HelpDesk

Version 5.4 – New features

Our company and our data centre are ISO 27001 certified and located in Sweden.

Read more about HelpDesk >>

Pricing >>

Contact us via form >>

info@artologik.com

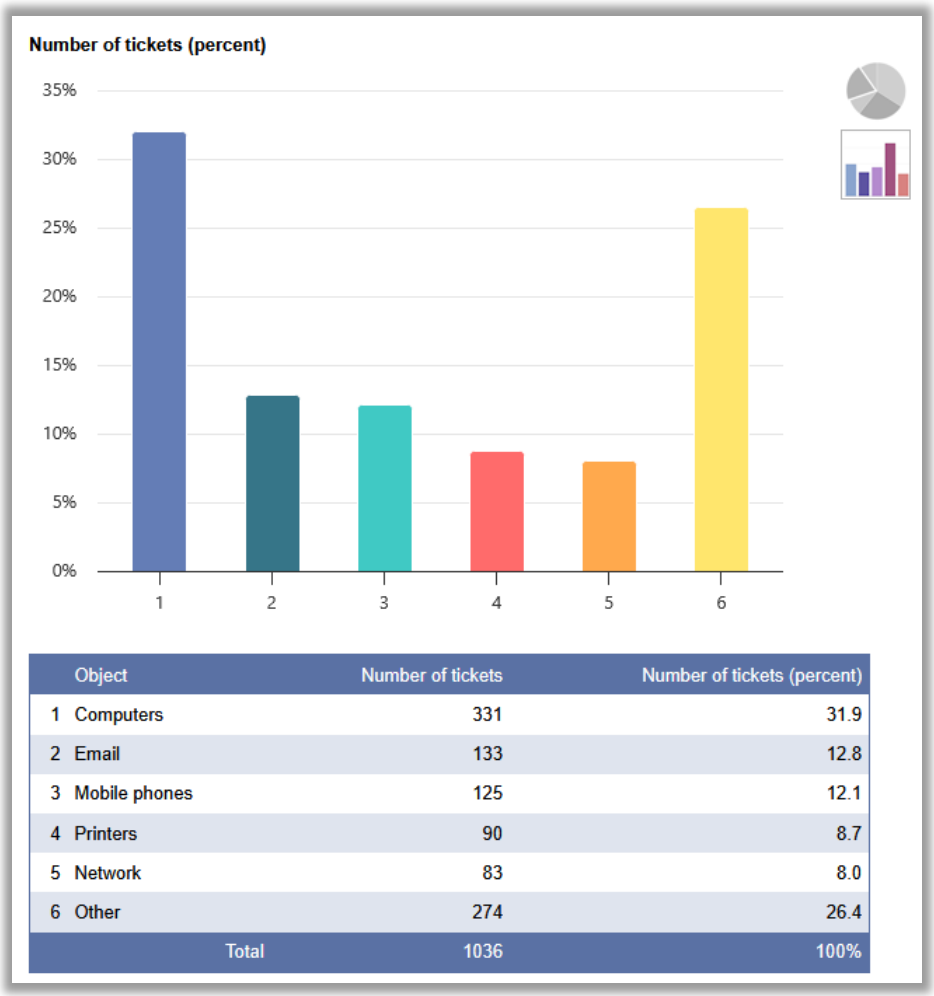
Artologik®
SOFTWARE FOR THE WEB

Table of Contents

Reports

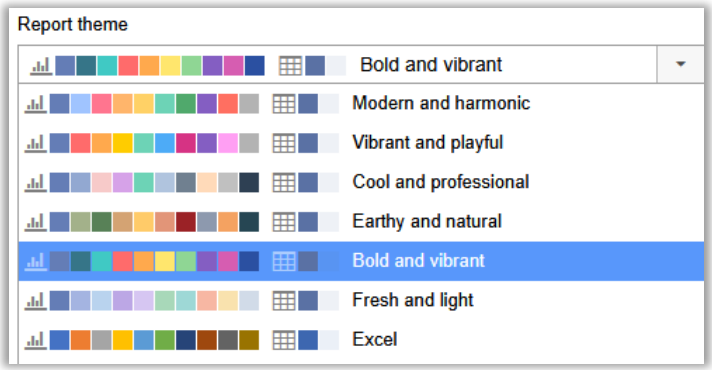
Report design improvements

In this version, the report section uses a new chart engine, generating modern, visually enhanced charts in both display and export modes.



	Object	Number of tickets	Number of tickets (percent)
1	Computers	331	31.9
2	Email	133	12.8
3	Mobile phones	125	12.1
4	Printers	90	8.7
5	Network	83	8.0
6	Other	274	26.4
	Total	1036	100%

The colours used in the charts are determined by the Report Theme you select under *Administration > System Settings > Advanced*. The primary colour of the Report Theme also appears in the tables in the report display mode.



Report 'Ticket list': Present the coordinates of the ticket

If you use the HD-Map plugin, you can now include the coordinates of any mark (specific location or area) added to the map for a ticket in the *Ticket List* report.

Object	Ticket no	Ticket title	Registered (date)	Map marking (coordinates)
Street lights	20251208:082	Broken street lamp	2025-12-08 14:20	18.063771,59.396299
Earth works	20251208:079	Drainage	2025-12-08 13:01	18.063203,59.391063 18.063203,59.391232 18.063846,59.391232 18.063846,59.391063 18.063203,59.391063

Administration

Add objects at the same level

With HD-Advanced, you can build hierarchies of objects and child objects. The object administration already includes:

- The *Add main object* button to create an object at the top level
- The *Add child object* button to add a child object to the object currently being administered

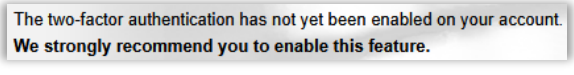
In this version, we have added a third button: *Add object on same level*, which becomes available when you administer a child object and create a new object as a 'sibling' to the existing one, i.e. as a child object to the same parent object.

Two-factor authentication

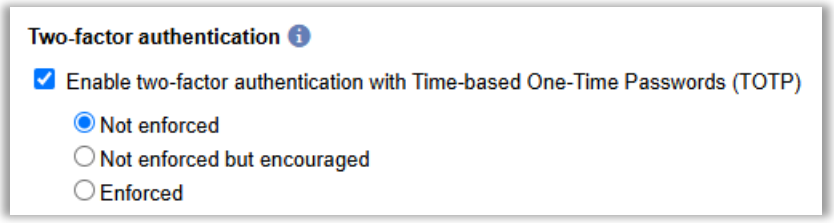
To strengthen login security, you can enable two-factor authentication. It has previously been possible to enable additional authentication using a login code sent to the user via email; however, this version also allows users to authenticate themselves using a TOTP (Time-based One-Time Password) app on their phone. After logging in as usual with their username and password, the user has to enter a code generated by the TOTP app.

The setting is enabled under *Administration > System settings > Advanced*, and you can choose from the following options:

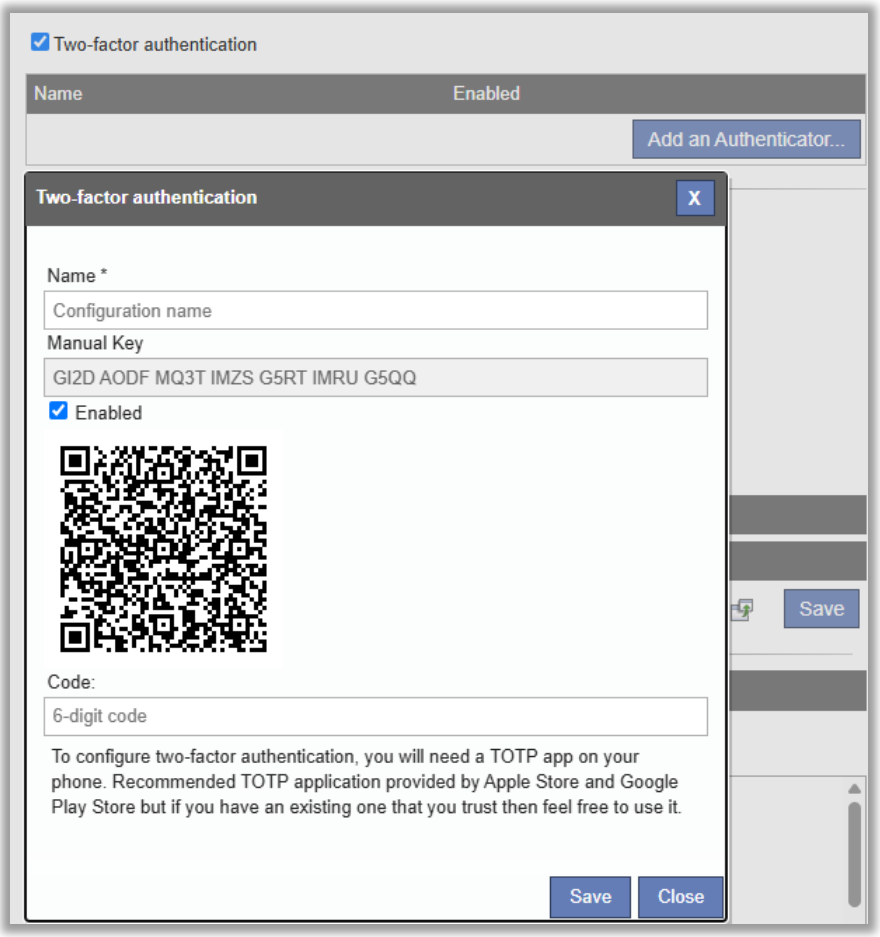
- *Not enforced*: Two-factor authentication is optional for the user to enable
- *Not enforced but encouraged*:
  Two-factor authentication is optional, but the user is prompted to enable it at each login



- *Enforced*: Two-factor authentication is mandatory to use, and the user is required to enable it at the next login

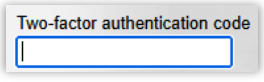


In his/her profile, the user selects *Two-factor authentication enabled* and then clicks *Add an authenticator…* to open the window where two-factor authentication is configured. When two-factor authentication is enforced, the user will come directly to this window at login, if he/she has not previously enabled it.



The user downloads a TOTP app on his/her phone and creates a new account in the app by scanning the QR code. It is then possible to retrieve a code from the app, which is entered in the *Code* field. Finally, give the configuration a name and save.

At each login, the user opens the app and clicks on the account to see the code that is currently valid (changes every 30 seconds). After logging in with his/her username and password, the user enters the code in the *Two-factor authentication code* field.



Both types of two-factor authentication (with TOTP and via e-mail) can be enabled simultaneously, but only if the *Not enforced* option is selected for TOTP. In this mode, the following applies:

- For users who have added TOTP authentication, TOTP will be used.
- For users who have not added TOTP authentication, e-mail authentication will be used.

If either the *Not enforced but encouraged* or *Enforced* option is selected for TOTP, e-mail authentication will be disabled.

New editor

We have replaced the editor used in the program for writing and formatting text. The editor is used in the following parts of the program:

- E-mail
- E-mail templates
- Standard Responses
- The Dashboard
- SLA reminders
- E-mail signature in the user administration
- Newsadministration