t-Risk
Método de Avaliação de Riscos

Two Factor Authentication for t-Risk Platform

Revisado em Julho/2021 A - EN

Why is it neccesary?

It makes your t-Risk account **more secure**. With the Two Factor Authentication your account will be protected by your password as well as by your cell phone.

Hacking your password is much easier than you believe.
Any of the following simple actions may put your account and passwords at risk:

- Using the same password in more that one website;
- Downloading software from the Internet;
- Clicking links sent by e-mail or other message Apps.

Two Factor Authentication provides a more secure process to keep hackers away even if they have your password.

Why do you need this?

Try to imagine what losing access to your account and its contents could mean.

A hacker that gets your password may block your access and:

- Access and even totally delete your projects, steal confidential information, pictures etc.;
- Act as if he/she were you and order tasks to your contacts through the 5W2H Plan;
- Use your credentials to set passwords, include or delete users or other non desirable actions in your corporate t-Risk account.

How does it work?

Accessing your account becomes slightly different

1

Enter your password

Enter your password as usual.

2

Further information is required

The secure code which is automatically generated by the *Google Authenticator App* on your cell phone must be entered as a second authentication factor.

How does this protect you?

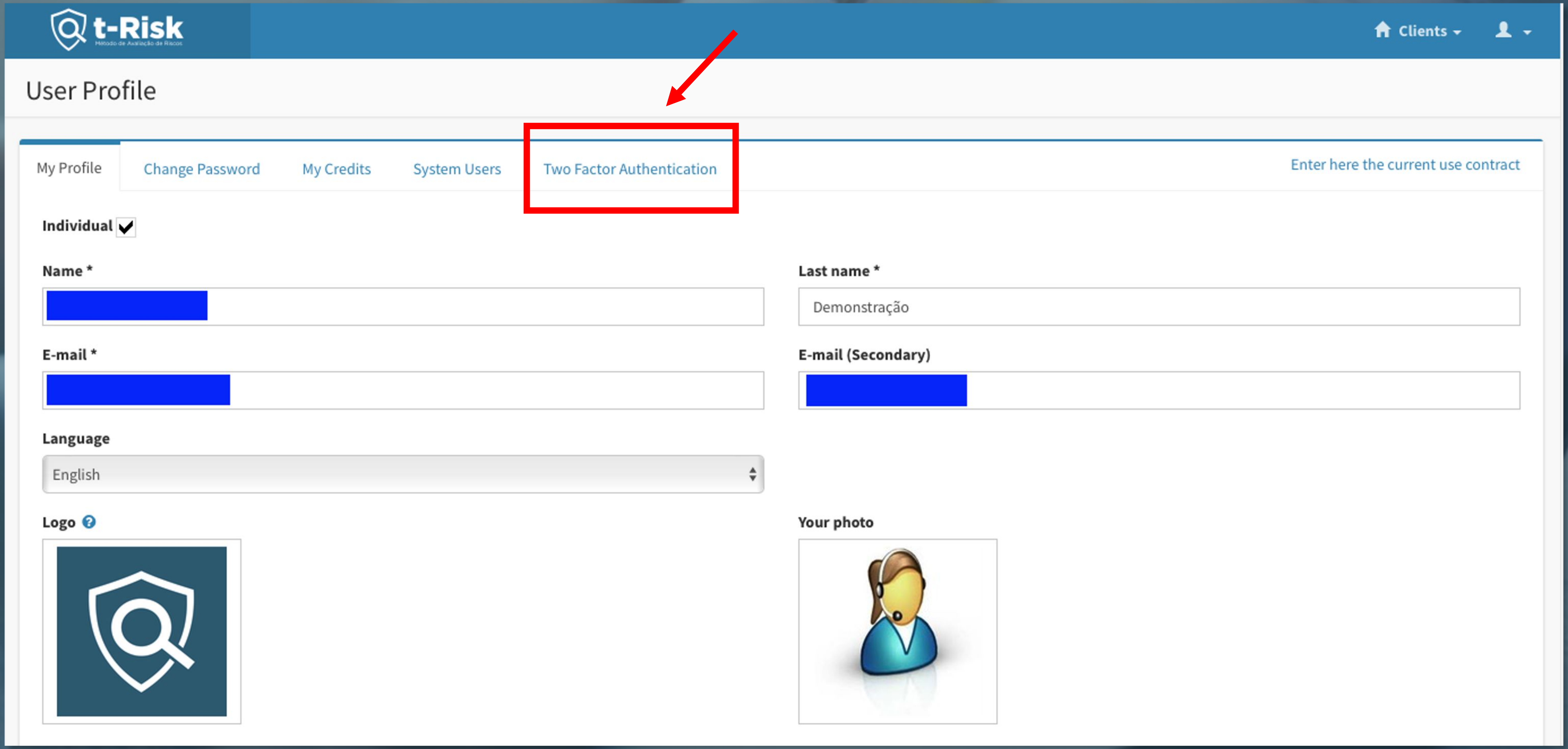
Higher security level. Most people have only one resource to protect their account, which is their password. With the Two Factor Authentication, anyone trying to hack your account will also need your cellphone with the *Google Authenticator App* to gain access.

To initiate the session, you will require something you know and something you have. With the Two Factor Authentication your account is protected with something you know (your password) and something you have (your cell phone with the *Google Authenticator App*).

What is this based on?

Authentication Codes created on demand only for you
Codes are created exclusively for your account, for single use only and only when needed.

Follow the next steps to enable the Two Factor Authentication on your t-Risk account.



User Profile

Enter here the current use contract

Individual ☑

Name * [redacted]

Last name * Demonstração

E-mail * [redacted]

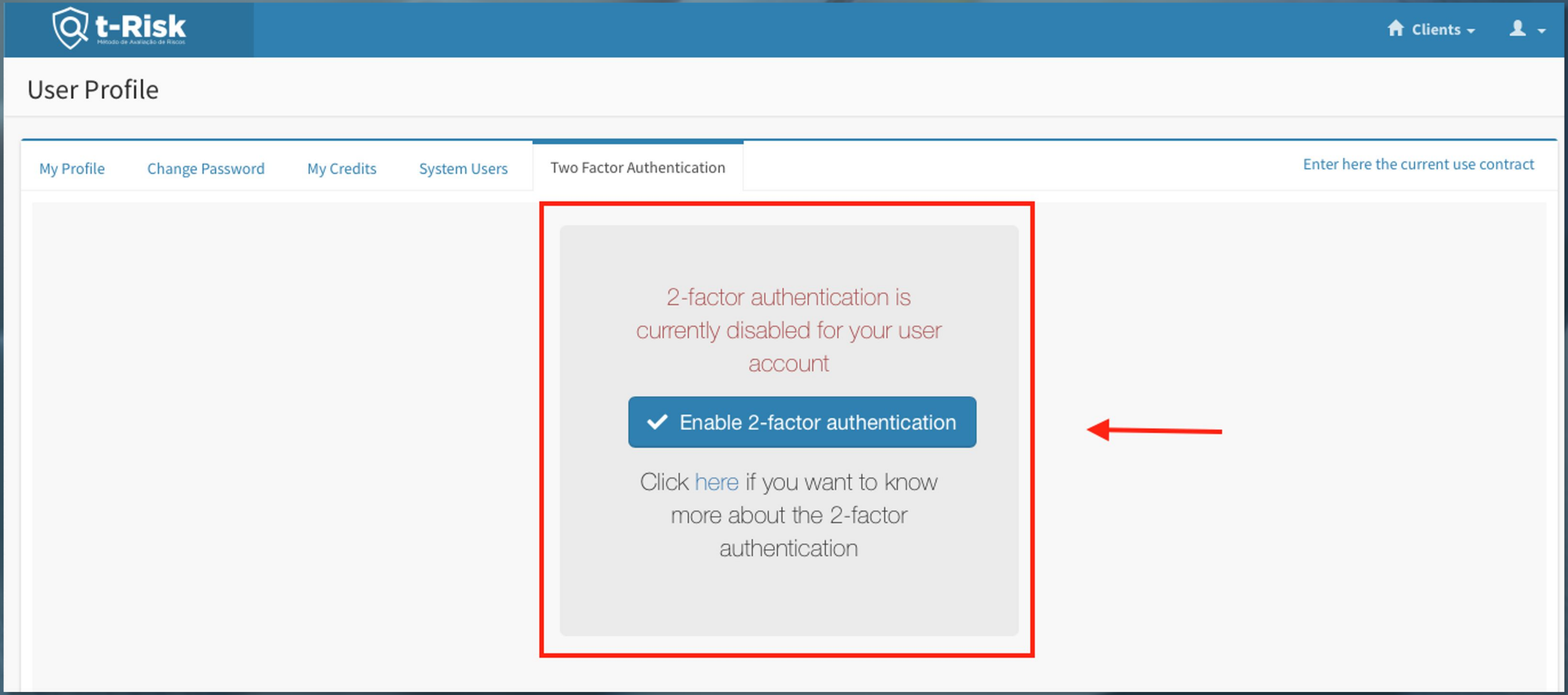
E-mail (Secondary) [redacted]

Language: English

Logo

Your photo

1 Access to your User’s profile and click the “Two Factor Authentication" tab.

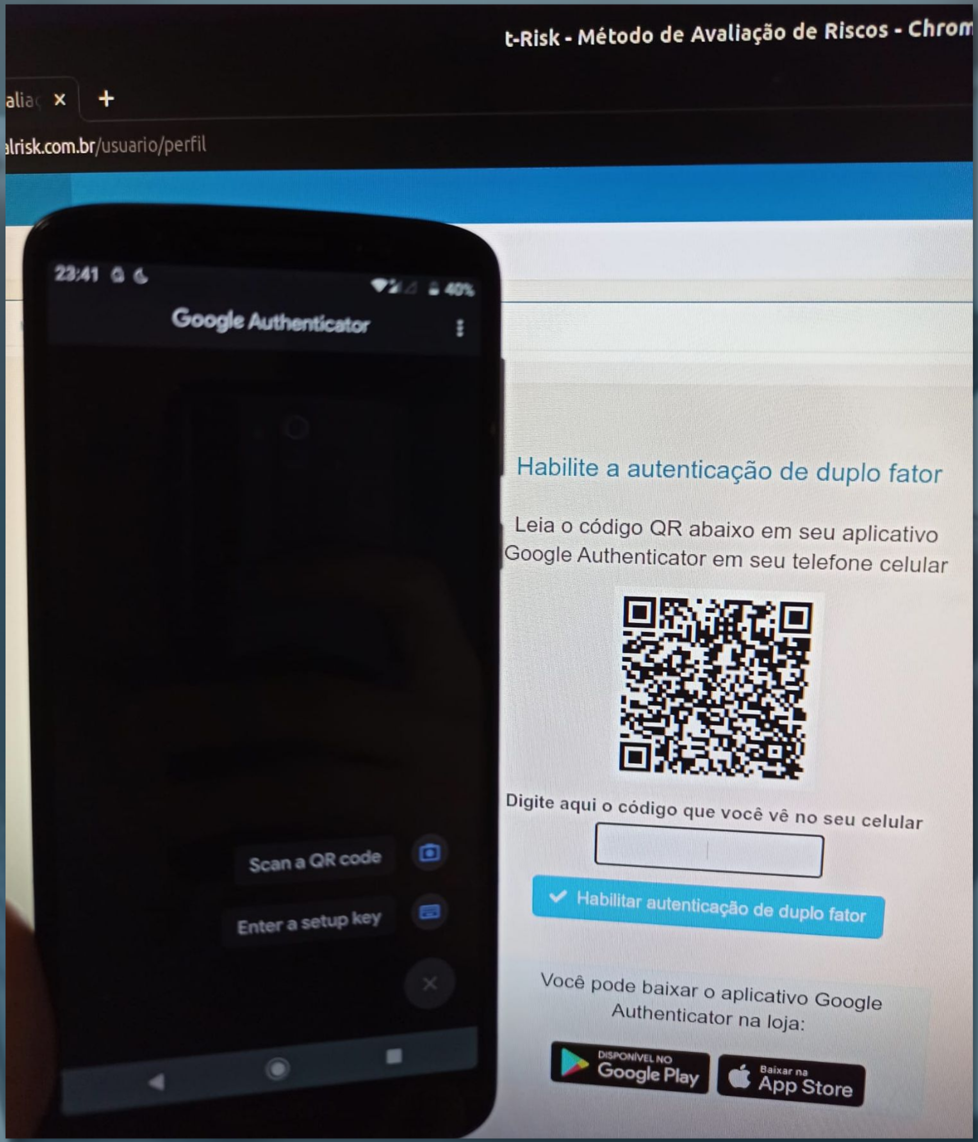

t-Risk
Clients
My Profile
Change Password
My Credits
System Users
Two Factor Authentication
Enter here the current use contract
Enable 2-factor authentication

User Profile

2-factor authentication is currently disabled for your user account

Click here if you want to know more about the 2-factor authentication

2 Click the “Enable Two Factor Authentication" button.



t-Risk - Método de Avaliação de Riscos - Chrom
aliac ×
alrisk.com.br/usuario/perfil
23:41
40%
Google Authenticator
Scan a QR code
Enter a setup key

Habilite a autenticação de duplo fator

Leia o código QR abaixo em seu aplicativo Google Authenticator em seu telefone celular

Digite aqui o código que você vê no seu celular

✓ Habilitar autenticação de duplo fator

Você pode baixar o aplicativo Google Authenticator na loja:

DISPONÍVEL NO Google Play
Baixar na App Store

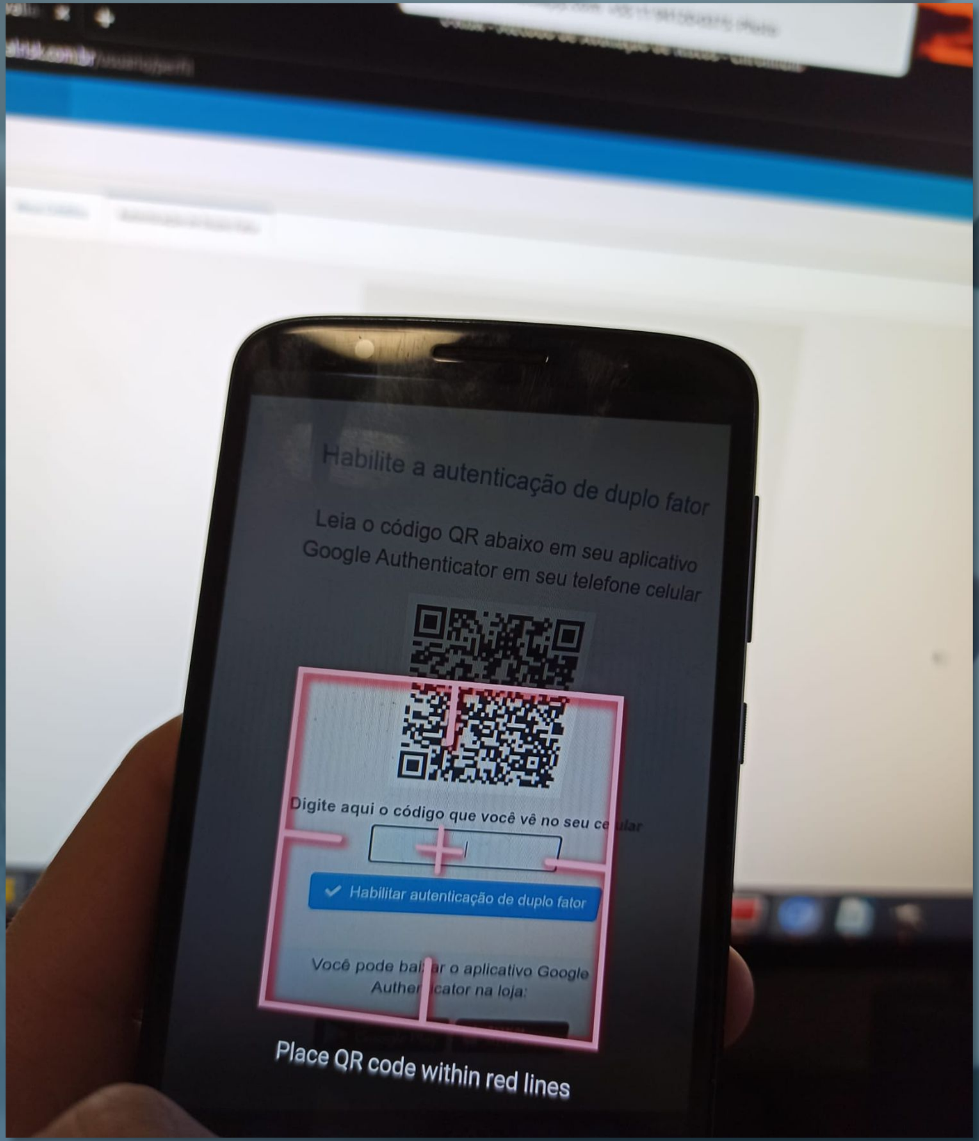
3

Access the *Google Authenticator* App on your cell phone. If it’s not yet installed, please follow the links below to download it.

No mobile internet signal? No problem. The *Google Authenticator App for* Android, iPhone o BlackBerry may create codes even when your device is offline.

Link to Apple Store
https://apps.apple.com/br/app/google-authenticator/id388497605

Link to Google Play
https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2



Habilite a autenticação de duplo fator

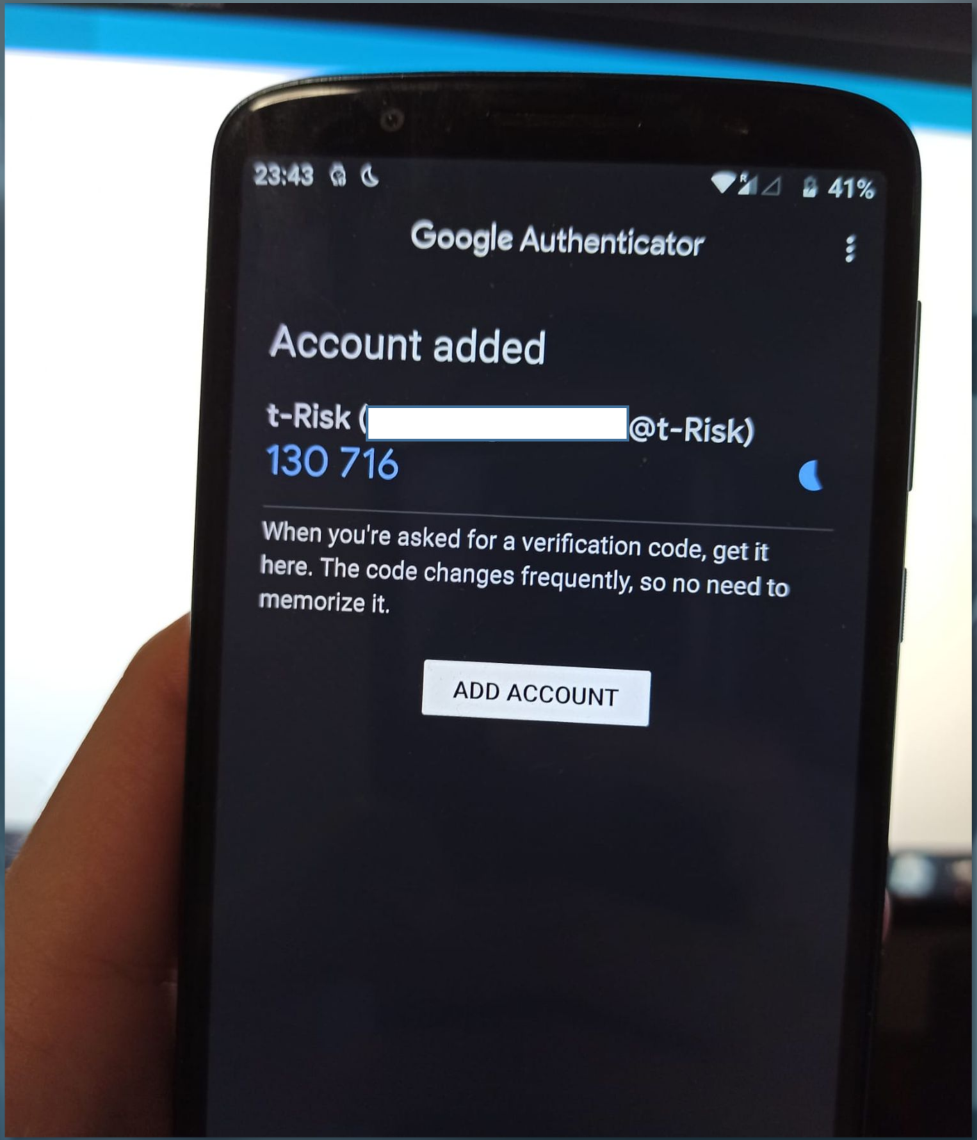
Leia o código QR abaixo em seu aplicativo Google Authenticator em seu telefone celular

Digite aqui o código que você vê no seu celular

Você pode baixar o aplicativo Google Authenticator na loja:

✓ Habilitar autenticação de duplo fator
Place QR code within red lines

4 Then you will have to scan the image displayed in the App.



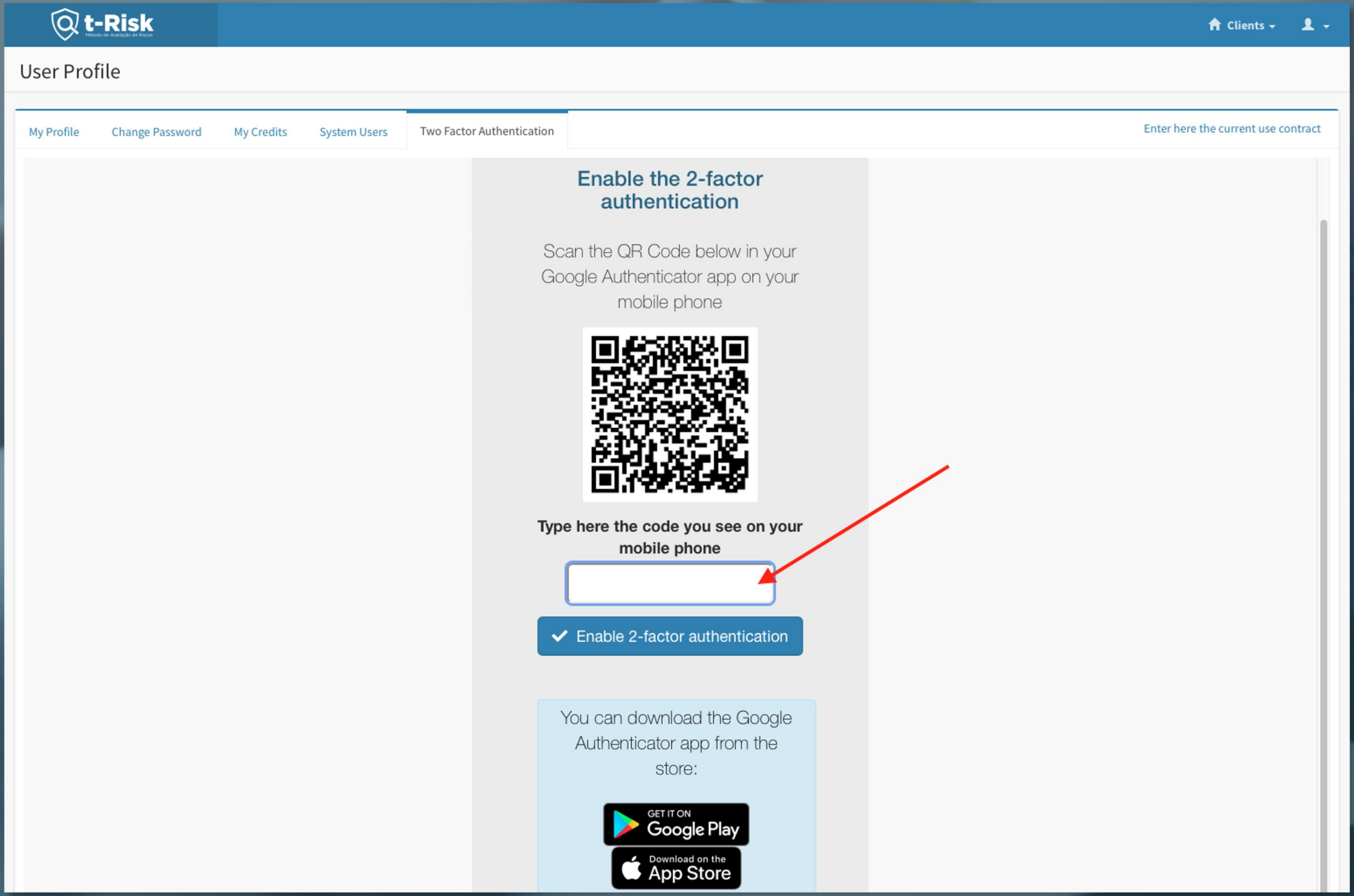
Account added

t-Risk ([redacted]@t-Risk)
130 716

When you're asked for a verification code, get it here. The code changes frequently, so no need to memorize it.

5

Once you scan the image, you will see that your account has been registered in the App and a validation code is already available.


t-Risk
Clients
User Profile
My Profile
Change Password
My Credits
System Users
Two Factor Authentication
Enter here the current use contract
Enable 2-factor authentication
GET IT ON Google Play
Download on the App Store

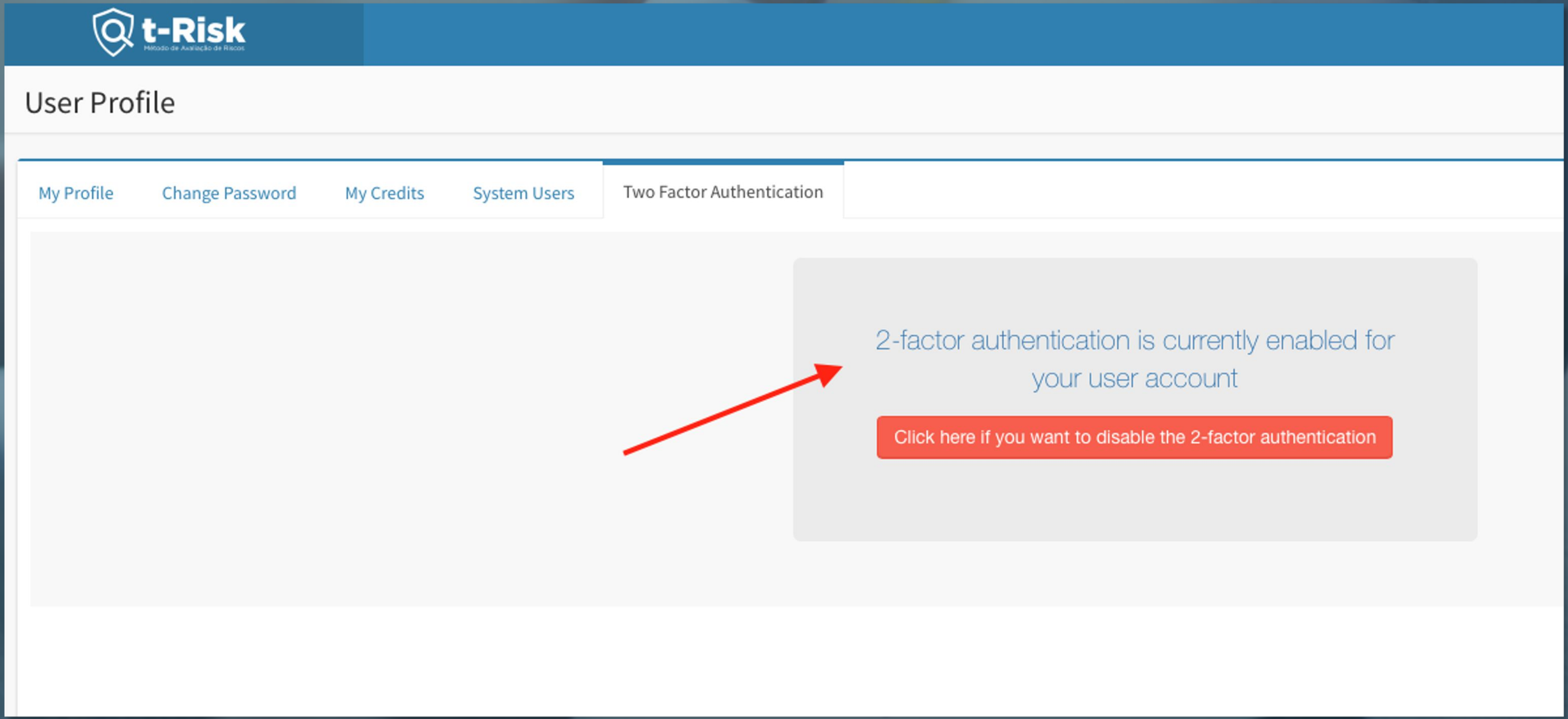
Enable the 2-factor authentication

Scan the QR Code below in your Google Authenticator app on your mobile phone

Type here the code you see on your mobile phone

You can download the Google Authenticator app from the store:

6 Insert the code displayed by *Google Authenticator App* in this field and click the “enable Two Factor Authentication" button.

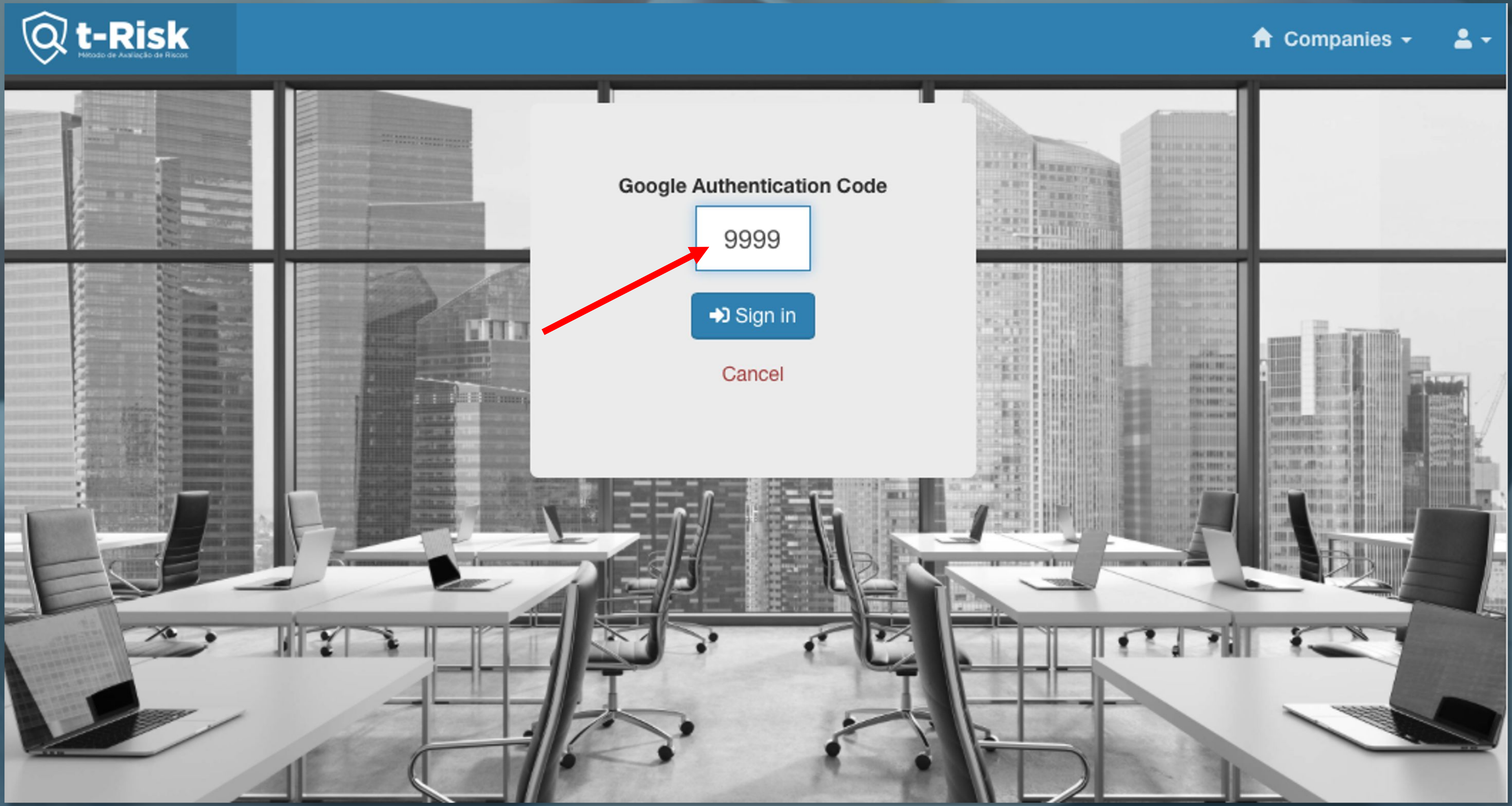


User Profile

2-factor authentication is currently enabled for your user account

Click here if you want to disable the 2-factor authentication

7 You will see this text confirming that Two Factor Authentication has been enabled.



Google Authentication Code

9999

8 From your next access, after inputting your user's name and password, t-Risk will request you to input the *Google Authenticator* code to grant access to the platform.

t-Risk

Método de Avaliação de Riscos

Practitioner
t-Risk
Expert
Practitioner
t-Risk
Expert
Practitioner
t-Risk
Expert

t-Risk Practitioner Badge

Include the t-Risk badge to your Job record and share it!

Contact us for further information!