

Finanzdepartement

Dienststelle Informatik

Postfach 3439

6002 Luzern

Paketadresse: Ruopigenplatz 1, 6015 Luzern

Telefon 041 228 56 15

informatik@lu.ch

informatik.lu.ch

Umstellung auf Microsoft Entra ID

Anleitung zur Passwort- und MFA Zurücksetzung (Self-Service)

für Lernende, Lehrpersonen und Mitarbeitenden an kantonalen Schulen

Inhalt

1 Einleitung	3
2 Benutzererfassung und Passwortausgabe	3
3 Zugang zu kantonalen Systemen	3
4 Passwortänderung	4
4.1 Einleitung	4
4.2 Übersicht: Was ändert sich	4
4.3 Neue Anmeldemaske	4
4.4 Passwort-Rücksetzung (Self-Service)	5
4.5 Passwort abgelaufen – iWP mit PIN & Gesichtserkennung	7
5 Alternative Authentifizierungsmethode für MFA registrieren	8
6 MFA zurücksetzen (Self-Service) – Neues Smartphone	13
7 Benutzer mit FIDO2 (2FA Alternative)	19
8 Weisung Benutzernamen und Passwörter (Passwort-Policy)	19
9 Hilfe	20

Zweck des Dokuments / Ausgangslage

Dieses Dokument beschreibt den Umgang mit dem persönlichen kantonalen Benutzerkonto und beinhaltet Informationen zur Passwortregistrierung und –Rücksetzung.

1 Einleitung

Die Anleitung liefert Informationen wie das Passwort für Lernende, Lehrpersonen und Mitarbeitenden an kantonalen Schulen zurückgesetzt werden kann. Zudem gibt es Hinweise wie eine alternative Authentifizierungsmethode registriert und bei einem Smartphone-Wechsel die MFA zurückgesetzt werden kann.

2 Benutzererfassung und Passwortausgabe

Die Schuladministrationssoftware schulNetz ist das Basistool für die Erfassung aller Personen aus dem Schulumfeld. Mit der Erfassung einer Person kann auch gleichzeitig ein kantonales Benutzerkonto bestellt werden.

In einer automatischen Verarbeitung wird in der kommenden Nacht das Benutzerkonto erstellt. Die Zugangsdaten werden dem Besteller zugestellt. Mit Benutzernamen/Passwort erhält der künftige Benutzer eine elektronische Identität.

Es gibt unterschiedliche Benutzergruppen:

- Lernende (**vorname_nachname@sluz.ch**)
- Lehrpersonen (**vorname.nachname@sluz.ch**)
- Angestellte der kantonalen Schulverwaltung (**vorname.nachname@edulu.ch**)

3 Zugang zu kantonalen Systemen

Gleichzeitig zum kantonalen Benutzerkonto mit Benutzername und Passwort, erhält der Benutzer je nach Rolle und Berechtigung umfassenden Zugriff auf folgende Services:

- PC am Schulstandort
- Exchange-Konto (E-Mail-Adresse für @sluz.ch)
- Berechtigungen auf verschiedene Datenbereiche (Laufwerk G:, Z:, usw.)
- persönliches M365-Konto (ehemals O365)
- Internet
- SharePoint (Intranet, Teambereiche, Projektbereiche, usw.)
- WLAN am Schulstandort
- Webmail (OWA)
- Netzwerk-Drucker

Zusätzliche Services sind über den Servicekatalog im [Self Service Portal](#)¹ zu bestellen.

¹ Diese Seite ist nur mit einem EDULU-Login erreichbar.

4 Passwortänderung

Das Passwort muss selbständig zurückgesetzt werden, vorausgesetzt die Registrierung von Microsoft Authenticator 2FA M365 (siehe separate Anleitung) wurde erfolgreich durchgeführt.

Wenn die Registrierung Authenticator 2FA M365 noch nicht durchgeführt wurde, kann eine Passwortänderung nicht ausgeführt werden. Zudem kann dein Sekretariat, ICT-Koordinator oder den DIIN Service-Desk keine manuellen Passwortänderungen vornehmen.

Passwortänderung mit CTRL-ALT-DEL und Link <https://pwdreset.sso.sluz.ch> nicht mehr benutzen, da die Synchronisierung zu Entra ID nicht sofort ausgeführt wird und länger dauert.

Passwortänderung für Benutzerkonto mit @lu.sluz.ch siehe Kapitel 4.4 analog @sluz.ch.

4.1 Einleitung

Gemäss kantonomer Sicherheitsvorgabe muss das persönliche Passwort regelmässig, spätestens aber nach jeweils 365 Tagen geändert werden. Der Benutzer erhält dabei 45, 24, 8 und 1 Tag(e) vor dem Ablauf entsprechende Informationen per E-Mail, dass das Passwort demnächst abläuft.

Die Passwortrichtlinien für das kantonale Benutzerkonto finden Sie unter dem Weblink <https://informatik.lu.ch/Passwortrichtlinien>.

4.2 Übersicht: Was ändert sich

Die Anmeldung bei Microsoft 365 wird modernisiert. Damit stehen folgende Funktionen zur Verfügung, die die Verwaltung deines Kontos vereinfachen:

- Passwort zurücksetzen über «Kennwort vergessen» auf der neuen Anmeldemaske (siehe Kapitel 4.4) oder über <https://mylogin.microsoft.com/security-info/password/change>.
- MFA (Multi-Faktor-Authentifizierung) zurücksetzen über <https://mylogin.microsoft.com/security-info> (siehe Kapitel 6)

4.3 Neue Anmeldemaske

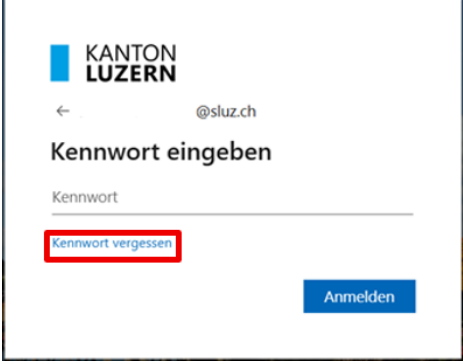
Beim Login erscheint künftig folgende neue Anmeldemaske:

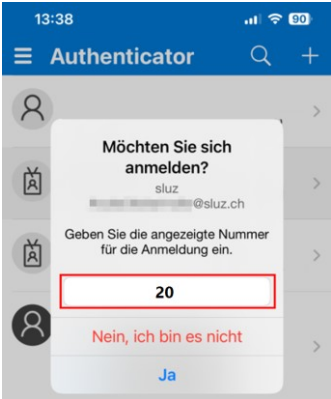


4.4 Passwort-Rücksetzung (Self-Service)

Mit «Kennwort vergessen» kann ein Passwortwechsel bei der Anmeldemaske erzielt werden.

Alternativer Link für Passwort-Rücksetzung: <https://mysignins.microsoft.com/security-info/pass-word/change>

	1. In der Anmeldemaske auf «Kennwort vergessen» klicken.
	2. Eingabe von Benutzername bzw. E-Mail-Adresse und Zeichen unten in der Abbildung. Auf «Weiter» klicken.
	3. Klicke auf «Ich habe mein Kennwort vergessen». Auf «Weiter» klicken.

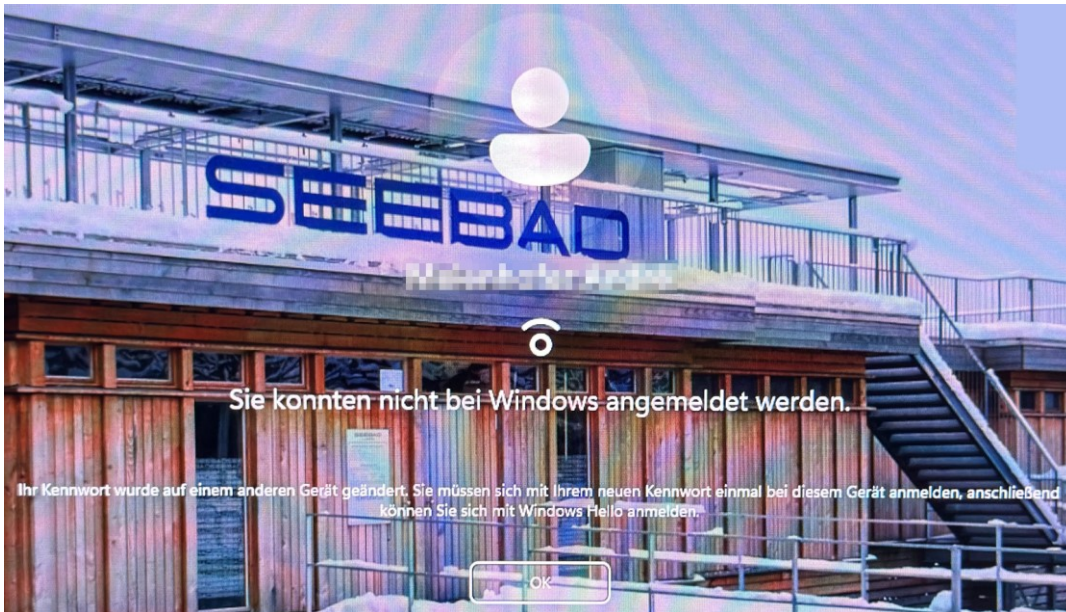
 KANTON LUZERN Konto wieder aktivieren Überprüfungsschritt 1 > Neues Kennwort auswählen Wählen Sie die Kontaktmethode aus, die zur Überprüfung verwendet werden soll: ☒ Benachrichtigung in meiner Authenticator-App bestätigen ☐ Code aus meiner Authenticator-App eingeben Senden Sie eine Benachrichtigung an Ihre Authenticator-App auf Ihrem Mobilgerät. Benachrichtigung senden Abbrechen	4. Nun folgt die Überprüfung, ob das Konto korrekt mit der App verbunden worden ist. Auf «Benachrichtigung in meiner Authenticator-App bestätigen» und «Benachrichtigung senden» klicken.
Konto wieder aktivieren Überprüfungsschritt 1 > Neues Kennwort auswählen Wählen Sie die Kontaktmethode aus, die zur Überprüfung verwendet werden soll: ☒ Benachrichtigung in meiner Authenticator-App bestätigen ☐ Code aus meiner Authenticator-App eingeben Genehmigen Sie die Benachrichtigung, die wir an Ihre App senden, indem Sie die untenstehende Nummer eingeben. → 20	5. Es wird auf dem Computer eine Zahl angezeigt.
	6. In der Authenticator-App auf dem Smartphone erscheint nun die Frage, ob man sich anmelden möchte. Die Zahl von ihrem Computer (roter Kreis) muss im umrandeten Feld auf dem Smartphone eingegeben werden. Mit «Ja» bestätigen.
Konto wieder aktivieren Überprüfungsschritt 1 ✓ > Neues Kennwort auswählen * Neues Kennwort eingeben: * Neues Kennwort bestätigen: Fertig stellen Abbrechen	7. Ein neues Kennwort mit Bestätigung eingeben. Auf «Fertig stellen» klicken.

4.5 Passwort abgelaufen – iWP mit PIN & Gesichtserkennung

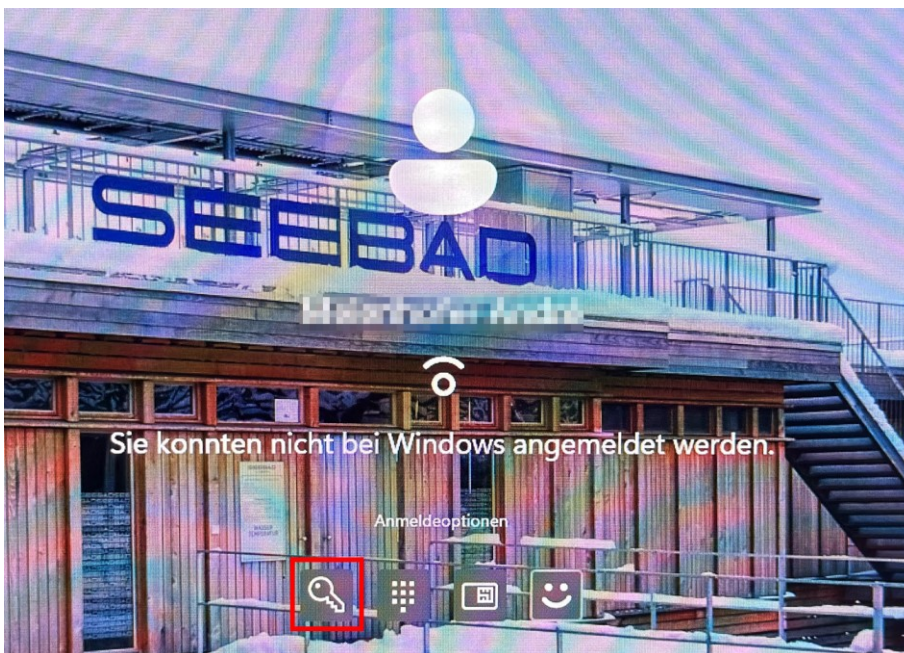
Gemäss kantonomer Sicherheitsvorgabe muss das persönliche Passwort regelmässig, spätestens aber nach jeweils 365 Tagen geändert werden.

Wenn das Passwort abgelaufen ist, kann eine Anmeldung am PC/Notebook mit PIN oder Gesichtserkennung (Kamera) nicht durchgeführt werden.

Sobald das Passwort geändert wurde, erscheint folgendes Bild:



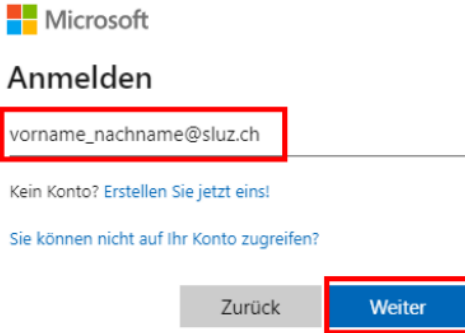
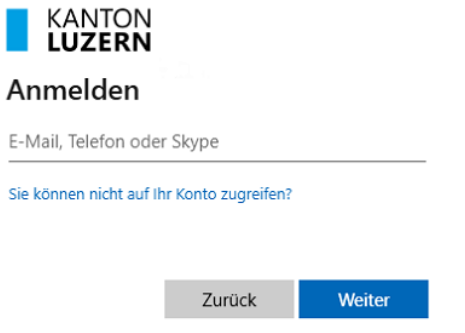
Danach muss zuerst bei der Anmeldung bei "Anmeldeoptionen" das Schlüssel-Symbol ausgewählt und das neue Passwort eingegeben werden. Danach funktioniert bei der nächsten Anmeldung der PIN oder Gesichtserkennung wieder.



5 Alternative Authentifizierungsmethode für MFA registrieren

Damit du deine Microsoft Authenticator App selbständig zurücksetzen kannst (z.B. bei einem neuen Smartphone), musst du vorab eine alternative Authentifizierungsmethode registrieren.

Dies kann jegliche Authenticator App sein wie z. B. auch Microsoft Authenticator oder Google Authenticator.

	1. Öffne die folgende Webseite auf deinem PC (nicht Smartphone): https://mysignins.microsoft.com/security-info Dein SLUZ-Benutzernamen eingeben. Auf «Weiter» klicken.
	2. Den SLUZ-Benutzernamen eingeben und auf «Weiter» klicken.
	3. Das Kennwort eingeben und auf «Anmelden» klicken.

Anmeldeanforderung bestätigen

- Öffnen Sie Ihre Authenticator-App, und genehmigen Sie die Anforderung. Geben Sie die Nummer ein, wenn Sie dazu aufgefordert werden.

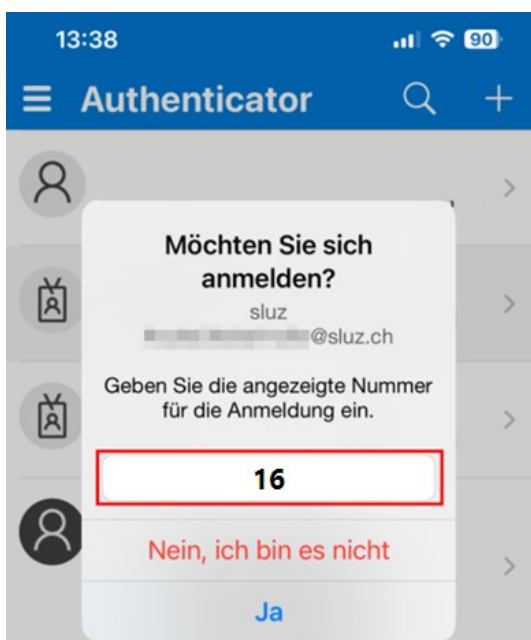
16

Haben Sie keine Anmeldeanforderung erhalten?
Wischen Sie nach unten, um den Inhalt in Ihrer App zu aktualisieren.

Ich kann meine Microsoft Authenticator-App im Moment nicht verwenden.

[Weitere Informationen](#)

4. Es erscheint auf dem Computer die Meldung die Aufforderung zur Anmeldeanforderung bestätigen.



5. In der Authenticator-App auf dem Smartphone erscheint nun die Frage, ob man sich anmelden möchte. Die Zahl von ihrem Computer muss im umrandeten Feld auf dem Smartphone eingegeben werden.

Mit «Ja» bestätigen.

Sicherheitsinformationen

Die folgenden Methoden werden zum Anmelden bei Ihrem Konto oder zum Zurücksetzen Ihres Kennworts verwendet.

+ Anmeldemethode hinzufügen

☰ Kennwort

Zuletzt aktualisiert:
vor einem Monat

[Ändern](#)

6. «Anmeldemethode hinzufügen» wählen.

Anmeldemethode hinzufügen ×  Microsoft Authenticator Anmeldeanforderungen genehmigen oder Einmalcodes verwenden	7. «Microsoft Authenticator» wählen.
Microsoft Authenticator installieren ×  Installieren Sie die App auf Ihrem mobilen Gerät und kehren Sie dann hierher zurück, um fortzufahren.   Andere App für die Authentifizierung einrichten Zurück Weiter	8. Es erscheint die Aufforderung die Authenticator-App zu installieren. Falls die App auf dem Mobiltelefon bereits eingerichtet worden ist, «Andere App für die Authentifizierung einrichten» wählen. Falls die App «Authenticator» auf dem Mobiltelefon noch nicht installiert worden ist, kann diese via App Store (iPhone) oder Play Store (Android) installiert werden.
Konto in der App einrichten ×  Fügen Sie zunächst Ihr Konto hinzu. Zurück Weiter	9. Es erscheint Fenster «Konto in der App einrichten». Auf «Weiter» klicken.

QR-Code scannen Verwenden Sie Ihre Authenticator-App, um den QR-Code zu scannen. Auf diese Weise wird die App mit Ihrem Konto verknüpft. Kehren Sie dann zurück und wählen Sie Weiter aus. Can't scan the QR code? Zurück Weiter	10. Es erscheint ein QR-Code auf deinem Computer Bildschirm. Mit der Authenticator App deiner Wahl (z. B. Microsoft Authenticator oder Google Authenticator) den QR-Code scannen. Auf «Weiter» klicken.
sluz XXXXXXXXXXXX@sluz.ch sluz XXXXXXXXXXXX@sluz.ch 224 109 3	11. Die alternative Authenticator App auf dem Smartphone öffnen und das SLUZ-Konto antippen.
Code eingeben Geben Sie den von Ihrer Authenticator-App generierten 6-stelligen Code ein. Code Zurück Weiter	12. Nun folgt ein Test zur Überprüfung, ob das Konto korrekt mit der App verbunden worden ist. Dazu wird auf dem Computer das Fenster für «Code eingeben» angezeigt. Den 6-stelligen «Code für Einmal-kennwort» auf dem Computer eingeben. Auf «Weiter» klicken.

✓ **Authenticator-App
hinzugefügt**



Verwenden Sie Codes aus dieser App, wenn Sie sich
das nächste Mal anmelden.

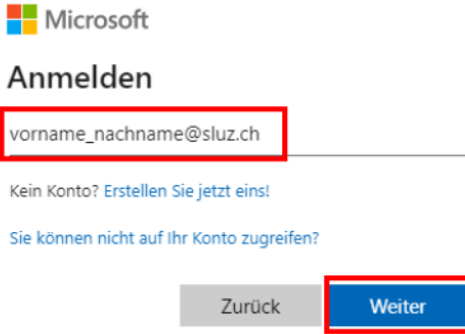
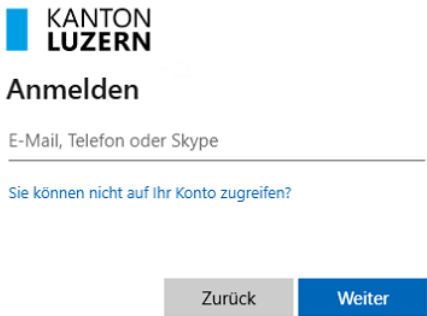
Fertig

13. Nachdem in der App die Authentifizierung bestätigt worden ist, erscheint die Meldung, dass die Authentifizierungsmethode erfolgreich hinzugefügt wurde.

Auf «Fertig» klicken.

6 MFA zurücksetzen (Self-Service) – Neues Smartphone

Hinweis: Ohne zusätzliche registrierte alternative Authentifizierungsmethode (siehe Kapitel 5) ist kein Self-Service MFA Reset möglich.

 The screenshot shows the Microsoft login page. At the top is the Microsoft logo. Below it is the heading 'Anmelden'. A text input field contains the email address 'vorname_nachname@sluz.ch', which is highlighted with a red rectangle. Below the input field are two links: 'Kein Konto? Erstellen Sie jetzt eins!' and 'Sie können nicht auf Ihr Konto zugreifen?'. At the bottom are two buttons: 'Zurück' (grey) and 'Weiter' (blue), with the 'Weiter' button highlighted by a red rectangle.	1. Öffne die folgende Webseite auf deinem PC (nicht Smartphone): https://mysignins.microsoft.com/security-info Dein SLUZ-Benutzernamen eingeben. Auf «Weiter» klicken.
 The screenshot shows the Kanton Luzern login page. At the top is the Kanton Luzern logo. Below it is the heading 'Anmelden'. A text input field is labeled 'E-Mail, Telefon oder Skype'. Below the input field is a link: 'Sie können nicht auf Ihr Konto zugreifen?'. At the bottom are two buttons: 'Zurück' (grey) and 'Weiter' (blue).	2. Den SLUZ-Benutzernamen eingeben und auf «Weiter» klicken.
 The screenshot shows the Kanton Luzern password screen. At the top is the Kanton Luzern logo. Below it is a back arrow and a text input field containing '@sluz.ch'. Below the input field is the heading 'Kennwort eingeben'. A password input field is shown with dots. Below the password field is a link: 'Kennwort vergessen'. At the bottom is a blue button labeled 'Anmelden'.	3. Das Kennwort eingeben und auf «Anmelden» klicken.

Anmeldeanforderung bestätigen

 Öffnen Sie Ihre Authenticator-App, und genehmigen Sie die Anforderung. Geben Sie die Nummer ein, wenn Sie dazu aufgefordert werden.

82

Haben Sie keine Anmeldeanforderung erhalten?
Wischen Sie nach unten, um den Inhalt in Ihrer App zu aktualisieren.

Ich kann meine Microsoft Authenticator-App im Moment nicht verwenden.

[Weitere Informationen](#)

4. Es erscheint auf dem Computer die Meldung die Aufforderung zur Anmeldeanforderung bestätigen.

Auf «**Ich kann meine Microsoft Authenticator-App im Moment nicht verwenden**» klicken.

Überprüfen Ihrer Identität



Eine Anforderung in meiner Microsoft Authenticator-App bestätigen

123

Verwenden eines Prüfcodes

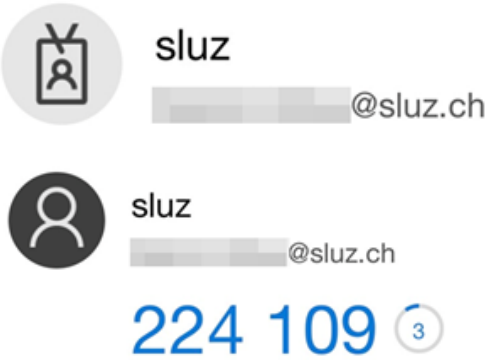
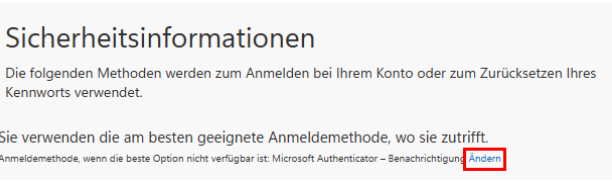
[Weitere Informationen](#)

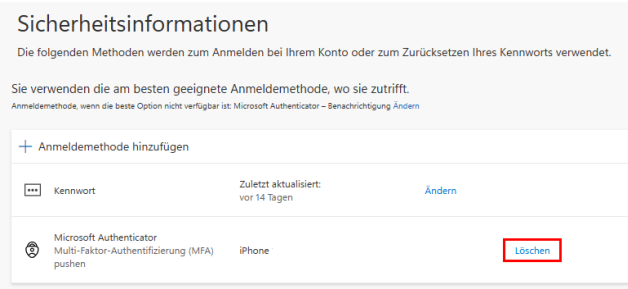
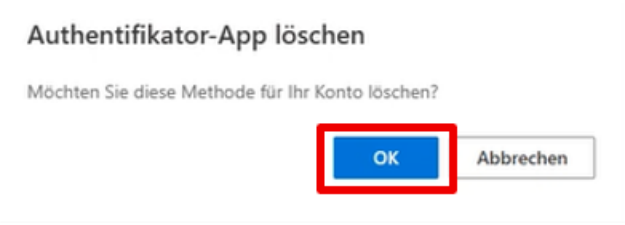
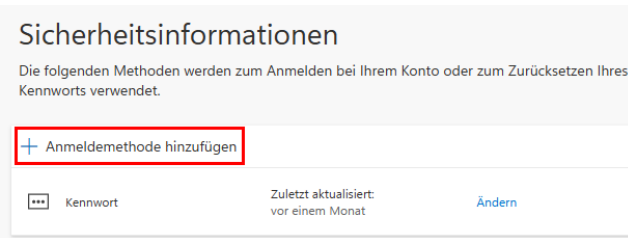
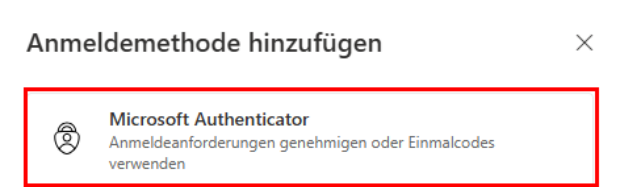
Sind Ihre Überprüfungsmethoden aktuell? Überprüfen sie unter <https://aka.ms/mfasetup>

Abbrechen

5. Es erscheint auf dem Computer die Meldung über die Überprüfung Ihrer Identität.

Auf «**Verwenden eines Prüfcodes**» klicken.

	6. Die alternative Authenticator App auf dem Smartphone öffnen und das SLUZ-Konto antippen.
	7. Den 6-stelligen «Code für Einmal-kennwort» auf dem Computer eingeben. Auf «Überprüfen» klicken.
	8. Bei Sicherheitsinformationen die Standardmethode ändern. Auf «Ändern» klicken.
	9. Es erscheint das Fenster Standardmethode ändern. Bei Dropdown-Menü die Methode «App-basierte Authentifizierung oder Hardwaretoken-...» auswählen. Auf «Bestätigen» klicken.

	10. Es erscheint das Fenster, dass die Standardanmeldemethode aktualisiert wurde.
	11. Bei Sicherheitsinformationen die alte Standardmethode von Microsoft Authenticator löschen. Auf «Löschen» klicken.
	12. Auf «OK» klicken.
	13. Es erscheint das Fenster, dass die Standardmethode gelöscht wurde.
	14. Anschliessend «Anmeldemethode hinzufügen» wählen.
	15. «Microsoft Authenticator» wählen.

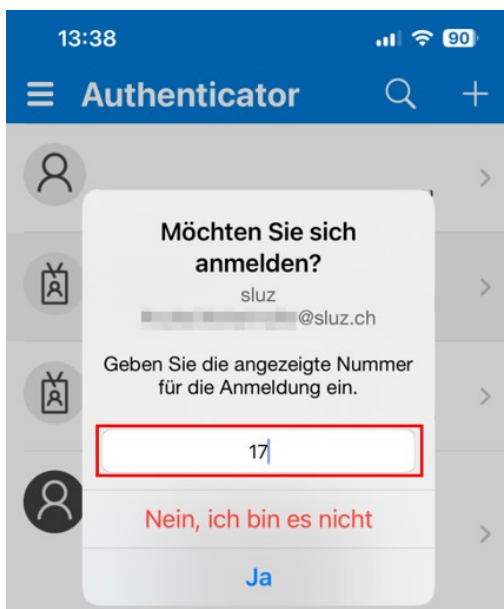
Microsoft Authenticator installieren Installieren Sie die App auf Ihrem mobilen Gerät und kehren Sie dann hierher zurück, um fortzufahren. Andere App für die Authentifizierung einrichten Zurück Weiter	16. Es erscheint Fenster «Microsoft Authenticator installieren». Auf «Weiter» klicken.
Konto in der App einrichten Fügen Sie zunächst Ihr Konto hinzu. Zurück Weiter	17. Es erscheint Fenster «Konto in der App einrichten». Auf «Weiter» klicken.
QR-Code scannen Verwenden Sie die Microsoft Authenticator-App, um den QR-Code zu scannen. Auf diese Weise wird die App mit Ihrem Konto verknüpft. Kehren Sie dann zurück und wählen Sie Weiter aus. Can't scan the QR code? Zurück Weiter	18. Es erscheint ein QR-Code auf ihrem Computer Bildschirm. Mit der geöffneten Microsoft Authenticator App den QR-Code scannen. Auf Weiter klicken.

Probieren wir es aus



Geben Sie die in der App angezeigte Nummer ein, um die Anmeldeanforderung zu genehmigen.

Zurück



19. Nun folgt ein Test zur Überprüfung, ob das Konto korrekt mit der App verbunden worden ist. Dazu wird auf dem Computer eine Zahl angezeigt.

In der Authenticator-App auf dem Smartphone erscheint nun die Frage, ob man sich anmelden möchte. Die Zahl von ihrem Computer (roter Kreis) muss im umrandeten Feld auf dem Smartphone eingegeben werden.

Mit «Ja» bestätigen.

✓ Authenticator Added



Sie können jetzt Microsoft Authenticator verwenden, um Anmeldungen zu genehmigen, einmalige Codes abzurufen und mehr.

Dies ist jetzt Ihre Standardanmeldemethode.

Fertig

20. Nachdem in der App die Authentifizierung bestätigt worden ist, erscheint die Meldung, dass die Authentifizierungsmethode erfolgreich hinzugefügt wurde.

Auf «Fertig» klicken.

7 Benutzer mit FIDO2 (2FA Alternative)

Benutzer, die den FIDO2-Sicherheitsschlüssel als Anmeldemethode verwenden, können ihr Passwort und MFA nicht selbstständig zurücksetzen. Diese Einschränkung besteht aufgrund technischer Vorgaben von Microsoft.

In diesem Fall gilt folgendes Vorgehen:

- Meldung an den M365 PowerUser der Schule
- Dieser eröffnet ein Ticket beim DIIN ServiceDesk
- Der DIIN ServiceDesk setzt dein Passwort / MFA zurück

8 Weisung Benutzernamen und Passwörter (Passwort-Policy)

Für die Mitarbeitenden des Kantons Luzern und die Lernenden an kantonalen Schulen sollen klare Regeln für den Umgang mit Benutzernamen und Passwörtern gelten und bekannt sein. Dazu gehören insbesondere Regeln für das Erstellen und das Anpassen von Benutzernamen und Passwörtern. So wird das Risiko des Eindringens eines Angreifers in die IT-Systeme des Kantons infolge nicht gesetzter, schwacher oder bekannter Passwörter reduziert.

Die Weisung finden Sie unter diesem Weblink: https://informatik.lu.ch/-/media/Informatik/Dokumente/Informationssicherheit/Dokumentenablage/W101_Weisung_Benutzernamen_Passwoerter.pdf.¹

Diese Weisung ist für alle Personen mit kantonalen Benutzerkonto verbindlich.

9 Hilfe

Falls Sie Unterstützung benötigen, wenden Sie sich bitte an:

- Ihre/n ICT-Koordinator/In oder IT-Verantwortliche/r Ihrer Organisation
- Häufig gestellte Fragen: <https://informatik.lu.ch/intern/faq>
- Serviceanfrage (Ticket): <https://it-serviceportal.lu.ch>¹
- servicedesk@lu.ch / 041 228 69 99

Änderungs-/Versionenkontrolle

Version	Datum	Status	Autor	Bemerkung
1.0	14.08.2023	Final	DIIN	
1.1	22.01.2024			
1.2	13.02.2024			
1.3	12.03.2024			
1.4	17.12.2024			
2.0	04.12.2025			
2.1	17.12.2025			
2.2	20.02.2026			



Finanzdepartement
Dienststelle Informatik
Ruopigenplatz 1
6015 Luzern

Telefon 041 228 56 15
www.informatik.lu.ch
informatik@lu.ch

¹ Diese Seite ist nur mit einem EDULU-Login erreichbar.