

Securing access to UKE portals

Subject: IT-Security / Userdata

Instructions for setting up the login method for UKE portals

Access to UKE portals such as webmail.uke.de and access.uke.de from GWIS and the public Internet is only possible with a secure one-time password. This password is generated via an app on the business or personal smartphone. It is valid for 60 seconds and can be used only once.

Inhalt

1) Install authentication app	1
2) Setting up the authentication app (required only once)	1
2a) Setting up the authentication app again after changing the device (reset token)	2
3) Generate one-time password	2
4) Login to UKE Portal	2

1) Install authentication app

For the new method, you need the authentication app "**FortiToken Mobile**" on your business or personal smartphone. You can download the application via the app stores for iOS or Android.

Note: You must choose one smartphone when setting up the one-time password, as parallel setup on multiple devices is not possible for security reasons.



iOS App



Android App

2) Setting up the authentication app (required only once)

For security reasons, an additional preparatory step must be carried out when setting up a KIS1 account for the first time.

Preparatory step for KIS1 account via the self-service portal.

- Log in to <https://it-service.uke.de>
 - Click on „Anträge und Berechtigungen“
 - „IT-Arbeitsplatz“
 - „KIS1 Token beantragen“
- After submitting the web form, a system message „Abgeschlossen“ will be sent to your main UKE address.
- After receiving this email, please wait 60 minutes and continue as for setting up a KIS2/GWIS account (see next section).

For KIS1 accounts (after the above preparatory step), as well as for KIS2 and GWIS accounts, please follow these steps for initial registration:

1. Login to the GetMyQRCode website: <https://GetMyQRCode.uke.de>
 - For security reasons, only accessible from the UKE network (including VPN)
2. After typing in the login-credentials please click on **"Scan Token"** (blue button)
 - Please log in with the ID for which you would like to receive a one-time password (e.g., KIS1 username + KIS1 password for a KIS1 token).
3. Click on the "QR-Code" button
4. Select „FortiToken“ -> „Mobile“ -> „QR-Code scannen“ and confirm with „OK“
5. Scan the displayed QR code with the **"Scan Barcode"** function of the FortiToken Mobile app

2a) Setting up the authentication app again after changing the device (reset token)

If you switch to a new device you need to reset your token.

6. Login to the GetMyQRCode website: <https://GetMyQRCode.uke.de>
7. After typing in the login-credentials please click on **"Reset Token"** (red button)
8. Click on the "QR-Code" button
9. Select „FortiToken“ -> „Mobile“ -> „QR-Code scannen“ and confirm with „OK“
10. Scan the displayed QR code with the **"Scan Barcode"** function of the FortiToken Mobile app

3) Generate one-time password

The 6-digit one-time password is visible immediately after opening the app and is only valid for 60 seconds. The blue closing circle indicates the duration of validity.

Note: If you want to access the portal externally with multiple accounts, you must set up a separate QR code for each account. We recommend renaming the entry within the app accordingly (e.g. "FortiTokenGWIS", "FortiTokenKIS1", etc.).

4) Login to UKE Portal

You will find all UKE services accessible via Internet on the UKE Portal: <https://portal.uke.de>

Log in with your usual KIS1, KIS2 or GWIS user name and the generated one-time password from the app.

Note: Due to security reasons, it is still not possible to access KIS1-Webmail outside of the UKE-Network. The "Webmail"-Button is not available if you login with your KIS1-credentials on <https://portal.uke.de>.