

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 Benutzernamen 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](#)<sup>1</sup> zu bestellen.

<sup>1</sup> 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 kantonaler 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://informatic.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:

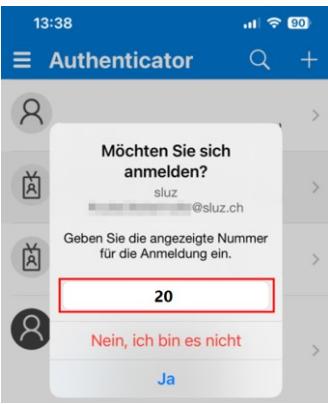


The screenshot shows a modern login interface for the Kanton Luzern (@sluz.ch) account. At the top left is the Kanton Luzern logo. To the right is the text '@sluz.ch' and a back arrow icon. The main title 'Kennwort eingeben' is centered above a text input field labeled 'Kennwort'. Below the input field is a blue link 'Kennwort vergessen'. At the bottom right is a blue 'Anmelden' (Login) button. The background is white with a thin black border around the form area.

## 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/password/change>

	<p>1. In der Anmeldemaske auf «<b>Kennwort vergessen</b>» klicken.</p>
 <p>Konto wieder aktivieren</p> <p>Wie heißen Sie?</p> <p>Geben Sie zum Wiederherstellen Ihres Kontos zunächst Ihre E-Mail-Adresse oder Ihren Benutzernamen sowie die in der Abbildung oder Aufnahme angegebenen Zeichen ein.</p> <p>E-Mail oder Benutzername: *</p> <p>Beispiel: benutzer@contoso.onmicrosoft.com oder benutzer@contoso.com</p> <p>Geben Sie die Zeichen in der Abbildung bzw. die Wörter in der Aufnahme ein. *</p> <p>Weiter Abbrechen</p>	<p>2. Eingabe von Benutzername bzw. E-Mail-Adresse und Zeichen unten in der Abbildung.</p> <p>Auf «Weiter» klicken.</p>
 <p>Konto wieder aktivieren</p> <p>Warum gibt es Probleme bei der Anmeldung?</p> <p><input checked="" type="radio"/> Ich habe mein Kennwort vergessen.</p> <p>Keine Sorge, wir helfen Ihnen beim Zurücksetzen des Kennworts anhand der Sicherheitsinformationen, die Sie bei uns registriert haben.</p> <p><input type="radio"/> Ich kenne mein Kennwort, kann mich aber dennoch nicht anmelden.</p> <p>Möglicherweise haben Sie sich zu oft mit dem falschen Kennwort angemeldet. Wenn Sie diese Option wählen, behalten Sie Ihr vorhandenes Kennwort, und wir entsperren Ihr Konto, damit Sie sich wieder anmelden können.</p> <p>Weiter Abbrechen</p>	<p>3. Klicke auf «<b>Ich habe mein Kennwort vergessen</b>».</p> <p>Auf «Weiter» klicken.</p>

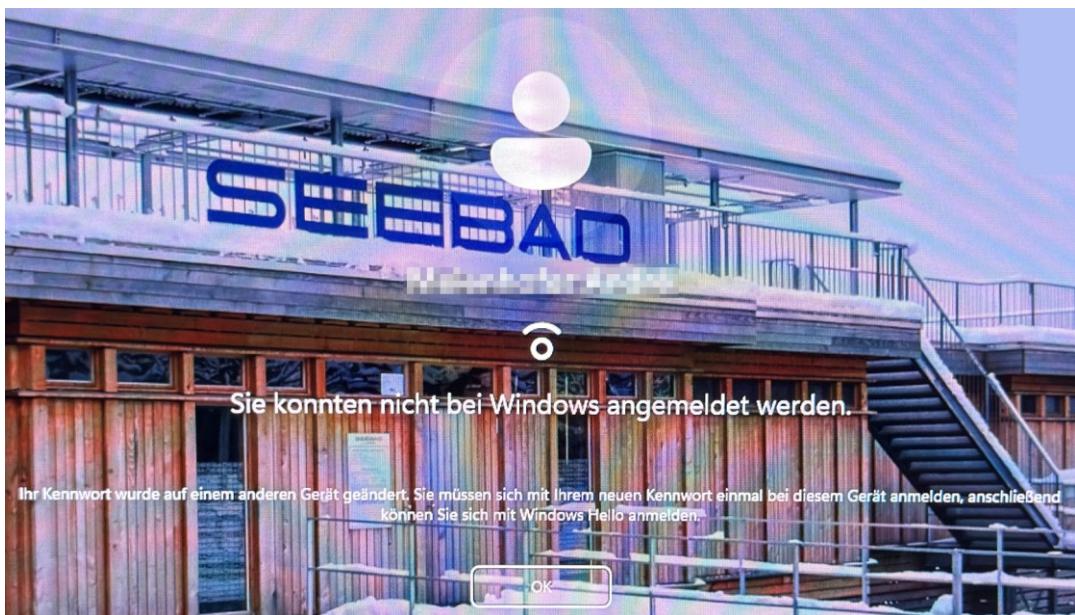
 <h2>Konto wieder aktivieren</h2> <p><b>Überprüfungsschritt 1 &gt; Neues Kennwort auswählen</b></p> <p>Wählen Sie die Kontaktmethode aus, die zur Überprüfung verwendet werden soll:</p> <p><input checked="" type="radio"/> Benachrichtigung in meiner Authenticator-App bestätigen</p> <p><input type="radio"/> Code aus meiner Authenticator-App eingeben</p> <p>Senden Sie eine Benachrichtigung an Ihre Authenticator-App auf Ihrem Mobilgerät.</p> <p><b>Benachrichtigung senden</b></p> <p><a href="#">Abbrechen</a></p>	<p>4. Nun folgt die Überprüfung, ob das Konto korrekt mit der App verbunden worden ist.</p> <p>Auf «<b>Benachrichtigung in meiner Authenticator-App bestätigen</b>» und «<b>Benachrichtigung senden</b>» klicken.</p>
<h2>Konto wieder aktivieren</h2> <p><b>Überprüfungsschritt 1 &gt; Neues Kennwort auswählen</b></p> <p>Wählen Sie die Kontaktmethode aus, die zur Überprüfung verwendet werden soll:</p> <p><input checked="" type="radio"/> Benachrichtigung in meiner Authenticator-App bestätigen</p> <p><input type="radio"/> Code aus meiner Authenticator-App eingeben</p> <p>Genehmigen Sie die Benachrichtigung, die wir an Ihre App senden, indem Sie die untenstehende Nummer eingeben.</p> <p>20</p>	<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>
<h2>Konto wieder aktivieren</h2> <p><b>Überprüfungsschritt 1 ✓ &gt; Neues Kennwort auswählen</b></p> <p>* Neues Kennwort eingeben:</p> <p>* Neues Kennwort bestätigen:</p> <p><b>Fertig stellen</b> <a href="#">Abbrechen</a></p>	<p>7. Ein neues Kennwort mit Bestätigung eingeben.</p> <p>Auf «<b>Fertig stellen</b>» klicken.</p>

## 4.5 Passwort abgelaufen – iWP mit PIN & Gesichtserkennung

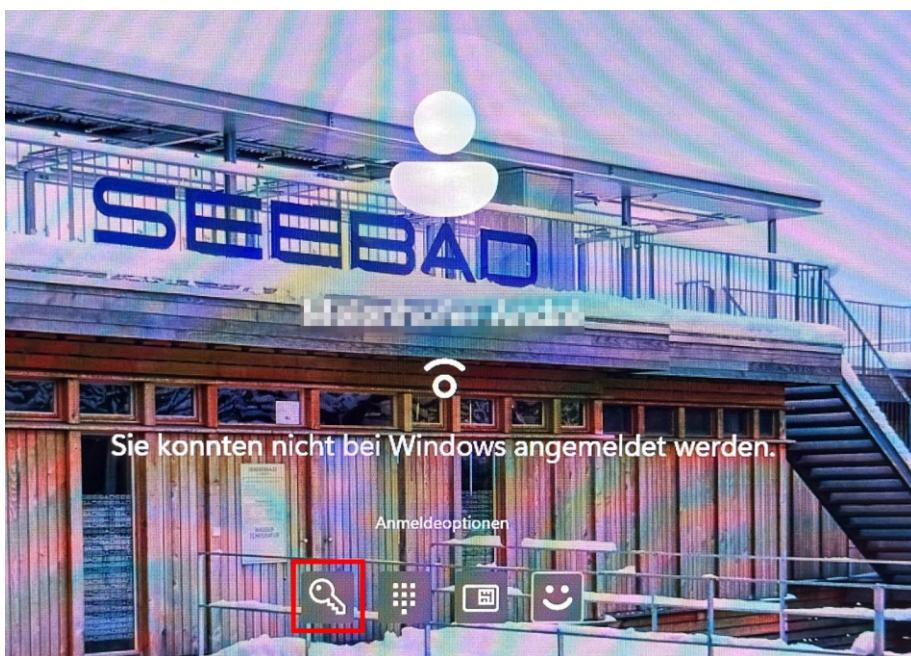
Gemäss kantonaler Sicherheitsvorgabe muss das persönliche Passwort regelmässig, spätestens aber nach jeweils 90 Tagen geändert werden.

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:



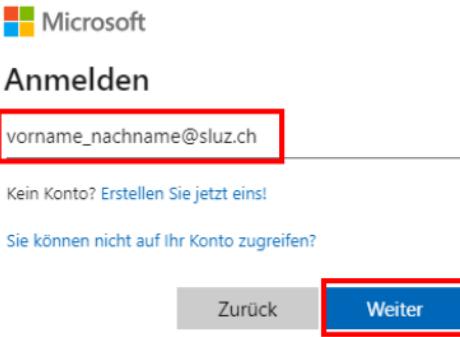
Danach muss zuerst bei der Anmeldung bei "Anmeldeoptionen" das Schlüssel-Symbol ausgewählt und das neue Passwort eingegeben werden. Danach funktioniert bei der nächsten Anmeldung der PIN oder Gesichtserkennung wieder.



## 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>Microsoft</p> <p>Anmelden</p> <p>vorname_nachname@sluz.ch</p> <p>Kein Konto? <a href="#">Erstellen Sie jetzt eins!</a></p> <p>Sie können nicht auf Ihr Konto zugreifen?</p> <p>Zurück <span style="background-color: #0078D4; color: white; border: 1px solid #0078D4; padding: 5px 10px; border-radius: 5px;">Weiter</span></p>	<ol style="list-style-type: none"><li>1. Öffne die folgende Webseite auf deinem PC (nicht Smartphone):  <a href="https://mysignins.microsoft.com/security-info">https://mysignins.microsoft.com/security-info</a>  Dein SLUZ-Benutzernamen eingeben.  Auf «Weiter» klicken.</li></ol>
 <p>KANTON LUZERN</p> <p>Anmelden</p> <p>E-Mail, Telefon oder Skype</p> <p>Sie können nicht auf Ihr Konto zugreifen?</p> <p>Zurück <span style="background-color: #0078D4; color: white; border: 1px solid #0078D4; padding: 5px 10px; border-radius: 5px;">Weiter</span></p>	<ol style="list-style-type: none"><li>2. Den SLUZ-Benutzernamen eingeben und auf «Weiter» klicken.</li></ol>
 <p>KANTON LUZERN</p> <p>← [REDACTED]@sluz.ch</p> <p>Kennwort eingeben</p> <p>.....</p> <p>Kennwort vergessen</p> <p>Anmelden</p>	<ol style="list-style-type: none"><li>3. Das Kennwort eingeben und auf «Anmelden» klicken.</li></ol>

## Anmeldeanforderung bestätigen

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

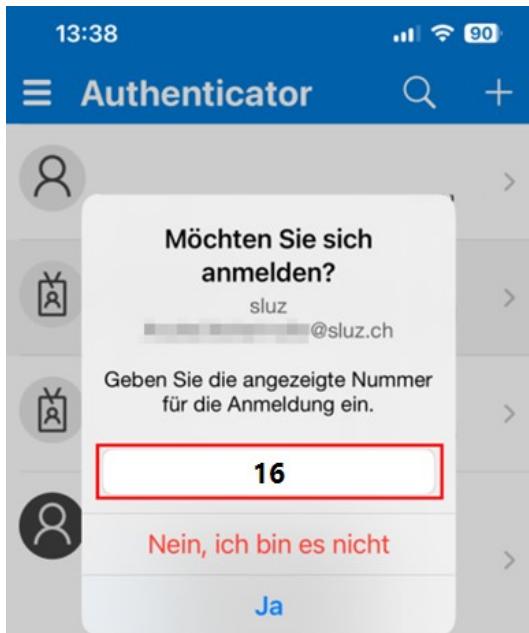
16

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.

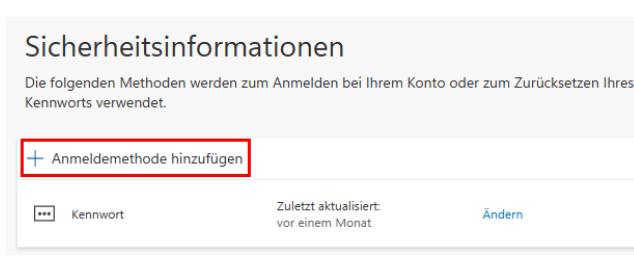
[Weitere Informationen](#)

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



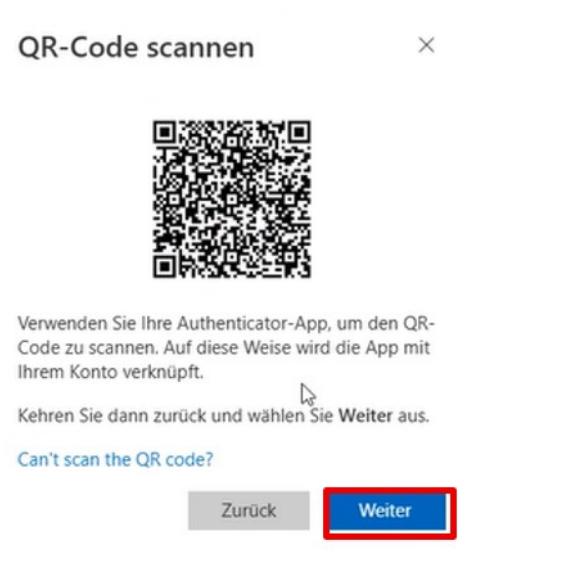
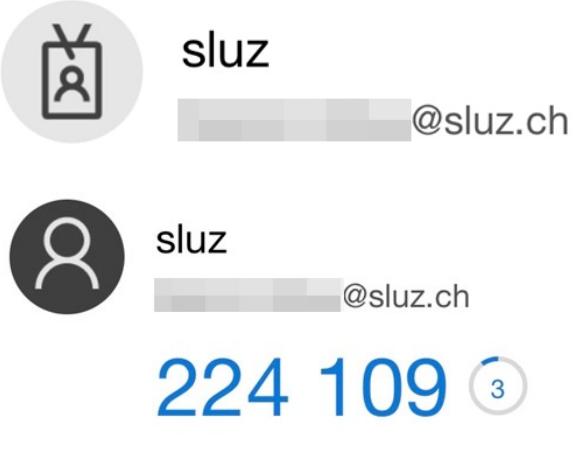
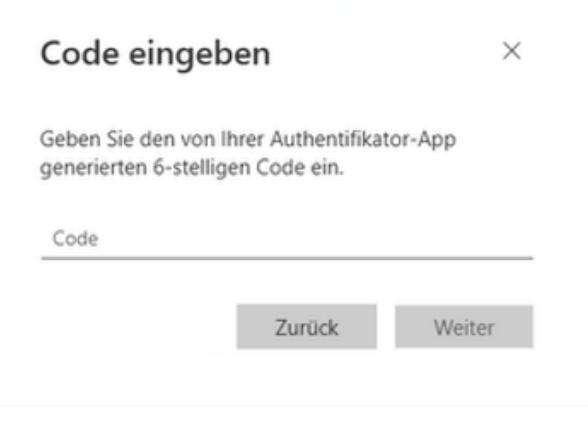
5. In der Authenticator-App auf dem Smartphone erscheint nun die Frage, ob man sich anmelden möchte. Die Zahl von ihrem Computer muss im umrandeten Feld auf dem Smartphone eingegeben werden.

Mit «Ja» bestätigen.



6. «Anmeldemethode hinzufügen» wählen.

	<p>7. «Microsoft Authenticator» wählen.</p>
	<p>8. Es erscheint die Aufforderung die Authenticator-App zu installieren.</p> <p>Falls die App auf dem Mobiltelefon bereits eingerichtet worden ist, <b>«Andere App für die Authentifizierung einrichten» wählen.</b></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>
	<p>9. Es erscheint Fenster «Konto in der App einrichten».</p> <p>Auf «Weiter» klicken.</p>

	<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>
	<p>11. Die alternative Authenticator App auf dem Smartphone öffnen und das SLUZ-Konto antippen.</p>
	<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 <b>«Code für Einmal-kennwort»</b> 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.

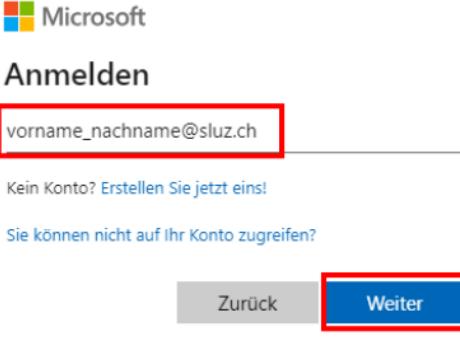
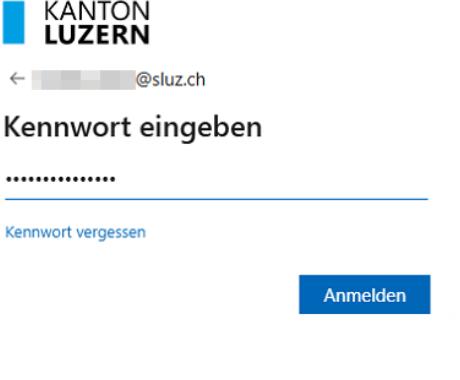
Fertig

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>Microsoft</p> <p>Anmelden</p> <p>vorname_nachname@sluz.ch</p> <p>Kein Konto? <a href="#">Erstellen Sie jetzt eins!</a></p> <p>Sie können nicht auf Ihr Konto zugreifen?</p> <p>Zurück <span style="background-color: #0078D4; color: white; padding: 5px 10px; border-radius: 5px;">Weiter</span></p>	<ol style="list-style-type: none"><li>1. Öffne die folgende Webseite auf deinem PC (nicht Smartphone):  <a href="https://mysignins.microsoft.com/security-info">https://mysignins.microsoft.com/security-info</a>  Dein SLUZ-Benutzernamen einge- ben.  Auf «Weiter» klicken.</li></ol>
 <p>KANTON LUZERN</p> <p>Anmelden</p> <p>E-Mail, Telefon oder Skype</p> <p>Sie können nicht auf Ihr Konto zugreifen?</p> <p>Zurück <span style="background-color: #0078D4; color: white; padding: 5px 10px; border-radius: 5px;">Weiter</span></p>	<ol style="list-style-type: none"><li>2. Den SLUZ-Benutzernamen einge- ben und auf «Weiter» klicken.</li></ol>
 <p>KANTON LUZERN</p> <p>← [REDACTED]@sluz.ch</p> <p>Kennwort eingeben</p> <p>.....</p> <p>Kennwort vergessen</p> <p>Anmelden</p>	<ol style="list-style-type: none"><li>3. Das Kennwort eingeben und auf «Anmelden» klicken.</li></ol>



@sluz.ch

## 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.



@sluz.ch

## Überprüfen Ihrer Identität



Eine Anforderung in meiner Microsoft Authenticator-App bestätigen

123

Verwenden eines Prüfcodes

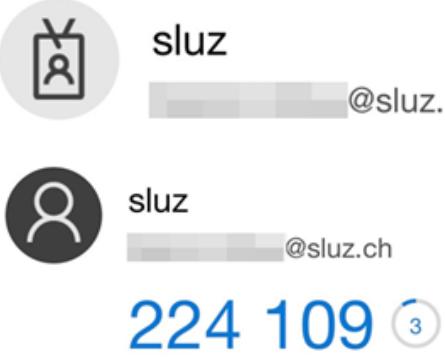
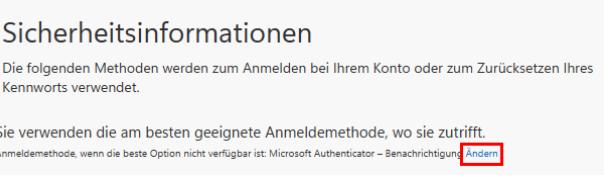
Weitere Informationen

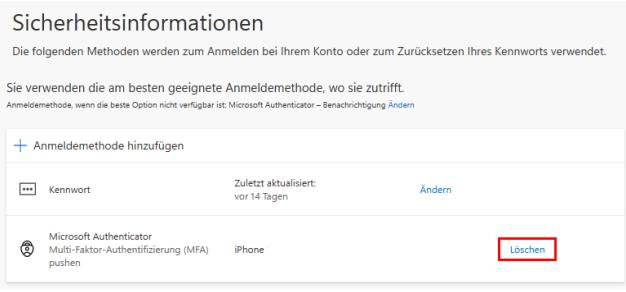
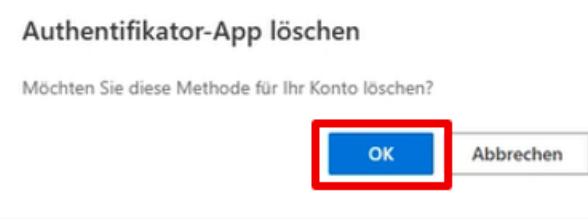
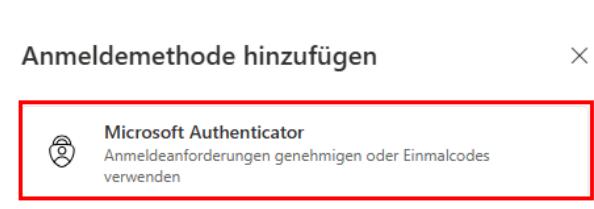
Sind Ihre Überprüfungsmethoden aktuell? Überprüfen sie unter <https://aka.ms/mfasetup>

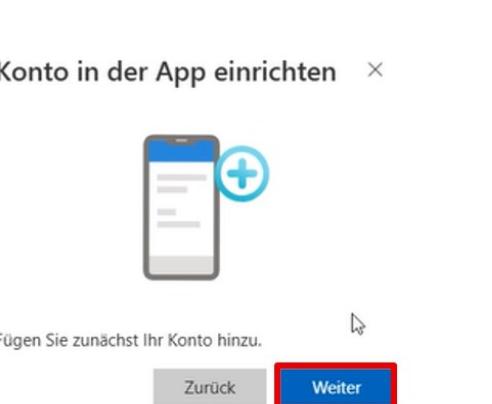
Abbrechen

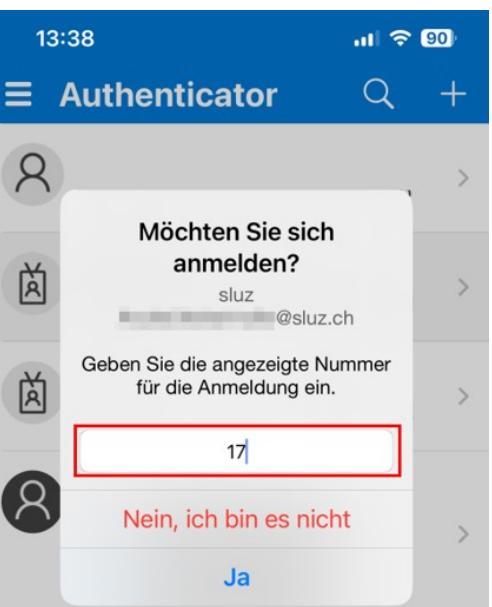
5. Es erscheint auf dem Computer die Meldung über die Überprüfung Ihrer Identität.

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 <b>«Code für Einmal-kennwort»</b> auf dem Computer eingeben. Auf «Überprüfen» klicken.</p>
	<p>8. Bei Sicherheitsinformationen die Standardmethode ändern. Auf «Ändern» klicken.</p>
	<p>9. Es erscheint das Fenster Standardmethode ändern. Bei Dropdown-Menü die Methode <b>«App-basierte Authentifizierung oder Hardwaretoken-...»</b> auswählen. 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>

	<p>16. Es erscheint Fenster «Microsoft Authenticator installieren».</p> <p>Auf «Weiter» klicken.</p>
	<p>17. Es erscheint Fenster «Konto in der App einrichten».</p> <p>Auf «Weiter» klicken.</p>
	<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>

 <p>Probieren wir es aus</p> <p>17</p> <p>Geben Sie die in der App angezeigte Nummer ein, um die Anmeldeanforderung zu genehmigen.</p> <p>Zurück</p>	<p>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.</p>
	<p>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>
<p>✓ Authenticator Added</p>  <p>Sie können jetzt Microsoft Authenticator verwenden, um Anmeldungen zu genehmigen, einmalige Codes abzurufen und mehr.</p> <p>Dies ist jetzt Ihre Standardanmeldemethode.</p> <p>Fertig</p>	<p>20. Nachdem in der App die Authentifikation bestätigt worden ist, erscheint die Meldung, dass die Authentifizierungsmethode erfolgreich hinzugefügt wurde.</p> <p>Auf «Fertig» klicken.</p>

## **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](https://informatik.lu.ch/-/media/Informatik/Dokumente/Informationssicherheit/Dokumentenablage/W101_Weisung_Benutzernamen_Passwoerter.pdf).<sup>1</sup>

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><sup>1</sup>
- [servicedesk@lu.ch](mailto: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](http://www.informatik.lu.ch)  
[informatik@lu.ch](mailto:informatik@lu.ch)

<sup>1</sup> Diese Seite ist nur mit einem EDULU-Login erreichbar.