



Release Notes

Navigil Service release 1.19.0

Date: 11.4.2023

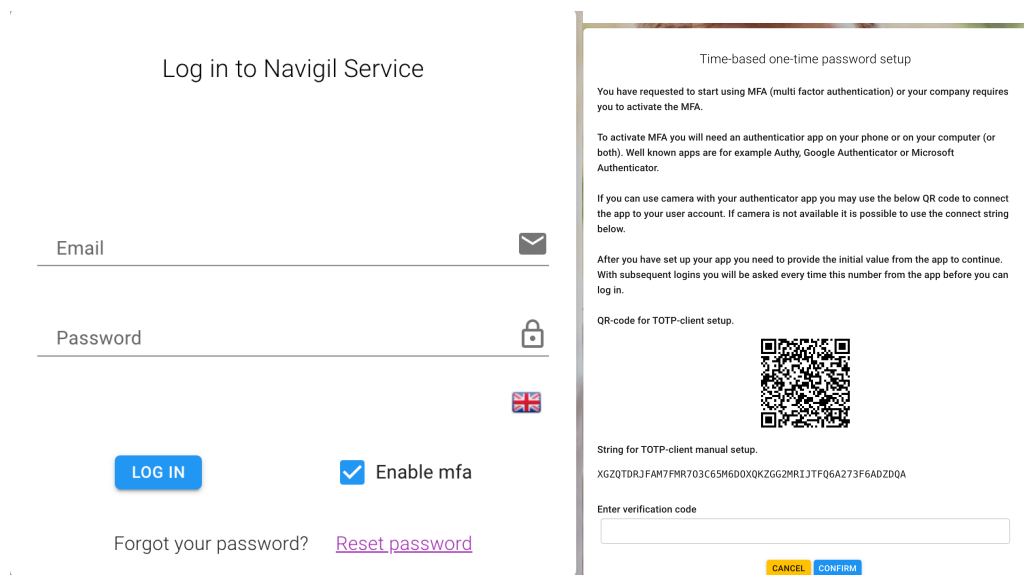
1 Release summary

The release includes new features such as Multifactor authentication, Company and Group based automatic firmware updates, customizable beacon area codes and portal for Rafael users. There are also many smaller improvements and bugfixes.

2 Multifactor authentication (MFA)

It is now possible for any user to activate MFA. It is also possible to force the MFA for the whole company or any group. This must be requested from Navigil. In the future it will be possible to require MFA based on the user level. Using multifactor authentication requires the use of an authentication app.

If wishing to activate the MFA the Enable mfa checkbox must be selected. After that user should log in normally and there will be an instruction screen shown. There the user may activate MFA using the shown QR code or the connection string.

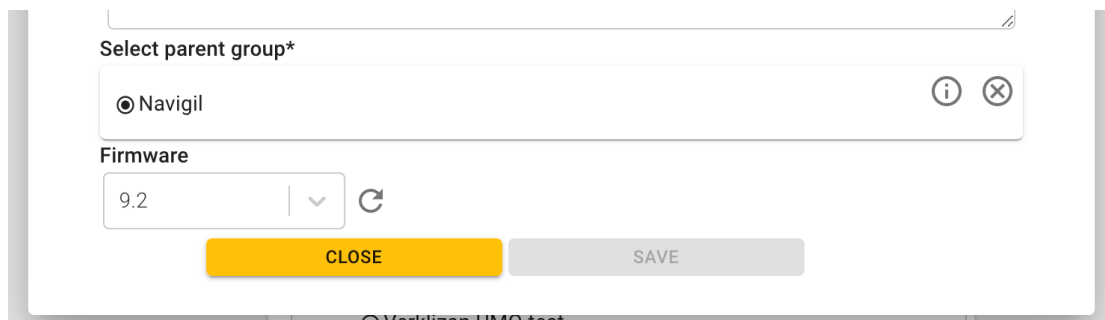


3 Company and group based Firmwares

It is now possible to set the required Firmware level for the whole company or any group. Company setting must be made by Navigil but group-based setting is manageable by customers.

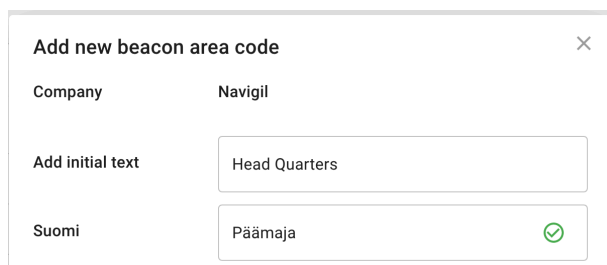
If there is a Firmware selected the Devices will try to upgrade (or downgrade) to that level as soon as they connect to the service and battery and other required parameters are met.

Users should use this with caution because it will influence all devices. Using this feature, it is easy to setup a test group for devices having the latest software.

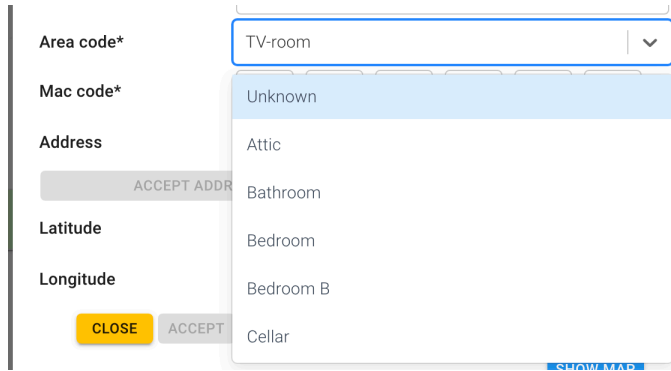


4 Customized beacon area codes

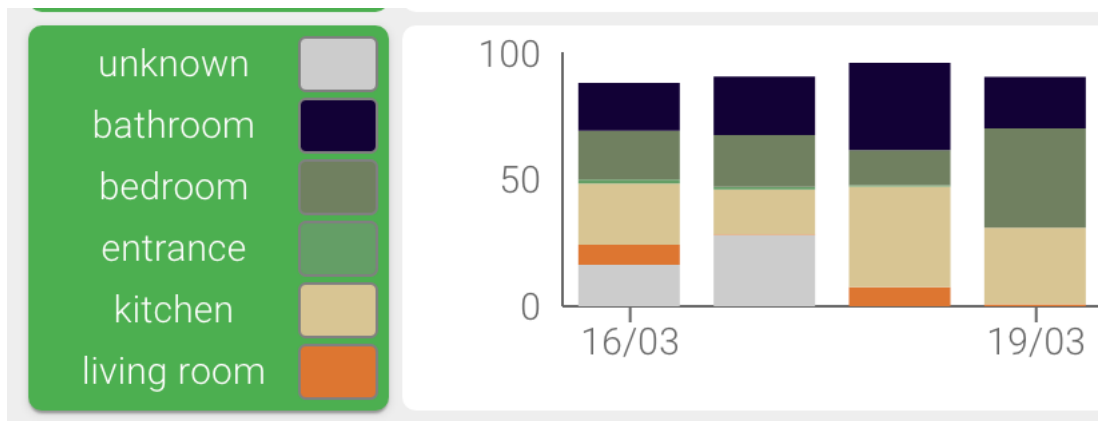
It is now possible to use custom names for any beacon. There are 10 predefined names and an option to add 20 company-named beacons.



After adding the name it is possible to give that name to any beacon connected to a watch.



The time spent within any beacon is then shown in the dashboard same way as earlier but with the option of having custom titles there.



5 Optional Security improvements

By request It is now possible to upgrade devices to the release 10 which makes it possible to add more security features to further strengthen the defences against unauthorized access to data and service performance degradation. A more detailed description of the security enhancements available can be provided under the non-disclosure agreement.

The optional security enhancements include the following elements:

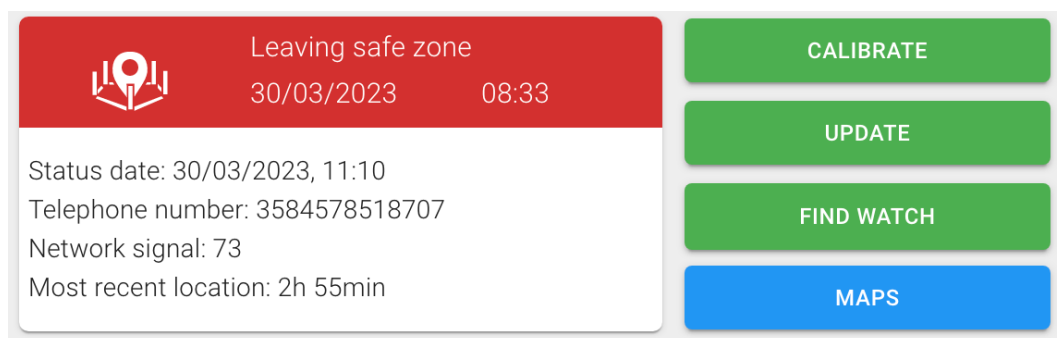
- Secure element in the device for storage of encryption and authentication keys with memory access protection
- Encryption of protocol messages between the device and the service

- Encryption of the device data storage including message pool and critical log files
- Encryption of critical files during transfer within the infrastructure
- Authentication of each device and server with authentication keys
- Secure device boot process utilizing firmware signature functions, compatibility, and authentication checks
- Device hardware JTAG, UART, and USB service port access restriction

These optional features in effect enable encryption of communication between the device and the service within the private infrastructure with regularly rotated keys. They also prohibit unauthorized use of firmware in devices and impersonation attacks with stolen SIM cards or by illicit service elements that might have gained access to the infrastructure. These features keep authentication and encryption keys safe in the system including attempts to gain access to secrets via disassembling devices for tampering purposes.

6 Update button functionality changed

In the dashboard the Update button used to only load all notifications but now it also asks the watch to send a status report to the service. When the Update button is clicked a request is sent to the watch and the service will wait for max 30sec for an answer. If an answer is received the status date timestamp will be updated. It can sometimes take up to a minute for the response to arrive, so it may be required to click the button again.



7 Schedule for Homebeacon range exit alarm added

We have added a scheduling option for Homebeacon range exit alarm. If there are any Homebeacon range exist alarms set up there will be in Section 4, General settings the possibility to select the time period when the alarm is inactive.

Please note, that in current firmwares, there is a bug until 9.2 that if the user is outside of Homebeacon range and the allowed schedule expires, the alarm will not be activated. This is fixed in the coming release 9.3, which is not released yet.

Home beacon alarm schedule


Use schedule Off

→

Home beacon alarm schedule

Use schedule On

Start 08:00
End 16:00



0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 0

8 Rafael portal – landing page

For customers using also S1 or S3 watches there is a portal page available. The portal can be found at <https://test.navigil.com/portal> or <https://customaddress/portal>

The portal makes it possible to find the device also from the old Rafael service. To make this possible, it is required for the user to have the same email address both in Navigil Service and Rafael.

Opening the page in Rafael also requires logging into that system.

Filter devices

NAVIGIL SERVICE
RAFAEL
RELOGIN
CLOSE PORTAL

Search options

DEVICES:39
ALARM:78

DEVICES:24
WARNING:35

DEVICES:27
INFO:40

Searching all

Phone number	Status	Status date	Dashboard	Serial number
Demo 2 User +3584578515046 Navigil		2023-03-29 00:01:12	NS 2 1	LEAVING SAFE ZONE 1200000326 - fw:4.12.1 sim:dna
Demo User +447723599682 Navigil <i>Jarnon laitteet 2</i>		2023-03-03 11:39:24	NS 4 1 1	LEAVING HOME AREA 1200000740 - fw:5.10.0 sim:telefonica
Navigil Demo 1 +3584578502527 Navigil			RAFAEL	1000017137 - fw: sim:
Navigil Demo 2 +3584578507150 Navigil			RAFAEL	1000032414 - fw: sim:
Navigil Asennusdemo +3584578501875 Navigil			RAFAEL	1000008769 - fw: sim:

Rows per page: 10 ▼ 1-5 of 5 << < > >>

Filling in the search word in Filter devices field will search both Navigil Service and Rafael and shows the data in the table. NS or RAFAEL button can be clicked to show the devices.

Please note, that the Rafael devices are always from the Production environment since there is no test environment available.

9 Bugfixes

There have been bugs when creating group admin users, company employees or relatives. It has been possible that the creator could not select the correct group or device for the user after creating. These are fixed.

Signal strength query has often timed out and showed an error. The backend query is now optimized and should work fine.