

Mailkonto-Einrichtung

In diesem Dokument finden Sie Ihre individuellen Daten und eine Anleitung.

Ihre Zugangsdaten

Um sich im System anzumelden, benötigen Sie den Zugang (Link) und Ihre Zugangsdaten. Diese lauten wie folgt:

- Webmailer: <https://mail.seminar-bw.de/>
- Benutzername: vorname.nachname.ref26@gym-hd.seminar-bw.de
bzw. vorname.nachname.LA26@sop-hd.seminar-bw.de
wobei 26 das Jahr des Beginns ist,
also z. B. max.mustermann.ref26@gym-hd.seminar-bw.de
oder z. B. max.mustermann.LA26@sop-hd.seminar-bw.de
- Passwort: <wird individuell mitgeteilt>

Bitte beachten Sie, dass das neue Passwort gemäß unseren Sicherheitsrichtlinien generiert wurde und ausreichend komplex ist, um Ihre Daten bestmöglich zu schützen. Nach rechtlichen Vorgaben müssen Sie Ihr Passwort aber ändern, damit die Administration des Mail-Systems Ihr Passwort nicht kennt. Eine entsprechende Anleitung wird per Video bereitgestellt (siehe unten).

Verwenden Sie immer die oben angegebene URL. Sie werden intern zu einer anderen URL weitergeleitet, diese kann aber nicht zum Login beim nächsten Mal verwendet werden. Insbesondere darf in der URL, mit der man startet, NICHT "login" vorkommen.

Hinweise zur Verwendung von TOTP (Time-Based One-Time Password)

Zusätzlich zum Passwort erzwingt das neue System beim Webmailer die Nutzung einer Zwei-Faktor-Authentifizierung mittels TOTP. Hier sind einige wichtige Schritte und Hinweise.

- Aktivierung der TOTP-App: Um TOTP zu nutzen, müssen Sie vor der ersten Anmeldung eine Authentifizierungs-App auf Ihrem Gerät (Computer, Tablet oder Smartphone) installieren.
⚠ Beachten Sie dabei aus rechtlichen Gründen unbedingt die weiter unten aufgeführten Richtlinien bzgl. erlaubter Geräte und Anwendungen
- QR-Code scannen: Nach dem ersten Login mit Benutzernamen und Passwort werden Sie gezwungen, die 2-Faktor-Authentifizierung einzurichten. Es wird Ihnen ein QR-Code angezeigt der von den gängigen TOTP-Authenticator-Apps eingescannt werden kann. Über einen Klick auf "Unable to scan?" kann auch TOTP-Key als Zeichen-/Zahlenkette angezeigt werden. Wir empfehlen, diesen Key sicherheitshalber, z. B. im Falle eines Verlusts Ihres Smartphones, in einer Passwort-Manager-Anwendung (z. B. KeePassXC) redundant zu speichern.

- Nachdem Ihre Authenticator-App einen TOTP-Code für Ihr Konto anzeigt, muss dieser zur Verifikation der korrekten Einrichtung einmal eingegeben werden. Dieser Dialog kann erst beendet werden, wenn die Einrichtung offenbar erfolgreich war. Bei Erfolg werden Sie zur erneuten Anmeldung am System aufgefordert und gelangen, bei erfolgreicher Anmeldung mit
 - Username
 - Passwort
 - TOTP-Code (hier bitte beachten, dass der TOTP-Code alle 30 Sekunden neu erzeugt werden muss)

zum Webmailer auf Basis von SOGo (Scalable Open Groupware).

Weitere Hinweise

- 2-Faktor-Authentifizierung mit TOTP (Quelle u.a. [hier](#))
 - Bei Verwendung einer 2-Faktor-Authentifizierung auf Basis von Einmalpasswörtern (OTP- bzw. TOTP-Verfahren) ist zu deren Erzeugung grundsätzlich ein zweites Gerät zwingend erforderlich. Dieses Gerät muss sich im persönlichen Besitz der Lehrkraft befinden. Die Lehrkraft hat für einen Zugriffsschutz entsprechend dem Stand der Technik zu sorgen. Sofern sich das Gerät, mittels dem auf Webmail zugegriffen werden soll, im ausschließlichen persönlichen Besitz der Lehrkraft befindet (also z. B. ein Tablet, das alleine von dieser Lehrkraft genutzt wird und nicht im Klassenzimmer verbleibt), ist es zulässig, dass der zweite Faktor auch auf diesem Gerät erzeugt wird.
 - Zudem sollen nur Softwareanwendungen zur Erzeugung dieser Einmalpasswörter genutzt werden, welche aus der EU bzw. EWR-Raum stammen (Geltungsbereich der EU-DSGVO). Es wird empfohlen, keine Softwarelösungen von Anbietern aus Drittstaaten (z.B. USA, China, Russland, ...) zu verwenden.
 - Wir raten explizit von den häufig verwendeten Apps "*Google Authenticator*" und "*Microsoft Authenticator*" ab.
 - Software- / App-Möglichkeiten:
 - Android: FreeOTP bzw. FreeOTP+, Aegis, KeePassDX
 - iOS, Mac OS: FreeOTP aus dem App Store oder iOS- bzw. Mac OS Bordmittel:
<https://support.apple.com/de-de/guide/iphone/iph6173c19f/ios>
<https://support.apple.com/de-de/guide/passwords/mchl873a6e72/mac>
 - Linux, Mac OS Windows: KeePassXC (auch aus dem Grund, dass dieser Passwort-Manager auch bei der Verwaltung von Zugangsdaten ein Top-Werkzeug ist)

- Um Ihnen den Einstieg in das System so einfach wie möglich zu machen, ist **Schulungsmaterial und Anleitungen in Form von Videos** in folgendem Portal bereitgestellt: https://pt01.lehrerfortbildung-bw.de/c/mailserver_saf_zsl/videos. Für die Ansicht der Videos benötigen Sie das **Passwort "Mail4you"**. Dieses Angebot wird sukzessive ausgebaut. Wir empfehlen Ihnen, regelmäßig vorbeizuschauen, um von neuen Ressourcen und Funktionen zu profitieren.
- **E-Mail-Clients mit SMTPS/IMAPS-Zugriff** (Thunderbird, K9-Mail, ...)
 - Die Nutzung ist vorläufig möglich. Bitte beachten Sie unbedingt die nachfolgenden Punkt.
 - Die Nutzung lokal auf den Geräten installierter E-Mail-Clients ist und war generell untersagt. In Abstimmung mit dem Landesbeauftragten für Datenschutz und Informationsfreiheit (LfDI) Baden-Württemberg werden wir aber versuchen, hier eine Lösung auf Basis technisch-organisatorischer Maßnahmen (TOMs) zu erzielen, um den Einsatz zu ermöglichen. Mit Sicherheit dürfen aber auch hierfür **nur Geräte verwendet werden, die sich im ausschließlichen persönlichen Besitz befinden**. Ebenfalls sicher dürfen nur Geräte mit **verschlüsselter Festplatte** eingesetzt werden. Vergleichbare Regelungen sind bereits heute in der "[Anlage 1 zur Verwaltungsvorschrift „Datenschutz an öffentlichen Schulen](#)" festgelegt.
 - Die Verwendung eines E-Mail-Clients (Thunderbird, K9-Mail, ...) wird irgendwann ebenfalls nur noch mit einem 2. Faktor verwendbar sein.