



Two factor authentication

●	Introduction	3
●	Login with two factor authentication	4
●	Reset two factor secret	5
●	Authenticator-app	5
●	Appendix	6
●	Activate two factor authentication	6
●	Troubleshooting	8

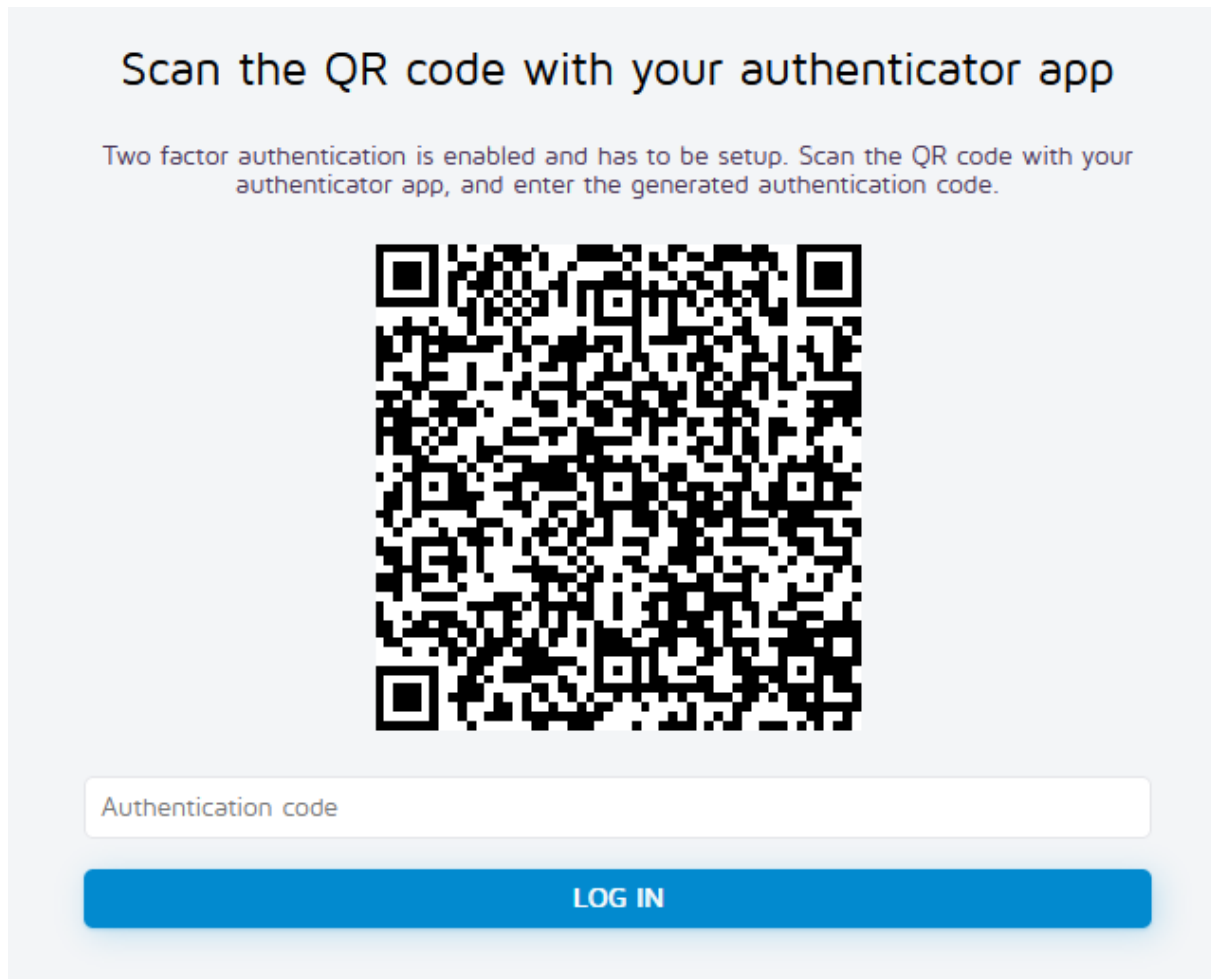
Introduction

With 2-factor authentication activated, this means that login is not only done with a password, but also with the help of "a second factor". Antura has chosen to build a solution for the purpose where a mobile device and an app are used to generate a code that is the second factor.

The support for two-factor authentication is aimed at organizations that use what we call "form login", which means organizations that have no other solution for authentication, such as identity federation or AD login.

Login with two factor authentication

When 2-factor authentication is activated (see section "Activating two factor authentication" in the Appendix), the user is presented with the following dialog when they login with form authentication for the first time.

The image shows a login dialog on a light blue background. At the top, the text "Scan the QR code with your authenticator app" is displayed in a bold, dark font. Below this, a smaller line of text states: "Two factor authentication is enabled and has to be setup. Scan the QR code with your authenticator app, and enter the generated authentication code." In the center of the dialog is a large, square QR code. Below the QR code is a white rectangular input field with the placeholder text "Authentication code" in a light blue font. At the bottom of the dialog is a prominent blue button with the white text "LOG IN".

Scan the QR code with your authenticator app

Two factor authentication is enabled and has to be setup. Scan the QR code with your authenticator app, and enter the generated authentication code.



Authentication code

LOG IN

Figure 1 – The first login

The user will get a QR code presented to them which is scanned in the Authenticator app.

After the code is scanned a code will be generated in the Authenticator app. After the code is entered into the form the user will be sent to the login page.

For subsequent logins with form login, the user will see the following dialog instead. The user should enter the generated code in order to log into Antura.

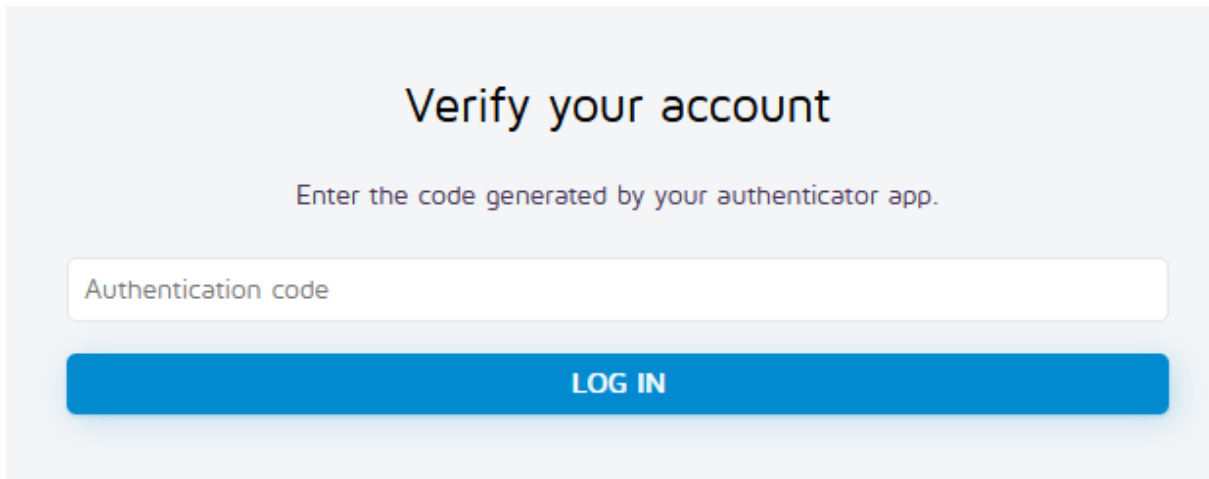
A light blue rectangular box representing a login screen. At the top, the text "Verify your account" is centered in a large, bold, black font. Below it, the instruction "Enter the code generated by your authenticator app." is centered in a smaller, regular black font. Underneath the instruction is a white rectangular input field with the placeholder text "Authentication code" in a light blue font. At the bottom of the box is a solid blue rectangular button with the text "LOG IN" in white, uppercase, sans-serif font.

Figure 2 – Subsequent logins

Reset two factor secret

If a user for some reason loses his second factor, it needs to be reset by a user administrator before the user can create a new "secret". This is done on the user in the *Administration - User* view.

This means that the user will need to re-enable two-factor authentication in order to log in.

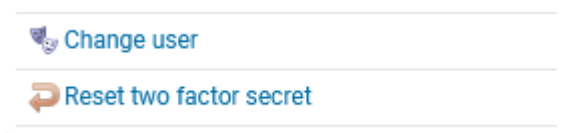
A white rectangular button with a thin grey border. It contains two lines of text. The top line has a small blue icon of a person with a keyhole next to the text "Change user" in blue. The bottom line has a small orange icon of a circular arrow next to the text "Reset two factor secret" in blue.

Figure 3 – Reset two factor secret

Authenticator-app

There are several apps that can be used for authentication. Two common apps are Microsoft Authenticator and Google Authenticator. Both are available for free download from the Google Play Store or the Apple App Store.

Appendix

Activate two factor authentication

Support for two-factor authentication is activated in the *Administration - System Settings - General* view under "Forms Authentication Settings" sections.

1. Check "Enable two factor"
2. Click OK

Edit form authentication settings

Passwords can be changed after N days:

Passwords must be changed after N days:

Passwords must not be reused for N days:

☐ Weak passwords must be changed at next login

Password strength

Passwords must contain at least N characters:

Passwords must contain at least N numerics:

Passwords must contain at least N special characters:

☒ Passwords must not contain usernames

☐ Passwords must contain mixed case characters

Deactivation of accounts

Deactivate accounts after N days of inactivity:

Deactivate accounts after N failed login attempts:

Two factor

☒ Enable two factor

CancelOK

Figure 4 – Activate two factor authentication

When the setting is activated, the user will next time be asked to set up the "secret" which will be the second factor when logging in.

Troubleshooting

If it does not work to log in with the Authentication Code, it may be because the phone's time settings are not synchronized. This means that the Authentication code you see in the app (Google Authenticator or Microsoft Authenticator) is never valid. Try turning the time synchronization on / off in the phone and then try again.

If it still does not work, you can reset the user's two-factor secret via the *Administration - Users* view:

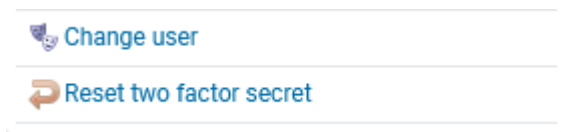


Figure 5 – Reset two factor secret