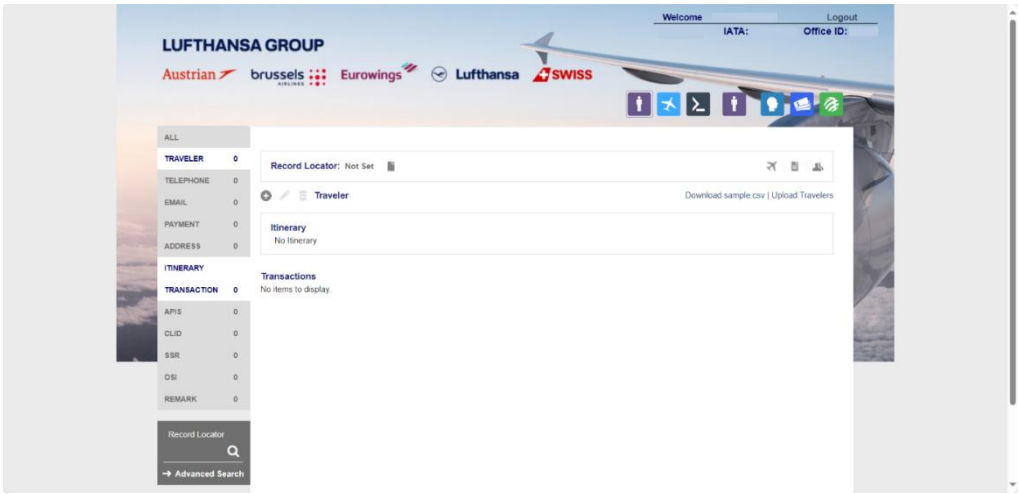


Figure 10: SPRK screen after successful login.

You have now successfully configured Two Factor Authentication for your SPRK user account.

What will be different the next time you log in to SPRK?

The next time you log in to SPRK, you will need to enter Office ID, Agent ID and your password as usual and then click on LOGIN - again as usual.

Figure 11: SPRK login screen. Log in as usual by entering your credentials

However, a dialog will then appear in which you must enter the Second Factor, i.e. the 6-digit number from your Authenticator app.

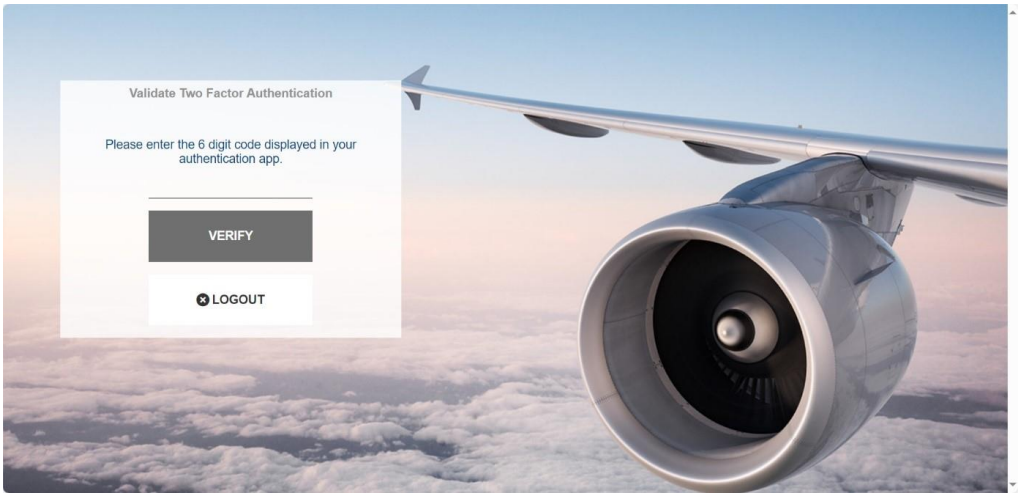


Figure 12: Every time you log in to SPRK you will have to enter the 6-digit code displayed in your Authenticator app.

Enter the 6-digit number from your Authenticator app and click on VERIFY.

After clicking VERIFY you will then see the normal SPRK screen of your agency.

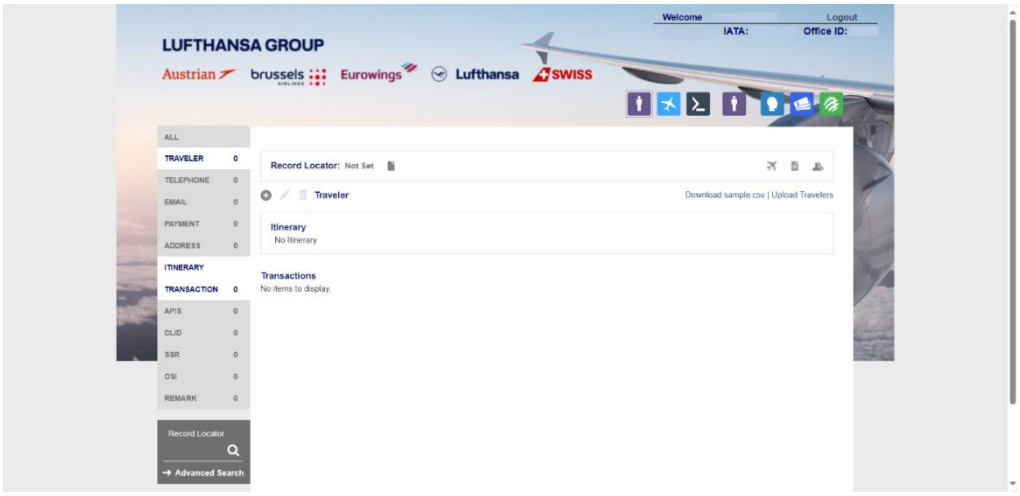


Figure 13: SPRK screen after successful login.

3 SETTING UP TWO FACTOR AUTHENTICATION IN MULTIPLE ENVIRONMENTS

Issues when setting up 2FA in multiple environments

Accelya operates several environments. The environments relevant for the Lufthansa Group and its partners are Sandbox, User Acceptance Testing and Production.

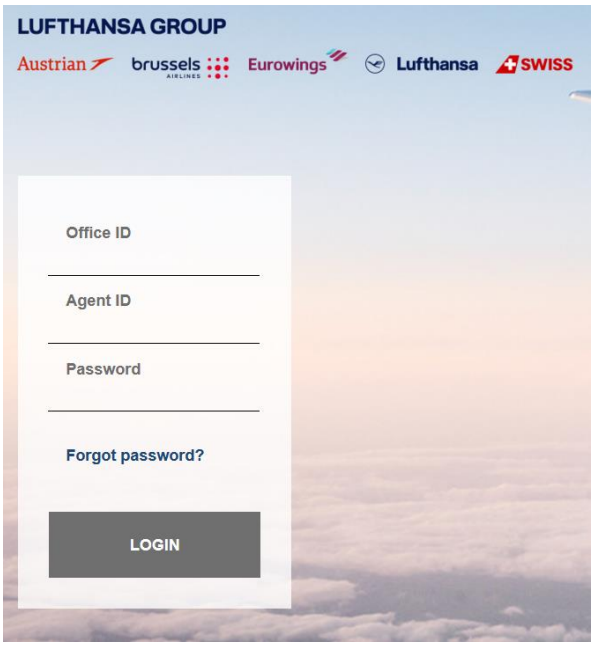


Figure 14: SPRK users can have user accounts with identical Office ID (aka PCC) and Agent ID in different environments. This means that they enter the same Office ID and Agent ID when logging into Sandbox (https://sprk.accelya.io/lhg/sandbox-uat) and Production (https://dcwebc.farelogix.com/sprk-lhg).

Our example user Paul Smith (Agent ID PaulS) has a user account for Office ID LX13 in both Sandbox and Production.

If he sets up two-factor authentication for both of his SPRK user accounts, he will receive the QR codes shown below.

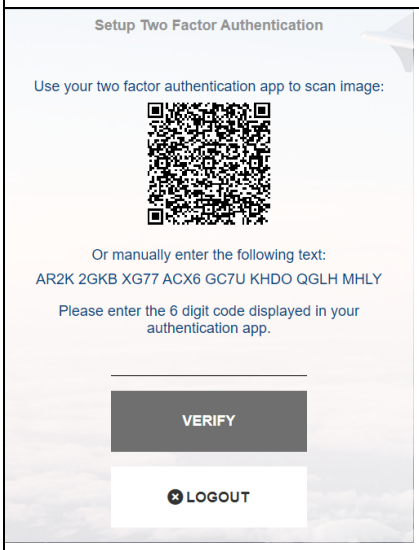
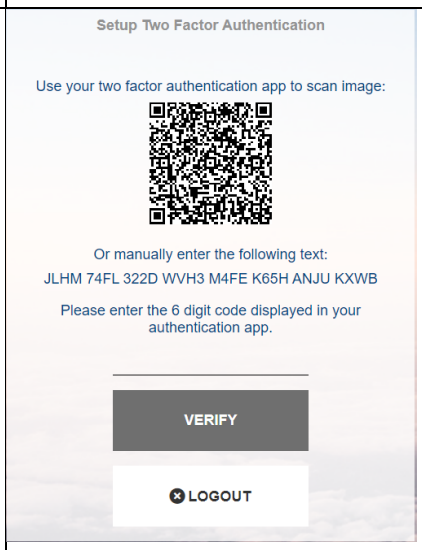
2FA Setup in Sandbox for Paul's LX13 SPRK User Account	2FA Setup in Production for Paul's LX13 SPRK User Account
	

Table 1: Example QR codes for the same combination of Office ID and Agent ID, but belonging to different environments. n our example, the Office ID is LX13 and the Agent ID is PaulS.

When scanning above QR codes in Google Authenticator App or Microsoft Authenticator App, the applications behave differently, but the basic problem is the same: the QR code does not contain any information about which environment it belongs to. When Paul scans the QR codes for his two LX13 SPRK user accounts in Sandbox and Production, he sees the following in the Google Authenticator app, for example.

Figure 15: Google Authenticator App displays several Second Factors with the same Account name (Office ID and Agent ID are also identical). It is not possible to recognize which Second Factor belongs to which environment.

I.e. in Google Authenticator it is possible to create Second Factors from the two QR codes mentioned above. Google Authenticator does not inform you that the resulting Second Factors are ambiguous (see screenshot above). You can see that two authenticators have been created, both labeled "Farelogix: LX13:PaulS". From this you cannot tell which belongs to Sandbox and which belongs to Production.

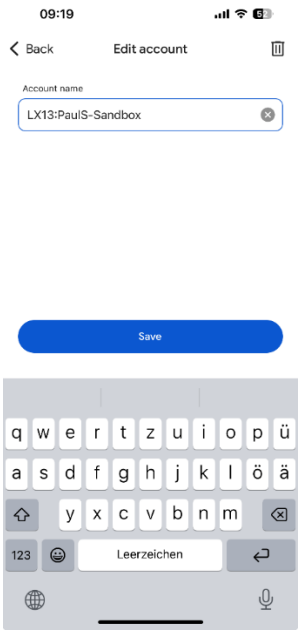
Below we describe how this problem can be addressed in Google Authenticator App, Microsoft Authenticator App and WinAuth. If you use other Authenticator apps, please contact your Agency Admin or your IT department.

Google Authenticator App

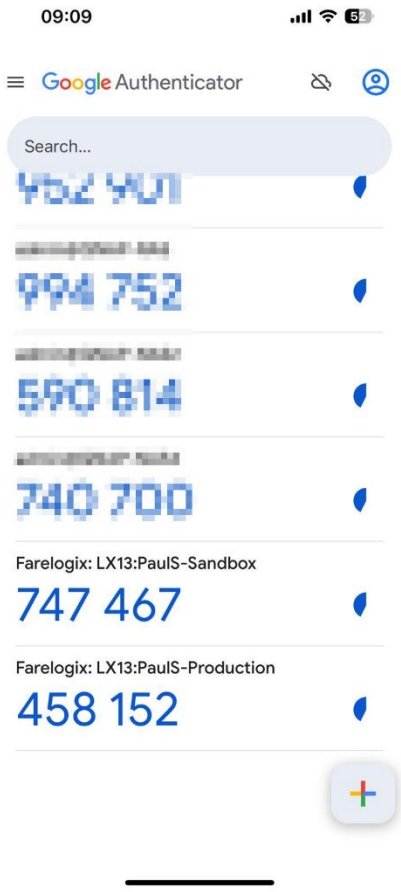
To avoid ambiguous Second Factors in the Google Authenticator App, please proceed as follows.

1. Scan the QR code. Then swipe the newly created Second Factor in Google Authenticator to the left and select the edit icon (pencil).
   Example: If we scan the QR code from the table above for the sandbox environment, we see the result illustrated in the screenshot below.

2. Enter a unique name, e.g. add the environment, so that the name of the Google Authenticator account contains Office ID, Agent ID and Environment. Then tap Save.
   Example: Paul will use LX13:PaulS-Sandbox to uniquely identify the second factor for his Sandbox SPRK user account (see screenshot below).



3. Proceed as described above for all your Google Authenticator accounts (aka Second Factors). Your Second Factors will then have unique and unambiguous names (see screenshot below).



Microsoft Authenticator App

Our example user Paul first scans the above QR code from the Sandbox environment. When he then scans the QR code from the Production environment, he receives the following warning:

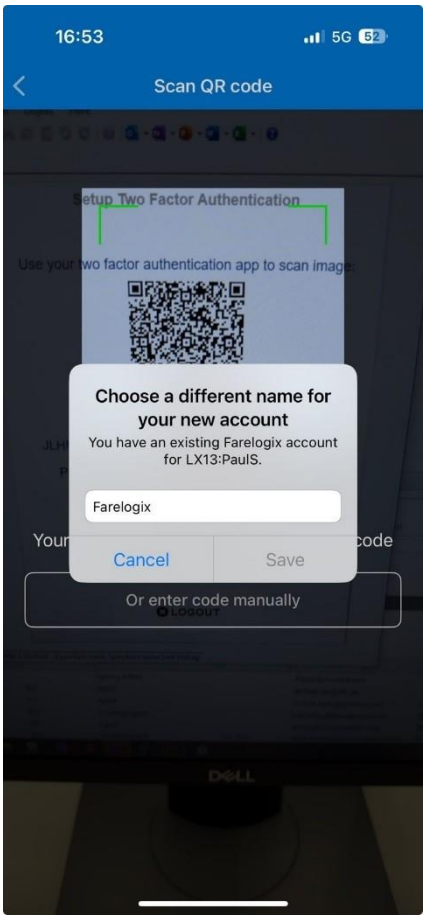


Figure 16: If a second QR code for the same combination of Office ID and Agent ID is scanned in the Microsoft Authenticator app, a warning appears.

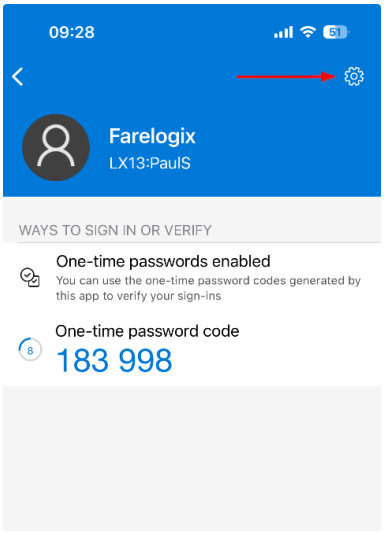
So, if you scan more than one QR code from Accelya for the same combination of Office ID and Agent ID in the Microsoft Authenticator app, you will receive this warning.

The above warning is not displayed if users have multiple SPRK user accounts in the same environment and scan the associated QR codes (because then either Office ID or Agent ID is different).

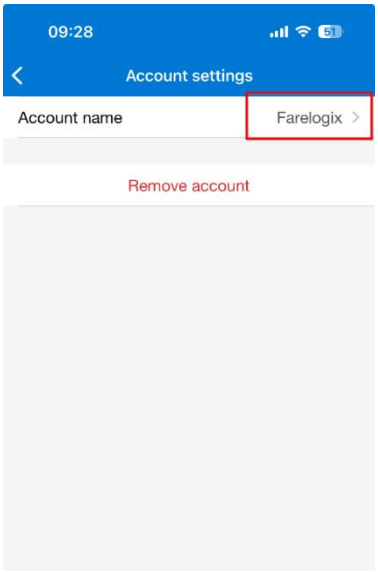
If the above warning is displayed, please enter in Microsoft Authenticator App a unique name that clearly indicates the environment. In above screenshot it would make sense to enter e.g. Farelogix-Production and then tap Save.

The best way to avoid ambiguous second factors in the Microsoft Authenticator app is to proceed as follows:

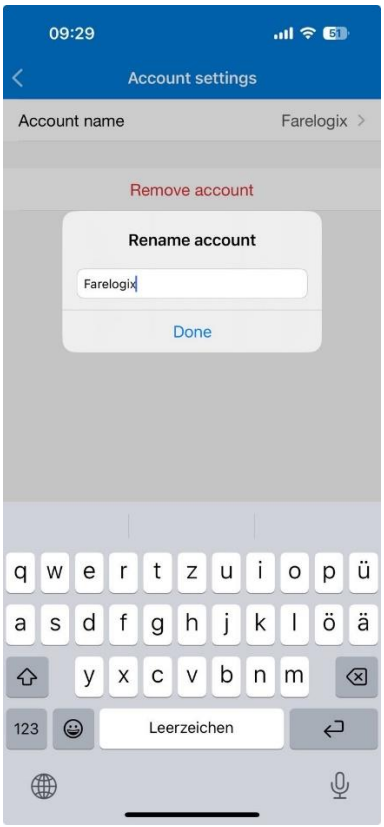
1. If you see a second factor in the Microsoft Authenticator app where it is not immediately obvious which environment it belongs to, proceed as follows. Tap on the Second Factor that you want to change. The detail view for this Second Factor will then be displayed (see below screenshot). Then tap on the Settings icon (gear wheel).



2. You will see the Account settings. Tap one the name (red outlined in the screenshot).



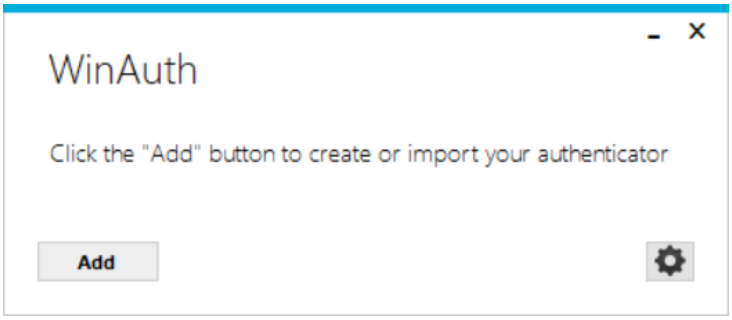
3. Edit the Account name and give it a unique name by appending the environment name, i.e., resulting in Farelogix-Sandbox or Farelogix-Production. Then tap on Done.



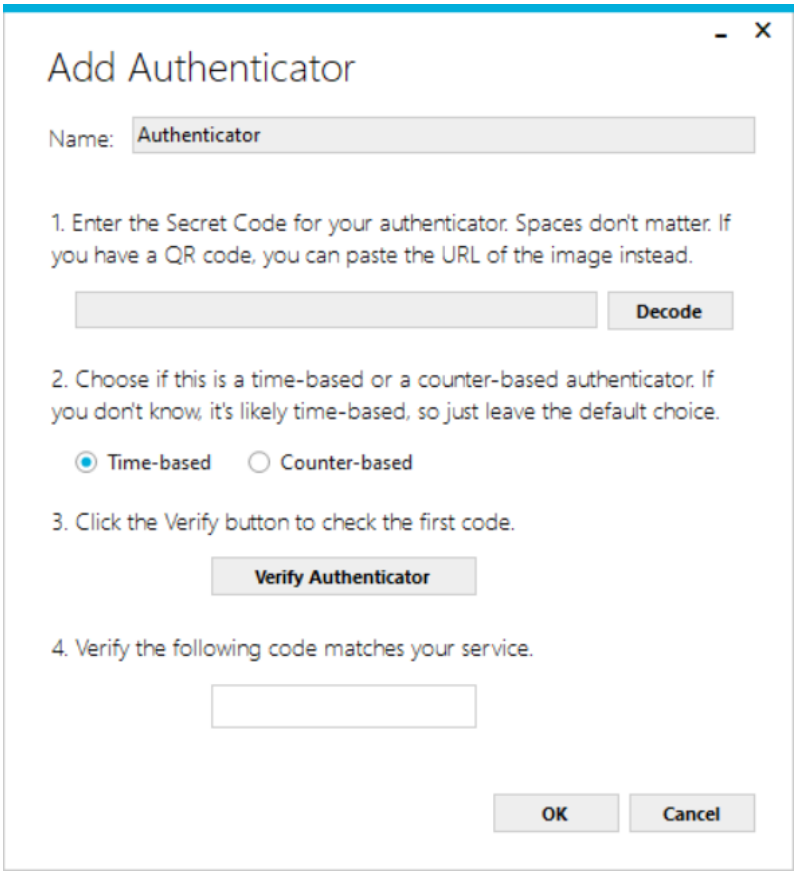
WinAuth

If you are using WinAuth, it is recommended that you proceed as follows, which allows you to create unique names for each second factor yourself.

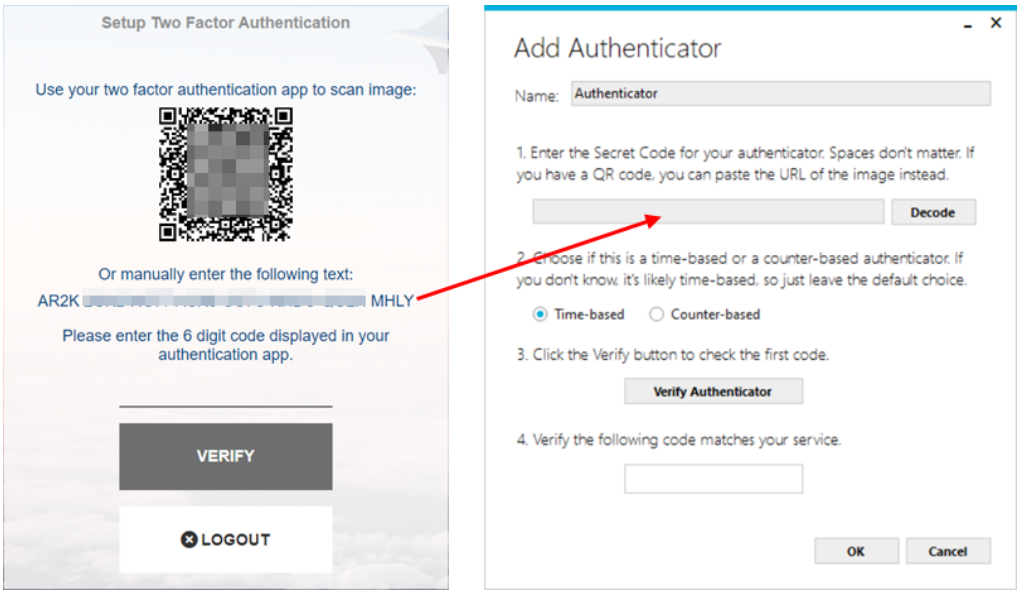
1. Open WinAuth .
2. Click the Add button in the main WinAuth window and choose “Authenticator” as the type of Authenticator you need.



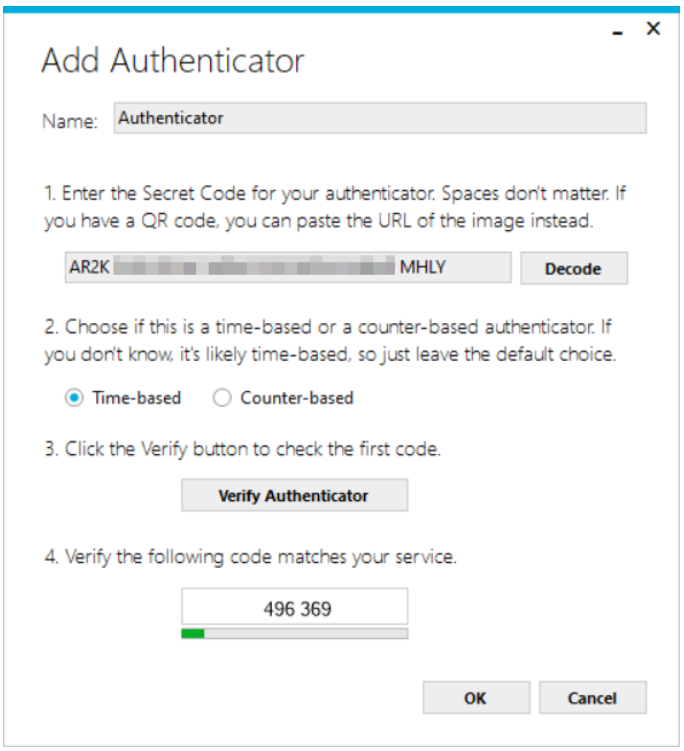
3. Enter a unique name, e.g. “SPRK-Production:LX13:PaulS”, i.e. enter the environment, office ID and agent ID.



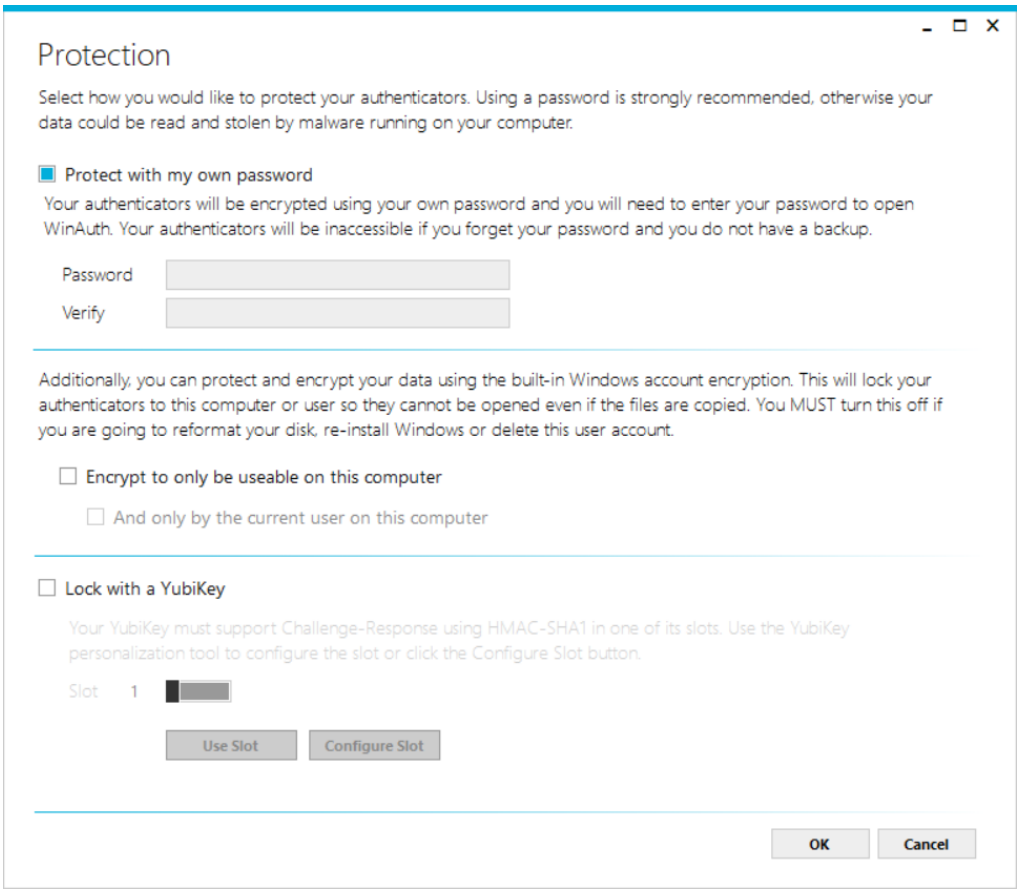
4. Copy and paste the the Secret (the 32-digit alphanumeric code that was displayed together with the QR code when setting up Two Factor Authentication) into the field in WinAuth. The Time-based radio button should be selected.



5. Click the Verify Authenticator button to check the key is valid and you will see the first code



6. Protection. Chose “Protect with my own password”.



7. Click the OK button to save the authenticator.

8. Your Second Factor has now a unique name.