ICF
SDP
MFA

Guideline

Atos

Table of contents

1. SDP- MFA Authentication

Multi-factor Authentication (MFA) is an authentication method that requires the user to provide two or more verification factors to gain access to a resource such as an application, online account, or a VPN. MFA is a core component of a strong identity and access management (IAM) policy. Rather than just asking for a username and password, MFA requires one or more additional verification factors, which decreases the likelihood of a successful cyber-attack.

With MFA authentication implemented in the SDP system, after entering their login credentials for the first time, users will have to enable authentication in another application (Google authenticator, Microsoft authenticator, etc.) using the QR code generated and displayed on the screen (Figure 2).

**Important:

In order to be able to generate six-digit codes to log in to the system, it is necessary to have a previously installed authenticator application on any device. Our recommendation is to install it on a mobile phone.

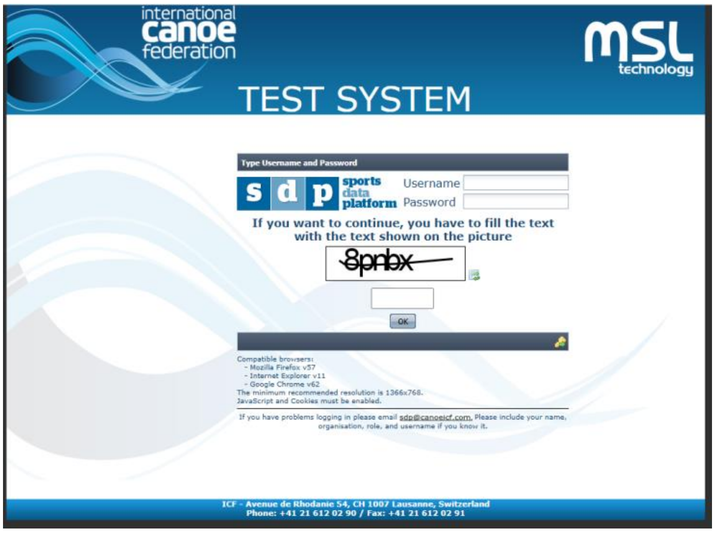
*Below are two options of authentication applications:

Google Authenticator

Microsoft Authenticator

2.Process to log in in SDP (first time)

2.1. Log in as usual



Type Username and Password

Username
Password

If you want to continue, you have to fill the text with the text shown on the picture

Compatible browsers:
- Mozilla Firefox v57
- Internet Explorer v11
- Google Chrome v62

The minimum recommended resolution is 1366x768.
JavaScript and Cookies must be enabled.

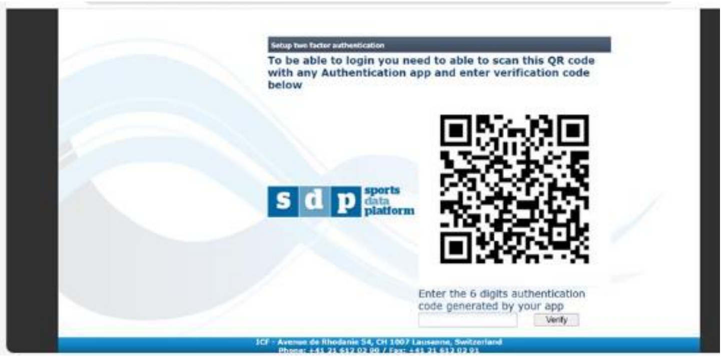
If you have problems logging in please email sdp@canoeicf.com. Please include your name, organisation, role, and username if you know it.

ICF - Avenue de Rhodanie 54, CH 1007 Lausanne, Switzerland
Phone: +41 21 612 02 90 / Fax: +41 21 612 02 91

Figure 1- Login

2.2. Redirection to QR to add MFA account into authenticator app

After entering your login credentials and the captcha code, you will be have to enter the generated six-digit code at the bottom of the screen to verify it. Please follow the steps below how to generate the code to your authenticator app.



Setup two factor authentication

To be able to login you need to able to scan this QR code with any Authentication app and enter verification code below

Enter the 6 digits authentication code generated by your app

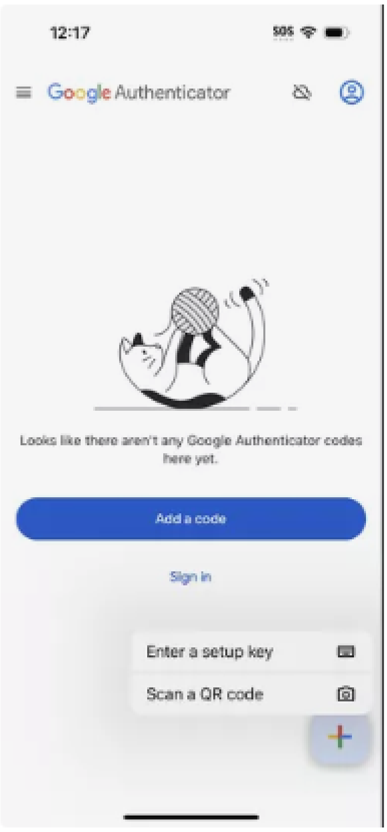
ICF - Avenue de Rhodanie 54, CH 1007 Lausanne, Switzerland
Phone: +41 21 612 02 90 / Fax: +41 21 612 02 91

Figure 2- QR Screen

2.2.1. Google authenticator

To add account authenticator in app authenticator if you choose google authenticator, the process would be:

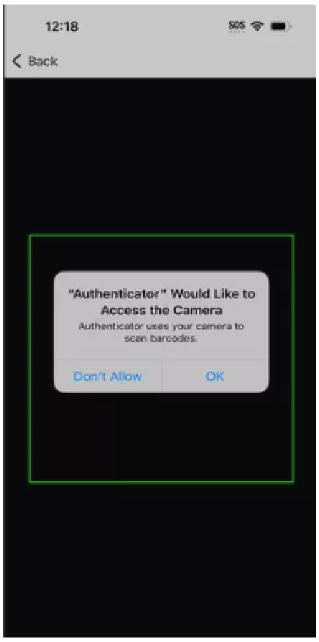
1) **Download and install the app from the App Store or the Google Play Store.**
2) **Open Google Authenticator and tap the + sign. If this is your first time using the app, you'll be asked if you want to log in to your Google account or use Authenticator without an account. The choice is yours, but we recommend logging in so you can back up your codes to your Google account.**



Looks like there aren't any Google Authenticator codes here yet.

Figure 3- Google authenticator main screen

3) **Select Scan a QR code and for the next screen press ok**



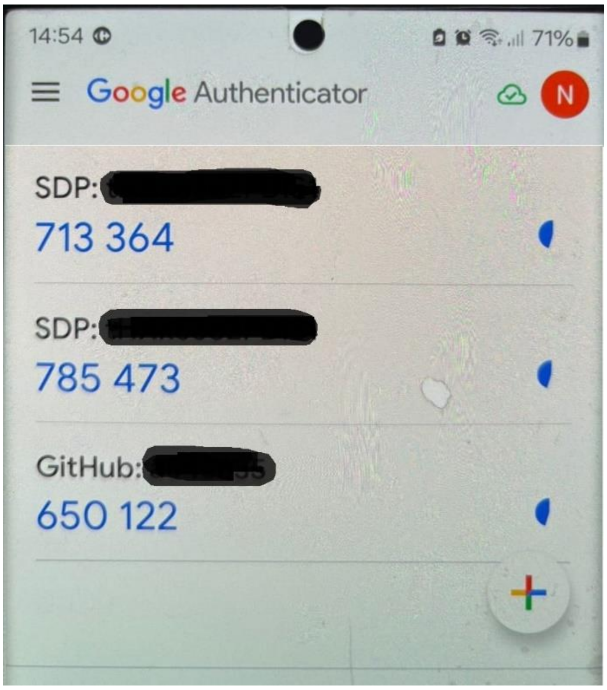
12:18

< Back

"Authenticator" Would Like to Access the Camera

Authenticator uses your camera to scan barcodes.

4) **Scan the code generated by SDP (Figure 2). After this you'll get new entry in your authenticator app like the first entry in the image below**



SDP: [redacted]

713 364

SDP: [redacted]

785 473

GitHub: [redacted]

650 122

-

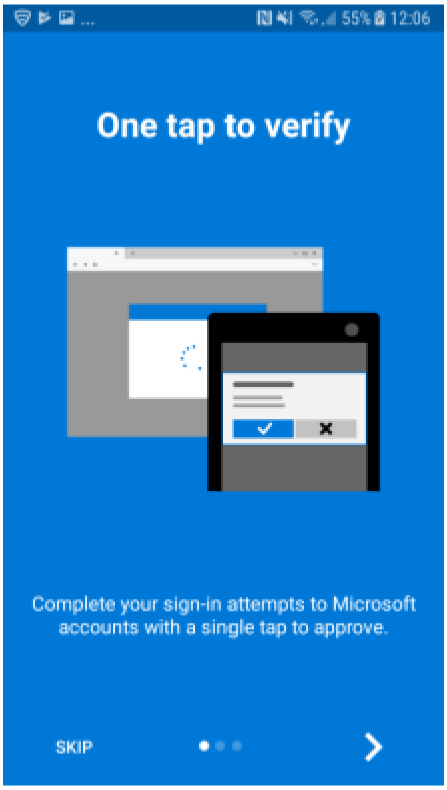
Figure 4- Example of google authenticator main screen with accounts added

From that time on, that will be the code you will need to enter into the SDP after entering your usual credentials.

2.2.2. Microsoft authenticator

1) **Download and install the app from the Microsoft Store or the Google Play Store.**

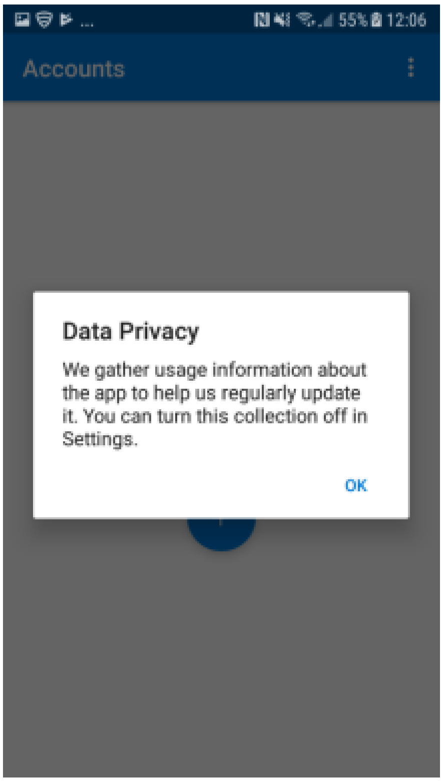
2) **If this is the first time that you have opened the application you will be shown the following screen.**



One tap to verify

Complete your sign-in attempts to Microsoft accounts with a single tap to approve.

3) The first time you run the application you will be shown a data privacy alert, Press OK.

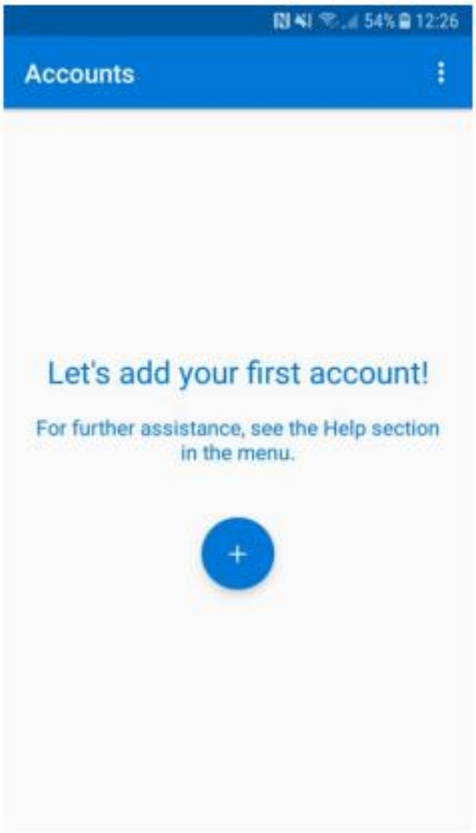


Data Privacy

We gather usage information about the app to help us regularly update it. You can turn this collection off in Settings.

4) Setting up an account

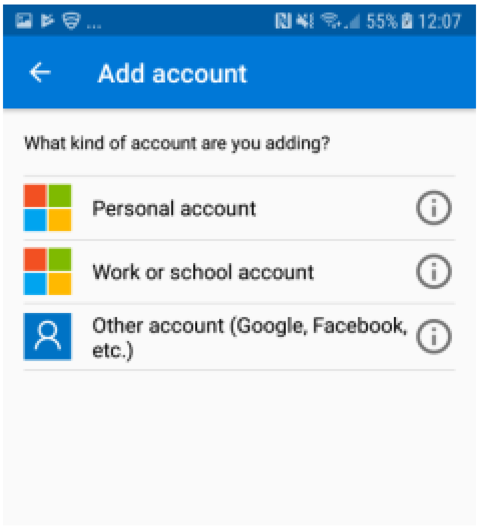
If this is the first time using the account press the + in the middle of the screen



Let's add your first account!

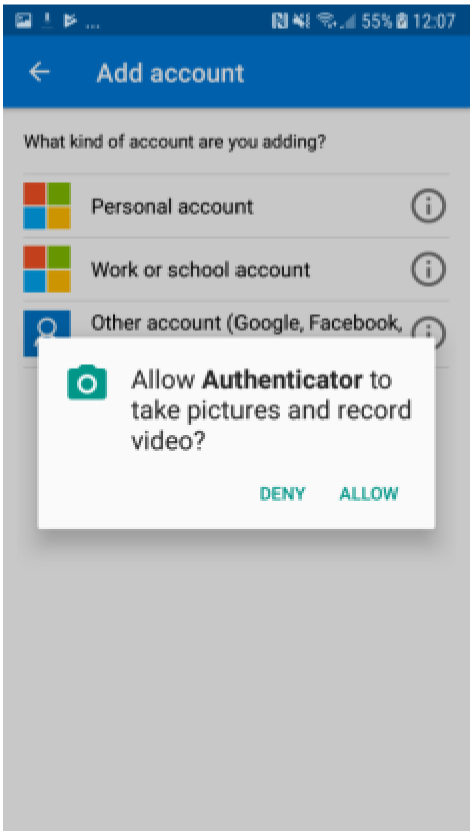
For further assistance, see the Help section in the menu.

5) **Now press work or school account.**



What kind of account are you adding?

6) **You will then get an alert asking permission to access the camera. Press Allow**



Add account

What kind of account are you adding?

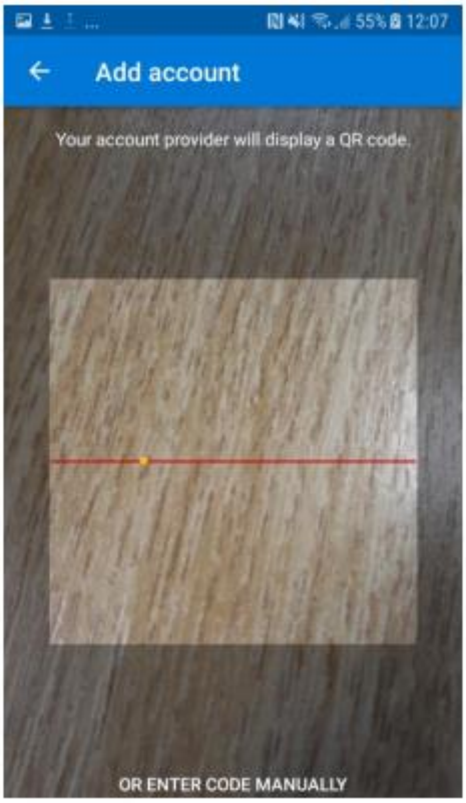
Personal account

Work or school account

Other account (Google, Facebook,

Allow **Authenticator** to take pictures and record video?

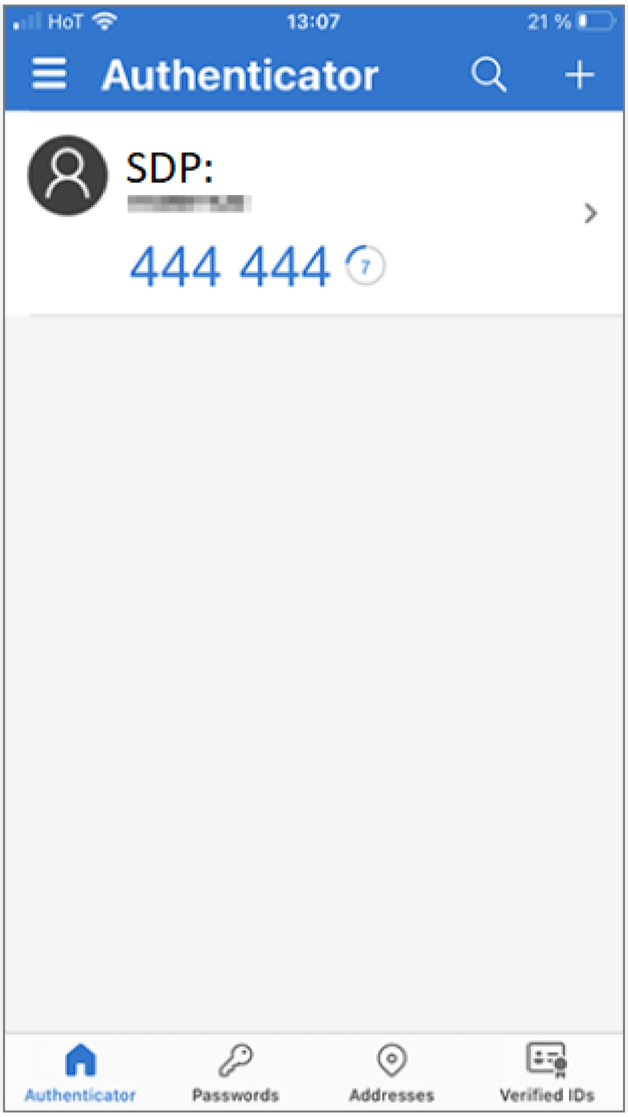
7) The app will then ask you to scan the QR code.



Add account

Your account provider will display a QR code.

8) **Scan the code generated by SDP (Figure 2). After this you'll get new entry in your authenticator app like the first entry in the image below:**



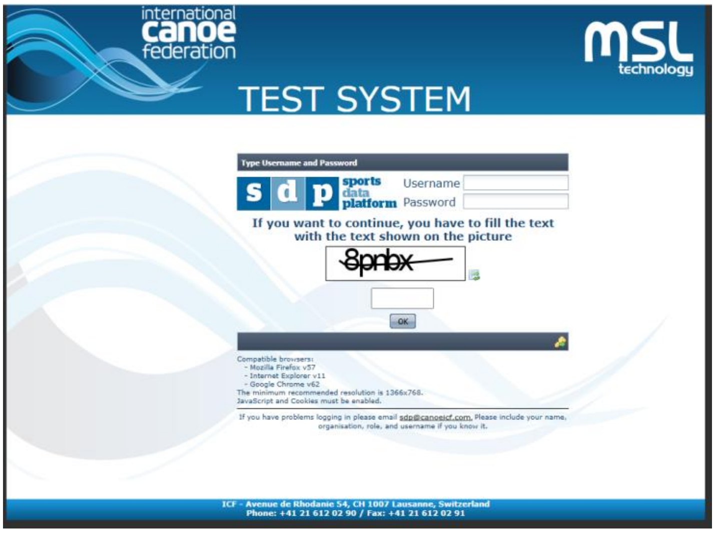
SDP:
[redacted]
444 444

Figure 5

From that time on, that will be the code you will need to enter into the SDP after entering your usual credentials.

3. Process to log in in SDP after you set up multi-factor authentication

3.1. Log in as usual



If you want to continue, you have to fill the text with the text shown on the picture

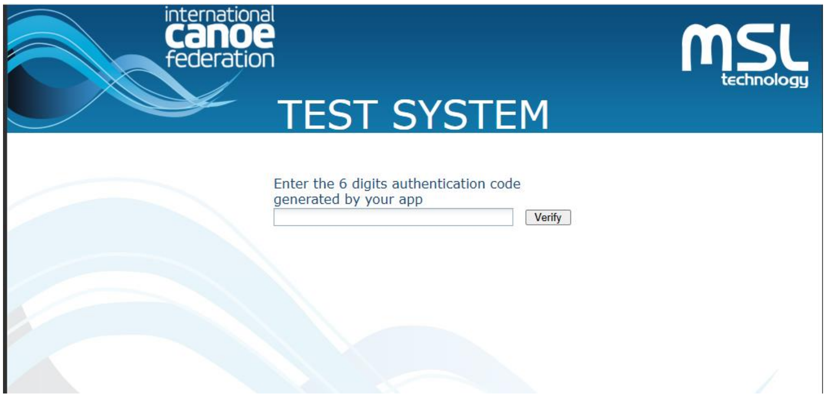
Compatible browsers:
- Mozilla Firefox v57
- Internet Explorer v11
- Google Chrome v62

The minimum recommended resolution is 1366x768.
JavaScript and Cookies must be enabled.

If you have problems logging in please email sdp@canoeicf.com. Please include your name, organisation, role, and username if you know it.

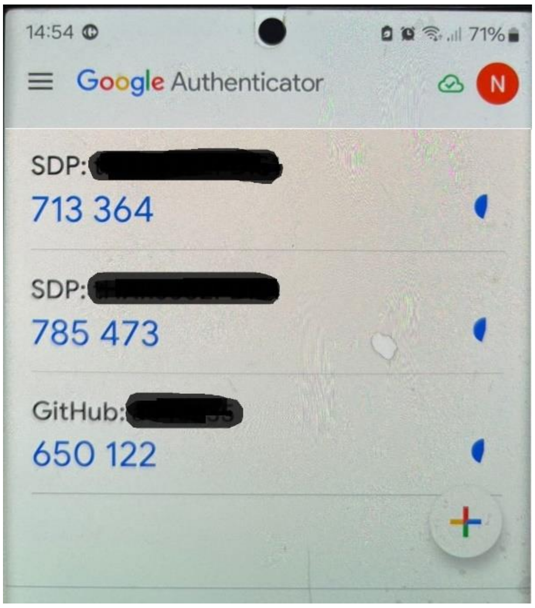
ICF - Avenue de Rhodanie 54, CH 1007 Lausanne, Switzerland
Phone: +41 21 612 02 90 / Fax: +41 21 612 02 91

3.2. Next screen to enter six-numbers code



Enter the 6 digits authentication code generated by your app

You could find this code in your google authenticator (Figure 6) or Microsoft authenticator (Figure 5)



14:54 71%

Google Authenticator N

SDP:[redacted]
713 364

SDP:[redacted]
785 473

GitHub:[redacted]
650 122

+

Figure 6- Six-numbers code for SDP account

About Atos

Atos is a global leader in digital transformation with c. 95,000 employees and annual revenue of c. € 11 billion. European number one in cybersecurity, cloud and high-performance computing, the Group provides tailored end-to-end solutions for all industries in 69 countries. A pioneer in decarbonization services and products, Atos is committed to a secure and decarbonized digital for its clients. Atos is a SE (Societas Europaea) and listed on Euronext Paris.

The purpose of Atos is to help design the future of the information space. Its expertise and services support the development of knowledge, education and research in a multicultural approach and contribute to the development of scientific and technological excellence. Across the world, the Group enables its customers and employees, and members of societies at large to live, work and develop sustainably, in a safe and secure information space.

About Tech Foundations

Tech Foundations is the Atos Group business line leading in managed services, focusing on hybrid cloud infrastructure, employee experience and technology services, through decarbonized, automated and AI-enabled solutions. Its 48,000 employees advance what matters to the world's businesses, institutions and communities. It is present in 69 countries, with an annual revenue of € 6 billion.

Learn more at: atos.net

Atos Group is deploying safe and responsible AI solutions (internal and/or 3rd party based) for the internal use by its employees, collaborators and advisors when developing and delivering products and/or services to its customers as well as when and offering AI based solutions. A specific policy has been deployed across all the Group employees to ensure the protection of the confidentiality and the security of own data and our customers' data through the use of solutions vetted by our legal, security and data protection teams.

Additionally, the Group offers professional services that can help companies to understand requirements, to anticipate legislations applicable to AI, and to be better prepared to achieve compliance with those AI regulations as they are adopted.

105043-RR