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

onPrem MFA (Multifaktor-Authentifizierung)

Kurzbeschrieb:	Benutzeranleitung zum MFA-Portal der Hochschule Luzern (onPrem MFA)	
Klassifikation:	☐ IT intern	☒ Public
	☐ Andere	
Kundengruppe:	☒ HSLU	☒ PHLU
	☐ Andere	
Rolle:	☒ Mitarbeitende/Doz.	☒ Studierende
	☐ Andere	
Geräteverwaltungstyp:	☒ HSLU/PHLU-Geräte	☒ Private Geräte
	☐ Andere	
Betriebssystem:	☒ Windows	☒ Mac
	☐ Andere	
Publikation:	☒ hslu.ch/helpdesk	☒ Intranet
	☐ Andere	

Support:	Web:	hslu.ch/helpdesk
	E-Mail:	informatikhotline@hslu.ch
	Tel:	041 / 228 21 21
	Portal:	helpdesk.hslu.ch

Änderungsverzeichnis

Version	Datum	Status	Änderungen und Bemerkungen	Bearbeitet von
1.0	05.05.2017		Dokument erstellt	NiL
1.1	08.05.2017		Dokument ergänzt	GrP
1.2	09.05.2017		Dokument ergänzt	GrP
1.3	10.05.2017		Dokument ergänzt	GrP
1.4	21.06.2017		Dokument angepasst	NiL
1.5	09.05.2019		Dokument angepasst	Kju, Poa
1.6	08.01.2020		Änderung BKZ-GS	ReM

Inhaltsverzeichnis

1. Warum MFA

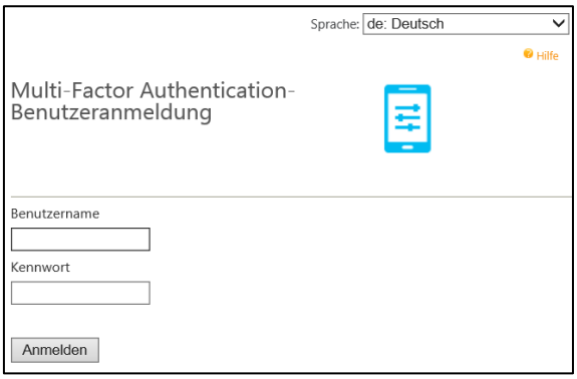
Um das Risiko von unberechtigtem Zugriff zu minimieren, wird mittels Kombination unterschiedlicher und insbesondere unabhängiger Komponenten (Faktoren) der Zugang zu einigen Anwendungen an der Hochschule Luzern durch MFA geschützt.

2. Voraussetzungen / Anforderungen

Folgende Voraussetzungen müssen erfüllt sein, um das MFA-Portal verwenden zu können:

- gültiges Benutzerkonto HSLU/PHLU/BKZ-GS
- Smartphone mit Internetzugang ODER Mobiltelefon mit SIM-Karte ODER Telefonanschluss

3. Registrierung



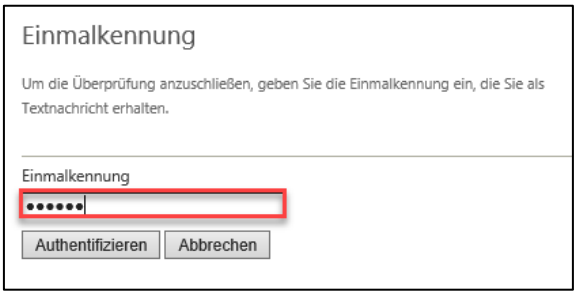
Öffnen Sie https://mfa.hslu.ch und melden Sie sich mit Benutzername und Kennwort an.

Hinweis: Bei Probleme mit der Anmeldung bitte Punkt 6 beachten.

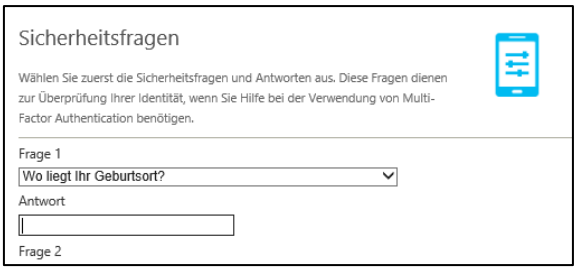
Wählen Sie die gewünschte Authentifizierungsmethode. Standardmässig wird SMS (Textnachricht) als Authentifizierungsmethode vorgeschlagen und hier als Beispiel verwendet.

Hinweis: Eine Übersicht der anderen Authentifizierungsmethoden finden Sie unter Punkt 4)

Unter Rufnummer fügen Sie Ihre Mobilfunknummer im internationalen Format ein.



Sie erhalten daraufhin eine SMS mit einem Code. Tragen Sie diesen Code im Browserfenster ein.



Wählen Sie als nächstes die Sicherheitsfragen und -antworten aus. Diese Fragen dienen zur Überprüfung Ihrer Identität, wenn Sie Probleme bei der Verwendung von MFA haben.

Mithilfe der Sicherheitsfragen können Sie auf das MFA-Portal zugreifen, falls Ihre gewählte MFA-Methode nicht funktioniert (z.B. Handy vergessen oder Handynummer gewechselt). Mit den Sicherheitsfragen, können Sie aber nicht auf eine MFA-geschützte Anwendung (z.B. VPN) zugreifen. Dafür wird immer ein Telefon benötigt.

Hinweis: Legen Sie Ihre Fragen-/Antworten-Paare ein einem Passworttresor ab. So sind sie vor Offenlegung und Verlust geschützt.

Damit ist die Registrierung abgeschlossen. Bei Bedarf haben Sie nun die Möglichkeit, weitere Einstellungen vorzunehmen.

4. MFA-Methoden

Es stehen drei Varianten zur Nutzung von MFA zur Verfügung. Nebst **SMS**, wie bereits bei der Registrierung erwähnt, stehen zudem **Mobile App** und **Telefonanruf** zur Auswahl:

4.1. Mobile App

Wählen Sie diese Methode aus, um sich mithilfe von Push-Benachrichtigungen an die mobile Microsoft Authenticator-App zu authentifizieren. Die Seite ist so lange am Laden, bis die Push-Benachrichtigung bestätigt wird.

Anforderungen:
- Smartphone (iOS, Android oder Windows 10 Mobile) mit Internetzugang
- Die *Microsoft Authenticator* App

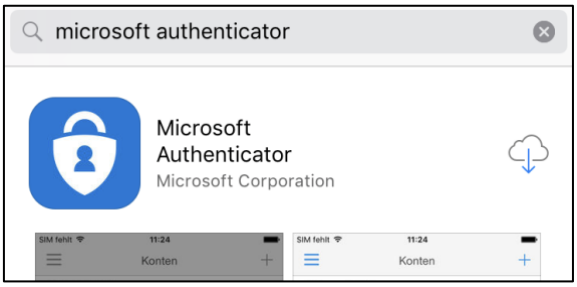
Vorteile:
- Gilt als sicherste der drei Methoden
- Funktioniert ohne Telefon-Nr.

Nachteile:
- Funktioniert nicht ohne Internetzugang

Einrichtung:

Wählen Sie *Mobile Anwendung aktivieren*.

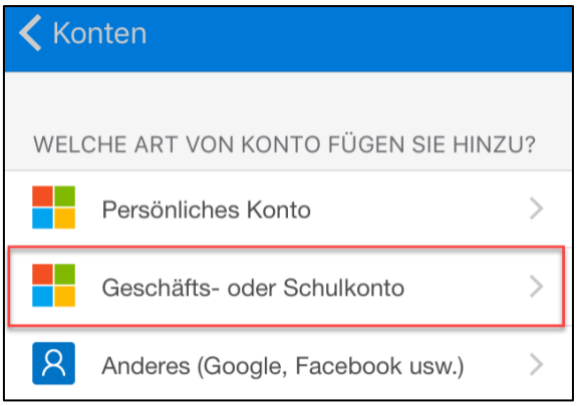
Generieren Sie den Aktivierungscode.



Installieren Sie die kostenlose Authenticator App von Microsoft auf Ihrem Smartphone. Suchen Sie dazu im…

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

…nach *Microsoft Authenticator*.



Starten Sie die App und fügen Sie ein Konto hinzu, indem Sie *Geschäfts- oder Schulkonto* wählen.

Scannen Sie nun mit der App den QR-Code aus dem Browserfenster.

Hinweis: Aktivierungscode und URL wird nur benötigt, wenn keine Kamera zum Scannen des QR-Code zur Verfügung steht.

Das Konto wurde hinzugefügt und die Mobile Anwendung damit eingerichtet.

Um die Mobile App als Methode auszuwählen, klicken Sie im Navigationsmenü auf den Link *Methode ändern*, und wählen Sie als Methode *Mobile App* an, um die App zu verwenden.

Bestätigen Sie die Eingabe mit *Aktivierung abschliessen*.

4.2. SMS

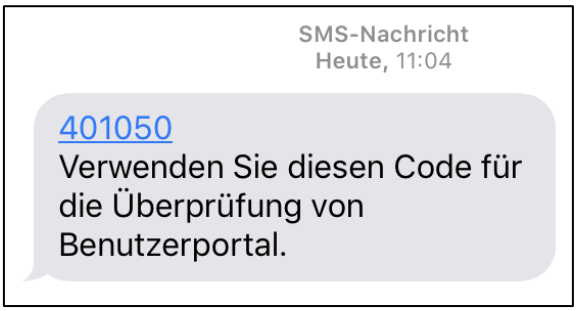
Wählen Sie diese Methode aus, um eine SMS zur Authentifizierung zu erhalten.

Anforderungen:
- Mobiltelefon mit SIM-Karte
- Mobilfunkempfang

Vorteile:
- Funktioniert ohne Internetzugang

Nachteile:
- Benötigt Mobilfunkempfang oder Festnetzanschluss

Anwendung:



Wenn Sie sich für die SMS Methode entscheiden, erhalten Sie bei jeder Anmeldung einen 6-stelligen Code per SMS, welchen Sie dann in Ihrem Browserfenster eingeben müssen. Der Code ist nur einmal gültig und bei jeder Anmeldung wird Ihnen ein neuer Code zugeschickt.

4.3. Telefonanruf

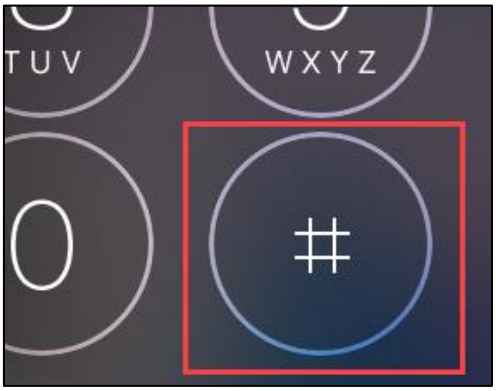
Wählen Sie diese Methode aus, um einen Telefonanruf zur Authentifizierung zu erhalten.

Anforderungen:
- Telefon-Nr. um Anruf entgegen nehmen zu können

Vorteile:
- Funktioniert mit Mobilfunk und Festnetz

Nachteile:
- Verursacht im Ausland möglicherweise Roaming-Kosten

Anwendung:



Entscheiden Sie sich für den Telefonanruf, so werden Sie bei der Anmeldung angerufen. Eine Stimme fordert sie dazu auf die # Taste zu drücken. Sobald Sie dies getan haben, werden Sie angemeldet und der Telefonanruf kann beendet werden.

5. Praxisbeispiel: VDI-Zugriff

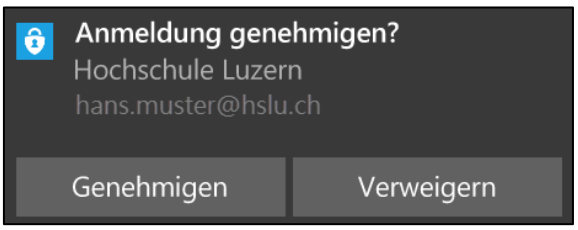
Sie haben sich für mindestens eine MFA-Methode aus Punkt 4 entschieden und diese eingerichtet; dann können Sie nun auf Anwendungen zugreifen, welche MFA erfordern.

Im nachfolgenden Beispiel wird gezeigt, wie MFA beim Zugriff auf VDI (Virtual Desktop Infrastructure) verwendet wird.

Beim Zugriff auf https://vdi.hslu.ch von ausserhalb des Campus-Netzwerk, wird ein zusätzlicher Authentifizierungsfaktor benötigt.

Geben Sie Ihren Benutzernamen und Ihr Passwort ein und klicken auf *Anmeldung*.

Die Seite lädt solange, bis Sie die Meldung auf Ihrem Smartphone bestätigen oder die Seite in ein Timeout fällt.

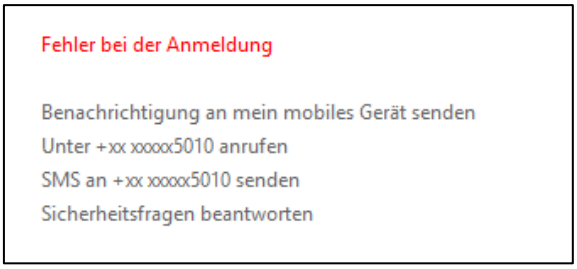


Daraufhin erhalten Sie (abhängig davon, welche MFA Methode Sie gewählt haben) einen Code per SMS oder eine Push-Nachricht (siehe Abbildung) oder einen Anruf.

Nach erfolgter MFA steht Ihnen der Inhalt von https://vdi.hslu.ch zur Verfügung.

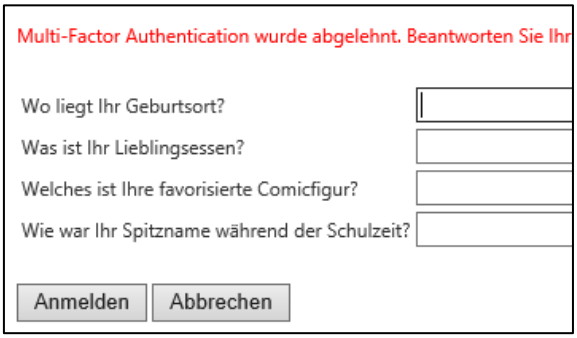
6. Fehler bei der MFA-Portal-Anmeldung

Schlägt die Anmeldung fehl (z.B. Smartphone nicht zur Hand) können Sie das Portal trotzdem verwenden, indem Sie z.B. die Sicherheitsfragen beantworten:



Bleibt die MFA Anfrage knapp zwei Minuten unbeantwortet, zeigt der Browser folgende Optionen (siehe Bild)

Wählen Sie *Sicherheitsfragen beantworten* um z.B. MFA ohne Smartphone zu verwenden.

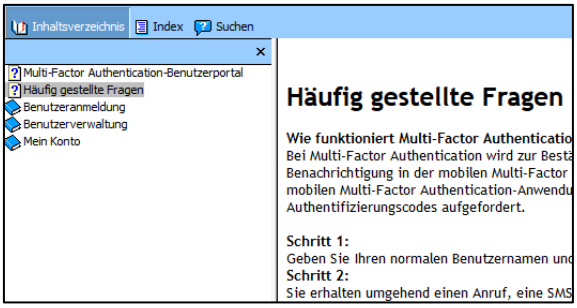


Beantworten Sie Ihre Sicherheitsfragen, um sich anzumelden.

Wichtig: Falls Ihnen die hinterlegte Rufnummer oder Sicherheitsfragen unbekannt sind, kontaktieren Sie unbedingt den IT Helpdesk (https://hslu.ch/helpdesk)

7. Häufig gestellte Fragen

Antworten auf häufig gestellte Fragen finden Sie, indem Sie unter https://mfa.hslu.ch auf *Hilfe* klicken.



Sie finden darin Antworten wie z.B. „Was passiert, wenn mein Telefon verloren geht?“

8. Unaufgeforderte Anfragen

Was ist, wenn ich von MFA einen Telefonanruf, eine SMS oder eine Benachrichtigung in der App erhalte, obwohl ich gar nicht versuche, mich irgendwo anzumelden?

Dies geschieht nur, wenn jemand anders versucht, sich bei Ihrem Konto anzumelden, und dieser Person Ihr Kennwort bereits bekannt ist. Bedenken Sie, dass Anrufe, SMS und Benachrichtigungen in der App nur dann erfolgen, wenn Benutzername und Kennwort bereits überprüft wurden.
In diesem Fall wurden Sie durch MFA also vor einem unerlaubten Zugriff bewahrt. Sie können Ihr Konto auch vorübergehend für Authentifizierungsversuche sperren, indem Sie Sich beim Helpdesk von IT Services melden.