

Autentificare folosind platforma login.upb.ro

Platforma <https://login.upb.ro> implementează autentificarea folosind doi pași:

- Nume de utilizator și parolă
- Utilizarea unui cod de autentificare de tip [TOTP](#)

IMPORTANT: Vă rugăm raportați probleme de funcționalitate pe platforma de ticketing (<https://support.upb.ro/>) pentru a putea fi adresate în cel mai scurt timp posibil.

IMPORTANT: După realizarea configurărilor din acest tutorial, la autentificarea pe platforma <https://login.upb.ro> vă este cerut doar codul OTP (din aplicația folosită, codul de 6 cifre generate o dată la 30 secunde). Nu mai trebuie să refaceți pașii de scanare cod QR".

Nu dezinstalați aplicația configurată după realizarea setărilor și nu ștergeți codul din aplicație.

Numele de utilizator și parola sunt cele care au fost folosite și până acum pe platformele universității. Resetarea parolei se poate realiza prin intermediul platformei <https://my.upb.ro/>. Al doilea pas de autentificare utilizează un dispozitiv sau program secundar pentru generarea unui cod la fiecare 30 de secunde; procesul este detaliat în secțiunile de mai jos. Nu toate platformele au implementat acest tip de autentificare în mod implicit; acest ghid se adresează doar pentru platformele care utilizează platforma login.upb.ro pentru autentificare.

Pe pagina de autentificare a platformei Moodle puteți observa un buton pentru autentificare (în imaginea de mai jos) pentru redirectarea autentificării către platforma login.upb.ro.



Cookies must be enabled in your browser ?

Log in using your account on:



Acest tutorial vă prezintă 3 modalități de configurare a autentificării în doi pași folosind:

1. **Telefon cu posibilitate de scanare a unui cod QR:** Procesul de autentificare (secțiunea [Procesul de autentificare](#)) folosind una din aplicațiile GoogleAuthenticator sau FreeOTP (secțiunea [Configurare aplicație OTP telefon \(recomandat\)](#)), prin scanare unui cod QR (secțiunea [Cod QR](#))
2. **Telefon fără posibilitate de scanare a unui cod QR:** Procesul de autentificare (secțiunea [Procesul de autentificare](#)) folosind una din aplicațiile GoogleAuthenticator sau FreeOTP (secțiunea [Configurare aplicație OTP telefon \(recomandat\)](#)), prin introducerea unei chei secrete (secțiunea [Cod secret \(manual\)](#))
3. **Aplicație desktop:** Procesul de autentificare (secțiunea [Procesul de autentificare](#)) folosind aplicația KeePass ([Configurare aplicație OTP desktop \(alternativă telefon\)](#)) prin introducerea unei chei secrete (secțiunea [Cod secret \(manual\)](#)).


[La sfârșitul acestui document, aveți o listă cu întrebările frecvente.](#)

Procesul de autentificare

Ecran 1: nume de utilizator și parolă

Primul ecran de autentificare conține un formular două câmpuri în care trebuie introduse numele de utilizator și parola (vizibil în imaginea de mai jos).

IMPORTANT: Opțiunea “Remember me” are efectul de a păstra sesiunea activă după închiderea ferestrei de browser, iar la următoarea pornire nu se va cere autentificarea. În cazul în care opțiunea nu este folosită, după repornirea browser-ului se va cere din nou autentificarea.



UNIVERSITATEA POLITEHNICA BUCUREȘTI

Sign in to your account

Username or email
example.user

Password
.....

Remember me [Forgot Password?](#)

Sign In


Ecran 2: Configurare aplicație OTP

IMPORTANT: Codul OTP va fi cerut la fiecare autentificare. Indiferent de aplicația utilizată pentru generarea codurilor, este recomandat să aveți o variantă de backup a codurilor pentru a nu pierde accesul în cazul în care nu mai aveți acces la dispozitiv (utilizați un alt telefon mobil, păstrați o copie a bazei de date în care păstrați codul secret într-un loc sigur în cazul în care folosiți o aplicație desktop, utilizați și o aplicație desktop pentru backup în cazul în care telefonul mobil este principalul dispozitiv). **Nu ștergeți acest cod din aplicația utilizată pentru înregistrare și nu dezinstalați aplicația.**

În cazul în care numele de utilizator și parola sunt acceptate, următorul ecran o să ceară configurarea unui dispozitiv de tip OTP (FreeOTP sau Google Authenticator pe un dispozitiv Android sau iOS) prin scanarea unui cod QR (1). În cazul în care doriți să scrieți codul manual (camera video a telefonului nu funcționează, sau folosiți o aplicație desktop pentru generarea codului), puteți apăsa pe “Unable to scan?” (2).

IMPORTANT: Codul generat diferă la fiecare reîncărcare a paginii. Din acest motiv este recomandată reîncărcarea paginii imediat înainte de scanarea sau introducerea codului.

Cod QR



UNIVERSITATEA POLITEHNICA BUCUREȘTI

Mobile Authenticator Setup

⚠ You need to set up Mobile Authenticator to activate your account.

1. Install one of the following applications on your mobile:

- FreeOTP
- Google Authenticator

2. Open the application and scan the barcode:

1



2

[Unable to scan?](#)

3. Enter the one-time code provided by the application and click Submit to finish the setup.

Provide a Device Name to help you manage your OTP devices.

One-time code *

Device Name

Submit

Cod secret (manual)

Dacă optați să nu scanați codul QR, după apăsarea “Unable to scan?” veți vedea un ecran ca cel de mai jos. De interes este codul secret (1) pe care va trebui să îl introduceți manual în aplicația de generare de coduri.

UNIVERSITATEA POLITEHNICA BUCUREȘTI

Mobile Authenticator Setup

⚠ You need to set up Mobile Authenticator to activate your account.

1. Install one of the following applications on your mobile:
FreeOTP
Google Authenticator
2. Open the application and enter the key:
1 → AAAA BBBB CCCC DDDD EEEE FFFF GGGG HHHH
[Scan barcode?](#)
3. Use the following configuration values if the application allows setting them:
Type: Time-based
Algorithm: SHA1
Digits: 6
Interval: 30
4. Enter the one-time code provided by the application and click Submit to finish the setup.
Provide a Device Name to help you manage your OTP devices.

One-time code *

Device Name

Submit

Instrucțiuni configurare aplicație OTP

Telefon: Pentru instrucțiuni legate de folosirea unei aplicații de telefon mergeți la secțiunea [Configurare aplicație OTP telefon \(recomandat\)](#).

Aplicație desktop: Pentru instrucțiuni legate de folosirea unei aplicații desktop mergeți la secțiunea [Configurare aplicație OTP desktop](#).

După configurarea aplicației de OTP, următoarele autentificări o să necesite introducerea codului OTP generat de aplicații, iar interfața o să fie similară cu cea din imaginea de mai jos.



Observație: Puteți gestiona dispozitivele dumneavoastră OTP la adresa <https://login.upb.ro/auth/realms/UPB/account/#/security/signingin>.

Configurare aplicație OTP telefon (recomandat)

Pentru telefon aveți de ales între Google Authenticator (disponibil pe [Android](#) sau [iOS](#)) și FreeOTP (disponibil pe [Android](#) și [iOS](#)).

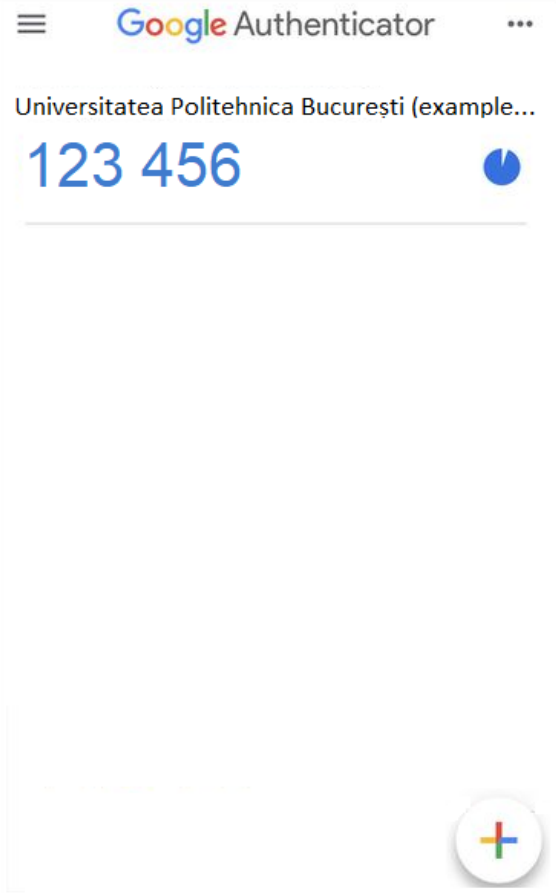
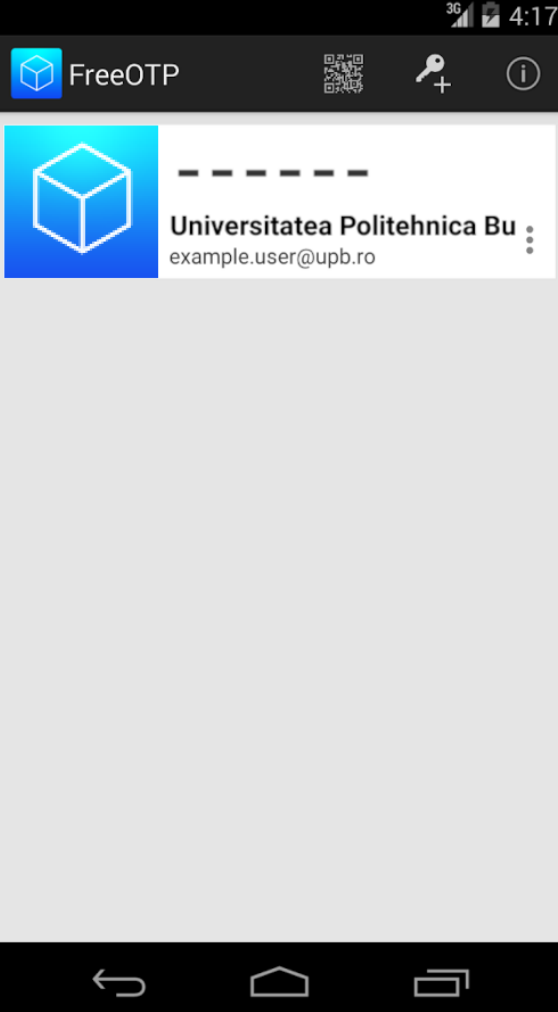
Pentru configurarea codului puteți utiliza una dintre două metode: scanare cod QR sau introducerea manuală a codului secret.

Scanare cod QR

Accesați meniul de configurare a codului OTP prin scanarea codului QR ca în imaginea de mai jos.

Google Authenticator	FreeOTP
<p>Apăsați butonul + pentru a adăuga o nouă intrare (din chenarul roșu de mai jos) și alegeți opțiunea "Scanați un cod QR/ Scan a QR code"</p> 	<p>Apăsați butonul de scanare de cod QR (chenarul roșu din imaginea de mai jos)</p> 

Filmați cu telefonul ecranul monitorului și încadrați codul QR în chenarul din aplicație. Codul QR este detectat și scanat aproape imediat după ce pătratul ajunge în fața camerei video.


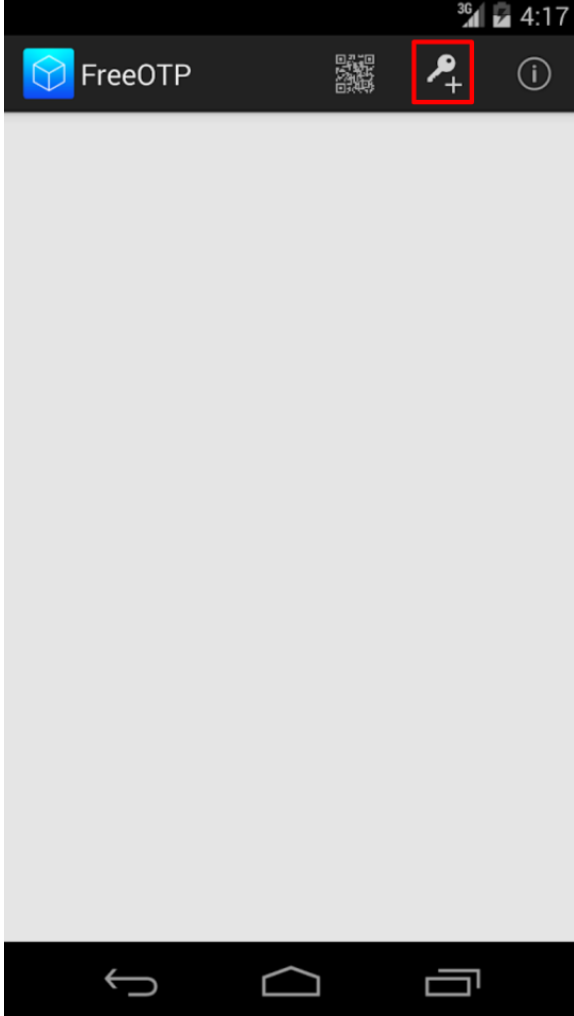
Google Authenticator	FreeOTP
<p data-bbox="204 389 783 488">După scanarea codului QR, se generează o intrare nouă, asemănătoare celei de mai jos,</p>  <p data-bbox="231 584 762 613">Universitatea Politehnica București (example...)</p> <p data-bbox="245 629 464 685">123 456</p>	<p data-bbox="810 389 1380 488">După scanarea codului QR, se generează o intrare nouă, asemănătoare celei de mai jos.</p>  <p data-bbox="833 551 1002 584">FreeOTP</p> <p data-bbox="847 640 970 752">Universitatea Politehnica Bu</p> <p data-bbox="986 707 1198 763">example.user@upb.ro</p>

Pentru generarea codului OTP, apăsați pe intrarea din listă. Codul OTP este valabil 30 de secunde.

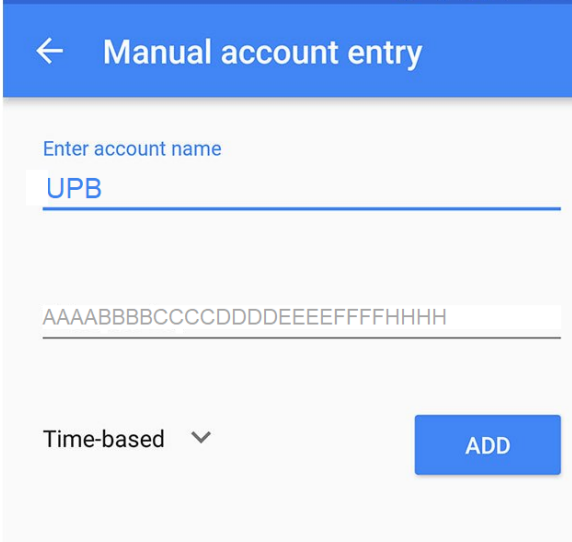
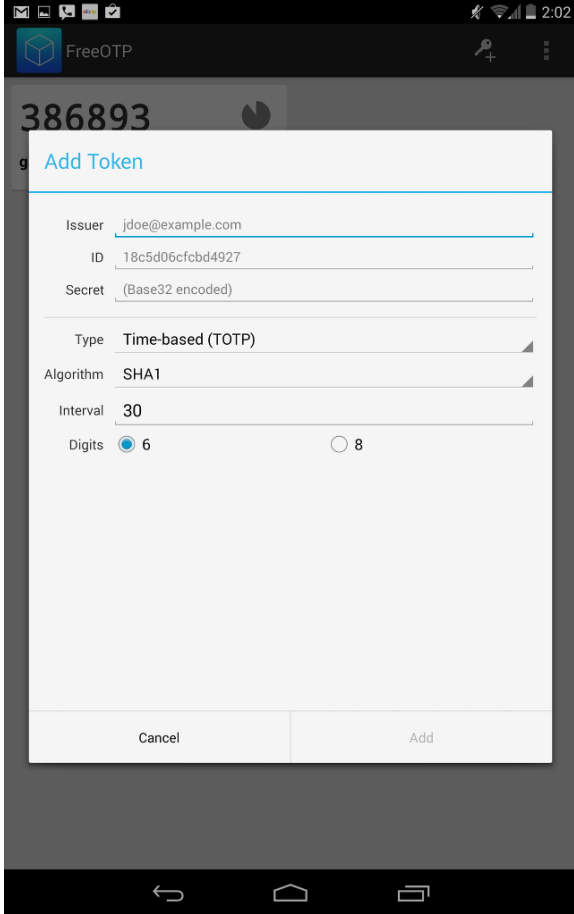


Introducerea manuală a codului

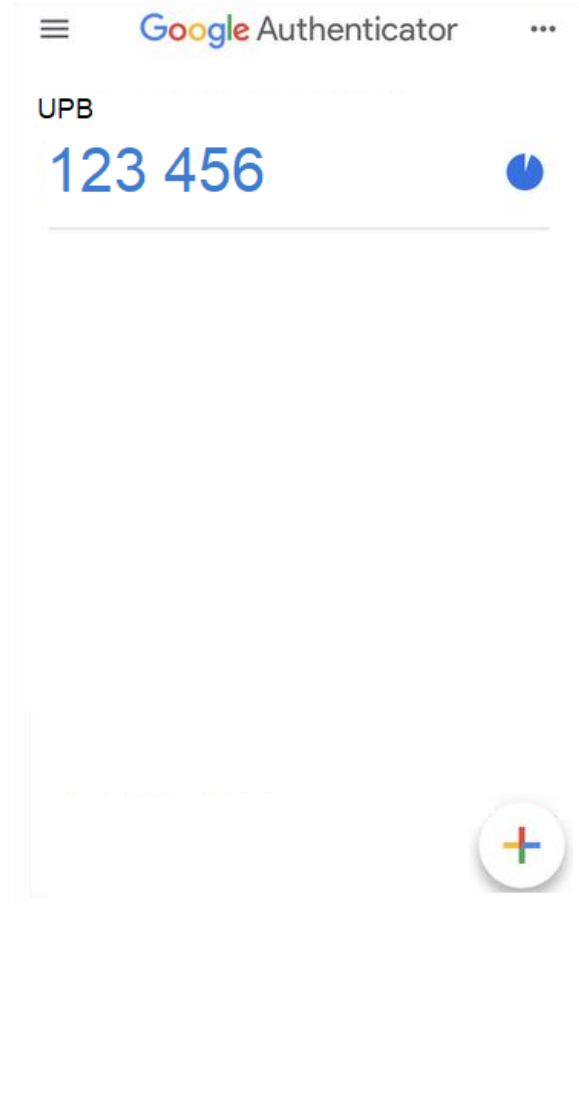
Accesați meniul de configurare manuală a codului OTP ca în imaginea de mai jos.

Google Authenticator	FreeOTP
<p data-bbox="204 369 735 504">Apăsați butonul + (reprezentat în chenar roșu în imaginea de mai jos) și alegeți "Introduceți cheia de configurare/Enter a setup key".</p> 	<p data-bbox="810 369 1353 470">Apăsați butonul de configurare manuală a codului (reprezentat în chenar roșu în imaginea de mai jos).</p> 

O dată ce vă aflați în meniul de configurare, introduceți codul secret afișat pe pagina de autentificare în câmpul aplicației.

Google Authenticator	FreeOTP
<p>Configurați intrările de mai jos astfel:</p> <ul style="list-style-type: none">• Numele contului/ Enter account name: Denumirea pe care o doriți pentru a reține mai ușor intrarea (ex: UPB, Universitatea Politehnica București etc.)• Cheia dvs/Enter your key: Codul afișat pe pagina de browser (Cod secret (manual))• Tipul cheii: În funcție de oră/Time-based <p>Apăsați butonul Add.</p> 	<p>Configurați intrările de mai jos astfel:</p> <ul style="list-style-type: none">• Issuer: Universitatea Politehnica București• ID: nume utilizator (ex: contul dumneavoastră de LDAP)• Secret: Codul afișat de pagina de browser (Cod secret (manual))• Type: Time-based/TOTP (lăsați valoarea implicită)• Algorithm: SHA1 (lăsați valoarea implicită)• Digits: 6 (lăsați valoarea implicită)• Interval: 30 (lăsați valoarea implicită) <p>Apăsați butonul Add.</p> 

După configurarea manuală a intrării, veți avea o intrare nouă în aplicație, asemănătoare imaginii de mai jos:

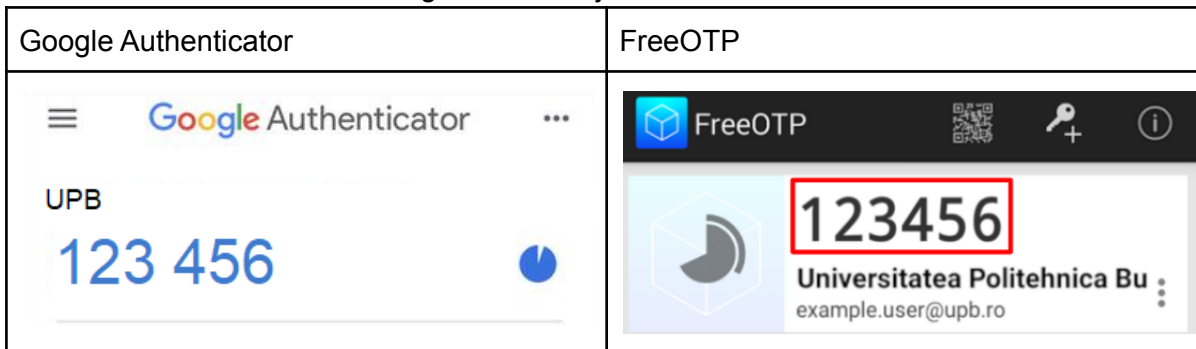


După configurarea manuală a intrării, veți avea o intrare nouă în aplicație, asemănătoare imaginii de mai jos. Pentru generarea unui cod unic, apăsați pe intrarea de mai jos.



Introducerea codului de autentificare

Dacă ați urmat pașii corect, veți vedea în aplicație un cod numeric care se generează la fiecare 30 de secunde ca în imaginea de mai jos.



Acest cod trebuie introdus în câmpul “One-time code” al paginii de autentificare ca în imaginea de mai jos (1). Opțional, puteți să atribuiți și un nume aplicației (2) pe care îl puteți vedea în consola de administrare a contului de pe platforma de autentificare.

The image shows a 'Mobile Authenticator Setup' page from the University of Bucharest. The page contains the following text and form elements:

- Header: UNIVERSITATEA POLITEHNICA BUCUREȘTI
- Section: Mobile Authenticator Setup
- Warning: You need to set up Mobile Authenticator to activate your account.
- Step 1: Install one of the following applications on your mobile:
 - FreeOTP
 - Google Authenticator
- Step 2: Open the application and enter the key:
 - AAAA BBBB CCCC DDDD EEEE FFFF GGGG HHHH
 - Scan barcode?
- Step 3: Use the following configuration values if the application allows setting them:
 - Type: Time-based
 - Algorithm: SHA1
 - Digits: 6
 - Interval: 30
- Step 4: Enter the one-time code provided by the application and click Submit to finish the setup.
- Provide a Device Name to help you manage your OTP devices.
- Form fields:
 - One-time code * (with value 123456)
 - Device Name (with value Phone)
- Submit button

Red arrows labeled '1' and '2' point to the 'One-time code' and 'Device Name' fields respectively.

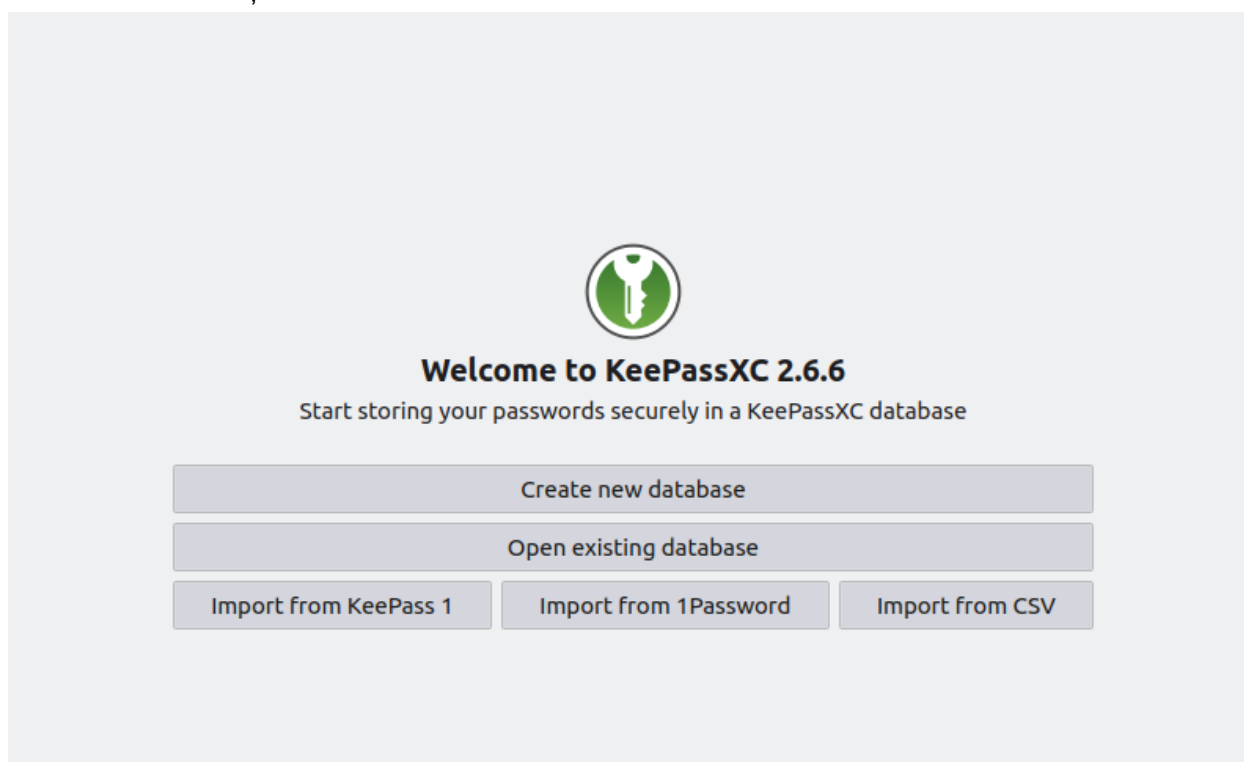
Configurare aplicație OTP desktop (alternativă telefon)

Pentru generarea de coduri OTP puteți utiliza o aplicație desktop sau extensii de browser. Puteți utiliza orice aplicație doriți, dar vă rugăm să folosiți doar aplicații în care aveți încredere. Extensii populare pentru managementul parolelor (ex. LastPass sau Bitwarden) au funcționalitatea de generare a codurilor OTP în variantele premium.

În acest ghid vom prezenta folosirea [KeepassXC](#), care este un program de gestionare a parolelor disponibil pe Windows, macOS și Linux în mod gratuit. Aplicația folosește baze de date criptate local pe sistemul de calcul, care nu sunt sincronizate în mod implicit cu servicii externe. Din acest motiv este responsabilitatea dumneavoastră să vă asigurați că baza de date este păstrată în siguranță.

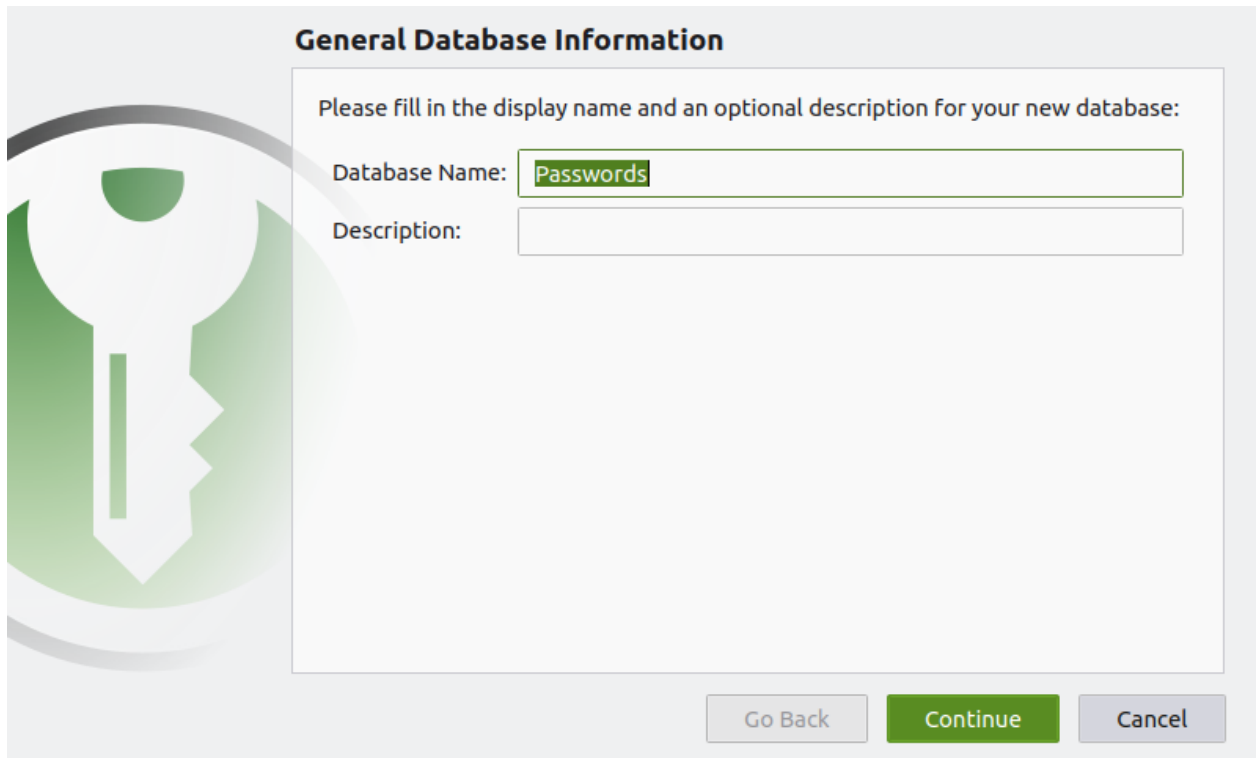
Configurare prima pornire

La prima pornire a aplicației veți vedea un ecran ca cel de mai jos pentru crearea sau deschiderea unei baze de date. Vom presupune că o bază de date nu este deja creată și vom alege opțiunea "Create new database". Aveți posibilitatea să folosiți o bază de date existentă dacă aveți.



În continuare vor fi prezentate diferite opțiuni pentru configurarea bazei de date:

- Configurarea unui nume. Puteți alege orice nume doriți; acest nume este afișat în partea de sus a ferestrei atunci când baza de date este folosită



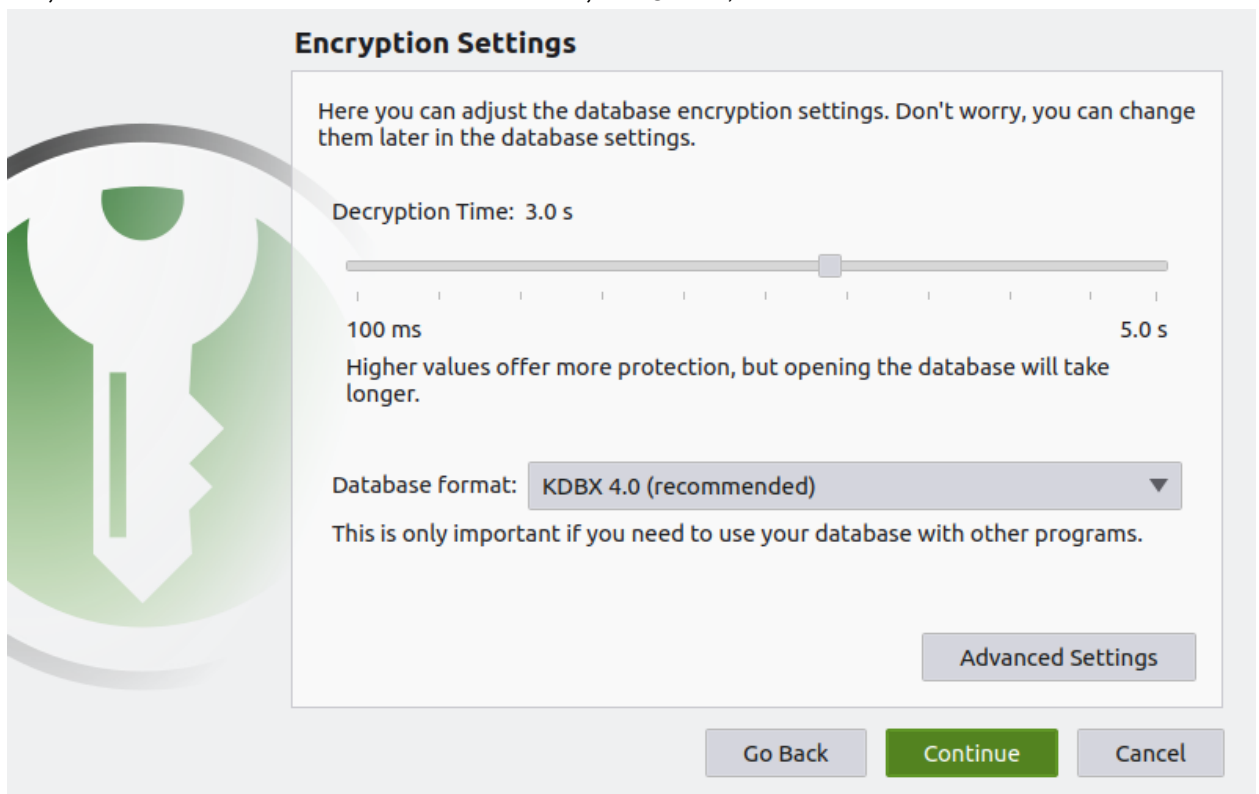
General Database Information

Please fill in the display name and an optional description for your new database:

Database Name:

Description:

- Configurarea unui format de bază de date și a timpului necesar decriptării. Puteți crește timpul necesar decriptării pentru a crește siguranța bazei de date.



Encryption Settings

Here you can adjust the database encryption settings. Don't worry, you can change them later in the database settings.

Decryption Time: 3.0 s

100 ms 5.0 s

Higher values offer more protection, but opening the database will take longer.

Database format:

This is only important if you need to use your database with other programs.

- Configurarea unei parole de criptare a bazei de date. Recomandăm folosirea unei parole sigure, dar diferită de cea pe care o utilizați la diferite conturi.

Database Credentials

A set of credentials known only to you that protects your database.

Password

Enter password:

Confirm password:

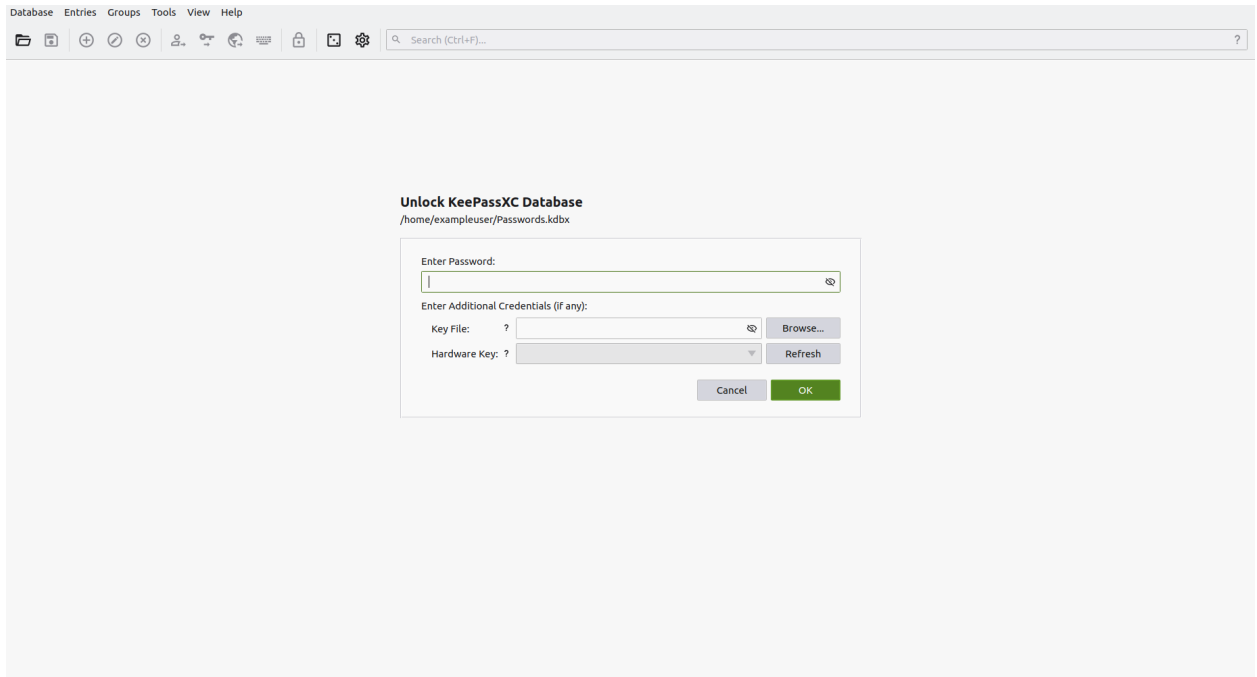
Cancel

Add additional protection...

Go Back Done Cancel

După ce ați configurat acești parametri, o să apară o fereastră în care să alegeți unde va fi salvată baza de date. După ce este salvată, baza de date va fi deblocată și puteți adăuga intrări pentru a salva parole sau coduri OTP.

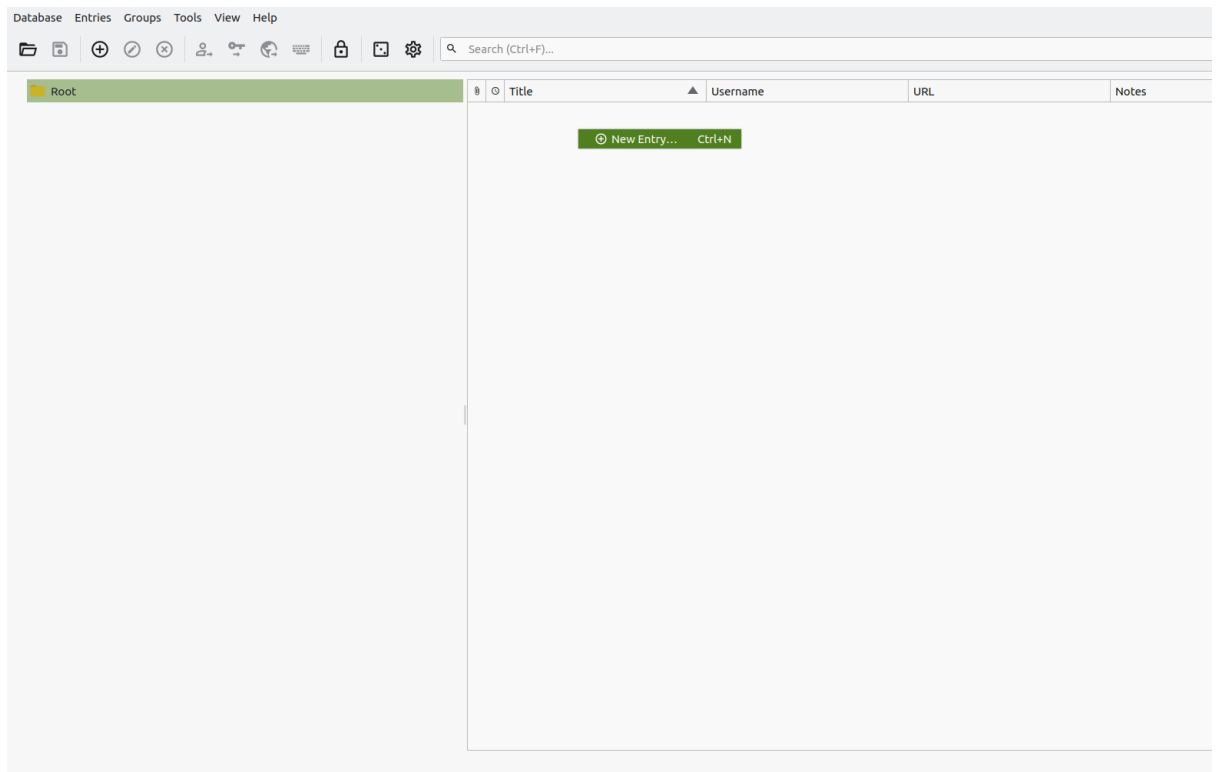
IMPORTANT: După o perioadă de inactivitate, la blocarea ecranului sistemului sau după închiderea aplicației baza de date este blocată automat, iar la următoarea accesare vi se va cere să o deblocați. Parola cu care ați criptat baza de date în timpul creării este singurul mod în care aceasta poate fi decriptată. În cazul în care uitați parola, pierdeți permanent accesul la baza de date. Din acest motiv este foarte important să nu uitați parola. Interfața după prima pornire (dacă baza de date este creată, dar blocată) arată ca cea din imaginea de mai jos.



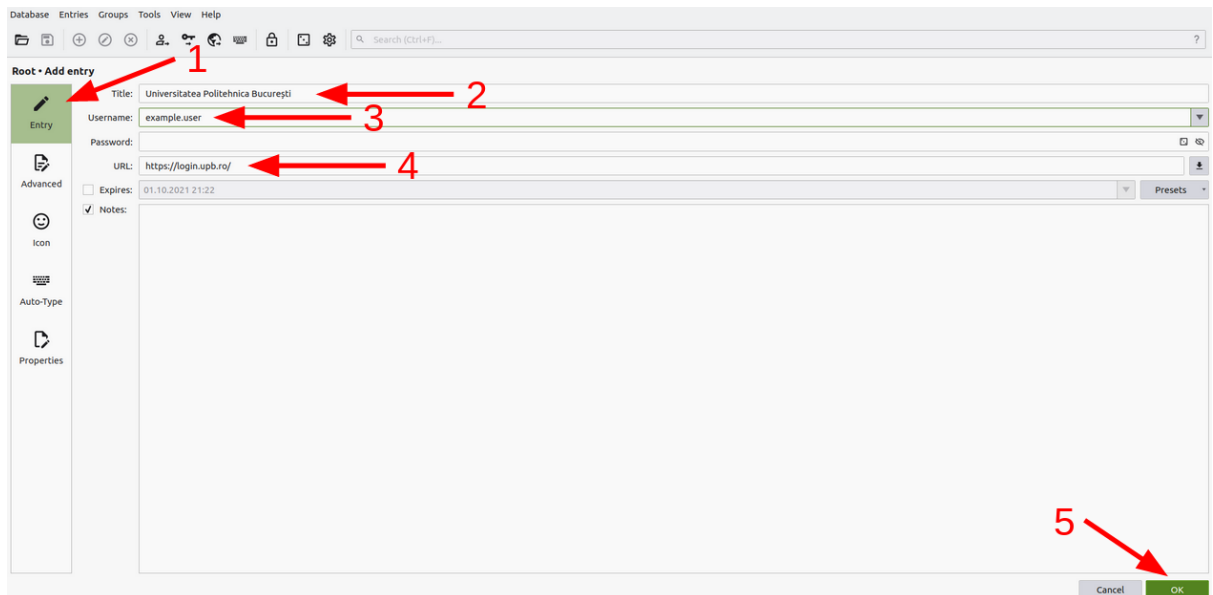
Adăugare date de acces (cod TOTP)

Pentru adăugarea unui cod TOTP, urmați pașii de mai jos:

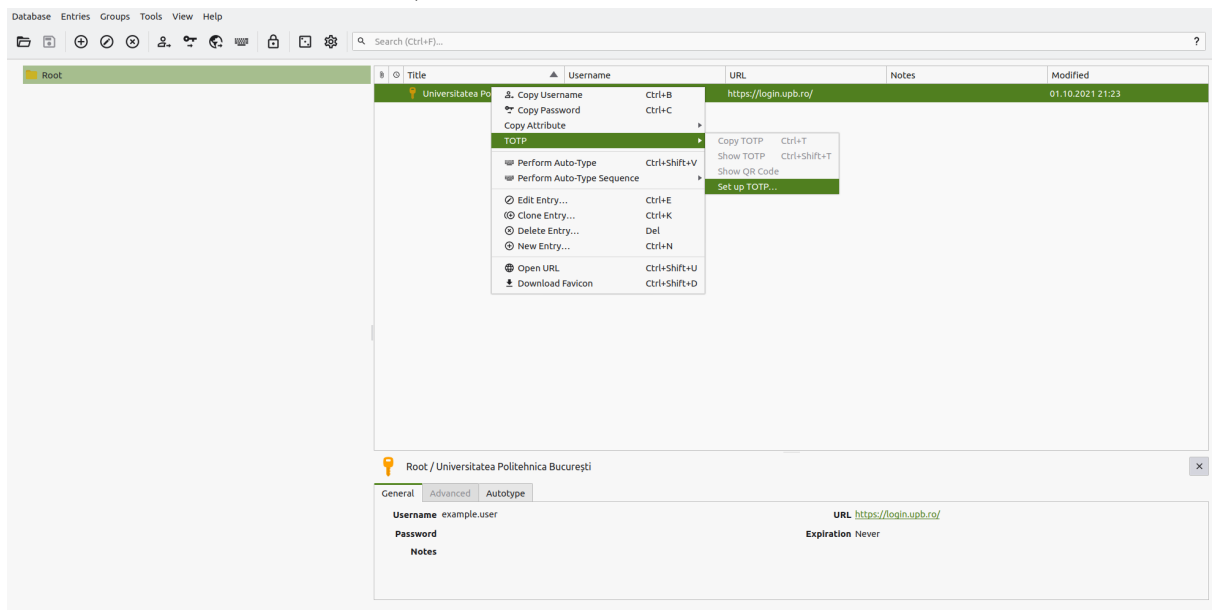
- Apăsați click dreapta pe spațiul alb din partea dreaptă a interfeței și apăsați butonul “New Entry...”. Alternativ, apăsați combinația de taste “Ctrl+N”.



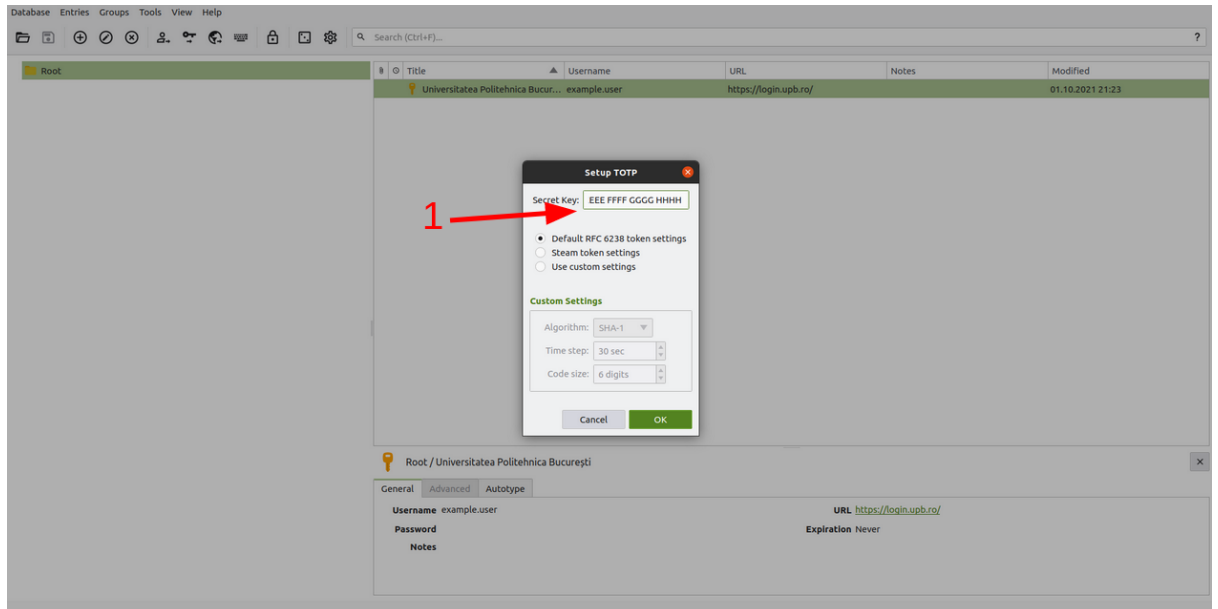
- În secțiunea “Entry” (1) introduceți datele pentru intrarea curentă: pentru “Title” (2) adăugați textul “Universitatea Politehnica București”, pentru “Username” (3) adăugați numele de utilizator al contului, iar pentru “URL” (4) introduceți <https://login.upb.ro/>, iar apoi salvați setările folosind butonul “OK” (5) din partea dreapta-jos a interfeței.



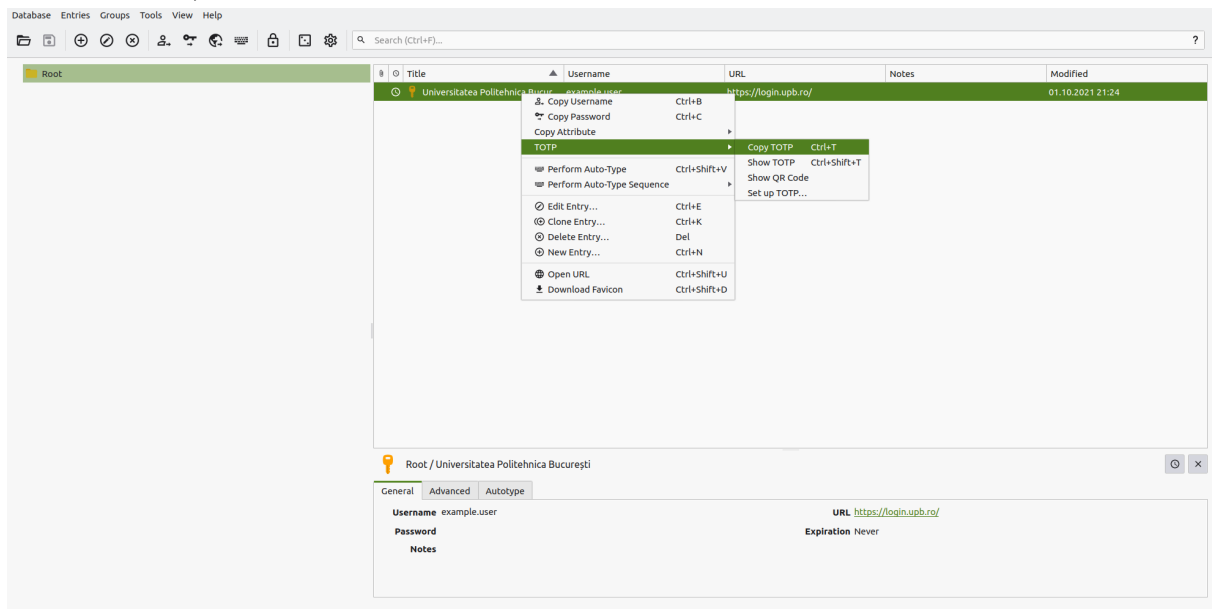
- Apăsați click dreapta pe linia cu intrarea nou creată, iar din meniul apărut alegeți “TOTP”, iar din submeniu alegeți “Set up TOTP...”.



- Adăugați codul secret din interfața paginii de login, similară cu cea din secțiunea [Cod secret \(manual\)](#), în câmpul “Secret Key” (1), după care salvați setările.
Observație: este posibil ca dacă ați început procesul de instalare după ce ați afișat codul, pagina de autentificare să fi expirat, iar codul să fi devenit invalid. Încercați să reîncărcați pagina de autentificare înainte de a copia codul. Dacă a expirat, vi se va cere să introduceți din nou numele de utilizator și parola, după care puteți continua procesul.



- Copiați codul generat prin apăsarea click dreapta pe linia cu intrarea configurată, iar din meniu alegeți “TOTP”, iar din submeniu alegeți “Copy TOTP”. Alternativ, puteți folosi combinația de taste “Ctrl+T”.



- Copiați codul în pagina de autentificare câmpul “One-time code” (1). Opțional, puteți să atribuiți și un nume aplicației (2) pe care îl puteți vedea în consola de administrare a contului de pe platforma de autentificare.

Observație: conținutul copiat este disponibil în clipboard timp de 10 secunde, după care este eliminat; din acest motiv codul trebuie copiat rapid.

UNIVERSITATEA POLITEHNICA BUCUREȘTI

Mobile Authenticator Setup

⚠ You need to set up Mobile Authenticator to activate your account.

1. Install one of the following applications on your mobile:
FreeOTP
Google Authenticator
2. Open the application and enter the key:
AAAA BBBB CCCC DDDD EEEE FFFF GGGG HHHH
[Scan barcode?](#)
3. Use the following configuration values if the application allows setting them:
Type: Time-based
Algorithm: SHA1
Digits: 6
Interval: 30
4. Enter the one-time code provided by the application and click Submit to finish the setup.
Provide a Device Name to help you manage your OTP devices.

One-time code *
123456

Device Name
Phone

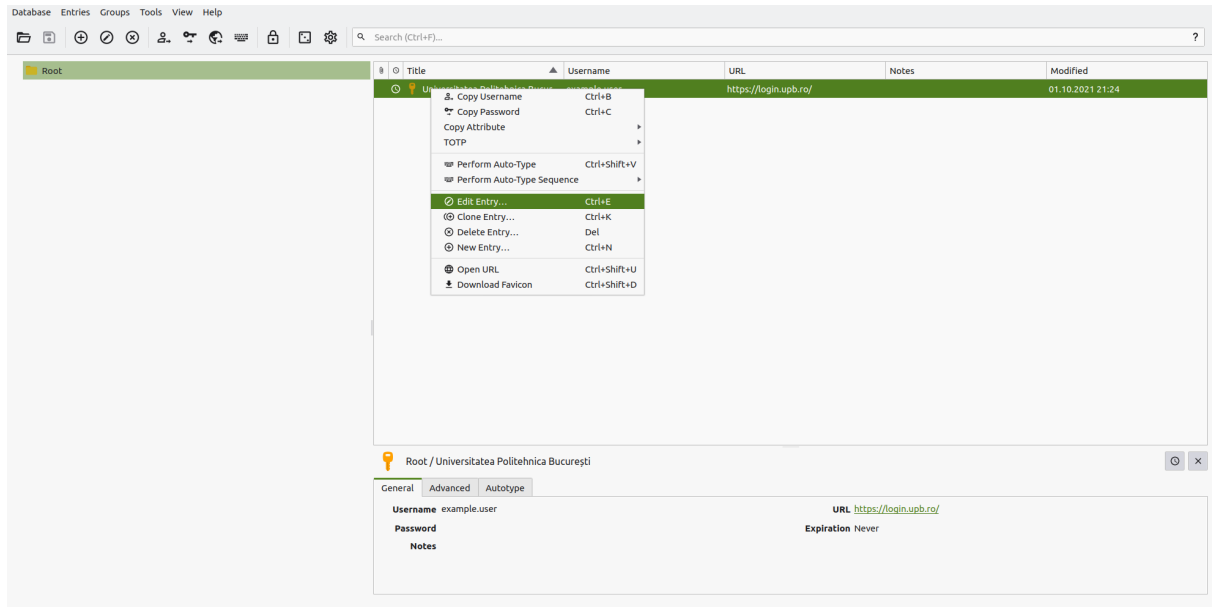
Submit

Utilizare global autotype (opțional)

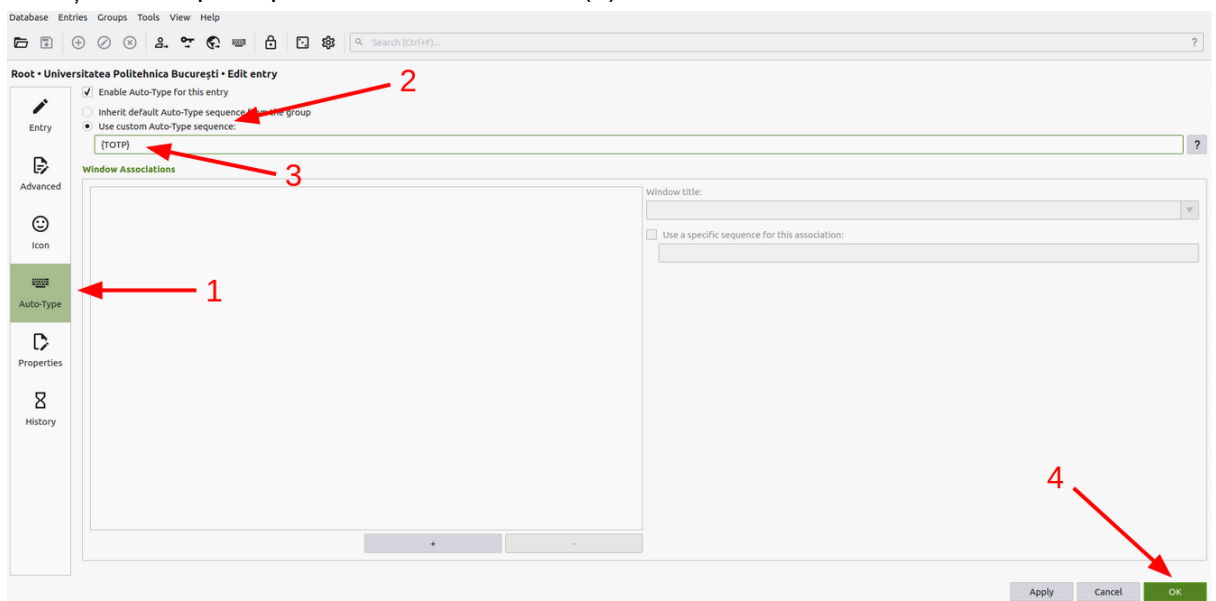
Pentru a face mai facilă introducerea codului de autentificare, poate fi utilizată o funcționalitate numită “Global Auto-Type”. Aceasta permite aplicației să înregistreze o combinație de taste (ex. “Ctrl+Shift+Alt+O”) pentru introducerea automată a codului.

Pentru configurare, urmați pașii următori:

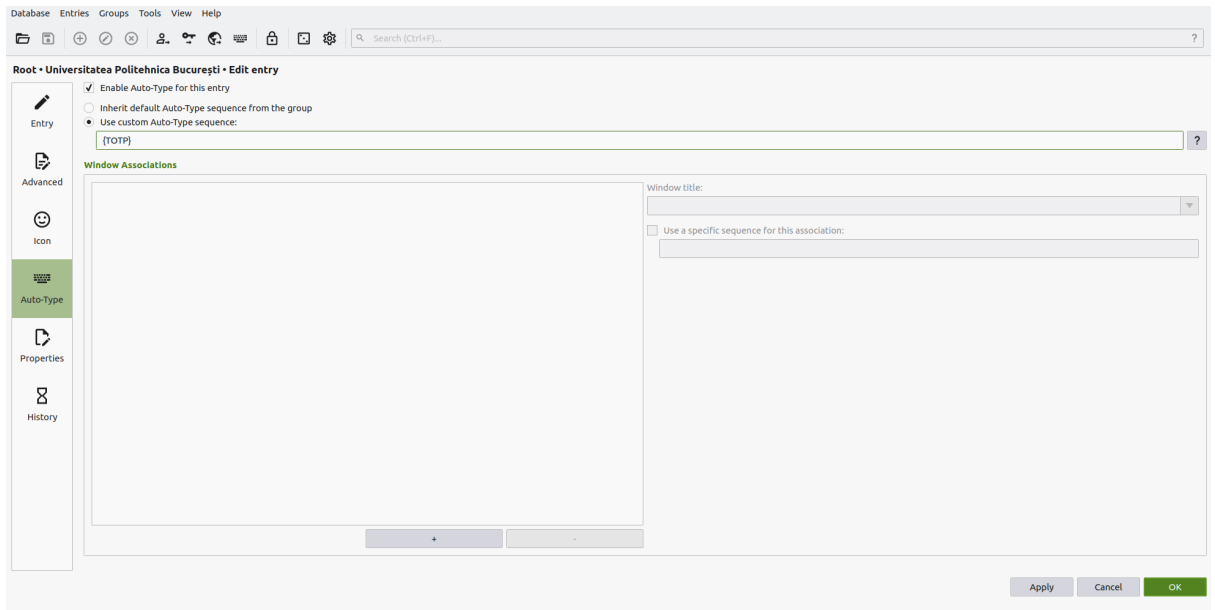
- Intrați în meniul de editare al intrării cu codul OTP prin apăsarea click dreapta pe linia cu intrarea și selectarea “Edit Entry...”. Alternativ, apăsați combinația de taste “Ctrl+E” după selectarea intrării.



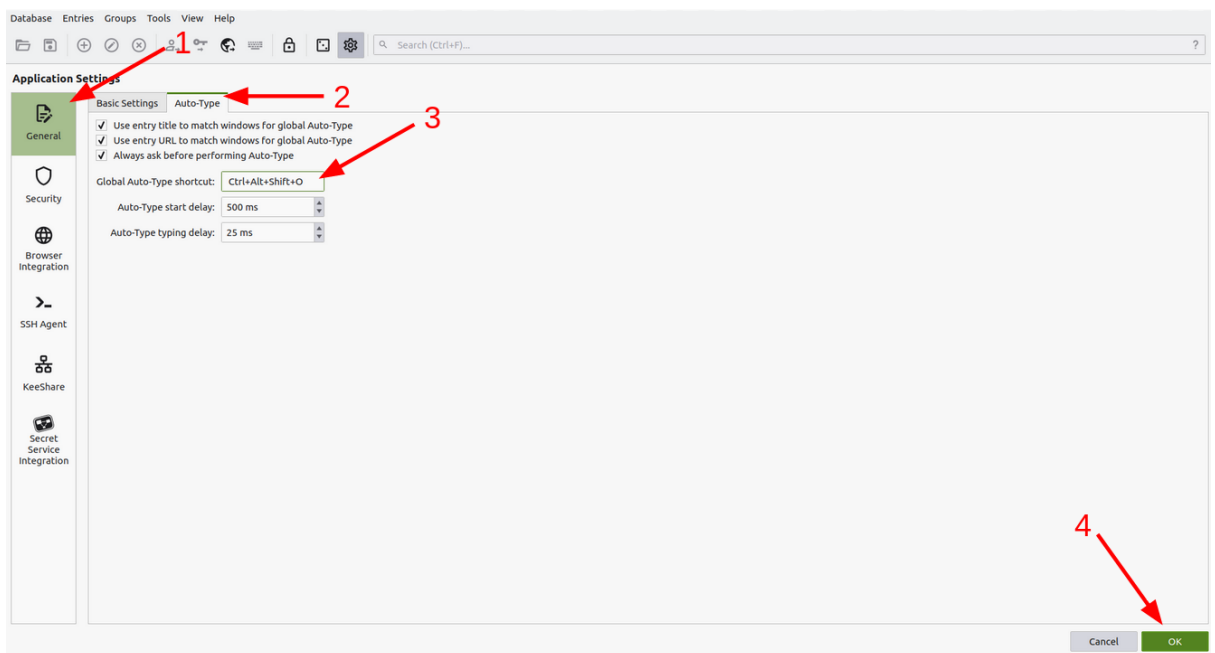
- Din meniul de configurare, în secțiunea “Auto-Type” (1), selectați “Use custom Auto-Type sequence” (2), iar în câmpul text introduceți textul “{TOTP}” (3). La final salvați setările prin apăsarea butonului “OK” (4).



- Din meniul “Tools” apăsați butonul “Settings”.



- Din secțiunea “General” (1), mergeți în tab-ul “Auto-Type” (2), apăsați pe zona “Global Auto-Type shortcut” (3) și introduceți o combinație de taste pe care să le apăsați pentru a realiza auto-type (apăsați tastele combinației - ex. țineți apăstate tastele “Ctrl”, “Alt” și “Shift”, iar apoi apăsați pe tasta “O”). La final salvați setările prin apăsarea butonului “OK” (4).



- Mergeți pe pagina de autentificare, ajungeti la secțiunea unde este cerut codul de autentificare și apăsați combinația de taste înregistrată. Dacă totul a fost configurat corect, ar trebui să apară o fereastră care vă permite să alegeți intrarea pentru care să realizeze auto-type. În cazul în care baza de date este blocată, prima dată o să fie cerută parola pentru deblocarea bazei de date.

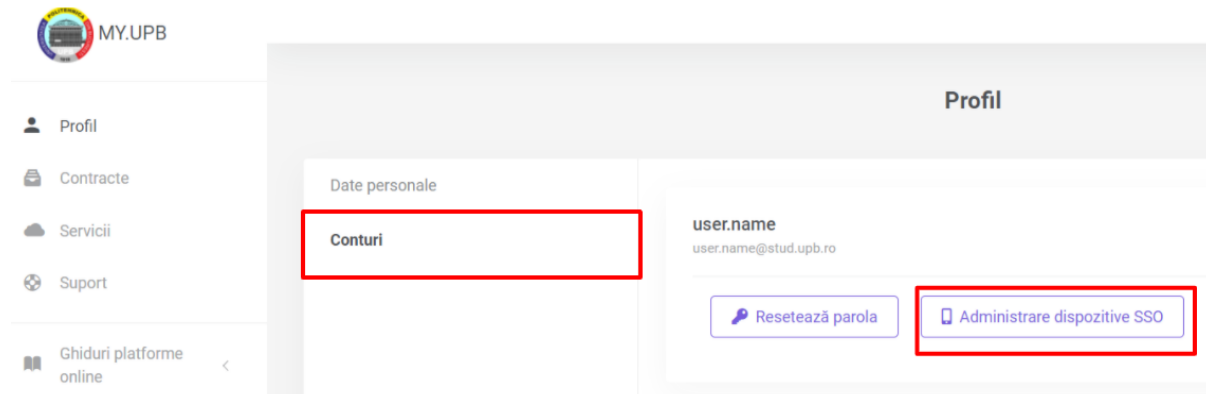
Observație: această funcționalitate caută ca titlul ferestrei în care realizează auto-type să conțină titlul intrării din baza de date - pagina de login, care are titlul “Log in to Universitatea Politehnica București” conține titlul intrării “Universitatea Politehnica București”.



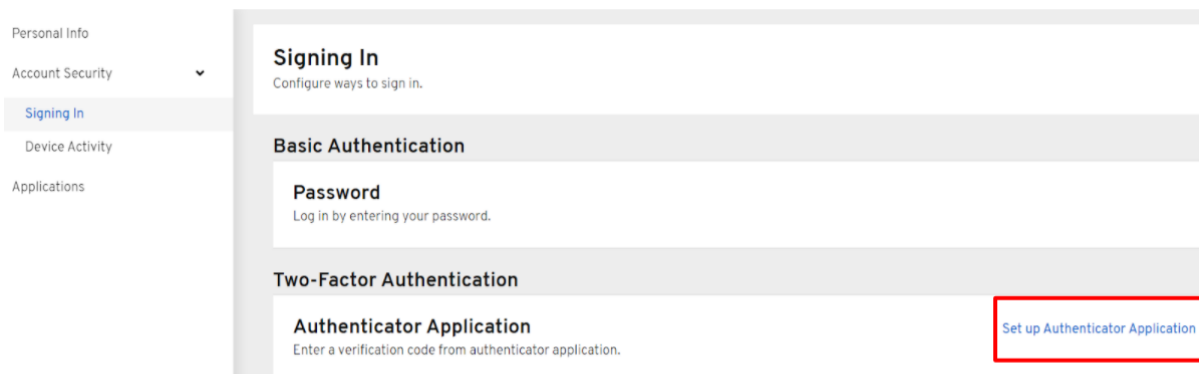
Întrebări frecvente

Cum adaug mai multe dispozitive de generare OTP?

Intrați în contul de administrare al dispozitivelor SSO



Apăsați "Set up Authenticator Application". Urmăriți pașii descriși în acest ghid.



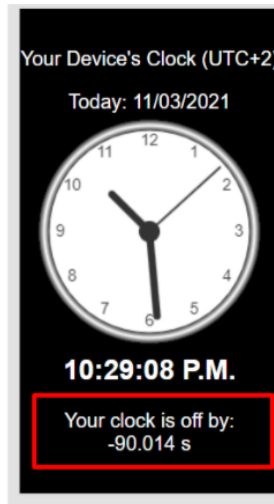
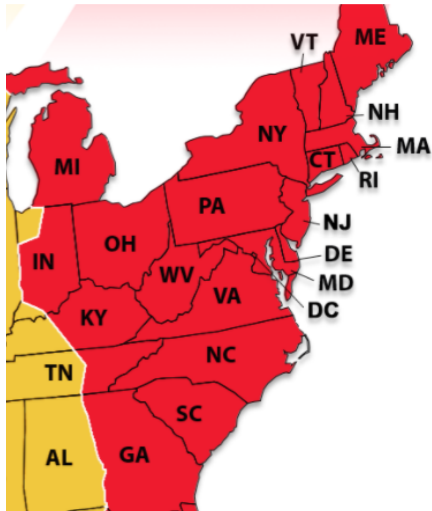
Vreau să schimb telefonul. Cum mut generatorul de coduri OTP?

Înainte de ștergerea codului și a aplicației de pe telefonul vechi, înregistrați un cod nou folosind pașii prezentați anterior.

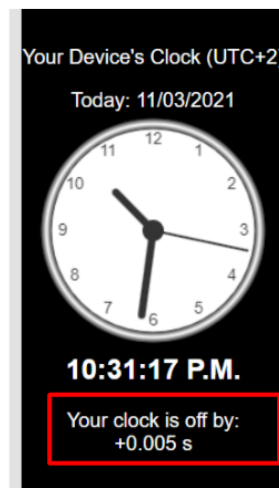
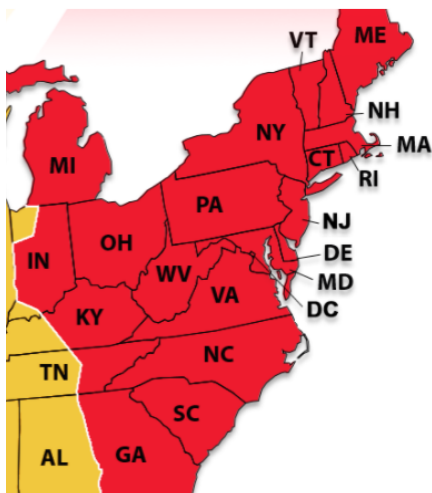
Când aveți acces folosind codurile de pe noul telefon, puteți șterge codul OTP de pe telefonul vechi, respectiv din consola de management a contului.

Primesc “cod invalid”. Ce fac?

Dacă nu ați făcut modificări asupra aplicației sau codului, verificați sincronizarea dispozitivului de generare accesând <https://nist.time.gov/>. Diferența de timp indicată de site trebuie să fie foarte mică (sub 2 secunde).



Sincronizați timpul dispozitivului.



Nu merge corect camera foto pentru scanarea codului QR. Ce fac?

Configurați codul OTP introducând manual codul secret conform indicațiilor din acest ghid.

Nu am telefon mobil. Ce fac?

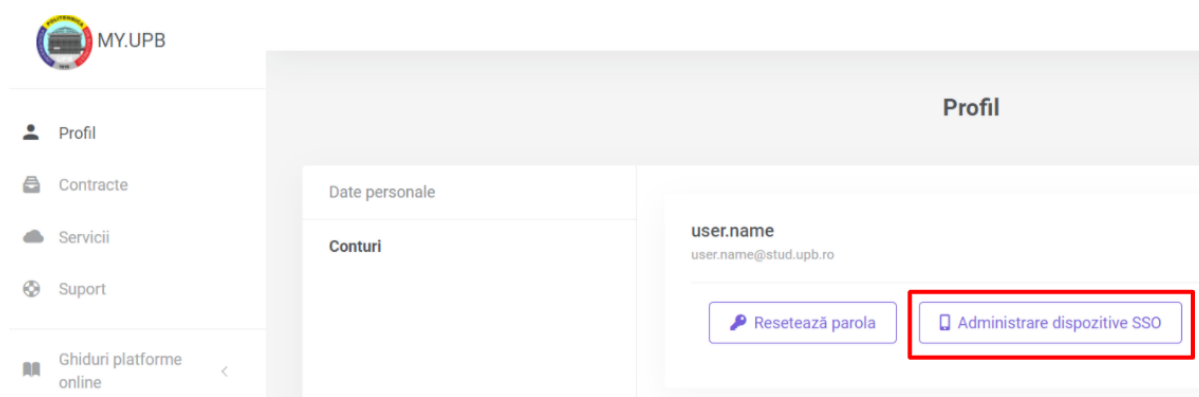
Folosiți aplicația desktop KeePassXC urmând pașii descriși în ghid.

Cum mă autentific în alt browser sau pe alt dispozitiv?

Introduceți numele de utilizator, parola și codul OTP.

Cum mă deloghez?

Intrați în consola contului folosind butonul din platforma myUPB.

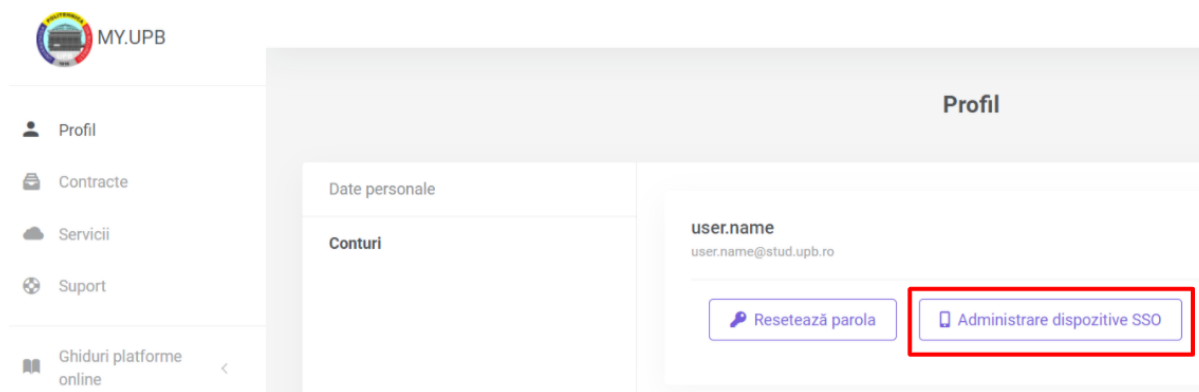


Apăsați butonul “Sign Out” din colțul dreapta sus al paginii.

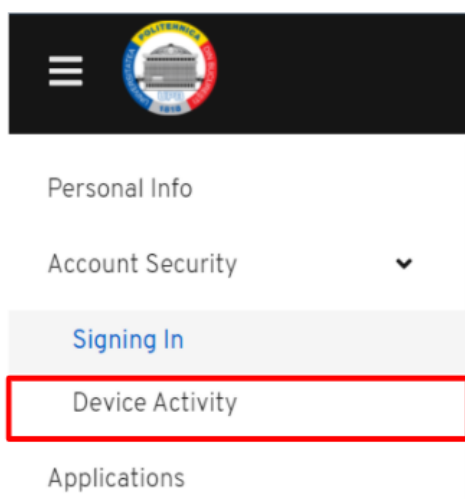


Cum mă deloghez de pe un anumit dispozitiv?

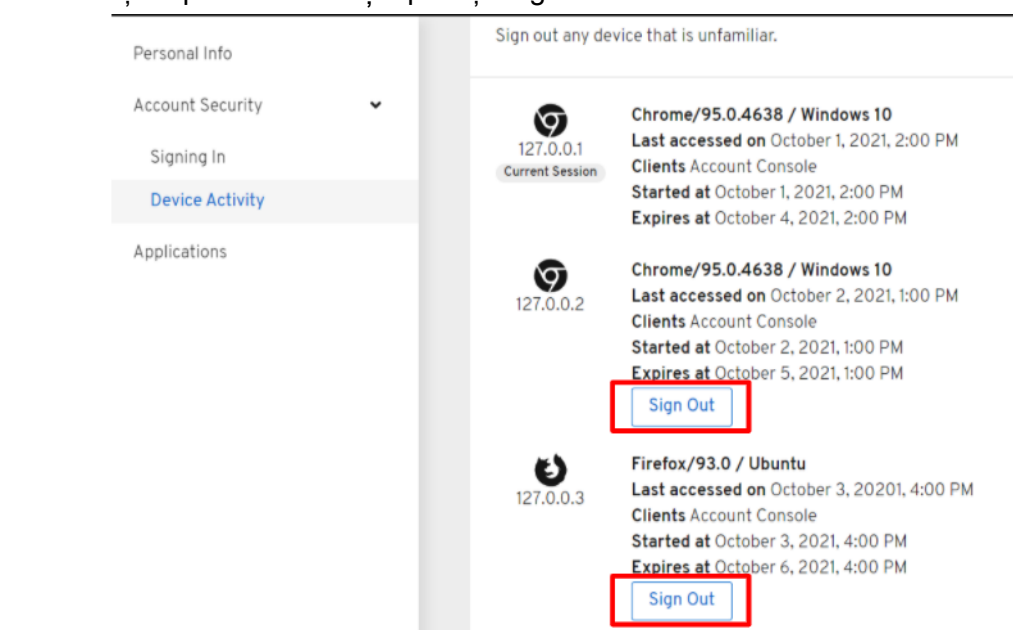
Intrați în consola contului folosind butonul din platforma myUPB.



Alegeți "Device Activity" din meniul afișat în partea stângă a paginii



Identificați dispozitivul dorit și apăsați "Sign out".



Sunt în imposibilitatea de a folosi dispozitivul vechi. Ce fac?

Pentru preîntâmpinarea acestor probleme, este recomandat să adăugați o configurație de rezervă pe un alt dispozitiv la care să aveți acces în cazul în care pierdeți accesul la dispozitivul curent.

Dacă nu aveți, deschideți tichet pe <https://support.upb.ro>.

Am șters aplicația/codul. Ce fac?

Nu ștergeți aplicația sau codurile. Dacă totuși se întâmplă, deschideți tichet pe <https://support.upb.ro>.

Alte probleme

Deschideți tichet pe site-ul <https://support.upb.ro>.