

Setting up 2FA in the TTK Mail System

To set up two-factor authentication, you need the capability to generate tokens (one-time codes derived from a secret key). While users typically achieve this with some kind of authenticator software, most often in the form of an app on a smartphone, numerous companies also manufacture dedicated hardware for this purpose, which can be the size of a flash drive or even a credit card.

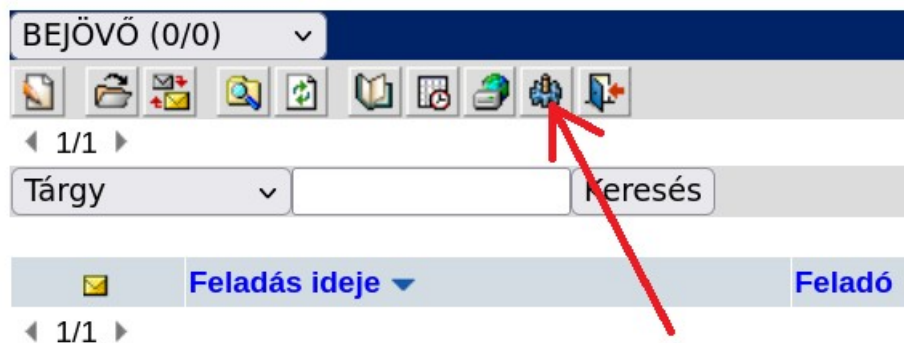
The advantage of hardware token generation over a software solution is that the authenticator software used by users often runs on the same devices they use to log into their email, which prevents the most important goal of two-factor authentication from being achieved: the physical separation of the factors. Without this, 2FA can only provide limited additional protection for users' email accounts.

For software token generation, for example, **Authy** can be used for macOS and iOS, **FortiToken** for Windows, **OTPClient** for Linux, and **Google Authenticator** for Android devices.

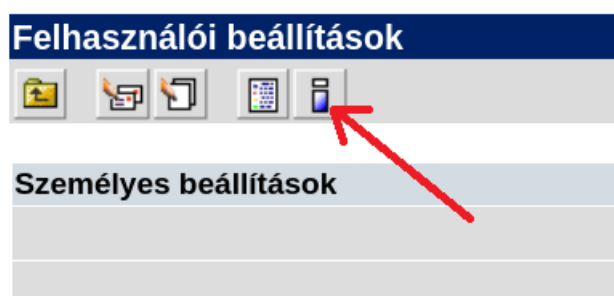
If the user is currently using any software authenticator program, they do not need to install a new piece of software specifically for setting up two-factor authentication in the TTK mail system. The existing one can almost certainly be used.

1. Setting up 2FA on the classic interface:


After logging in, you need to click on the gear icon in the top left menu bar to enter the settings.



Within the settings, you need to click on the 'i' icon.



Here you can find the option to enable two-factor authentication in the "Tufa two-factor authentication settings" menu item.

About	
	
CLIENT	
Tufa kétfaktoros azonosítás beállítások	<input type="button" value="Tufa bekapcsolás"/>

By clicking on the "Enable Tufa" button, the two-factor authentication key, the QR code, and the one-time use login keys are generated for the user. An example of this:

Tufa token aktiválás
secret: UMRQRVRHCMSE2RR5

Recovery kulcsok: 0566685654 0790379600 9489102283 9263757512 2963467829 3423829084 4501347956 1707873965 4261406039
bekapcsoláshoz adja meg a token: <input type="text"/> <input type="button" value="teszt"/>

The two-factor authentication can be set up in the user's chosen authenticator application, such as Google Authenticator, by both entering the setup key (e.g., "UMRQVRHCMSE2RR5" in the example image) and scanning the QR code.


It is important that if the user does not use the QR code, when entering the setup key, they must verify that the key type is set to time-based (TOTP) in the authenticator software.

Precisely because token generation also requires the current value of the precise time, while general-purpose desktop computers, for example, are extremely unreliable in this regard, it is advisable to enable regular time synchronization with a time server under both Windows and Linux operating systems. For Windows operating systems, time synchronization can be performed within the "Settings" under "Time & Language / Date & time," while under Linux, this can also be achieved from the command line.


The "Recovery keys" shown in the example image can only be used once, and are specifically designed to allow the user to log in even if the authenticator software and the tokens it can generate are unavailable, for example, after a reinstallation. This is why it is very important for the user to copy these one-time keys.

After the user has successfully set up two-factor authentication in their authenticator application, the most recently generated token must be entered into the field "enter the token to enable:" at the very bottom, and then the test button must be pressed.

bekapcsoláshoz adja meg a tokent:

If successful, two-factor authentication is enabled in the mail system, making further settings available in the "Tufa two-factor authentication settings" menu item.

About			
			
CLIENT			
Tufa kétfaktoros azonosítás beállítások	<input type="button" value="TTK-ról ne kérje"/>	<input type="button" value="PTE-ről ne kérje"/>	<input type="button" value="Magyarországról ne kérje"/>
	<input type="button" value="tufa ki"/>		

The "tufa off" button disables two-factor authentication, and the three buttons above it serve for the user to set the range within which they do not want to provide a two-factor authentication token at all during login. All three functions can be turned off or back on at any time as desired.

The "Don't ask from TTK" function applies to the wired network of the Faculty of Sciences and the PTE TTK Wi-Fi channel.

The "Don't ask from PTE" function applies to the entire university wired network and the Eduroam Wi-Fi channel from within the PTE area.

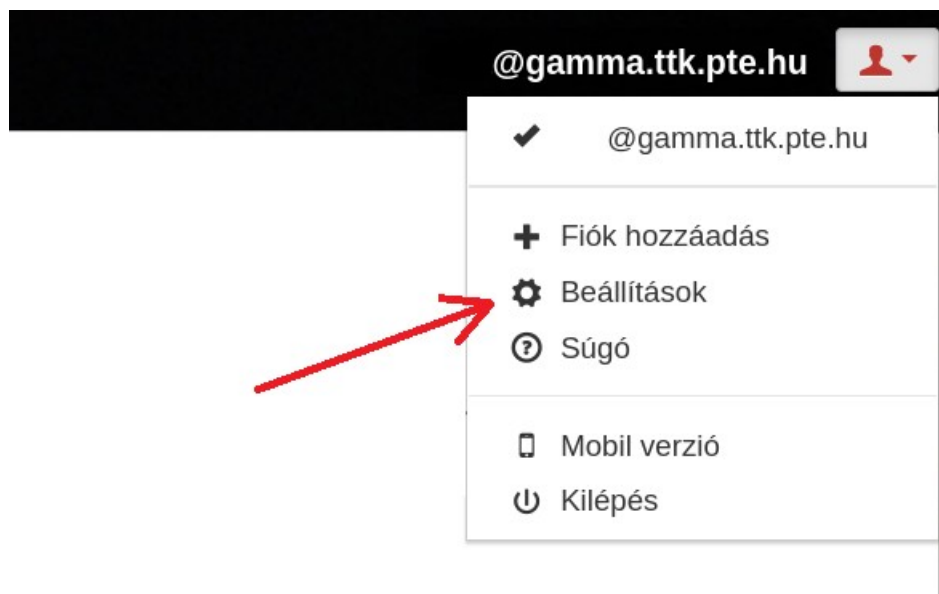
The "Don't ask from Hungary" function applies to logging in from any domestic location.

With these functions, using two-factor authentication in the TTK mail system can become much easier, because, for example, by enabling "Don't ask from TTK," there's no need to constantly bother with entering tokens while at the Faculty of Sciences, while two-factor authentication continues to protect the user's mail against external attackers.

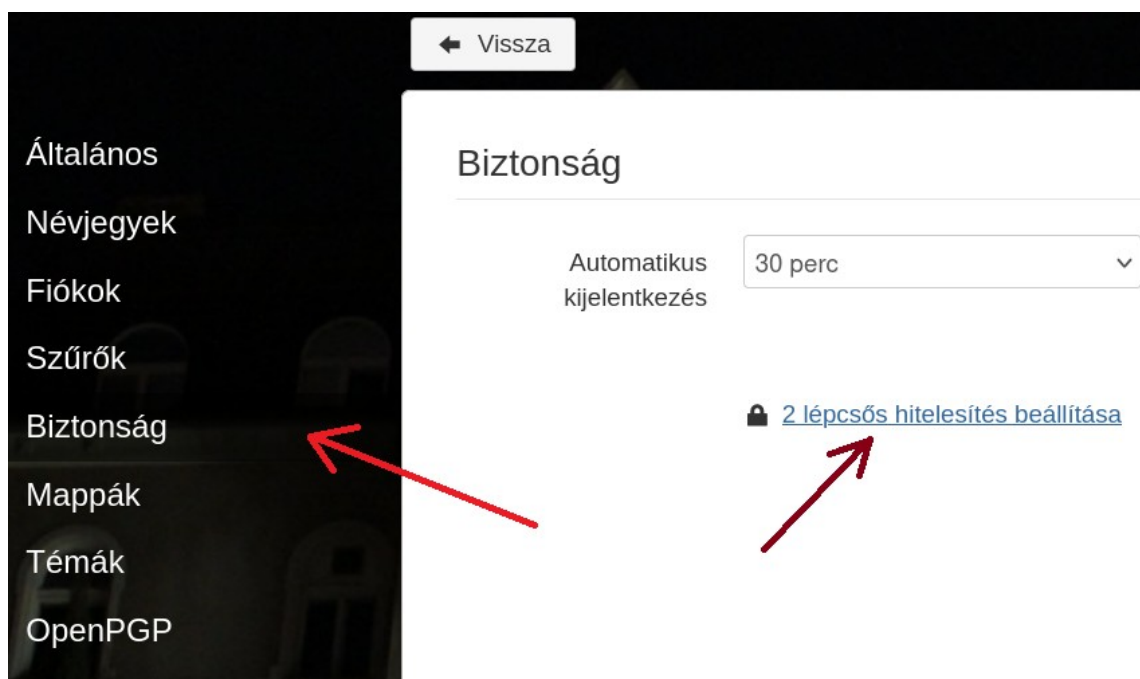
In addition, upon successful authentication on the classic interface, the system will not ask the user for a token again for nine hours when logging in, which can conveniently cover an average workday.

2. Setting up 2FA on the modern interface:

After logging in, click on the profile picture in the top right corner and select "Settings" from the dropdown menu.



Within the settings, first click on the "Security" menu item on the left, and then click on the "Set up 2-step authentication" link that appears on the right.



The next step is to use the "Activate" button.

2 lépcsős hitelesítés

×

Felhasználó

@gamma.ttk.pte.hu



▶ Aktivál

✓ Kész

By clicking on the "Activate" button, the two-factor authentication key, the QR code, and the one-time use login keys are generated for the user. An example of this:

2 lépcsős hitelesítés

×

☐ 2 lépcsős hitelesítés engedélyezése [teszt](#)

Felhasználó

@gamma.ttk.pte.hu

Titok

RPUTR5U7XVGC5DCE [Titok elrejtése](#)

Importáld ezt az infót a Google Authenticator kliensedbe (vagy más TOTP kliensbe) az alábbi QR kód használatával vagy a kód manuális megadatosával.



Biztonsági kódok

172477479 872173176
170802633

Ha nem kapod meg a kódokat a Google Authenticator kliensből (vagy más TOTP kliensből), akkor a bejelentkezéshez használhatod a biztonsági kódot. A biztonsági kód használata után inaktívvá válik.

✕ Töröl

✓ Kész

The two-factor authentication can be set up in the user's chosen authenticator application, such as Google Authenticator, by both entering the setup key (e.g., "RPUTR5U7XVGC5DCE" in the example image) and scanning the QR code.

It is important that if the user does not use the QR code, when entering the setup key, they must verify that the key type is set to time-based (TOTP) in the authenticator software.

Precisely because token generation also requires the current value of the precise time, while general-purpose desktop computers, for example, are extremely unreliable in this regard, it is advisable to enable regular time synchronization with a time server under both Windows and Linux operating systems. For Windows operating systems, time synchronization can be performed within the "Settings" under "Time & Language / Date & time," while under Linux, this can also be achieved from the command line.

The "Recovery keys" shown in the example image can only be used once, and are specifically designed to allow the user to log in even if the authenticator software and the tokens it can generate are unavailable, for example, after a reinstallation. This is why it is very important for the user to copy these one-time keys.

After the user has successfully set up two-factor authentication in their authenticator application, they must test it before activating it in the mail system by clicking on the "test" link at the very top.

2 lépcsős hitelesítés

☐ 2 lépcsős hitelesítés engedélyezése [teszt](#)



If the user has entered a valid token, clicking on the "Test" button will make it turn green.

2-lépéses hitelesítés teszt



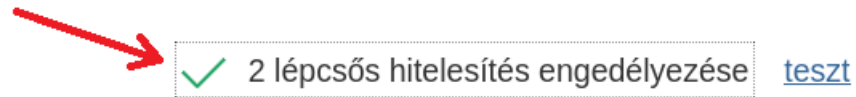
Kód

043098

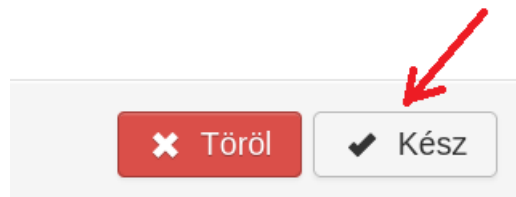
✓ Tesztelés

After this, a very important step follows. Stepping back one screen from here, you must tick the "Enable 2-step authentication" checkbox.

2 lépcsős hitelesítés



Finally, the authentication can be activated with the "Done" button at the bottom of the page.



After the user has successfully enabled two-factor authentication on the modern interface of the TTK mail system, at the next login, there is an option to tick the "Don't ask for the code for two weeks" box. However, this function only applies to the specific device on which the user is currently logging in.

