

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)	20
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 90 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://mysignins.microsoft.com/security-info/password/change>.
- MFA (Multi-Faktor-Authentifizierung) zurücksetzen über <https://mysignins.microsoft.com/security-info> (siehe Kapitel 6)

4.3 Neue Anmeldemaske




Beim Login erscheint künftig folgende neue Anmeldemaske:


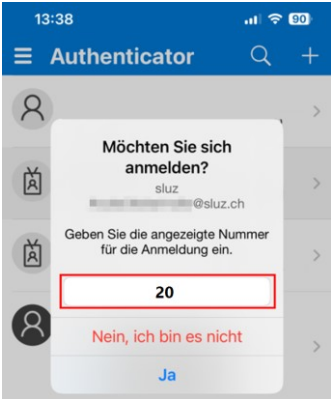


4.4 Passwort-Rücksetzung (Self-Service)

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>

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

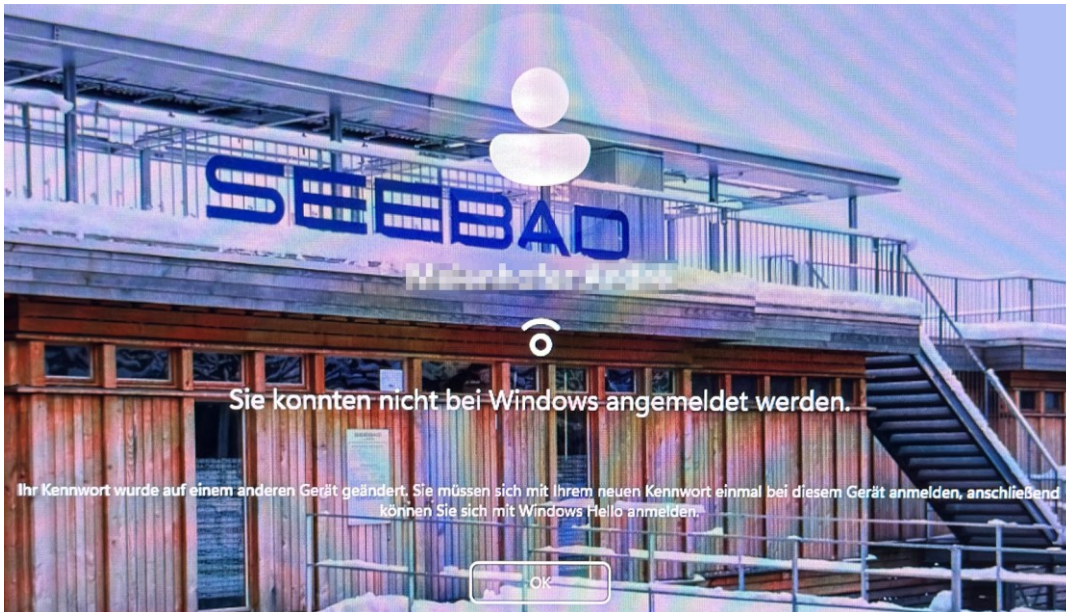
<div data-bbox="178 241 392 311">  KANTON LUZERN </div> <div data-bbox="178 322 497 358"> <h2>Konto wieder aktivieren</h2> </div> <div data-bbox="178 380 561 407"> <p>Überprüfungsschritt 1 > Neues Kennwort auswählen</p> </div> <div data-bbox="178 434 638 456"> <p>Wählen Sie die Kontaktmethode aus, die zur Überprüfung verwendet werden soll:</p> </div> <div data-bbox="178 477 647 600"> <div> <input checked="" type="radio"/> Benachrichtigung in meiner Authenticator-App bestätigen </div> <div> <input type="radio"/> Code aus meiner Authenticator-App eingeben </div> <div> <p>Senden Sie eine Benachrichtigung an Ihre Authenticator-App auf Ihrem Mobilgerät.</p> <p>Benachrichtigung senden</p> </div> </div> <div data-bbox="178 649 245 669"> <p>Abbrechen</p> </div>	<p>4. Nun folgt die Überprüfung, ob das Konto korrekt mit der App verbunden worden ist.</p> <p>Auf «Benachrichtigung in meiner Authenticator-App bestätigen» und «Benachrichtigung senden» klicken.</p>
<div data-bbox="178 763 521 801"> <h2>Konto wieder aktivieren</h2> </div> <div data-bbox="178 826 590 855"> <p>Überprüfungsschritt 1 > Neues Kennwort auswählen</p> </div> <div data-bbox="178 884 644 929"> <p>Wählen Sie die Kontaktmethode aus, die zur Überprüfung verwendet werden soll:</p> </div> <div data-bbox="178 952 558 1050"> <div> <input checked="" type="radio"/> Benachrichtigung in meiner Authenticator-App bestätigen </div> <div> <input type="radio"/> Code aus meiner Authenticator-App eingeben </div> </div> <div data-bbox="199 1066 651 1108"> <p>Genehmigen Sie die Benachrichtigung, die wir an Ihre App senden, indem Sie die untenstehende Nummer eingeben.</p> </div> <div data-bbox="260 1111 450 1140"> <p>→ 20</p> </div>	<p>5. Es wird auf dem Computer eine Zahl angezeigt.</p>
	<p>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.</p> <p>Mit «Ja» bestätigen.</p>
<div data-bbox="178 1711 517 1747"> <h2>Konto wieder aktivieren</h2> </div> <div data-bbox="178 1774 603 1800"> <p>Überprüfungsschritt 1 ✓ > Neues Kennwort auswählen</p> </div> <div data-bbox="178 1827 481 1995"> <div> <p>* Neues Kennwort eingeben:</p> <input type="password"/> </div> <div> <p>* Neues Kennwort bestätigen:</p> <input type="password"/> </div> <div> <p>Fertig stellen</p> </div> </div> <div data-bbox="300 1964 367 1984"> <p>Abbrechen</p> </div>	<p>7. Ein neues Kennwort mit Bestätigung eingeben.</p> <p>Auf «Fertig stellen» klicken.</p>

4.5 Passwort abgelaufen – iWP mit PIN & Gesichtserkennung

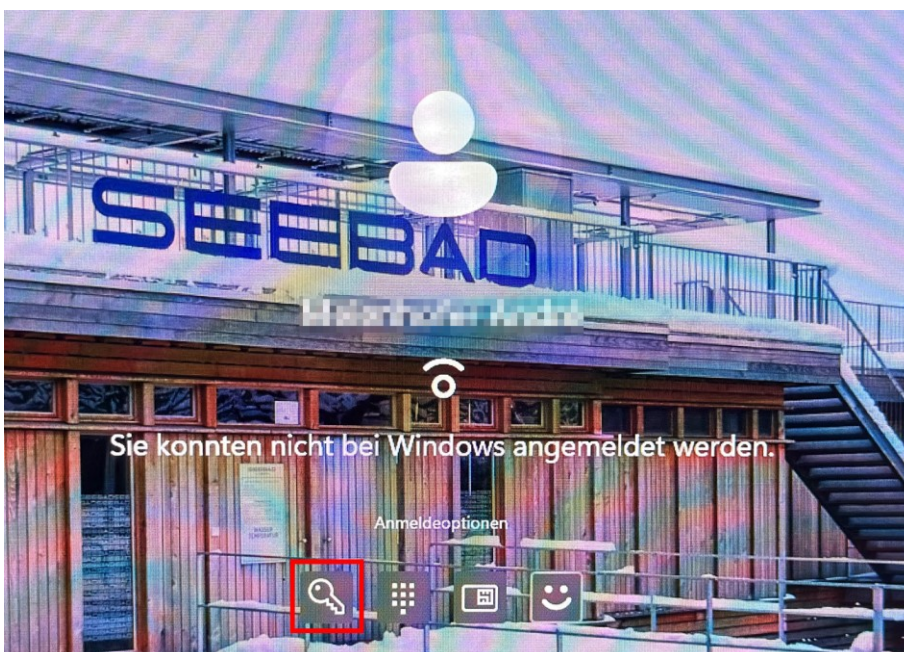
Gemäss kantonomer Sicherheitsvorgabe muss das persönliche Passwort regelmässig, spätestens aber nach jeweils 90 Tagen geändert werden.

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:



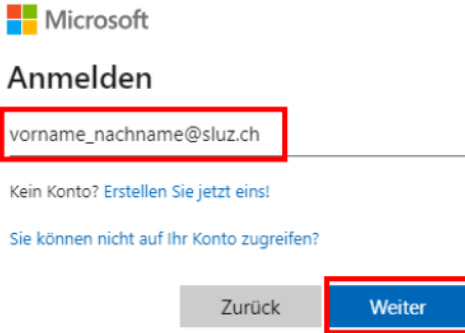
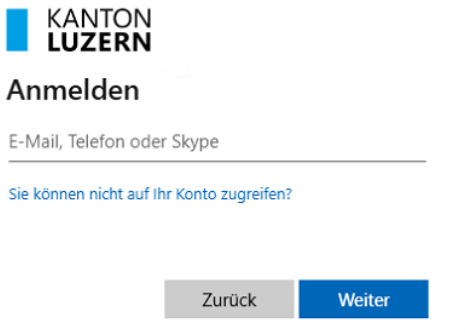

Danach muss zuerst bei der Anmeldung bei "Anmeldeoptionen" das Schlüssel-Symbol ausgewählt und das neue Passwort eingegeben werden. Danach funktioniert bei der nächsten Anmeldung der PIN oder Gesichtserkennung wieder.



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.

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

Anmeldeanforderung bestätigen

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

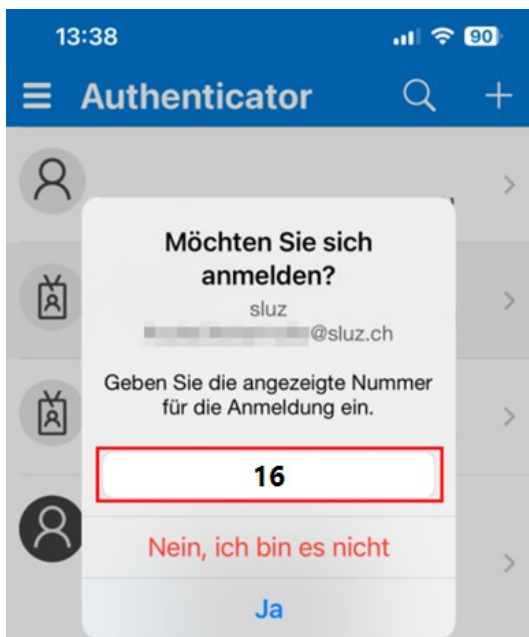
16

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.

<div data-bbox="188 241 766 280">Anmeldemethode hinzufügen ×</div> <div data-bbox="188 309 766 407">  Microsoft Authenticator Anmeldeanforderungen genehmigen oder Einmalcodes verwenden </div>	<p>7. «Microsoft Authenticator» wählen.</p>
<div data-bbox="199 562 601 629">Microsoft Authenticator installieren ×</div> <div data-bbox="328 669 483 860">  </div> <div data-bbox="199 875 606 920"> <p>Installieren Sie die App auf Ihrem mobilen Gerät und kehren Sie dann hierher zurück, um fortzufahren.</p> </div> <div data-bbox="199 936 360 983">  </div> <div data-bbox="387 936 545 983">  </div> <div data-bbox="199 1003 580 1032"> Andere App für die Authentifizierung einrichten </div> <div data-bbox="363 1048 611 1088"> Zurück Weiter </div>	<p>8. Es erscheint die Aufforderung die Authenticator-App zu installieren.</p> <p>Falls die App auf dem Mobiltelefon bereits eingerichtet worden ist, «Andere App für die Authentifizierung einrichten» wählen.</p> <p>Falls die App «Authenticator» auf dem Mobiltelefon noch nicht installiert worden ist, kann diese via App Store (iPhone) oder Play Store (Android) installiert werden.</p>
<div data-bbox="204 1256 601 1290">Konto in der App einrichten ×</div> <div data-bbox="355 1332 483 1480">  </div> <div data-bbox="204 1525 478 1550"> <p>Fügen Sie zunächst Ihr Konto hinzu.</p> </div> <div data-bbox="363 1563 611 1608"> Zurück Weiter </div>	<p>9. Es erscheint Fenster «Konto in der App einrichten».</p> <p>Auf «Weiter» klicken.</p>

<div data-bbox="193 262 440 295" data-label="Section-Header"> <h3>QR-Code scannen</h3> </div> <div data-bbox="331 349 496 512" data-label="Image"> </div> <div data-bbox="193 539 620 616" data-label="Text"> <p>Verwenden Sie Ihre Authenticator-App, um den QR-Code zu scannen. Auf diese Weise wird die App mit Ihrem Konto verknüpft.</p> </div> <div data-bbox="193 629 616 658" data-label="Text"> <p>Kehren Sie dann zurück und wählen Sie Weiter aus.</p> </div> <div data-bbox="193 674 399 701" data-label="Text"> <p>Can't scan the QR code?</p> </div> <div data-bbox="399 725 462 752" data-label="Text"> <p>Zurück</p> </div> <div data-bbox="534 725 598 752" data-label="Text"> <p>Weiter</p> </div>	<p>10. Es erscheint ein QR-Code auf deinem Computer Bildschirm.</p> <p>Mit der Authenticator App deiner Wahl (z. B. Microsoft Authenticator oder Google Authenticator) den QR-Code scannen.</p> <p>Auf «Weiter» klicken.</p>
<div data-bbox="180 902 325 1048" data-label="Image"> </div> <div data-bbox="355 927 458 976" data-label="Text"> <p>sluz</p> </div> <div data-bbox="355 999 756 1043" data-label="Text"> <p>XXXXXXXXXXXX@sluz.ch</p> </div> <div data-bbox="188 1099 309 1218" data-label="Image"> </div> <div data-bbox="330 1120 414 1160" data-label="Text"> <p>sluz</p> </div> <div data-bbox="330 1178 655 1216" data-label="Text"> <p>XXXXXXXXXXXX@sluz.ch</p> </div> <div data-bbox="330 1252 711 1323" data-label="Text"> <p>224 109 3</p> </div>	<p>11. Die alternative Authenticator App auf dem Smartphone öffnen und das SLUZ-Konto antippen.</p>
<div data-bbox="215 1494 458 1538" data-label="Section-Header"> <h3>Code eingeben</h3> </div> <div data-bbox="215 1583 643 1644" data-label="Text"> <p>Geben Sie den von Ihrer Authenticator-App generierten 6-stelligen Code ein.</p> </div> <div data-bbox="228 1684 285 1713" data-label="Text"> <p>Code</p> </div> <div data-bbox="448 1771 526 1800" data-label="Text"> <p>Zurück</p> </div> <div data-bbox="609 1771 683 1800" data-label="Text"> <p>Weiter</p> </div>	<p>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.</p> <p>Den 6-stelligen «Code für Einmal-kennwort» auf dem Computer eingeben.</p> <p>Auf «Weiter» klicken.</p>

✓ **Authenticator-App
hinzugefügt**



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

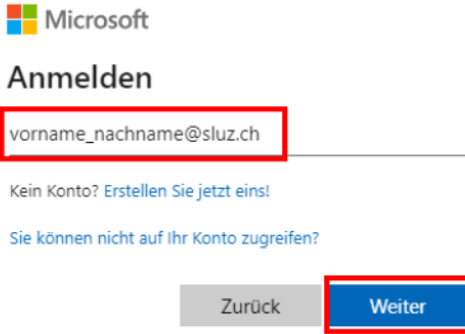
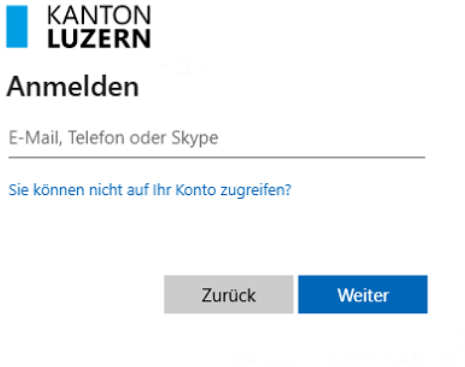

Fertig

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.

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

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

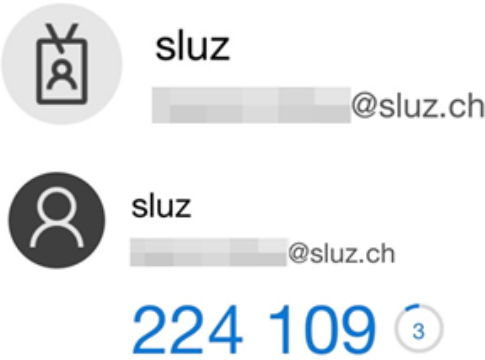

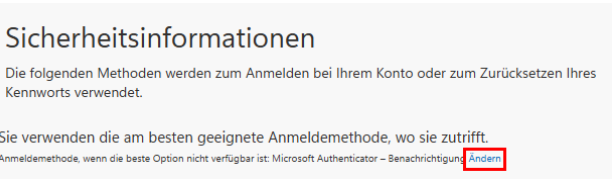

[Weitere Informationen](#)

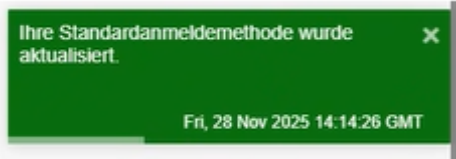
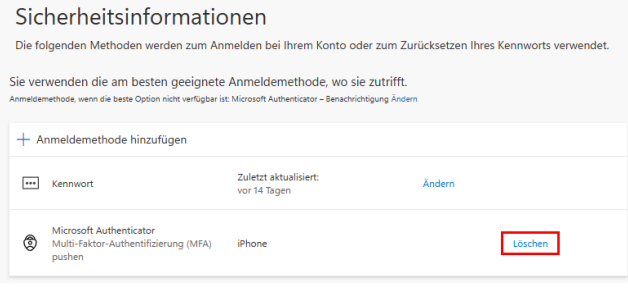
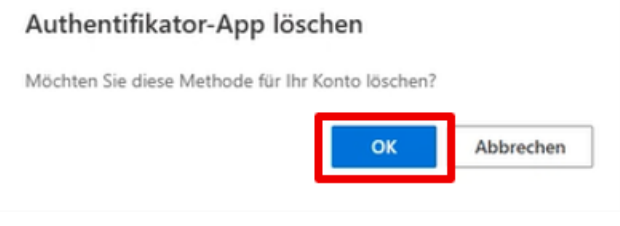
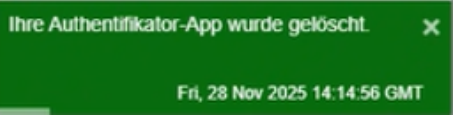
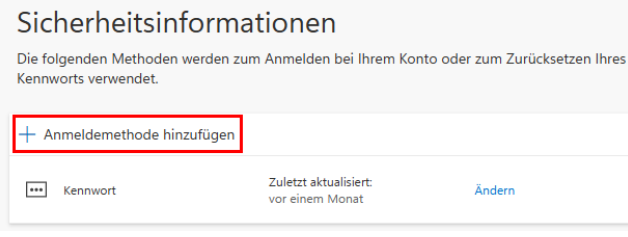
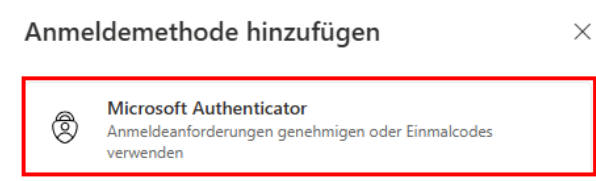
Sind Ihre Überprüfungsmethoden aktuell? Überprüfen sie unter <https://aka.ms/mfasetup>






Abbrechen

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

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

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

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

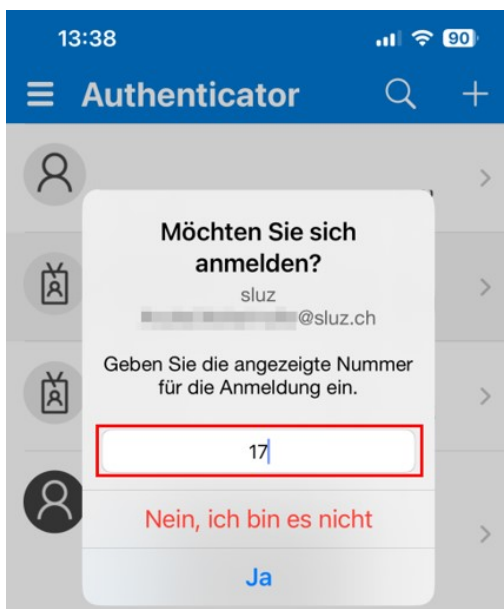
<div data-bbox="210 275 572 353"> <h3>Microsoft Authenticator installieren</h3> </div> <div data-bbox="363 405 544 622">  </div> <div data-bbox="210 638 687 694"> <p>Installieren Sie die App auf Ihrem mobilen Gerät und kehren Sie dann hierher zurück, um fortzufahren.</p> </div> <div data-bbox="217 712 403 768">  </div> <div data-bbox="430 712 617 768">  </div> <div data-bbox="210 790 643 822"> <p>Andere App für die Authentifizierung einrichten</p> </div> <div data-bbox="405 828 703 904"> <div>Zurück</div> <div>Weiter</div> </div>	<p>16. Es erscheint Fenster «Microsoft Authenticator installieren».</p> <p>Auf «Weiter» klicken.</p>
<div data-bbox="202 1059 601 1095"> <h3>Konto in der App einrichten</h3> </div> <div data-bbox="354 1137 485 1288">  </div> <div data-bbox="202 1330 478 1357"> <p>Fügen Sie zunächst Ihr Konto hinzu.</p> </div> <div data-bbox="365 1366 612 1415"> <div>Zurück</div> <div>Weiter</div> </div>	<p>17. Es erscheint Fenster «Konto in der App einrichten».</p> <p>Auf «Weiter» klicken.</p>
<div data-bbox="193 1541 579 1574"> <h3>QR-Code scannen</h3> </div> <div data-bbox="317 1621 466 1771">  </div> <div data-bbox="193 1792 580 1861"> <p>Verwenden Sie die Microsoft Authenticator-App, um den QR-Code zu scannen. Auf diese Weise wird die App mit Ihrem Konto verknüpft.</p> </div> <div data-bbox="193 1872 574 1899"> <p>Kehren Sie dann zurück und wählen Sie Weiter aus.</p> </div> <div data-bbox="193 1912 378 1939"> <p>Can't scan the QR code?</p> </div> <div data-bbox="351 1953 585 1991"> <div>Zurück</div> <div>Weiter</div> </div>	<p>18. Es erscheint ein QR-Code auf ihrem Computer Bildschirm.</p> <p>Mit der geöffneten Microsoft Authenticator App den QR-Code scannen.</p> <p>Auf Weiter klicken.</p>

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 selbständig 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			



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.