Passwords

The following guidelines apply to user account passwords:

- Minimum number of characters in the password: 8 characters.
- Differentiation of upper and lower case in the password (a - z, A - Z)
- Numeric characters are allowed (0 - 9)
- Non-alphanumeric characters are allowed (! + -)
- **Non-alphabetic characters are not allowed (ä ö ü ß, Ä Ö Ü)**
- No expiration date

Password change and reset

Students are advised to change their password immediately after receiving their accessdata. Furthermore, all university members and staff should change your password at regular intervals.

In our Password portal you can change your password and additionally use other password reset options. There you can set up security questions in case you forget your password. Likewise, you can set up your smartphone to reset a forgotten password.

Please note that changing your password will affect almost all services:

- Collaboration Cloud
- Printing services, especially locally mounted network printers.
- Email account on your iPad, iPhone, PC.
- Jade eCampus
- Messaging via Cisco Jabber
- WLAN access eduroam

Note: On the Microsoft Windows operating system, you can manage your saved passwords in the Control Panel under Logon Information Management / Windows Credentials.

Forgot your password

If you have forgotten your password, you can have the access data sheet printed out again at the University Computer Center at any study location by presenting a photo ID and a handwritten signature. Forgotten passwords will not be emailed as we are unable to verify your identity.

Alternatively, you can use the eIDentity Portal to enable various password reset methods.

Recommendations for strong passwords

Please use your password only for the central IT systems of Jade University. You should use your own

passwords for the various online services.

A good introduction to the topic are the recommendations of the BSI:

- BSI for Citizens - Passwords
- BSI for Citizens - Dealing with Passwords

Password Management

To store and manage your passwords securely, we recommend using password management software.

KeePass

Description

KeePass is basically first of all a password management program. KeePass stores the usernames / passwords and some other data in a database and stores them encrypted as a file. The main functions are:

- Storing usernames, passwords, etc.
- Storing in an encrypted file
- Opening the KeePass database with one (!) master key (e.g. a password) or optionally with a second factor (2FA, password and YubiKey)
- Transfer of usernames / passwords via clipboard to other programs
- Automatic input of username and password into the corresponding application (e.g. Firefox) via a global keyboard shortcut (Auto-Type)
- Automatic input of username and password in Firefox via a PlugIn

At the first call the database is created and the name for the corresponding file is requested. Also the master key (e.g. a strong password) must be entered now.

PC software

A specialized variant of KeePass is KeePassXC. This is an open source variant that is available for all three PC operating systems (Apple macOS, Linux, Microsoft Windows) (cross-platform).

KeePassXC can be downloaded and installed for all PC operating systems (for Microsoft Windows, the „EXE Installer (64-bit)“ variant is usually suitable).

Apple iOS

A specialized variant of KeePass is KeePassium. This is a variant that is optimized for Apple iOS.

- Apple App Store: KeePassium

Another alternative is Strongbox:

- Apple App Store: Strongbox

Google Android

A specialized variant of KeePass is KeePass DX. This is an open source variant optimized for Android.

- F-Droid: KeePass DX
- Google Play Store: KeePass DX

From:
https://hrz-admin-wiki.jade-hs.de/ - **HRZ-Admin-Wiki**

Permanent link:
https://hrz-admin-wiki.jade-hs.de/en/tp/uadm/passwords

Last update: **2024/08/17 12:47**