Secure Remote Control with two-factor authentication

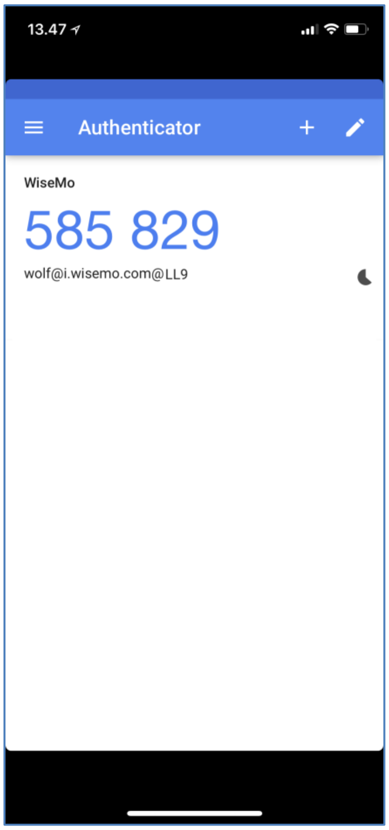
What is two-factor authentication

Two-factor authentication provides an extra layer of protection to secure your computers and devices running the WiseMo Host module from unauthorized access. In addition to user credentials, a second factor (the verification code) is needed.

Two-factor authentication can be used with the following authentication modes:

- Shared password
- User name and password
- Windows Security Management / System authentication (on macOS)

The verification code is generated by an authenticator app on your mobile device.



WiseMo

585 829

wolf@i.wisemo.com@LL9

After enabling two-factor authentication, the app generates a temporary verification code every 30 seconds. When connecting from a WiseMo Guest module to a Host you will, as part of the logon process, have to enter the verification code displayed on the Authenticator app at this very moment. A verification code can only be used once, and is only available and valid for 30 seconds.

Authenticator apps

The verification code is generated by an Authenticator App on your mobile device. WiseMo recommends and tests compatibility with Google Authenticator and Microsoft Authenticator for Android and iOS but other authenticator apps or hardware devices supporting the totp specification (RFC6238) might work.

To install the authenticator app on your phone or tablet, open App Store on iOS or Play Store on Android. Search for “Google Authenticator” or “Microsoft Authenticator”.

Alternatively use the following links.

iOS (iPhone/iPad):

- Google Authenticator
- Microsoft Authenticator

Android (phones and tablets):

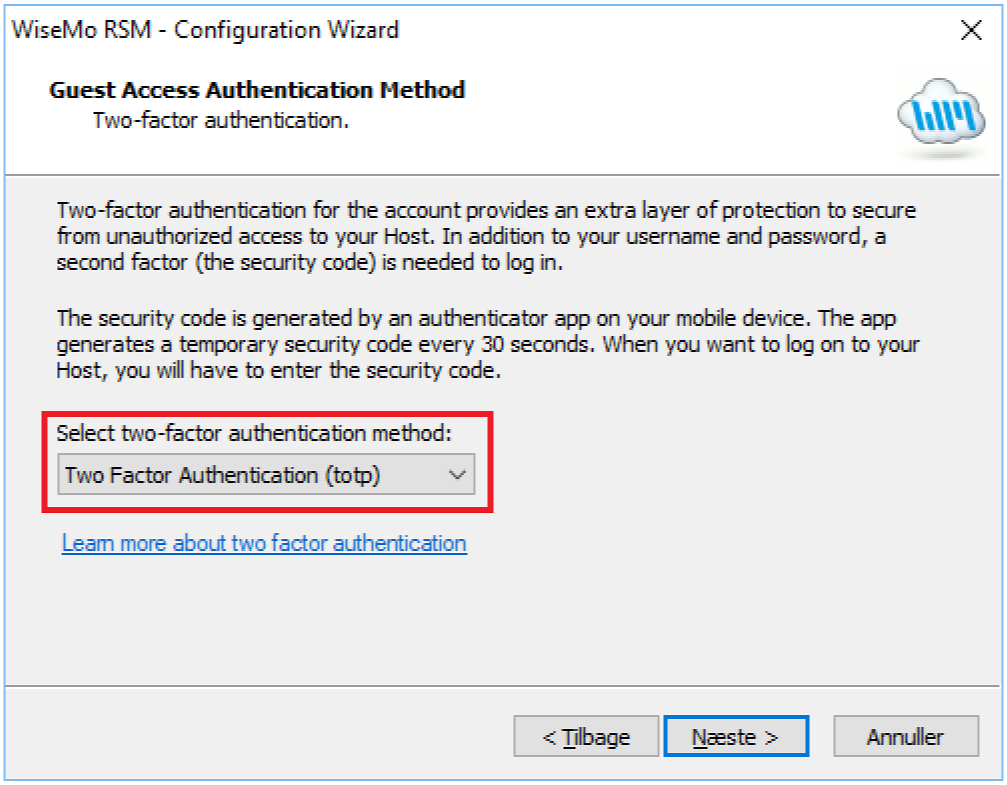
- Google Authenticator
- Microsoft Authenticator

How to enable two-factor authentication

Protection of the Host module with two-factor authentication is enabled and configured via the configuration wizard or directly via settings in the Host Manager user interface.

Using the configuration wizard

For each of the supported authentication modes you will have the option to select “Two-factor authentication”. Start the configuration wizard and click “Next” until you come to the “Guest Access Authentication Method” screen (the page shown below):



Guest Access Authentication Method

Two-factor authentication.

Two-factor authentication for the account provides an extra layer of protection to secure from unauthorized access to your Host. In addition to your username and password, a second factor (the security code) is needed to log in.

The security code is generated by an authenticator app on your mobile device. The app generates a temporary security code every 30 seconds. When you want to log on to your Host, you will have to enter the security code.

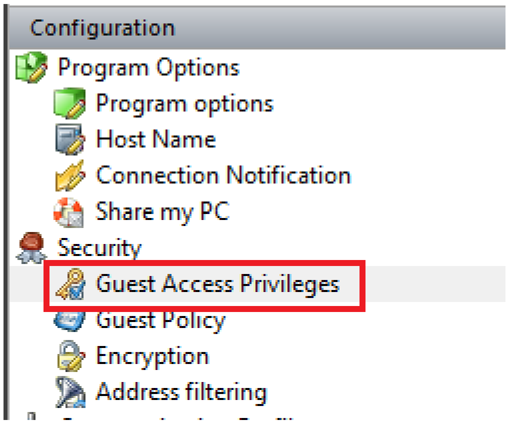
Select two-factor authentication method: Two Factor Authentication (totp)

Learn more about two factor authentication

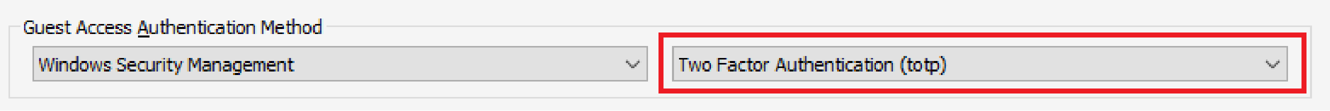
Then select the setting: "Two Factor Authentication (totp)".

Using Settings:

Select "Guest Access Privileges" in the left pane:



And then "Two-factor authentication (totp)" in the "Guest Access Authentication Method" in the right pane:



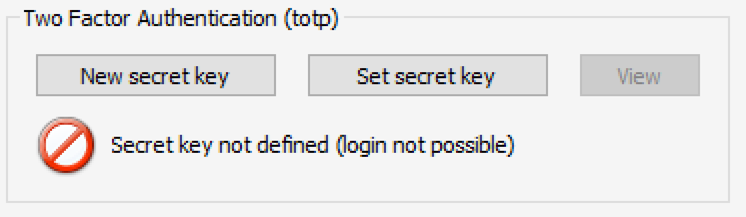
Guest Access Authentication Method

Windows Security Management

Two Factor Authentication (totp)

How to configure two-factor authentication for users

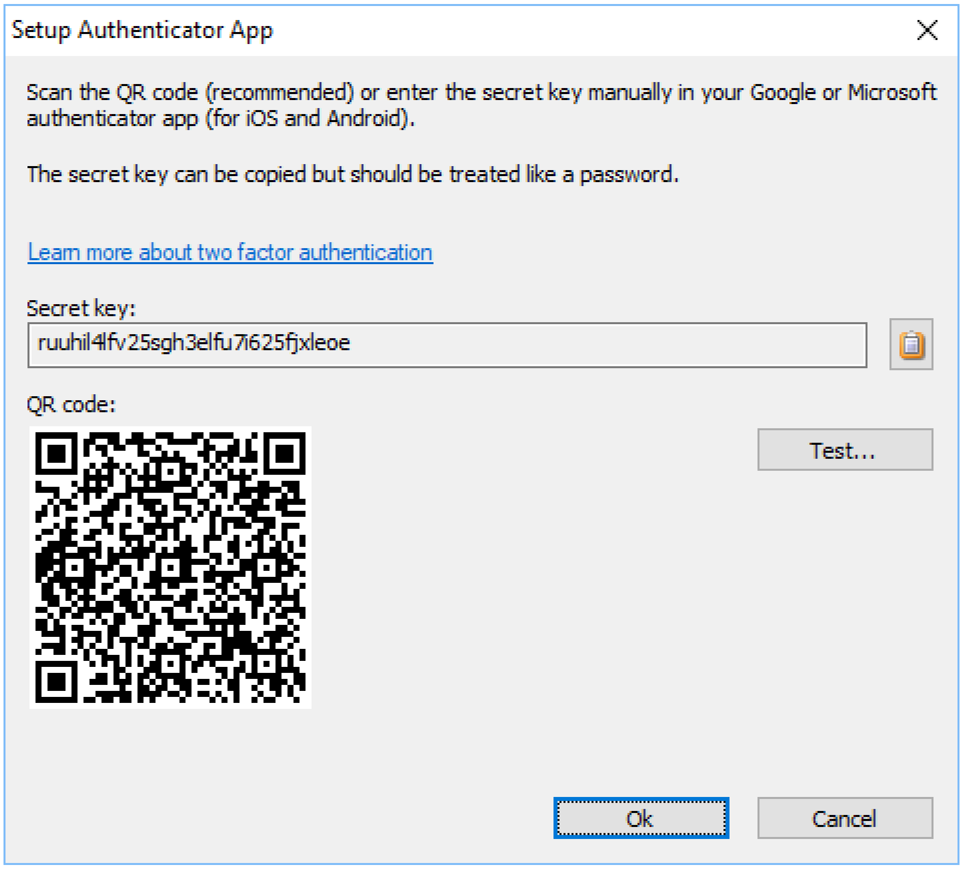
Once you have enabled two-factor authentication you will need to configure on the Host who should be able to remote control the Host. The user interface varies a bit depending on what Authentication mode you are using and whether you are using the configuration wizard or settings directly, but it all ends up in the following screen:



Two Factor Authentication (totp)

Secret key not defined (login not possible)

The red image means that the user is not yet configured. Click the "New secret key" button and the following screen opens:



Setup Authenticator App

Scan the QR code (recommended) or enter the secret key manually in your Google or Microsoft authenticator app (for iOS and Android).

The secret key can be copied but should be treated like a password.

Learn more about two factor authentication

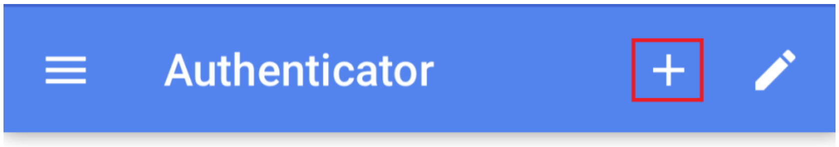
Secret key: ruuhil4lfv25sgh3elfu7i625fjxleoe

QR code:

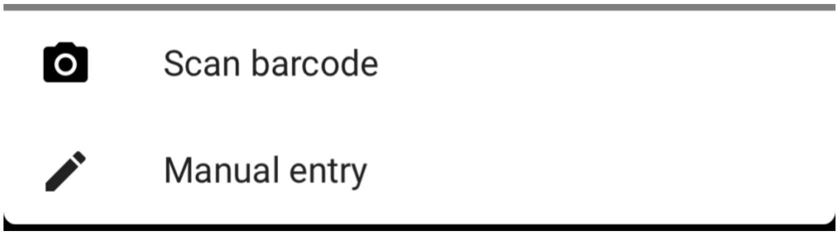
The secret key is what links the user account defined on the Host and the Authenticator App together. The easiest way to transfer the secret key to the Authenticator App is to scan the QR code image (the barcode image). The method is a bit different between the two apps.

Configure Google Authenticator

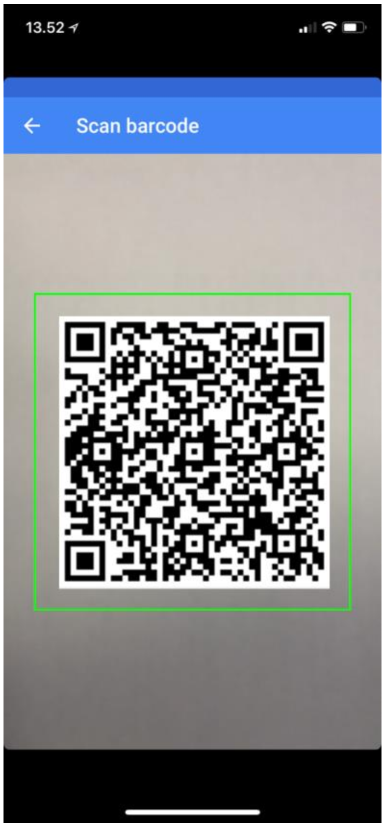
Click the '+' in the toolbar:



Select "Scan barcode" in the menu:

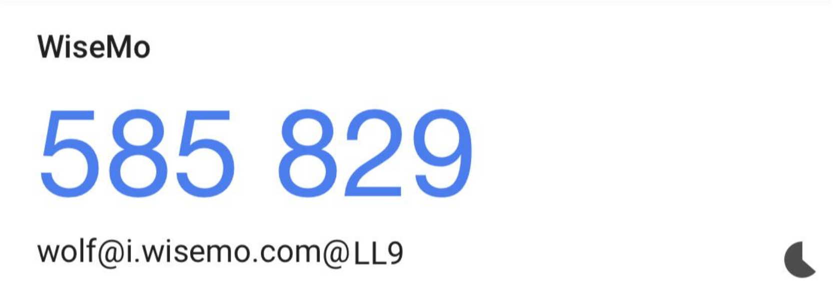


Hold up phone so the camera catches the QR image (the barcode). Move the phone a bit back and forth until the app succeeds reading the QR image.



The app will automatically go back to the main screen and is now configured.

The app shows some information that will help you identify the verification code (in blue) to use, which is especially helpful when you have multiple codes.



WiseMo

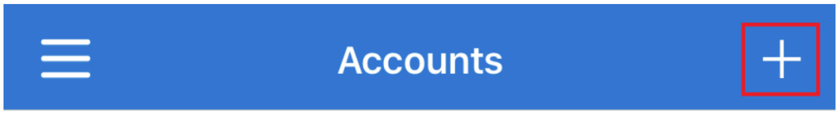
585 829

wolf@i.wisemo.com@LL9

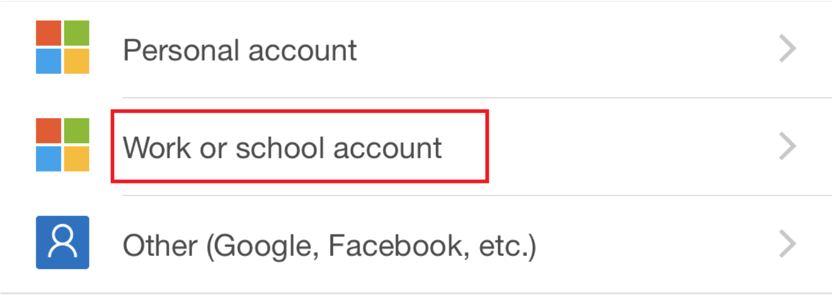
By the title in bold you can determine it is a verification code for WiseMo. Below the 6 digit code, you can see information about the computer name and the user defined for access to the Host. In this example the user is “wolf” in domain “i.wisemo.com” on computer “LL9”

Configure Microsoft Authenticator

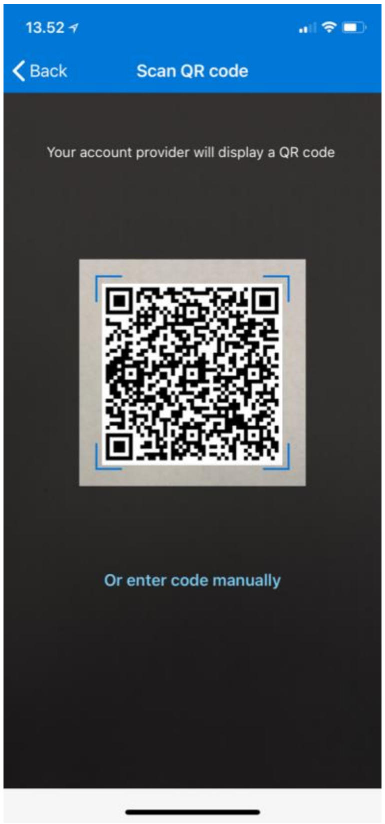
Click the ‘+’ in the toolbar:



Select “Work or school account” in the menu:



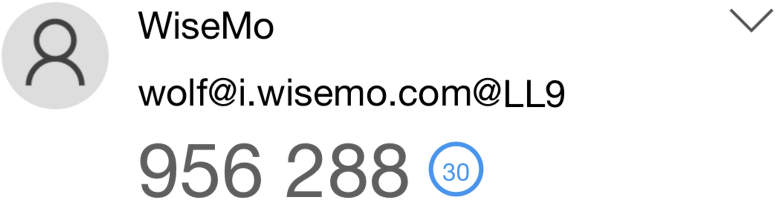
Hold up the phone so the camera catches the QR image (the barcode). Move the phone a bit back and forth until the app succeeds reading the QR image.



Your account provider will display a QR code

The app will automatically go back to the main screen and is now configured.

The app shows some information that will help you identify the verification code (the numbers).



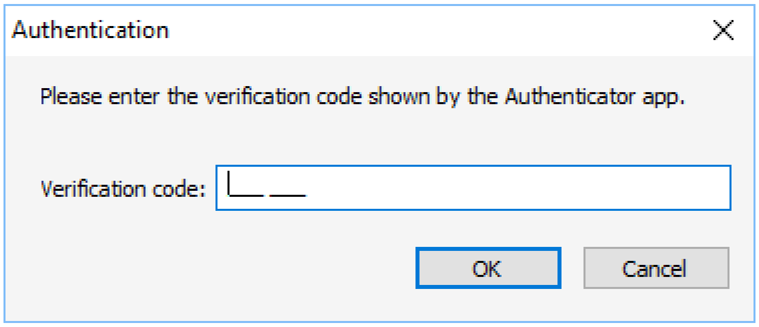
WiseMo

wolf@i.wisemo.com@LL9

956 288

In this example the user is “wolf” in domain “i.wisemo.com” on computer “LL9”.

When the Google or Microsoft Authenticator App is configured you can test it locally on the Host by clicking the “Test” button next to the QR code in the Host Manager dialog. You will be prompted for the verification code displayed in your app:



Authentication

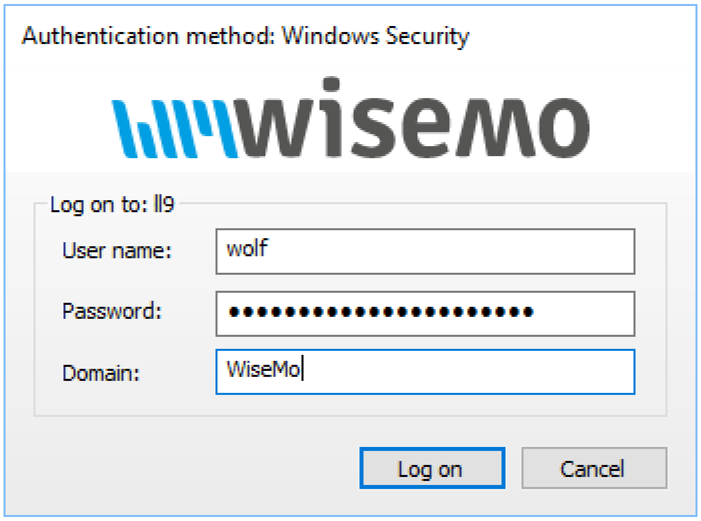
Please enter the verification code shown by the Authenticator app.

Verification code: ___ ___

Enter the 6 digit number (the space should not be entered, it’s only for readability) and click “Ok”. If it was correct you will see the QR code and secret key again.

How to login from a Guest

Now that the Host is set up for two-factor authentication you can try to connect from a Guest. Connect as usual to the Host. Enter username, password etc. depending on Authentication mode:



Authentication method: Windows Security

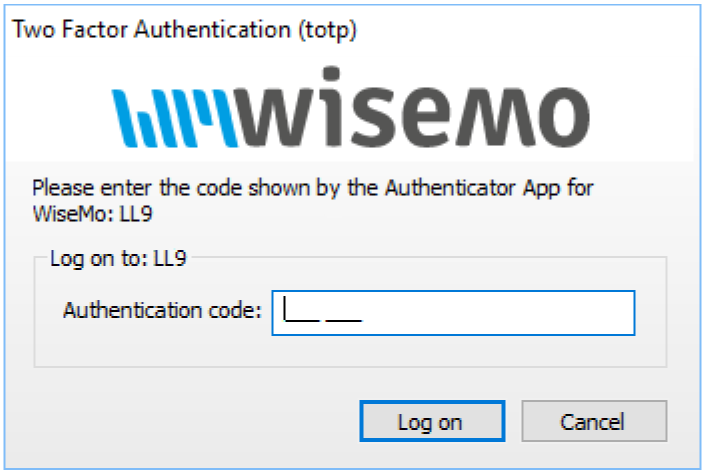
Log on to: ll9

User name: wolf

Password: ••••••••••••••••••••••

Domain: WiseMo

Click “Log on”. Because two-factor authentication is enabled on the Host, you will be prompted for the verification code:



Two Factor Authentication (totp)

Please enter the code shown by the Authenticator App for WiseMo: LL9

Log on to: LL9

Authentication code: ___ ___

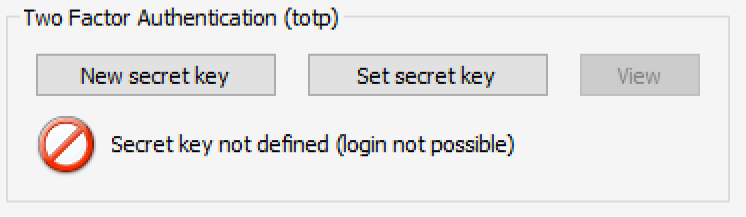
Enter the Authentication Code currently shown in the Authentication App. Only numbers should be entered – the space is for readability.

Click “Log on” again and you have access if everything was correct. Please note that if there’s an error, you will NOT be able to tell whether it was the password or the Authentication code that was wrong. This is part of the PCI Security Standard requirement. This method increases security as the two factors are then multiplied, not added.

Notes about the secret key

The secret key is what links the user account and the Authenticator App together. The secret key should be treated like a password – at best it should only be stored by the Authenticator App and you should make sure that its keys are backed up so you can restore them if access to the Authenticator App should be lost. A secret key can be copied from one user account to another and even between computers / devices – but confer with your security policy whether that is allowed.

If you have a secret key and you need to set it for a user account you can click "Set secret key" in the screen below:



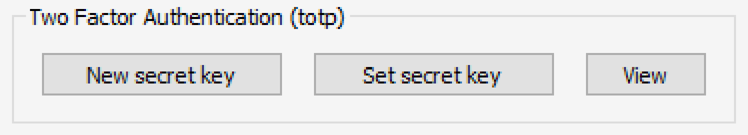
Secret key not defined (login not possible)

If you have a secret key defined, you can view it, for example to configure a different Authenticator App with this key. To do that click "View", enter the Authentication Code, and the secret key is shown.

Verifying the Authenticator App configuration

You can at any time verify on the Host whether your Authenticator App is setup correctly for a particular user account. Start the Host Manager. Select "Guest Access Privileges" in the left pane of the Host Manager. Find and select the user account you want to check in the list. If the "View" button is disabled and you see the ⊘ image then the user account is not configured at all.

Assuming that the account is setup and looks like the image below,



click the "View" button and enter the verification code. If you see the secret key your Authenticator App is setup correctly for this account.

Notes about PCI requirements

Two-factor authentication of all remote control accounts at the application level is required by PCI-DSS 8.3.1 and 8.3.2. PCI-DSS 8.1.1 and 8.5 requires that access is provided individually, i.e. the "Shared password" authentication mode is not recommended.

Troubleshooting

If you have problems logging on:

- Verify that the login credentials (User name, Password, Domain) are correct.
- Verify that you are entering the verification code for the right user and for the right Host computer.
- Test two-factor authentication locally on the Host, see paragraph "Verifying the Authenticator App configuration".
- Verify that you actually configured a secret key for this user, see paragraph "Verifying the Authenticator App configuration".
- Verify that the time is set correctly on both the Authenticator App device and on the Host PC/device. Two-factor authentication (totp) works between time zones but the time needs to be correct within approximately 30s.
- If you lost access to the Authenticator App your only options are:
  - Restore the Authenticator App configuration on another device from a backup.
  - If you saved the secret key, it can be configured manually in another Authenticator App.
  - Configure a new secret key for the user on the Host PC/device

  WiseMo doesn't know the secret key and cannot help you recovering it!