Lucerne University of
Applied Sciences and Arts

HOCHSCHULE
LUZERN

20 Jahre

IT Services Support

Werftestrasse 4, Postfach 2969, CH-6002 Luzern
T +41 41 228 21 21
hslu.ch/helpdesk, informatikhotline@hslu.ch

Multi-factor Authentication (MFA)

Short description:	User manual for the MFA portal of the Lucerne University of Applied Sciences and Arts.	
Classification:	☐ IT internal	☒ Public
	☐ Other	
Customer group:	☒ HSLU	☒ PHLU
	☐ Other	
Function:	☒ Employees/lecturers	☒ Students
	☐ Other	
Device management type:	☒ HSLU/PHLU devices	☒ Private devices
	☐ Other	
Operating system:	☒ Windows	☒ Mac
	☐ Other	
Publication:	☒ hslu.ch/helpdesk	☒ Intranet
	☐ Other	
Support:	Web: hslu.ch/helpdesk	
	Email: informatikhotline@hslu.ch	
	Phone: 041 / 228 21 21	
	Portal: helpdesk.hslu.ch	

Änderungsverzeichnis

Version	Datum	Status	Änderungen und Bemerkungen	Bearbeitet von
1.0	05/05/2017		Document created	NiL
1.1	08/05/2017		Document amended	GrP
1.2	09/05/2017		Document amended	GrP
1.3	10/05/2017		Document amended	GrP
1.4	21/06/2017		Document adjusted	NiL
1.5	09/05/2019		Document adjusted	Kju, Poa
1.6	08/01/2020		Altered BKZ-GS	ReM

Inhaltsverzeichnis

1. Why MFA

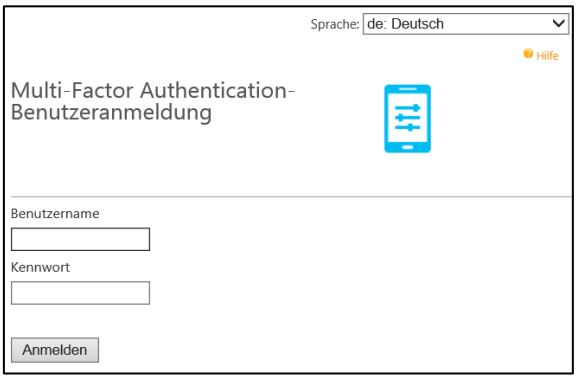
To minimise the risk of unauthorised access, MFA, or, in other words, the combination of various mutually independent components (factors) is used to protect access to certain applications of the Lucerne University of Applied Sciences and Arts.

2. Requirements

In order to use the MFA portal, users need:

- a valid HSLU/PHLU/BKZ-GS user account
- a smartphone with internet access OR a mobile phone with a SIM card OR a landline phone

3. Registration



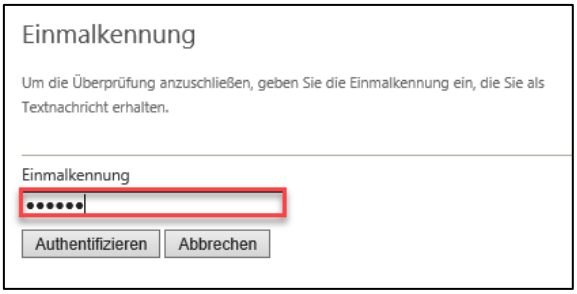
Open https://mfa.hslu.ch and sign in with your username and password.

Please note: In case of problems with the registration, refer to point 6.

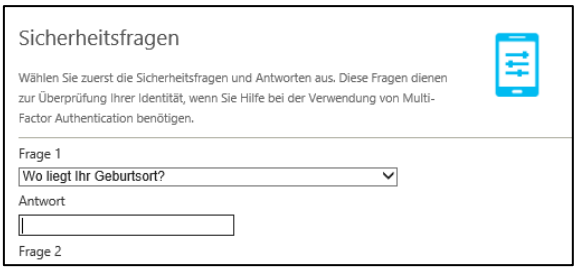
Select your preferred authentication method. The system suggests SMS (text messages) as an authentication method by default - it will be used here as an example.

Please note: refer to point 4 for other authentication methods.

Enter your mobile number in the “phone number” box using an international format.



A code will then be texted to your phone. Enter the code into the browser window.



Select your security questions and answers next. These questions are required for your identification should you ever have problems with MFA.

With the help of security questions you can access the MFA portal if your chosen MFA method does not work (e.g. because you have left your mobile at home or changed your mobile number). However, you cannot access a MFA-protected application (e.g. a VPN) with the security questions. You always need your phone for that.

Please note: Save your question/answer pairs in a password vault. It's a great way to protect them from publication or loss.

This concludes your registration. If required, you now have the possibility for additional configuration.

4. MFA methods

There are three options for the use of MFA. In addition to **SMS** (texts), as mentioned in the registration section, you can opt to use the **mobile app** or a **phone call**:

4.1. Mobile app

Select this option to use push notifications to the mobile Microsoft Authenticator app to authenticate. The page continues to load until the push notification has been confirmed.

Requirements:

- Smartphone (iOS, Android or Windows 10 mobile) with internet access.
- Die *Microsoft Authenticator* app

Pros:

- Considered the safest option of the three
- Works without phone number

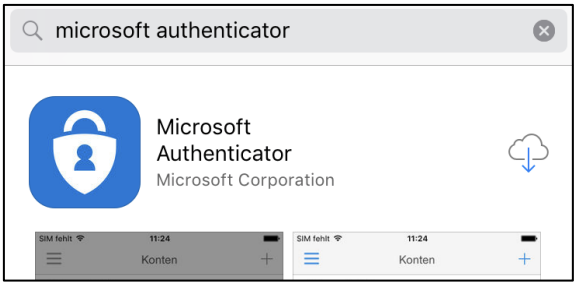
Cons:

- Does not work without internet access

Configuration:

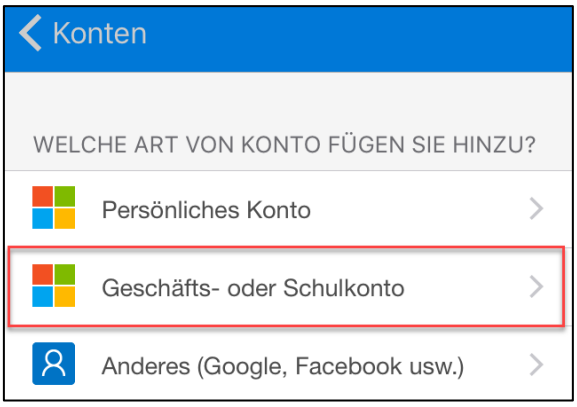
Select *activate mobile application*.

Generate an activation code.



Install the free “Authenticator” app from Microsoft on your smartphone. Search for *Microsoft Authenticator* in your....

- iOS = App Store
- Android = Play Store
- Windows Mobile = Microsoft Store



Launch the app and add an account by selecting *business or school account*.

Now, scan the QR code in the browser window with the app.

Please note: Activation code and URL are only required if there is no camera available to scan the QR code.

The account has been added and the mobile application set up.

To select the mobile app as your method, click on the *change method* link in the navigation menu and, to use the app, select *mobile app* as your method.

Confirm your entry with *complete activation*.

4.2. SMS

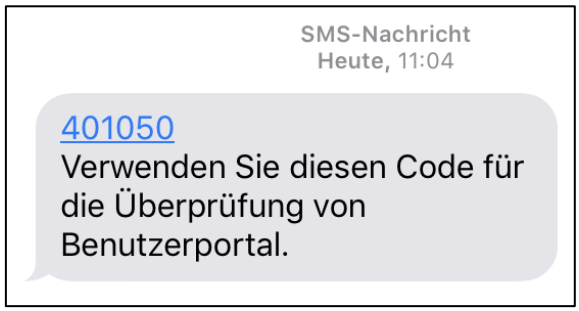
Select this method to be sent a text (SMS) for the authentication.

Requirements:
- Mobile phone with SIM card
- Mobile signal

Pros:
- Works without internet access

Cons:
- Requires a mobile signal or a landline

Utilisation:



If you pick the SMS method, you will be sent a 6-digit code via text every time you sign in. You will then have to type it into the browser window. The code is only valid for one use - you will be sent a new one for each sign-in.

4.3. Phone call

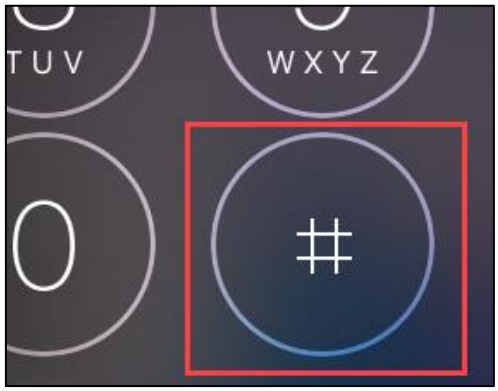
Select this method to receive a phone call for your authentication.

Requirements:
- Phone number to be called on.

Pros:
- Works with mobile and landline

Cons:
- Might cause roaming charges abroad

Application:



If you select the phone call, you will receive a phone call for each sign-in. A voice will prompt you to press the # key. As soon as you have done this, you will be signed in and you may terminate the call.

5. Practical example: VDI access

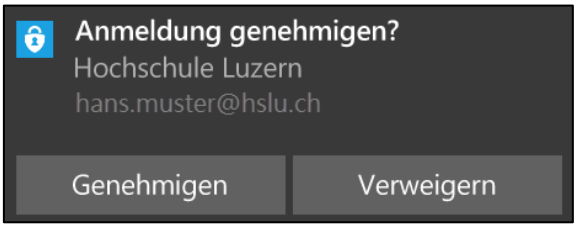
You have selected and set up at least one MFA method from point 4. You now have access to applications that require MFA.

The following example illustrates how MFA is used to access VDI (Virtual Desktop Infrastructure).

When accessing https://vdi.hslu.ch from outside the campus network, an additional authentication factor is required.

Enter your user name and password and click *sign in*.

The page continues to load until you confirm the notification on your smartphone or if the page times out.

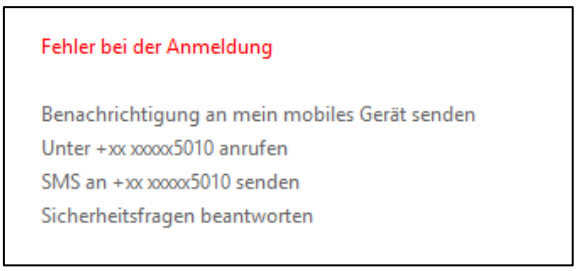


You will then (irrespective of your chosen MFA method) receive a code via SMS or push notification (see image) or a phone call.

Once the MFA is completed, you have full access to https://vdi.hslu.ch .

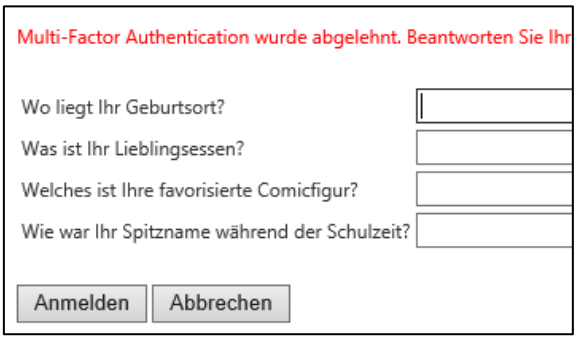
6. Error during MFA portal registration

If the application fails (e.g. smartphone unavailable), you may still use the platform, e.g. by answering the security questions.



If the MFA remains unanswered for just under two minutes, the browser will display the following options (see image)

Select answer security questions, e.g. to use MFA independent of a smartphone.

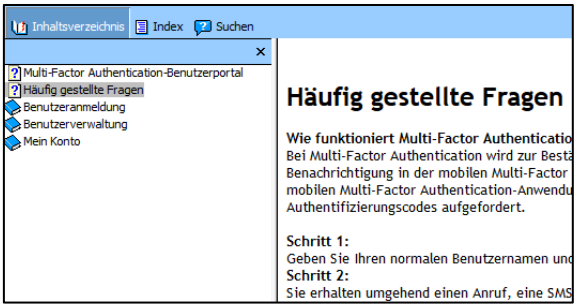


Answer your security questions to sign in.

Important: If you do not know your phone number on file, make sure to contact the IT Helpdesk (https://hslu.ch/helpdesk)

7. FAQs

Click on *help* under https://mfa.hslu.ch to find answers to frequently asked questions.



There, you will find answers to questions such as “What happens if I lose my phone?”

8. Unprompted requests

What is the problem if I receive a MFA phone call, text or notification in the app even though I am not trying to sign in anywhere?

This only happens if a third party attempts to sign into your account, and if this person already knows your password. Please consider that phone calls, texts and notifications in the app are only initiated after a successful verification of user name and password.
In this case MFA has actually saved you from unauthorised access. You may also temporarily block your account for any authentication attempts (by getting in touch with the IT Services helpdesk) if you like.