SonarLogin User Guide

Version:	1.1
Creation date:	19/08/2021
Last update:	23/12/2021

Table of Contents

1. About SonarLogin

SonarLogin allows the user to authenticate on Windows without having to manually enter the login and password. By using ultrasounds, the user is able to send this information from the mobile application, and the "SonarLogin Credential Provider" installed on Windows will receive them and will automatically authenticate the user.

Sonarlogin can also have another operation mode, which allows you to use your phone as a second factor for the authentication.

The communication between the PC and the mobile devices is based on CopSonic universal system to exchange secure data by ultrasounds. Compatibility with 100% of devices is guaranteed because only microphones and speakers are necessary.

2. Environment

2.1 Overview

2.1.1 Software

The SonarLogin demo environment is composed out of:

- The mobile application, available for Android and iOS, which is used to send the credentials to the computer, using the ultrasounds.
- The Windows package containing the Windows Credential Provider and the manager application.

2.1.2 Compatibility

The compatible Operating System versions for the applications are:

Operating system	Android	iOS	Windows
Requirements	7.0+	11.0+	Windows 7 or above (64-bit) .NET Framework v4.7

2.2 Installing the demo applications

2.2.1 Mobile app installation

The mobile applications can be downloaded and installed using the following links:

- Android :
  http://apps.copsonic.com/ApplicationDetails.aspx?ApplicationId=339

- iOS :
  http://apps.copsonic.com/ApplicationDetails.aspx?ApplicationId=332

  In the case of iOS, because this application it's a custom enterprise app you need to manually trust the certificate, you can find here more information about how to do it:

  https://support.apple.com/en-us/HT204460

2.2.2 Windows components installation

The Windows installer can be download from:

https://sonarlogin.copsonic.com/app/SonarLoginInstaller.msi

3. Testing SonarLogin

3.1 SonarLogin operation modes

3.1.1 Automatic Login

When SonarLogin is configured in Automatic Login mode, once the mobile application is open, it will emit automatically an encrypted ultrasound with the username and password information (previously saved in the application), which will be received in the PC to log in to the session that corresponds to the provided credentials.

Any session in the PC can be accessed this way by simply entering the corresponding credentials in the mobile device, without any previous paring between the PC and mobile.

3.1.2 Two-factor Authentication (2FA)

If SonarLogin is configured in Two-factor Authentication (2FA) mode, once the application is open, it will emit automatically an encrypted ultrasound with the previously configured 2FA code which will be received in the PC.

When the Two-factor Authentication is configured for a user, it is not possible for him to work on the computer without having the phone to prove their presence because the computer must detect the ultrasonic 2FA code emitted by the mobile application, otherwise the windows session will be locked.

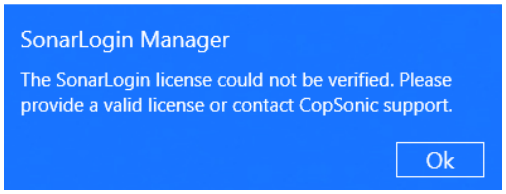
The detection of the 2FA code should be done on the login screen, but in case it has not been detected in the login screen, the user will be able to log in but must detect the code during the first 15 seconds once within the windows session. If it is not detected in these 15 seconds, the windows session will be locked and the next time the user must absolutely detect the code on the login screen.

3.2 Manager Configuration

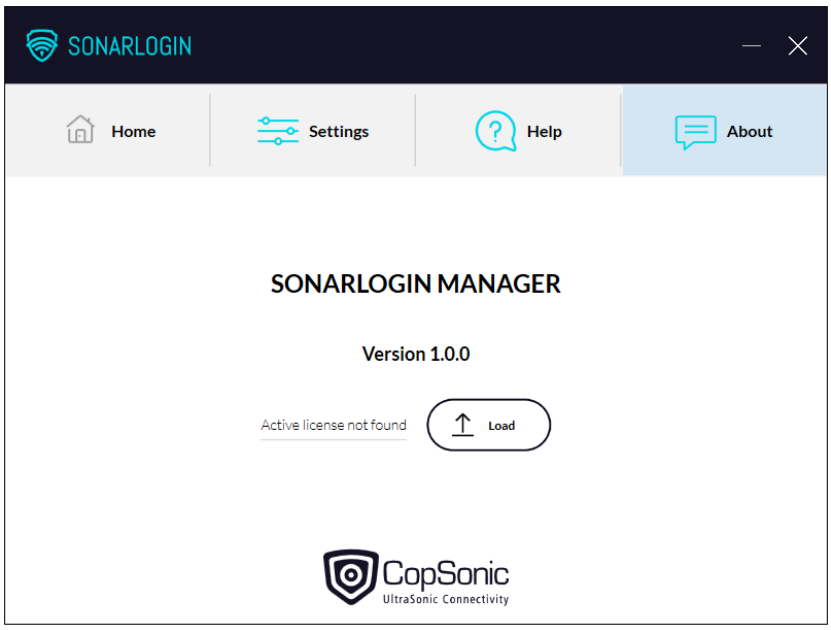
3.2.1 License

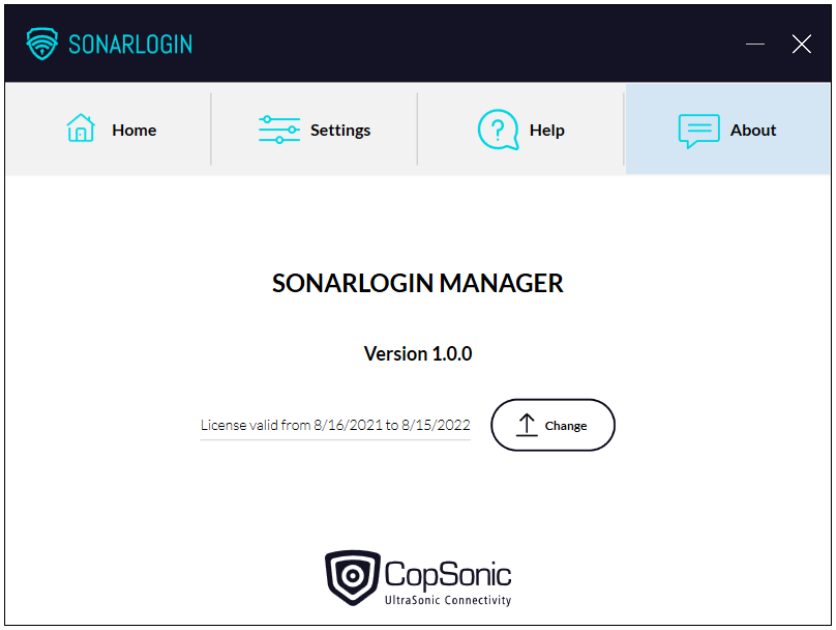
Once the windows application is installed, the first step must be upload the license:

Run the manager app, the following notification will appear:



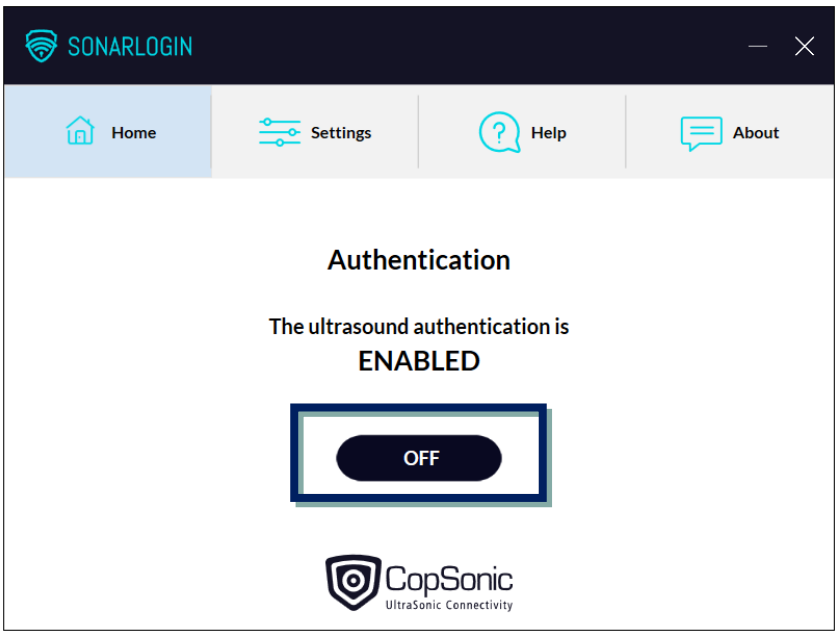
Click on the «Load» button to upload the license file provided by CopSonic:



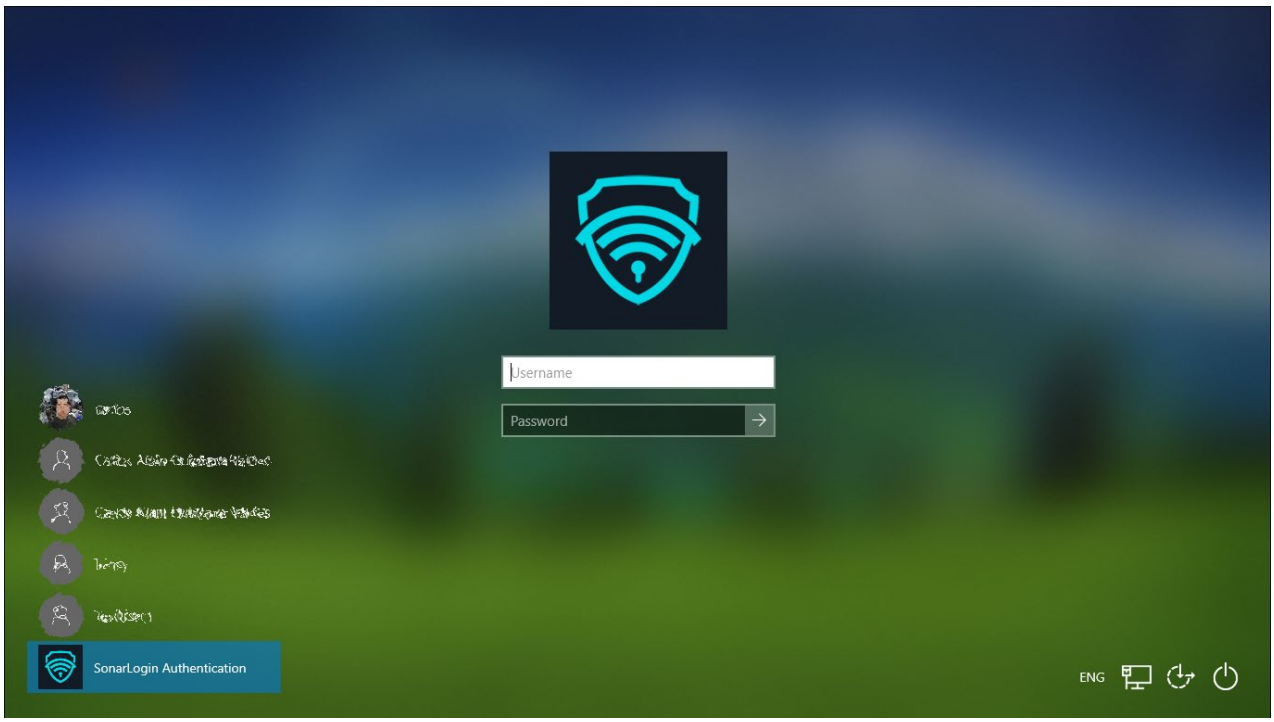


3.2.2 Activate or deactivate the ultrasound authentication

By default, the Credential Provider is activated. You can activate it or deactivate it by clicking on the ON/OFF button:

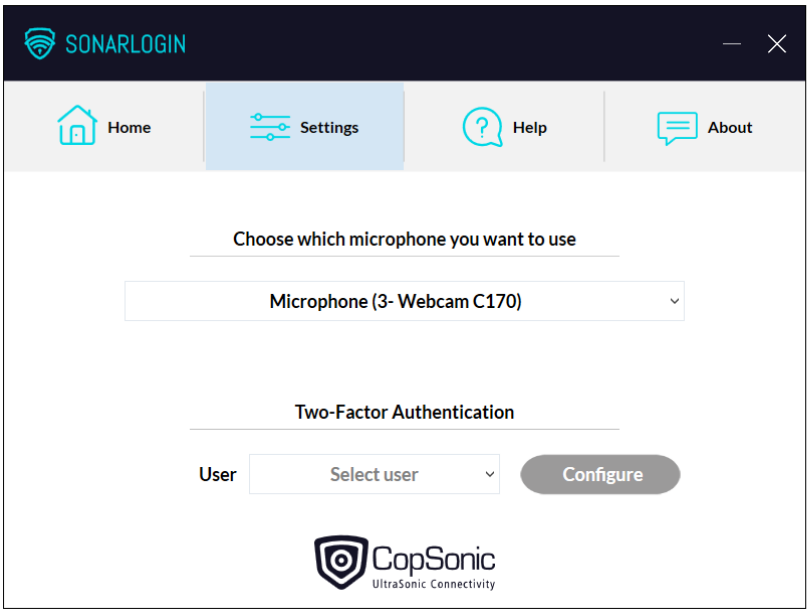


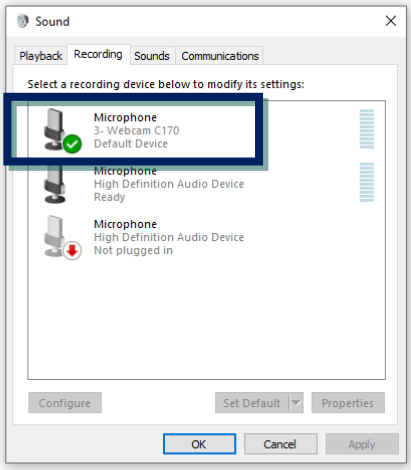
When the ultrasound authentication is activated, you will see the SonarLogin Credential Provider on the Windows login screen:



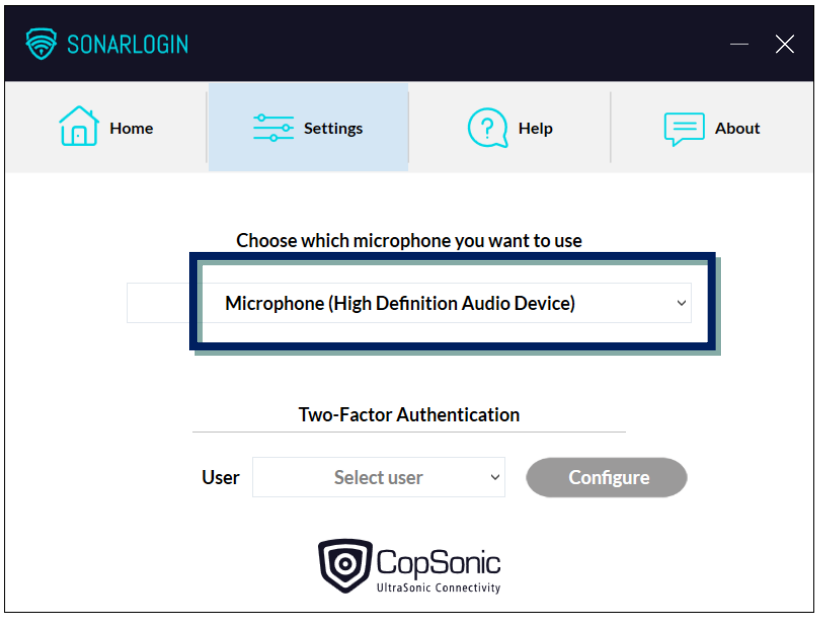
3.2.3 Select the recording device

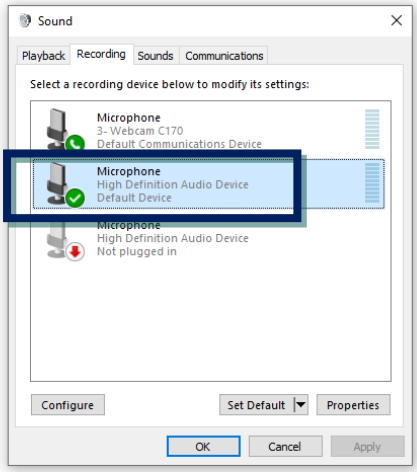
When the application is opened for the first time, the manager will configure the credential provider to use the default recording device selected in the system.





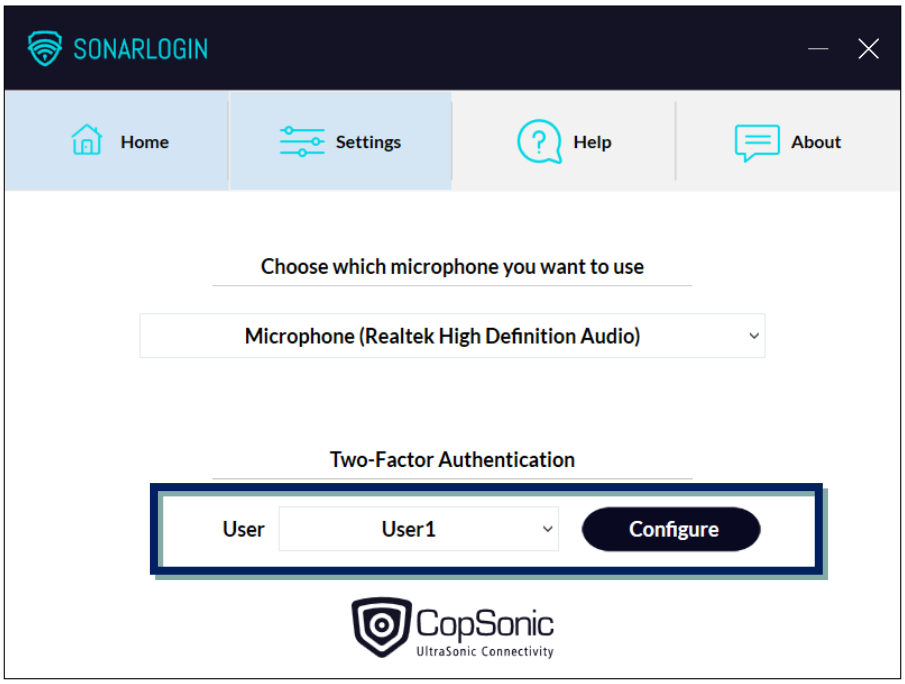
In the «Settings» screen the user can change the recording device that will be used in the Windows login screen to record the ultrasound emitted by the application.



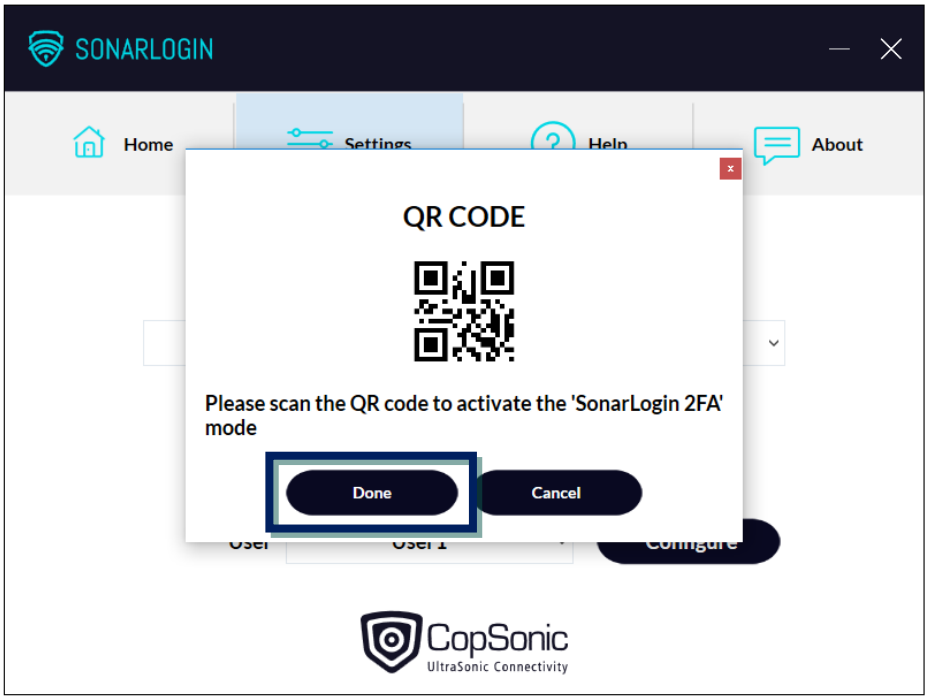


3.2.4 Two-Factor Authentication Configuration

Select the user for whom you want to configure the Two-Factor Authentication mode and click on “Configure”:



Scan the QR Code with the SonarLogin mobile application (see 3.3.3) and once correctly scanned click on “Done”:

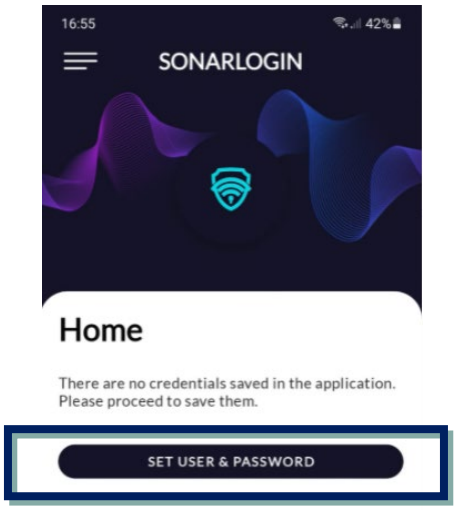


Note that there must be always 1 user left on the computer without 2FA for security reasons.

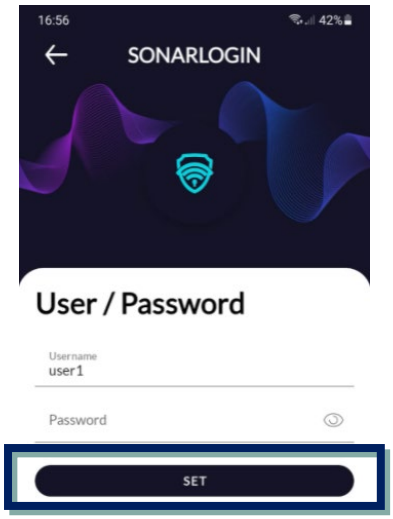
3.3 Mobile Application

3.3.1 User credentials

When the user opens the application for the first time, it is required to set the credentials that will be sent to the PC.



Click on the « SET USER & PASSWORD » button to go directly to the «Credentials» configuration screen:



At any time, the user can change the credentials using the application settings.

3.3.2 Adjust broadcast volume

In the android device you can adjust the speaker volume using this control:

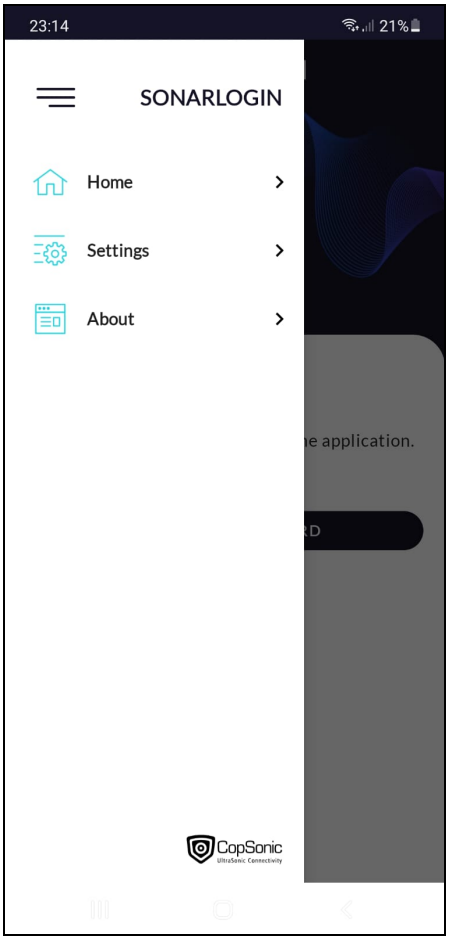
In the iOS device the volume cannot be changed directly using this control, you need to use the device's volume buttons instead, but it will allow the user to know the volume level.

Increasing and decreasing the volume in the application will allow to control the transmission distance of the ultrasound between the phone and the computer.

It is recommended not to have the volume too low as it will make the reception distance very small. The recommended volume level is about 80 %.

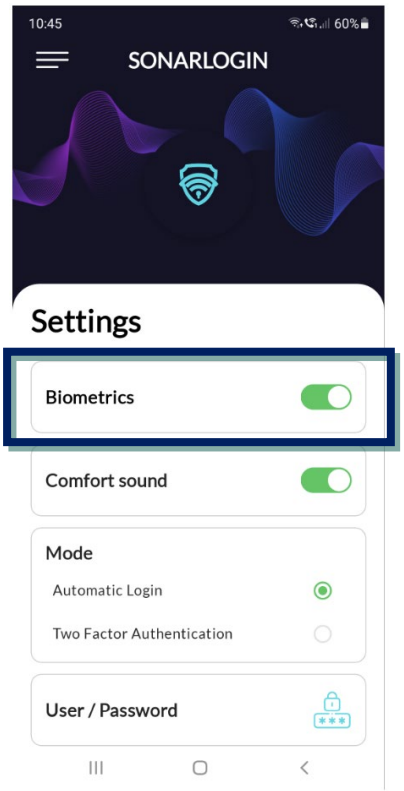
3.3.3 Settings

The user can access the settings using the application menu:



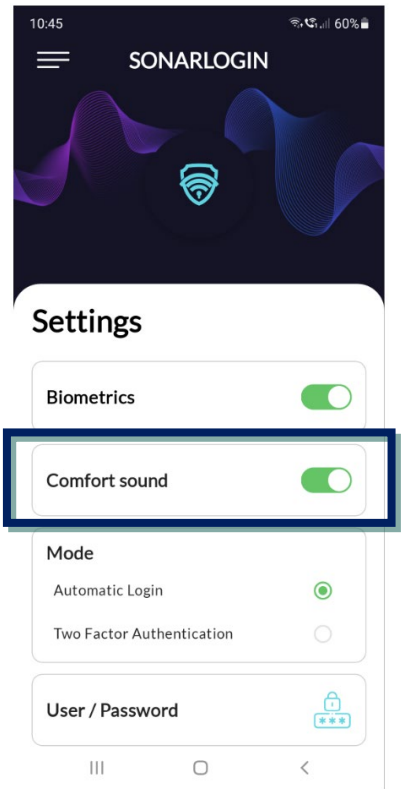
Enable and disable biometrics

As the application can be used to login in the PC, the user can prevent unauthorized use of the application by enabling the smartphone biometric authentication.



Comfort sound

If the option « Comfort sound » is activated, an audible sound is played at the beginning of the ultrasound transmission to give feedback to the user.



Mode

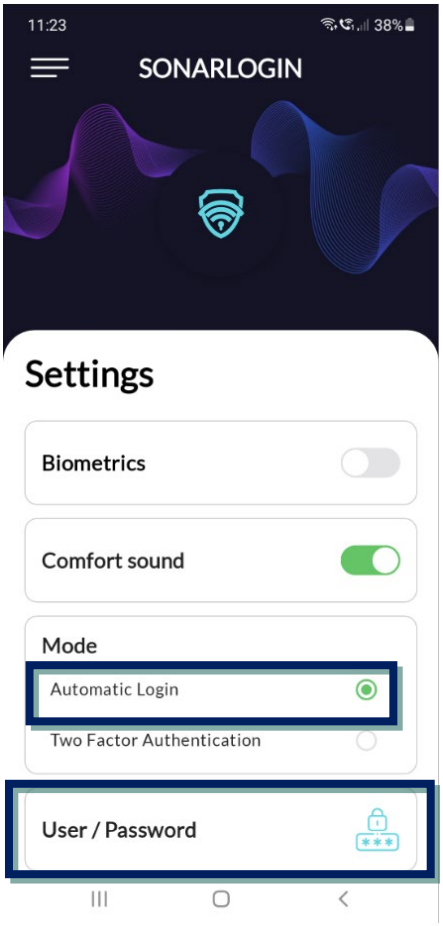
SonarLogin can be used in 2 different ways, for automatic login or as a second authentication factor.

In the settings screen you can choose the mode to be used:

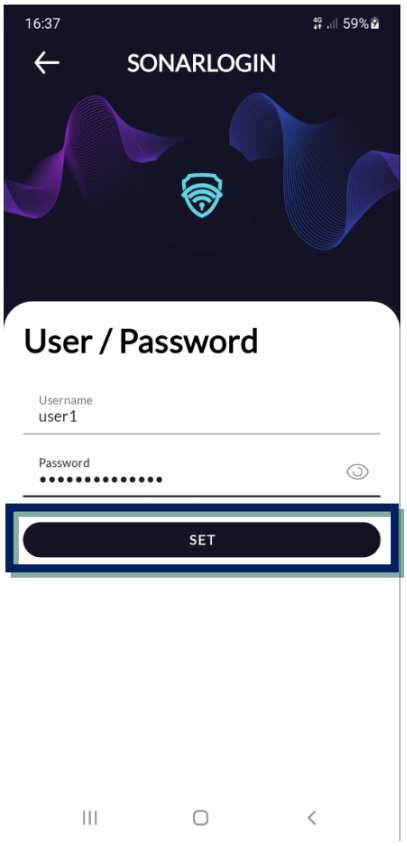
- **Automatic Login**

When the Automatic Login mode is activated you have to enter the username and password of your windows session:

- Select the “Automatic Login” option
- Click on “User/Password”



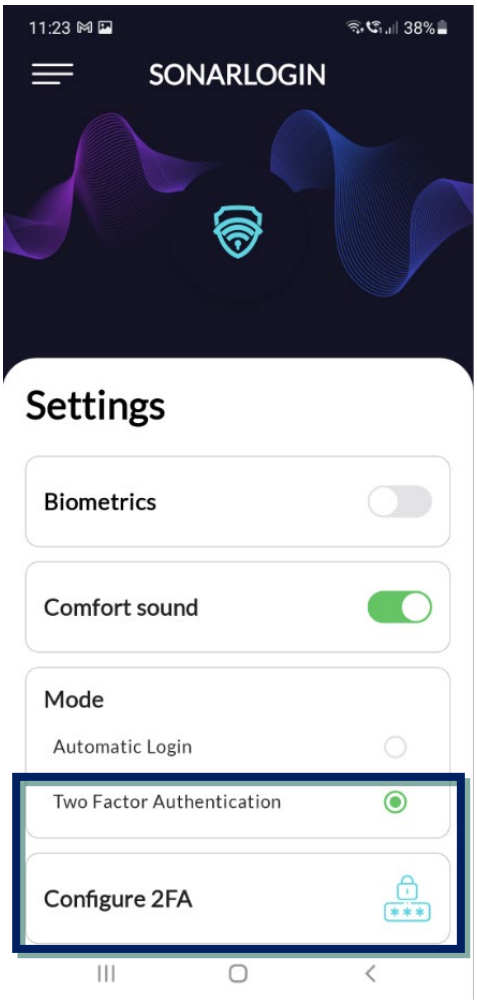
- Enter the username and password and click on “Set” :



- **Two-Factor Authentication**

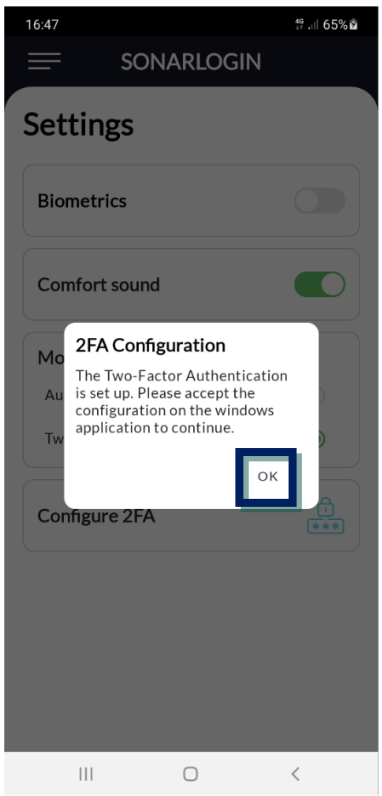
Using this mode, the user must scan a Qr Code in order to configure SonarLogin as a second factor for the authentication:

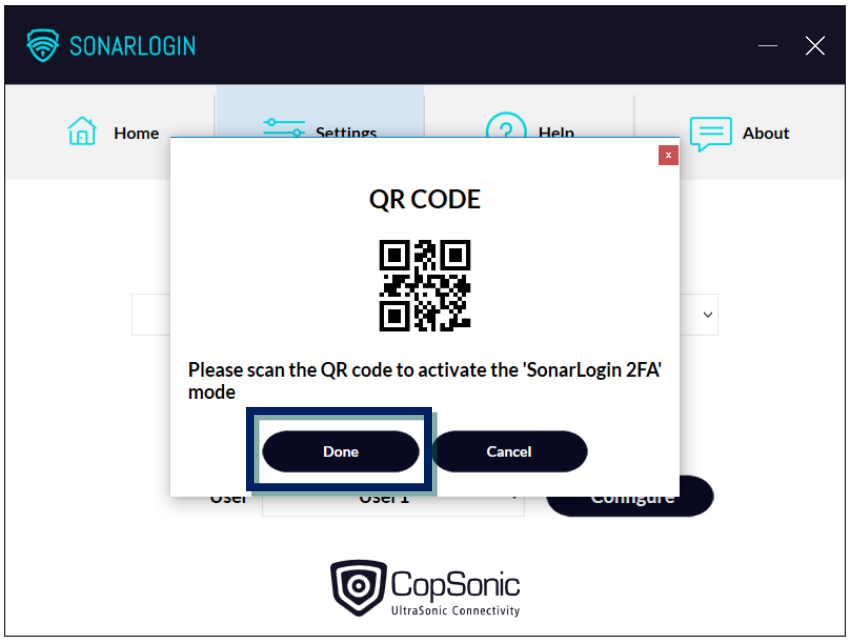
- Select the “Two Factor Authentication” option
- Click on “Configure 2FA”



On the SonarLogin manager configure Two-factor Authentication for the user (see 3.2.4).

Scan the Qr Code with the mobile application, and once the QR code is correctly scanned confirm the configuration in both, manager and mobile application:


16:47
65%
SONARLOGIN
Settings
Biometrics
Comfort sound
2FA Configuration
The Two-Factor Authentication is set up. Please accept the configuration on the windows application to continue.
OK
Configure 2FA


SONARLOGIN
Home
Settings
Help
About
QR CODE
Please scan the QR code to activate the 'SonarLogin 2FA' mode
Done
Cancel
CopSonic
UltraSonic Connectivity

4. Support and F.A.Q

Do not hesitate to contact us for assistance or further information:

-By mail: support@copsonic.com

- By phone: +33 563 67 81 20

You do not get open session windows:

a) Check the volume of the smartphone speakers.

b) Check if you have headphones connected.

c) Make sure your smartphone is close enough to the speakers; we recommend starting with a 30 cm distance or less.

- END of DOCUMENT -