

Safety first.

Protection against cyber attacks: We are introducing 2-factor authentication (2FA).

Recent incidents at the universities in Karlsruhe, Furtwangen and Villingen-Schwenningen show that cybercrime against universities is on the rise. The attack is often carried out via phishing: criminals use fake emails to gain access to a university's systems.

We want to further strengthen the protection of the university of applied sciences Offenburg against cyber attacks. That is why we will be introducing two-factor authentication (2FA) in the coming weeks. With 2FA, employees and students can effectively protect themselves against phishing.

How does 2FA work?

With 2FA, you use another factor in addition to the user password, such as a smartphone or hardware token, to log in. This secures your user account twice against unauthorized access. Many of you are already familiar with this procedure from online banking (SMS/TAN).

Our systems will be converted to 2FA on December 4. After that, logging in to VPN, Mail (Groupwise/Webmail) and Filr will only work with 2FA. Furthermore, additional services will only be accessible in the university network (on site) or via VPN.

Inhalt

Quickstart Guide.....	2
Registration (AA-Portal)	2
Login.....	5
FAQ	7
Alternative methods	7
TOTP / HSO-Token / Google-Auth / Microsoft Authenticator	7
Google/Microsoft Authenticator.....	9
FIDO2 (Yubikey, USB-Stick).....	10
More alternatives	13
Emergency password / lost device / broken device.....	13
New Smartphone	13
Third-party Mail Programms (Thunderbird/Outlook/Applemail/Uninow)	15
IMAP and CalDAV.....	15

Quickstart Guide

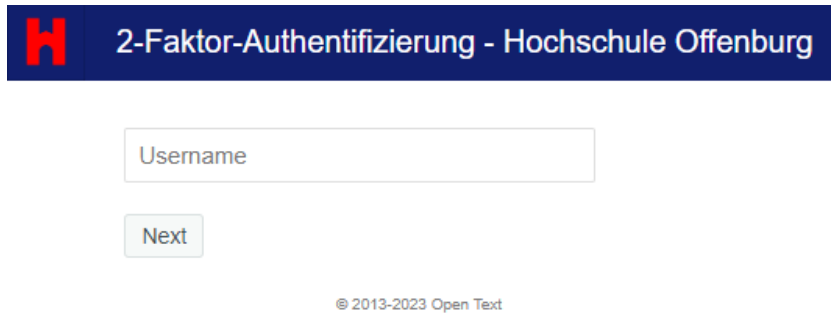
In order for a device to be used as a second factor, it must be registered first. The device is then assigned to your campus user account and can then be used for 2FA logins together with your campus username and password.

The setup only takes a few minutes.

Registration (AA-Portal)

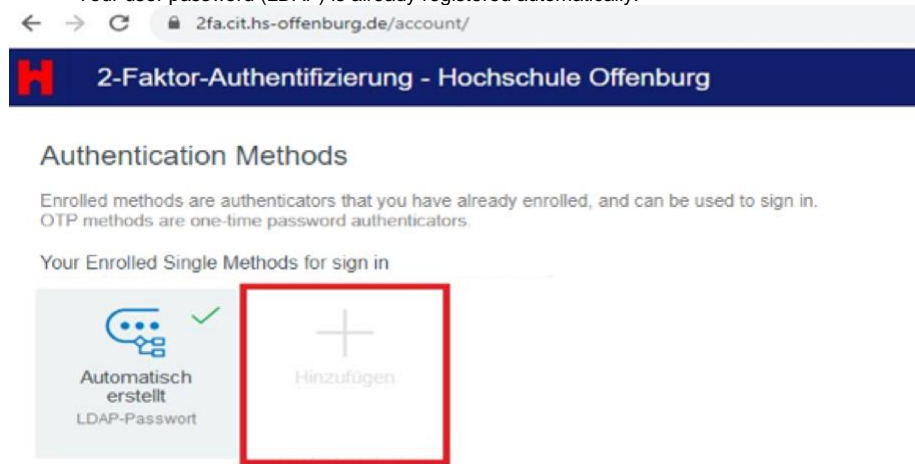
Registration is done via <https://2fa.cit.hs-offenburg.de/account/>

1. Log in with your campus user name and password



2. After logging in, you will see a page with already registered factors. To add a second factor, click on the plus button.

Your user password (LDAP) is already registered automatically.

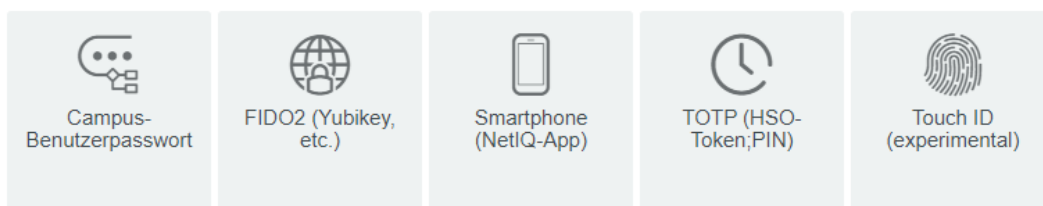


3. Various possible methods are offered to you. The simplest and most straightforward option is the smartphone method. Click on the smartphone symbol.

(Alternative methods without smartphone: see below)

Available Methods for Enrollment

Select an authentication method for enrollment. Once enrolled, the method can be used for sign in. OTP methods are one-time password authenticators.



4. Download the NetIQ Advanced Authentication app to your smartphone.

You can find the app in the Google Playstore/Apple Appstore.

The app is free of charge.



Android:



Apple:

You must set your own PIN for the app. You can also store your fingerprint (Android) or FaceID (Apple) in the settings later as an alternative.

In case the NetIQ app does not work on your smartphone, because your Android/iOS version is too old, you can still register 2FA via your smartphone. 2FA then works via TOTP with Google/Microsoft Authenticator, the instructions for this can be found under "Alternative methods" -> "TOTP / HSO-Token / Google-Auth /MS authenticator".

5. Get the QR Code

Smartphone (NetIQ-App)

The Smartphone method allows authentication with your smartphone. It is an out-of-band authentication. The NetIQ Advanced Authentication application sends a push message to your smartphone, which you can accept or reject. Installing the NetIQ Advanced Authentication mobile app on your smartphone is required.

Display Name

My Smartphone (NetIQ-App)

Category

Default

To enroll, get a QR code and scan it using the Advanced Authentication mobile app.

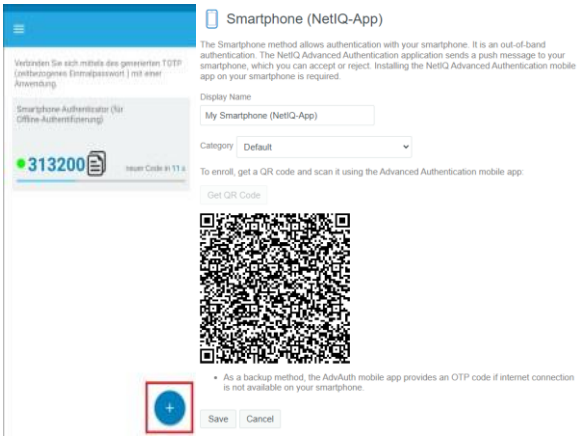
Get QR Code

- As a backup method, the AdvAuth mobile app provides an OTP code if internet connection is not available on your smartphone.

Save

Cancel

6. Scan the QR code with your NetIQ app. To do this, click on the blue plus-symbol in the app.
(for Apple/iOS the plus is at the top)



7. Once the code has been scanned, click on Save

Smartphone (NetIQ-App)

The Smartphone method allows authentication with your smartphone. It is an out-of-band authentication. The NetIQ Advanced Authentication application sends a push message to your smartphone, which you can accept or reject. Installing the NetIQ Advanced Authentication mobile app on your smartphone is required.

Display Name
My Smartphone (NetIQ-App)

Category Default

1.

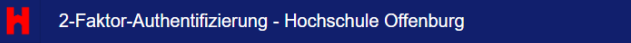
Enrollment is complete
To enroll, get a QR code and scan it using the Advanced Authentication mobile app:
Get QR Code

• As a backup method, the AdvAuth mobile app provides an OTP code if internet connection is not available on your smartphone.

2.

Save Cancel

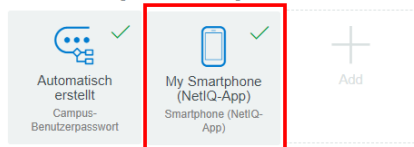
Your second factor should now be displayed.



Authentication Methods

Enrolled methods are authenticators that you have already enrolled, and can be used to sign in. OTP methods are one-time password authenticators.

Your Enrolled Single Methods for sign in



The registration of your second factor is now complete. If you do not wish to register another factor, you can log out and leave the page.

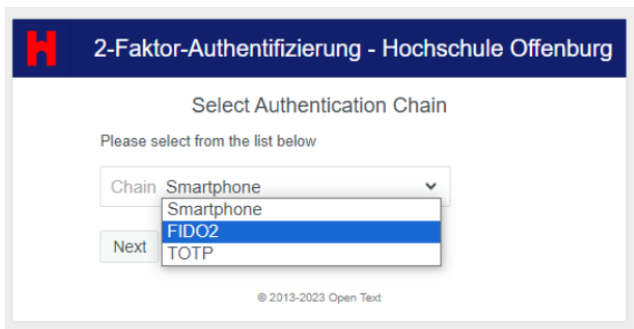
Login

Once you have registered your second factor, this will be required for future logins to Mail (Groupwise/Webmail).

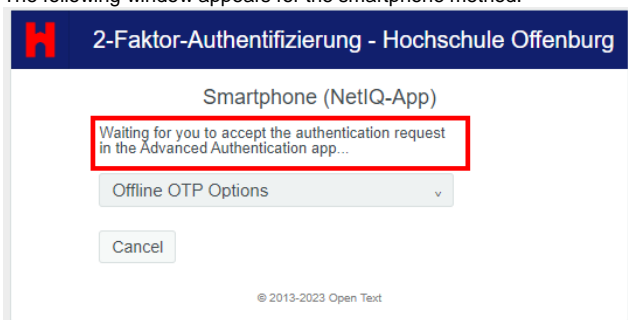
Try logging in via webmail: <https://webmail.hs-offenburg.de/>

After entering your user name + password, another factor will be requested. Depending on the login, the user name and password will be requested separately.

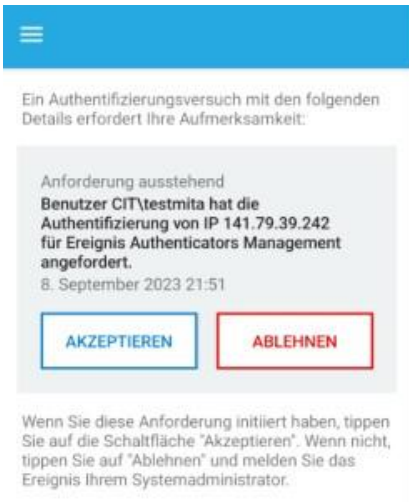
If several second factors are registered, the desired method is asked for:



The following window appears for the smartphone method:



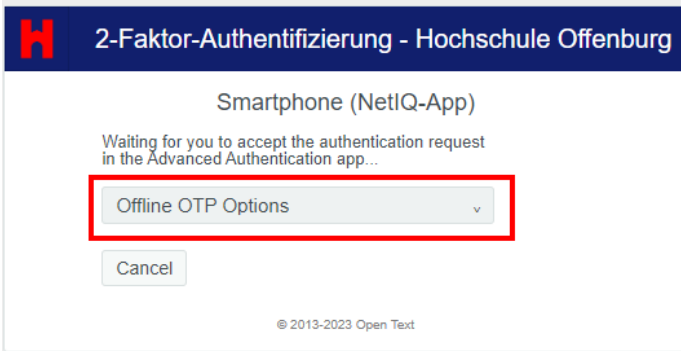
Open the NetIQ Advanced Authentication app on your smartphone and wait a moment. A dialog box with an "Accept" button will appear on your smartphone.



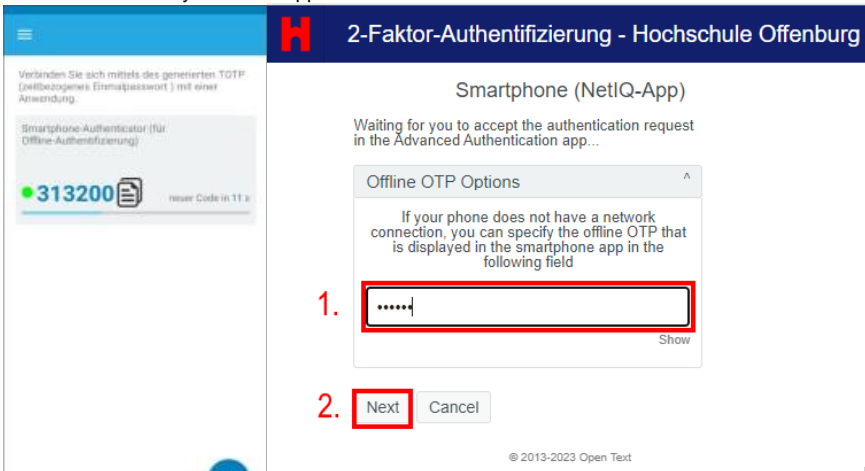
After tapping on "Accept", you will be automatically logged in. Wait a moment, the process may take a while.



If your smartphone is offline and you do not get an "Accept" dialog box, you can use the Offline OTP option.



Enter the code from your NetIQ app and click on "Next".



FAQ

Alternative methods

You can register additional factors as you wish via <https://2fa.cit.hs-offenburg.de/account/>

If you do not want to use your smartphone, you can use a token generator such as TOTP or FIDO2

TOTP / HSO-Token / Google-Auth / Microsoft Authenticator

One-time password tokens are small devices the size of key chains that have a button and a display with 6 digits.

For 2FA login with one-time password tokens, you must press the button on the device after logging in with your campus user name and password and then enter the 6 digits displayed.

The term TOTP has also become established for this method. (Time Based One Time Password).

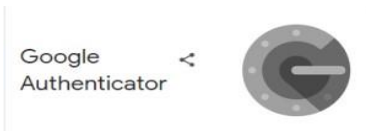
Employees and lecturers can obtain the HSO token (TOTP) from Campus IT (B205c).

Students can borrow the HSO token from the university library in Offenburg or Gegenbach.



HSO-Token

Alternatively, apps such as Google/MS Authenticator can also be used as a one-time password generator.



Log in to <https://2fa.cit.hs-offenburg.de/account/> . Click on the plus sign.



Choose TOTP.



For the HSO-Token:


Click on "OATH-Token".

The serial number can be found on the back of the device (under Barcode). You can obtain the one-time password (PIN) by pressing the red button.

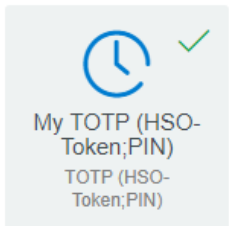
OATH Token ^

OATH Token Serial Number

One-time Password (OTP)

Then click on **Save**. Your hardware token has been added




Google/Microsoft Authenticator (or similar Apps):

Get the QR code and scan the code with your app.

OATH Token ∨

[Get QR Code](#)

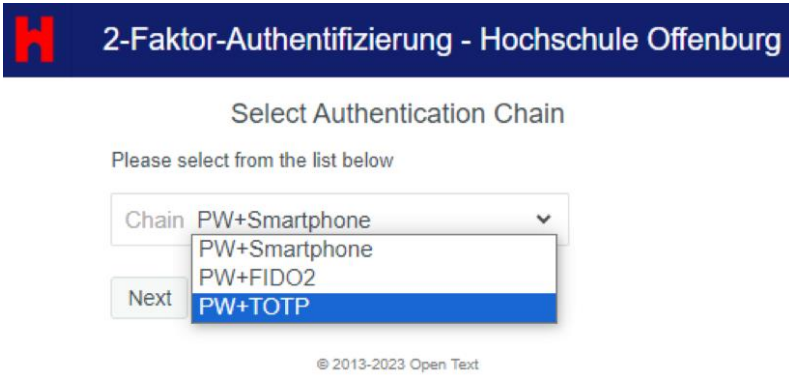


Manual TOTP ∨

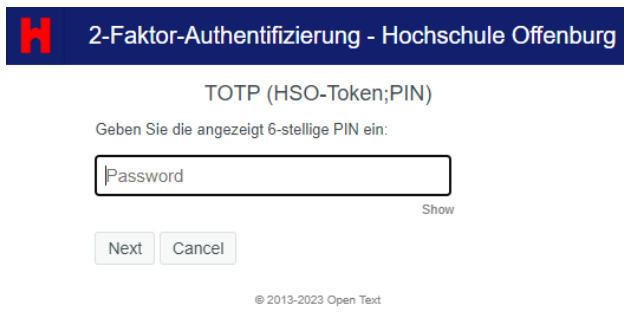
Then click on **Save**.

Log in as usual with user name + password.

Select TOTP as the login method.



Enter the PIN generated by your HSO token or Google Authenticator



Click on Next.

FIDO2 (Yubikey, USB-Stick)

A Yubikey (also known as a FIDO2 stick) is a special USB stick that can be carried as a key chain. For 2FA login, the Yubikey must be plugged into the PC/notebook; after logging in with the campus username and password, a touch button on the Yubikey must be touched - this completes the login.

Yubikeys have different functions - we only support the method called "FIDO2"; this is also the name under which the method appears in the user interface of programs.



Log in to <https://2fa.cit.hs-offenburg.de/account/>.

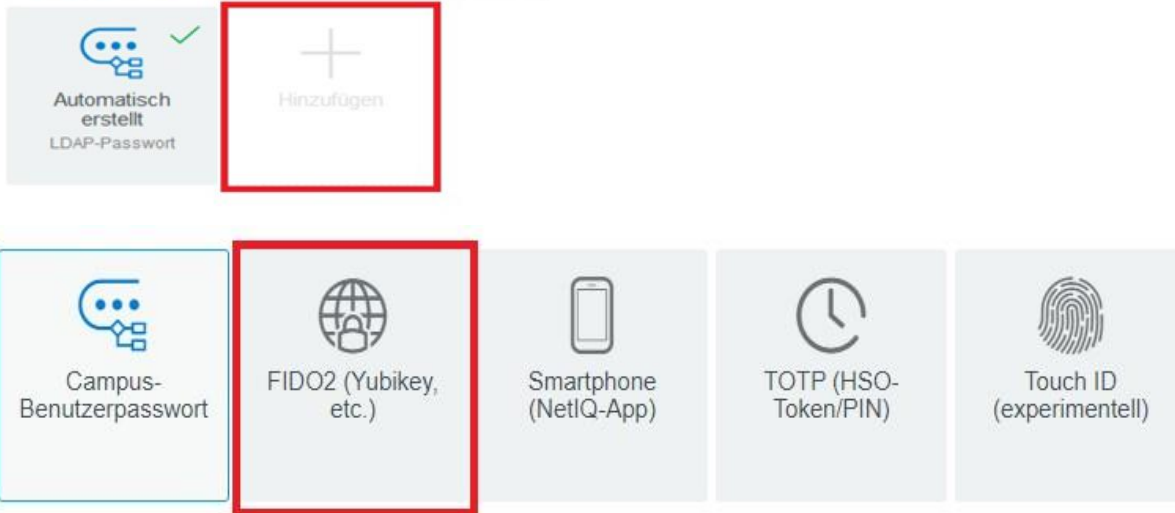
Click on the plus sign.

2-Faktor-Authentifizierung - Hochschule Offenburg

Authentication Methods

Enrolled methods are authenticators that you have already enrolled, and can be used to sign in. OTP methods are one-time password authenticators.

Your Enrolled Single Methods for sign in



Insert your FIDO2 stick (Yubikey) into a USB port on your computer.

Click on "Detect Device"

FIDO2 (Yubikey, etc.)

The FIDO2 method is an improvement to the FIDO U2F method that uses the Web Authentication standard, offering a high degree of security even without an accompanying password. FIDO2 can authenticate using phones, U2F devices, and more.

Display Name

My FIDO2 (Yubikey, etc.)

Category

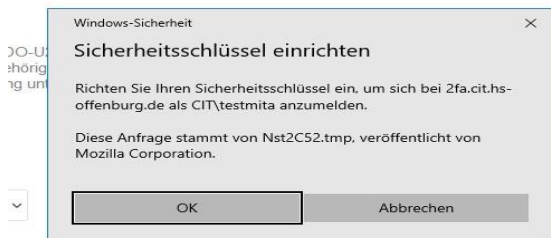
Default

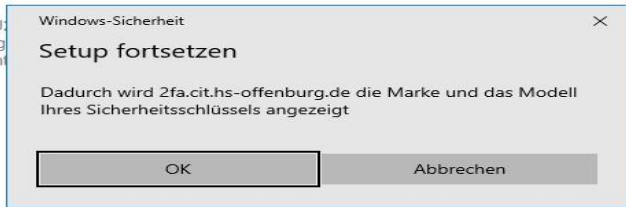
Detect Device

Save

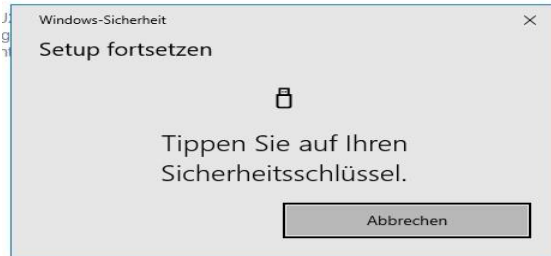
Cancel

Follow the instructions and click ok.





Tap on your Yubikey/Fido2 stick.



Click on Save.

FIDO2 (Yubikey, etc.)

The FIDO2 method is an improvement to the FIDO U2F method that uses the Web Authentication standard, offering a high degree of security even without an accompanying password. FIDO2 can authenticate using phones, U2F devices, and more.

Display Name
My FIDO2 (Yubikey, etc.)

Category Default

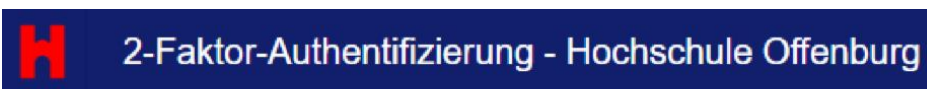
Enrollment is complete

Detect Device

Save Cancel

Log in as usual with user name + password.

Select FIDO2 as the login method.



Select Authentication Chain

Please select from the list below

Chain PW+Smartphone

Next

- PW+Smartphone
- PW+FIDO2**
- PW+TOTP

© 2013-2023 Open Text

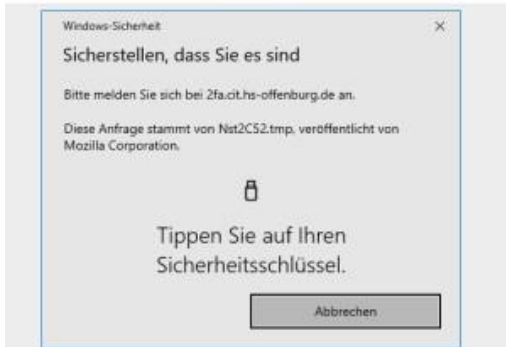
Insert the FIDO2 stick/Yubikey into a USB port on your PC.

FIDO-2.0-Authentifizierung (Fast Identity Online Device 2.0)

Tippen Sie auf Ihr FIDO-2.0 (Fast Identity Online-2.0)-Gerät zum Authentifizieren

Abbrechen

© 2013-2023 Open Test



Tap on the FIDO2 stick

More alternatives

Campus IT supports the methods described above (one-time password/TOTP, Yubikey/FIDO2, smartphone method).

In some cases, other methods may be offered, but these are not actively supported by Campus IT. If everything works, great - if not, unfortunately we can't help.

At the moment, this mainly applies to "Touch ID" for Macs. Some colleagues report that the method works, the handling is similar to Yubikey /FIDO2.

We are still checking whether "Windows Hello" is also useful - the method may disappear from the list again.

Emergency password / lost device / broken device

If you forget your smartphone/token or it is no longer functional, you can obtain a one-day emergency password from Campus IT on site (B205c) or register a new second factor.

The emergency password is valid as a second factor for this day.

New Smartphone

If you use the smartphone method and have a new smartphone, you can register 2FA for your new device.

You will still need your old device for the registration.

If your old smartphone is broken or lost, we will need to reset your second factor.

To do this, come by on site in B205c (bring your ID!) or write a ticket to helpdesk@hs-offenburg.de

Register 2FA for new device yourself:

Install the NetIQ-App ([see "Quickstart"](#)) on your new device and go to <https://2fa.cit.hs-offenburg.de/account> to change your 2-factor authentication.

Log in as usual with your username + PW + 2FA (old smartphone)

Click on the already existing registered smartphone method

Authentication Methods

Enrolled methods are authenticators that you have already enrolled, and can be used to sign in. OTP methods are one-time password authenticators.

Your Enrolled Single Methods for sign in



1. Click on "Get QR Code"
2. Scan QR Code with new Device
3. Click on "Save"

Smartphone (NetIQ-App) ✓

The Smartphone method allows authentication with your smartphone. It is an out-of-band authentication. The NetIQ Advanced Authentication application sends a push message to your smartphone, which you can accept or reject. Installing the NetIQ Advanced Authentication mobile app on your smartphone is required.

Display Name

Meine Smartphone (NetIQ-App)

Test Method

Category Default

To enroll, get a QR code and scan it using the Advanced Authentication mobile app:

Get QR Code

1. Get QR Code



2. Scan with new Device

- As a backup method, the AdvAuth mobile app provides an OTP code if internet connection is not available on your smartphone.

Save Cancel

3. Save after successful enrollment

Important:

There must always be a smartphone registered with the "Default" category. If you create another smartphone method (second device) and delete the default method, you will exclude yourself from your account!

Third-party Mail Programms (Thunderbird/Outlook/Applemail/Uninow)

Third-party mail programs such as Thunderbird, Outlook and Applemail retrieve mails via IMAP and the calendar via CalDAV. The mail function in UniNow also works via IMAP. Officially, the CIT only supports Groupwise and Webmail, but mail connections with IMAP will continue to be available. You can find more information on this under "IMAP and CalDAV"

IMAP and CalDAV

IMAP and CalDAV are a special case with regard to 2FA and are problematic because the programs, such as Thunderbird, Outlook or Apple Mail, do not directly support the technology (they do not display a window for entering the second factor). Therefore, of the methods presented here, the smartphone method is the most practicable one. There is also a workaround for TOTP.

The general procedure is as follows:

- Register your smartphone in the AA portal using the smartphone method.
- As soon as 2FA is active for GroupWise, the IMAP or CalDAV program waits after you have logged in with your campus user name and password until you have confirmed access on your smartphone by clicking "Accept".
- In this case, the second factor is valid for 10 hours - i.e. no further "Accept" is necessary until then, unless the IP address changes.
 - Example scenario for the IP address change: You use a notebook and retrieve your mails on it via IMAP. You have successfully authenticated yourself at your workstation (connected via cable) using 2FA. Now you change your location to a meeting room and want to access your emails there (via WLAN). This requires re-authentication as your notebook is in a different network and therefore has a different IP address.

Notes:

- The exact behavior depends on the respective program.
- A workaround can be used for TOTP. To do this, the TOTP pin must be entered with the password. This works with the connecting character "&". This means PW + & + TOTP as Password. The method does not work if "&" is already present in the password.
- IMAP and CalDAV programs often have several connections to the server open in the background. This can lead to strange effects - for example e.g. that the subjects of new emails are displayed, but the second factor for displaying complete emails is only displayed again on the smartphone.
- IMAP and CalDAV are different connections, in some cases these must be accepted separately.