

Two-factor authentication

Computerome 2.0 requires two-factor authentication for access:

- User name is sent to you in email.
- For first factor authentication, use the temporary password sent to you in SMS. Change it at first login using **passwd** command.
- For second factor authentication, use:
 - Either the passcode sent to you in SMS (the default option)
 - Or install the Entrust IdentityGuard soft token on your mobile.

In Computerome 2.0, no other software token is available for second factor authentication, than Entrust Identity app.

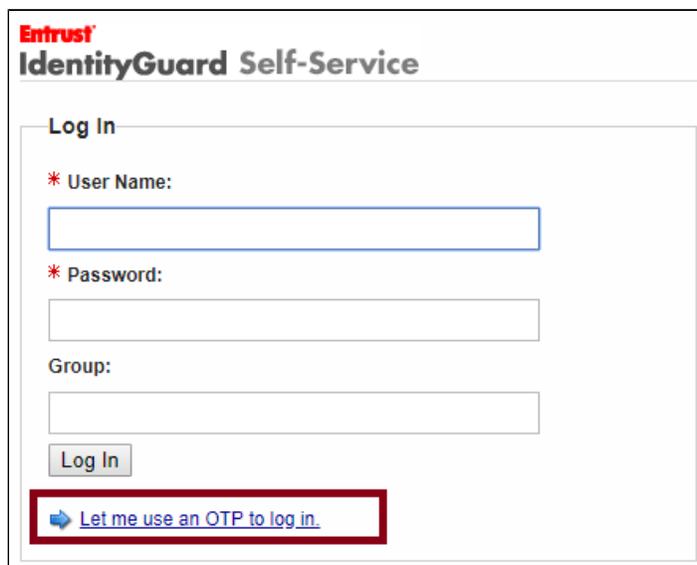
Setting up the Entrust Identity soft token

On your mobile phone:

1. Open Google Play or Apple App Store, and install the **Entrust Identity** app.

On your computer:

2. Open a web browser and go to: <https://ssm.computerome.dk/IdentityGuardSelfService/authenticate/firstFactorAuthentication>
3. Click on the "Let me use an OTP to log in" link in the bottom line.



It takes app. 10 minutes for the script to enable OTP after user activation. In case you get the below error message 10 minutes after you received the welcome mail, contact computerome@dtu.dk.

 The user you specified is not eligible for one-time password (OTP) login.

4. Type your personal Computerome 2.0 user name (sent to you in mail) into the User Name field. Press OK.

Entrust
IdentityGuard Self-Service

OTP Login

* **User Name:**

Group:

5. Click OK to the OTP (one-time password). This will send a code to your mobile phone in SMS.

Entrust
IdentityGuard Self-Service

OTP Login

Challenge

A one-time password (OTP) will be delivered to your Phone.

6. Type the code received in SMS into the field. Press OK.

Entrust
IdentityGuard Self-Service

A request to deliver an OTP to the location you specified has been made.

OTP Login

Challenge

Please enter the one-time password (OTP) delivered to your requested location:

7. Press Yes in the next panel, as you already installed **Entrust Identity** application on your mobile phone in the very first step.



IdentityGuard Self-Service

Soft Token

You have been selected to use a soft token for second-factor authentication.

Have you downloaded and installed the Entrust IdentityGuard Mobile ST application onto your mobile device, or the Entrust IdentityGuard Desktop Soft Token application onto your computer?

Not sure what to do?

Answer **Yes** if you've successfully downloaded and installed the Entrust IdentityGuard Mobile ST or Desktop Soft Token application. After answering Yes, you will be prompted to set up a soft token.

Answer **No** if:

- You have **not** downloaded and installed the Entrust IdentityGuard Mobile ST or Desktop Soft Token application yet.
- You don't have a mobile device or computer that can support the application.
- Your attempts to download and install the Entrust IdentityGuard Mobile ST or Desktop Soft Token application have repeatedly failed.
- You are unclear about what to do.

8. Select option 3 in the next panel saying, "I want to activate a soft token identity on a mobile device that may not be connected to the internet". Press Next. The QR code will pop up in the browser.



IdentityGuard Self-Service

Entrust IdentityGuard Mobile ST or Desktop Soft Token Activation Options

Please select the option that best matches your current situation:

1. I want to activate a soft token identity on my current device.
2. I want to activate a soft token identity on another device where I can have an email message delivered.
3. I want to activate a soft token identity on a mobile device that may not be connected to the Internet.
4. I am unable to activate my soft token identity using any of the above methods, so I'll perform a manual activation.
5. I want to delay activating my soft token identity until later.

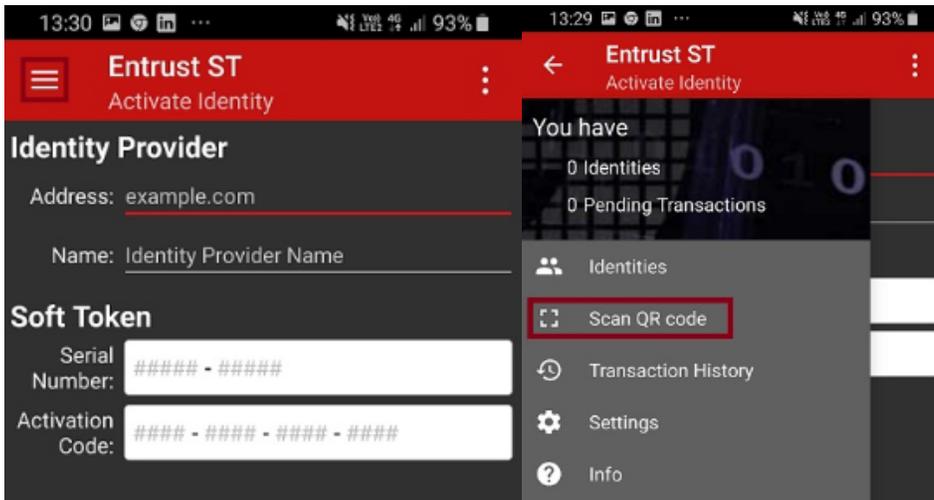
Option 3

The mobile device where I want to activate my soft token identity has Entrust IdentityGuard Mobile ST version 3 or above installed. You can tell which version of the app is installed by opening it and going to the About section of the main Info screen.

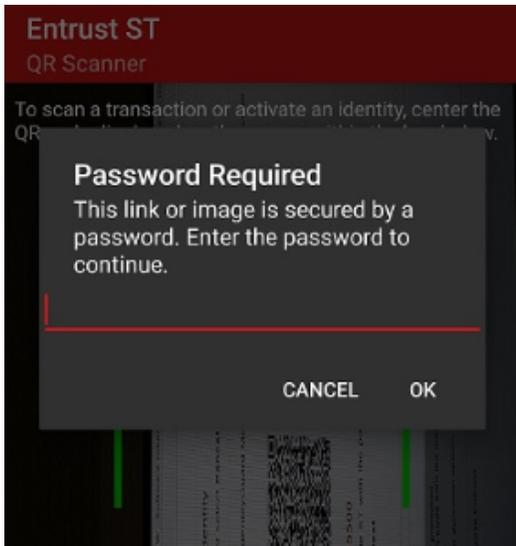
On your mobile phone:

9. Open the **Entrust Identity** app on your mobile phone.

10. In the top left corner open the menu and select Scan QR Code menu item. This will activate the camera on your phone.

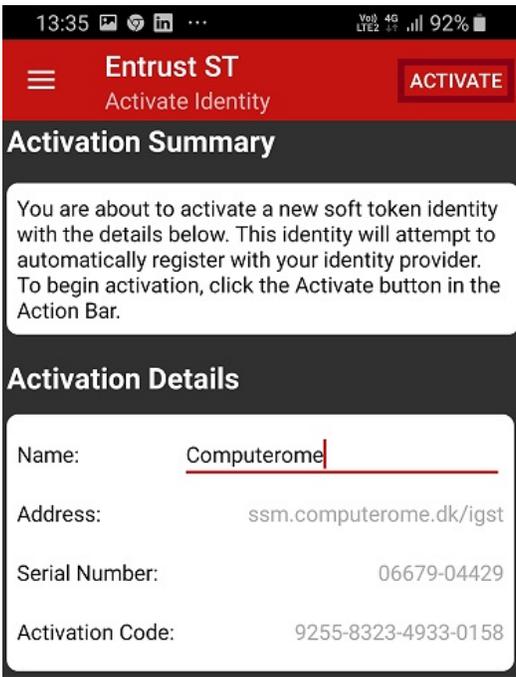


11. Use the camera to scan the QR code displayed in the web browser on your computer. When the mobile app reads to QR code, a field for the password pops up.

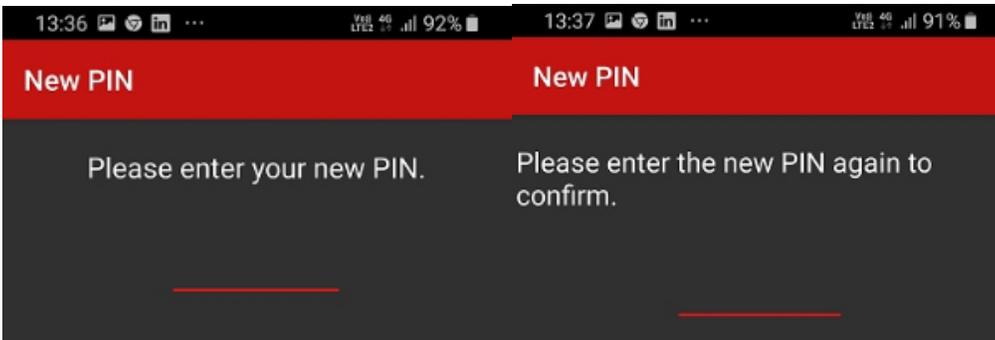


12. Enter the code in red letters displayed below the QR code in the web browser on your computer. Press OK.

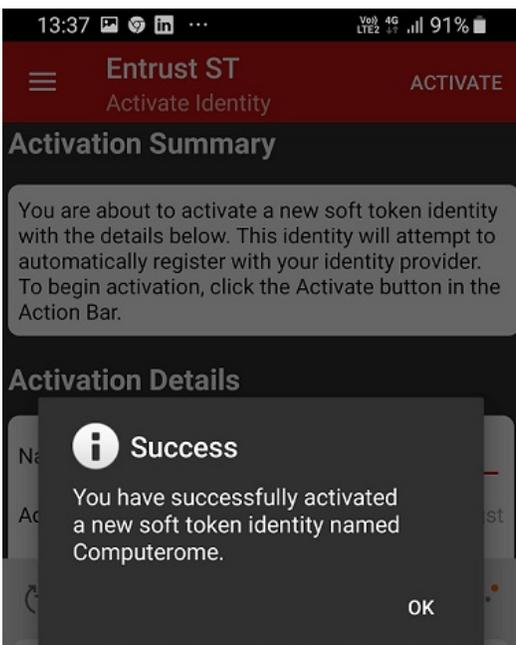
13. The Activation Summary shows up in your app. Press Activate in the upper right corner.



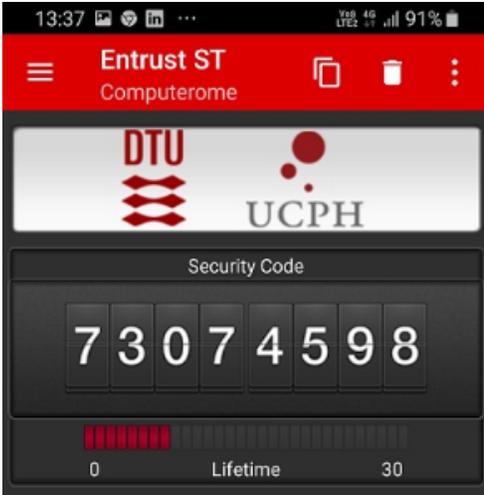
14. Create the four digit PIN for accessing the **Entrust Identity** app on your mobile in the future.



15. You have successfully activated the soft token on your mobile phone.



16. The generated security code for the second factor authentication is shown in the mobile app.



On your computer:

17. Press Next in the browser. The below message is expected to be displayed in the browser.

Entrust
IdentityGuard Self-Service

✔ Your soft token has been activated.

Additional Authentication Types

Soft Token

You have successfully activated the soft token with serial number 06679-04429. You can start using this soft token for second-factor authentication right away!

Next

18. Press Next, then Done in the browser. The soft token has been successfully activated. You may close the browser.

Entrust
IdentityGuard Self-Service

✔ You've successfully completed your registration with Entrust IdentityGuard Self-Service!

Self-Administration Actions

Please select one of the actions below or click Done if you're finished:

- [I'd like to recreate my soft token since I deleted its Identity from my device.](#)
- [I'd like to reinstall the Entrust IdentityGuard Mobile ST or Desktop Soft Token application on my current device or a new device.](#)

Done