# Mobile

SECURAZE

1. Administration 9
1.1 System environment ... 10
1.2 Hardware ... 16
1.3 Wireless network recommendations ... 16
1.4 Installation ... 18
2. Supported Device OS 23
3. Getting started 27
3.1 Preparations ... 28
3.1.1 Creating a new user ... 28
3.1.2 Create new logo ... 29
3.1.3 Create new report data ... 31
3.1.4 Create new file name pattern ... 32
3.1.5 Creating a new printer ... 33
3.2 External Systems ... 34
3.2.1 Re-trigger data sending ... 34
3.3 Recurring operations ... 38
3.3.1 Create a new Warehouse ... 38
3.3.2 Create a new Lot ... 40
3.3.3 Create a new Sale Lot ... 40
3.3.4 Creating a new Order ... 41
3.3.5 Set presets ... 44
4. Operation 47
4.1 Login ... 48
4.2 Options & Settings ... 49
4.3 Workflows ... 50
4.4 Select Lot ... 52
4.5 Select Sale Lot ... 53
4.6 Exit ... 53
4.7 Connect devices ... 54
4.7.1 Connect iOS Device ... 58
4.7.2 Connect Android device ... 60
4.7.2.1 Android USB-Debugging bypass with QR-Code ... 60
4.7.2.2 Manual Android USB-Debugging ... 65
4.7.3 Microsoft Apple Driver ... 67
4.7.4 Apple Watch & AirPods ... 68
4.8 Manual Entry ... 69
4.9 Check the connected devices ... 72
4.10 Infrastructure issues ... 73



© 2026 Securaze GmbH

4.11 Mobile Icons ... 75
4.12 Enter Device details ... 77
4.13 Register devices ... 80
4.14 Perform erasure ... 81
4.14.1 Erasure Methods ... 82
4.14.2 Erase iOS device ... 85
4.14.3 Erase Android device ... 86
4.14.4 Erase a Mac ... 86
4.15 Check erasure in the main menu ... 88
4.16 Perform diagnose ... 89
4.16.1 Description Manual Tests ... 103
4.16.1.1 Flashlight ... 104
4.16.1.2 Camera Tests ... 104
4.16.1.3 Camera Quick Tests ... 110
4.16.1.4 Various buttons ... 111
4.16.1.5 Headphones ... 116
4.16.1.6 Screen Display ... 117
4.16.1.7 TouchScreen ... 119
4.16.1.8 MultiTouch ... 122
4.16.1.9 3D Touch ... 124
4.16.1.10 Accelerometer ... 127
4.16.1.11 Face ID Quick & Face ID ... 128
4.16.1.12 Fingerprint Quick & Fingerprint ... 130
4.16.1.13 Proximity ... 132
4.16.1.14 Speaker ... 133
4.16.1.15 Microphone ... 136
4.16.1.16 Vibration ... 139
4.16.1.17 Wireless Charging ... 140
4.16.1.18 Live Call ... 141
4.16.1.19 Battery Discharge ... 142
4.16.2 Automatic Sensor Tests ... 143
4.16.3 After tests are completed ... 144
4.16.4 Diagnosis Case Preselection Description ... 149
5. Reports 151
5.1 Download erasure or diagnose report ... 152
6. FAQ 157
6.1 OEM parts validation (iOS only) ... 159
6.2 Upload iOS Firmware ... 162
6.3 Two-Factor Authentication (2FA) ... 163
7. Release notes 167
8. Menu items 169
8.1 Overview ... 170


© 2026 Securaze GmbH

8.1.1 Login ... 170
8.1.1.1 Help ... 171
8.1.1.2 Options & Settings ... 174
8.1.1.2.1 General ... 175
8.1.1.2.2 Processing ... 176
8.1.1.2.3 Workflows ... 178
8.1.1.2.4 Printer ... 180
8.1.1.2.5 Network & Storage ... 181
8.1.1.2.6 Integrations ... 182
8.1.1.2.7 Tools ... 183
8.1.1.2.8 About ... 183
8.1.2 Pre-selection ... 183
8.1.2.1 Support ... 185
**8.2 Dashboard ... 185**
8.2.1 Menu ... 187
8.2.2 USB Hubs ... 190
8.2.2.1 General information ... 190
8.2.2.2 Setting up a USB hub ... 191
8.2.2.3 Managing hubs ... 195
8.2.3 Device details ... 196
**8.3 Data erasure ... 197**
8.3.1 iOS ... 198
8.3.1.1 Requirements ... 199
8.3.1.2 Erasure process ... 200
8.3.1.3 Problem solutions ... 201
8.3.2 Android ... 203
8.3.2.1 Requirements ... 203
8.3.2.1.1 Developer mode and USB debugging ... 204
8.3.2.1.2 Install via USB ... 205
8.3.2.2 Erasure process ... 205
8.3.2.3 Problem solutions ... 206
**9. Cheatsheet 209**
**10. Securaze Dashboard 215**
**10.1 Menu items ... 217**
10.1.1 Dashboard ... 217
10.1.1.1 Asset overview ... 217
10.1.2 Assets ... 219
10.1.2.1 Work ... 219
10.1.2.2 Mobile ... 220
10.1.2.3 Single disk-drives ... 221
10.1.2.4 Watch & Headphones ... 223
10.1.3 Reports ... 223
10.1.4 Logistic ... 226
10.1.4.1 Orders ... 226
10.1.4.1.1 Create new Orders ... 227
10.1.4.1.2 Edit Orders ... 227


© 2026 Securaze GmbH

10.1.4.1.3 Delete Orders ... 228
10.1.4.2 Lot ... 229
10.1.4.2.1 Create new Lot ... 229
10.1.4.2.2 Edit Lot ... 230
10.1.4.2.3 Delete Lot ... 231
10.1.4.3 Sale Lots ... 231
10.1.4.3.1 Create new Sale Lot ... 232
10.1.4.3.2 Edit Sale Lot ... 233
10.1.4.3.3 Delete Sale Lot ... 234
10.1.5 Download ... 235
10.1.6 Account Management ... 235
10.1.6.1 User ... 235
10.1.6.1.1 Create new Users ... 236
10.1.6.1.2 Edit User ... 237
10.1.6.1.3 Delete User ... 238
10.1.6.2 Roles ... 239
10.1.6.2.1 Create new Role ... 239
10.1.6.2.2 Edit Role ... 239
10.1.6.2.3 Delete Role ... 240
10.1.6.3 Customer ... 241
10.1.6.3.1 Details ... 242
10.1.7 Settings ... 244
10.1.7.1 Presets ... 244
10.1.7.1.1 General ... 244
10.1.7.1.2 Mobile ... 248
10.1.7.1.3 Work ... 250
10.1.7.1.4 Work Verifier ... 252
10.1.7.1.5 Single Disk-Drives ... 253
10.1.7.2 Installed software ... 253
10.1.7.3 Grading ... 255
10.1.7.3.1 Grades ... 256
10.1.7.3.2 Typical problems (Optional) ... 257
10.1.7.3.3 Operating Systems ... 257
10.1.7.3.4 Chassis Types ... 258
10.1.7.4 Report Customization ... 259
10.1.7.4.1 Logos ... 259
10.1.7.4.1.1 Create new Logo ... 260
10.1.7.4.1.2 Edit Logo ... 261
10.1.7.4.1.3 Delete Logo ... 262
10.1.7.4.2 Report Data ... 263
10.1.7.4.2.1 Create new Report Data ... 263
10.1.7.4.2.2 Edit Report Data ... 264
10.1.7.4.2.3 Delete Report Data ... 265
10.1.7.4.3 File Patterns ... 266
10.1.7.4.3.1 Create new File Pattern ... 266
10.1.7.4.3.2 Edit File Pattern ... 267
10.1.7.4.3.3 Delete File Pattern ... 268
10.1.7.5 SKU ... 269
10.1.7.5.1 SKU Pattern ... 269


© 2026 Securaze GmbH

10.1.7.5.2 SKU Mapping ..... 270
10.1.7.6 Printer ..... 271
10.1.7.6.1 Creating a new printer ..... 271
10.1.7.6.1.1 Printer Type ..... 272
10.1.7.6.1.1 Godex ..... 272
10.1.7.6.1.2 Zebra ..... 272
10.1.7.6.1.3 Brother ..... 272
10.1.7.6.1.2 Printer network adress (URL) ..... 272
10.1.7.6.1.3 Direct connected USB printer ..... 273
10.1.7.6.2 Edit printer ..... 273
10.1.7.6.3 Delete printer ..... 273
10.1.7.7 Network Zone ..... 274
10.1.7.8 Securaze Standards ..... 276
10.1.7.9 Securaze API ..... 277
10.1.7.9.1 Authentication & conventions ..... 279
10.1.7.9.2 Products ..... 279
10.1.7.9.3 Users ..... 280
10.1.7.9.4 Logistics ..... 280
10.1.7.9.5 Integrations & webhooks ..... 281
10.1.7.9.6 Testing & errors ..... 281
10.1.7.10 Further settings ..... 281
10.1.8 Statistic ..... 282

**Index** **0**


© 2026 Securaze GmbH

# Administration

# 1 Administration

## 1.1 System environment

### Prerequisites

- Windows: Windows 11 (64-bit).
- macOS: a Mac with Apple silicon and macOS 13 or later - see Mac below.
- Linux: nothing to prepare - the Mobile Linux Installer brings its own operating system (see Installation).


© 2026 Securaze GmbH

## System requirements

| | Minimum Configuration | Recommended Configuration | Production Configuration |
|---|---|---|---|
| **Dedicated for** | **Processing 1-10 devices simultaneously** | **Processing more than 10 devices simultaneously** | **Processing more than 20 devices simultaneously** |
| Operating system | Windows 11 or Mobile Linux Installer | Windows 11 or Mobile Linux Installer | Windows 11 or Mobile Linux Installer |
| CPU | 64Bit CPU (e.g. Intel i7 - 10th Gen) | 64Bit CPU (e.g. Intel i9 - 10th Gen) | 64Bit CPU (e.g. Core i9 - 10th gen or newer) |
| Graphic Card (GPU) | Onboard GPU | Dedicated GPU with 1 GB+ RAM | Dedicated GPU with 4 GB RAM |
| Memory (RAM) | 16 GB | 16 GB | 32 GB |
| Storage requirements | 256GB SSD | 512GB SSD | 1TB SSD |
| USB-Ports | USB 3.0 compatible ports | At least 1x PCI Express USB 3.0 interface/adapter<br>From recommended USB adapters list | At least 2x PCI Express USB 3.0 interface/adapter<br>From recommended USB adapters list |
| USB-Connection | 1x Professional grade 10 Port USB hub<br>From recommended USB hubs list | At least 1x Professional grade 20 Port USB hub<br>From recommended USB hubs list | At least 2-4x Professional Grade hubs independently connected to PCIe USB interface.<br>From recommended USB hubs list |


© 2026 Securaze GmbH

| | Minimum Configuration | Recommended Configuration | Production Configuration |
|---|---|---|---|
| Resolution | 1280 * 1024 resolution | 1920 * 1080 or higher | 1920 * 1080 or higher |
| Internet | 25 Mbps or higher | 50 Mbps or higher | 100 Mbps or higher |

**Processing more than 100 devices simultaneously**

For simultaneous mass processing (more than 100 devices) it is suggested to replicate PCs with Production Configuration and split the load on the installed Securaze Mobile machines.

**Mac**

Securaze Mobile runs on a Mac with Apple silicon and macOS 13 or later; Intel Macs are not supported. The memory, storage, USB hub, cable and internet recommendations above apply to a Mac as well; the PCI Express USB adapters are for Windows and Linux PCs.

A Mac that is to be erased is connected directly to one of the station's own USB-C ports, not through a hub or dock - see Erase a Mac.

| USB-Connection requirements | All Configurations |
|---|---|
| USB hubs | Professional grade USB hubs with external power supply<br>at least 900 mA per port (USB 3.0) are recommended; iPads and other tablets need 1.5 A per port. See list of our recommended USB hubs 16. |
| Devices per USB bus | It is recommended to connect up to 20 devices per USB bus. |
| USB cables | Use high-quality USB cables that carry data. Charge-only cables are not detected.<br>Lightning cables should be certified by Apple and have the "Made for iPod/iPhone/iPad" logo.<br>iPhone 15 and later, iPads and Android phones with USB-C need USB-C data cables. |


© 2026 Securaze GmbH

**Additional Recommendations**

- Avoid Notebooks due to USB & Power Draw limitations.
- Avoid Intel-U and Intel-T CPUs as they are not meant for heavy processing.
- Install only Securaze Mobile on the machine. Windows only: if a competitor's app or driver was installed, reinstall Windows before the first use of Securaze Mobile.


© 2026 Securaze GmbH

## Software settings

| Firewall settings | |
|---|---|
| Internet connection | Permanent Internet connection is required |
| Securaze servers | The firewall must allow traffic to the following Securaze pages:<br>• https / http to *.securaze.com<br>• https://cdn.securaze.icu<br>• https://securaze.blob.core.windows.net and https://securazeeu.blob.core.windows.net (downloads)<br>• https://o263587.ingest.sentry.io (error reports) |
| Allow Apple download pages | The firewall must allow traffic to the following Apple download pages:<br>• albert.apple.com<br>• appldnld.apple.com<br>• appldnld.apple.com.edgesuite.net<br>• appldnld.g.aaplimg.com<br>• captive.apple.com<br>• gs.apple.com<br>• gg.apple.com<br>• humb.apple.com<br>• itunes.apple.com<br>• mesu.apple.com<br>• ppq.apple.com<br>• skl.apple.com<br>• swcdn.apple.com<br>• swdist.apple.com<br>• swdownload.apple.com<br>• swquery.apple.com<br>• swscan.apple.com<br>• updates-http.cdn-apple.com<br>• updates.cdn-apple.com<br>• xp.apple.com<br>• *.itunes.apple.com<br>• *.apps.apple.com<br>• *.mzstatic.com |
| Remote Support | The firewall may have to be modified.<br>Securaze uses RustDesk for remote support. Allow outgoing connections to the Securaze remote-support server:<br>· connect.securaze.com (ID and relay server)<br>· TCP ports 21115 - 21119<br>· UDP port 21116 |
| Local DNS | if local DNS is used, it has to be correctly propagated:<br>· SSH port 22 in case of support issues |


© 2026 Securaze GmbH

| Firewall settings | |
|---|---|
| | · ICMP enabled to outside world (currently 8.8.8.8 is used) |


© 2026 Securaze GmbH

## 1.2 Hardware

The following USB hubs are on our preferred type list:

| Vendor | Model | Link |
|---|---|---|
| Sipolar | A-223<br>20 Port USB 3.0 HUB | Sipolar A-223 |
| Sipolar | Sipolar A-103<br>10 Port USB3.0 HUB | Sipolar A-103 |

### The Sipolar 20-port hub in Securaze Mobile

The Sipolar 20-port hub has two USB cables, so Securaze Mobile sees it as two 10-port hubs: one half with the ports printed USB1 to USB10, the other with the ports printed USB11 to USB20. Each half gets its own letter and its own sticker, and each half is one entry in Mobile - in the hub setup and in Manage hubs.

Mobile knows this hub. Its setup shows **Detected hub: Sipolar 20-port charging hub (one half)** and can number the ports in the order printed on the hub, without a phone in each port.

Plug in the cable of the USB1-USB10 half first and set it up, then the cable of the USB11-USB20 half. If the numbers come out swapped - the port printed USB1 shows as B11 - the halves were set up in the other order. With one such hub on the station, the check with one phone at the end of the setup puts them in order: the halves swap letters, and you swap their stickers. With two or more of these hubs on one station, set up the halves in order.

For any other hub, you map the ports by hand once - see Setting up a USB hub.

The following USB adapter PCI Express Cards are on our preferred type list:

| Vendor | Model | Link |
|---|---|---|
| Startech | PEXUSB312A3<br>2-port USB 3.1 Gen 2, USB-A PCIe Card | PEXUSB312A3 |
| Startech | PEXUSB312A2<br>2-port USB 3.1 Gen 2, USB-A PCIe Card | PEXUSB312A2 |
| Startech | PEXUSB3S44V<br>4-Port PCI Express, USB 3.0 Card | PEXUSB3S44V |

Please contact our sales or support team at support@securaze.com or sales@securaze.com if you need support with the purchase process.

## 1.3 Wireless network recommendations

During processing, test devices join your Wi-Fi network for diagnostics and activation. In a


© 2026 Securaze GmbH

facility that processes hundreds to thousands of devices per day, this creates a high-churn wireless environment: many short-lived clients joining and leaving constantly. A standard office network is usually not prepared for this.

## Key requirement: short DHCP lease times

Configure DHCP lease times of 1–5 minutes for the processing network. With default lease times (hours or days), the address pool fills up with devices that have long left the station, and new devices fail to obtain an IP address.

Note that many consumer all-in-one and mesh routers (e.g. Eero, Google Nest WiFi, consumer Netgear Nighthawk models) lock or severely restrict DHCP lease time configuration and are therefore not suitable for processing environments.

## Use access points, not all-in-one routers

For processing facilities we recommend an access-point-based network layered on top of your existing gateway (ISP modem, firewall or router), rather than a single all-in-one wireless router:

• Warehouse spaces are large – a single router rarely covers a full processing floor consistently.

• Device density is high – spreading devices across multiple access points prevents any single radio from becoming a bottleneck.

• You need to scale – access points can be added as the operation grows, without replacing the core infrastructure.

## Suitable hardware (examples)

Access points with full DHCP/VLAN control that have proven suitable for device processing:

• Entry: Ubiquiti UniFi U6 Lite (Wi-Fi 6, ~150 concurrent clients; requires the free UniFi Network Controller)

• Recommended: Ubiquiti UniFi U6 Pro (Wi-Fi 6, 300+ concurrent clients, VLAN segmentation, ceiling mount – the sweet spot for most processing floors); UniFi U6 Mesh where ceiling mounting is not practical

• High density / enterprise: Ubiquiti UniFi U6 Enterprise (Wi-Fi 6E – a dedicated 6 GHz band for test devices), Aruba Instant On AP25, or Cisco Meraki MR56 for large multi-site operations with dedicated IT teams

If the facility has no existing gateway: ASUS RT-AX58U / RT-AX88U Pro (DHCP lease configurable down to 1 minute) or Ubiquiti UniFi Dream Machine Pro as gateway – and let the access points handle the wireless.


© 2026 Securaze GmbH

### Sizing guide

• Up to 100 devices/day: 1–2 entry-level access points

• 100–500 devices/day: 2–4 U6 Pro class access points

• 500–2,000 devices/day: 4–8 U6 Pro / U6 Enterprise class access points

• 2,000+ devices/day: 8+ enterprise access points (U6 Enterprise / Meraki MR56)

### Deployment checklist

• DHCP lease time: 1–3 minutes on the processing SSID

• Dedicate the 5 GHz (or 6 GHz) band exclusively to test devices

• Size the DHCP pool for peak concurrent devices plus 20% buffer

• Isolate test devices from staff/office traffic via VLAN segmentation

• One access point per processing zone; avoid overlapping channels

• Allow the required outgoing connections (activation and remote support) as described in the System environment topic

## 1.4 Installation

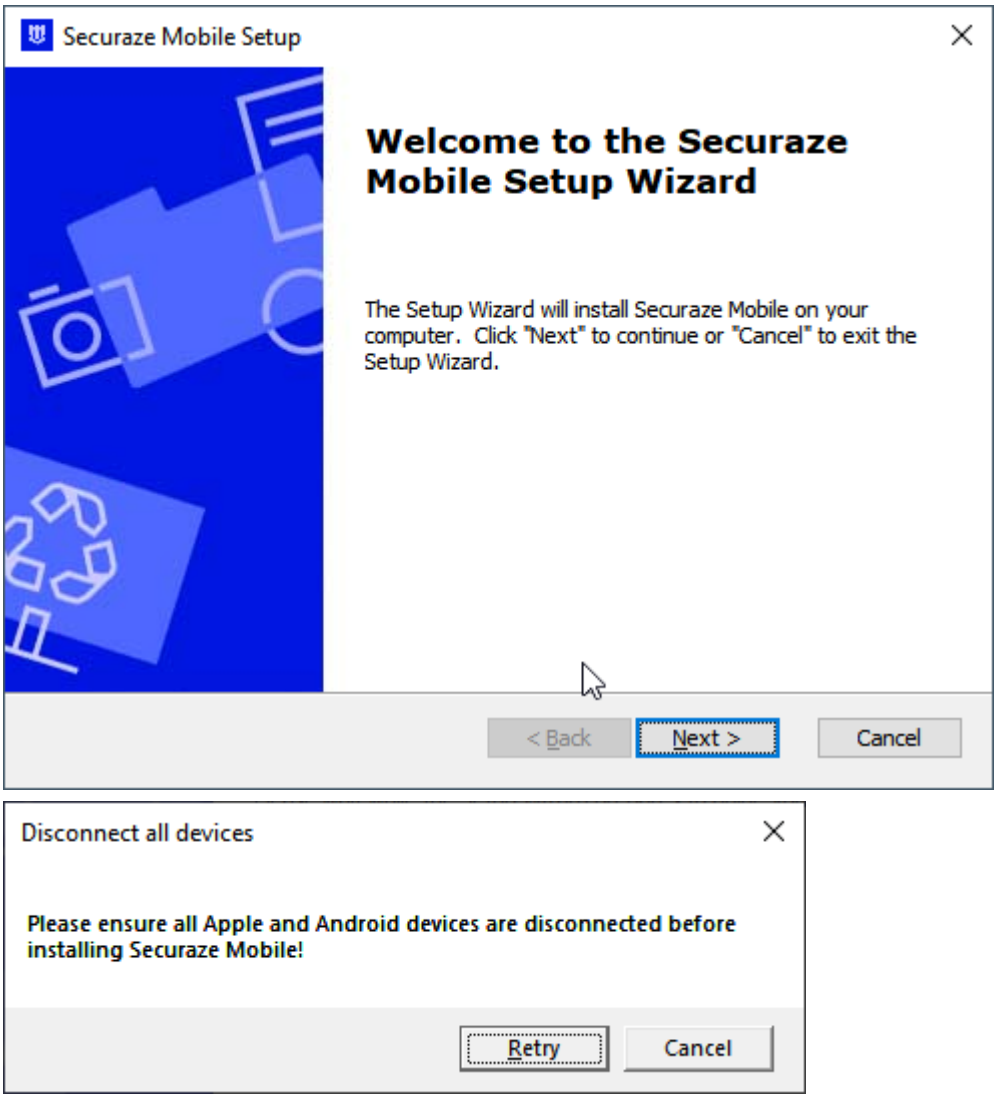
Download Securaze Mobile in the Securaze Dashboard under **Downloads > Mobile**: **Windows**, **macOS** or **Linux**. **Linux application** is the update package for a Linux station that is already installed.

### Windows

Run the installer, **Securaze Mobile-<version>_eu.exe** for the EU region. Windows asks for administrator rights.

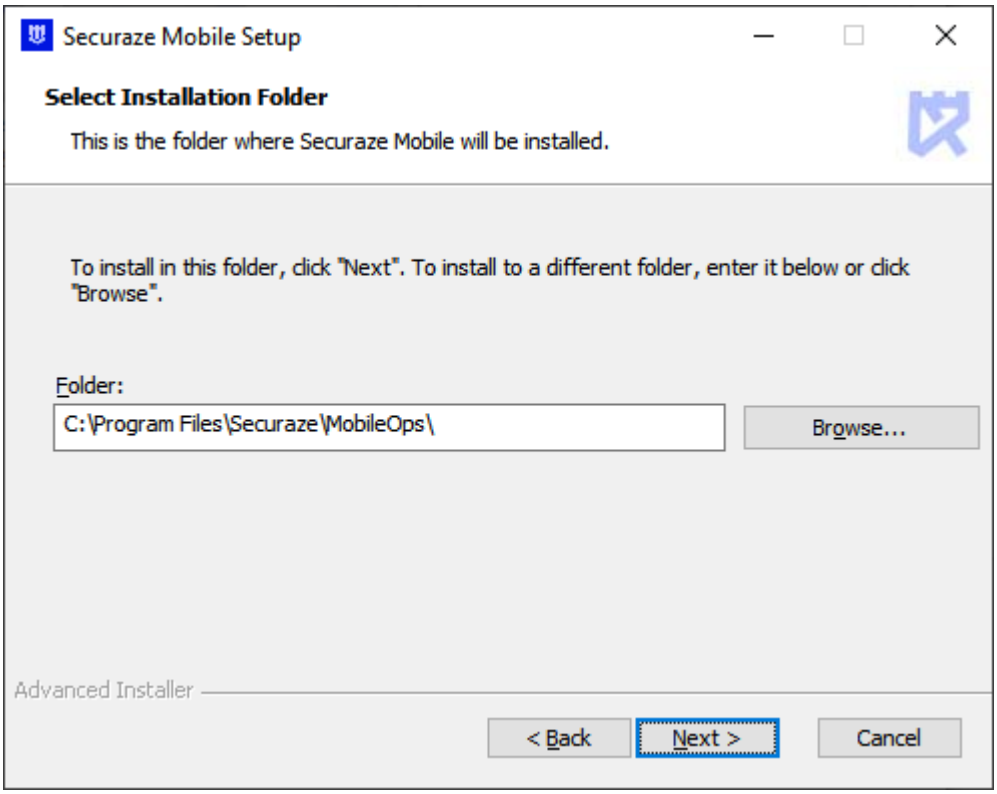
Unplug all phones, tablets and USB hubs first. The installer asks for it and then checks for connected Apple devices: **Retry** continues once they are unplugged, **Cancel** stops the installation.


© 2026 Securaze GmbH




The steps are Welcome, the optional features - **Remote Support** is ticked; untick it if this station is not to offer remote support - the installation folder (**C:\Program Files\Securaze\MobileOps** unless you choose another one) and Ready.


© 2026 Securaze GmbH




Besides Securaze Mobile, the installer sets up what it needs to talk to the devices: Apple Mobile Device Support and Apple's USB driver - it replaces Microsoft's Apple driver, which Windows Update then no longer installs -, the Android USB driver, adb and the Visual C++ runtime. iTunes is not needed. The installer also switches AutoPlay off.

For administrators: the installer takes the standard Windows Installer switches, for example **/qb!**. A silent installation does not check for connected devices - unplug them first.

#### Updates

After login, Securaze Mobile checks for a newer version in the release channel set under About. **Install now** runs the new installer and closes Securaze Mobile; it starts again when the installation is done. Settings, the stored data and the Remote Support choice are kept. You can also download the new installer from the Dashboard and run it.

## macOS

Securaze Mobile runs on a Mac with Apple silicon and macOS 13 or later; Intel Macs are not supported.

The download is a disk image, **SecurazeMobile-<version>_EU-macOS.dmg** for the EU region, signed and notarized by Securaze. Open it and drag Securaze Mobile into the **Applications** folder. Start it from there: started from the disk image or the Downloads folder, it shows **Move SecurazeMobile to Applications** and quits.


© 2026 Securaze GmbH

Each time it starts, Securaze Mobile asks for an administrator password - it needs administrator rights to manage the connected devices. **Continue** uses the password once; **Save & Continue** keeps it in the login keychain, so later starts do not ask again. If the saved password no longer works, it asks again. **Cancel** quits Securaze Mobile.

macOS asks once whether Securaze Mobile may use the microphone, and the camera, Bluetooth and the local network when they are first needed. Allow them.

Apple devices need no iTunes and no driver on a Mac. While Securaze Mobile runs, it stops Finder's own iPhone syncing and other Android tools (adb), so that they do not take the devices.

Set once in **System Settings > Privacy & Security**:

• **Allow accessories to connect**: **Automatically allow when unlocked**. Otherwise every restart of an iPhone during an erasure waits until someone clicks Allow. Securaze Mobile shows this with the first iPhone (**OPEN SETTINGS**). Keep the Mac unlocked while it processes.

• **Full Disk Access** for Securaze Mobile - Headphones mode needs it to recognize headphones quickly; Securaze Mobile shows **Full Disk Access is off** when it is missing.

To erase Macs from DFU, install Apple Configurator (free, Mac App Store) into Applications - see Erase a Mac.

#### Updates

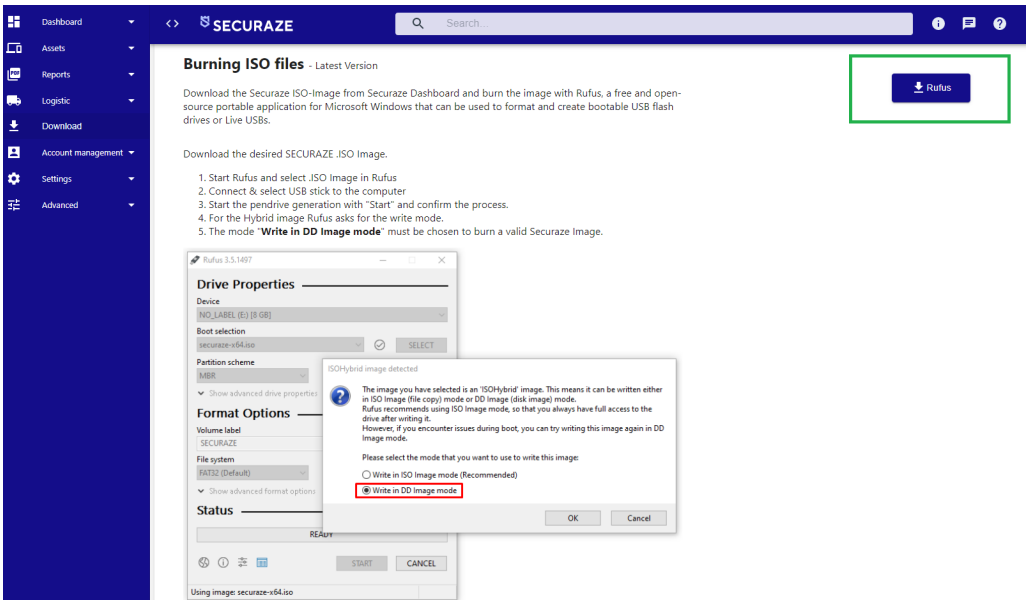
After login, Securaze Mobile checks for a newer version. **Install now** downloads it, checks that it is signed by Securaze and replaces the app; the window does not respond for about 15 seconds meanwhile. The path to Securaze Mobile must not contain spaces - the Applications folder is fine. You can also download the new disk image and drag Securaze Mobile into Applications again.

## Linux

Mobile Linux is a complete station: the Mobile Linux Installer puts Linux and Securaze Mobile onto the station's own disk. The download is the installer image **securaze-mobile-x64-<version>-eu.iso** for the EU region.

Write the image to a USB stick, for example with Rufus: select the image, choose the stick, click **Start** and choose **Write in DD Image mode** when Rufus asks.


© 2026 Securaze GmbH




Start the station from the stick. The installer opens with **Install Securaze Mobile Station** and lists the station's disks; the stick itself is not listed, and disks that are too small are marked. Choose the disk to install onto - it is erased completely - and click **Install (erases disk)**.

If the disk already holds a station, **Keep this Securaze Mobile Station's existing data & settings** is offered: **Install (keep data)** installs the system again and keeps the station's data and settings. A station that was installed with the earlier installer is not recognized as such - installing on it erases its data.

The installation shows its progress (**Show log** for the details). When it is done, remove the stick and click **Reboot now**; the station starts from its disk. **Need help?** on the installer page offers remote support, sending a system report and this manual.

### Updates

An installed station updates itself from Securaze Mobile (**Install now**), from a Securaze Command in the network if one is set up; settings are kept. The download **Linux application** (**securaze-mobile-x64-<version>-eu.zip**) is this update package - it runs inside an installed station and does not install one.


© 2026 Securaze GmbH

# Supported Device OS

# 2 Supported Device OS

In this chapter, we provide an overview of the device operating systems compatible with Securaze Mobile. Understanding the supported operating systems is crucial for effectively using the software for your device needs.

We will discuss the different erasure and diagnostic support options available for each compatible Android and iOS version. By the end of this chapter, you will have a clear understanding of the compatibility and capabilities of Securaze Mobile for various devices.

## Overview about Erasure and Diagnostics Support

| Device OS | Erasure Support | Diagnostics Support |
|---|---|---|
| Android 5.0+ | Data Clear, Smart Erasure, Advanced Erasure | Yes |
| iOS 6 up to iOS 10 | Data Clear, Smart Erasure | No |
| iOS 11+ | Data Clear, Smart Erasure, Advanced Erasure | Yes (Auto-Start App on device) |
| iOS 16+ | Data Clear, Smart Erasure, Advanced Erasure | Yes (Manual start of App on device) |
| iOS 26 | Data Clear, Smart Erasure, Advanced Erasure | Yes (Auto-Start App on device) |
| iOS 27 | Data Clear, Smart Erasure, Advanced Erasure | Yes |

## Android 5.0+ Compatibility

Securaze Mobile is compatible with Android devices running version 5.0 (Lollipop) and later.

The supported erasure and diagnostic options for these devices include Data Clear, Smart Erasure, Advanced Erasure, and comprehensive diagnostics support.

Android 16 and later, including Android 17, can be connected without USB debugging or developer mode: switch on **Android Express Mode** in **Options & Settings**, tab **Processing** (it is on by default). Such a phone shows its Android version as a lower bound, for example "Android 17+".


© 2026 Securaze GmbH

## iOS 6 up to iOS 10 Compatibility

Securaze Mobile is compatible with iOS devices running versions 6 through 10.

The supported erasure options for these devices include Data Clear and Smart Erasure. Diagnostics support is not available for iOS devices running versions 6 through 10.

## iOS 11+ Compatibility

Securaze Mobile is compatible with iOS devices running version 11 and later.

The supported erasure and diagnostic options for these devices include Data Clear, Smart Erasure, Advanced Erasure, and comprehensive diagnostics support.

The mobile application can be automatic started on the device.

## iOS 16+ Compatibility

Securaze Mobile is compatible with iOS devices running version 16 and later.

The supported erasure and diagnostic options for these devices include Data Clear, Smart Erasure, Advanced Erasure, and comprehensive diagnostics support.

The mobile application needs to be started manual on the device. (a warning appears and notifies the operator)

## iOS 26 Compatibility

Securaze Mobile fully supports iOS devices running iOS 26.

The supported erasure and diagnostic options include Data Clear, Smart Erasure, Advanced Erasure, and comprehensive diagnostics support.

On iOS 26 the mobile application can again be started automatically on the device (Auto-Start / skip hello screen is supported).

Advanced Erasure is available for iOS 26 devices; due to system restrictions of iOS 26, the overwrite covers up to 99.5% of the device storage.

## iOS 27 Compatibility

Securaze Mobile supports iOS devices running iOS 27 with Data Clear, Smart Erasure, Advanced Erasure and diagnostics.

Checking the battery of a device on iOS 27 for original parts needs Securaze Mobile 5.16.15 or later (see OEM parts validation 159).

## Supported Apple devices

The device database is updated continuously. Recently added Apple devices include:

• iPhone 17, iPhone 17 Pro, iPhone 17 Pro Max, iPhone Air and iPhone 17e


© 2026 Securaze GmbH

• iPhone 18 Pro, iPhone 18 Pro Max and iPhone Duo

• iPad Air M4 (11-inch and 13-inch, Wi-Fi and Wi-Fi + Cellular)

• macOS only: Macs with Apple silicon, erased in DFU mode - the MacBook Neo and the 2026 MacBook Air, MacBook Pro, Mac Studio and Mac mini models (see Erase a Mac 86)

Earlier additions include the iPhone 16 family (iPhone 16, 16 Plus, 16 Pro, 16 Pro Max and 16e) and the iPad Pro M4 models.


© 2026 Securaze GmbH

# Getting started

# 3 Getting started

Before you start with the first erasure operations, please configure some basic settings in Securaze Dashboard.

The settings which you make once before the first use of the erasure software are explained in Preparations 28 section.

In the area of recurring activities 38, the settings that you will make more often in the course of the application are dealt with. In addition, you will get an overview of the possibilities of storing customer-specific requirements for the deletion, which Securaze Mobile executes immediately after login.

## 3.1 Preparations

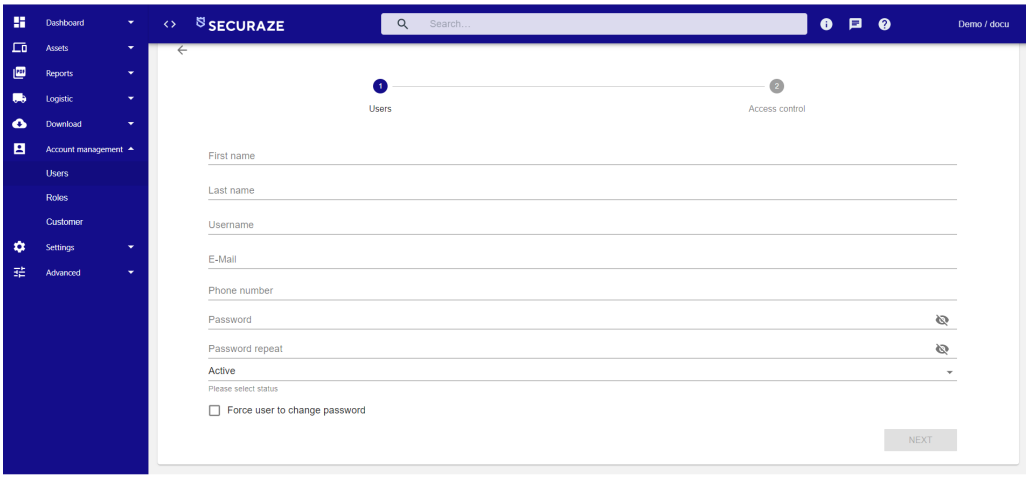
Before you start Securaze Mobile for the first time, make preparations in Securaze Dashboard.

### 3.1.1 Creating a new user

To create a new user, click on **Account management - Users** in the Menu area and then on + Create new

Here you enter the data of the new user and define a password.

By selecting the item **Force user to change password**, you assign a temporary password which the user must change after the first login.



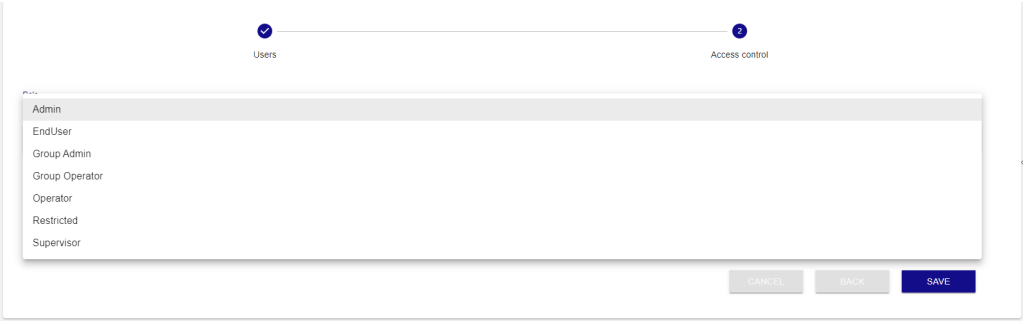

Confirm the entry of your data with **NEXT**.

In the next step, you select the authorization level of the user (the user's **role**).


© 2026 Securaze GmbH

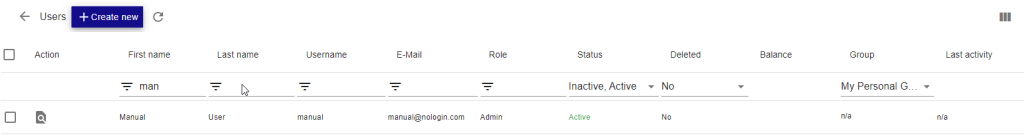
Each role has a predefined set of **permissions**, but additional permissions can be included, or excluded, if necessary.
Default system roles are: **Admin, Operator, Supervisor, End User** and **Restricted**.

Users with the Admin role have the possibility to create custom roles, and grant them a customized set of permissions.




*

After confirming your selection by clicking **SAVE**, the newly created user is visible in the **Users** menu.




For information on editing or deleting an existing user, see Securaze Dashboard - Menu Items - Users 235.

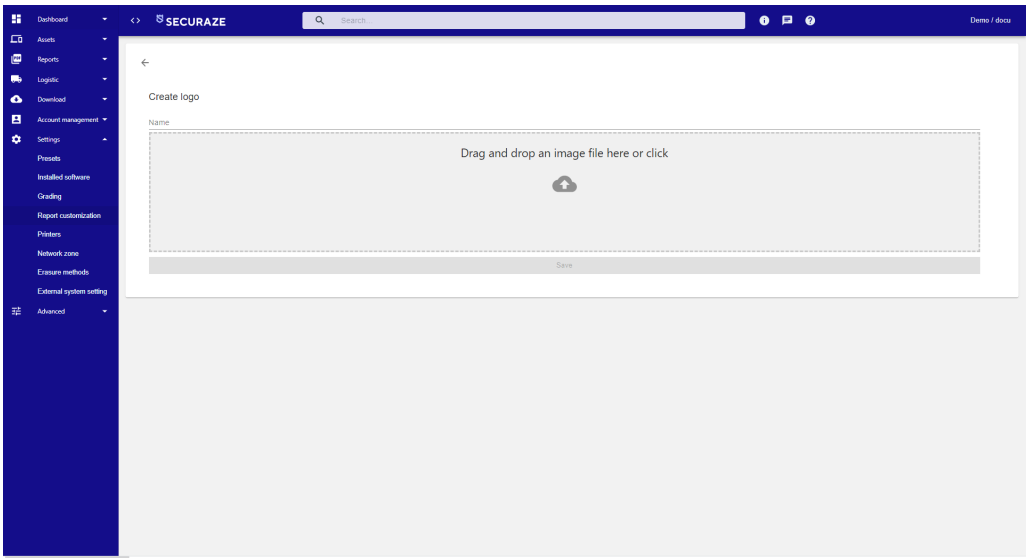
### 3.1.2 Create new logo

To create a new logo to be displayed on the erasure report, click on **Settings - Report customization** in the Menu section and then on the tab **LOGOS.**

There you select + Create new

Here you define the name of the logo (in **Name** box) and upload the desired logo image by clicking on upload box, or via drag and drop.


© 2026 Securaze GmbH



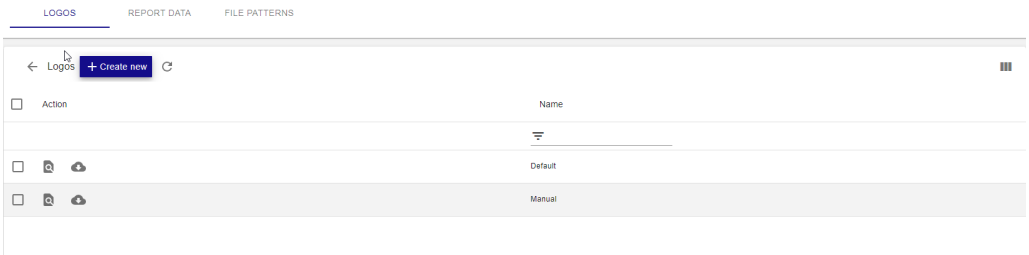

**Recommended size of the logo:**

Square shaped: 512 x 512 pixel

Rectangular shaped:
600 x 400 pixel

It is recommended to use a logo with a size of about 25kb, resolution 256 pixels at about 100 dpi. Otherwise the erasure reports will be very large.

After confirming the selection by clicking **SAVE**, the newly created logo is visible in the menu **Settings - Report customization** in the tab **LOGOS.**




For information on editing or deleting an existing logo, see Securaze Dashboard - Menu Items - Settings - Logos 259.

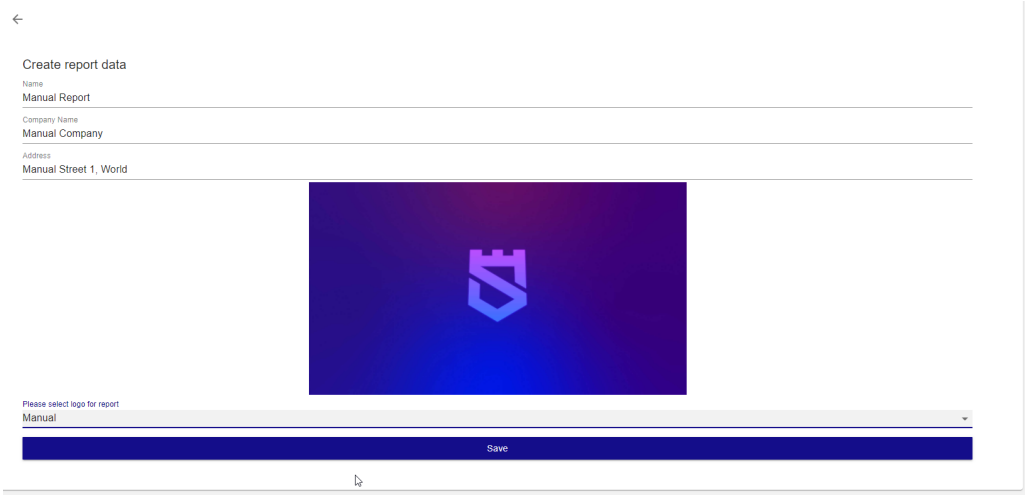

© 2026 Securaze GmbH

### 3.1.3 Create new report data

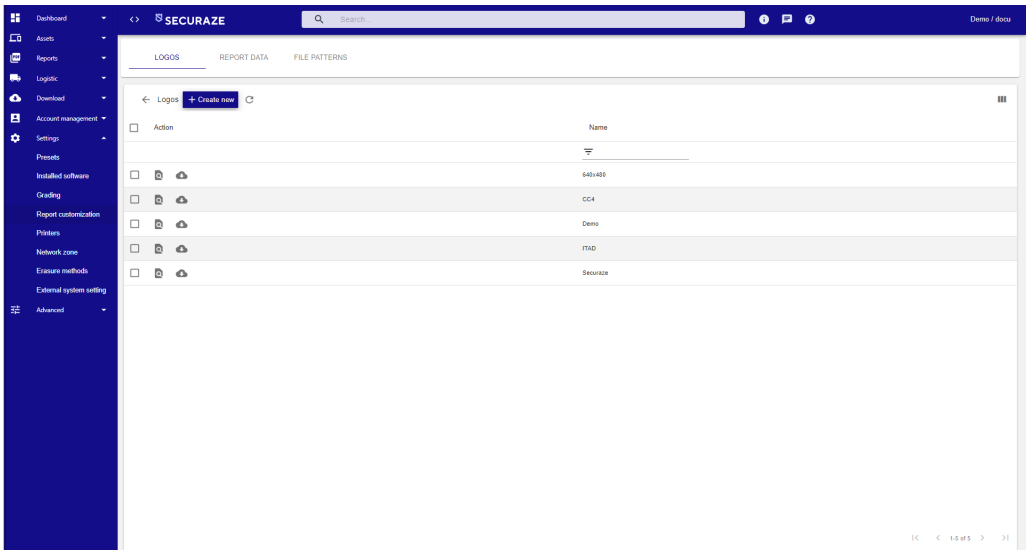
To create a new report data, click on **Settings - Report customization** in the Menu section and then on the tab **REPORT DATA.**

There you select + Create new

Here you enter the data that should appear on the erasure report and select the logo.




After confirming the selection by clicking **SAVE**, the newly created report data can be viewed in the menu **Settings - Report customization** in the tab **Report data.**




Information on editing or deleting already created report data can be found under Securaze Dashboard - Menu items - Settings - Report data 263.

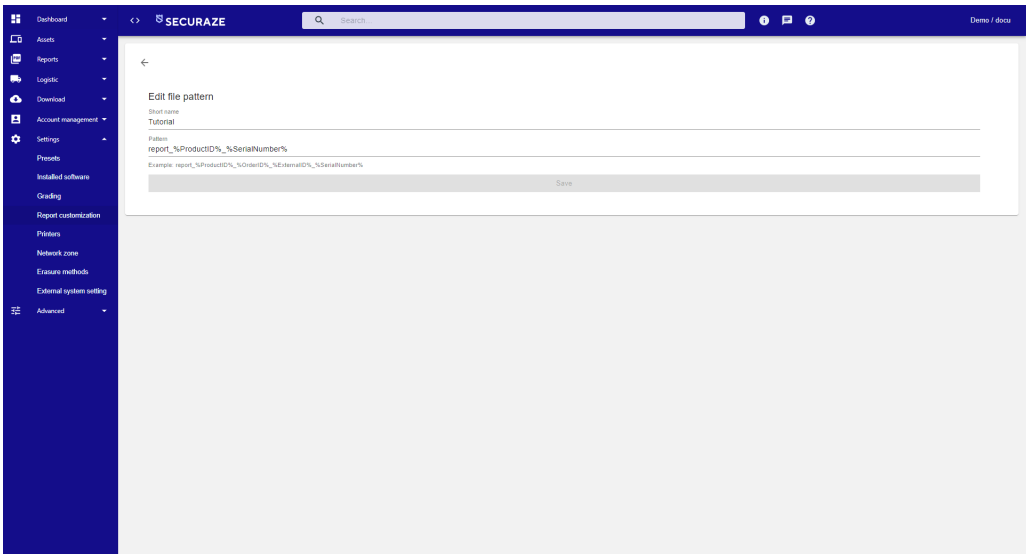

© 2026 Securaze GmbH

### 3.1.4 Create new file name pattern

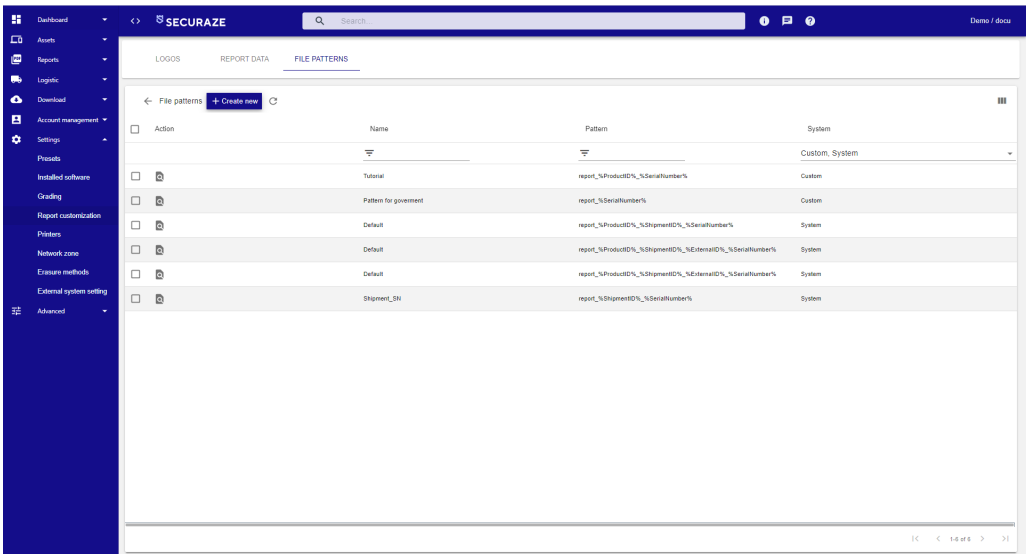
To create a new file pattern, click on **Settings - Report customization** in the Menu section and then on the tab **FILE PATTERNS.**

There you select + Create new

Here you assign a name and a pattern for the file name under which you can save erasure reports in the future.




After confirming the selection by clicking **SAVE**, the new pattern created is visible in the menu **Settings - Report customization** in the tab **File Name Pattern**.



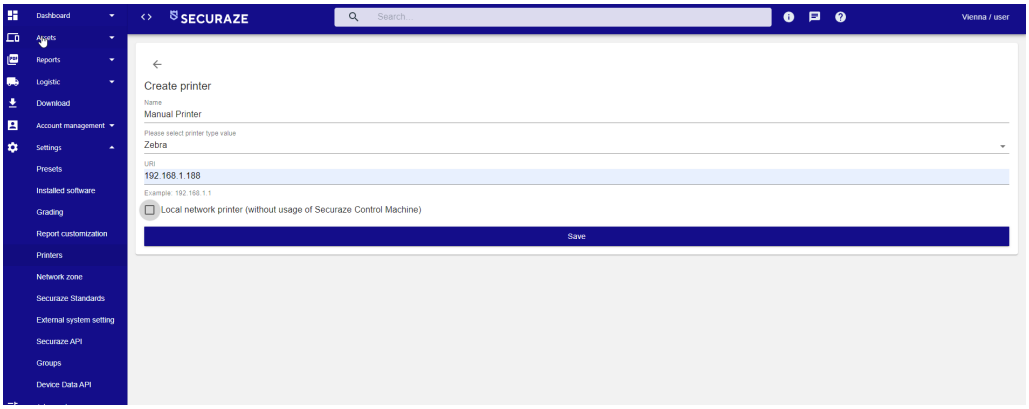


© 2026 Securaze GmbH

### 3.1.5 Creating a new printer

To create a new printer, click on **Settings - Printers** in the menu and then on + Create new

Here you enter the name of the printer and select the printer type from the list.




At the moment, Securaze supports Brother, GoDex, Zebra and DYMO label printers, excluding Zebra ZSB series (small office / home printers), due to their limitations.

The following GoDex printers are supported:

RT700 / RT730

RT700x / RT730x

RT700i / RT730i

RT700iW / RT730iW

RT200 / RT230

RT200i / RT230i

RT863i

GE300 / GE330

G500 with Ethernet / G530 with Ethernet

DT2x / DT4x

The following Brother printers are supported: QL-810W and QL-820NWB, and - connected by USB - QL-800 and QL-700.

The server sends Brother labels in the ESC/P format. The QL-800 and QL-700 do not understand it, so Securaze Mobile draws their labels and sends them as raster. Which format a printer gets follows from its model. To set it yourself, put "Raster" or "ESC/P" in the printer's name: a printer whose name contains "Raster" always gets raster, one whose name contains "ESC/P" always gets ESC/P.


© 2026 Securaze GmbH

DYMO LabelWriter printers are supported when they are connected by USB:

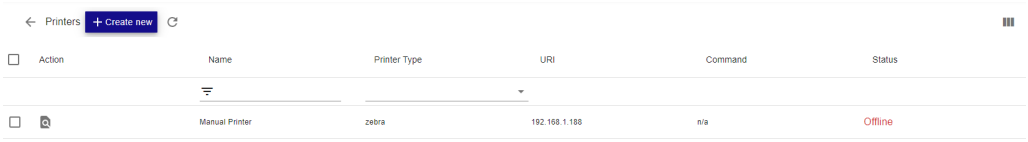
• Windows only: install DYMO Connect and keep it running - Securaze Mobile prints through it. Without it, Securaze Mobile says what is missing, for example "No Windows driver for the DYMO label printer is installed. Install DYMO Connect (dymo.com), then print the labels again." or, when DYMO Connect is not running, "Printer driver/software not installed. Install printer drivers."

• macOS only: install DYMO Connect for Mac (dymo.com) - it brings the printer driver. Securaze Mobile draws the label itself and prints it through that driver; DYMO Connect does not have to be running. Without the driver, Securaze Mobile says "No DYMO printer driver is installed on this Mac. Install DYMO Connect for Mac (dymo.com), which brings the driver, then print the labels again."

• Linux only: Securaze Mobile draws the label itself and sends it to the printer; DYMO Connect is not needed.

If a label does not print, Securaze Mobile says why instead of counting it as printed, for example "Printer (name) out of labels.", "Printer (name) cover open.", "Printer (name) did not print: ..." or "Printer (name) not connected.", together with what to do, such as "Load a new label roll, then print the label again." The message also stays in the **Infrastructure issues** list, which you open from the header.

After confirming the selection by clicking **SAVE**, the newly created printer is visible in the **Settings - Printers** menu.




To edit or delete an existing printer, refer to Securaze Dashboard - Menu Items - Settings - Printers 271.

## 3.2 External Systems

### 3.2.1 Re-trigger data sending

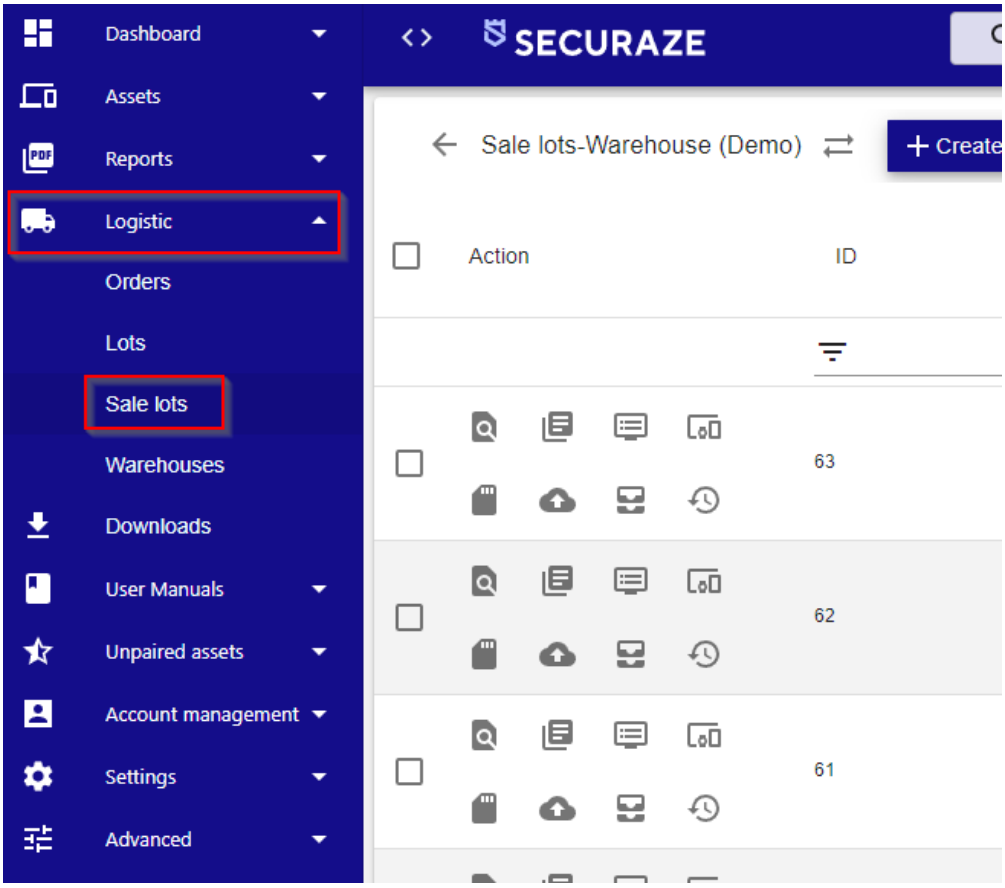
If for any reason diagnose and erasure data was not sent to your integrated external system, there is a way for you to manually re-trigger this process.

This can be done by asset (you can find the exact asset in Securaze Dashboard in the tab Assets - Work / Mobile / Single-disk drives) or by Sale Lot (so erasure data for all the assets from a particular Sale Lot can be re-sent to the external system).

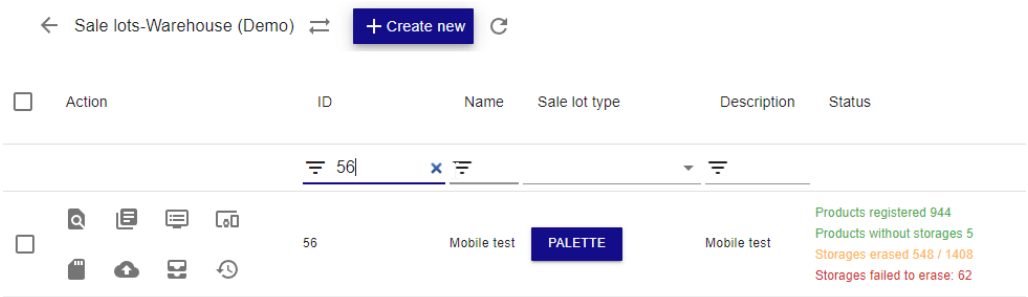
To perform the re-triggering by Sale Lots, follow these steps:


© 2026 Securaze GmbH

1. Go to your **Securaze Dashboard**, and in the left sidebar menu select **Logistic**, and then **Sale Lots.**



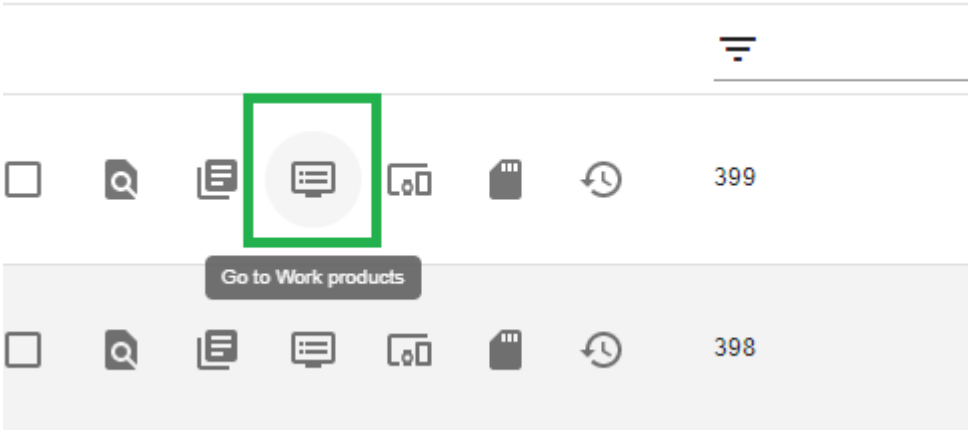

2. Search for the Sale Lot by ID, Name or Description.



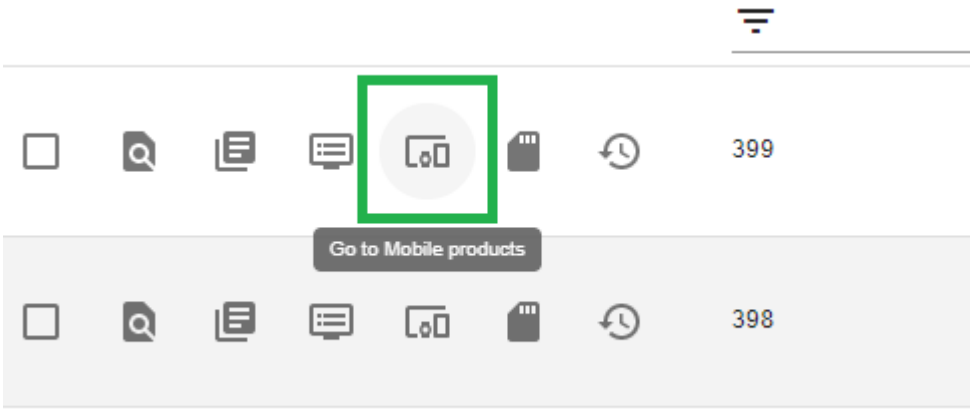

3. After you have found the Sale Lot, depending on what assets are included, select the button to go to:


© 2026 Securaze GmbH

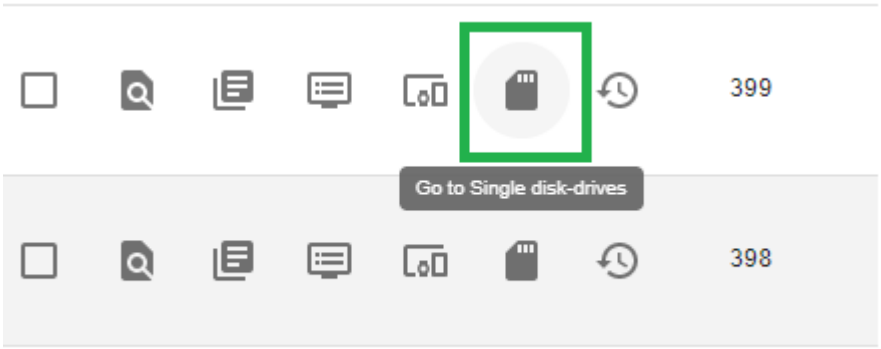
a) Work products (PCs, laptops etc.):




b) Mobile products (Smart phones, tablets etc):




c) Single disk-drives (single disks):

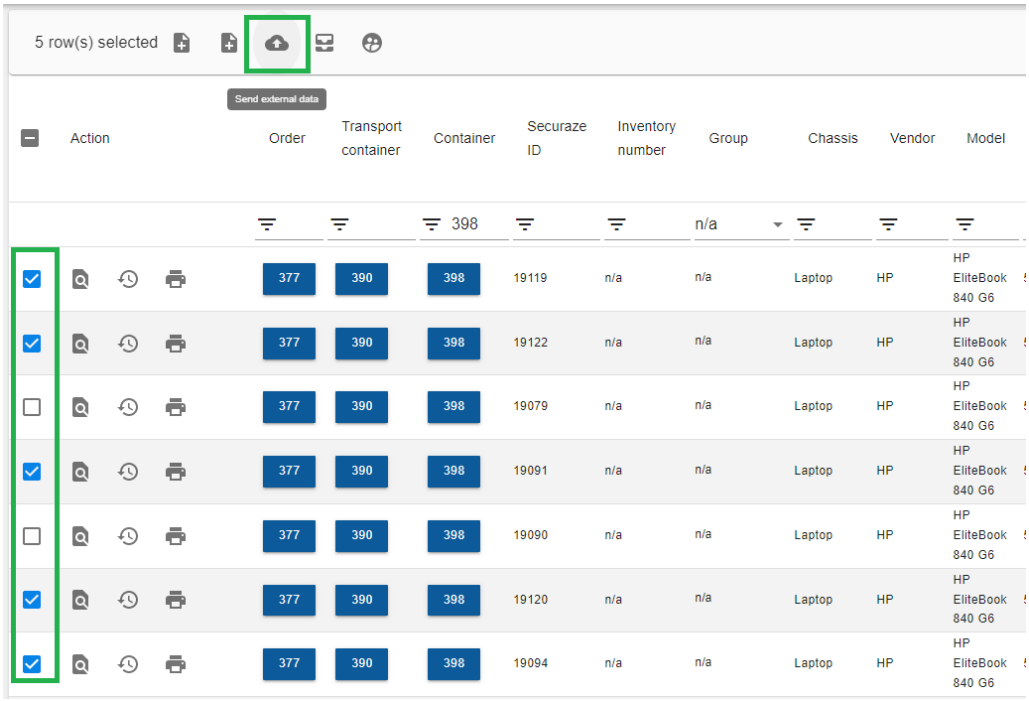




© 2026 Securaze GmbH

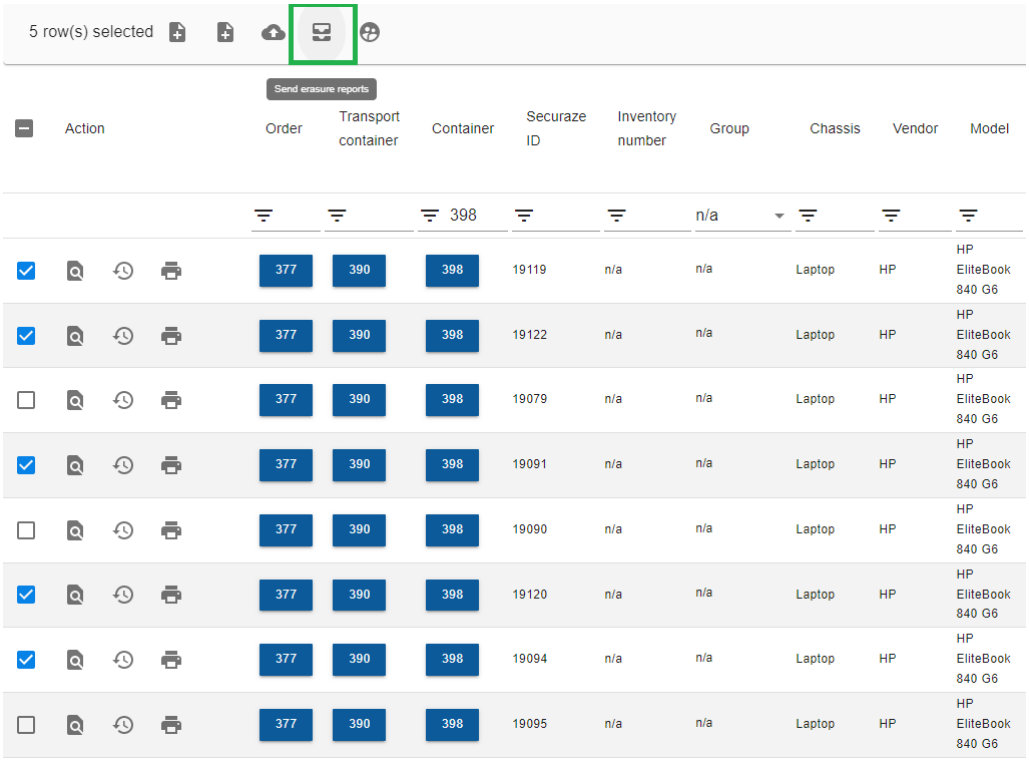
4. In case you have selected Work product, you will be taken to a list of these assets within the selected Sale Lot, where you can select manually number of assets, or all of the assets on that page by clicking on check box next to "Action".

After you have selected the assets, in the upper part of the screen you will be able to click on button "Send external data".




5. After this action has been successfully performed, click on button "Send erasure reports", to generate the diagnose / erasure reports for these assets and send them to the external system as well.


© 2026 Securaze GmbH




This may take a few minutes, depending on the number of assets in the Sale Lot. If there are more assets than the maximum number of displayed assets per page (100), make sure to go onto every page and repeat the actions.

## 3.3 Recurring operations

During the operation of Securaze Mobile, some recurring activities are performed in Securaze Dashboard.

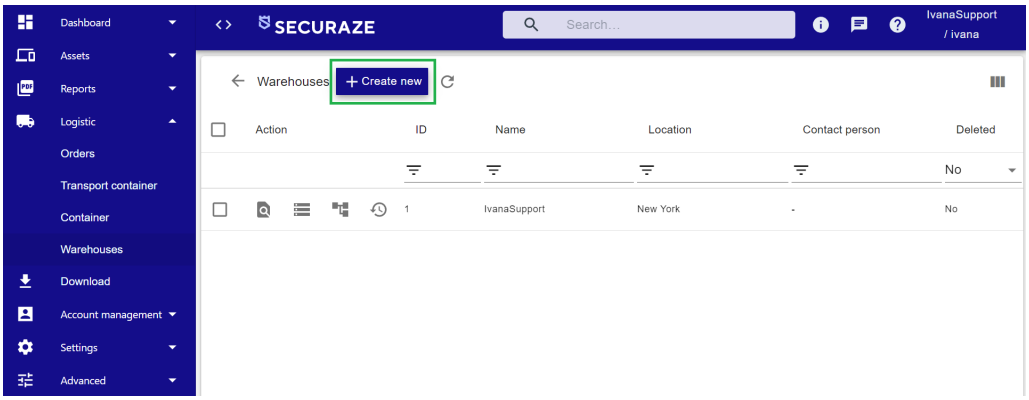
### 3.3.1 Create a new Warehouse

**Warehouses**

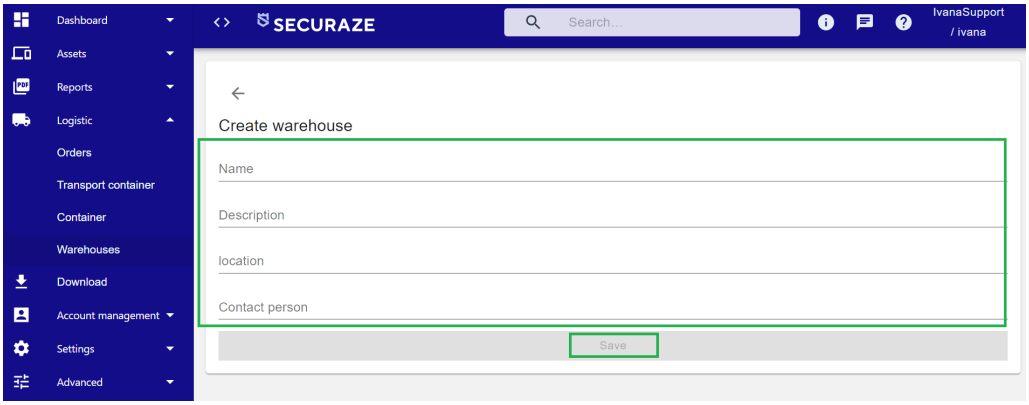
The first component needed in the logistics section to allow a clean workflow of receiving, processing, storing and sending out assets is a warehouse.

This tab can be found in the Dashboard, in the left sidebar menu, under Logistics.

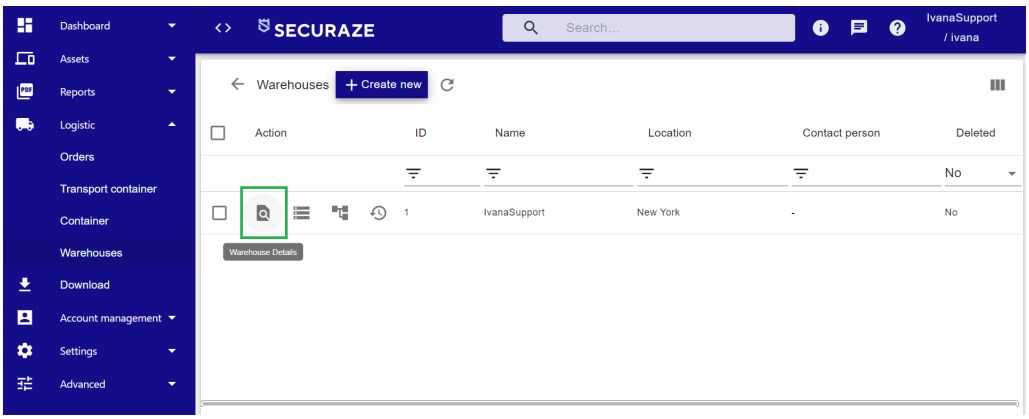

© 2026 Securaze GmbH




You can create a new Warehouse by clicking on **+ Create new** button.
In this new window you can type in the name, description, location and contact person for the warehouse.
After you are done filling in the information, click on **Save** button.




In case you want to edit the information about any warehouse, you can simply click on **Warehouse Details** button, and you will be taken to the details page.
When editing is completed, you should click on **Save** button.





© 2026 Securaze GmbH

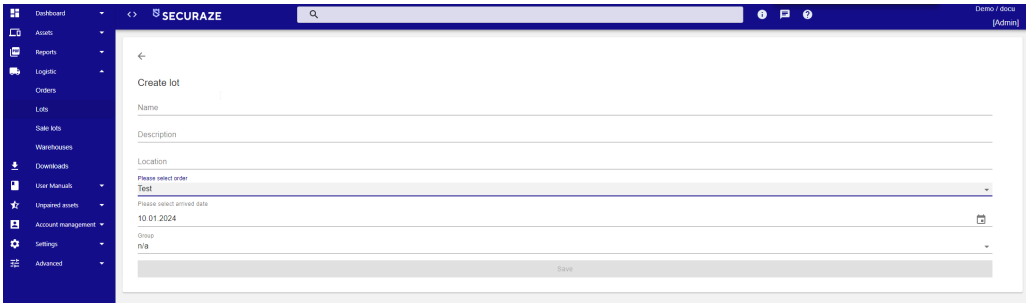
### 3.3.2 Create a new Lot

Each time you start an erasure or diagnostic session, you will be asked to select the Sale Lot. This Sale Lot is the Lot to which the asset in question was assigned.
The Lot is the Sale Lot on which the assets were delivered to you.

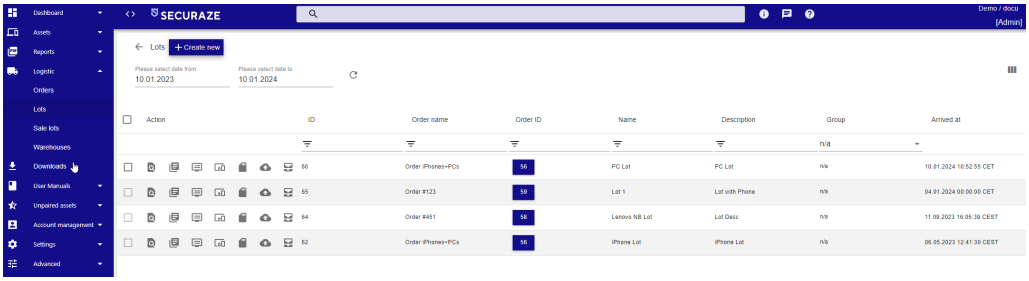
These Lots can be created in Dashboard, under Logistics – Lot.
By using the concept of Lot and orders you are able to split the assets into smaller pieces so they are easier to handle and track during daily operation.

To create a new Lot, click on **Logistic - Lot** in the Menu section and then click + Create new

Here you enter the name, description and location of the Lot and select the order and arrival date.




After confirming the selection by clicking **SAVE**, the newly created Lot is visible in the menu **Logistic - Lot**.



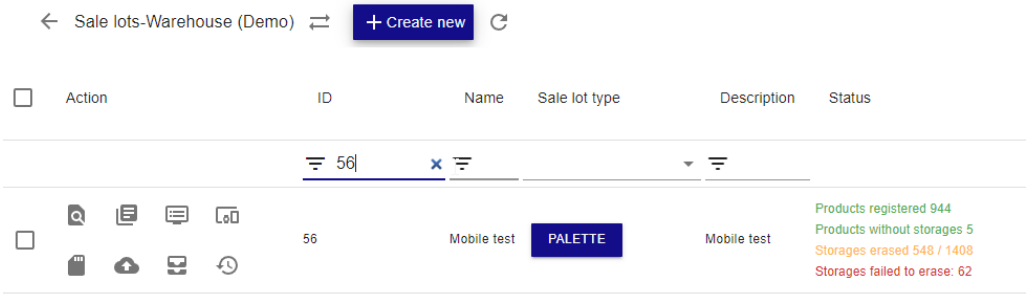

For more information on Lots, see Securaze Dashboard - Menu Items - Lot 229.

### 3.3.3 Create a new Sale Lot

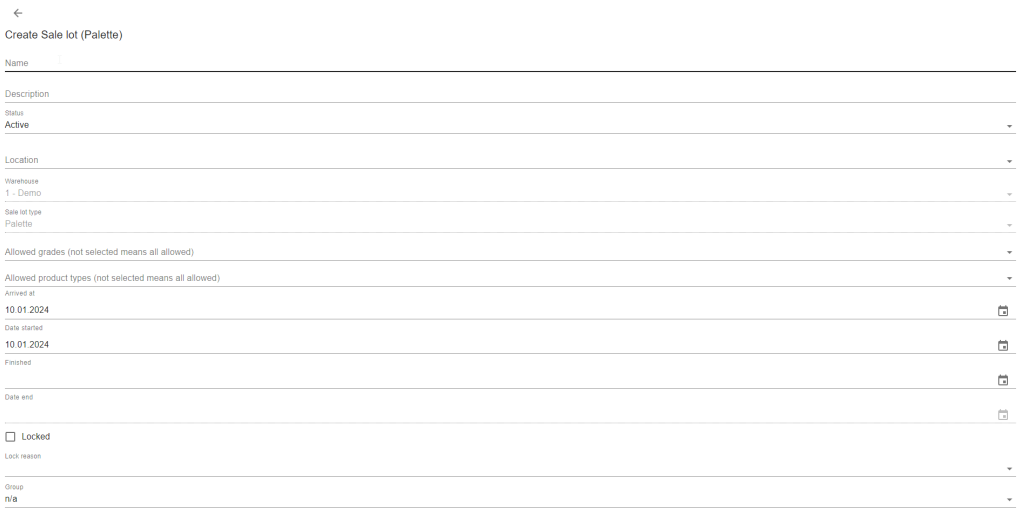
To create a new Sale Lot, click on **Logistic - Sale Lots** in the Menu section and then on

+ Create new


© 2026 Securaze GmbH




Here you enter the name, description and location of the Sale Lot and select the date.




After confirming the selection by clicking **SAVE**, the newly created Sale Lot is visible in the menu **Logistic - Sale Lots**.

For more information on Sale Lots, please refer to Securaze Dashboard - Menu items - Sale Lots 231.

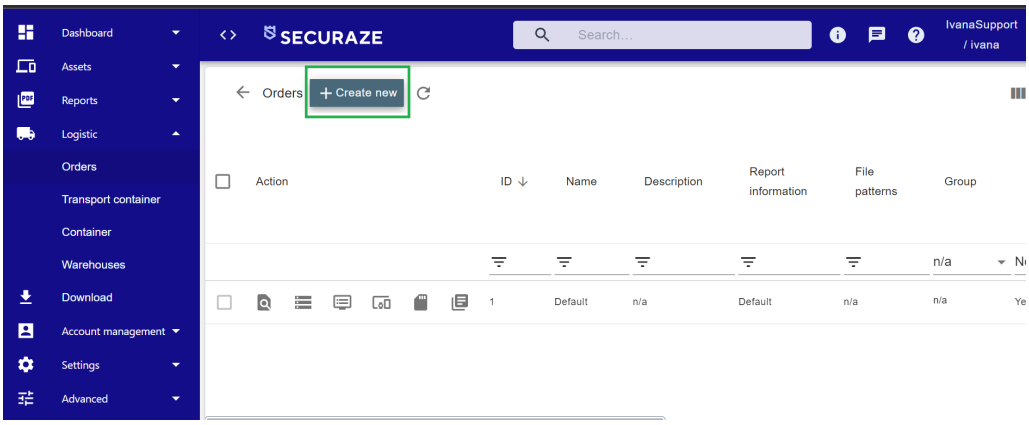
### 3.3.4 Creating a new Order

To create a new order, click on **Logistic - Orders** in the Menu section and then on

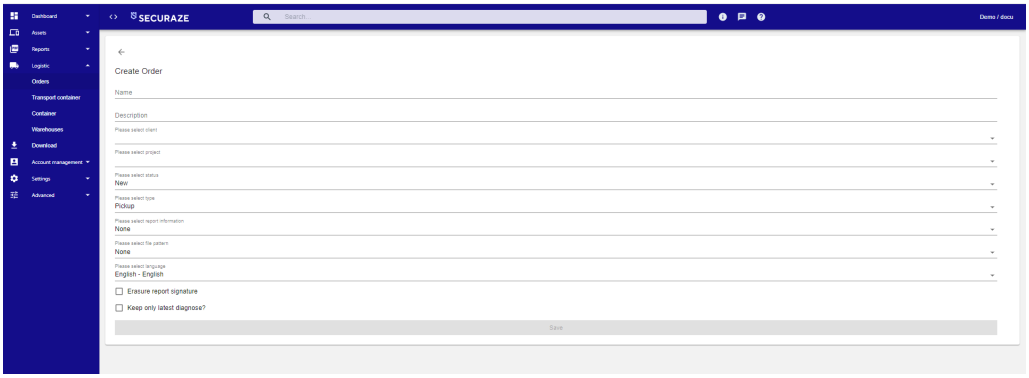




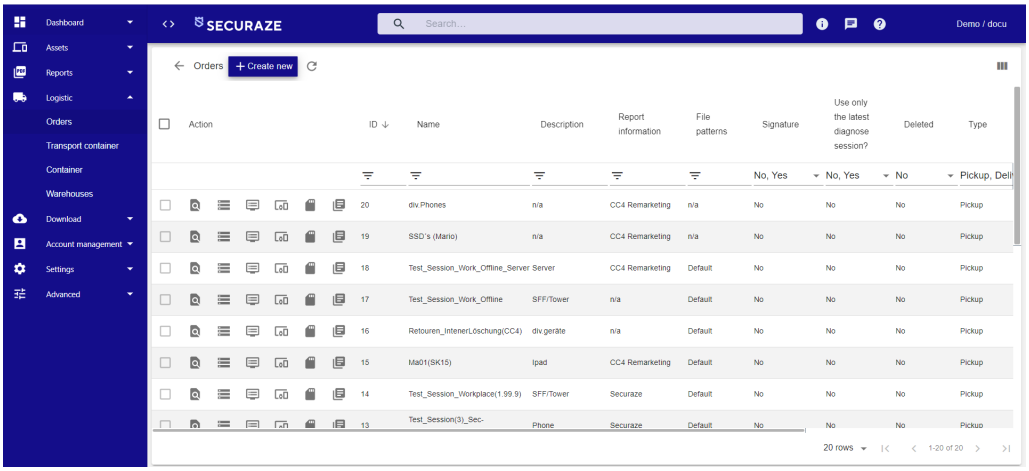
© 2026 Securaze GmbH




Enter the name and description of the order and select the report information and file name pattern you entered.

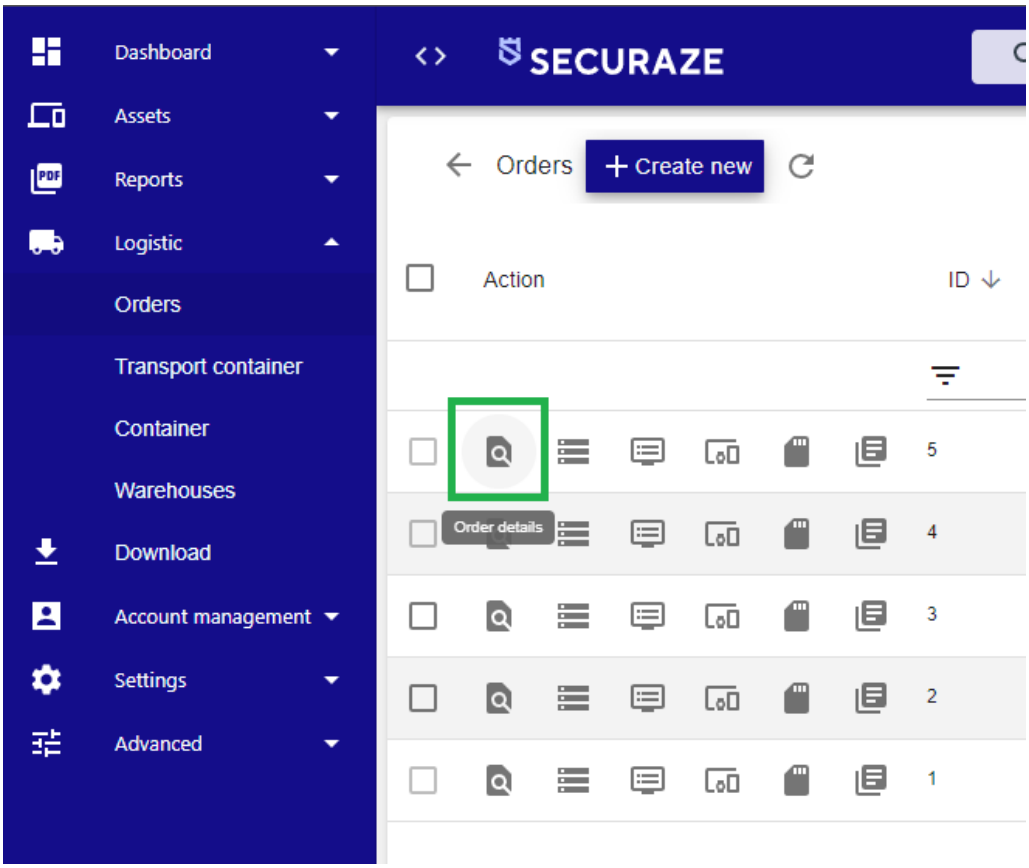



After confirming the selection by clicking on **SAVE**, the newly created order can be seen in the menu **Orders.**

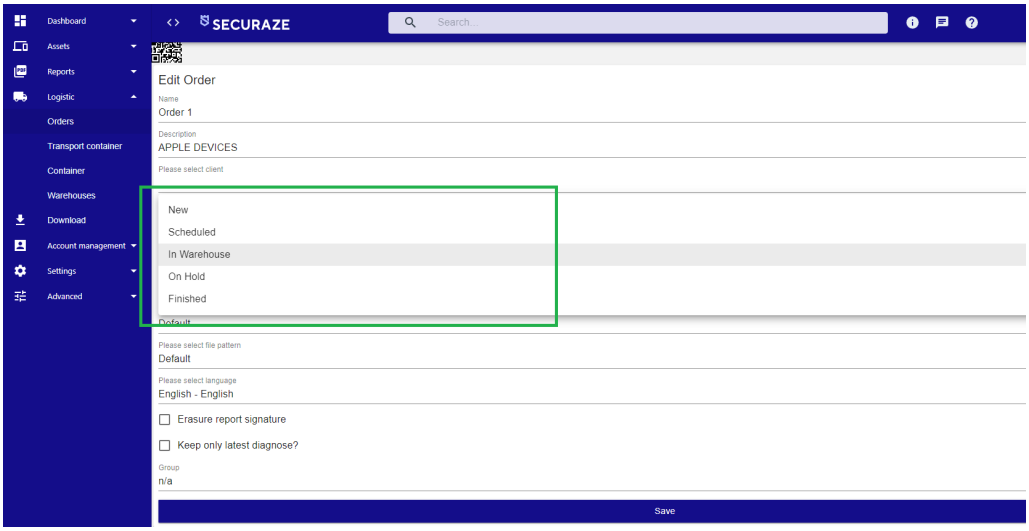



At any point, you can edit Order details, by clicking on Order details button:


© 2026 Securaze GmbH




Most common change you will make is the status:




For more information on orders, see Securaze Dashboard - Menu Items - Orders 226


© 2026 Securaze GmbH

### 3.3.5 Set presets

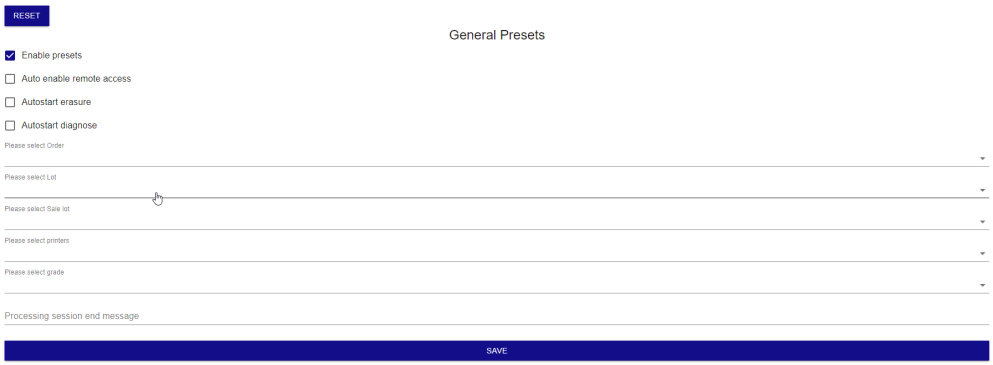
To define specific settings that Securaze should execute immediately after login, click on **Settings - Presets - General** in the Menu section.
Before you can make the desired settings, click **Enable preset**.

**Order** - select the desired order from the list.

**Lot** - select the desired Lot from the list.

**Sale Lot** - select the desired Sale Lot from the list.

After that, you can make the following preset settings for Mobile in Menu section **Settings - Presets - Mobile**:



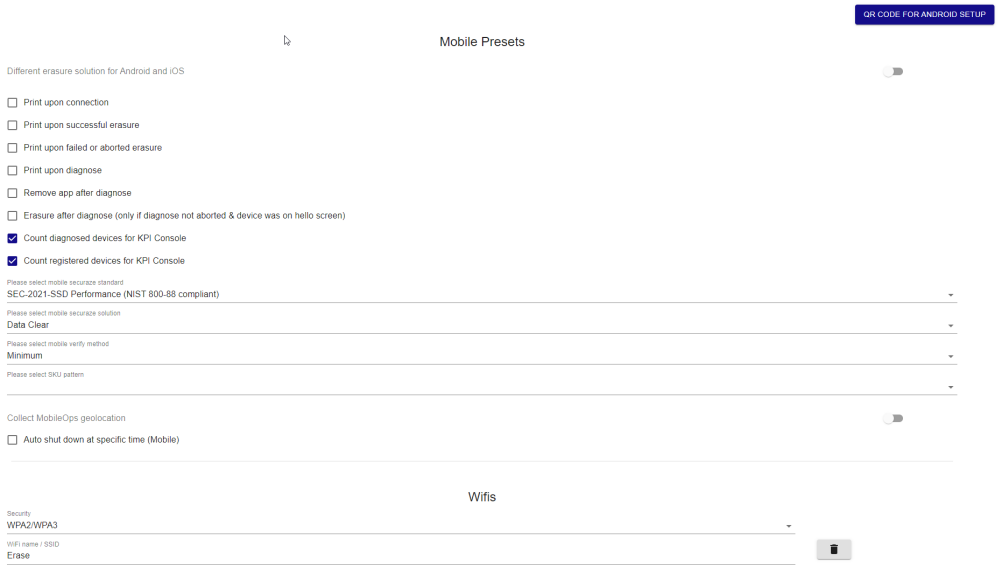

| Setting | Description |
|---|---|
| Print upon connection | Print a label on connection of a device. |
| Print upon successful erasure | Print a label on successful erasure. |
| Print upon failed or aborted erasure | Print a label on failed or aborted erasure. |
| Print upon diagnose | Print a label on diagnose of a device. |
| Print upon successful erasure | Print a label on successful erasure. |
| Remove app after diagnose | Remove the Securaze app from the device after the diagnose, when no erasure follows. |
| Erasure after diagnose | Erase the device by itself after a diagnose in which all tests passed. iPhones only when Find My is off and the setup (hello) screen was skipped. |


© 2026 Securaze GmbH

| Setting | Description |
|---|---|
| Count diagnosed devices for KPI Console | Count diagnosed devices for the KPI Console. |
| Count registered devices for KPI Console | Count registered devices for the KPI Console. |
| Please select mobile securaze standard | Default value for the Securaze Standard. |
| Please select mobile securaze solution | Default value for the Securaze Solution. |
| Please select mobile verify method | Select the desired verification method from the list. |
| Select SKU pattern | Select a custom SKU pattern which can be defined in Settings / SKU in advance. |
| Collect MobileOps geolocation | Collects the geolocation of the device in the moment of processing the device. |
| Auto shut down at specific time | Shutdown the Mobile station at a specific time to save energy after working hours. |
| Wifis | Define the wifi(s) which should be used when processing the devices.<br>It is mandatory for iOS diagnose and iOS Advanced erasure.<br>And it can be used for generating QR-Codes for faster Android USB-Debugging bypass.<br>For iOS, open Wifi networks without a password can also be used for provisioning the devices. |
| QR Code for Android Setup | This functionality allows to send the QR-Code for Android setup via mail. |
| | |
| | |

The diagnose settings **Remove app after diagnose** and **Erasure after diagnose** apply only on stations that do not run workflows. On a station with workflows, the workflow decides what happens after the diagnose.


© 2026 Securaze GmbH




Set your settings and confirm the entry with **SAVE.**


© 2026 Securaze GmbH

# Operation

# 4 Operation

After you have made all the settings, you can now start Securaze Mobile and perform erasures.

## 4.1 Login

After Securaze Mobile has been installed on the station (see Installation), start it. It opens with the login screen: **Hello, who's this ?**

macOS only: before the login screen, Securaze Mobile asks for the password of your macOS administrator user - see Login 170 in the chapter Menu items.

### Log in

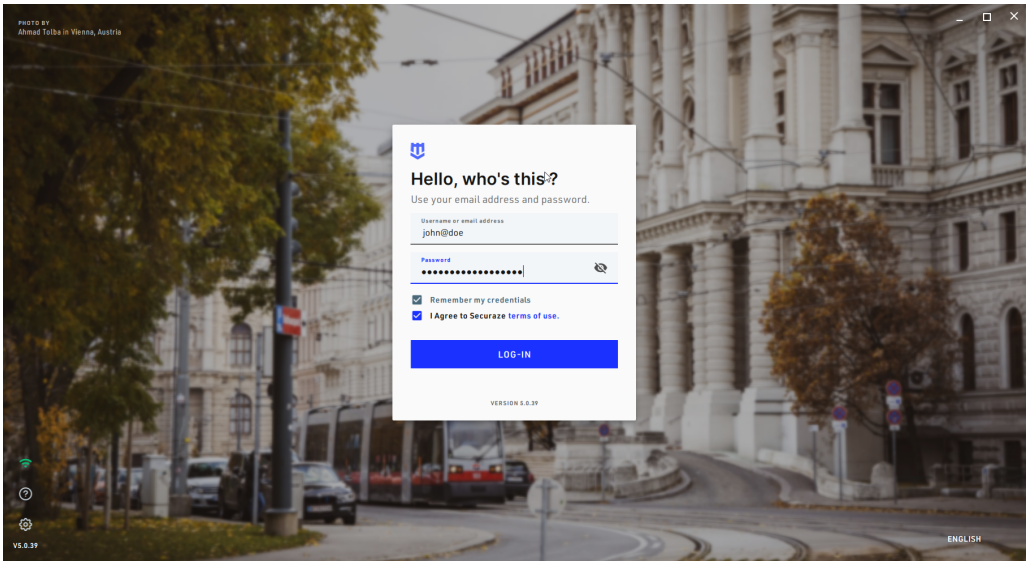
1. If you want to work in another language, change it now: click the language at the bottom right of the screen and choose one from the list. After the login, the language cannot be changed.

2. Type your user name or e-mail address in **Username or email address** and your password in **Password**. Your administrator gives you the user.

3. As soon as you type, two check boxes and the **LOG-IN** button appear. To have Securaze Mobile fill in your user name and password next time, tick **Remember my credentials**.

4. Leave **I Agree to Securaze terms of use.** ticked - you cannot log in without it. Click **terms of use** to read them.

5. Click **LOG-IN** or press Enter.




If the login fails, the reason appears under the title. If the station has no connection to the Securaze server, check the network and try again.


© 2026 Securaze GmbH

### Language

The list offers 40 languages, each shown in its own name and in English. The language of the station's operating system is at the top; the other languages follow below a line, in alphabetical order.

### Settings

Settings are in the sidebar on the left: **General settings** (F9). You can open them before the login as well. See Options & Settings 49.

### After the login

Securaze Mobile asks for what this session needs - for example the company, the workflow, the Lot and the Sale Lot - and then opens the dashboard. See Pre-selection 183, Select Lot 52 and Select Sale Lot 53.

Everything else on the login screen, for example the messages when the login fails and the release notes after an update, is described in Login 170 in the chapter Menu items.

## 4.2 Options & Settings

Click **General settings** (the gear icon) in the sidebar or press **F9**. The window **Options & Settings** has these tabs:

General 175 - screen resolution, scaling, language, card view, expert modes, station ID, hubs and port layout

Processing 176 - how devices are handled: unplugging, erasure retries, Android and iOS options, diagnose

Workflows 178 - run this station from workflows, import workflows

Printer 180 - print server and preferred printer

Network & Storage 181 - Securaze backend, data folder, iOS firmware copy

Integrations 182 - robot integration

Tools 183 - additional programs for the station (Linux only)

About 183 - version, Coming Soon, release channel

Some settings change how the whole station works. They are grayed out unless you are logged in as a user whose role allows changing the Mobile settings. In this manual they are marked (settings permission). The **Tools** tab can only be opened by such a user.

Some settings can only be changed before you log in, for example **Language**.


© 2026 Securaze GmbH

## 4.3 Workflows

A workflow is the process the phones on this station go through: what happens to each phone and in what order - for example what is checked, what is erased and when a label is printed. Workflows are drawn in the workflow editor.

When a phone is plugged in, the workflow takes it over and runs its steps. It asks you only where a step needs you.

Securaze Mobile gets its workflows from a workflow server, if one is set up for the station, or from workflow files imported in **Options & Settings** > **Workflows**. Workflows run only while **Run this station from workflows** is on in that tab. There you also set **Workflow this station runs**: a station set to one workflow runs it, and nobody is asked. See the topic about the Workflows tab in Options & Settings.

### Choose a workflow after login

If several workflows can run on this station and none is set for it, Securaze Mobile asks after login, before the lot: **Select the process the phones in this session go through.** If only one can run, it runs without asking.

• Click a workflow, press its number (1 to 9), or use the arrow keys and Enter. The list starts on the workflow chosen last time.

• To work without a workflow, click **Skip — no workflow** or press Esc. The phones are then worked by hand: nothing is tested, printed or erased by itself.

The list shows only the workflows that can run on this station. You are asked again at the next login and when the station's setting changes. If the chosen workflow is no longer there, the list comes up again.

### The workflow beside the station name

The header shows the running workflow in a pill beside the station name, with a tree icon. After **Skip — no workflow** it says **No workflow**.

Click the pill to change the workflow. Where the operator does not choose the workflow, the pill opens **Options & Settings** > **Workflows** instead.

### Change the workflow

Click **Change workflow** (Ctrl+Shift+W) in the sidebar, or click the pill. The list says **Select the process for the phones you plug in next. Phones already running finish with theirs.** The running workflow is marked **Running now**.

• Click another workflow to run it.

• **Keep** and the workflow's name (Esc) keeps the running one.


© 2026 Securaze GmbH

• **No workflow** works the next phones by hand.

A change applies to the phones you plug in next. A phone already in a workflow finishes with the workflow it started with.

**Change workflow** is shown only where the operator chooses the workflow.

## The workflow on the tile

In the Detailed card view each tile has a Workflow tab (lightning icon). The tile switches to it when a run starts, when a step waits for you, and when the run finishes or fails. You can go to the other tabs at any time.

The Workflow tab shows:

• **WORKFLOW** - where the run stands: **Running**, **Waiting for** and the step, **Finished**, **Failed** or **Stopped**. Before the first run: **No workflow has run on this device yet.** While the workflow erases the phone, the erasure's progress is shown here.

• **NEXT** - the next steps, or **End of the workflow**.

• **STEPS** - the run from **Start** to **End**, the newest step at the bottom.

• **RUN AGAIN** - runs the workflow on this phone again from the beginning, once nothing runs.

• **STOP WORKFLOW** - stops the workflow on this phone and gives the phone back to you. What the station already did, such as an erasure under way, is not undone.

• **SHOW RESULTS** - shows a finished grading or test again.

In the Standard card view the tile shows the lightning icon. Click it to open the workflow in the device details (**WORKFLOW**).

To see the Workflow tab on every tile at once, click **All tiles** in the sidebar and choose **Workflow** (Detailed card view).

## When a step waits for you

Some steps wait for the operator - a question, a grading or manual tests. Then:

• On a detailed tile, the Workflow tab shows the step, and its lightning icon gets an orange dot.

• On a standard tile, an orange strip **Workflow waits for you** appears. Click **OPEN** to answer the step in the device details. For a grading or manual tests the lightning icon is highlighted as well (**A workflow step waits for you - click to open it**).

• In the device details, **WORKFLOW** gets the orange dot.

Answer the step, and the workflow goes on.


© 2026 Securaze GmbH

### Safe test mode

To try a workflow out on this station, switch on the **Safe test mode** check box in **Options & Settings** > **Workflows** (see Workflows 178). It is there only while **Run this station from workflows** is on.

While safe test mode is on, a yellow bar at the top of every screen says **Safe test mode – workflow steps that would erase, reset, report or save are only simulated**. The workflows run as usual, but no phone is erased or reset by a workflow step, no report is sent, grades and test results are not recorded, and station settings are changed for this session only.

• **Switch off** in the bar ends safe test mode. It also ends when you log out and when workflows are switched off.

• Each phone's workflow keeps the mode it started in: a run that started in safe test mode stays simulated until it ends, and a run that started before stays real.

• Safe test mode covers workflow steps only. An erasure you start by hand, for example with **ERASE SELECTED**, erases the phone for real.

## 4.4 Select Lot

After the login, Securaze Mobile asks where the devices of this session come from. The screen **Lot** (**1 of 2**) lists the Lots from the Securaze Dashboard.

The Lot is where the devices you process in this session are now - usually the Lot they were delivered on. Securaze Mobile assigns the devices of this session to this Lot.

Lots are created in the Securaze Dashboard. There a Lot can belong to a Pickup Order, the collection the devices came from. See Create new Lots 40.

### Select the Lot

1. Find the Lot. The list shows **ID**, **Lot** and **Description**. Long lists are split into pages; the Left and Right arrow keys switch pages. With more than nine Lots, the search icon at the bottom opens a search field: type a search term and press Enter.

2. Click the Lot, press its number (1 to 9), or move to it with the arrow keys and press Enter.

Securaze Mobile then asks for the Sale Lot - see Select Sale Lot 53.

**Updated ... ago** shows when the list was loaded. If a Lot is missing, press **F5** to load the list again.

If the Securaze Dashboard preset sets a Lot, Securaze Mobile skips this screen. See Set presets 44.


© 2026 Securaze GmbH

To change the Lot later without logging out, click **Change lot** (Ctrl+Shift+L) in the sidebar. See Pre-selection 183.

## 4.5 Select Sale Lot

After the Lot, Securaze Mobile asks where the devices of this session go after processing. The screen **Sale Lot** (**2 of 2**) lists the Sale Lots from the Securaze Dashboard.

The Sale Lot is the container or storage area in your company or warehouse where the devices are stored after processing. Securaze Mobile assigns the devices of this session to this Sale Lot.

Sale Lots are created in the Securaze Dashboard, where they group devices for resale or return. See Create a new Sale Lot 40.

### Select the Sale Lot

1. Find the Sale Lot. The list shows **ID**, **Name**, **Description** and **Type**. Long lists are split into pages; the Left and Right arrow keys switch pages. With more than nine Sale Lots, the search icon at the bottom opens a search field: type a search term and press Enter.

2. Click the Sale Lot, press its number (1 to 9), or move to it with the arrow keys and press Enter.

Securaze Mobile then opens the dashboard - see Dashboard 185. If **AUTO-START ERASURE** is on in the Securaze Dashboard, a warning comes first - see Pre-selection 183.

**Updated ... ago** shows when the list was loaded. If a Sale Lot is missing, press **F5** to load the list again.

If the Securaze Dashboard preset sets a Sale Lot, Securaze Mobile skips this screen. See Set presets 44.

To change the Sale Lot later without logging out, click **Change lot** (Ctrl+Shift+L) in the sidebar. The Lot screen opens first; **Keep** with the current name (Esc) keeps the Lot in use, then you choose the Sale Lot. See Pre-selection 183.

## 4.6 Exit

Click your user name (**User Profile**) at the bottom of the sidebar, then **Exit**. The dialog **Ready to exit ?** opens. Any running processes are interrupted, which could leave devices corrupted.

Windows and macOS: **EXIT** (Enter) closes Securaze Mobile.

Linux only: the first button is **LOGOUT** (Enter) - Securaze Mobile closes and starts again.

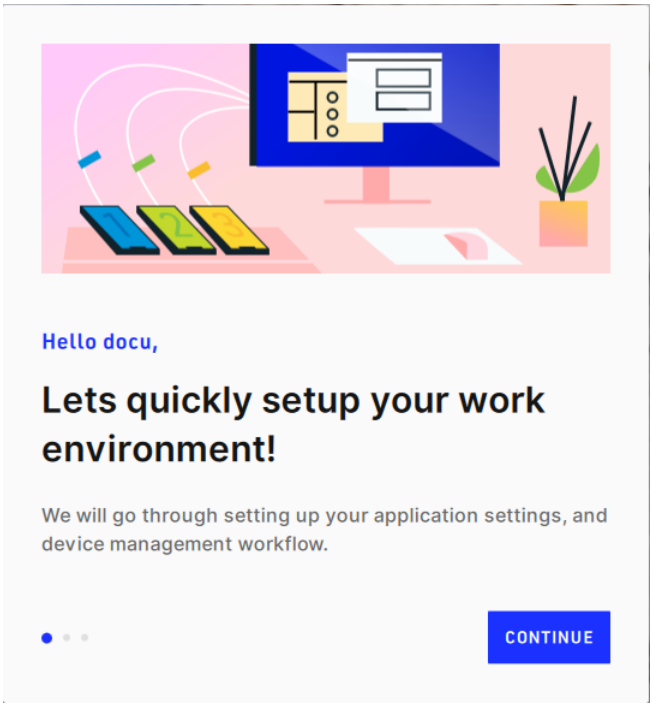
**REBOOT** (Ctrl+R) restarts the computer.

**SHUT-DOWN** (Ctrl+S) shuts the computer down.


© 2026 Securaze GmbH

## 4.7 Connect devices

After login a quick setup will start.

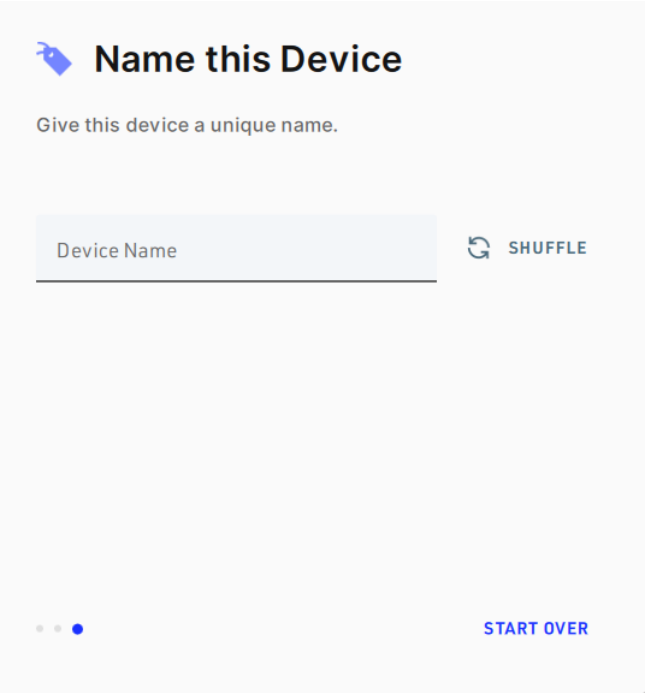



License selection:

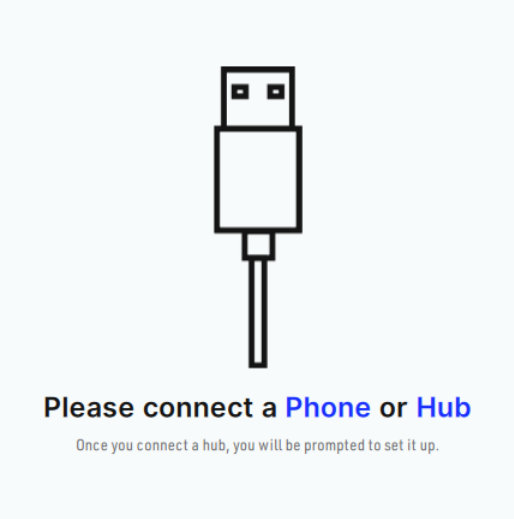
Select the license you want to use with this station. Besides the standard Mobile licenses, the license type **Mobile Lite Erasure** is supported, which provides a reduced erasure-only feature set.

Here you can name your device or select a name by clicking on **SHUFFLE.**
This device name is used in erasure reports.


© 2026 Securaze GmbH



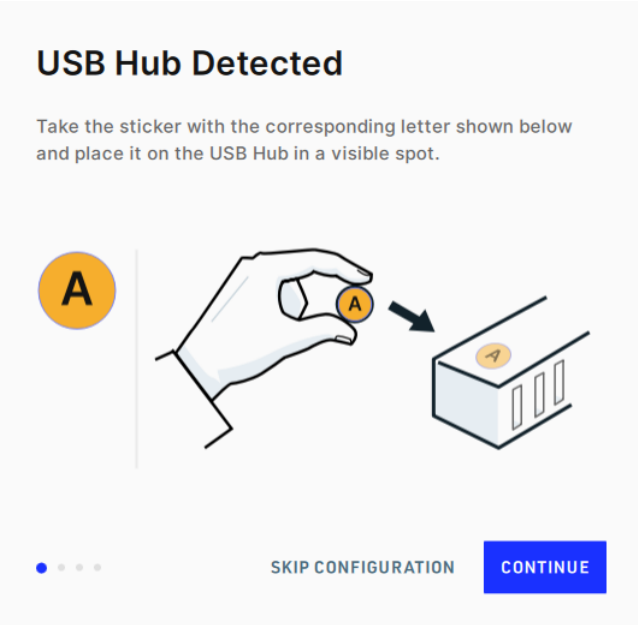

After that, your device is ready and you can connect a phone or hub.

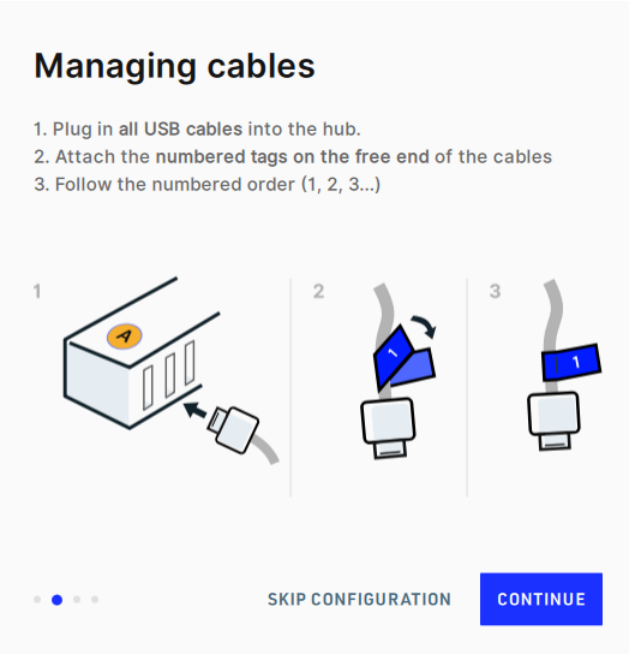



As soon as you connect a mobile device to a port on your USB hub or directly to the USB port on your computer, the tutorial will start.

To quickly identify and better manage plugged-in devices, you can mark the Hubs and devices with Securaze stickers, which will also be explained in the tutorial.

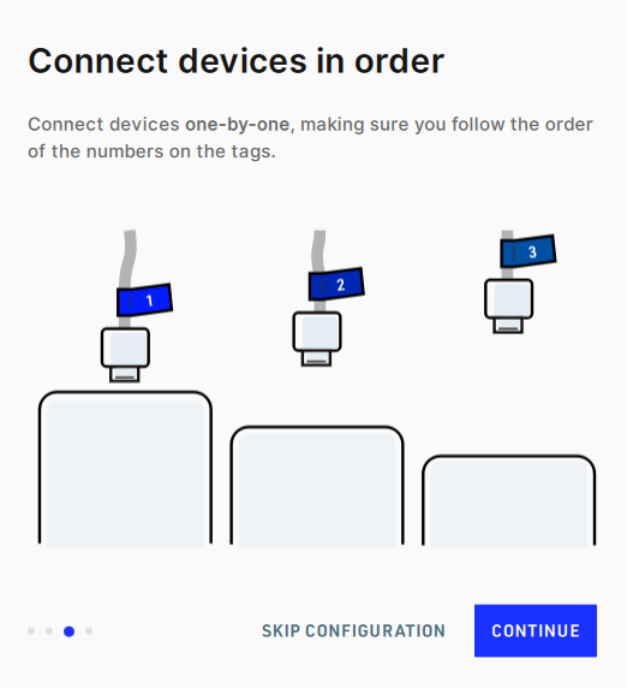

© 2026 Securaze GmbH

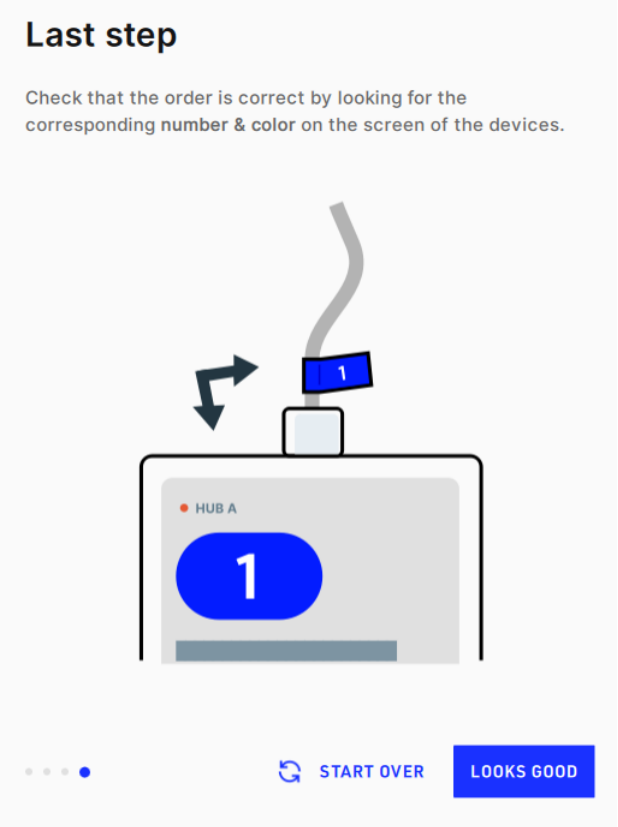




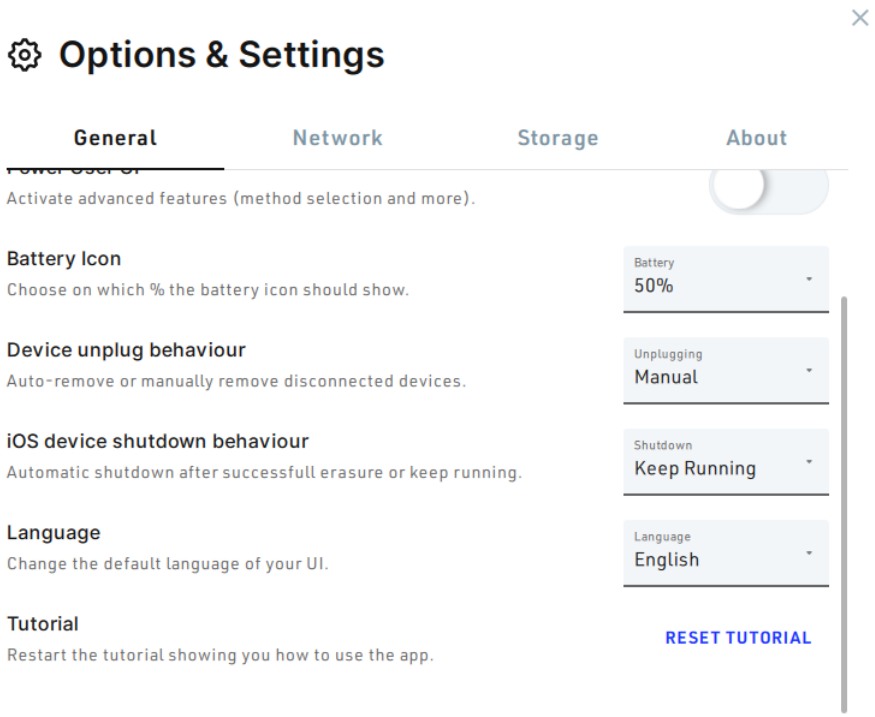
© 2026 Securaze GmbH




You can run the tutorial again at any time. To do this, select the **General** tab in the **Options & Settings** menu and then **RESET TUTORIAL**. The tutorial will be displayed again the next time you start Securaze mobile.


© 2026 Securaze GmbH

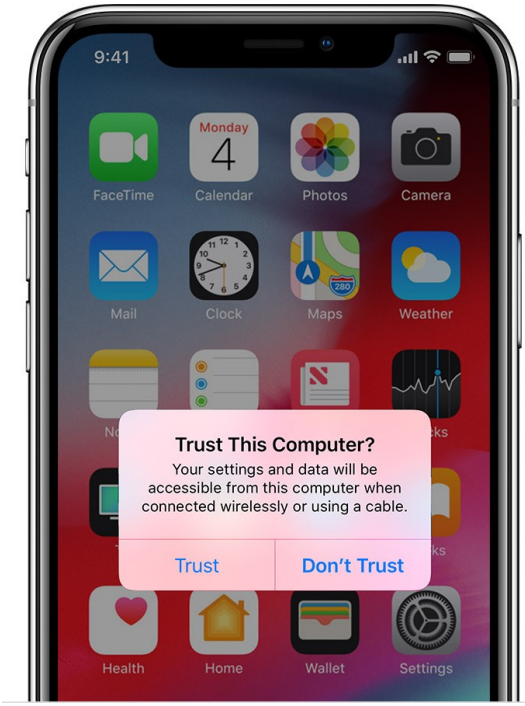



After connecting the phone you will need to make actions on the device. Depending on whether the device is an Android or an iOS device, there are different procedures.

### 4.7.1 Connect iOS Device

Connect the iOS device to the station with a USB cable that carries data. If the device has been set up, unlock it and confirm **Trust This Computer?** with **Trust**.


© 2026 Securaze GmbH




Trust This Computer (Source Apple Inc.)

Securaze Mobile then reads the device and shows it on its tile. What the device and the station need: see Requirements 199. If the device does not appear: see Problem solutions 201.

## Allow accessories to connect

macOS only: an erasure restarts an iPhone up to three times. Each time, macOS can ask **Allow accessory to connect?**, and the erasure waits until someone clicks **Allow**. Set it once to avoid that: in System Settings > Privacy & Security, set **Allow accessories to connect** to **Automatically allow when unlocked** (it asks for the administrator password), and keep the station unlocked while it processes.

With the first iPhone after the start, Securaze Mobile shows this as the hint **macOS may ask to allow each iPhone**. **OPEN SETTINGS** opens Privacy & Security. **Ignore** closes the hint and does not show it again on this station - press it once the setting is made.

## Recovery mode

macOS only: right-click the tile of an iPhone or iPad and choose **Put into Recovery Mode**. On a device in recovery mode the entry reads **Leave Recovery Mode** and restarts it normally. For several devices in normal mode, select them and choose **Put into Recovery [iOS]** under **MORE**. The entry is grayed out while the device is registered or erased, waits for its erasure, or is unplugged.


© 2026 Securaze GmbH

A message says when the device is in recovery mode or restarts normally, or why the command did not work. A locked device that does not trust the station takes the command only from a computer it trusts - put it into recovery mode with its buttons then.

A device in recovery mode shows **RECOVERY MODE** on its tile, a device in DFU mode **DFU MODE** - see Erase iOS device 85.

### Macs

macOS only: Macs are erased in DFU mode on macOS stations - see Erase a Mac 86.

## 4.7.2 Connect Android device

Connect the Android device to the station with a USB cable. How Mobile reaches it depends on the Android version and on your settings in Options & Settings > **Processing**.

### Android 16 and later: Android Express Mode

**Android Express Mode** is on by default. Mobile then connects supported Android 16 devices and later (API 36+) without USB debugging or developer mode. This works for a device that has not been set up yet, that is, it shows its setup screen. While Mobile reads the device, the tile shows **Reading device** (detailed tiles) or **ANALYZING** (standard tiles).

When **Android Express Mode** is off, these devices need USB debugging as well.

### All other Android devices: USB debugging

Mobile talks to the device over USB debugging. If it is not on, the tile shows **Turn ON and ALLOW USB debugging**. There are two ways to turn it on:

• **QR code** - on the setup screen, tap the screen 7 times and scan the QR code that Mobile shows. This skips the setup and turns on USB debugging. See Android USB-Debugging bypass with QR-Code 60.

• **Manually** - turn on the developer options and USB debugging in the device's settings. See Manual Android USB-Debugging 65.

When the device asks **Allow USB debugging?**, tap **Allow**.

### Samsung devices without USB debugging

With **Samsung Non-ADB communication** (Options & Settings > Processing, off by default), Mobile detects and erases Samsung devices without USB debugging. While it is on, devices with USB debugging are not shown, and the FRP / Google reactivation lock cannot be checked.

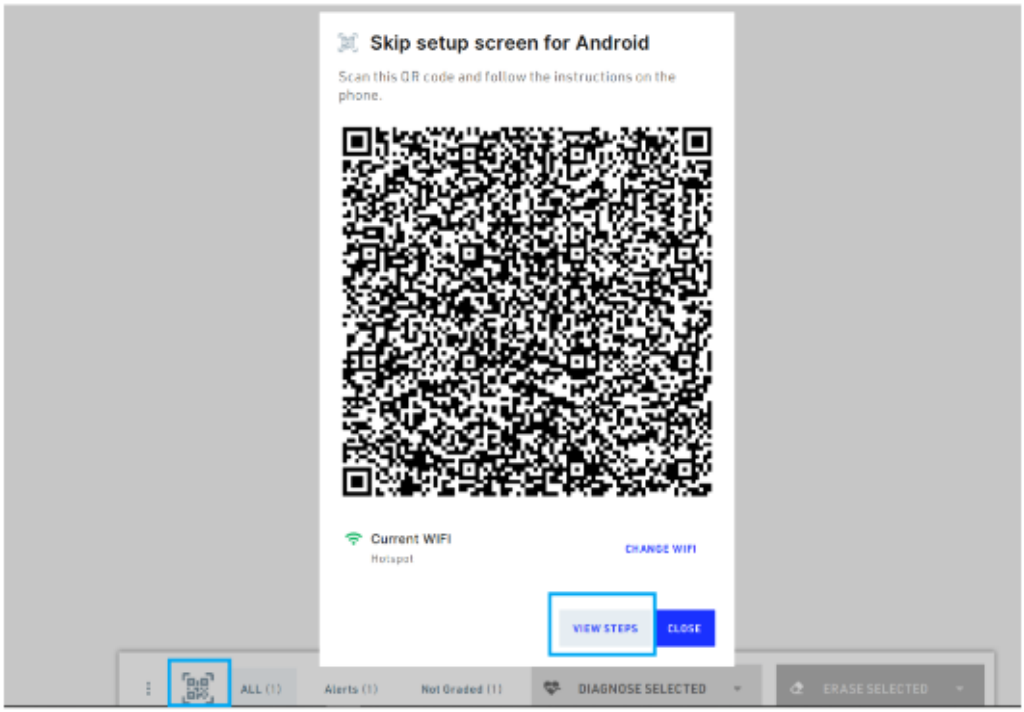
#### 4.7.2.1 Android USB-Debugging bypass with QR-Code

With the QR code, an Android device skips its setup screen and turns on USB debugging by itself. This works for all Android devices, including non-Samsung models. Supported


© 2026 Securaze GmbH

Android 16 devices and later can also be connected without USB debugging in **Android Express Mode** - see Connect Android device 60.

1. First, make sure **Samsung Non-ADB communication** is off: **General settings** (F9) in the menu, then Options & Settings > **Processing**. While it is on, devices with USB debugging are not shown.
2. Click the QR code icon next to **ALL** in the bar at the bottom of the dashboard. **Skip setup screen for Android** shows the QR code and, below it, the Wi-Fi network the QR code contains (**Current WIFI**; **Change WIFI** picks another one). **View steps** shows the steps on the station.




The steps on the device:

1. Tap anywhere on the screen 7 times.
2. Scan the QR code.
3. Press 'Next' / 'Approve' (text on screen may vary).
4. Press 'Continue'.
5. Wait for the Securaze App screen to pop up.
6. Plug in the phone to a station running Securaze Mobile.
7. Allow USB debugging (press 'Allow' button).
8. Done!

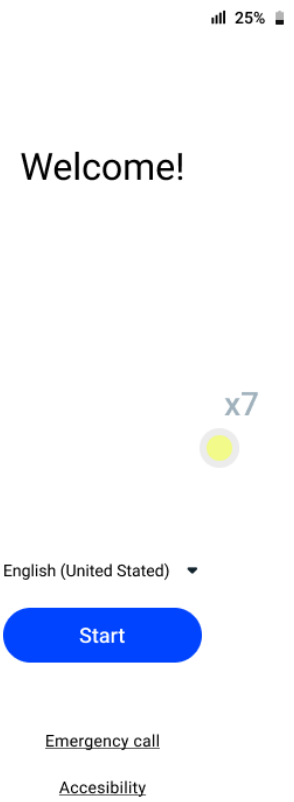

© 2026 Securaze GmbH

Here you can see 8 screenshots of how the process works.

Step 1:



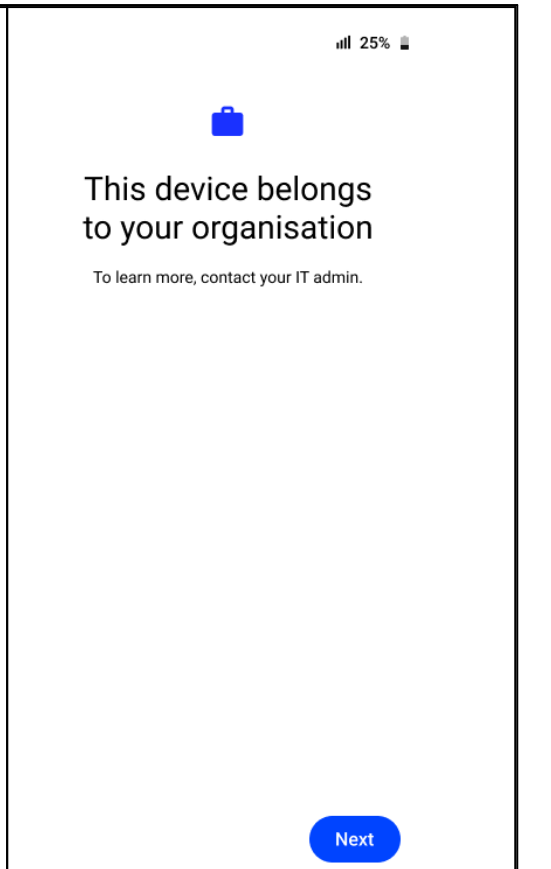

Step 2:



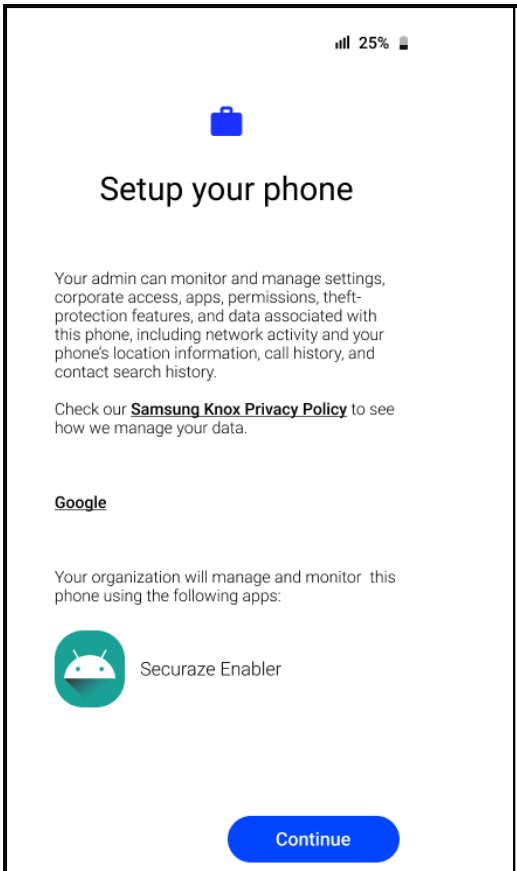

Step 3:

Step 4:

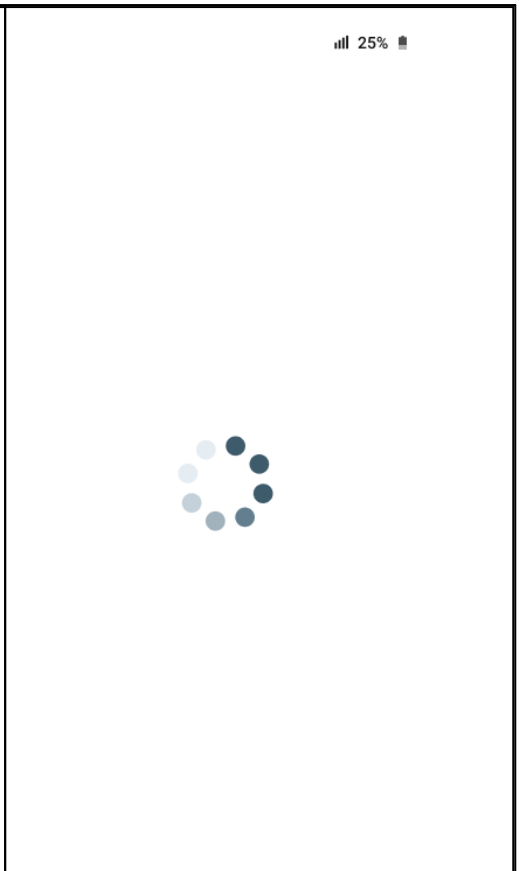

© 2026 Securaze GmbH

<table>
<tr>
<td>
</td>
<td>
</td>
</tr>
<tr>
<td>Step 5:</td>
<td>Step 6:</td>
</tr>
</table>


© 2026 Securaze GmbH

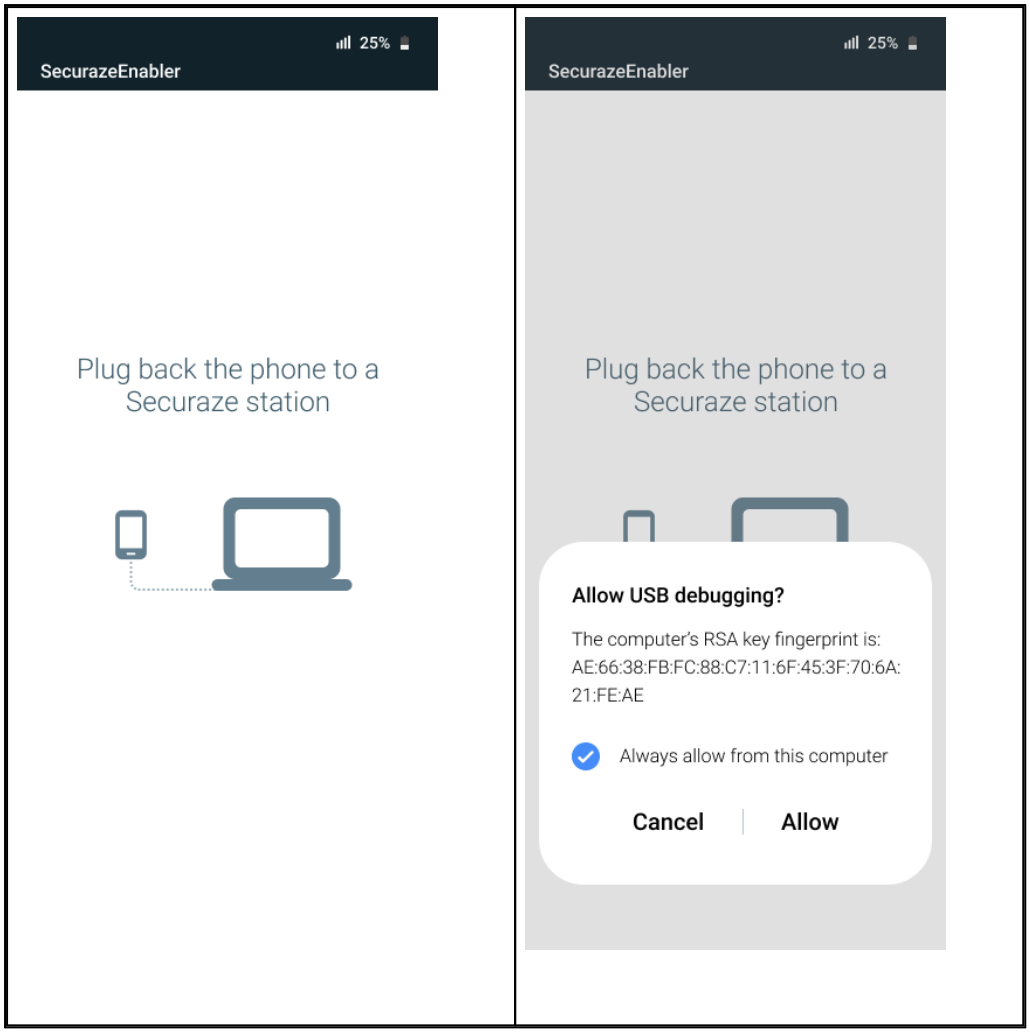



Step 7:




Step 8:


© 2026 Securaze GmbH




3. Close the steps. Tap the setup screen of the device 7 times; it opens a QR code scanner. Scan the QR code on the station and follow the device. When the Securaze app asks for it, plug the device into the station and allow USB debugging.

The device needs Wi-Fi to download the Securaze app. The QR code contains the network chosen under **Preferred Wifi** (Options & Settings > Processing). The networks come from the Wi-Fi networks of the Mobile preset in the Securaze Dashboard - see Set presets 44. An open network without a password works too. If several networks are set up, choose the right one with **Change WIFI**.

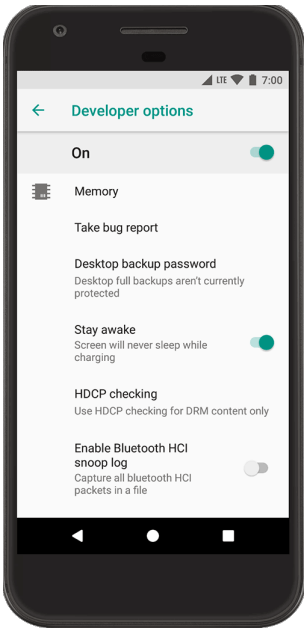
### 4.7.2.2 Manual Android USB-Debugging

Most Android devices need USB debugging so that Securaze Mobile can read and erase them. If you do not connect the device with Android Express Mode or the QR code (see Connect Android device 60), turn on USB debugging in the device's settings:

1. On the device, open **Settings** > **About phone** and tap **Build number** seven times. Developer mode is now on.


© 2026 Securaze GmbH

2. Go back to **Settings**, open **Developer options** and turn on **USB debugging**.




Developer options (Source: Google Inc.)

3. Connect the device to the station with a USB cable. When the device asks **Allow USB debugging?**, tick **Always allow from this computer** and tap **Allow**.

Securaze Mobile then reads the device.

The menu names differ between manufacturers, and some devices need more settings. See Developer mode and USB debugging 204.

## Samsung devices

Samsung devices can also be detected and erased without USB debugging: turn on **Samsung Non-ADB communication** in **Options & Settings** > **Processing**. While it is on, devices with USB debugging are not shown. See Processing 176.

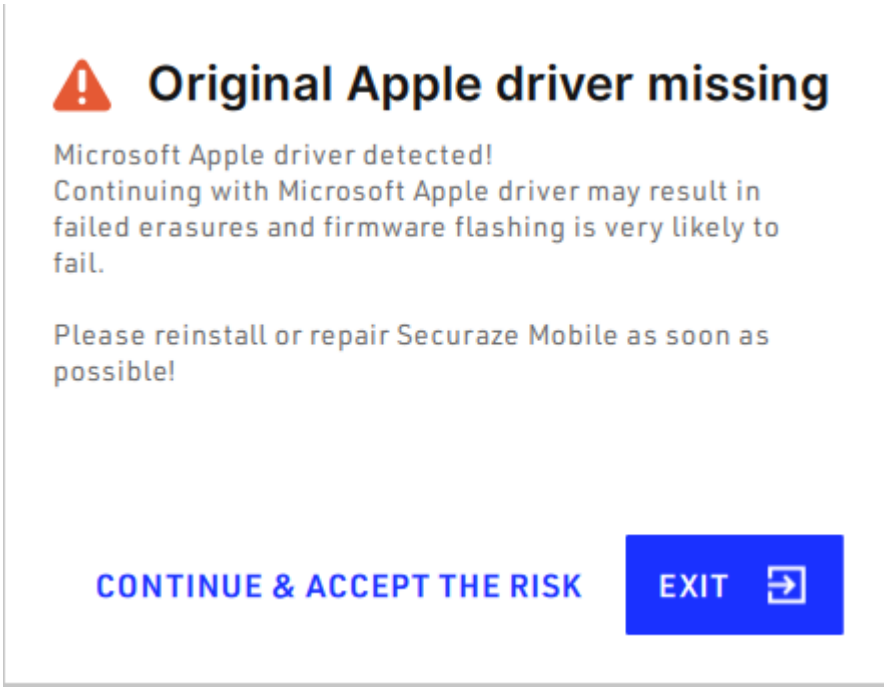

© 2026 Securaze GmbH

### 4.7.3 Microsoft Apple Driver

Windows only: after an iOS device is connected, Securaze Mobile checks whether the correct Apple driver is installed.

The Securaze Mobile installer installs the correct driver, but in some cases Windows uses another one - for example when other tools install their own drivers, after a Windows Update, or after manual changes to the drivers.

If it detects the Microsoft Apple driver, Securaze Mobile shows this warning.




**Attention:**

If this warning message appears you should exit the application or continue only if you know that there is a risk that erasures may abort and leave devices in unusable state!

As next step the following steps are possible:

- Uninstall & Reinstall
  To uninstall the existing Securaze Mobile just go to "Add or remove programs" and uninstall Securaze Mobile alternative you can just run the installer of Securaze Mobile again and choose Uninstall in the dialog.
  The original Apple driver will be installed when Securaze Mobile is installed.

- Install newer Securaze Mobile version:
  Download the most recent version of Securaze Mobile from Securaze Dashboard / Downloads and install it.
  The original Apple driver will be installed when Securaze Mobile is installed.


© 2026 Securaze GmbH

- Repair existing Securaze Mobile installation
  Run the installer of Securaze Mobile again and choose Repair in the dialog.
  The original Apple driver will be installed when Securaze Mobile gets repaired.

### 4.7.4 Apple Watch & AirPods

macOS only: Securaze Mobile processes Apple Watch and headphones - AirPods and Beats - on macOS stations. Windows and Linux stations do not have these modes.

#### Choose the mode

After the login, while no hub is connected, the dashboard shows **Select a mode** with three cards:

• **USB Hub** - **Connect a Mobile Device or a Hub**: phones and tablets on USB hubs.

• **Dock** - **Enable Watch mode**: Apple Watch, connected through the USB hub.

• **Bluetooth** - **Enable Headphones mode**: Securaze Mobile scans for headphones nearby over Bluetooth.

Click **SWITCH** on a card to change to its mode. Later, **Change mode** in the header opens the same choice. Switch to Watch mode before you plug in a watch. When you leave Headphones mode, the scan stops, a running headphone diagnose ends as not tested, and the headphone tiles are removed.

The header shows the licenses of the mode: check, erasure and diagnose licenses in Watch mode, check and diagnose licenses in Headphones mode.

#### Apple Watch

Switch to Watch mode, then connect the watch through its dock to the USB hub. The watch appears on a tile once it is detected.

**DIAGNOSE SELECTED** opens **Watch Diagnose**: choose the tests and click **Start testing (Enter)**. You carry out the tests on the watch and confirm each step with **Pass (Enter)**, **Fail (F)** or **Skip (S)**; **Abort (Esc)** stops. At the end, Securaze Mobile ticks the typical problems of the failed tests and grades the watch.

Securaze Mobile cannot erase an Apple Watch over USB. Erase the watch on the watch itself first: Settings > General > Reset > Erase All Content and Settings. Then select its tile and click **ERASE SELECTED** - the only solution is **Factory Reset**: Securaze Mobile checks that the watch is back at its setup screen and restarts it to confirm the erasure.

#### AirPods and other headphones

Switch to Headphones mode. If macOS asks whether Securaze Mobile may use Bluetooth, allow it. On the switch, Securaze Mobile can show two warnings:


© 2026 Securaze GmbH

• **This Mac is signed into iCloud** - for Apple headphones (AirPods, AirPods Max, Beats), sign the station out of iCloud first: a signed-in Mac hides the audio of headphones on its Apple ID and hands them to its other devices in the middle of a test. **OK** shows the warning again next time, **Ignore** never again on this station.

• **Full Disk Access is off** - testing still works, but headphones that are not connected yet can take longer to appear or stay on Pairing. **OPEN SETTINGS** opens the setting: switch Securaze Mobile on (add it with + if it is not listed), then restart Securaze Mobile. **Ignore** hides the warning on this station for good.

Put the AirPods into pairing mode: open the case and tap the touch sensor twice quickly, or press and hold the button on the back for 3-4 seconds until the LED flashes white. They then appear on a tile by themselves. While they are read, keep the case open and the buds out.

The tile shows the model, the battery of the left bud, the right bud and the case, and the originality check **OEM**: **Genuine**, **Not Genuine** or **Partial**.

**DIAGNOSE SELECTED** opens **Headphone Diagnose**: choose the automatic and manual tests and click **Start testing**. Diagnose one pair at a time. **Audio: Automatic** or **Audio: By ear** in the header decides whether the speaker test is judged with the station's microphone or by your ear.

**COMPLETE CHECK** records the headphones with a check report.

**REMOVE SELECTED** unpairs the selected headphones from the station and removes their tiles. For headphones still linked to another owner the button reads **FACTORY RESET**, and Securaze Mobile guides you through the reset on the headphones. The button's list holds both: **Forget** and **Factory Reset**.

**Reset AirPods + BT** in the header forgets all AirPods and Beats paired with the station and restarts its Bluetooth - use it when headphones do not show up. Click it, then click **Confirm reset?** within 3 seconds. All Bluetooth connections of the station drop for about 2 seconds.

Bluetooth audio devices that are not Apple products are listed apart: **TEST THIS** connects one and gives it a tile, **REPORT FAKE** reports it to Securaze, **IGNORE** hides it for good.

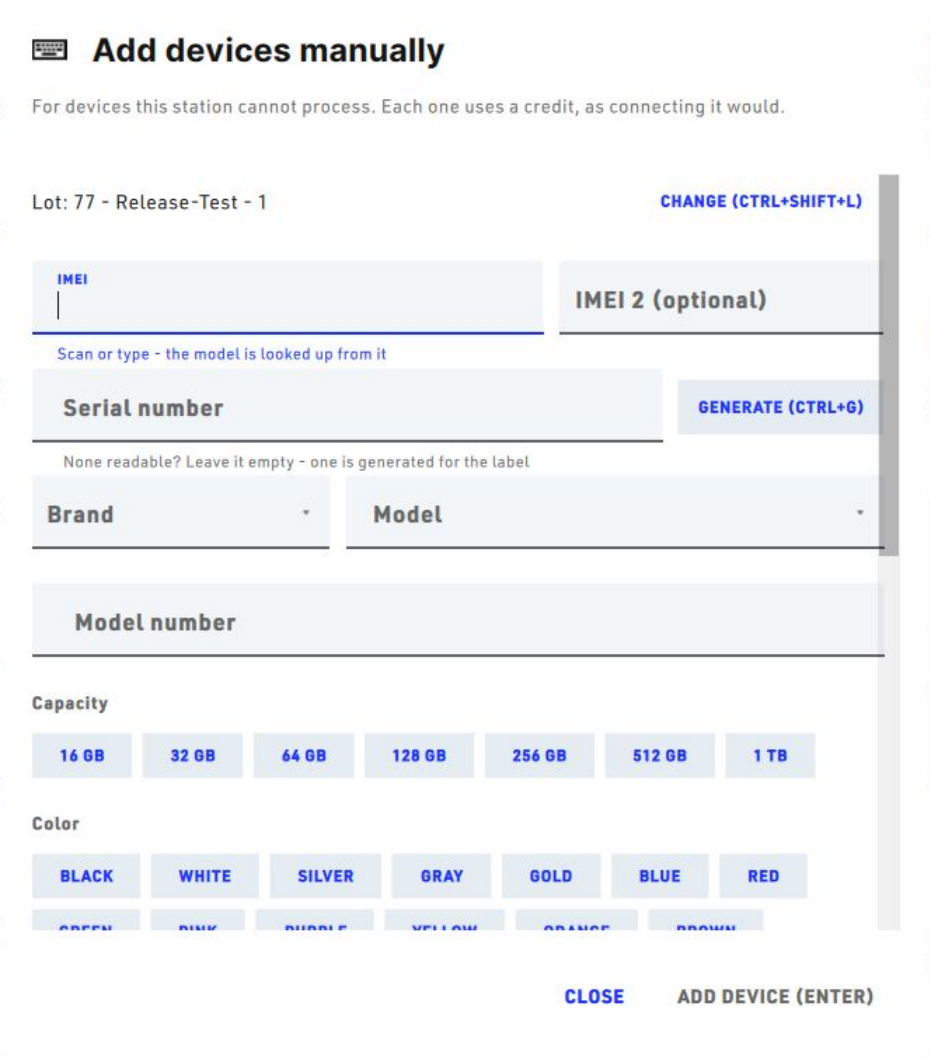
The results go to the Securaze Dashboard. To print a label, right-click the tile and choose **Print Label**.

## 4.8 Manual Entry

With Manual Entry you add a device by hand that this station cannot process - for example a phone that won't power on, won't connect or is locked. The device is registered in the Securaze Dashboard in the current lot, like a connected one, and can get a label, photos and notes.


© 2026 Securaze GmbH

Click **Add devices manually** in the sidebar, or press Ctrl+N. The dialog **Add devices manually** opens.




## Before you start

• A lot must be selected. The dialog shows it at the top (**Lot:** and its name). Click **Change** (Ctrl+Shift+L) to choose another lot. Without a lot it says **No lot selected - choose one first.**

• Each device you add uses a credit, as connecting it would - a Registration license, if your account has them.

## Enter a device

The dialog is built for a barcode scanner: scan the IMEI, press Enter, scan the next device. You need at least the IMEI, the serial number or the model.

• **IMEI** - scan or type it. Securaze Mobile looks the model up from the IMEI and says **Model found:** with brand and model, or **Model not known yet - please enter it**. A wrong number shows **Check digit does not match - please check the number**.


© 2026 Securaze GmbH

• **IMEI 2 (optional)** - the second IMEI, if the device has one.

• **Serial number** - if none is readable, leave it empty: a serial number is generated for the label. **Generate** (Ctrl+G) creates one at once.

• **Brand** and **Model** - filled in from the IMEI. Or type and pick them from the list of known brands and models; a model picked from the list fills the form as an IMEI does. Values filled in this way are marked **from IMEI** or **from list**.

• **Model number** - the most common one is filled in. If the model has several, they are offered below the field: pick the one you can read on the device.

• **Capacity** - pick it. If the model comes in one capacity only, it is already picked.

• **Color** - pick it. For an Apple model its own colors are offered; **More colors** shows the general ones.

• **Operating system** - iOS, iPadOS, Android or HarmonyOS. Filled in with the model.

• **Grade** - shown if your company has grades set up. If grades are set automatically from typical problems, the grade follows the problems you tick and is marked **automatic from typical problems**. A grade you pick yourself stays.

• **Typical problems** - tick the problems of the device.

• **Why by hand** - **Won't power on**, **Won't connect**, **Locked** or **Other**. The device's notes start with it, for example "Added by hand: Locked".

• **Notes (optional)** - anything else about the device.

• **Print label** - on by default: a label is printed on the selected printer once the device is registered.

• **Add photos** - pick photos of the device (JPG, PNG or HEIC).

Click **Add device (Enter)**. The form is cleared for the next device. The lot, a grade you picked, **Why by hand** and **Print label** stay as they are.

Tab moves to the next field, Shift+Tab back.

## The batch

Each device is registered as soon as you add it and is listed in **This batch** beside the form, newest on top. The heading shows how many are registered.

• **Checking...** / **Registering...** - the device is being registered.

• The inventory number (for example #12345), or **Registered** - the device is registered. Click **Print label** (**Print again**) to print its label, **Add photos** to add photos, or **Photos by phone** for a QR code: scan it with the Motion app (Upload) to add photos taken with a phone. Below the device you see **Label printed**, **Label failed** or **No printer selected**, and how many photos are saved.


© 2026 Securaze GmbH

• **Already registered** - the server already has this device. Registering it again uses a credit. Click **Register again** or **Discard**.

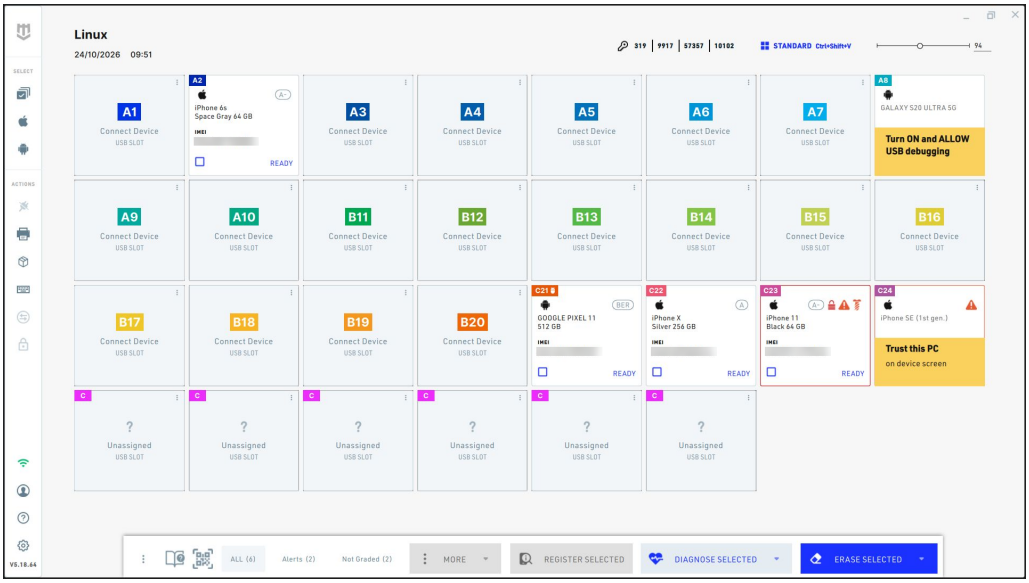
• **Not registered** - the server did not accept the device; the reason is shown. Click **Retry** or **Discard**.

**Clear registered** removes the registered devices from the list. **Hide** puts the batch away; **Show batch** at the bottom of the dialog, with the number of devices, brings it back. A device that was not registered, or is already registered, brings the batch back by itself.

A device that is already in the batch is not added again: **This device is already in this batch.**

## 4.9 Check the connected devices

After login, the dashboard shows all devices connected to the station. Each USB port is a tile.




### Layout

• **Left** - the menu: select devices, actions such as **Print labels** or **Change lot**, Help and General settings. See Menu 187.

• **Top** - station name, date and time, the station's licenses, the card view button and the UI scale. A red warning sign with a number appears when Mobile has found problems with the station - see Infrastructure issues 73.

• **Middle** - one tile per USB port. A tile shows the port (hub letter and port number, or the port's own name), the device and its state.

• **Bottom** - the filters and the buttons that start a run on the selected devices: **MORE**, **REGISTER SELECTED**, **DIAGNOSE SELECTED** and **ERASE SELECTED**. See Dashboard 185.


© 2026 Securaze GmbH

### Work with the tiles

• Tick the check box on a tile to select the device. To select many at once, use **All devices** (Ctrl+A), **Apple devices** or **Androids** in the menu.

• Click a tile to open the device details. See Device details 196.

• Right-click a tile for the device menu, for example **Print Label**, **Show device screen** or **Grade on device**. On an empty port, the ... icon at the top right opens the port menu, for example **Set as Charging Only** or **Deactivate Port**; a right-click on an empty port offers **Select all from Hub** and **Remap Hub**. See Menu 187.

• Choose how much a tile shows: **STANDARD** or **DETAILED**. Switch with the card view button in the header (Ctrl+Shift+V) or in Options & Settings > General > **UI Card View**. Detailed tiles have tabs; **All tiles** (Ctrl+Shift+G) in the menu puts every tile on the same tab, for example **Grading**, to grade one device after the other.

### Filters

The bottom bar shows **ALL** and the filters, each with the number of devices it matches. A filter appears only when at least one device matches it. Click the ... icon at the left of the bar and **CUSTOMIZE FILTERS** to choose which categories the bar shows.

• Click a filter to show only those devices. **ALL** shows every device again.

• Shift+Click adds a filter: devices that match either filter are shown, e.g. **Alerts** + **Not Graded**.

• Ctrl+Click combines filters: only devices that match both are shown, e.g. devices with an alert that are also not graded.

## 4.10 Infrastructure issues

Securaze Mobile watches for problems that are not caused by one device but by the station or its surroundings - the printer, the network, the Apple service, missing programs, or the same test failing on many devices. It collects them in the **Infrastructure issues** list.

### The warning sign in the header

As soon as Mobile has found a problem, a red warning sign with a number in brackets, for example [3], appears at the top right of the dashboard, left of the license counters. The number counts the reports. Point at the sign to see its name, **Infrastructure issues**. Without problems the sign is not shown.

### The list

Click the sign to open **Infrastructure issues**. Each row is one kind of problem; all devices it happened on are listed together in that row.


© 2026 Securaze GmbH

• **Issue** - the kind of problem and what happened.

• **Device(s)** - the devices affected. A device shown in blue and underlined has a Securaze ID: click it to open the device in the Securaze Dashboard. Problems of the station itself, such as the printer, list no device.

• **Solutions** - what to do.

• **Knowledge base** - **Open article** opens an article about the problem, where there is one.

## What to do

• Fix the cause as the **Solutions** column says, for example load a new label roll or close the printer cover.

• Then tick the rows you have dealt with and click **Resolve selected**, or click **Resolve all** with no row ticked. This only removes the rows from the list - it does not fix anything. If the problem happens again, it is listed again.

• **Send system report** (shown when you are logged in) opens **Send System Report**: type the reason and send the report to Securaze support. Do this before you contact support.

• **Close** closes the list. The problems stay in it.

The list is kept until you resolve its rows or close Securaze Mobile.

## Problems in the list

• **Printer** - the printer is not connected, its driver or software is missing, it is out of labels, its cover is open, the loaded roll does not match the label template, or a label did not print.

• **App install** - the Securaze app could not be installed on an iPhone.

• **VPP** - the Apple VPP token has expired. Contact support.

• **Prolonged analyze** - reading a device took longer than expected. Check the USB connection; if it keeps happening, contact support.

• **WiFi slow** and **WiFi connectivity** - the Wi-Fi setup of an iPhone took more than a minute, or five or more iPhones are waiting for Wi-Fi at the same time. Check the network; restart the router or access point if needed.

• **Diagnose cases** - the same diagnose case failed on five or more devices. This can point to a problem with the setup rather than with the devices. Contact support.

• **App stopped responding** - the Securaze app on a device stopped answering during a diagnose. Disconnect and reconnect the device, then run the diagnose again.

• **FRP not checked (Non-ADB)** - a Samsung device was processed in Samsung Non-ADB mode, so its FRP / Google reactivation lock could not be read. Process it with USB debugging to check FRP.


© 2026 Securaze GmbH

• **Installation incomplete** - programs Mobile needs are missing or cannot run. Reinstall or update Securaze Mobile.

• **Station disk full** - the station is out of disk space, so firmware downloads fail. Free up disk space, then start the erasure again.

• **Device model not supported yet** - update Securaze Mobile. If it is already the latest version, send a system report and contact support.

• **Firmware not found** - no firmware was found for a device. Check the station's internet connection, then start the erasure again.

• Windows only: **Apple service** - the Apple Mobile Device Service could not be restarted; without it, iPhones and iPads are not detected. Mobile restarts the service when it starts and when you click **Re-detect iPhones and iPads** in Help. The row shows a command to run in a command prompt as administrator.

• **No workflow switched on** - the station is set to run from workflows, but none is switched on, so nothing is tested, printed or erased by itself. Choose one under **Workflow this station runs** in **Options & Settings** > **Workflows**. If the one you want is not offered, switch it on in the workflow editor first.

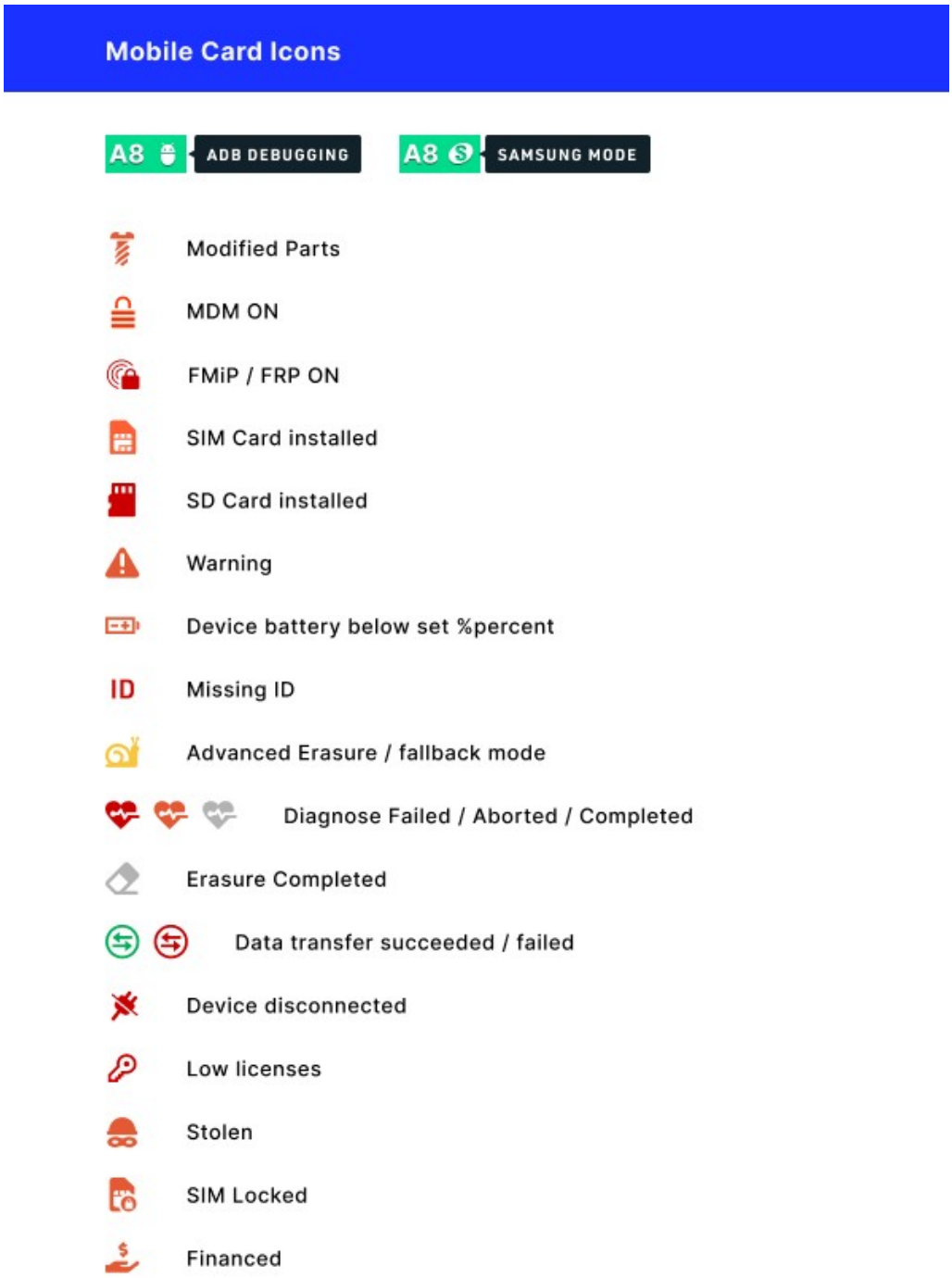
• **Workflow missing** - a workflow calls another workflow that is not on this station, so every phone fails at that step. Copy the missing workflow to this station - the name has to match exactly - or change the step in the workflow editor.

• macOS only: **Apple device support outdated** - the station's Apple device support is too old to erase (restore) a Mac. Securaze Mobile opens Apple's updater for it; **Install now** in the row opens it again. Install the update there - it asks for the station's password - or update macOS, then start the erasure again.

## 4.11 Mobile Icons

Icons displayed in Securaze Mobile application and their meaning:


© 2026 Securaze GmbH




Point at an icon on a tile to see what it means for this device:

• **Apple / Android / Samsung logo** - the platform. Click it to copy the device ID.

• **Workflow (lightning)** - only on a station that runs workflows. Click it for the workflow's status. It is blue when a workflow step waits for you - click it to open that step.

• **Grade** - the grade letter, once the phone is graded.

• **MDM lock** - MDM lock activated, with the reason if known.


© 2026 Securaze GmbH

• **FMiP / FRP** - Find My iPhone or Google FRP is on.

• **ID** - External ID not provided.

• **Battery** - the battery charge is at or below the set percentage; the tooltip shows the charge.

• **Warning** - the tooltip lists the warnings for this device.

• **Key** - device locked.

• **SD card** - the device contains an SD card.

• **SIM card** - a SIM card was detected.

• **Screw** - the device does not contain all of its original parts (see OEM parts validation 159).

• **Data transfer** - red: the connection with the backend failed; green: data export successful.

• **Financed** - the device is being financed.

• **Stolen** - the device was flagged for theft.

• **SIM lock** - SIM lock is active on this device.

• **Snail** - the slow erasure method was used, because the app-based erasure was not possible. The tooltip says why: the iOS version is below 11, MDM is present, FMiP is active, or there is no Wi-Fi preset (create one in Securaze Dashboard and log in again).

• **Diagnose** - the device is being diagnosed, or its diagnosis is done; orange: aborted, red: failed. Click it for the diagnose summary.

• **Plug** - the device is disconnected.

Note: Icons may also be white, when the tile itself is green, blue, or red.

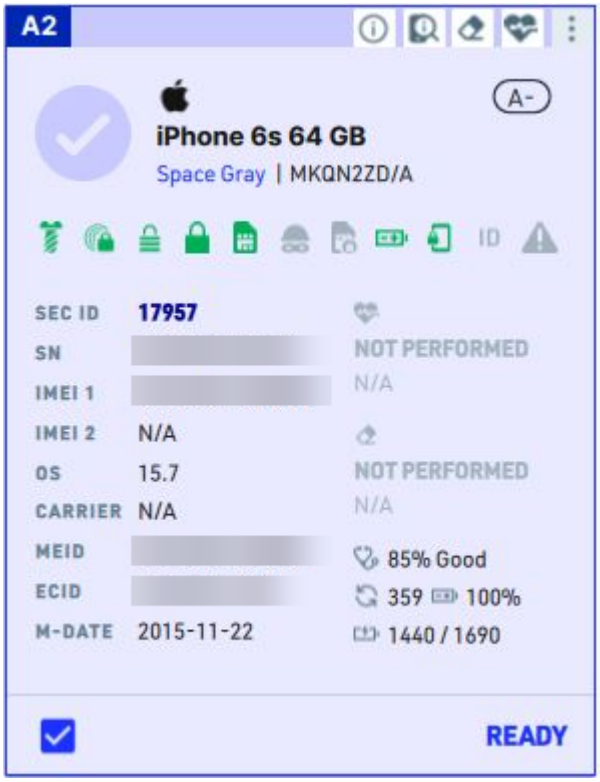
## 4.12 Enter Device details

You record a phone's grade, its issues, its color and further details on its tile. What a tile shows depends on **UI Card View** in **Options & Settings**, tab **General**: **Standard** tiles open their details at the bottom of the screen, **Detailed** tiles show them on the tile itself.

### Detailed tiles

Click the info icon in the tile's header. The tile then shows three tabs:

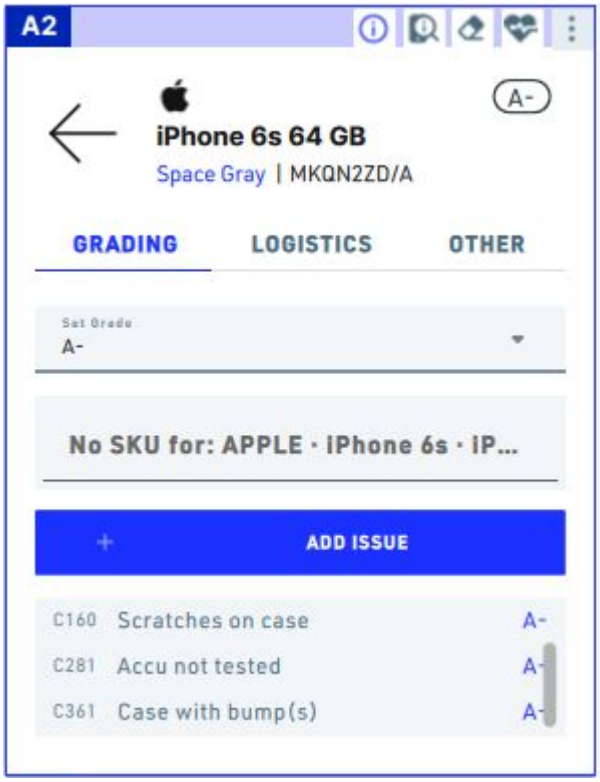

© 2026 Securaze GmbH




• **Grading** - choose the grade under **Set Grade**, enter the **SKU Code** and add issues with **ADD ISSUE**.

• **Logistics** - change the **LOT** and the **SALE LOT** of this phone.

• **Other** - enter the **INVENTORY NO.** and **Notes** (up to 255 characters). Click the QR code to enlarge it; scan it with Motion Ops to record the device.





© 2026 Securaze GmbH

The SKU can follow a custom pattern defined under Settings / SKU in Securaze Dashboard (see Set presets).

## Issues and the grade they result in

**ADD ISSUE** opens the list of typical problems. Type an issue code or a description to find one, tick the problems that apply and click **CONFIRM** (Ctrl+Enter). A problem you already added is marked **(Added)**.

Next to each problem, in bold blue, you see the letter of the grade it results in - in the list and among the problems you added.

To change a phone's grade, click the grade shown on its tile - on standard and detailed tiles. The tile is selected and the list of typical problems opens.

## Color

Under the phone's name, a detailed tile shows the color as a link - **Color?** if the phone reports none. The link works once the phone has its Securaze ID. Click it and pick the color: for an Apple device you see the colors Apple sold that model in first, and **More colors** shows the others. Pick the chosen color again to go back to the color the phone reports. In the device details, a color you picked is marked **set by hand**.

## All tiles

With Detailed tiles, **All tiles** in the sidebar puts every tile on the same tab: **Grading**, **Registration** (only with Registration licenses), **Erasure**, **Diagnose** or **Workflow** (only on a station that runs workflows). **Each tile on its own** lets each tile show its own tab again. Ctrl+Shift+G switches between **Grading** and **Each tile on its own**, so you can grade a whole bench without opening each tile.

## Grade on device

Right-click a tile and choose **Grade on device** to show the grading on the phone's own screen: it asks for the grade and which typical problems apply. The entry is grayed out until the phone has its session and while the phone is erased. AirPods do not have it.

## Standard tiles

Click a tile to open its details at the bottom of the screen. The arrow button shows more details, among them **LOT** and **SALE LOT**, which you can change there. **INVENTORY NUMBER** and **SKU CODE** can be edited in the details.

The icon buttons in the details open **WORKFLOW** (only on a station that runs workflows), **GRADE SUMMARY**, **REGISTRATION** (only with Registration licenses), **ERASURE SUMMARY** and **DIAGNOSE SUMMARY** - point at a button to see its name.


© 2026 Securaze GmbH

In **GRADE SUMMARY**, choose the grade under **Set grade** and add issues with **ADD ISSUE**. Click the QR code to enlarge it.

After you have captured all the information about the device, you can start the erasure (see Perform erasure 81).

## 4.13 Register devices

Registration records a phone in the Securaze Dashboard without erasing or diagnosing it. Use it when a phone only has to be on record.

Securaze Mobile records the phone's details and runs its lock checks, for example Find My and MDM on an iPhone. On an Android phone it first installs or updates the Securaze app, if needed. A report is created for the phone. Nothing on the phone is erased.

### Registration licenses

Registration needs **Registration licenses**. If your account has some, the header shows how many are left, next to the key icon and beside the erasure and diagnose licenses. Click a number to refresh it. The number is also read again after each registration.

Without Registration licenses, Securaze Mobile does not show **REGISTER SELECTED**, the Registration tab on the tile or **Register Device**.

Before a registration starts, Securaze Mobile checks that enough Registration licenses are left for the selected phones. If none are left, it says **Error: No registration licenses left.** If the server cannot be reached, it says **Registration could not start. Network error!**

### Register phones

• Select the phones: tick them on their tiles, or use **Select** in the sidebar - **All devices** (Ctrl+A), **Apple devices** or **Androids**.

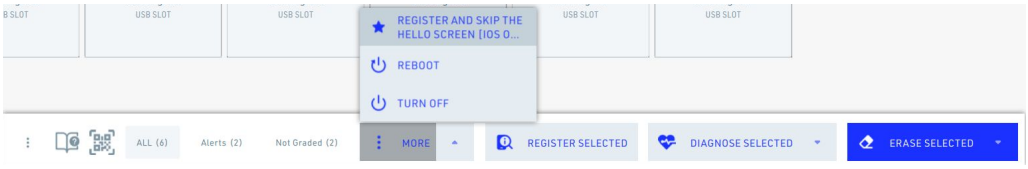
• Click **REGISTER SELECTED** in the bottom bar. The button can be clicked while at least one phone is selected.

The phones are deselected and their registration starts.

To register a single phone, right-click its tile and choose **Register Device**.

### MORE

**MORE**, left of REGISTER SELECTED in the bottom bar, holds the other actions for the selected phones; when the bar runs short of room, it shows only its dots. An entry runs as soon as you pick it:





© 2026 Securaze GmbH

• **Register and skip the hello screen [iOS only]** - registers the phones and skips the hello screen on each iPhone. Shown only with Registration licenses. If Find My or an MDM profile is on an iPhone, its hello screen is not skipped and its registration fails. An Android phone is only registered.

• **Reboot** - restarts the phones.

• **Turn Off** - turns the phones off.

• macOS only: **Put into DFU** for running Macs (see Erase a Mac 86) and **Put into Recovery [iOS]** (see Connect iOS Device 58).

### Results

The Registration tab of a tile in the Detailed card view, and **REGISTRATION** in the device details, show the result:

• **Registered** - the phone is registered.

• **Registration failed** - the registration did not finish, for example because the phone could no longer be reached.

• **Registration canceled** - the registration was stopped before it finished.

• **Not registered** - no registration has run on this phone.

The tile of a registered phone and its row in the list view say **REGISTERED**, a detailed tile says **Registered** - an erased phone says **COMPLETED**.

While the registration runs, it says **In Progress**. The Registration tab also shows **DATE & TIME** and **DURATION**.

In the Detailed card view, click **All tiles** in the sidebar and choose **Registration** to show the Registration tab on every tile at once.

### Only registration

To use a station for registration only, open **Options & Settings** > **General** and set **Application functionality** to **Only registration**. The bottom bar then shows **REGISTER SELECTED** and **MORE**; the erasure and diagnose buttons are hidden.

**REGISTER SELECTED** and **MORE** are shown only with **Full** and **Only registration**.

## 4.14 Perform erasure

To erase phones, select them first: tick the check box on their tiles, or use **All devices** (Ctrl+A), **Apple devices** or **Androids** under **Select** in the sidebar.

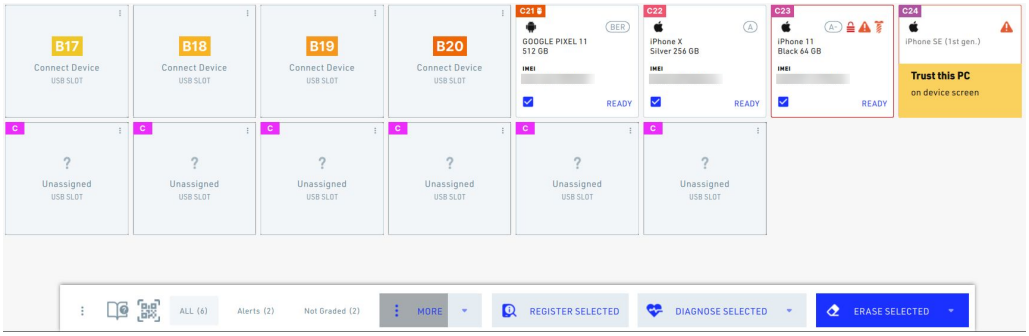
Then click **ERASE SELECTED** in the bar at the bottom of the window.

By default the **Erasure Settings** window opens. Choose the erasure solution there and click **START ERASURE**. If you tick **Don't show again** in that window, **ERASE SELECTED**


© 2026 Securaze GmbH

starts the erasure at once with the solution you chose there. For the solutions and the settings, see Erasure Methods 82.

The buttons at the right of that bar are, from left to right, **MORE**, **REGISTER SELECTED** (only with Registration licenses, see Register devices 80), **DIAGNOSE SELECTED** and **ERASE SELECTED**. **MORE** holds **Reboot**, **Turn Off** and, with Registration licenses, **Register and skip the hello screen [iOS only]**. When the bar runs short of room, **MORE** shows only its dots; it still opens the list.




macOS only: **MORE** also holds **Put into DFU** for running Macs (see Erase a Mac 86) and **Put into Recovery [iOS]** (see Connect iOS Device 58).

While a phone is erased, its tile shows the progress. To stop the erasure of the phone whose tile is in focus, click **CANCEL ERASURE** in the bar at the bottom.

What happens on the phone depends on its platform and on the erasure solution - see Erase iOS device 85 and Erase Android device 86; for Macs on macOS stations, see Erase a Mac 86.

### 4.14.1 Erasure Methods

You choose the erasure solution in the **Erasure Settings** window. It opens when you click **ERASE SELECTED** in the bar at the bottom of the window, unless you ticked **Don't show again** in it.

With **Expert Erasure Mode** on in the **General** tab of **Options & Settings** (it is on by default), the arrow next to **ERASE SELECTED** opens a list: **Erasure Settings** opens the window, and **Data Clear**, **Smart Erasure** and **Advanced Erasure** start that solution on the selected phones at once. Smart Erasure and Advanced Erasure are listed only with erasure licenses.

Here you can choose the desired erasure solution: Data Clear, Smart Erasure or Advanced Erasure.

**Data Clear**

This meets R2 requirements.
Data Clear procedure lasts anywhere between 6-20 seconds.


© 2026 Securaze GmbH

The devices have to complete the Factory Reset process (with optional firmware update on iOS) before being certified and issued a tamper-proof Erasure Report.

- iOS devices:
  Securaze Mobile is calling the iOS function (Apple's existing function) to throw away the encryption key. During the wipe process, Securaze mobile adds a certain data to the device's storage, and after the erasure is completed, it searches for that data. If the data is gone, the device is considered to be fully wiped.

**Smart Erasure**

This meets R2 requirements.

This method is most suitable to handle a huge amount of devices in an automated process and yet have a high data security level.

Following inspection of the device, Smart Erasure determines the most efficient means for delivering data sanitization. Unless an added layer of security is required, this option is usually selected as primary means of processing mobile devices as it yields the highest UPH (Units Per Hour).

- iOS devices – Smart Erasure is checking 8 conditions, while ensuring previous encryption keys are not recoverable and no residual data exists. These conditions are:
  - is the device on "Hello" screen?
  - could Securaze find any non-system files on the storage?
  - are there any third-party applications on the device?
  - is the device in an activated state?
  - does the device have FMiP activated?
  - does the device have MDM activated?
  - is iOS Jailbroken?
  - is there a SIM card in the device?

  If the devices pass these checks, Smart Erasure for iOS devices will quickly certify them in a matter of seconds (unless the optional iOS firmware update is selected for iOS) and provide an approved tamper-proof Erasure Report for audit purposes. In instances where these conditions are not met, the device will fallback to a Data Clear which takes a bit more time to process but provides the required level of data sanitization.
- Android Devices – Smart Erasure on Androids starts by ensuring the Android device was previously encrypted. If the device was previously encrypted, it will seek verification of the other conditions - Factory Reset to Hello Screen, previous encryption keys non-recoverable, and no residual data exists. If these conditions are met, it will pass the device. If these are not met, it will fallback to Data Clear, which provides the required level of data sanitization.


© 2026 Securaze GmbH

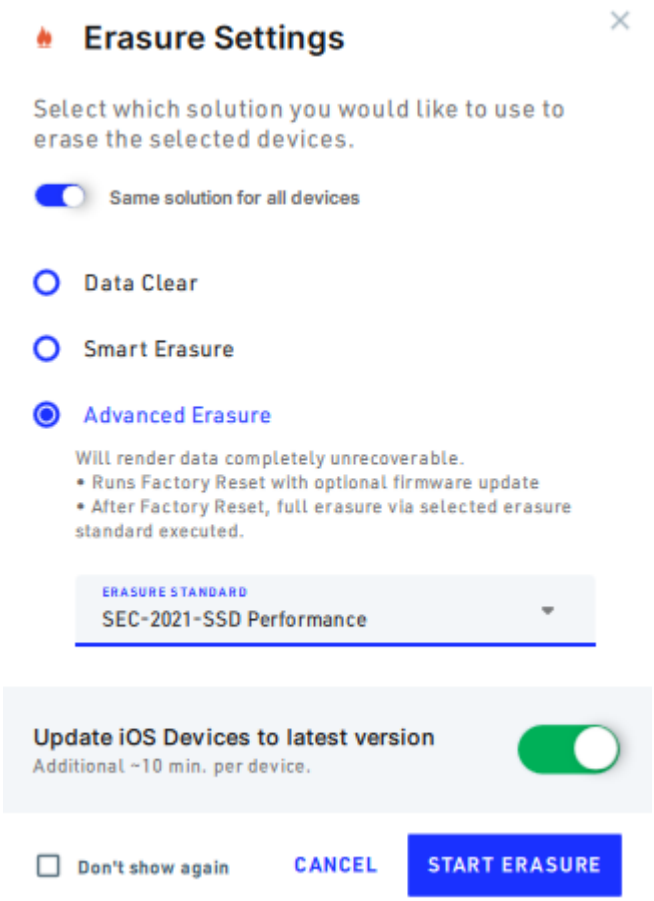
**Advanced Erasure**

This goes beyond R2 requirements to add an incremental layer of security.

This method is most suitable when there is a strict data security policy and to ensure all data is erased rigorously.

Once a Factory Reset (with optional firmware update on iOS) has been completed on the device, it will proceed to a full overwrite of the device based on the type of erasure algorithm chosen. This type of data sanitization is typically chosen when security is paramount – leveraging either a single-pass, three-pass or seven-pass overwrite.

The **Erasure Settings** window opens when you click **ERASE SELECTED**, or when you pick **Erasure Settings** from the arrow's list.




Here you will find more information about each Solution and you can select one of them.

You can also enable **Same solution for all devices** to use the same solution for all plugged-in devices.

When it is off, choose a solution for each platform on the **APPLE IOS** and **ANDROID** tabs.

If you select Advanced Erasure, you have the option to select the **Erasure Standard**.


© 2026 Securaze GmbH

Click on the pull down menu and select the desired Erasure Standard.

**Update iOS Devices to latest version** updates iOS devices to the latest iOS version as part of the erasure. It takes about 10 minutes more per device.

**START ERASURE** starts the erasure of the selected phones. Without a selected phone the button reads **CONFIRM** and only saves your choice. If you tick **Don't show again**, **ERASE SELECTED** starts the erasure at once with this choice from then on.

### 4.14.2 Erase iOS device

After the iOS device is connected and its details are read, select its tile and click **ERASE SELECTED** in the bar at the bottom of the window (see Perform erasure 81).

With **Advanced Erasure**, Securaze Mobile first resets the device to factory settings. Then it overwrites the storage with the selected erasure standard. Afterwards it resets the device to factory settings again and checks the result.

For the overwrite, Securaze Mobile normally uses its app on the device. The app needs a Wi-Fi preset from Securaze Dashboard. If the app cannot be used, Securaze Mobile overwrites the device directly, which is slower. The tile then shows the snail icon, and its tooltip says why: the iOS version is below 11, MDM is present, Find My (FMiP) is active, or there is no Wi-Fi preset (create one in Securaze Dashboard and log in again).

With **Data Clear**, Securaze Mobile resets the device to factory settings. **Smart Erasure** decides per device - see Erasure Methods 82.

#### Devices in recovery mode or DFU mode

A device in recovery mode or DFU mode shows **RECOVERY MODE** or **DFU MODE** on its tile instead of **READY**. Every erasure solution then restores its firmware at once, which erases the device - Advanced Erasure without the overwrite by the app. The station needs the firmware for the device (see Upload iOS Firmware 162).

macOS only: the tile's name ends in [Recovery] or [DFU]. A device in DFU mode is restored with Apple Configurator (see Requirements 199).

macOS only: for an iPhone or iPad in DFU mode, the bottom bar shows **FLASH SELECTED** instead of **ERASE SELECTED**, with the single entry **Flash firmware (no erasure report)**. In DFU mode the device shows only its ECID, so Securaze Mobile reinstalls its firmware but creates no erasure report. Once the device has started again, it is read as usual and can be erased with a report. A Mac in DFU mode keeps **ERASE SELECTED** and gets an erasure report - see Erase a Mac 86.

For more information on data erasure from iOS devices, see Menu Items - Data Erasure - iOS 198.


© 2026 Securaze GmbH

### 4.14.3 Erase Android device

After the Android device is connected and its details are read, select its tile and click **ERASE SELECTED** in the bar at the bottom of the window (see Perform erasure 81).

With **Data Clear**, Securaze Mobile resets the device to factory settings.

With **Advanced Erasure**, Securaze Mobile first clears the content of the device. If it cannot do that, it resets the device to factory settings instead and waits for it: go through the setup screen and turn on USB debugging again, as described in Connect Android device 60. Confirm "Allow USB debugging?" on the device with "Allow".

Then Securaze Mobile installs its app on the device, and the app overwrites the storage with the selected erasure standard. Afterwards the device is reset to factory settings again.

With **Smart Erasure**, an encrypted device is reset to factory settings as with Data Clear. A device that is not encrypted, or whose last run was a diagnosis, gets the full Advanced Erasure.

For more information on data erasure from Android devices, see Menu Items - Data Erasure - Android 203.

### 4.14.4 Erase a Mac

macOS only: Securaze Mobile erases Macs on macOS stations - Macs with Apple silicon and Intel-based Macs with the T2 chip. A Mac is erased in DFU mode: Securaze Mobile restores its firmware with Apple Configurator, which erases the Mac, and creates an erasure report for it.

#### Before you start

• **Apple Configurator**, free from the Mac App Store. If it is missing, Securaze Mobile shows **Apple Configurator required** when it starts; **OK** opens Apple Configurator in the Mac App Store.

• A USB-C cable that carries data, plugged into the DFU port of the Mac you erase - Apple's guide below names it for each model.

• The firmware: the macOS firmware for a Mac takes 17 to 27 GB. Securaze Mobile takes it from a Securaze Command on your network if there is one, otherwise from Apple (see Upload iOS Firmware 162). The station needs the free disk space for it.

• Current Apple device support on the station. If it is too old for the Mac's firmware, Securaze Mobile lists **Apple device support outdated** under Infrastructure issues 73 as soon as a Mac shows up, and Apple's updater opens. Install the update - it asks for the station's password; **Install now** in the issue opens the updater again - or update macOS.


© 2026 Securaze GmbH

## Put the Mac into DFU mode

Connect the Mac to the station. Then put it into DFU mode in one of two ways:

• **From Securaze Mobile**: a Mac that is switched on appears on a tile named **Mac (running)** - or **Mac / iPhone (running)** where the station cannot tell it from a locked iPhone - with the status **PUT INTO DFU**. Click **PUT INTO DFU**, or right-click the tile and choose **Put into DFU Mode**. For several Macs, select their tiles and choose **Put into DFU** under **MORE**; Securaze Mobile puts them into DFU mode one after the other. For this, the cable must go straight into a USB-C port of the station, not through a hub or dock.

• **By hand**: use the Mac's key combination, steps 1 and 2 in Revive or restore a Mac with Apple silicon using Apple Configurator 2 - Apple Support. Follow them exactly - it matters whether you hold the button before or after you connect the power. The Mac then appears on its tile by itself.

While Securaze Mobile puts the Mac into DFU mode, the tile shows **GOING INTO DFU**, and **DFU ATTEMPT** with the number of the attempt if the Mac needs further attempts - this can take a few minutes. In DFU mode the Mac appears on a tile whose name ends in [DFU], with the status **DFU MODE**.

If it does not work, a message says why - for example that the Mac is not directly on a USB-C port of the station, or that it did not come up in DFU mode. Check the cable and the ports, or use the key combination. To restart a Mac in DFU mode normally, right-click its tile and choose **Leave DFU Mode**.

## Erase the Mac

Select the Mac's tile and click **ERASE SELECTED**. A Mac is erased with Data Clear only: with Smart Erasure or Advanced Erasure chosen, the **Wipe Only Devices** window lists it, and **Continue** erases it with Data Clear (see Data erasure 197).

You can also select a running Mac and click **ERASE SELECTED**: Securaze Mobile puts it into DFU mode first, and the erasure starts by itself once the Mac is there. If the Mac is not in DFU mode within 3 minutes, the erasure is not started.

During the erasure the tile shows **Checking Apple device support**, the firmware download with its percent and speed, and the restore in percent. After the restore the Mac restarts, and the tile shows **Waiting for the serial number - the Mac shows it once it has restarted**, then **Checking the Mac by its serial number**. The erasure ends with **COMPLETED** or **FAILED**.

A Mac in DFU mode shows no serial number, so Securaze Mobile reads it after the restore. If it has not come 3 minutes after the restore, a message asks you to wake the Mac. You can also type the serial number - it is printed on the Mac - into **SERIAL NUMBER** in the device details, or click **Continue without serial number** there; the erasure report then has no serial number.


© 2026 Securaze GmbH

If the erasure fails because Apple Configurator waits to install a Device Support update, the message says so: install the update in Apple's Software Update window, then start the erasure again.

**FLASH SELECTED** is not used for Macs: it replaces **ERASE SELECTED** only for an iPhone or iPad in DFU mode (see Erase iOS device 85).

## 4.15 Check erasure in the main menu

While a phone is erased, its tile shows the progress.

With Standard tiles, click the tile to open its details; the **ERASURE SUMMARY** button in the details shows the erasure. With Detailed tiles, the eraser icon in the tile's header shows it on the tile. To show it on every detailed tile at once, choose **Erasure** under **All tiles** in the sidebar.

At the end of the erasure, Securaze Dashboard receives an erasure report, whether the erasure succeeded or failed.

You can find information on erasure reports under Reports - Download Deletion Report 152
.


© 2026 Securaze GmbH

## 4.16 Perform diagnose

Mobile Diagnostics is available in Securaze Mobile for Windows, macOS and Linux.

Prefer to watch it? Show me how to diagnose a phone – an animated step-by-step guide in your browser, with spoken narration.

The set of diagnose cases grows continuously. Recently added: the **Burn-In** case, and in the **Buttons** test the **Action Button** of newer iPhones and the **Camera Control** button of iPhone 16 and 17.

Open Securaze Mobile, connect the devices you want to diagnose and **select** them. The supported iOS and Android versions are listed under Supported Device OS 24.

At the bottom of the dashboard is a bar with the filters and the **DIAGNOSE SELECTED** and **ERASE SELECTED** buttons.

Click the **arrow** of **DIAGNOSE SELECTED** to open **Diagnose settings** and up to five favorite preselections (see below). Clicking a favorite starts it on the selected devices right away.

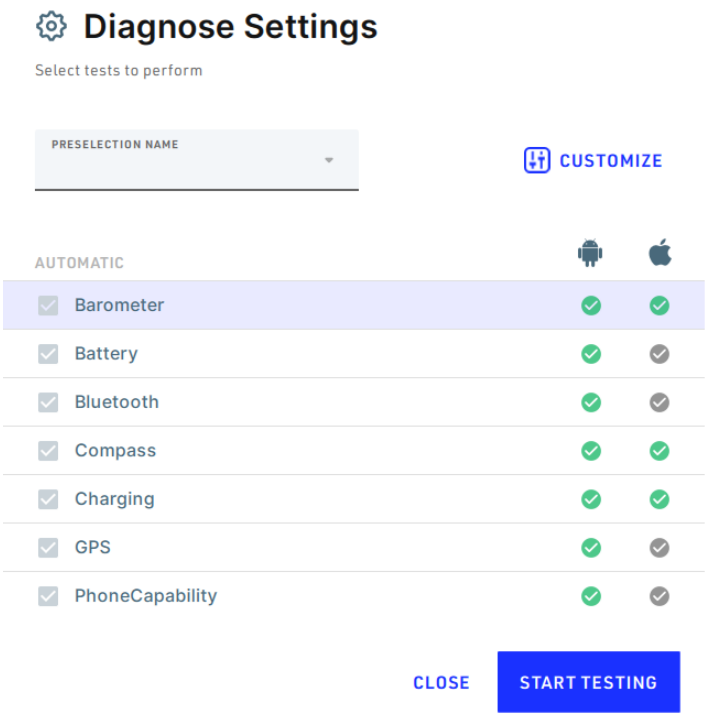
Click **DIAGNOSE SELECTED** to start the preselection chosen in **Diagnose Settings** on the selected devices. If no device is selected, the button opens **Diagnose Settings**.

In **Diagnose Settings** you see which preselection is chosen and which tests it runs. Choose another one under **PRESELECTION NAME**; each entry shows its number of tests.

In the upper area you will find the name of the preselection. Below that is a list of automatic and manual tests and whether they are available for iOS or Android.

At the very bottom you will find the buttons "Close" and "Start testing" ("Confirm" when no device is selected). At the top right, there is the "Customize" button. This leads to another window where you can select all available tests individually and either run them or save them as a new preselection.


© 2026 Securaze GmbH



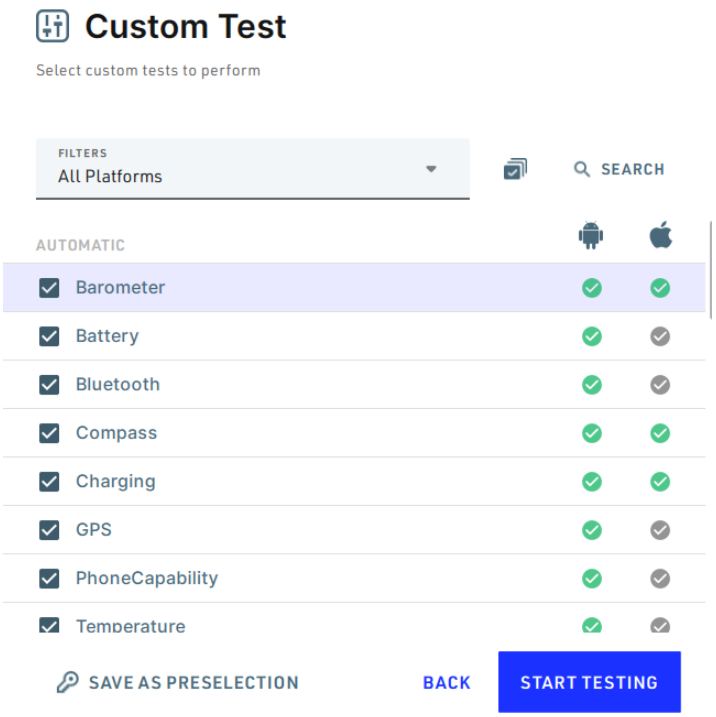

**Click** the "**Customize**" button.

The window **Custom Test** opens. There you can **filter** by platform, **select all tests** by clicking a button, or **search for a specific test**: click **Search** or press Alt+S. When filtering by platform, you can select either all platforms or only iOS or Android in each case.

Below that, you will find a list where you can select various automatic and manual tests and either run them immediately or save them as a pre-selection by an administrator.

At the bottom you can save the selection as a preselection (**Save as preselection**), go back (**Back**) or start the tests (**Start testing**).


© 2026 Securaze GmbH

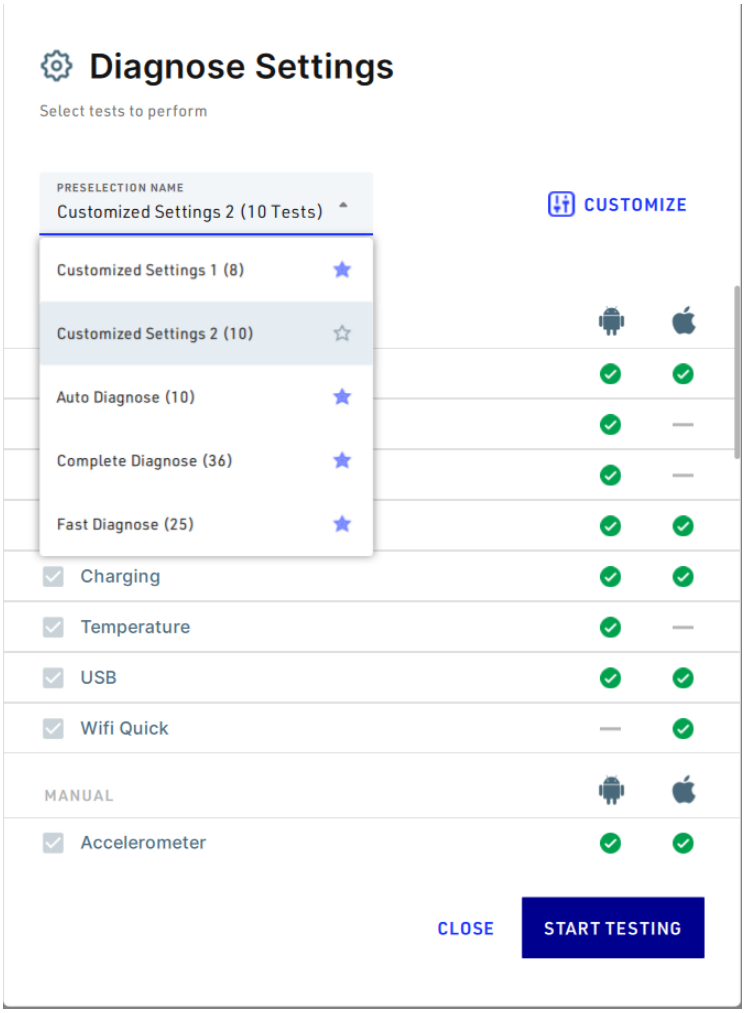



To save a preselection you need the right to do so. Without it, Mobile first asks for an admin login: **Change Settings** - enter **Securaze ID** and **Password**, then click **Log-in**.

In **Save as Preselection**, type a name and click **Save**. The preselection is saved on the Securaze server, so all stations of your company can use it.

To add a **preselection to your favorites** (so that it shows up under the arrow of DIAGNOSE SELECTED), simply **click on the star icon** next to the preselection name in the list. This will mark the preselection as a favorite, making it readily accessible for future diagnoses. You can mark up to five favorites.


© 2026 Securaze GmbH




In the bottom horizontal bar you will also find a **book icon**, which will take you to the pop-up window "**Instructions**".

In the **Instructions** there are the menu items **Pinned**, **Set-up** and **Diagnose**. Under **Pinned** you find the instructions you pinned (the … menu of an instruction, **Pin tutorial**). Under **Set-up**: **Wi-fi enabling / iOS** and **QR-Code / Android**. Under **Diagnose**: **Face ID setup**, **Touch ID setup**, **NFC** and **Wireless charging**.

## Setup

### Wi-fi Enabling/iOS

To install a Wi-Fi profile on the desired device, you need to follow these 5 steps:

1. Open the Settings app.
2. Go to General.
3. Select VPN & Device Management.
4. Select Wi-Fi Profile.


© 2026 Securaze GmbH

5. Tap Install in the upper-right corner and follow the onscreen instructions.

**QR-Code/Android**

To turn on USB debugging from the setup screen of an Android device, follow these 8 steps:

1. Tap anywhere on the screen 7 times.
2. Scan the QR code.
3. Press 'Next' / 'Approve' (text on screen may vary).
4. Press 'Continue'.
5. Wait for the Securaze App screen to pop up.
6. Plug in the phone to a station running Securaze Mobile.
7. Allow USB debugging (press 'Allow' button).
8. Done!

Supported Android 16 devices and later can also be connected without USB debugging in **Android Express Mode**, and Samsung devices in **Samsung Non-ADB communication** - see Connect Android device 60.

You can also find more information about the QR Code ADB Bypass Method here: Android USB-Debugging bypass with QR-Code 60

**Diagnose**

**Face ID setup**

To properly set up Face ID on your device, follow the 8 steps below:

1. Make sure that nothing is covering the camera or your face.
2. Go to Settings, then tap Face ID & Passcode. If needed, enter your passcode or set new one.
3. Tap Set Up Face ID.
4. Tap Get Started.
5. Position your face inside the frame and gently move your head to complete the circle.
6. When you finish the first Face ID scan, tap Continue.
7. Gently move your head to complete the circle for a second time.
8. Tap Done.

**Touch ID setup**

To create a fingerprint on your device, follow these 6 steps:


© 2026 Securaze GmbH

1. Create a passcode for your device if you don´t have one.
2. Tap Settings > Touch ID & Passcode.
3. Tap Add a Fingerprint.
4. Touch the Touch ID sensor with your finger without pressing. Hold your finger until you feel a quick vibration, or as indicated on screen.
5. Continue to lift and rest your finger slowly, adjusting the position of your finger each time.
6. Adjust your grip. Touch the Touch ID sensor with the outer areas of your fingertip, instead of the center portion that you scanned first.

### NFC

To confirm that NFC is working properly on your device, hold the top of your phone close to a NFC tag or terminal. Make sure the NFC tag contains information to prevent the test from failing.

### Wireless charging

To test the wireless charging, place the phone face up on the charging pad and look for the charging symbol on the phone display. Make sure the wireless charger is compatible with your device to prevent the test from failing.


© 2026 Securaze GmbH

# Operation

Below you will find an **overview** of all **diagnostics cases** divided into **categories**.

**Camera**

| Name | Type | Android | iOS | Short description | Link |
|---|---|---|---|---|---|
| Flashlight | Manual | x | x | The flashlight is activated; the operator verifies if it illuminates correctly. | Flashlight 104 |
| Front Camera | Manual | x | x | A front camera photo is taken; operator examines image clarity. | Camera Tests 104 |
| Rear Camera | Manual | x | x | A rear camera photo is taken; operator examines image clarity. | Camera Tests 104 |
| Rear Telephoto Camera | Manual | x | x | A rear telephoto camera photo is taken; operator examines image clarity. | Camera Tests 104 |
| Rear Ultrawide Camera | Manual | x | x | A rear ultrawide camera photo is taken; operator examines image clarity. | Camera Tests 104 |
| Rear Wide Camera | Manual | x | | A rear wide camera photo is taken; operator examines image clarity. | Camera Tests 104 |
| Rear Macro Camera | Manual | x | | A rear macro camera photo is taken; operator examines image clarity. | Camera Tests 104 |

| Name | Type | Android | iOS | Short description | Link |
|---|---|---|---|---|---|
| Rear Mono Camera | Manual | x | | A rear mono camera photo is taken; operator examines image clarity. | Camera Tests 104 |

**Camera Quick**

| Name | Type | Android | iOS | Short description | Link |
|---|---|---|---|---|---|
| Front Camera | Manual | x | x | A front camera photo is taken; operator examines image clarity. | Camera Tests 104 |
| Rear Camera | Manual | x | x | A rear camera photo is taken; operator examines image clarity. | Camera Tests 104 |

**Communication**

| Name | Type | Android | iOS | Short description | Link |
|---|---|---|---|---|---|
| Bluetooth | Automatic | x | | The operator needs a Bluetooth device to start a Bluetooth pairing on to see if the Bluetooth functionality of the device works. | |
| NFC | Manual | x | x | NFC functionality tested using an NFC tag. | |

# Operation

| Name | Type | Android | iOS | Short description | Link |
|---|---|---|---|---|---|
| Phone Capability | Automatic | x | | A sim card must be inserted and a phone number must be set in the dashboard, and then it will check if the phone can make a call. | |
| Wifi | Manual | x | | The operator must connect to Wifi to see if it is working and connecting to a network. | |
| Wifi Quick | Automatic | | x | The Wifi function of a device is checked. | |
| Live Call | Manual | x | x | A phone call is initiated. | Live Call 141 |

**Control**

| Name | Type | Android | iOS | Short description | Link |
|---|---|---|---|---|---|
| Buttons | Manual | x | x | The operator presses all buttons of the device one by one. On newer iPhones this includes the Action Button and, on iPhone 16 and 17, the Camera Control button. | Various buttons 111 |

**Physical connection**

| Name | Type | Android | iOS | Short description | Link |
|---|---|---|---|---|---|
| Headphones | Manual | x | | The operator connects headphones to the mobile device and verifies if the sound plays clearly. | Headphones 116 |

| Name | Type | Android | iOS | Short description | Link |
|---|---|---|---|---|---|
| USB | Automatic | x | x | It is checked whether the USB cable connection is working. | |

**Screen**

| Name | Type | Android | iOS | Short description | Link |
|---|---|---|---|---|---|
| Multi Touch | Manual | x | x | It is checked whether several simultaneous touches of the screen are detected or not. To do this, the operator must touch the screen several times at the same time. | MultiTouch 122 |
| Screen | Manual | x | x | The operator checks the phone's screen for possible malfunctions or damage. | Screen Display 117 |
| Burn-In | Manual | x | x | Gray and black fields that change with each tap show a faint ghost of an old image (burn-in), e.g. of the status bar or the keyboard. The operator marks the affected areas with a long press and taps Burn-in found, or taps Screen is clean. | |
| Screen Condition State | Manual | x | x | The operator is asked whether the screen has cracked or not. | |
| Touch Screen | Manual | x | x | The operator touches various points on the screen one by one to check if the whole screen reacts to touches. | TouchScreen 119 |

| Name | Type | Android | iOS | Short description | Link |
|---|---|---|---|---|---|
| 3D Touch | Manual | | x | The operator is required to apply pressure on the screen, and it is determined how the device responds to different levels of force applied by the user. | 3D Touch 124 |

**Sensors**

| Name | Type | Android | iOS | Short description | Link |
|---|---|---|---|---|---|
| Accelerometer | Manual | x | x | The operator has to tilt the mobile device 90 degrees to see if the status of the accelerometer changes. | Accelerometer 127 |
| Barometer | Automatic | x | x | it is checked whether the sensor provides values. | |
| Compass | Automatic | x | x | it is checked whether the compass of the device is working properly. | |
| Face ID | Manual | | x | The operator has to hold his face in front of the mobile device and let the face recognition scan it and see if it is fully recognized and working. | Face ID 128 |
| Face ID | Automatic | | x | Face ID sensor data is used for the diagnose case. | Face ID Quick 128 |
| Fingerprint | Manual | x | x | The operator has to place his finger on the fingerprint sensor and has to see if the finger is recognized correctly by the sensor. | Fingerprint 130 |
| Fingerprint Quick | Automatic | | x | Fingerprint sensor data is used for the diagnose case | Fingerprint Quick 130 |

| Name | Type | Android | iOS | Short description | Link |
|---|---|---|---|---|---|
| Gravity | Manual | x | | Both the accelerometer and gyroscope functionality of Android devices are checked. | |
| Gyroscope | Manual | x | x | The operator must move the mobile device and see if the device receives data or senses that it is being moved.. | |
| Proximity | Manual | x | x | The operator has to move the hand in front of the mobile device and it is tested whether the device senses any movement. | Proximity 132 |
| Temperature | Automatic | x | | it is checked whether the sensor provides values. | |

**Sound**

| Name | Type | Android | iOS | Short description | Link |
|---|---|---|---|---|---|
| Microphone | Manual | x | x | The operator emits sounds to test microphone's ability to perceive and record sound. | Microphone 136 |
| Speakers | Manual | x | x | The operator checks if the other speakers of the phone produce clear sound. | Speaker 133 |

**System**

| Name | Type | Android | iOS | Short description | Link |
|---|---|---|---|---|---|
| Battery | Automatic | x | | It is checked whether the battery of the device works or has problems. | |

# Operation

| Name | Type | Android | iOS | Short description | Link |
|---|---|---|---|---|---|
| Charging | Automatic | x | x | It is checked whether the device has registered the charger and is actively charging. | |
| Vibration | Manual | x | x | The operator must confirm whether the device vibrates or not. | Vibration 139 |
| Wireless Charging | Manual | x | | The operator has to place the mobile device on a wireless charging station and verify that wireless charging works. | Wireless Charging 140 |
| Battery Discharge | Manual | x | x | The battery is getting discharged based on the diagnose case parameter. | Battery Discharge 142 |

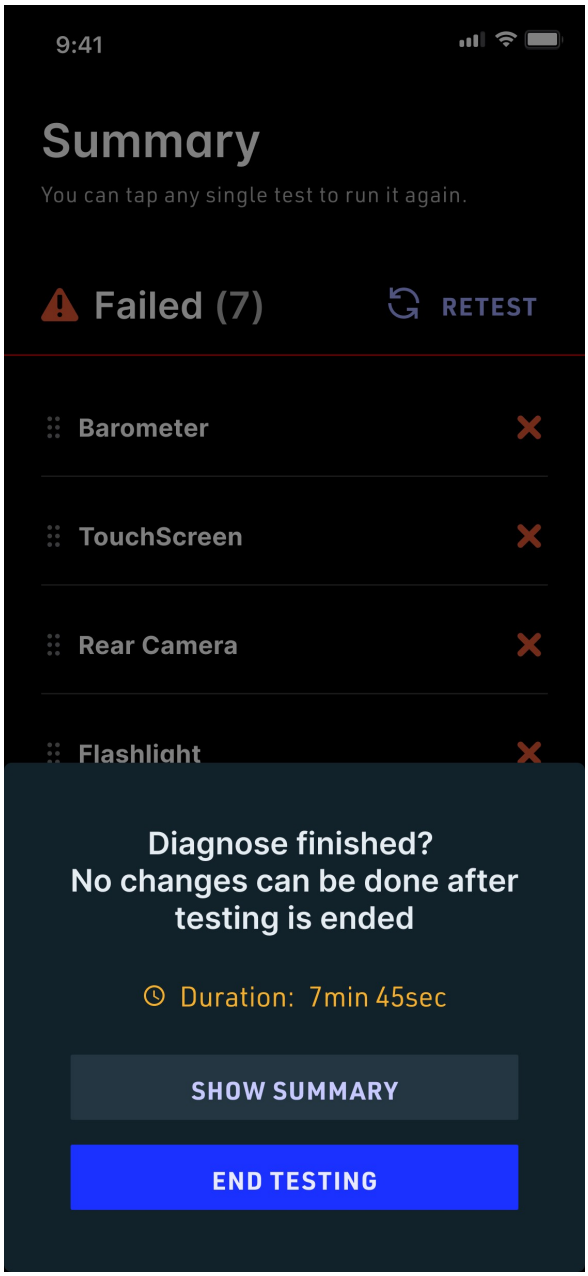
After the start, the device shows **Now you can unplug your phone and continue wireless**. Unplug it: the diagnose continues without the cable, and the tests run the same way.

With **Expert Diagnose Mode** (Options & Settings > General) the device stays plugged in, and the explanatory texts are skipped for a faster diagnose.

At the end the device shows **Diagnose finished?** with the duration, **Show summary** and **End testing**. Until then you can view the results and repeat tests. Tap **End testing**. Unplugged, the device then asks you to plug it back in (**All done! Please plug back your phone to the initial station**); as soon as it is plugged in, the results are sent. Plugged in, it shows **Please wait a moment while we upload the results**. With **Automatic Finish Diagnose and Upload results** (Options & Settings > Processing), the diagnose ends and uploads by itself after the last case.

NOTE: In wireless mode, it has to be noted that the device must be plugged back into the same mobile station where it was started, but it may be plugged into any cable/port on the station.


© 2026 Securaze GmbH




When a test is started, you can see in the upper left corner which device is being tested and the station ID.

The status of the tests can be "Not started", "No result", "In progress", "Succeeded", "Failed", "Aborted" and "Not available". Click on the test name to get the status described in words.

Here you will also find a button to either start or re-run the test.

To grade the device on the device itself after the diagnose, right-click its tile and choose **Grade on device**. See Menu 187.

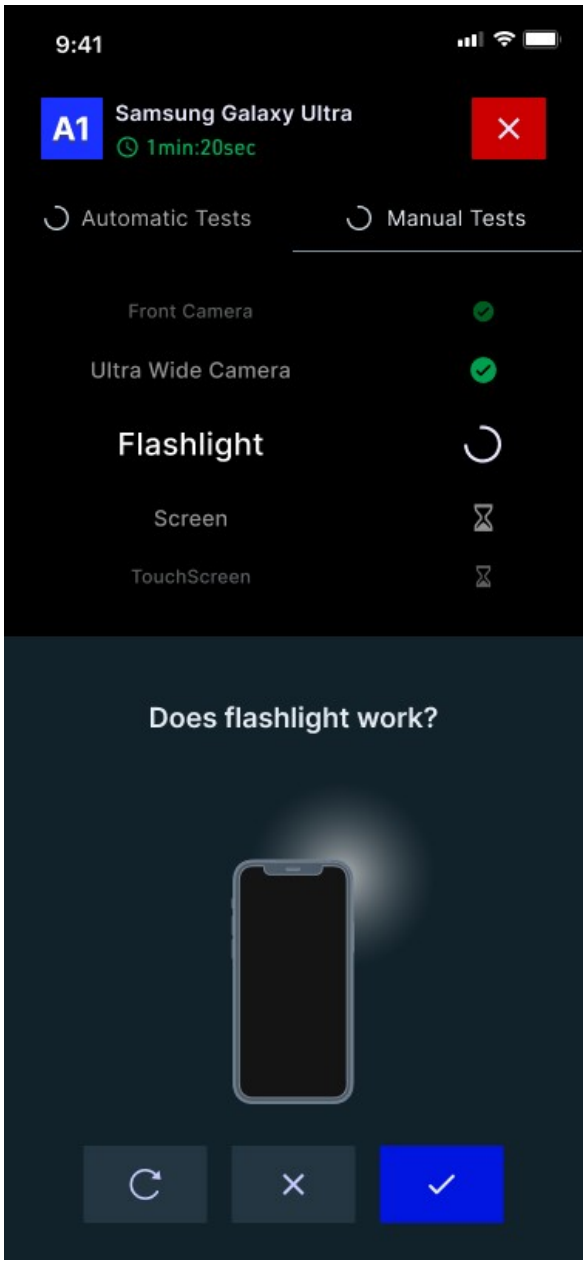
### 4.16.1 Description Manual Tests

Here you can find a **description of each manual test** with screenshots.


© 2026 Securaze GmbH

### 4.16.1.1 Flashlight

In the flashlight test, the **flashlight** is turned on and you are to see whether it **lights up or not**. Here you have to answer with a check mark for "Yes", x for "No" or the far left icon for "Repeat test".

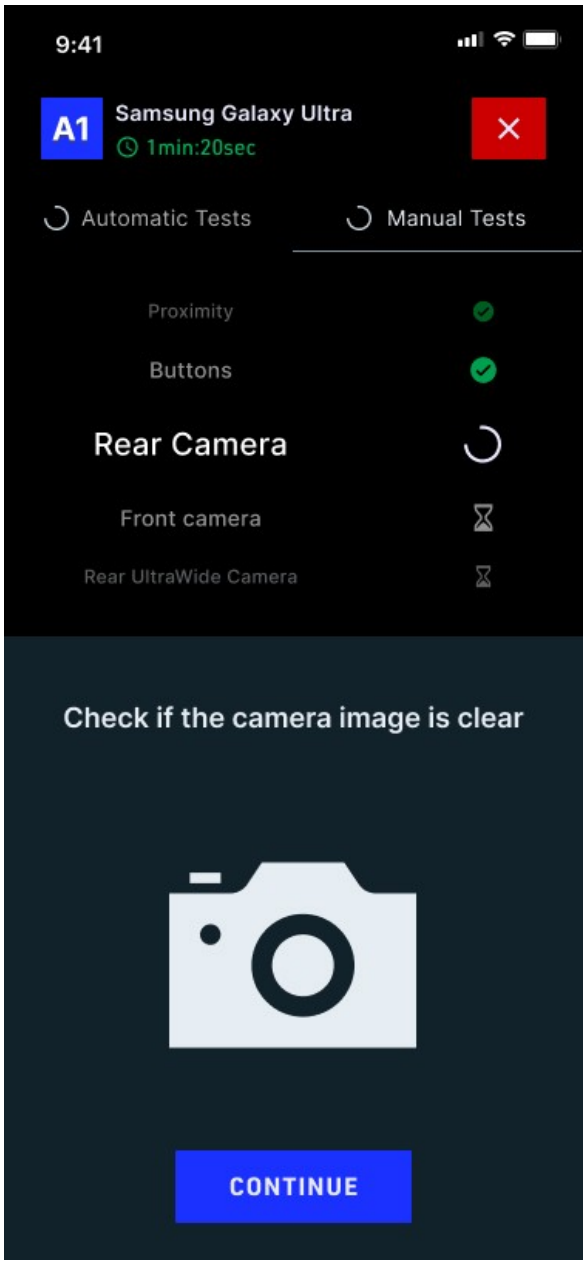



### 4.16.1.2 Camera Tests

#### Rear Camera

In this test, the rear camera is opened and you have to see if the **image** is **clear**. Answer with a check mark for "Yes", x for "No" or the icon on the far left for "Repeat test".


© 2026 Securaze GmbH





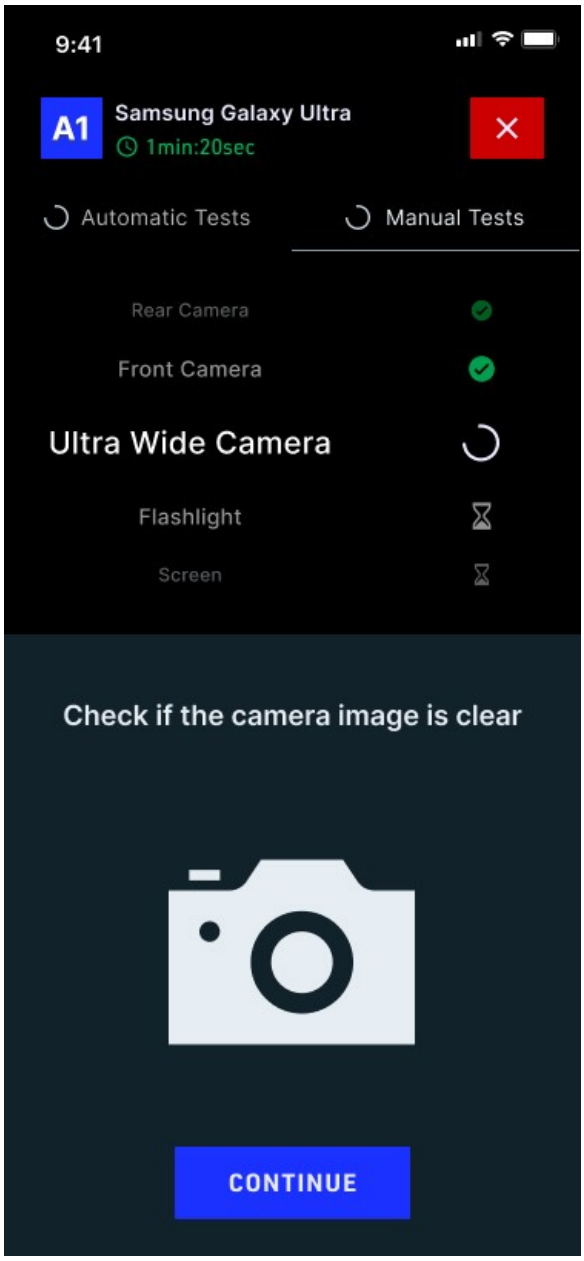
© 2026 Securaze GmbH




#### Ultra Wide Camera

This test also checks the rear camera and you need to see if the **image** is **clear**. The answer options are check marks for "Yes", x for "No" or the far left icon for "Repeat Test".

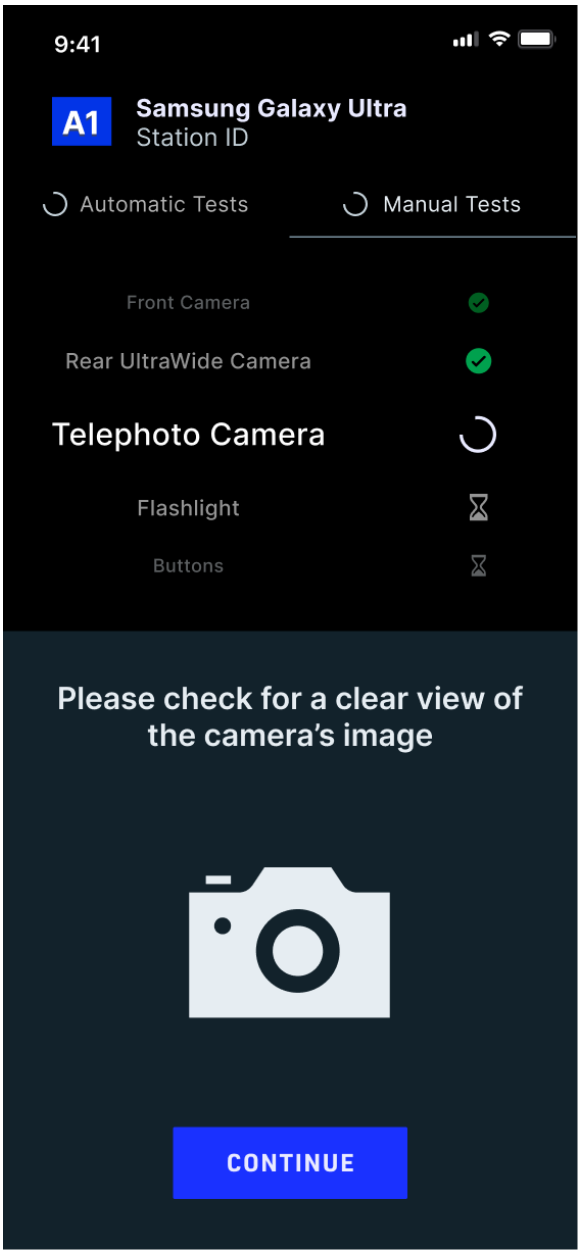

© 2026 Securaze GmbH




**Telephoto camera**

Here the rear camera is tested and you are to look for a **clear image**. The answer options are check marks for "Yes", x for "No" or the far left icon for "Repeat test".

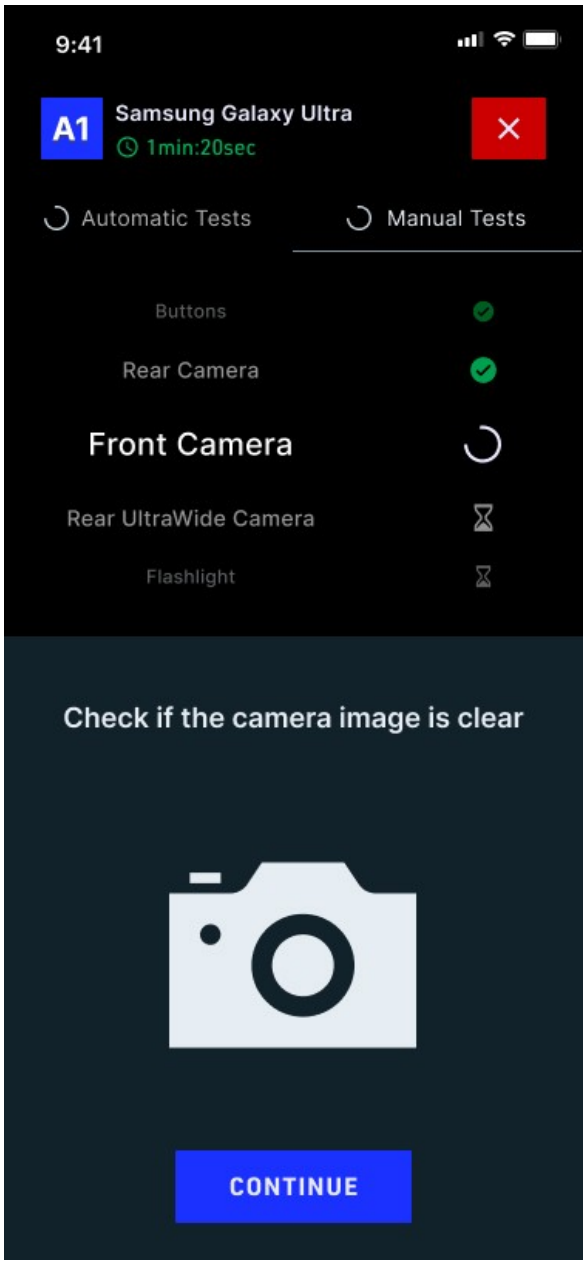

© 2026 Securaze GmbH




**Front camera**

In this test, the front camera is checked. Make sure that the **picture** is **clear** here as well. Answer with check marks for "Yes", an x for "No" or the far left symbol for "Repeat test".


© 2026 Securaze GmbH





© 2026 Securaze GmbH




#### Macro Camera

On devices that have a dedicated macro camera, follow the on-screen prompt to capture a close-up image and confirm the result.

#### Monochrome Camera

On devices that have a dedicated monochrome (black-and-white) camera, follow the on-screen prompt to capture an image and confirm the result.

### 4.16.1.3 Camera Quick Tests

Running a few Camera tests for Android and iOS:

- Front Camera

- Back Camera

This test case is useful if not all Android / iOS cameras need to be tested, which could be a lengthy process.


© 2026 Securaze GmbH

#### 4.16.1.4 Various buttons

**Depending** on the **phone brand** and **model**, there are **different buttons**.

First you will find the description for iPhones with Face ID and for iPhones with a Home button, then for Android and Samsung phones.

**iPhone**

**On/OFF**

On the **latest iPhones**, **press** the **volume up button** and the **power button at the same time**.

On **older iPhone** models, you need to **press** the **Home and Power buttons at the same time**.

**Volume up/down**

On the **latest iPhones**, **press** the **Volume Up** or **Volume Down** button first, and then press the other one.

On the **older models**, you will also need to press the **Volume Up** and **Volume Down** buttons in succession.

**Mute/Ringer switch**

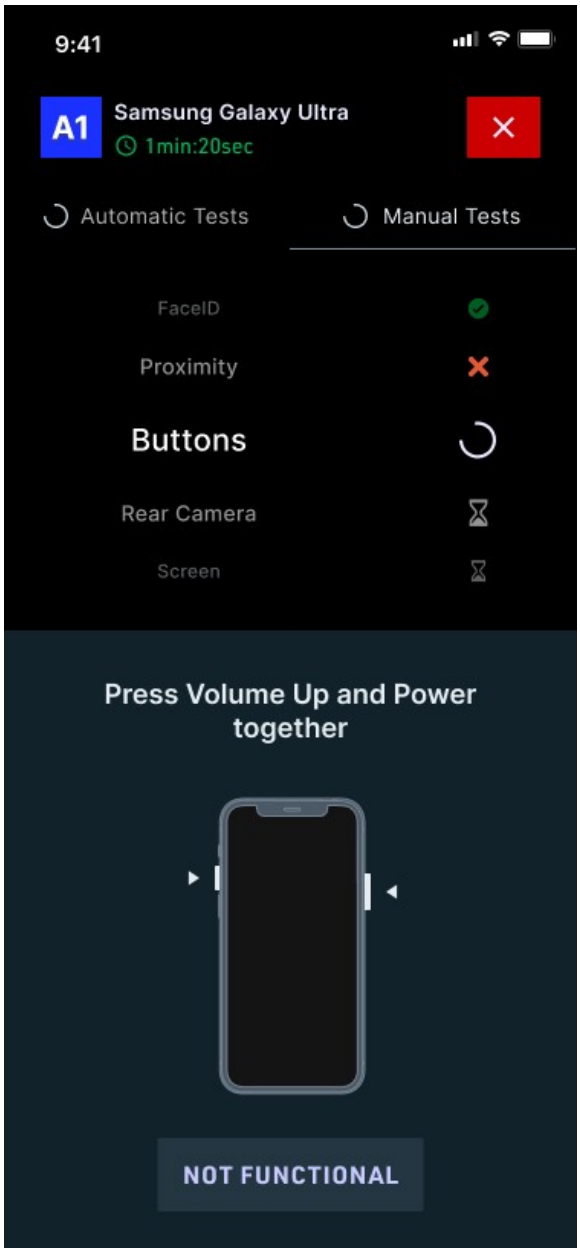
For the Mute test, **flip** the small **switch** above the volume buttons. On iPhone 15 Pro and later (also iPhone 16e) there is no switch: press the **Action Button** instead. The test detects Silent mode, which is what the Action Button does by default.

**Camera Control**

On iPhone 16 and iPhone 17 models (not iPhone 16e) with iOS 17.2 or later, a third step follows: **Press the Camera Control button**. Press the button on the lower right side of the phone.

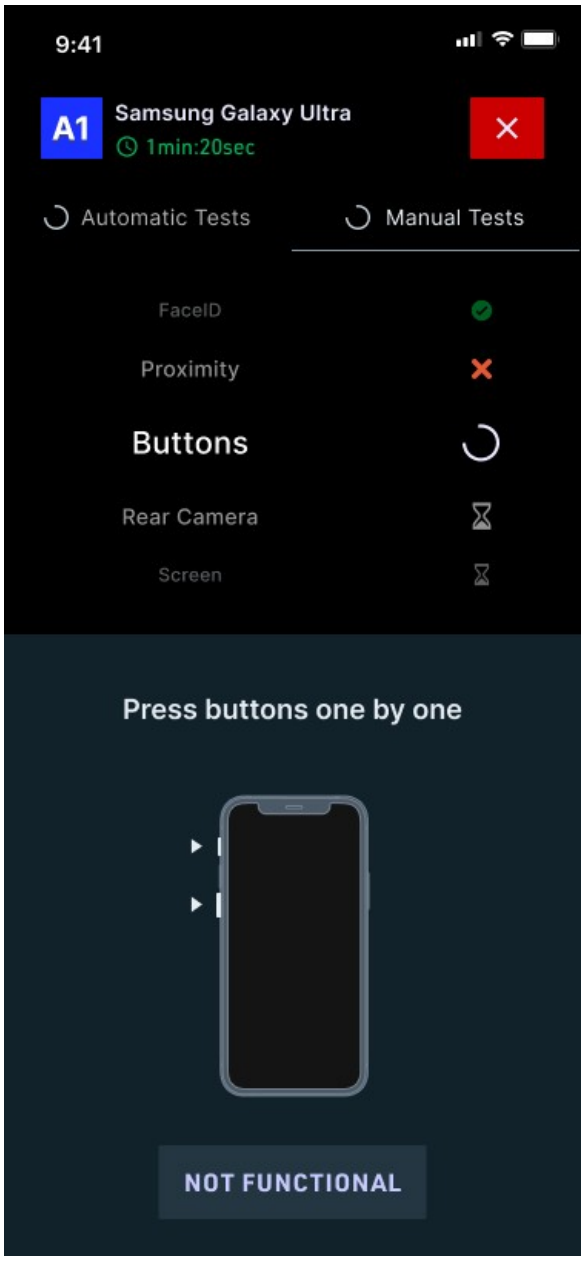
If a green check mark appears next to all buttons, the test is successful. Otherwise press **Not functional**: the buttons not pressed in this step fail. If a button does not exist on the device, tap **Remaining not available** - it appears after 5 seconds.


© 2026 Securaze GmbH



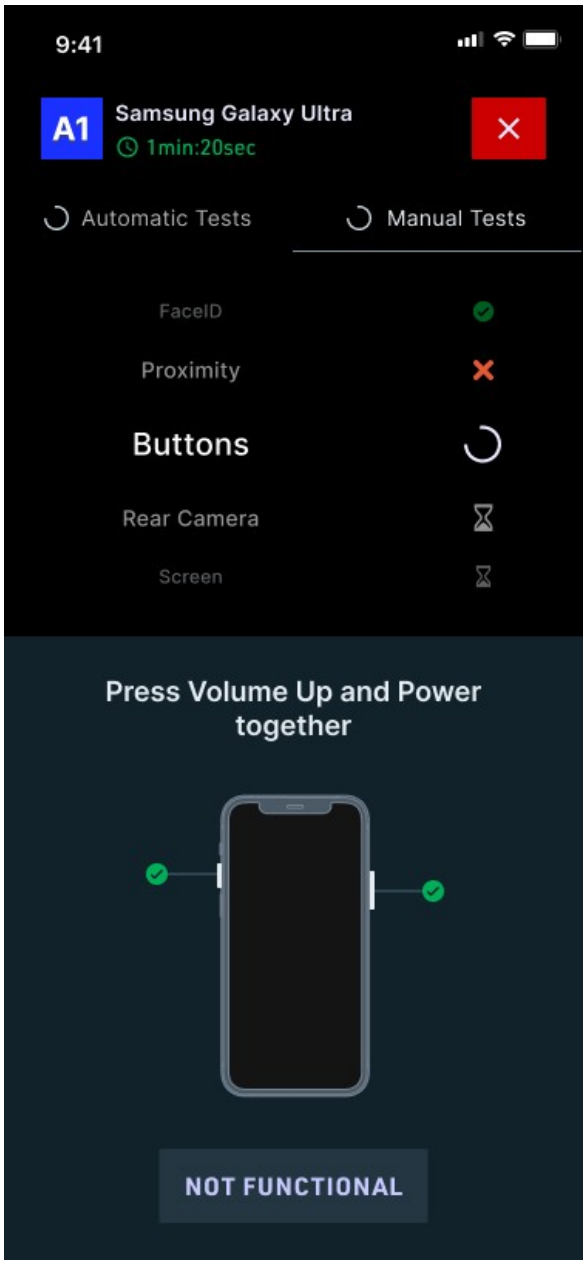


© 2026 Securaze GmbH



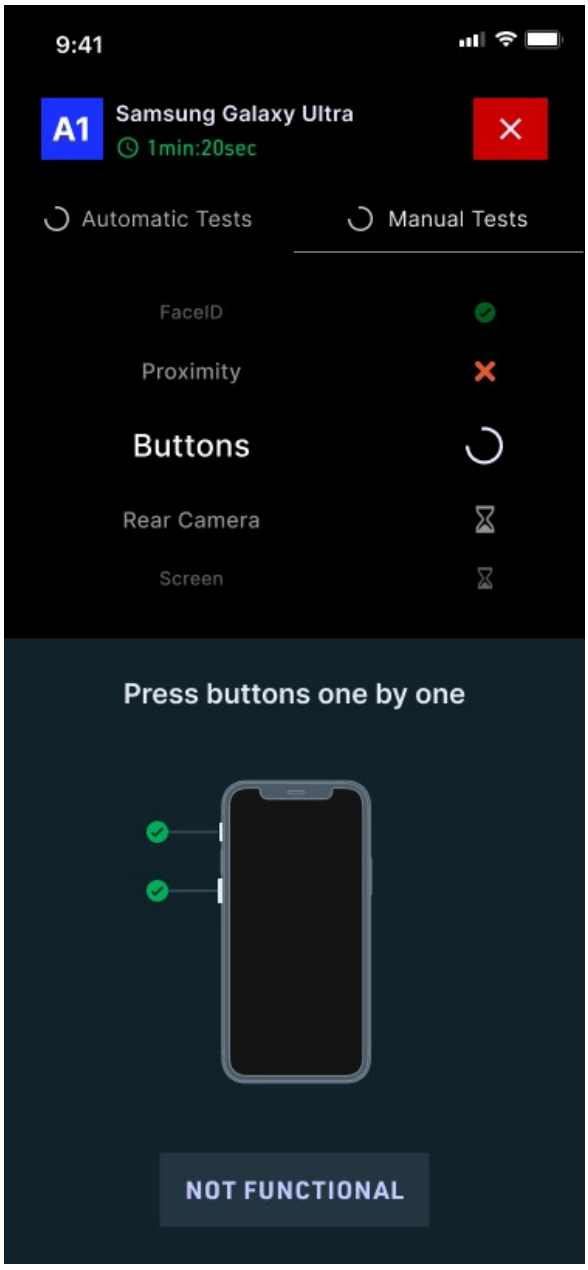


© 2026 Securaze GmbH





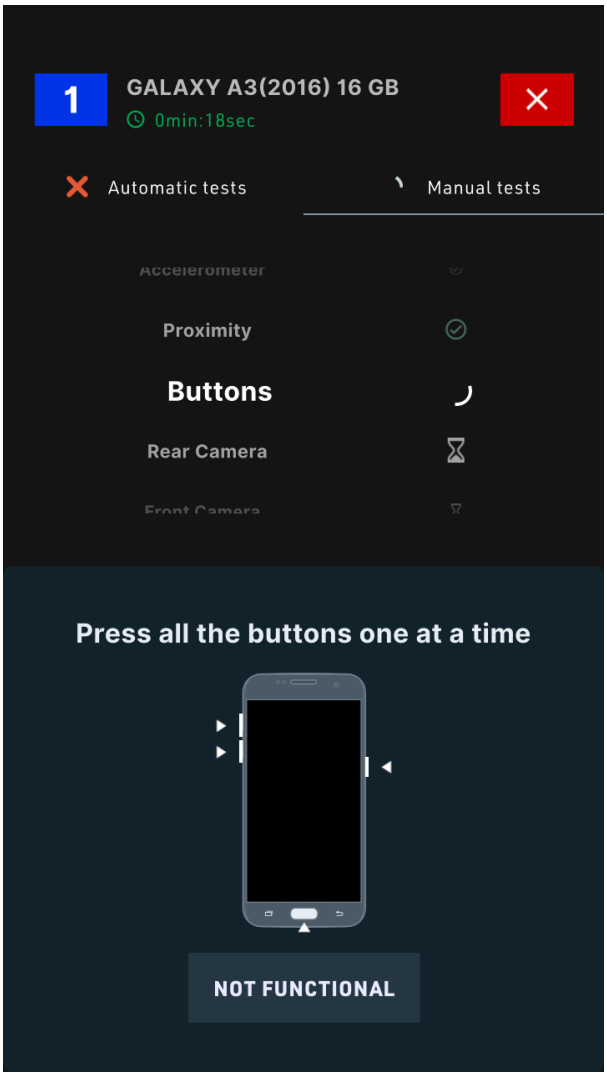
© 2026 Securaze GmbH




**Samsung**

On Android phones, press all buttons shown **one by one** - for example **volume up** and **volume down**, the **power button** and, where the phone has them, the **home button**, Back or Bixby - until a green check mark appears next to each.

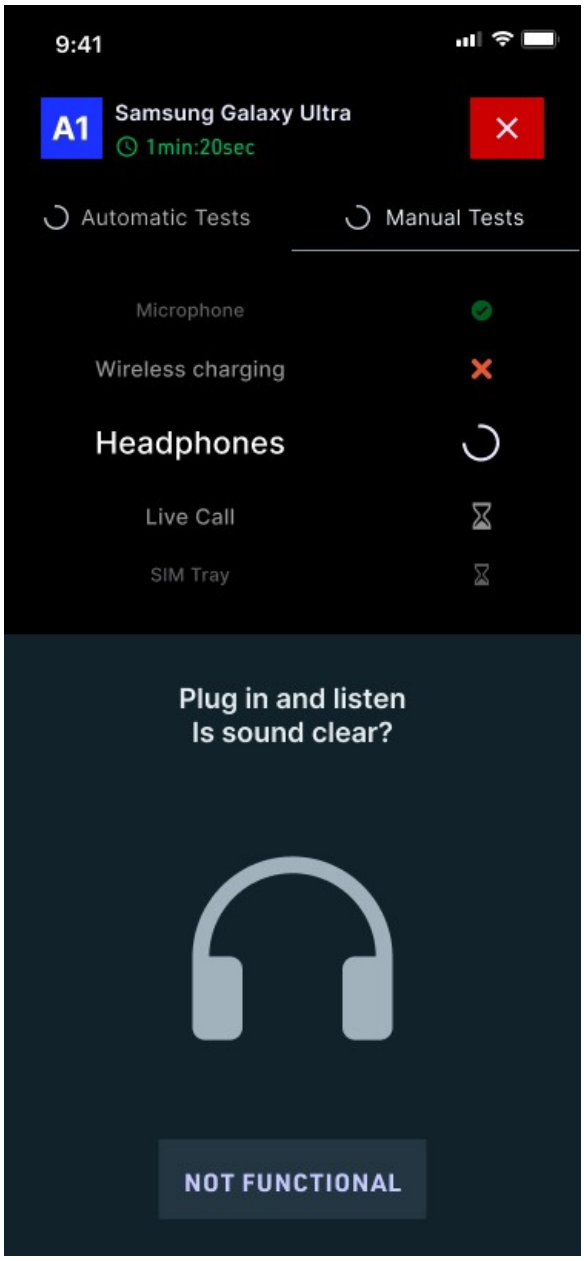

© 2026 Securaze GmbH




#### 4.16.1.5 Headphones

**Plug in headphones** during the headphone test. Then a sound is played through the headphones. Press the check mark when you have heard the sound loud and clear. If you did not hear the sound, you can repeat the test or click the x.

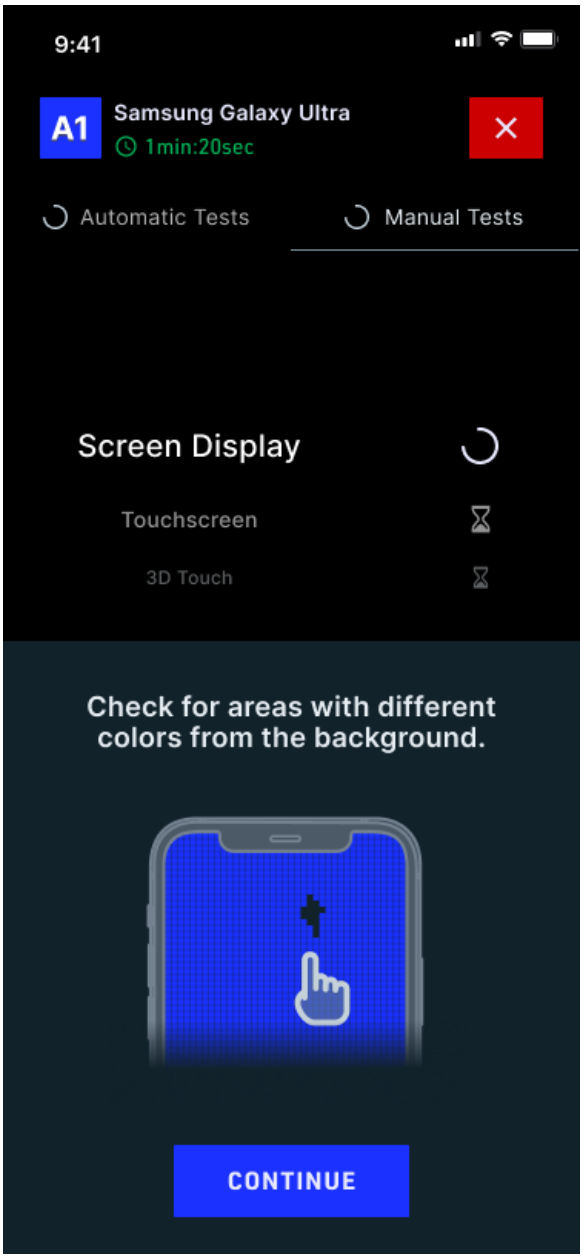

© 2026 Securaze GmbH




### 4.16.1.6 Screen Display

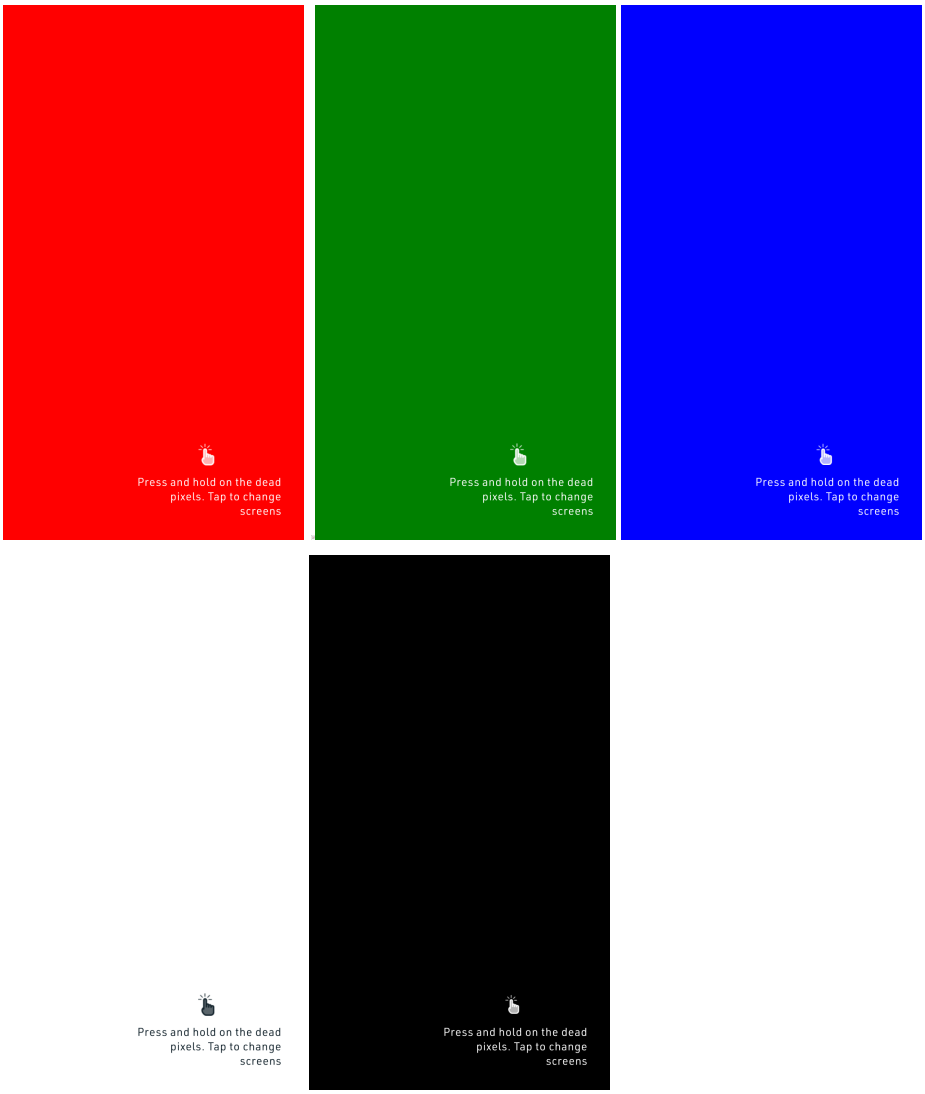
The screen test checks the phone's screen for possible malfunctions or damage. First, a window appears - **click "Continue"**. **Touch the screen** to see the next color. The screen will be completely colored one by one in red, green, blue, white and black. At the end, click "Dead pixels found", "No dead pixels found" or "Run again", depending on the result of your test.


© 2026 Securaze GmbH





© 2026 Securaze GmbH



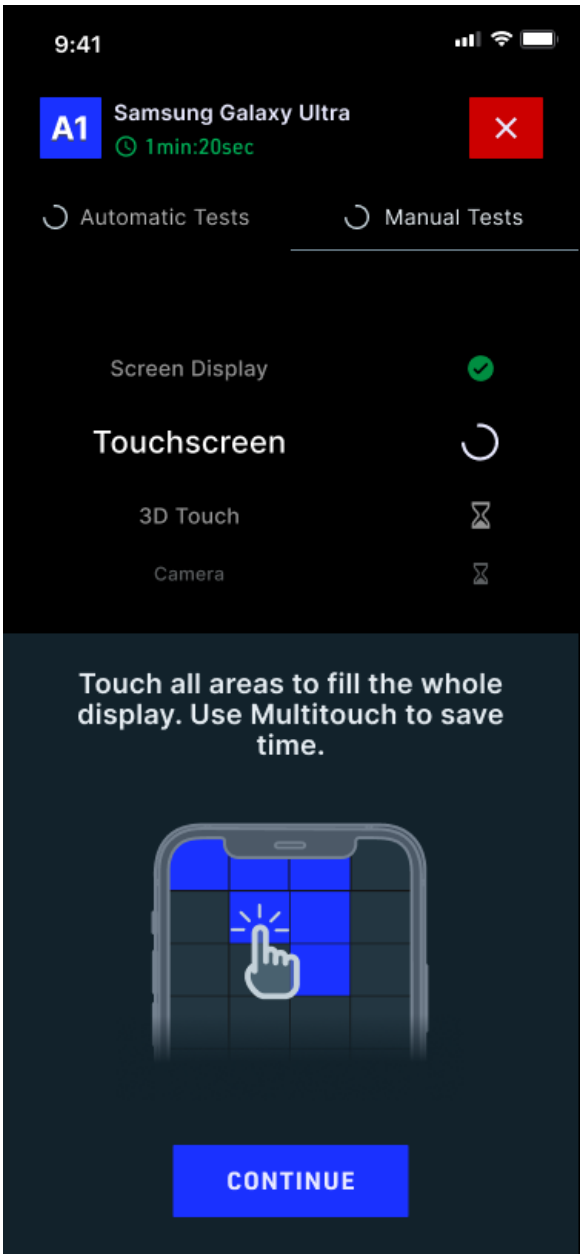

### 4.16.1.7 TouchScreen

In this test, the screen is filled with small gray squares that you have to touch all of them. **Press** on all the **squares**. If the screen works, the square will change color and become light blue.

In this test, the screen displays numerous small gray squares that need to be touched. **Press each square** individually or **touch multiple squares** at once; a functioning screen will cause the squares to change color to light blue. If you touch up to 3 squares simultaneously, the **multitouch test-case** will automatically pass.

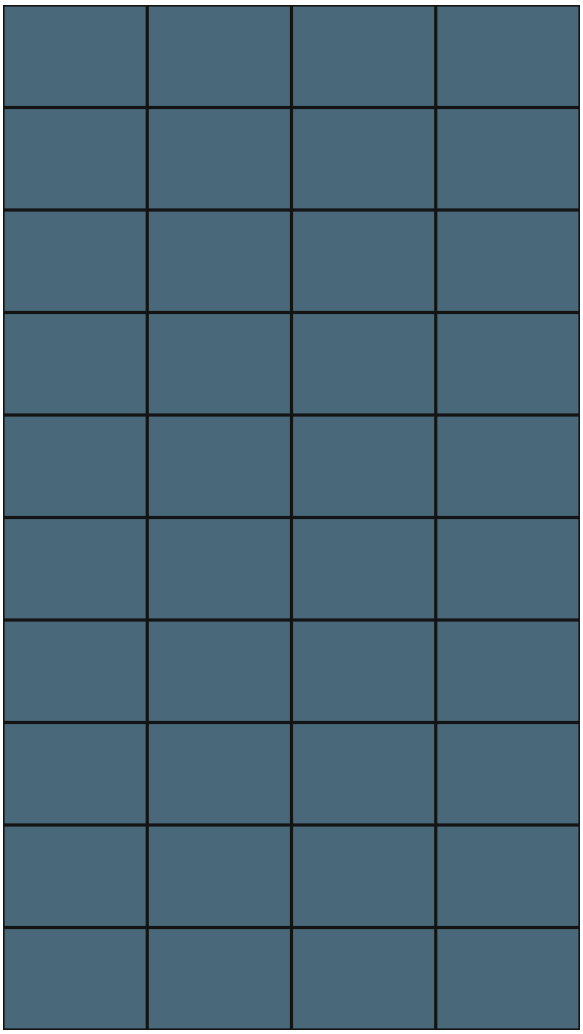
If not all areas are light blue, the application will ask you if the screen is defective and the operator can choose to continue or fail the test.


© 2026 Securaze GmbH

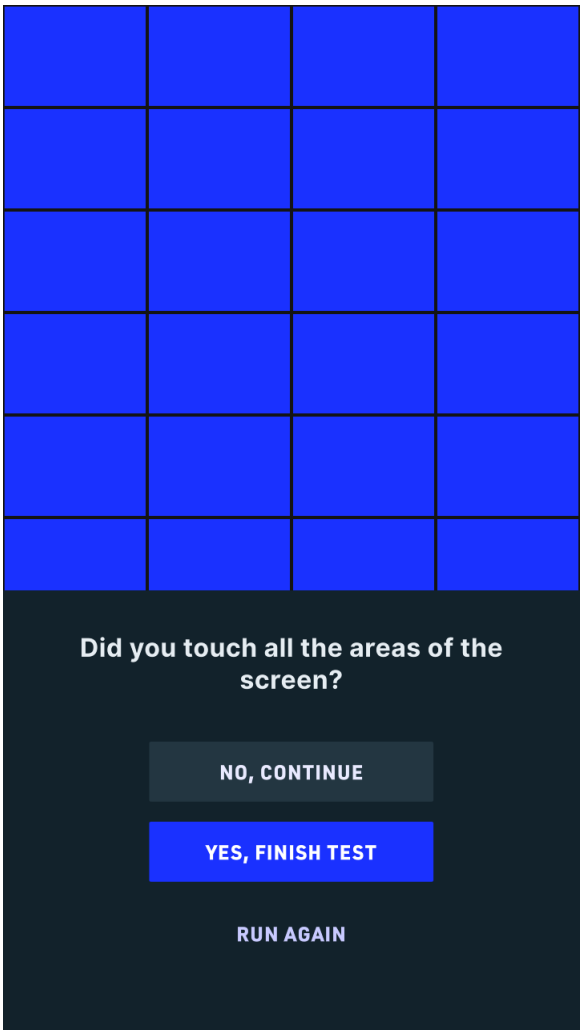




© 2026 Securaze GmbH



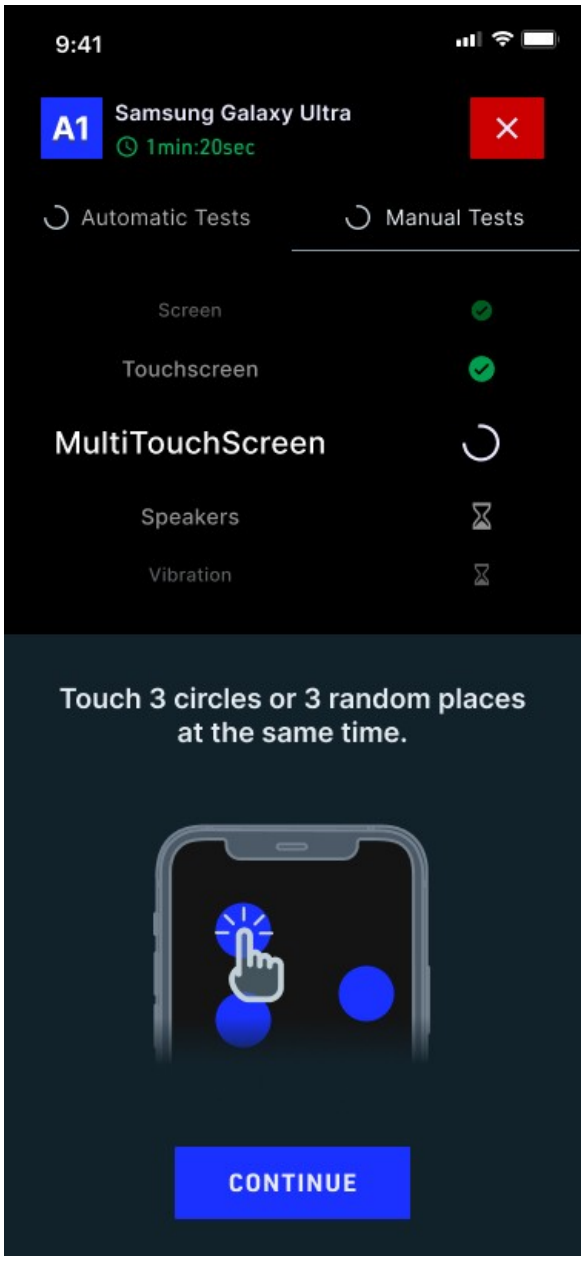

© 2026 Securaze GmbH




### 4.16.1.8 MultiTouch

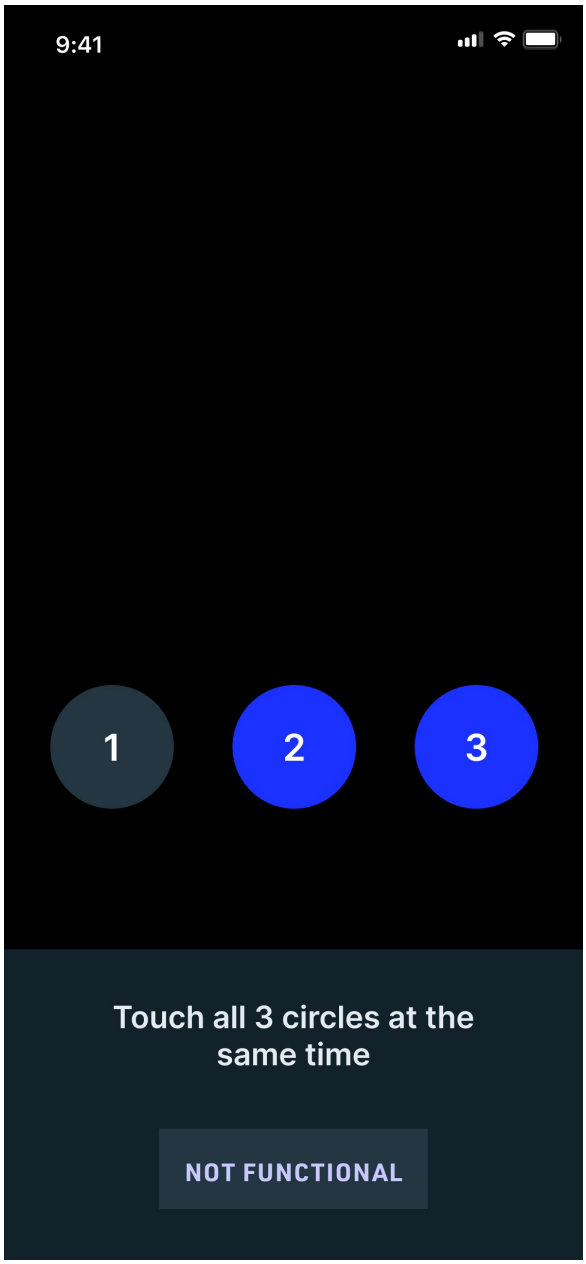
Here **3 circles** appear on the screen and you need to **press** all three at the same time. If all 3 circles do not turn light blue, click "Not functional".


© 2026 Securaze GmbH





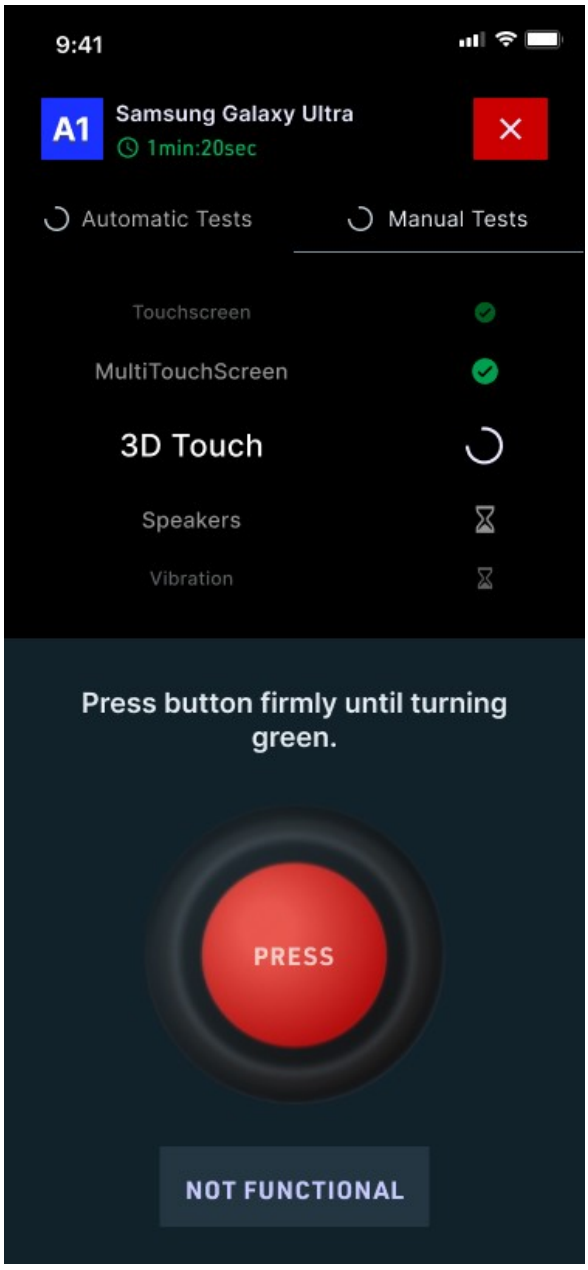
© 2026 Securaze GmbH




### 4.16.1.9 3D Touch

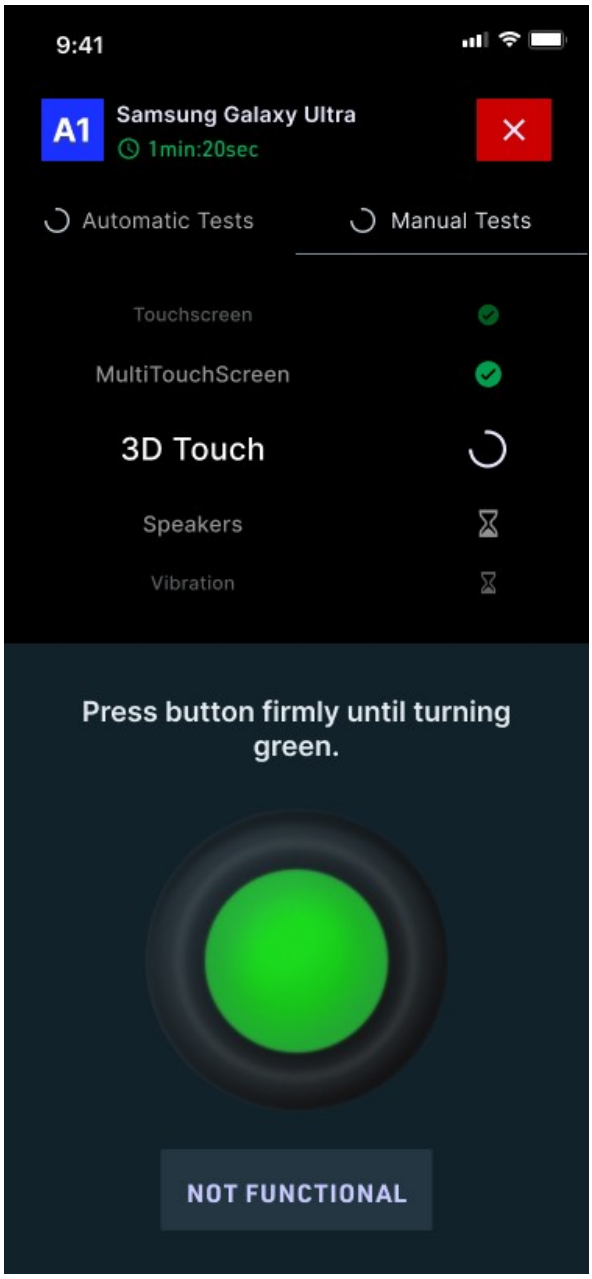
**Press** the **red button firmly** here until it turns green. If it does not turn green but remains red, the "Not functional" button must be pressed.


© 2026 Securaze GmbH



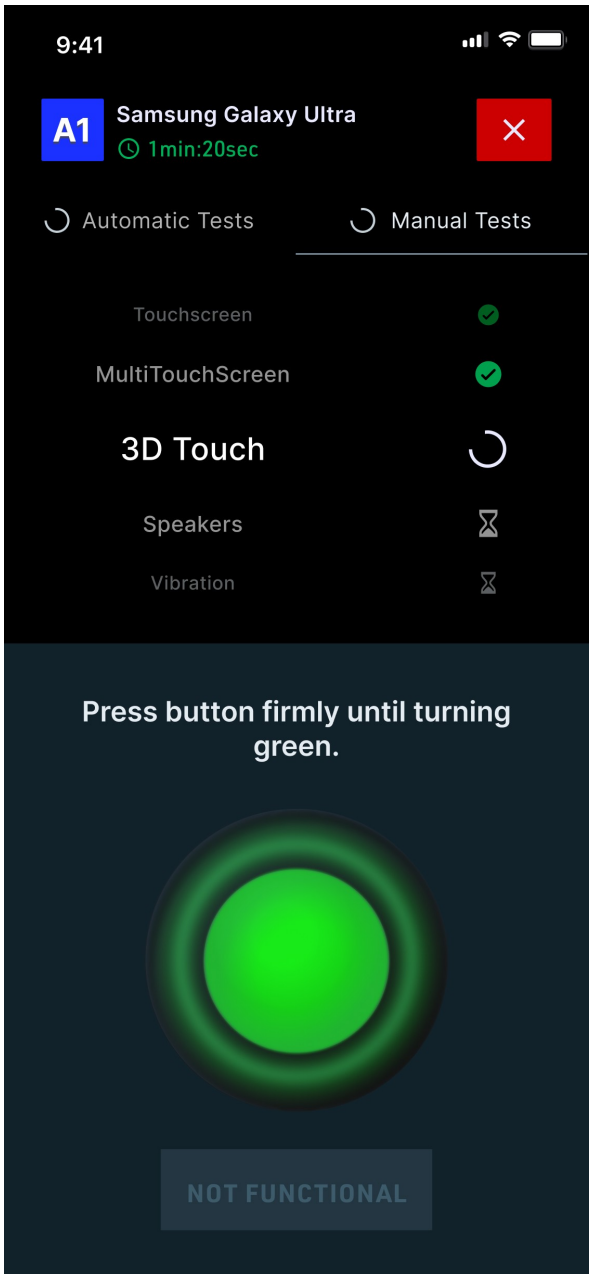


© 2026 Securaze GmbH





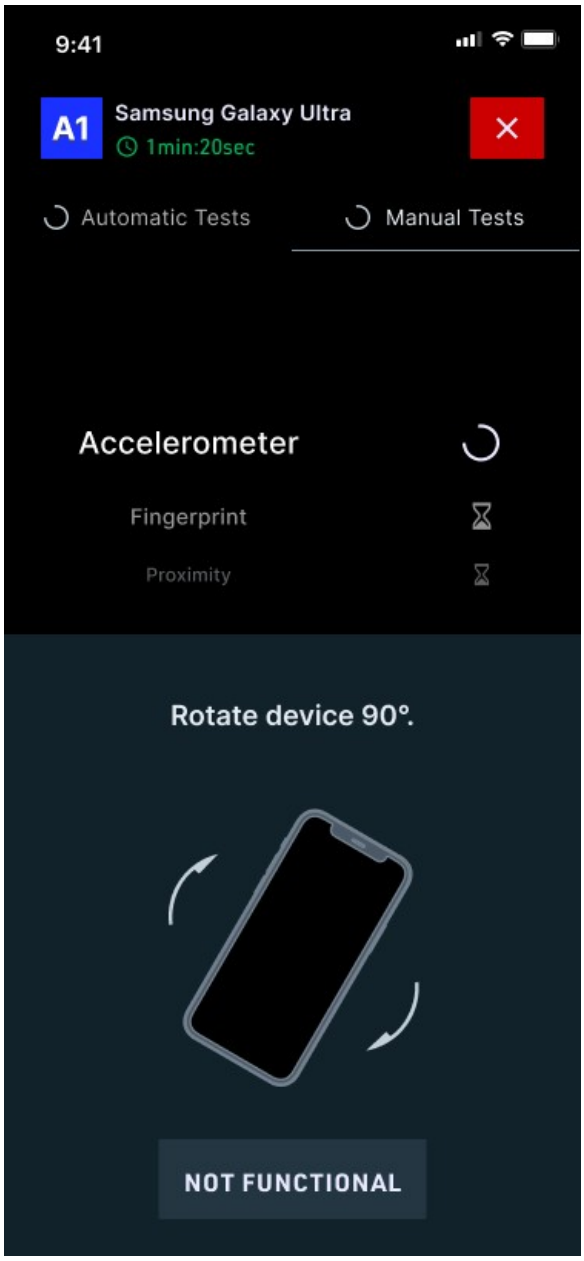
© 2026 Securaze GmbH




### 4.16.1.1 Accelerometer

**Tilt** the **phone** on its side. If it works, the test will automatically complete and a green check mark will appear. If not, press "Not working".


© 2026 Securaze GmbH




#### 4.16.1.11Face ID Quick & Face ID

### Face ID Quick

Face ID uses sensor data from the hardware to determine the Face ID status.

No registration of the face is required.

If both Face ID Quick and Face ID are selected, Face ID will be automatically passed if Face ID Quick was successfully.

### Face ID

To execute the Face ID test, you need to setup Face ID on the device.

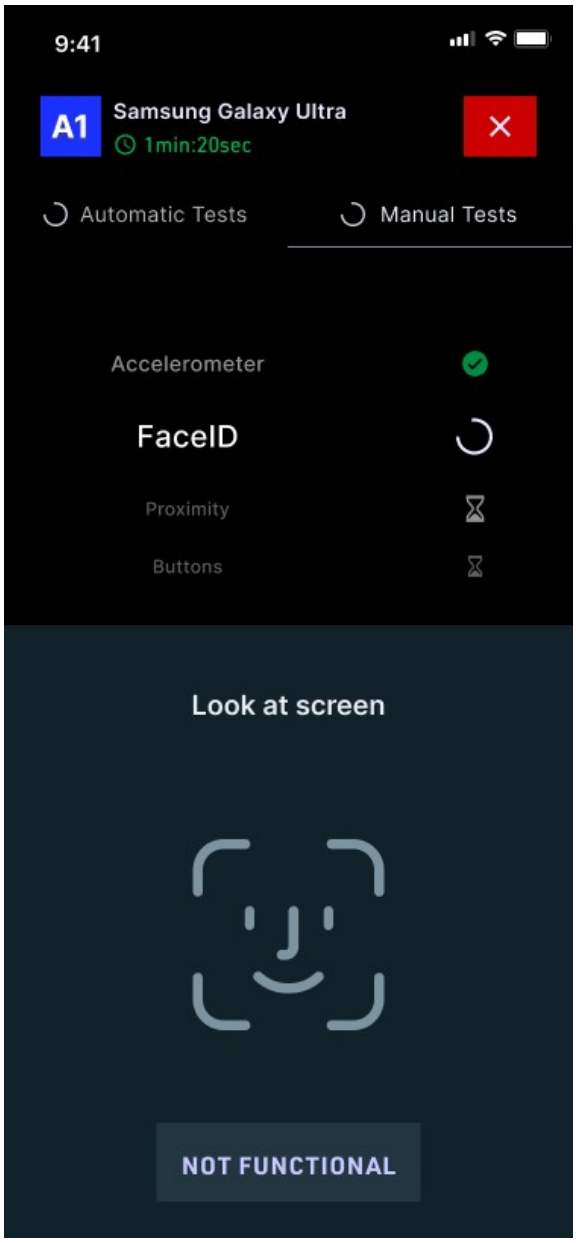
Please follow these steps:


© 2026 Securaze GmbH

- Open the "Settings" app on your device.
- Scroll down and tap on "Face ID & Passcode". You have to create a passcode first. It will be removed if you erase the device after the diagnose.
- Tap on "Set Up Face ID" or "Enroll Face" (depending on your device).
- Position your face within the frame displayed on the screen. Follow the on-screen instructions to move your head in a circular motion, allowing the device to capture your facial features.
- Once the first Face ID scan is complete, tap "Continue" and perform a second scan by moving your head in a circular motion again.
- After the second scan is completed, tap "Done" to finish setting up Face ID.
- Switch back to the Securaze Mobile application.

For Face ID test, **look at the screen** and if the framed face changes from gray to green, Face ID is working, otherwise press the "Not functional" button.


© 2026 Securaze GmbH




### 4.16.1.12 Fingerprint Quick & Fingerprint

#### Fingerprint Quick

Fingerprint Quick uses sensor data from the hardware to determine the Fingerprint status.

No registration of fingers is required.

If both Fingerprint Quick and Fingerprint are selected, Fingerprint will be automatically passed if Fingerprint Quick was successfully.

#### Fingerprint

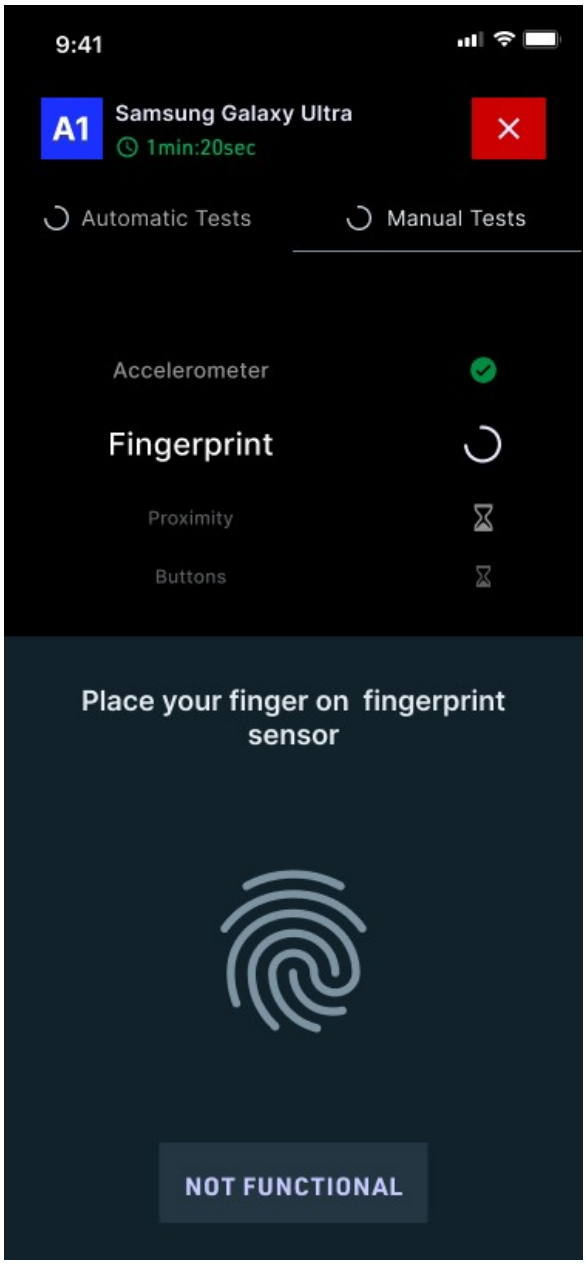
To execute the Fingerprint test, you need to setup Fingerprint on the device.


© 2026 Securaze GmbH

- Open the "Settings" app on your iPhone.
- Scroll down and tap on "Touch ID & Passcode". You may be asked to enter your device passcode.
- Tap on "Add a Fingerprint" under the "Fingerprints" section.
- Place your finger on the Home button (do not press it) and follow the on-screen instructions. The iPhone will vibrate when it captures your fingerprint. You'll need to lift and rest your finger on the Home button multiple times to capture different parts of your fingerprint.
- Once the initial fingerprint scan is complete, you'll be asked to adjust your grip to capture the edges of your finger. Continue to lift and rest your finger on the Home button until the process is complete.
- Tap "Continue" once the fingerprint setup is finished.
- Switch back to the Securaze Mobile application.

For the fingerprint test, simply **place your finger on the fingerprint sensor**. If the lines on the screen change from gray to green, the sensor is working, otherwise press the "Not working" button.


© 2026 Securaze GmbH

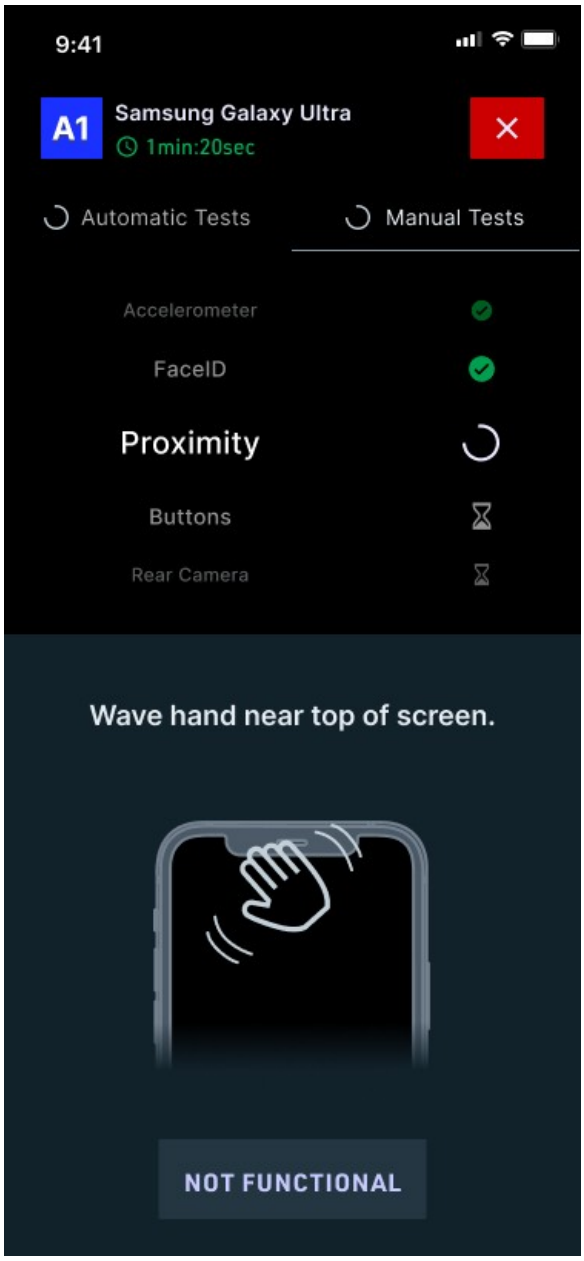



#### 4.16.1.13 Proximity

**Hold** your **hand near the top half** of the phone's display and **wave**, or move the **device towards your face.**

If it works, the test will automatically complete and a green check mark will appear. If not, press the "Not functional" button.

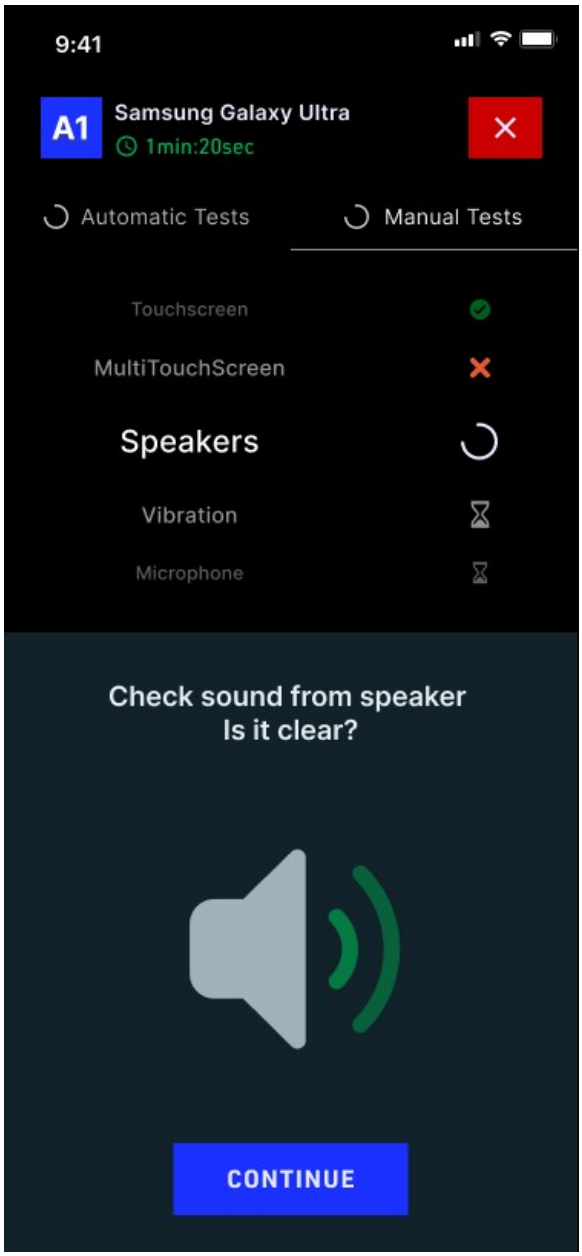

© 2026 Securaze GmbH




#### 4.16.1.14 Speaker

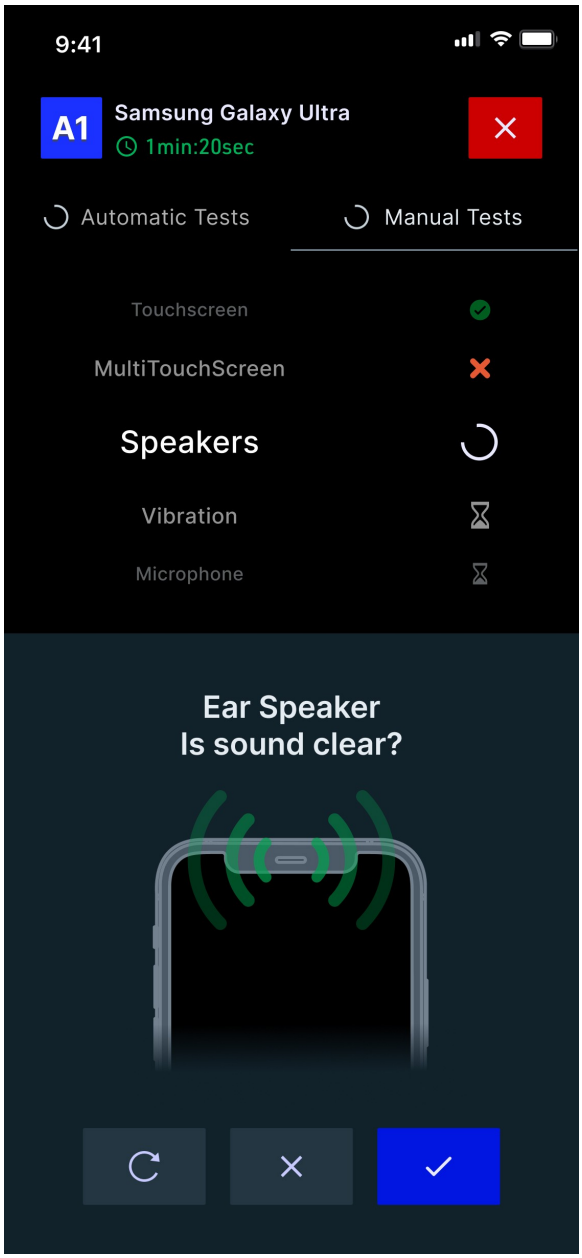
Tones are played through all speakers one after the other and you should answer with check marks for "Yes", the x for "No" or the circle for "Repeat test" whether you could **hear** the **sound from** the **respective speaker loud and clear**.


© 2026 Securaze GmbH



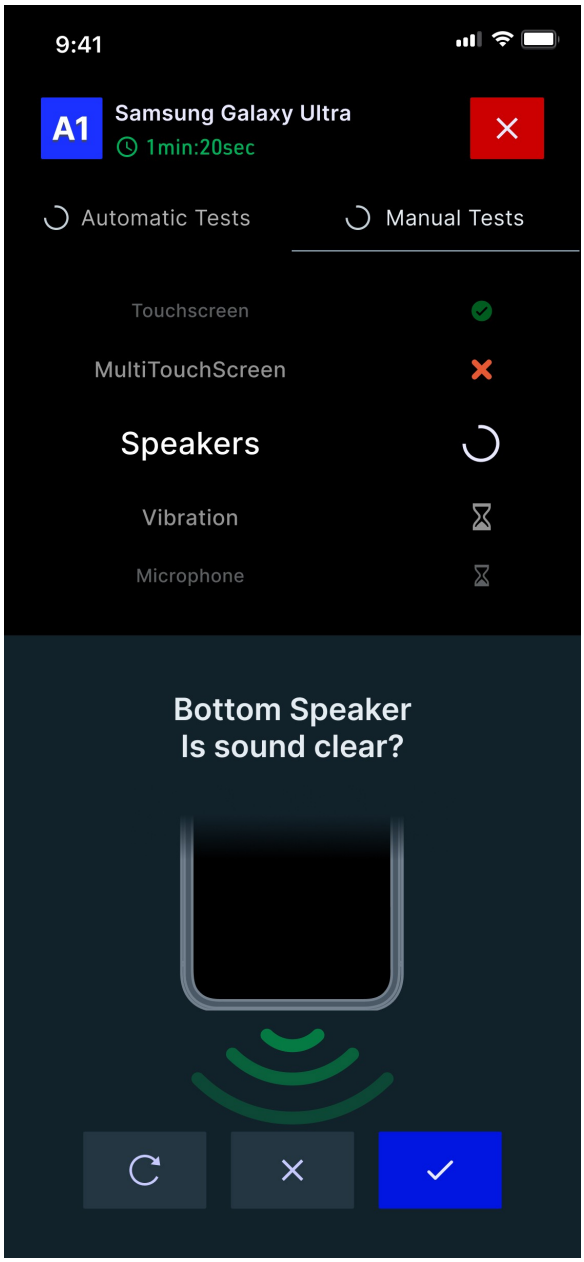


© 2026 Securaze GmbH





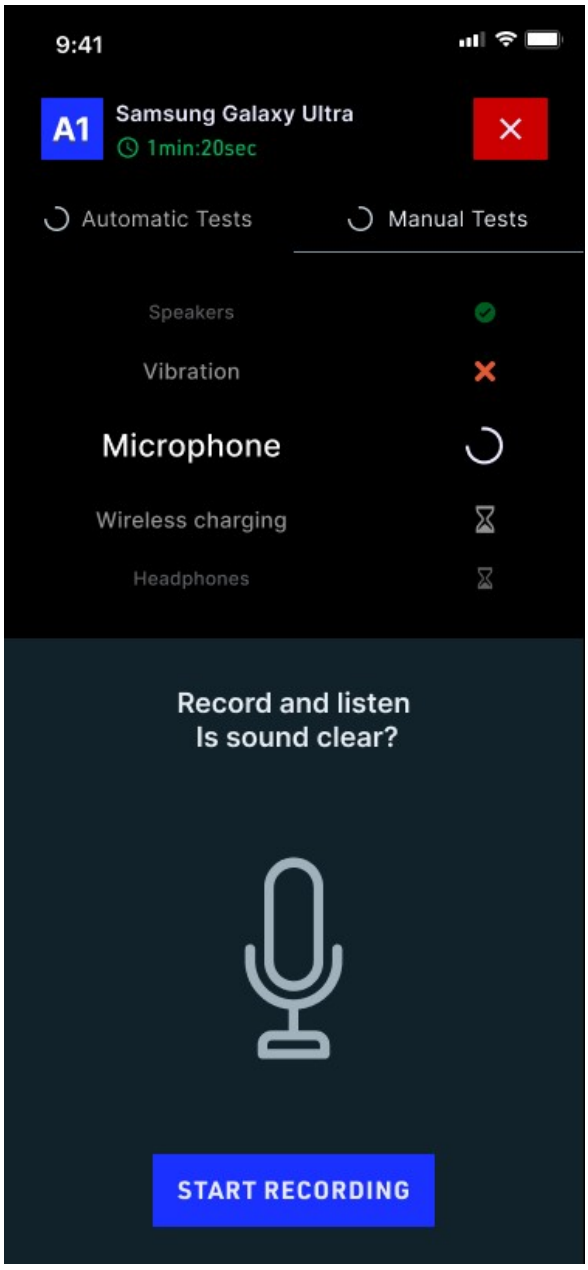
© 2026 Securaze GmbH




### 4.16.1.15 Microphone

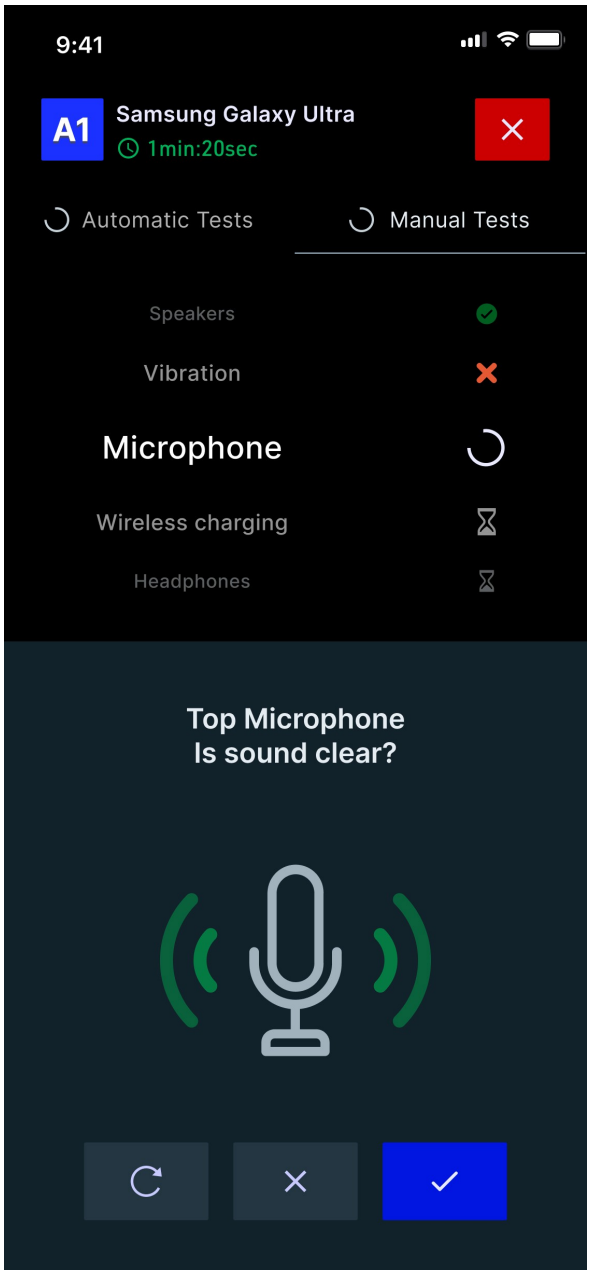
First **press** the **"Start recording"** key and **record** a **short tone**. When the phone detects and records sounds, green curved lines appear to the left and right of the microphone. Then do the same with the bottom and rear microphones.


© 2026 Securaze GmbH



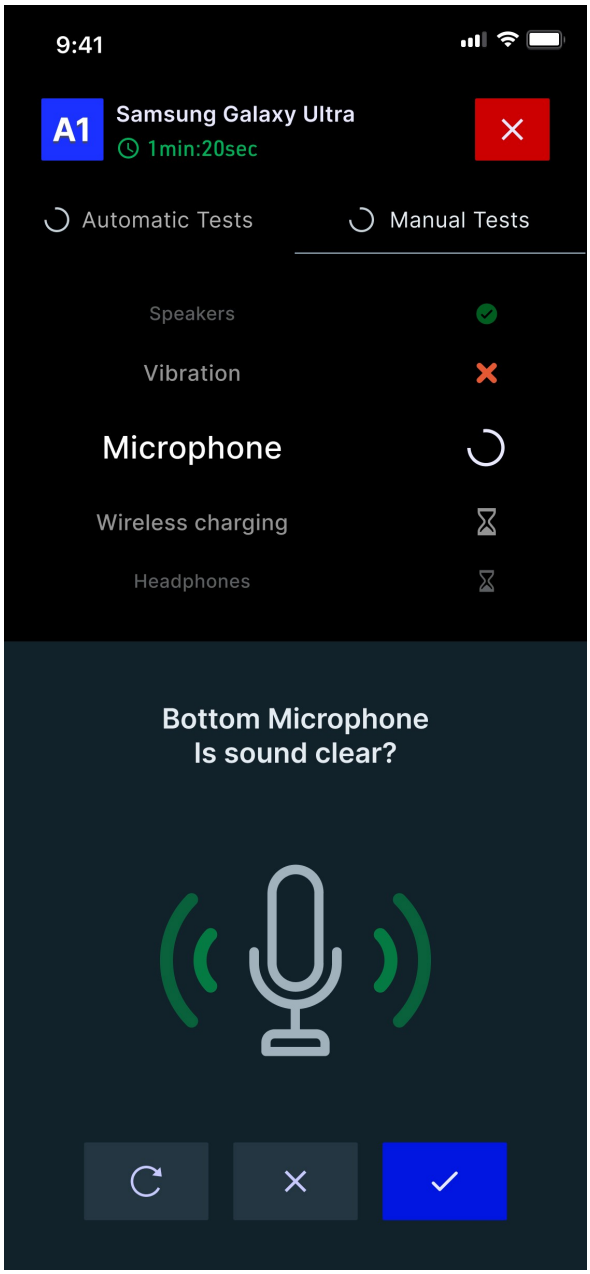


© 2026 Securaze GmbH





© 2026 Securaze GmbH

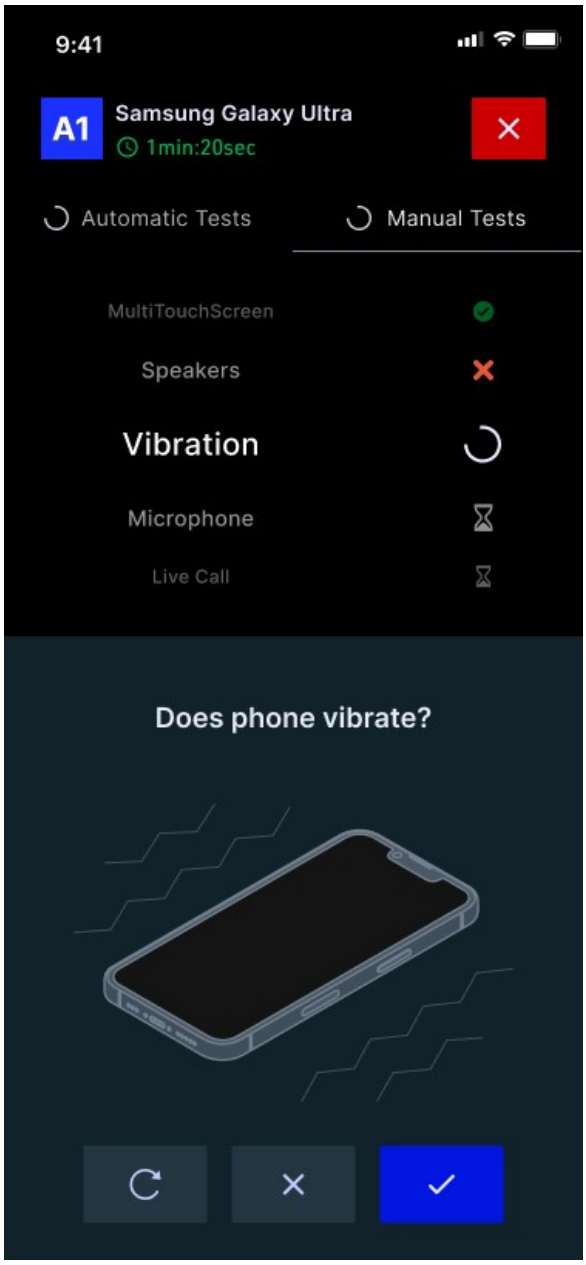



### 4.16.1.1€Vibration

In this test, the phone starts to vibrate and you have to **confirm** whether it **vibrates or not**.

Press the check mark for "Yes", x for "No" or the repeat icon for "Repeat test".

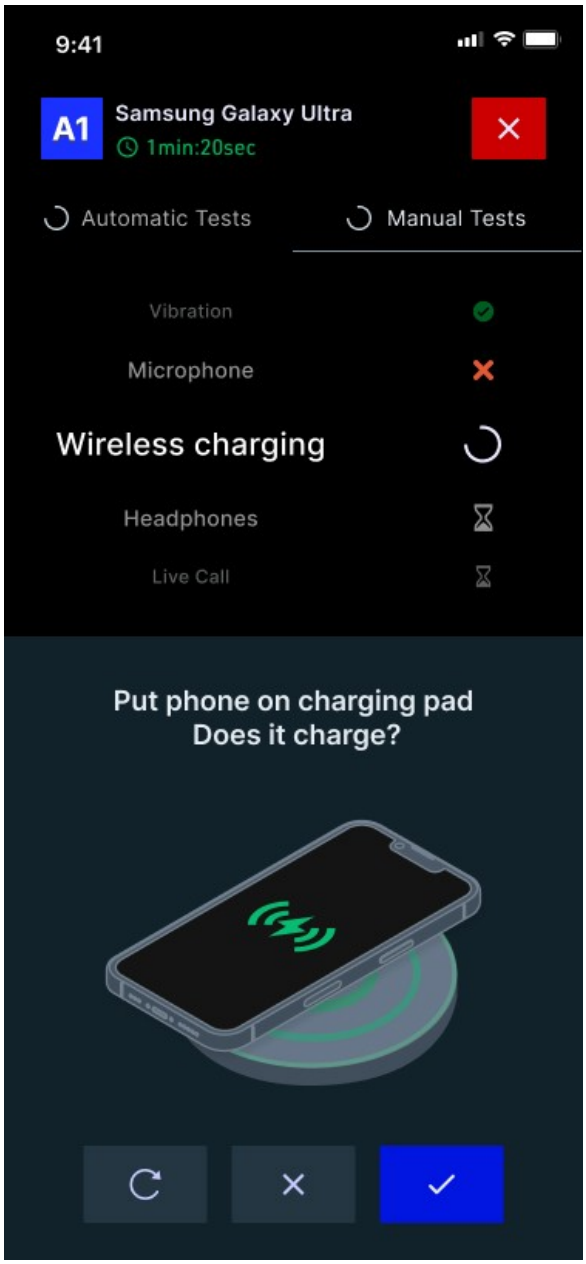

© 2026 Securaze GmbH




### 4.16.1.17 Wireless Charging

**Place** the **phone** on a **wireless charging pad**. If it works, the test will automatically complete and a green check mark will appear. If not, press "Not working".


© 2026 Securaze GmbH




### 4.16.1.18 Live Call

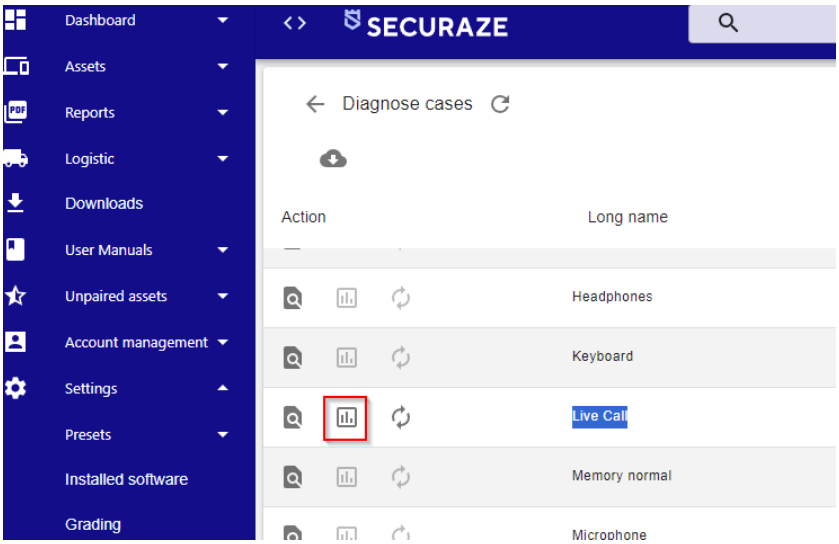
In the Live Call test, a call is initiated towards the number which gets specified in the Diagnose Case settings.

As soon the call is established the call will be stopped automatically or you need to hang up manually depending on the operating system capabilities.

**Attention! The Sim-Card should be inserted before starting the diagnose.**

These settings can be found in "Settings / Diagnose cases / Live Call" with the functionality "Update params".


© 2026 Securaze GmbH




### 4.16.1.19 Battery Discharge

In the Battery Discharge test, the battery's discharge speed is evaluated.

This includes 3 different Battery Drain Modes, and each mode has specific settings.

There are also general settings that are applicable to all modes.

**General settings**

Minimum battery percentage on start:

If the battery's current percentage is below this value, the diagnose case will fail. The operator needs to restart the diagnose case when the battery reaches the desired percentage.

Minimum battery percentage during drain:

If the battery's current percentage falls below this value during the test, the diagnose case will be aborted. The operator must restart the diagnose case after recharging to the desired percentage.

Specific settings for each drain mode:

**Duration:**

This setting determines the fixed duration for the Battery Discharge test. This mode is useful for varying the test length based on the device value, allowing shorter durations for lower value devices and longer for higher value devices.

Drain duration (minutes):

This is the time period for which the battery discharge is executed.

Maximum amount of battery loss after drain duration:


© 2026 Securaze GmbH

If the battery loss during the discharge equals or exceeds this value, the diagnose case fails. Conversely, if the battery loss is below this value, the diagnose case is successful.

**Percentage:**

The test runs until a specified battery loss is observed, or the minimum allowed time until this loss occurs is reached. If the minimum allowed time is reached before the specified loss, the test case is also deemed successfully passed.

Drain until this percentage loss occurred:

This specifies the battery loss percentage to be achieved.

Minimum allowed time until the percentage loss occurred (minutes):

If the battery loss during the discharge is below the specified time, the diagnose case fails. If it is equal or above the specified time, the diagnose case is successful.

**Full discharge:**

The test continues until the device is fully discharged to the specified minimum battery percentage during drain. The test case fails if the battery loss is not consistent (e.g., dropping suddenly from 40% to 35%), and passes if the loss is steady.

### 4.16.2 Automatic Sensor Tests

Automatic sensor tests run without any operator interaction. When the diagnose starts, Securaze Mobile reads the device sensors and marks each test as passed when the sensor returns a valid reading. No manual steps are required.

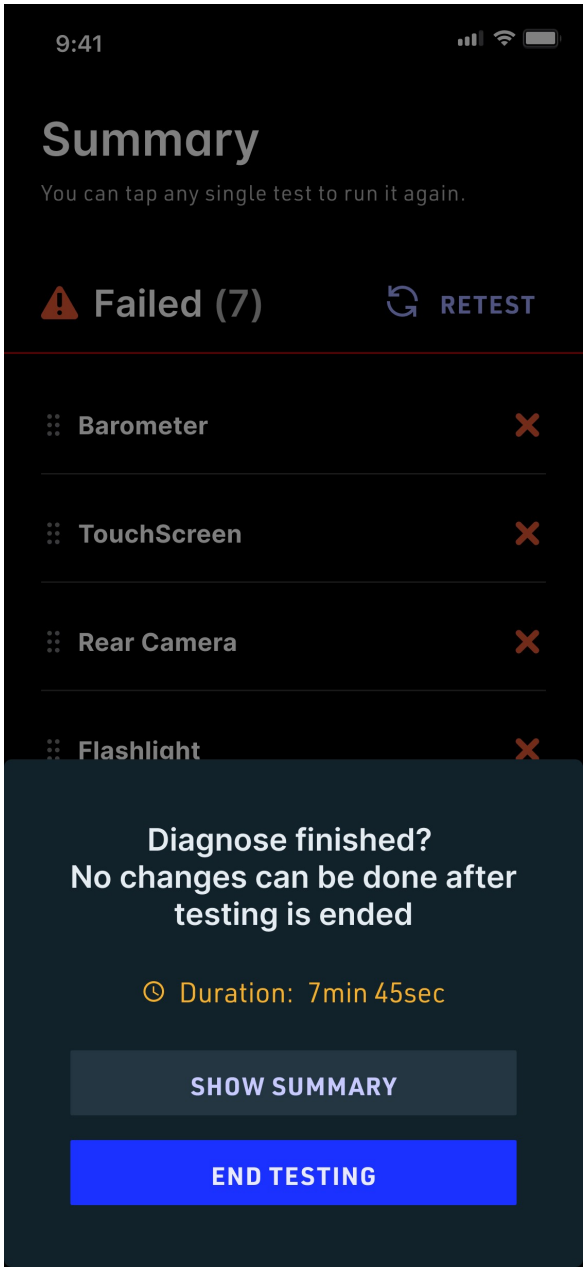
| Sensor | What is checked | Availability |
|---|---|---|
| Barometer | The barometric air-pressure sensor reports a valid reading. | Android, iOS |
| Compass | The magnetometer (compass) reports a valid magnetic-field reading. | Android, iOS |
| Gravity | The gravity sensor reports a valid gravity vector (assisted). | Android |
| Temperature | The device temperature sensor reports a valid reading. | Android |
| Phone Capability | SIM-card presence and mobile signal are detected. | Android |


© 2026 Securaze GmbH

Availability depends on the device and platform. Sensors that are not present on a device are skipped automatically.

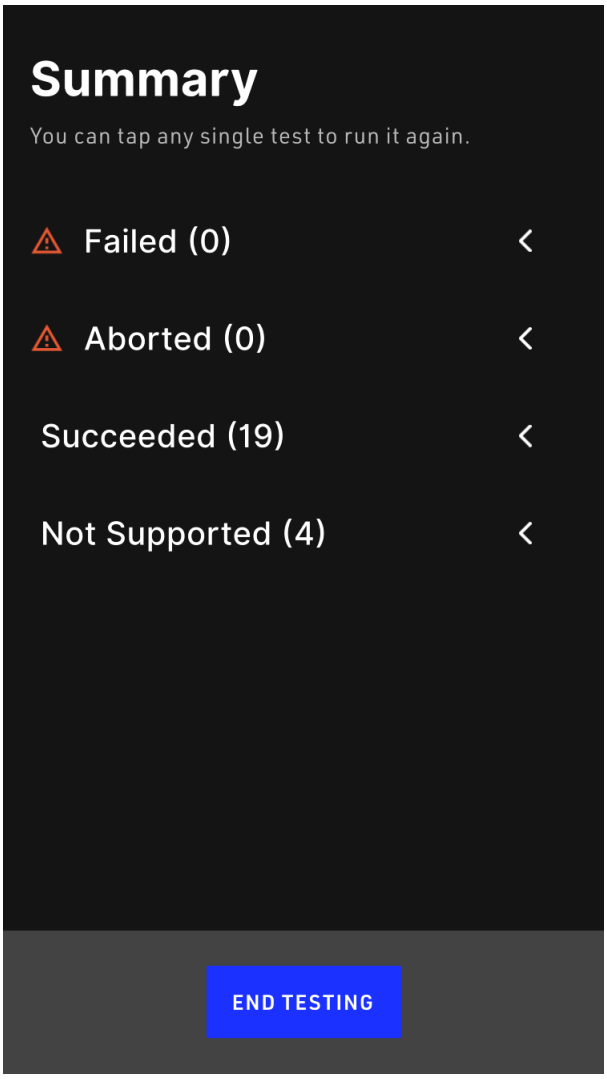
### 4.16.3 After tests are completed

After all tests are completed, a window will appear with "**View Summary**" buttons to view the summary or "**End Test**".



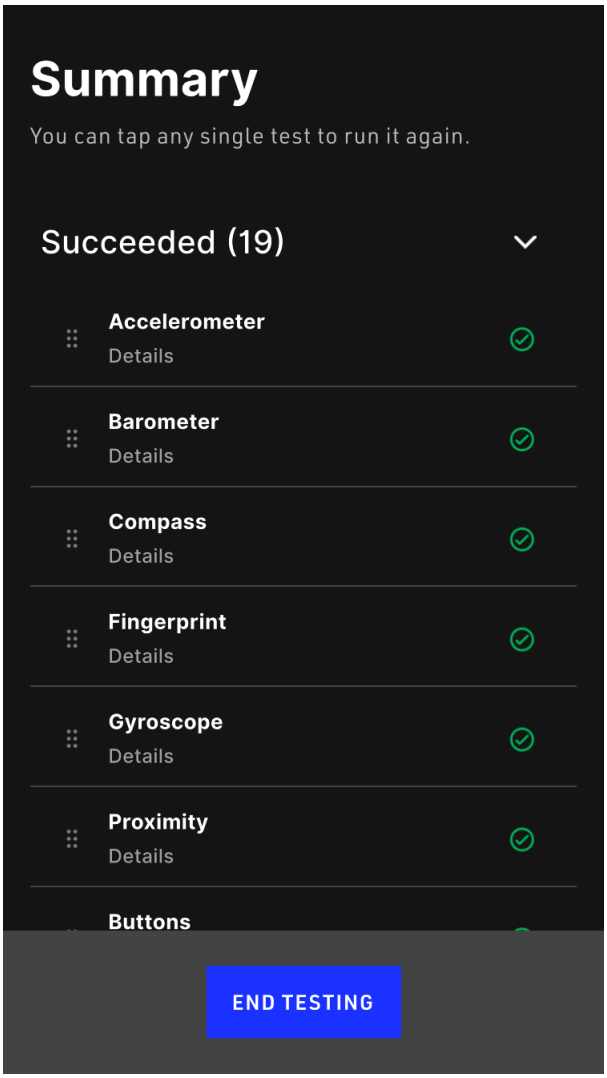

In the summary you will see the "Failed tests" at the top and next to it the button to retry the failed tests. Click on the respective test to see exact details. Below that are the successful tests and the unsupported tests.


© 2026 Securaze GmbH



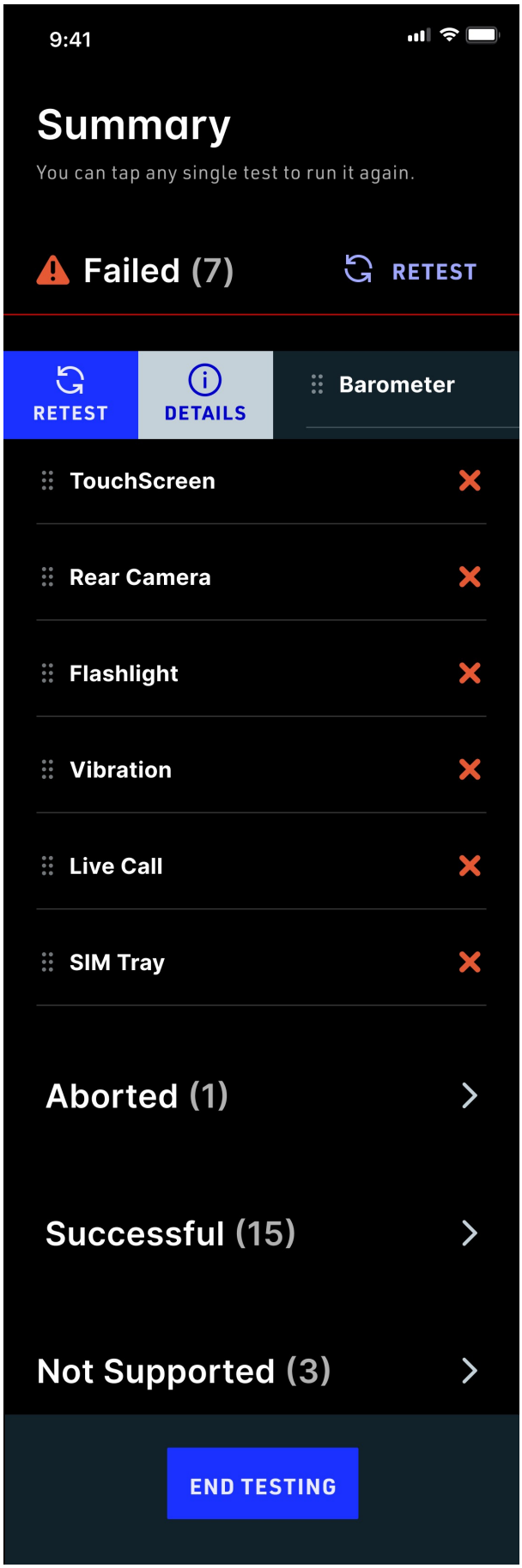


© 2026 Securaze GmbH





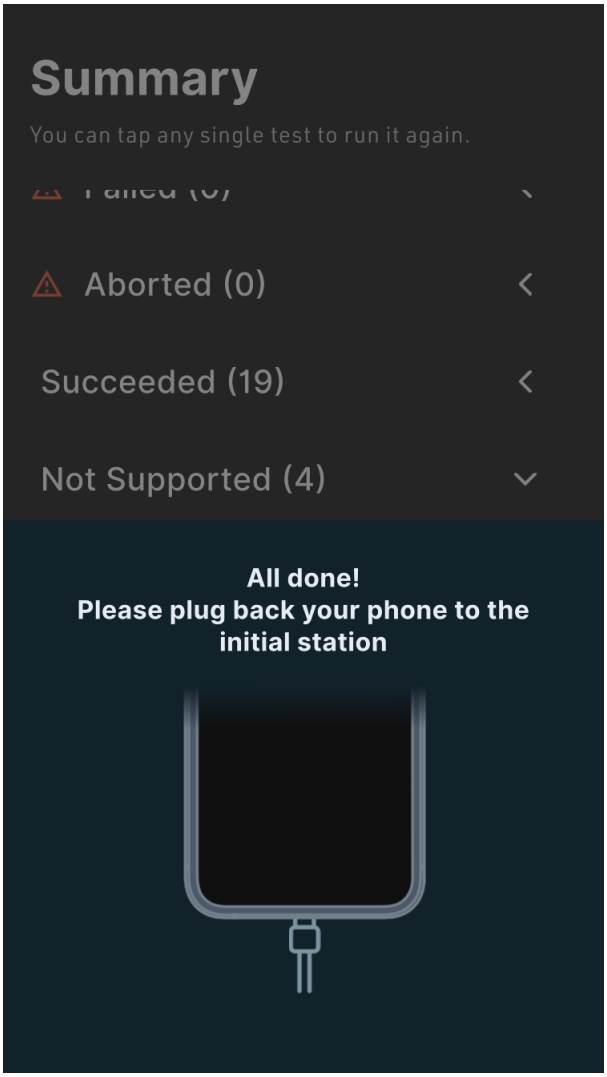
© 2026 Securaze GmbH





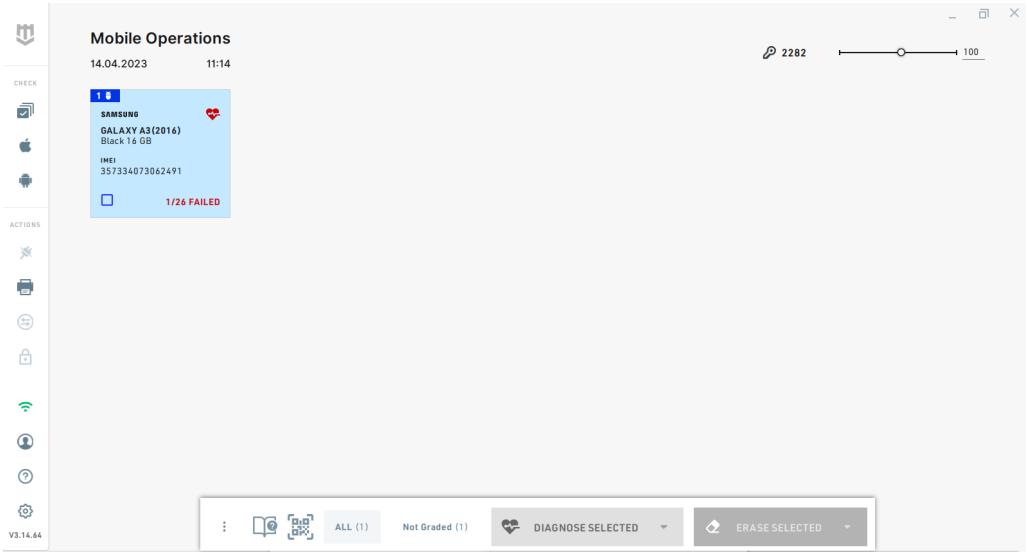
© 2026 Securaze GmbH

At the very bottom you will find the **"End test**" button. **Click** the button and **plug** the **unplugged device back to** the **original station**.




On the main page of Mobile, the analyzed **device** will then appear in light blue and the box will say "**Completed**" or or how many tests have failed.


© 2026 Securaze GmbH




## 4.16.4 Diagnosis Case Preselection Description

A **preselection** is a saved set of diagnose cases. With a preselection, operators start the diagnose with one click, because the cases are already chosen.

### Create a preselection

• Click the arrow of **DIAGNOSE SELECTED** and choose **Diagnose settings**.

• Click **Customize**. In **Custom Test**, select the cases. You can filter by platform (**All platforms**, **Androids**, **iOS**), select all cases at once, or search.

• Click **Save as preselection**, type a name and click **Save**. If your user may not save preselections, Mobile first asks for an admin login (**Change Settings**).

The preselection is saved on the Securaze server, so all stations of your company can use it.

### Use a preselection

• In **Diagnose Settings**, choose the preselection under **PRESELECTION NAME**. The station keeps it: **DIAGNOSE SELECTED** starts it on the selected devices.

• Mark up to five preselections as favorites with the star in the list. Favorites appear under the arrow of **DIAGNOSE SELECTED** and start right away.

Example: with five stations, you create the preselection once and use it on all five stations, instead of choosing the cases on each station again.

See also Perform diagnose 89.


© 2026 Securaze GmbH

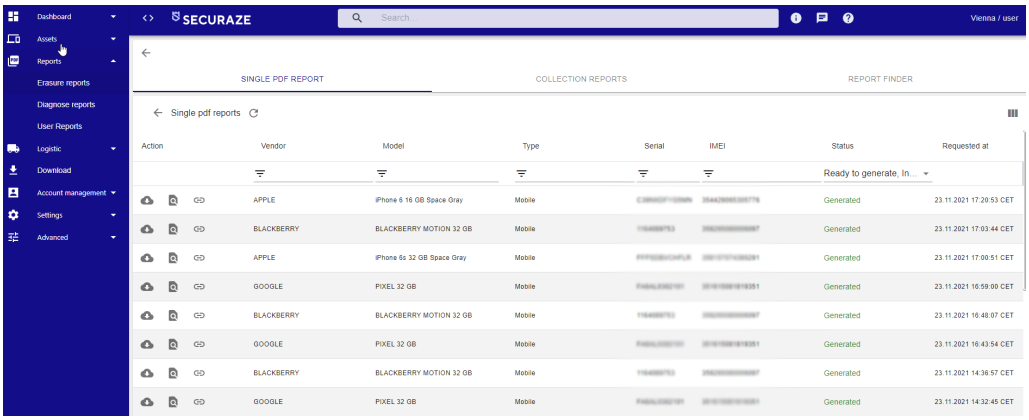
# Reports

# 5 Reports

You can find the erasure reports in Securaze Dashboard.

## 5.1 Download erasure or diagnose report

In the menu **Reports - Erasure reports** and **Reports - Diagnose reports** you can find the erasure report for one asset (Tab **SINGLE PDF REPORT**) or for all assets of one Sale Lot, one Lot or one whole order (Tab **COLLECTION REPORTS**).

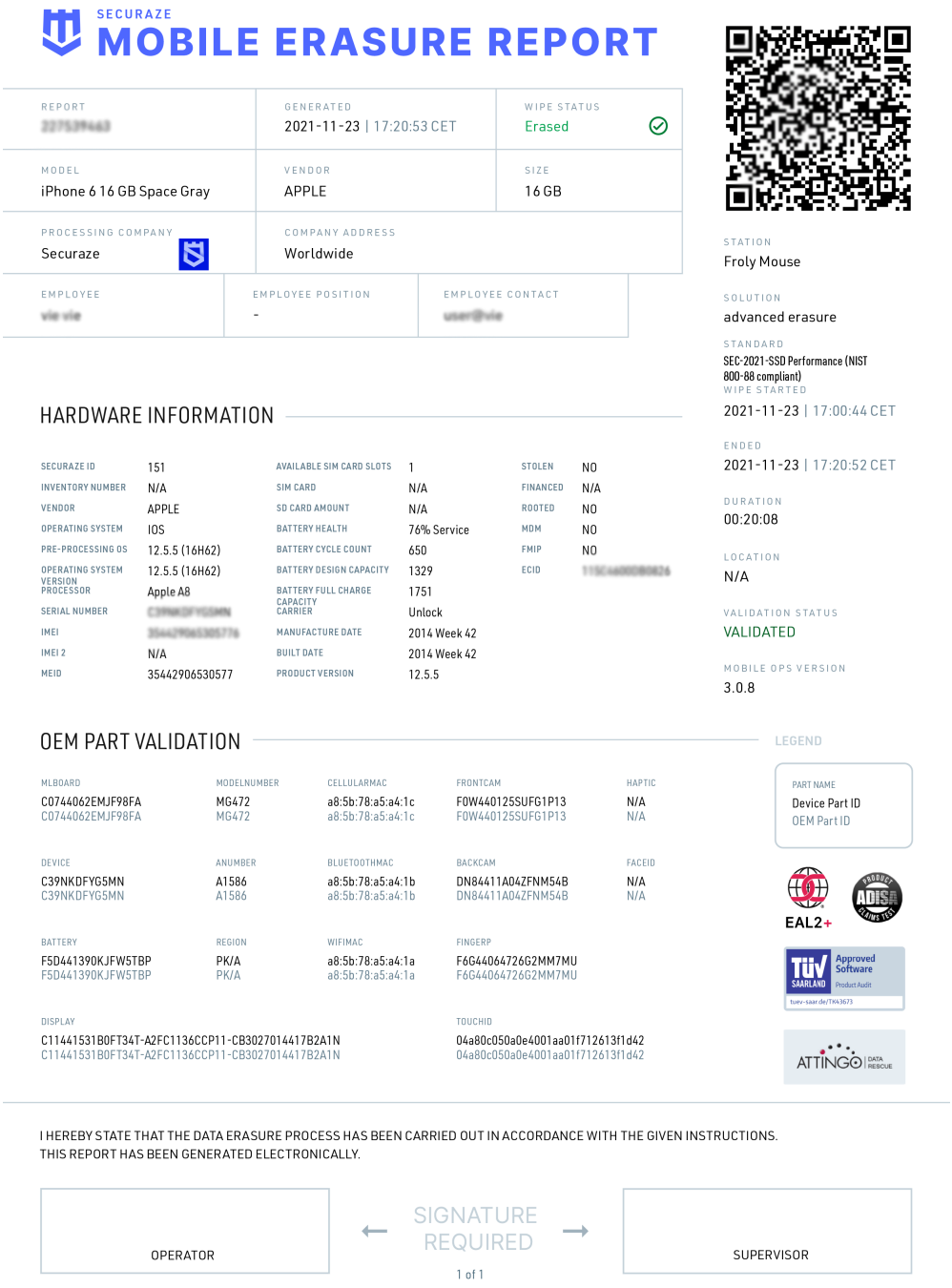



Download an report:

**One asset:**

To download an report of one asset, click on **Reports - Erasure reports** or **Reports - Diagnose reports** in the Menu section.


© 2026 Securaze GmbH



SECURAZE
MOBILE ERASURE REPORT

| REPORT | GENERATED | WIPE STATUS |
|---|---|---|
| [redacted] | 2021-11-23 \| 17:20:53 CET | Erased |
| **MODEL** | **VENDOR** | **SIZE** |
| iPhone 6 16 GB Space Gray | APPLE | 16 GB |
| **PROCESSING COMPANY** | **COMPANY ADDRESS** | |
| Securaze | Worldwide | |
| **EMPLOYEE** | **EMPLOYEE POSITION** | **EMPLOYEE CONTACT** |
| [redacted] | - | [redacted] |

STATION: Froly Mouse
SOLUTION: advanced erasure
STANDARD: SEC-2021-SSD Performance (NIST 800-88 compliant)
WIPE STARTED: 2021-11-23 | 17:00:44 CET
ENDED: 2021-11-23 | 17:20:52 CET
DURATION: 00:20:08
LOCATION: N/A
VALIDATION STATUS: VALIDATED
MOBILE OPS VERSION: 3.0.8

HARDWARE INFORMATION

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| SECURAZE ID | 151 | AVAILABLE SIM CARD SLOTS | 1 | STOLEN | NO |
| INVENTORY NUMBER | N/A | SIM CARD | N/A | FINANCED | N/A |
| VENDOR | APPLE | SD CARD AMOUNT | N/A | ROOTED | NO |
| OPERATING SYSTEM | IOS | BATTERY HEALTH | 76% Service | MDM | NO |
| PRE-PROCESSING OS | 12.5.5 (16H62) | BATTERY CYCLE COUNT | 650 | FMIP | NO |
| OPERATING SYSTEM VERSION | 12.5.5 (16H62) | BATTERY DESIGN CAPACITY | 1329 | ECID | [redacted] |
| PROCESSOR | Apple A8 | BATTERY FULL CHARGE CAPACITY | 1751 | | |
| SERIAL NUMBER | [redacted] | CARRIER | Unlock | | |
| IMEI | [redacted] | MANUFACTURE DATE | 2014 Week 42 | | |
| IMEI 2 | N/A | BUILT DATE | 2014 Week 42 | | |
| MEID | 35442906530577 | PRODUCT VERSION | 12.5.5 | | |

OEM PART VALIDATION

LEGEND: PART NAME — Device Part ID / OEM Part ID

| MLBOARD | MODELNUMBER | CELLULARMAC | FRONTCAM | HAPTIC |
|---|---|---|---|---|
| C0744062EMJF98FA<br>C0744062EMJF98FA | MG472<br>MG472 | a8:5b:78:a5:a4:1c<br>a8:5b:78:a5:a4:1c | F0W440125SUFG1P13<br>F0W440125SUFG1P13 | N/A<br>N/A |
| **DEVICE** | **ANUMBER** | **BLUETOOTHMAC** | **BACKCAM** | **FACEID** |
| C39NKDFYG5MN<br>C39NKDFYG5MN | A1586<br>A1586 | a8:5b:78:a5:a4:1b<br>a8:5b:78:a5:a4:1b | DN84411A04ZFNM54B<br>DN84411A04ZFNM54B | N/A<br>N/A |
| **BATTERY** | **REGION** | **WIFIMAC** | **FINGERP** | |
| F5D441390KJFW5TBP<br>F5D441390KJFW5TBP | PK/A<br>PK/A | a8:5b:78:a5:a4:1a<br>a8:5b:78:a5:a4:1a | F6G440647 26G2MM7MU<br>F6G440647 26G2MM7MU | |
| **DISPLAY** | | | **TOUCHID** | |
| C11441531B0FT34T-A2FC1136CCP11-CB3027014417B2A1N<br>C11441531B0FT34T-A2FC1136CCP11-CB3027014417B2A1N | | | 04a80c050a0e4001aa01f712613f1d42<br>04a80c050a0e4001aa01f712613f1d42 | |

EAL2+

I HEREBY STATE THAT THE DATA ERASURE PROCESS HAS BEEN CARRIED OUT IN ACCORDANCE WITH THE GIVEN INSTRUCTIONS.
THIS REPORT HAS BEEN GENERATED ELECTRONICALLY.

OPERATOR — SIGNATURE REQUIRED — SUPERVISOR

1 of 1

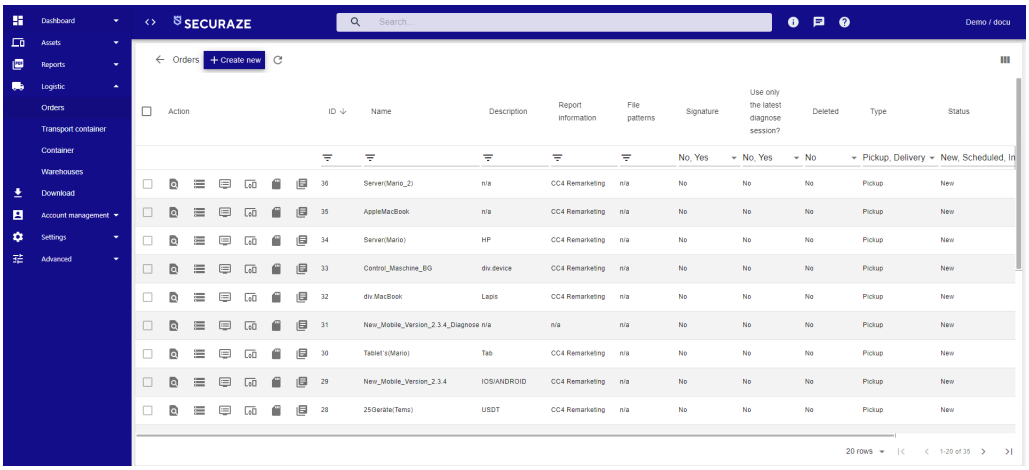
Select the desired report and click Download report(s). The report is downloaded in pdf format.

**Order:**

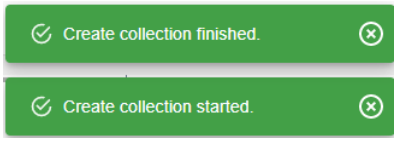
To download an erasure report for all assets of one Order, click on **Logistic - Orders** in the Menu section.

Select the desired Order and click on **Create Collection.**


© 2026 Securaze GmbH




The erasure report will be generated.




A ZIP file is downloaded containing single reports as a PDF file, aggregated report as a PDF file and a listing of assets as an .xlsx file. The erasure reports are displayed on **Reports - Erasure reports** in the Menu section.

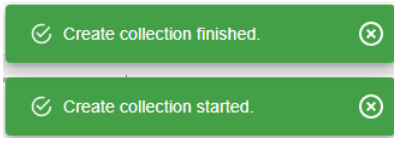
In the menu **Reports - Erasure reports** you can download the reports again any time by clicking on Download report(s).

**Lot:**

To download an erasure report of all assets of one Lot, click on **Logistic - Lot** in the Menu section.

Select the desired Order and click on **Create Collection.**

The erasure report will be generated.




A ZIP file is downloaded containing single reports as a PDF file, aggregated report as a PDF file and a listing of assets as an .xlsx file. The erasure reports are displayed on **Reports - Erasure reports** in the Menu section.


© 2026 Securaze GmbH

In the menu **Reports - Erasure reports** you can download the reports again any time by clicking on Download report(s).

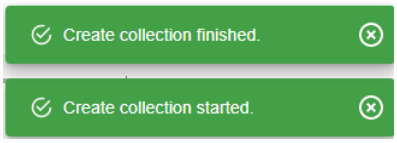
**Sale Lot:**

To download an erasure report of all assets of one Sale Lot, click on **Logistic - Sale Lot** in the Menu section.

Select the desired Order and click on **Create Collection.**



The erasure report will be generated.




A ZIP file is downloaded containing single reports as a PDF file, aggregated report as a PDF file and a listing of assets as an .xlsx file. The erasure reports are displayed on **Reports - Erasure reports** in the Menu section.

In the menu **Reports - Erasure reports** you can download the reports again any time by clicking on Download report(s).

The erasure report contains all the information about the erased device and the date and time of the erasure.


© 2026 Securaze GmbH

# FAQ

# 6 FAQ


© 2026 Securaze GmbH

## 6.1 OEM parts validation (iOS only)

Original Equipment Manufacturer (OEM) parts are checked upon connection for iOS devices to determine if parts are original.

### Supported OEM parts

| # | Component | Detail | Valid Example |
|---|---|---|---|
| 1 | Device | Device serial number | QCFQN12KK18Y |
| 2 | Model number | Device model number | MG8X2 for an iPhone 5c |
| 3 | Region | Region identifier | LL/A for a product for the North American market |
| 4 | Model identifier | Device identifier | A2230 for an iPad Pro 11" (Wi-Fi/Cell Global - 2nd Gen) |
| 5 | Mainboard | Mainboard serial number | YYY865400ZKMNO123 |
| 6 | Battery | Battery serial number | FFFF00000YYYY1111 |
| 7 | Display | Display serial number | FFF00000BBBB000CCCCCCCBBBBBBBBBAAAAAAAAA44444444 AAAAAAAA33333333FFFFFF |
| 8 | Wi-Fi | Wi-Fi MAC Address | a valid MAC Address 1a:a3:b0:14:42:4a |
| 9 | Front Camera | Front Camera serial number (often no factory-value available) | FFWWAA222BBXX0A0A |

| # | Component | Detail | Valid Example |
|---|---|---|---|
| 10 | Back Camera | Back Camera serial number (often no factory-value available) | FFWWAA222BBXX0A0B |
| 11 | Fingerprint | Fingerprint serial number | Y6082000X9LLKB26CB |
| 12 | Face ID | Face ID serial number | Y000AbCdEfGhIjKl |
| 13 | Haptic Touch | Haptic Touch serial number (starting with iOS 13) | XX12344440YYX1M0Y+YXX3YY |
| 14 | Bluetooth | Bluetooth MAC Address | a valid MAC Address 1a:a3:b0:14:42:4b |
| 15 | Cellular | Cellular MAC Address | a valid MAC Address 1a:a3:b0:14:42:4c |
| 16 | Touch ID | Touch ID serial number (often no factory-value available) | 01442142y3b32b1rab15620z103100zl |

## OEM part status

After the validation the parts can have the following status:

- OEM - part is original in the device
- Non-OEM - part was replaced with an Aftermarket part
- Missing-OEM - part is marked as missing part status for the user to determine if the part is OEM.

Note:

When a 'Factory' or 'Current' Serial number is unable to be identified, it would show "Missing-OEM" as validation result.

"Missing-OEM" is user-determined, you may want to check into the device settings for any messages that may point to it being a Non-OEM part.

**Battery on iOS 27:** Checking the battery of a device running iOS 27 needs Securaze Mobile 5.16.15 or later; older versions report a genuine battery as Non-OEM.

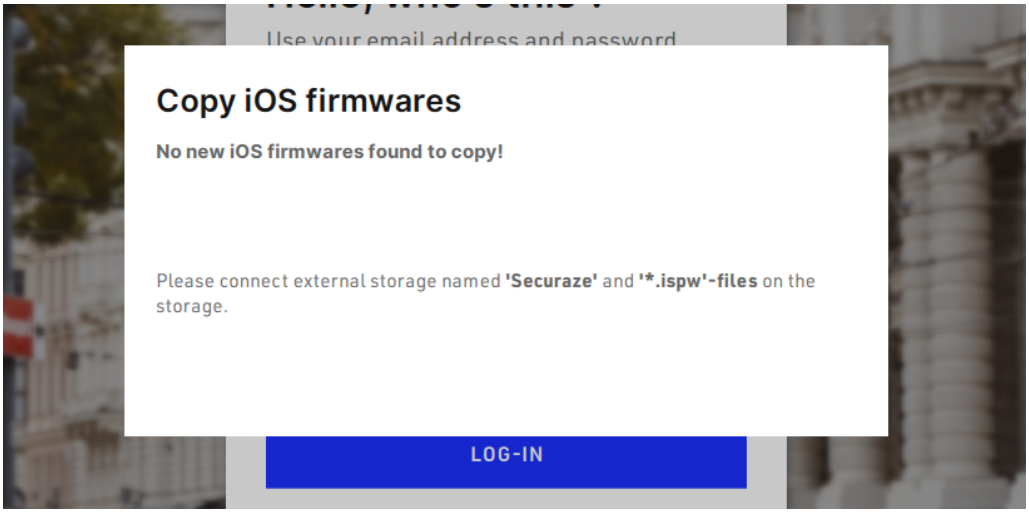
## 6.2 Upload iOS Firmware

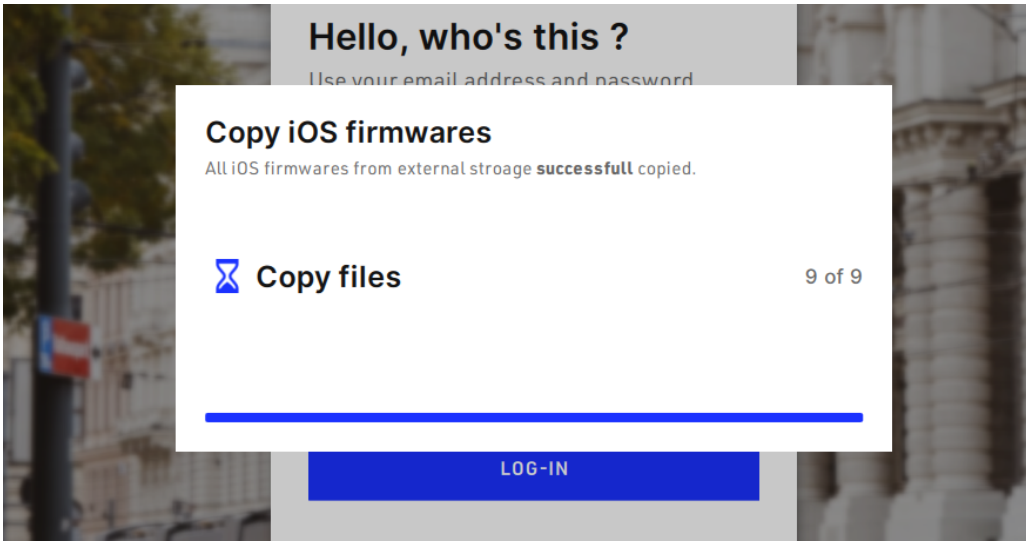
It is possible to copy iOS firmware from an external medium into the Securaze Mobile storage folder.

The external medium (USB stick, SSD, HDD) needs to be named "Securaze" and formatted as NTFS / FAT32 partition.

The iOS firmwares need to be placed in the folder "iOS" (named exactly like this) or in the root folder of the medium.

The copy process is only available **before** login: in **Options & Settings**, tab **Network & Storage**, click **START COPY** next to **Copy iOS firmwares (*.ipsw) from external medium**.





© 2026 Securaze GmbH

### Firmware from Securaze Command

Securaze Mobile can also get the firmware from Securaze Command. If a Securaze Command of your account is reachable on the local network, Securaze Mobile takes the firmware from there instead of from Apple. You do not need to set anything up for this. **Options & Settings**, tab **Network & Storage**, says which Command the firmware comes from.

If the Command does not hold the firmware yet, Securaze Mobile asks the Command to download it and waits for it. A detailed tile shows **Command downloading** with the Command's progress, then **Copying from Command** with the speed while the station copies the file. A standard tile shows the percent and the speed, and the device details say the same in words, for example **Copying the firmware from Securaze Command** with the percent and the speed. The next devices of the same model get the firmware from the Command at once.

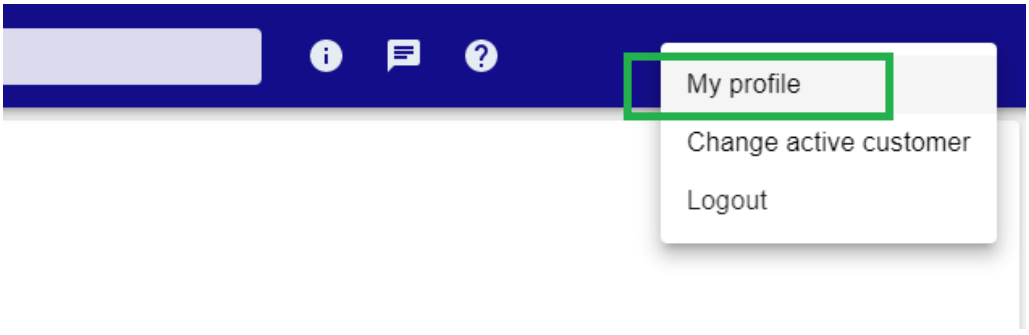
Securaze Mobile downloads the firmware from Apple instead when the Command's download does not move for 5 minutes, when the Command does not answer for 1 minute, when the download from the Command fails, or when the Command holds an outdated file - not Apple's current firmware. Without a reachable Command the firmware comes from Apple; a detailed tile then shows **Downloading**.

macOS only: a Mac gets its macOS firmware from the Command in the same way - see Erase a Mac 86.

## 6.3 Two-Factor Authentication (2FA)

**Securaze Dashboard** supports the two-factor authentication login method, to offer users an extra layer of protection, beyond just a username and password.

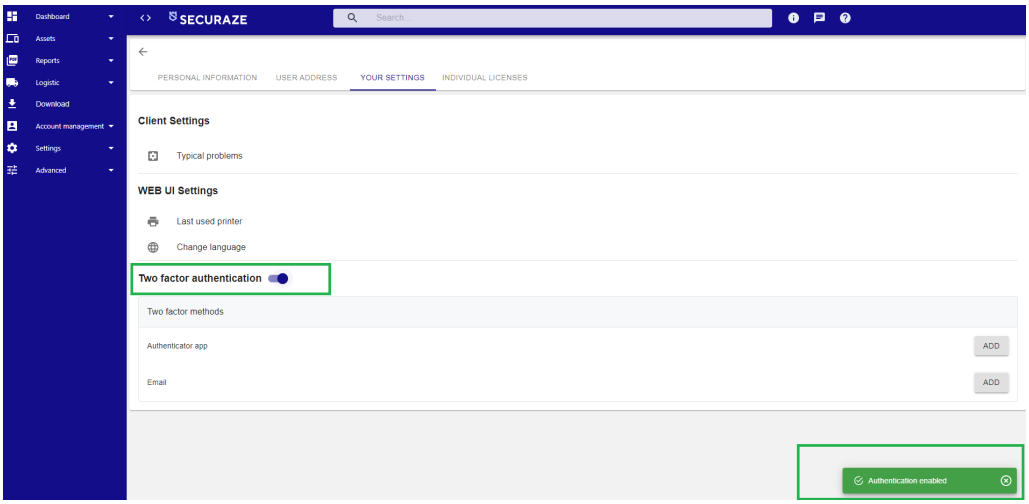
To activate this type of authentication, User needs to log in to Securaze Dashboard, and hover the mouse pointer over the customer name in the upper right corner of the screen. A drop-down menu appears, and the User should select **My profile**.





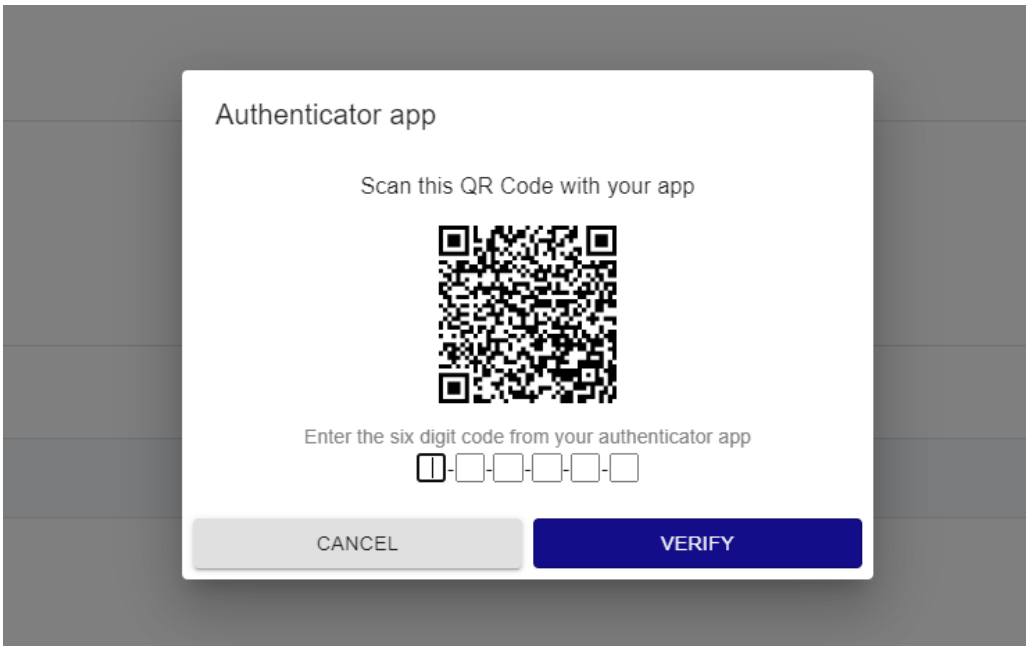
© 2026 Securaze GmbH

In the My profile section, select tab "**YOUR SETTINGS**". In this tab, you will see the option "**Two factor authentication**" and a toggle button on the right.
Click on the toggle button, and a menu for selecting the authentication method appears.




For Authenticator app method, we suggest using Google Authenticator, found in both App Store and Google Play, or Microsoft Authenticator, also found in both App Store and Google Play.

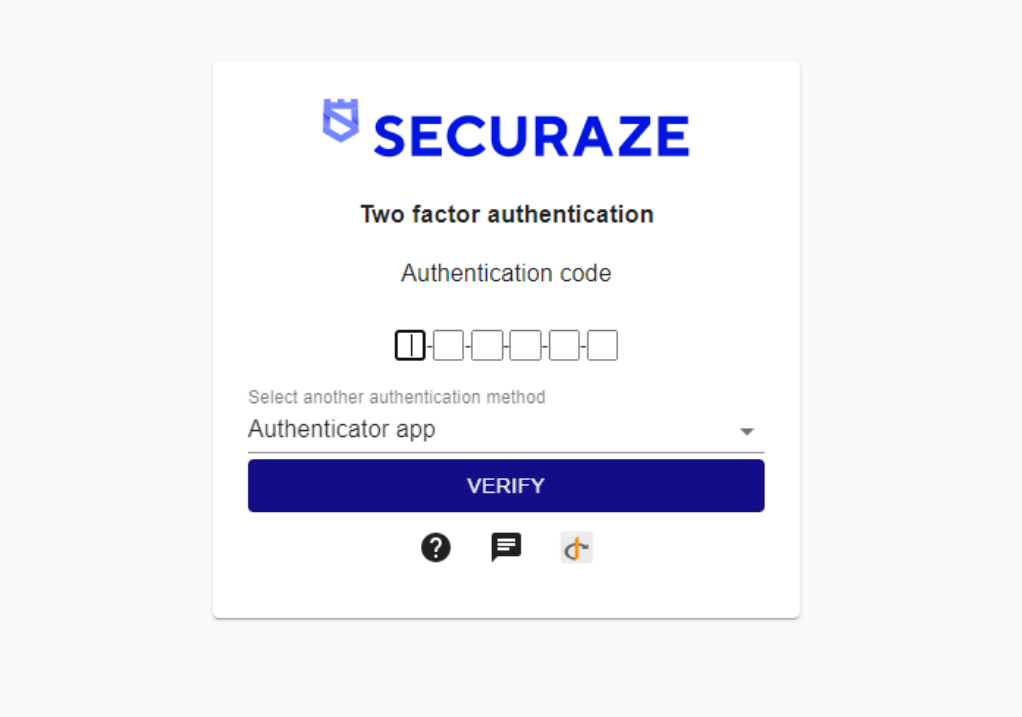
To select this method, click on "**ADD**" button on the right. A pop-up window will appear, asking you to scan the QR code with the app you chose to use.




After you have entered the code, click on "**VERIFY**" button.


© 2026 Securaze GmbH

You have now successfully activated this method of authentication.
Next time you try to log into the Securaze Dashboard, the authentication window will appear after you entered your login credentials, asking you for the code that was generated in your chosen app.




Be aware: the code in the app refreshes every 30 seconds.


© 2026 Securaze GmbH

# Release notes

# 7 Release notes

The current release notes can be found at:

Securaze Mobile Release Notes


© 2026 Securaze GmbH

# Menu items

# 8 Menu items

## 8.1 Overview

This part of the manual describes the screens of Securaze Mobile one by one. These screens come before the dashboard:

• Login 170 - log in with your Securaze user.

• Quick setup - only on a new station: choose the license and name the station. See Connect devices 54.

• Pre-selection 183 - choose the company, the workflow, the Lot and the Sale Lot for this session. Securaze Mobile shows only the screens it needs.

Then the dashboard opens. See Dashboard 185.

### Always at hand

The sidebar on the left is there from the login screen on:

• **Help** (Ctrl+H) - opens **Help & Support** with the Knowledge Base, the system report and remote support. See Help 171 and Support 185.

• **General settings** (F9) - opens **Options & Settings**. See Options & Settings 174.

• **Connected** / **Disconnected** - whether the station reaches the Securaze server.

The version of Securaze Mobile is shown at the bottom of the sidebar.

### 8.1.1 Login

After Securaze Mobile has been installed on the station (see Installation), start it. It opens with the login screen: **Hello, who's this ?**

macOS only: before the login screen, Securaze Mobile asks for an administrator password: **SecurazeMobile requires administrator privileges to manage connected devices.** Type the password of the macOS user you are logged in with - this user must be an administrator of the Mac - and click **Continue**. **Save & Continue** also keeps the password in your login keychain, so Securaze Mobile does not ask again at the next start; until then it asks at every start, and if the saved password stops working, it asks again. **Cancel** quits Securaze Mobile.

### Log in

1. Type your user name or e-mail address in **Username or email address** and your password in **Password**. Your administrator gives you the user. The eye icon in the password field shows or hides the password.

2. As soon as a field contains text, two check boxes and the **LOG-IN** button appear:


© 2026 Securaze GmbH

• **Remember my credentials** - saves the user name and password on this station and fills them in next time. Clear the box to delete the saved credentials.

• **I Agree to Securaze terms of use.** - must be ticked to log in. It is ticked by default. Click **terms of use** to read them.

3. Click **LOG-IN** or press Enter.

While Securaze Mobile logs you in, it shows **Logging in...**. If the login fails, the reason appears under the title, for example **Username or password incorrect. Please try again.** If the station has no connection to the Securaze server, it shows **You are disconnected. Please re-connect and try again.** - check the network; the sidebar shows **Disconnected**.

## Language

The language selector at the bottom right of the login screen shows the current language. Click it and choose another language; the screen switches at once. The language can only be changed before login - also in **Options & Settings** > **General** > **Language**.

## More on the login screen

• The sidebar on the left: **Help** (Ctrl+H), **General settings** (F9) and the connection status. See Help 171 and Options & Settings 174.

• **VERSION** under the login box - the version of Securaze Mobile.

• **Out of date** in the bar at the bottom - shown when a newer version of Securaze Mobile is available. Click it to open the update dialog.

• After an update, a panel beside the login box can show what is new: **Release Notes** opens the release notes in your web browser, **Understood** closes the panel.

• Linux only: while Securaze Mobile runs from the installation stick and is not installed yet, **INSTALL** and **UPDATE** appear under the login box. See Installation.

## After the login

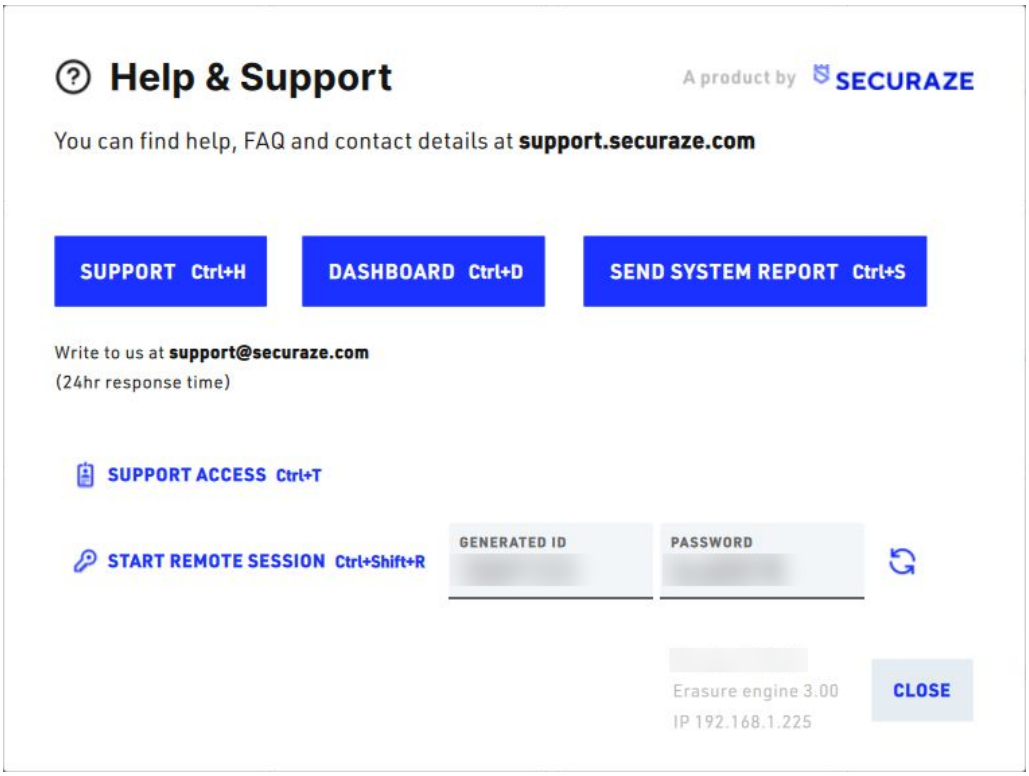
If the Mobile preset in your Securaze Dashboard has no Wi-Fi network, Securaze Mobile shows **Wi-Fi Preset Missing**. **Create preset** opens the Mobile presets in the Securaze Dashboard and logs you out - log in again once the preset is saved. **Continue** goes on without it; erasures are then slower and some functions are not available (see iOS requirements 199).

Then Securaze Mobile asks for what this session needs - see Pre-selection 183.

### 8.1.1.1 Help

Open the Help dialog with **Help** in the sidebar or with Ctrl+H. It is in the sidebar on every screen, also before you log in. The dialog is called **Help & Support**.


© 2026 Securaze GmbH




## Getting help

• **support** (Ctrl+H) - opens the Securaze Knowledge Base in your web browser.

• **Dashboard** (Ctrl+D) - opens the Securaze Dashboard in your web browser. If Securaze Mobile does not know the Dashboard's address yet, it opens securaze.com.

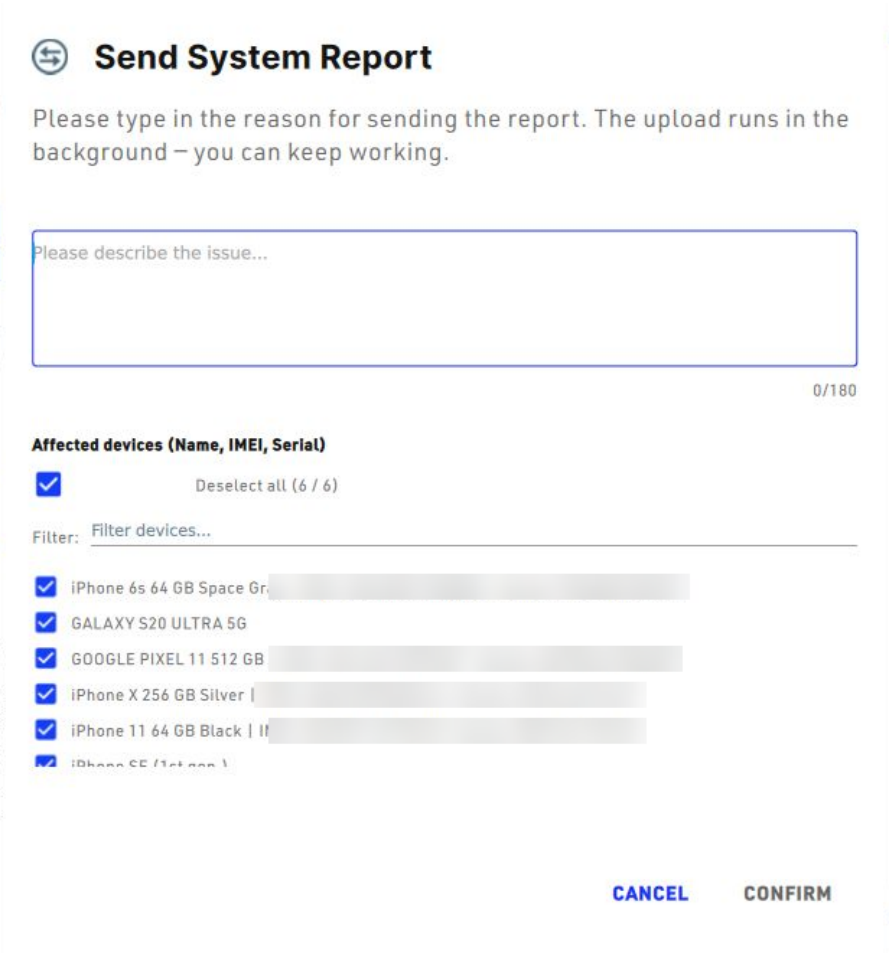
• **Send system report** (Ctrl+S) - sends a system report to Securaze support. The button is only there after you have logged in. See below.

The dialog also shows where to find help, FAQ and contact details (support.securaze.com) and the support e-mail address: support@securaze.com (24hr response time).

## Send a system report

Click **Send system report** (Ctrl+S). The dialog **Send System Report** opens.


© 2026 Securaze GmbH




• Type the reason for the report (up to 180 characters). **Confirm** can only be used once there is a reason.

• Under **Affected devices (Name, IMEI, Serial)** all connected devices are selected. Use **Filter:** to find a device. If exactly one device is selected, its name, IMEI and serial number are added to the report.

• Click **Confirm** or press Ctrl+Enter. **Cancel** or Esc closes the dialog without sending.

The report - with the station's log files - is uploaded in the background, so you can keep working. The notification line shows **Sending system report in the background...** and then **System report sent.** If the upload fails, the notification says why and offers **Retry** (Alt+R). While one report is still being prepared, a second one is not started.

You can also send a system report from **Infrastructure issues** on the dashboard.

## Remote support

Securaze support can connect to the station with RustDesk. The station must be online.

• Click **Start remote session** (Ctrl+Shift+R). While the session is prepared, the fields **GENERATED ID** and **PASSWORD** show **Loading...**.


© 2026 Securaze GmbH

• Give the ID and the password to Securaze support. Support connects to the station with them.

• The refresh icon next to the fields prepares a new session with a new password.

If the station is offline, Securaze Mobile shows **Support not available in offline mode.** Step by step: see Support 185.

### More in the dialog

• Windows only: **Re-detect iPhones and iPads** (Ctrl+I) - restarts the Apple service, as unplugging and plugging in again would. While it runs, the button reads **Re-detecting iPhones and iPads...**. Then Securaze Mobile shows **Apple service restarted. Connected iPhones and iPads show up again in a few seconds.** If the service cannot be restarted, Securaze Mobile says so; what to do is listed under **Infrastructure issues**.

• **Support Access** (Ctrl+T) - for Securaze support staff only. It asks for a support password.

• macOS only: **Open log folder** (after you have logged in) shows the log file of Securaze Mobile in Finder, and **Show configuration file** shows its configuration file in Finder. Support may ask you for them.

• If a newer version is available, the dialog shows **New version available** at the top. **Update now** opens the update dialog.

• At the bottom right: the version of Securaze Mobile, the version of the erasure engine and the station's IP address (**IP**). Support may ask you for them.

• **Close** or Esc closes the dialog.

## 8.1.1.2 Options & Settings

Click **General settings** (the gear icon) in the sidebar or press **F9**. The window **Options & Settings** has these tabs:

General 175 - screen resolution, scaling, language, card view, expert modes, station ID, hubs and port layout

Processing 176 - how devices are handled: unplugging, erasure retries, Android and iOS options, SKU list, diagnose

Workflows 178 - run this station from workflows, import workflows

Printer 180 - print server and preferred printer

Network & Storage 181 - Securaze backend, firmware folder, data folder, iOS firmware copy

Integrations 182 - robot integration

Tools 183 - Linux only: additional programs for the station

About 183 - version, Coming Soon, release channel

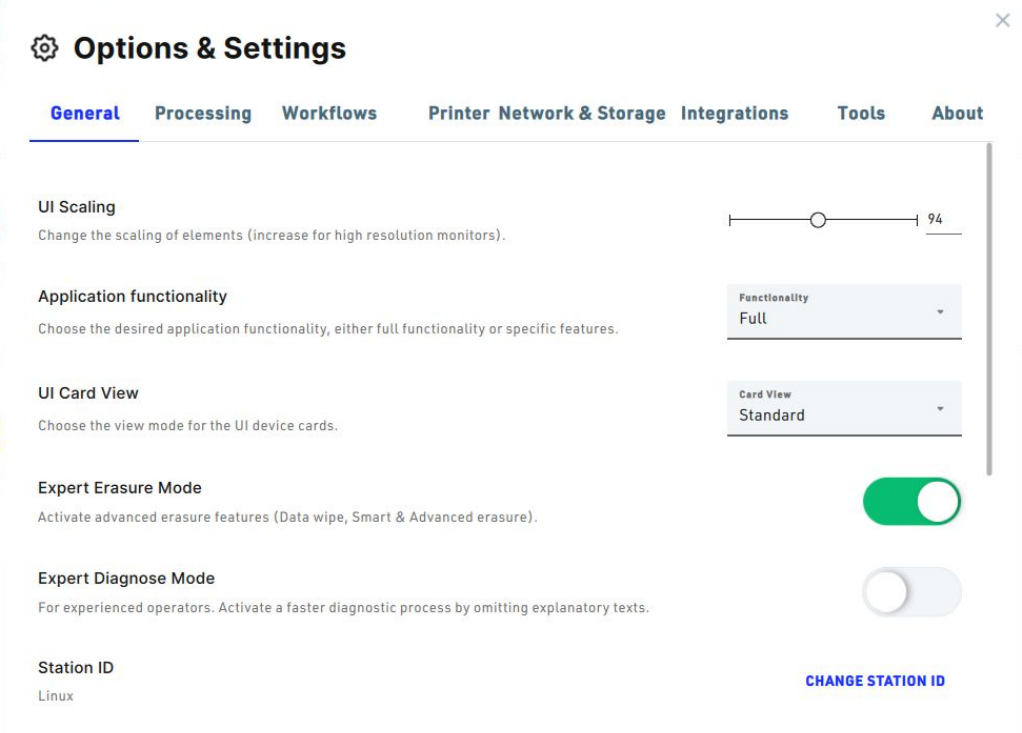

© 2026 Securaze GmbH

Some settings change how the whole station works. They are grayed out unless you are logged in as a user whose role allows changing the Mobile settings. In this manual they are marked (settings permission). The **Tools** tab can only be opened by such a user.

Some settings can only be changed before you log in, for example **Language**.

### 8.1.1.2.1 General

The **General** tab holds the settings for the screen, the language and the station.




**Change display resolution** - Linux only: shown before login. Changes the screen resolution. By default the highest available resolution is used. After a change, click **KEEP CHANGES** within 15 seconds - otherwise the previous resolution comes back.

**UI Scaling** - the size of the screen elements, from 45 to 150%. Increase it for high-resolution monitors.

**Application functionality** - which functions Securaze Mobile offers: **Full** (all features), **Only Erasure**, **Only Diagnose** or **Only Registration**.

**UI Card View** - **Standard** shows many devices at once, **Detailed** shows more details of each device on its card. The card view button in the dashboard header (Ctrl+Shift+V) switches between the two as well.

**Expert Erasure Mode** - turns on the advanced erasure features (Data wipe, Smart & Advanced erasure). With it on, the arrow of **ERASE SELECTED** offers **ERASURE SETTINGS** and the erasure solutions; with it off, only **ERASE ALL**.

**Expert Diagnose Mode** - for experienced operators: a faster diagnose that leaves out the explanatory texts.


© 2026 Securaze GmbH

**Language** - the language of the user interface. You can change it only before login.

**Station ID** - the name of this station (settings permission). Click **CHANGE STATION ID**, type the new name (up to 50 characters) and press Enter.

**Port numbers without hub letter** - labels and the Securaze Dashboard show a phone's port as its number only, for example 13 instead of B13.

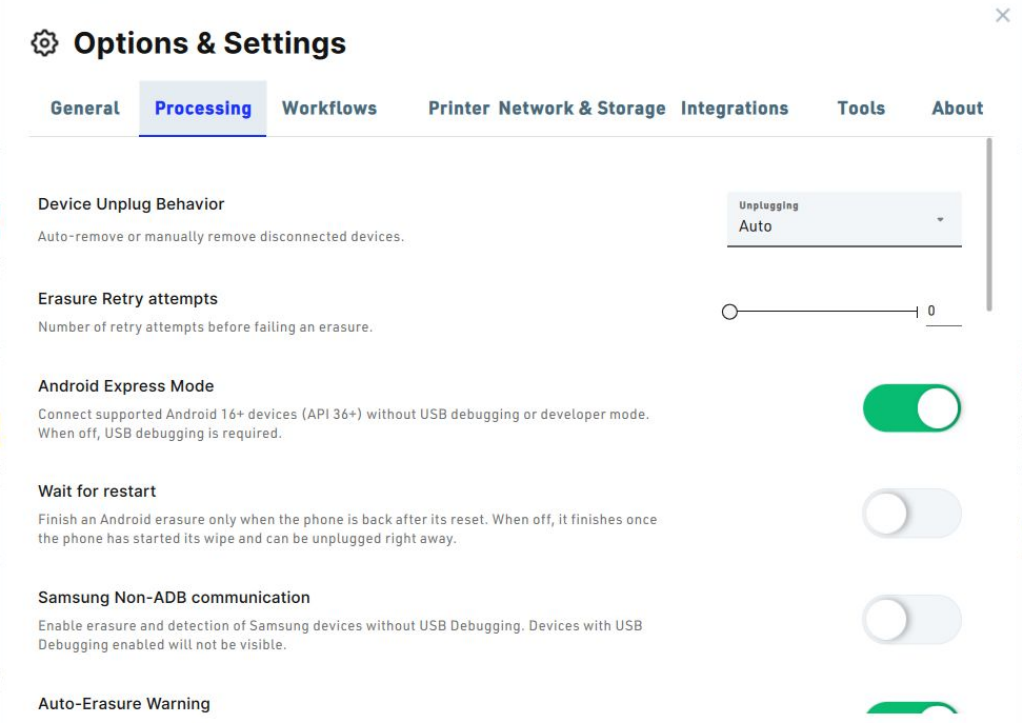
**Hubs** - **MANAGE HUBS** lists the hubs of this station with their letters and layouts. There you can set a hub up again, number its ports in the printed order or forget a hub that is gone. See USB Hubs 190.

**Reset EasyIDs. (Port layout)** - **RESET PORT LAYOUT** resets the port numbers and color IDs. Unplug all devices and hubs before you continue, then run the hub setup again.

**Tutorial** - **RESET TUTORIAL** shows the tutorial again the next time you start Securaze Mobile.

### 8.1.1.2.2 Processing

The **Processing** tab sets how Securaze Mobile handles the connected devices.




**Device Unplug Behavior** - (settings permission) **Auto** removes a device's card as soon as the device is unplugged. **Manual** keeps the card until you remove it.

**Erasure Retry attempts** - how often a failed erasure is tried again before it counts as failed (0 to 5).

**Android Express Mode** - connects supported Android 16 and later devices (API 36+) without USB debugging or developer mode. When it is off, USB debugging is required.


© 2026 Securaze GmbH

**Wait for restart** - off by default. When it is on, an Android erasure finishes only when the phone is back after its reset. When it is off, the erasure finishes once the phone has started its wipe, and you can unplug the phone right away. Workflows follow this setting too.

**Samsung Non-ADB communication** - erases and detects Samsung devices without USB debugging. Devices with USB debugging on are not visible in this mode. In this mode FRP (Google reactivation lock) cannot be detected - to check FRP, process the device in standard (ADB) mode. If you change it while logged in, Securaze Mobile asks first: running processes are interrupted, then Securaze Mobile logs out and restarts.

**Auto-Erasure Warning** - when **AUTO-START ERASURE** is on in the Securaze Dashboard, Securaze Mobile warns at start that phones you plug in are erased. **Don't show this again** in that warning switches this setting off - switch it on here to get the warning again.

**SKU list** - the SKU list is loaded at login. After SKUs were added in the Securaze Dashboard, click **RELOAD**: devices without an SKU get theirs.

**Hide Deactivated Ports** - hides the deactivated ports to keep the workspace clear.

**iOS device shutdown behavior** - (settings permission) **Automatic Shutdown** switches the device off after a successful erasure, **Keep Running** leaves it on.

**iOS Version.xml source** - (settings permission) where the list of iOS firmwares comes from: **Apple** or a version verified by **Securaze**. A change needs a restart: click **LOGOUT**. Some iOS firmwares already downloaded may be removed.

**iOS force device deactivation** - deactivates the iOS device when it is read, so the Find My (FMiP) and MDM lock values are always current. **Attention!** If Find My is on, the device needs the Apple ID and password before it can be used again.

**iOS Auto-Start Application on Device** - starts the Securaze app on the iOS device automatically - useful for diagnose and advanced erasure. On iOS 17 and later the app is started automatically only if the next setting is on as well. Otherwise start the app on the device by hand.

**Experimental iOS 17 and Later Versions Auto-Start Application on Device** - starts the app automatically on iOS 17 and later devices too. This is an experimental feature. It is shown only when **iOS Auto-Start Application on Device** is on and **Coming Soon** is on (About 183 tab).

**iOS keep WiFi Connection during diagnose** - the device stays on Wi-Fi after the diagnose has started. This can strain an access point that allows only a few connections at a time.

**Enhanced iOS Battery Analysis** - reads detailed battery data, including data of replacement batteries. It adds about 30 seconds to reading the device and to the erasure.

**Battery level notification** - (settings permission) shows a notification for devices whose battery is below this percentage (5 to 100%).

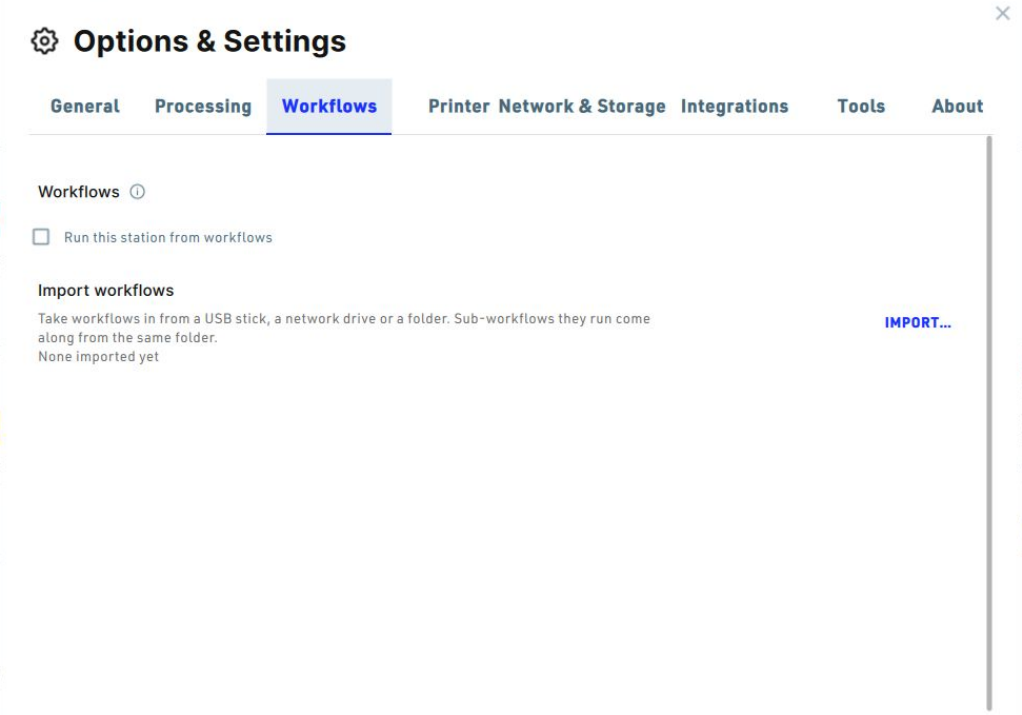

© 2026 Securaze GmbH

**Automatic Finish Diagnose and Upload results** - finishes the diagnose and uploads the results as soon as the last test is done. When it is off, the operator can review the results, retest and confirm them.

**Preferred Wifi** - the Wi-Fi network used for the setup QR codes, diagnose and advanced erasure. The list shows the Wi-Fi networks from your Securaze Dashboard presets - the setting is shown only if there are any. A network without a password can be used too.

### 8.1.1.2.3 Workflows

On the **Workflows** tab you set up whether this station runs from workflows. A workflow decides what happens to each device and in what order - what to check, what to erase, when to print. With workflows on, the station runs from the workflow instead of from its presets. How to work with workflows is described in Workflows 50.




**Run this station from workflows** - tick it to run this station from workflows. The station keeps the workflows it has been given.

**Safe test mode: workflow steps that would erase, reset, report or save are only simulated** - shown when workflows are on. Tick it to try a workflow out on this station: its steps that would erase, reset, report or save are only simulated. It stays on until you clear it, switch workflows off or sign out.

**Import workflows** - takes workflows in from a USB stick, a network drive or a folder. Sub-workflows they run come along from the same folder. The row shows how many workflows are imported. Before login anyone can import; after login only a user with the settings permission.


© 2026 Securaze GmbH

**Workflow this station runs** - shown when **Run this station from workflows** is ticked. Choose the workflow. With **Chosen after login** and several workflows on the station, the operator chooses one after login and can change it for the next phones with **Change workflow** (Ctrl+Shift+W). If the chosen workflow is no longer on the station, the list says so.

## Import workflows

1. Click **IMPORT...**.

2. Windows and macOS: click **Choose files...** and select the workflow files (*.json) in the system's file dialog. They are imported at once.

Linux only: in Mobile's own file browser, choose the USB stick, network drive or folder (Enter) and open the folder with the workflows. Select the workflows (Space, or **SELECT ALL** Ctrl+A) and click **IMPORT** (Ctrl+Enter).

3. The result lists what was imported, which sub-workflows came along and which earlier versions were replaced. Click **DONE**. If you imported from a USB stick, take the stick out.

Under **On this station** the import window lists the workflows on the station. **REMOVE** (Del) removes one.

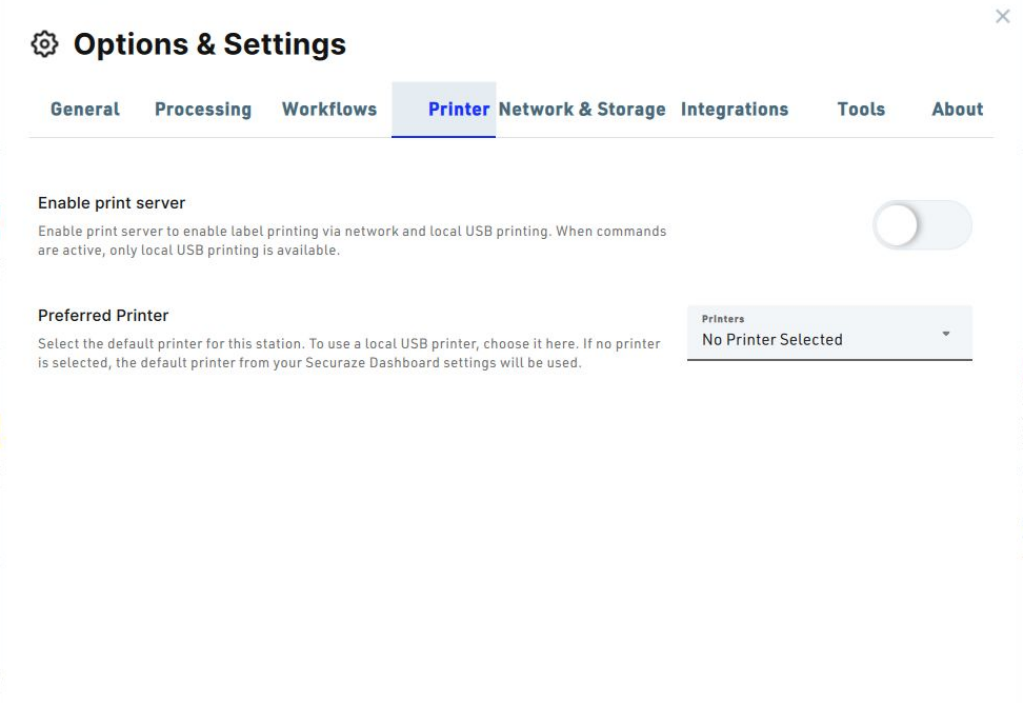
If workflows are switched off on this station, the import window offers **SWITCH WORKFLOWS ON**.

If the station takes its workflows from the server, imported workflows are kept but not used.


© 2026 Securaze GmbH

### 8.1.1.2.4 Printer

On the **Printer** tab you set how this station prints labels.




**Enable print server** - (settings permission) lets this station print labels over the network and to a local USB printer. If Securaze Command is active in the network, the tab says **Securaze Command is active in the network.** - then only local USB printing is available from this station.

**Preferred Printer** - the default printer for this station. To use a local USB printer, choose it here. The list shows (USB) or (Network) after a printer's name. If no printer is selected, the default printer from your Securaze Dashboard settings is used. With the list open, 1 to 9 picks one of the first nine printers.

If you choose a USB printer while the print server is off, the tab says **Enable the print server for local USB printing to work.**

For a USB label printer from Brother, DYMO or Zebra - the one chosen here, or the one the last label went to - a line below **Preferred Printer** shows what Securaze Mobile found, checked again every 5 seconds while the tab is open: **Found: <print queue> · driver: <driver> · ready**, or what is missing and what is expected instead, for example **Expected: Brother's QL driver**.

When labels cannot be printed like this, a hint says what to do, for example plug in the printer and switch it on, or add its print queue in the system's printer settings. Windows only: the hint names the driver to install - Brother's QL driver, DYMO Connect or the ZDesigner driver. macOS only: for a DYMO printer the hint names DYMO Connect for Mac, which brings the driver. If the printer's queue uses Windows' generic IPP driver, labels

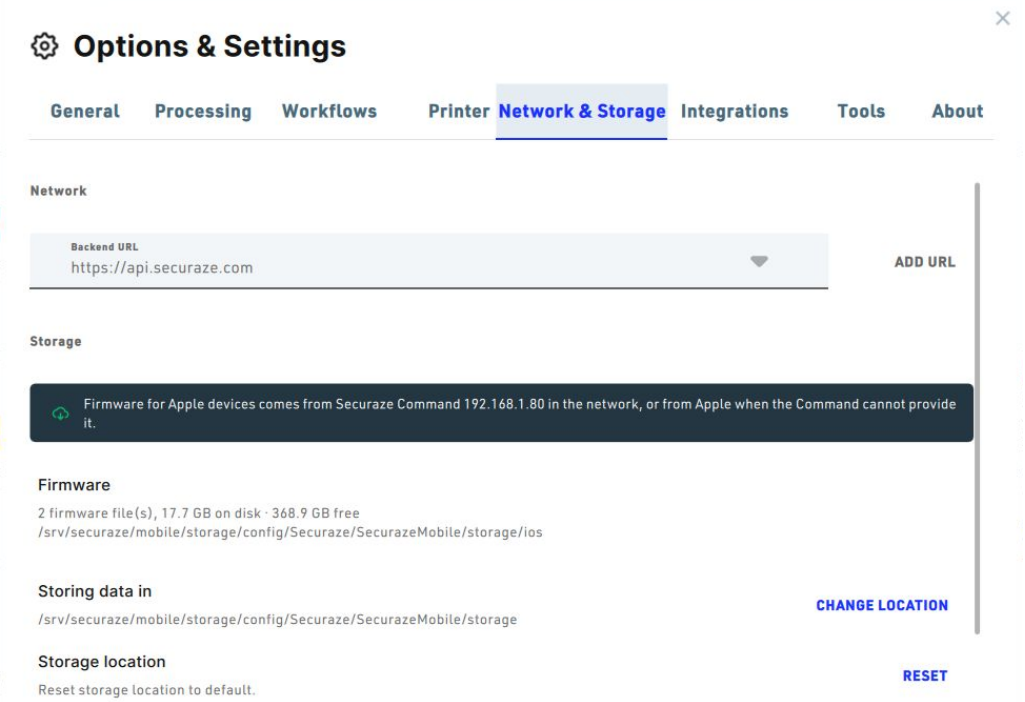

© 2026 Securaze GmbH

cannot print; the hint gives the steps: Printer properties > Advanced > Driver, pick the maker's driver, Apply.

When a label is not printed, the dashboard says **Label not printed on <printer>: <reason>.** and what to do, for example when the printer is out of labels or its cover is open. The problem is also listed under Infrastructure issues 73.

### 8.1.1.2.5 Network & Storage

The **Network & Storage** tab has two parts: the Securaze backend this station works with, and where Securaze Mobile stores its data.




## Network

Choose the Securaze backend in the **Backend URL** list. Normally there is only one. You can change the backend only before you log in.

To add a backend:

1. Click **ADD URL**.

2. Click **ADD LINE**, type the URL of the backend and press Enter. Use a URL that starts with https:// - other lines are marked with a warning sign.

3. Click **CLOSE**. The new backend can now be chosen in the **Backend URL** list.

When you choose another backend, Securaze Mobile shows **Backend URL change requires restart**: from then on all assets and reports are stored on the other Securaze backend. Click **LOGOUT** - Securaze Mobile restarts.


© 2026 Securaze GmbH

### Storage

When a Securaze Command answers in the network, the tab says **Firmware for Apple devices comes from Securaze Command <address> in the network, or from Apple when the Command cannot provide it.**

**Firmware** - the firmware folder: how many firmware files it holds, how much it takes on disk, downloads in progress, the free space and the folder's path. Windows and macOS: **OPEN FOLDER** opens the folder.

**Storing data in** - (settings permission) the folder where Securaze Mobile stores its data. Click **CHANGE LOCATION** to choose another folder. Securaze Mobile then shows **Storage location change requires restart**: click **RESTART NOW** - Securaze Mobile restarts and keeps its data and firmware in the new folder; erasures that are still running are stopped. **CANCEL** keeps the folder in use.

**Storage location** - (settings permission) **RESET** sets the default folder again - after the same question as **CHANGE LOCATION**.

**Revert Version Update** - Linux only: shown when a previous version is installed. **REVERT VERSION** goes back to the previously installed version if the current version has problems.

**Copy iOS firmwares (*.ipsw) from external medium** - shown before login. Connect an external drive named Securaze and click **START COPY**. The files are copied from its iOS folder and from its root folder. See Upload iOS Firmware 162.

## 8.1.1.2.6 Integrations

On the **Integrations** tab you connect Securaze Mobile to a robot (settings permission).

**Robot Integration** - **None** or **Adapta Robotics MATT (BETA)**. MATT is offered only when **Coming Soon** is on (About 183 tab). Switching Coming Soon off sets the robot integration back to None.

### Robot Connection

With MATT selected, the tab shows the robot connection settings. The robot connects to this station over the network. Changes apply after restarting Securaze Mobile.

**Robot Connection** - **ENABLE** or **DISABLE** the connection.

**Require Access Token** - **TURN ON** to accept only a robot that sends the access token. When it is off, the connection is open to the network.

**Access Token** - **EDIT** to type a token, **GENERATE** to create one.

**Network Port (HTTP)** and **Network Port (WebSocket)** - the ports the robot connects to, for example 8766 and 8765. Click **EDIT** to change one.


© 2026 Securaze GmbH

#### 8.1.1.2.7 Tools

The **Tools** tab is there on Linux only, and only a user with the settings permission can open it. Here you install additional programs that Securaze offers for the station, and start them.

Each entry shows the program's name and latest version, and whether it is installed (**Installed:** with the installed version, or **Not Installed**).

**INSTALL** - downloads and installs the program.

**UPDATE** - shown with **Update Available** - installs the latest version.

**REINSTALL** - installs the current version again.

**START** - starts an installed program.

#### 8.1.1.2.8 About

The **About** tab shows the version of Securaze Mobile and of the erasure engine.

Before you log in, it also shows these settings:

**Coming Soon** - lets you try new features before they are released for all customers. With Coming Soon on, the Beta and Internal release channels and beta features are offered, for example the Adapta Robotics MATT robot integration (Integrations 182 tab).

**Attention!** Beta versions and beta features are not fully tested yet. Use them carefully and only on advice of the Securaze support team.

**Release channel** - which versions this station receives from the update server: **RELEASE**, **BETA** or **INTERNAL**. Beta and Internal are offered only when Coming Soon is on; Internal is for Securaze staff only. Switching Coming Soon off sets the channel back to Release.

### 8.1.2 Pre-selection

After the login, Securaze Mobile asks a few questions for this session before the dashboard opens. It shows only the screens it needs.

#### Company

If your user belongs to more than one company, **Select a company** opens with the list **Available companies**. Click the company you work for in this session. A company marked **(Not in allowed network zone)** cannot be chosen from the network this station is in. **Exit** logs you out and returns to the login screen.

On a new station, the quick setup follows: choose the license and name the station. See Connect devices 54.

#### Workflow

On a station that runs workflows, Securaze Mobile can ask which workflow the phones of this session go through. See Workflows 50.

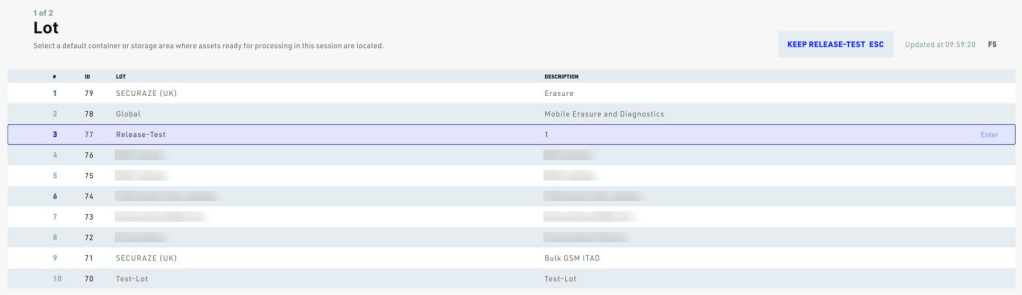

© 2026 Securaze GmbH

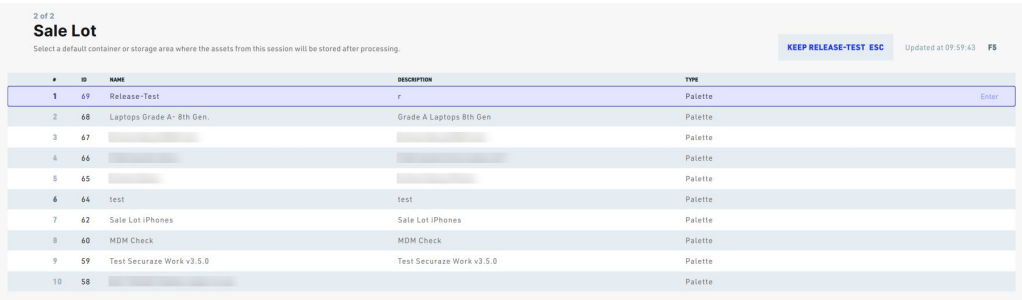
## Lot and Sale Lot

Then you choose where the devices of this session come from and where they go:

• **Lot** (1 of 2) - where the devices you process in this session are now.

• **Sale Lot** (2 of 2) - where the devices are stored after processing.




Choose a row: click it, press its number (1 to 9), or move with the arrow keys and press Enter. The Lot list shows **ID**, **Lot** and **Description**; the Sale Lot list shows **ID**, **Name**, **Description** and **Type**.

• Long lists are split into pages. The bar at the bottom shows **Items per page:** and which entries you see; the Left and Right arrow keys switch pages.

• With more than nine entries, the search icon in that bar opens a search field. Type a search term and press Enter.

• **Updated ... ago** shows when the list was loaded. **F5** loads it again.

If a Lot and a Sale Lot are set in the Securaze Dashboard preset, Securaze Mobile skips these screens, or asks only for the one that is missing. See Set presets 44.

To change the Lot or Sale Lot later without logging out, click **Change lot** (Ctrl+Shift+L) in the sidebar. The same screens open; **Keep** with the current name (Esc) keeps what is in use. See Menu 187.

## Then

The dashboard opens - see Dashboard 185. If **AUTO-START ERASURE** is on in the Securaze Dashboard, Securaze Mobile first shows **Auto-Erasure Enabled**: do not plug in phones that are not to be erased. **Continue** goes on, **Exit app** closes Securaze Mobile. **Don't show this again** switches the warning off (see Processing 176).


© 2026 Securaze GmbH

Help and support are in the sidebar on every screen: **Help** (Ctrl+H). See Help 171 and Support 185.

#### 8.1.2.1 Support

Everything for support is in the **Help & Support** dialog. Open it with **Help** in the sidebar or with Ctrl+H.

### Ways to get help

• Knowledge Base: **support** (Ctrl+H in the dialog) opens it in your web browser.

• E-mail: support@securaze.com (24hr response time).

• System report: **Send system report** (Ctrl+S) sends your description and the station's log files to Securaze support. Only after you have logged in.

• Remote session: **Start remote session** (Ctrl+Shift+R) lets Securaze support connect to the station with RustDesk.

### Remote session step by step

1. Check that the station is online: the sidebar shows **Connected**.

2. Open Help (Ctrl+H) and click **Start remote session** (Ctrl+Shift+R).

3. Wait until the fields **GENERATED ID** and **PASSWORD** show values instead of **Loading...**.

4. Give the ID and the password to Securaze support, for example on the phone or by e-mail. Support connects to the station with them.

For a new session, click the refresh icon next to the fields. It prepares a new session with a new password.

Remote support uses RustDesk only. Older versions of Securaze Mobile also offered AnyDesk; it is no longer used. The firewall must let the station reach the Securaze remote-support server - see System environment.

All buttons of the dialog: see Help 171.

## 8.2 Dashboard

The dashboard is the main screen of Securaze Mobile after login. It has four areas: the menu on the left, the header at the top, the device tiles in the middle and the bar at the bottom. The menu is described in Menu 187.

### Header

• Station name, date and time.

• The workflow the station runs, beside the station name - only on stations that run workflows. Click it to change the workflow. See Workflows 50.


© 2026 Securaze GmbH

• A red warning sign with a number, e.g. [2] - problems with the station. Click it to open the list. See Infrastructure issues 73.

• **Auto-erasure on** - the Securaze Dashboard preset starts the erasure by itself.

• License counters - how many licenses are left. Point at a counter to see which kind it is: **Registration licenses**, **Erasure lite licenses**, **Erasure licenses** or **Diagnose licenses**.

• **STANDARD** / **DETAILED** (Ctrl+Shift+V) - shows the card view in use. Click it to switch the tiles between the standard and the detailed view - the same setting as **UI Card View** in Options & Settings > General.

• UI scale - drag the slider or type a value between 45 and 150 %.

## Device tiles

One tile per USB port. Tick a tile's check box to select the device, click the tile for the device details, right-click it for the device menu. Empty ports show **Connect Device** or their own state, for example **Charge Port**, **Deactivated Port**, **Cable Issue** or **Port Issue**. See Check the connected devices 72.

## Bottom bar

• **...** - **CUSTOMIZE FILTERS**: choose which filter categories the bar shows.

• Book icon - **Instructions** for setting up and diagnosing devices.

• QR code icon - **Skip setup screen for Android**. See Android USB-Debugging bypass with QR-Code 60.

• **ALL** and the filters: **Alerts**, **Disconnected**, **In Progress**, **Not Graded**, **No External ID**, **Failed erasures**, **Failed Connection**, **Already processed**. Windows only: **Microsoft Driver**. A filter is shown only when at least one device matches it.

• **MORE** - for the selected devices: **Register and skip the hello screen [iOS only]** (with Registration licenses), **Reboot** and **Turn Off**. MORE sits left of **REGISTER SELECTED**. When the bar is short of room, MORE shows only its dots.

• **REGISTER SELECTED** - registers the selected devices. Shown with Registration licenses. See Register devices 80.

• **DIAGNOSE SELECTED** - starts the diagnose on the selected devices. The arrow opens the diagnose settings and your favorite preselections. See Perform diagnose 89.

• **ERASE SELECTED** - erases the selected devices. The arrow: with Expert Erasure Mode on, **ERASURE SETTINGS** and the erasure solutions **DATA CLEAR**, **SMART ERASURE** and **ADVANCED ERASURE** (without Erasure licenses only **DATA CLEAR**); with Expert Erasure Mode off, only **ERASE ALL**, which erases all connected devices. See Perform erasure 81.

• **Cancel diagnose** / **Cancel erasure** - appears while the device you clicked is running.


© 2026 Securaze GmbH

### 8.2.1 Menu

The menu runs down the left side of the dashboard. Point at an icon to see its name and keyboard shortcut; some also show their current value, for example the lot.

#### Select

• **All devices** (Ctrl+A) - selects all devices, or clears the selection.

• **Apple devices** - selects all Apple devices.

• **Androids** - selects all Android devices.

Click the Securaze Mobile logo at the top of the menu to show all devices again (filter **ALL**).

#### Actions

• **Clear Ports** - removes the tiles of devices that were unplugged. Available when a device is disconnected.

• **All tiles** (Ctrl+Shift+G) - puts every tile on the same tab: **Each tile on its own**, **Grading**, **Registration**, **Erasure**, **Diagnose** or **Workflow**. Ctrl+Shift+G switches between **Grading** and each tile on its own. Only with detailed tiles: switch to them with the card view button in the header (**STANDARD** / **DETAILED**, Ctrl+Shift+V) or in Options & Settings > General > **UI Card View**. **Registration** is offered with Registration licenses, **Workflow** on stations that run workflows.

• **Print labels** (Ctrl+P) - prints labels for the selected devices, or for all shown devices when none is selected. **Printer Selection** shows how many labels will be printed; choose the printer and click **Start printing**.

• **Change lot** (Ctrl+Shift+L) - opens the lot and sale lot screens again, without logging out. Devices connected afterwards go into the new lot. If selected devices are still in the previous lot, Mobile asks whether to move them too (**Move ... devices** or **Leave them**). See Select point of origin 52 and Select Sale Lot 53.

• **Change workflow** (Ctrl+Shift+W) - only on stations where the operator chooses the workflow: choose the workflow for the devices you connect next. See Workflows 50.

• **Add devices manually** (Ctrl+N) - Manual Entry: add a device by hand, for example one that does not turn on. See Manual Entry 69.

• **Retry All** - starts the session again for all devices whose connection to Securaze failed (filter **Failed Connection**).

• **Confirm All** - processes all devices marked **Already processed** again.


© 2026 Securaze GmbH

## Bottom of the menu

• **Connected** / **Disconnected** - the connection to the Securaze server. Point at it to see the address. Linux only: click it to choose a Wi-Fi network.

• User name - **User Profile**. Click it and then **Exit** to close Securaze Mobile or to restart or shut down the computer. See Exit 53.

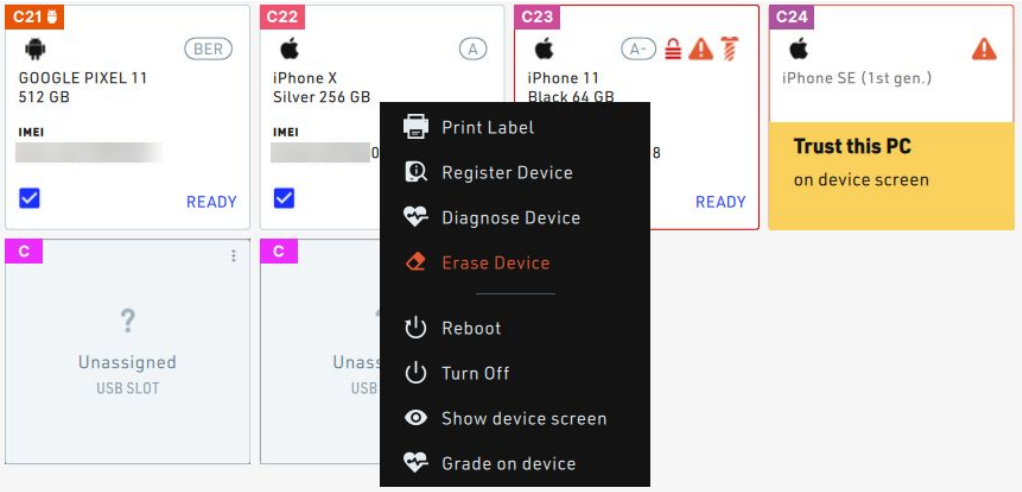
• **Help** (Ctrl+H).

• **General settings** (F9) - opens Options & Settings.

The version of Securaze Mobile is shown at the very bottom.

## Device menu

Right-click a device tile to open its menu (on a detailed tile, also the ... button). Entries that do not apply right now are grayed out.




• **Print Label** - prints the device's label. If no printer is selected yet, Mobile asks for one first.

• **Register Device** / **Cancel Registration** - starts or stops the registration of the device. Shown with Registration licenses. See Register devices 80.

• **Diagnose Device** / **Cancel Diagnose** - starts or stops the diagnose of the device.

• **Erase Device** / **Cancel Erasure** - starts or stops the erasure of the device.

• **Reboot** - restarts the device.

• **Turn Off** - turns the device off.

• **Restart USB port** - only for a device on a managed hub (Cambrionix): turns the port off and on, so a device that hangs restarts without unplugging it. It comes back after a few seconds.

• **Show device screen** - opens **Live preview**: repeated screenshots of the device's screen, not video, with **Pause**, **Save picture** and **Close**. Useful to show support what the device


© 2026 Securaze GmbH

shows. Grayed out where Mobile cannot reach the screen: AirPods, Macs, devices in DFU or recovery mode, and Android devices without USB debugging (Samsung Non-ADB mode, Android Express Mode).

• **Grade on device** - opens a grading form in the Securaze app on the device: pick the grade and the problems that apply on the device itself, then tap **Submit Grading**. The grade is saved for the device. Needs an active session and the grades of your company in the Securaze Dashboard; not during an erasure or while the phone's tests run; not for AirPods.

• **Select all from Hub** / **Remap Hub** - at the end of the menu, only when the device's hub has no empty port on the dashboard, for example with a device on every port. Otherwise right-click an empty port of the hub (see Port menu).

## Port menu

On an empty port, click the ... icon at the top right of the tile:

• **Set as Charging Only** - the port only charges. The tile shows **Charge Port** / **Power Only**.

• **Deactivate Port** - the tile shows **Deactivated Port**. On a port that is not active, **Reactivate Port** turns it back on.

• **Name this port** - gives the port its own name, for example Bay 3 / Slot 12. Labels and the Securaze Dashboard show this name instead of the hub letter and port number. Save an empty name to go back.

• **Report as** > **Report Bad Cable** - the tile shows **Cable Issue** / **Please replace cable**.

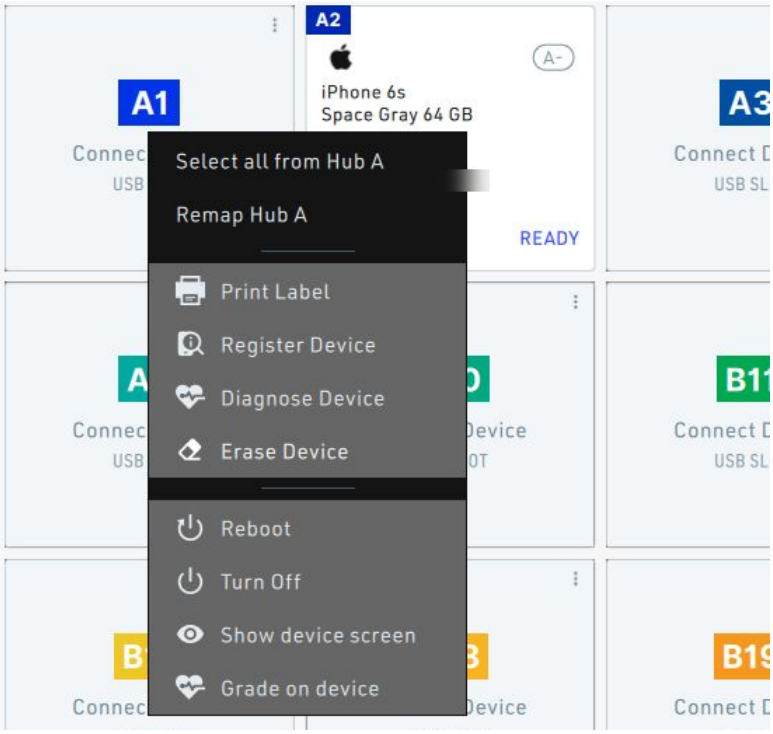
• **Report as** > **Report Broken Port** - the tile shows **Port Issue** / **Port not working**.

Right-click an empty port for the entries of its hub (the device entries are grayed out there):

• **Select all from Hub** / **Deselect all from Hub** - selects all devices on the hub, or clears the selection.

• **Remap Hub** - deletes the port layout of the hub and starts the hub setup again. See USB Hubs 190.


© 2026 Securaze GmbH




## 8.2.2 USB Hubs

Securaze Mobile tells your USB hubs apart by a letter - A, B, C and so on - and a color, and gives each port a number. You put a sticker with the letter on the hub. The port number shows on the phone's tile, on its labels and in the Securaze Dashboard.

You set up each hub once. After that, Mobile knows the hub and its ports every time it starts.

### In this chapter

• General information 190 - letters, colors and port numbers, and in which order to plug things in.

• Setting up a USB hub 191 - a new hub, numbered in the order printed on it or mapped by hand, and a hub moved to another USB port.

• Managing hubs 195 - set a hub up again, switch it to the printed order, forget a hub, and give a port a name of its own.

The hubs we recommend are listed under Hardware.

### 8.2.2.1 General information

A USB hub turns one USB port of the PC into several, like a power strip. All devices on a hub share the bandwidth available to that hub.


© 2026 Securaze GmbH

### Letters, colors and port numbers

Mobile gives each hub a letter in the order it first sees the hubs: the first hub is A, the next B, and so on. Each hub also has a color, shown as a dot next to its letter, for example in Manage hubs.

Port numbers run on from hub to hub. With two 10-port hubs, hub A has ports 1 to 10 and hub B ports 11 to 20. A phone on the third port of hub B shows B13 on its tile, and its labels and the Securaze Dashboard show B13 too.

You can give a port a name of its own, such as Bay 3 / Slot 12, or have labels show the number without the letter - see Managing hubs 195.

### The hub's layout

When you set up a hub, Mobile saves which physical port has which number. This is the hub's layout. Mobile keeps one layout per hub, recognizes the hub by the USB port of the PC it is plugged into.

A hub without a layout still works, but its phones get the next free number in the order you plug them in. The numbers then do not match the ports.

### Before you start

**Start Securaze Mobile first. Then plug in the hubs one at a time, and set up each hub before you plug in the next. Plug in the phones last.**

This way each hub gets the letter you expect, and the setup always knows which hub you mean.

Mapping a hub by hand needs an empty hub. Numbering a known hub in its printed order also works with phones on it - see Setting up a USB hub 191.

## 8.2.2.2 Setting up a USB hub

Mobile opens the hub setup for every hub that has no layout yet - after you log in, and whenever you plug in a new hub. It sets up one hub at a time.

The title of the setup's first page, **USB Hub setup**, ends with the hub's letter. Take the sticker with this letter and put it on the hub where you can see it.

Below it, the page says what Mobile found:

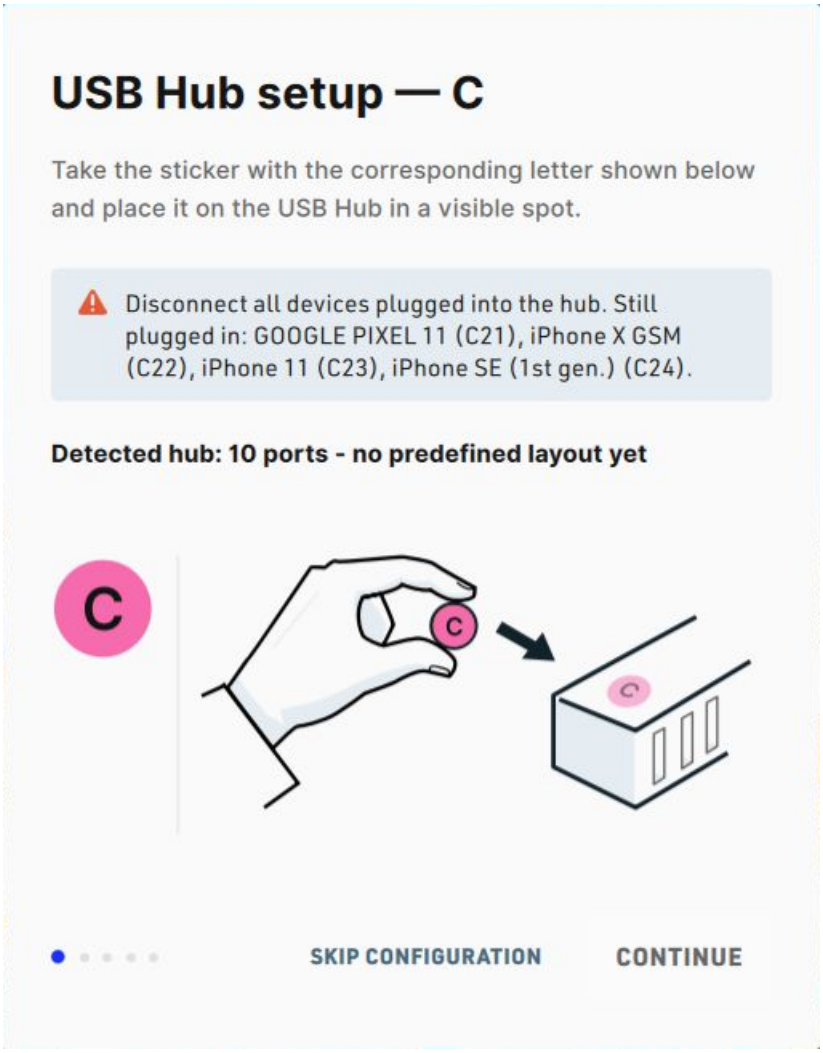
• **Is this hub A, moved to another USB port?** - see A hub moved to another USB port below.

• **Detected hub:** with the name of a hub Mobile knows - see Numbering a known hub in its printed order below.

• **Detected hub: 7 ports - no predefined layout yet** - Mobile does not know this hub, and you map its ports by hand. The number is how many ports Mobile found. If it is smaller


© 2026 Securaze GmbH

than the hub's, part of the hub did not start: check its power supply and cable before you go on.




**SKIP CONFIGURATION** closes the setup without a layout. Phones on this hub then get numbers in the order you plug them in, and Mobile asks again the next time it starts. To set the hub up sooner, use **SET UP AGAIN** in Managing hubs 195.

## Numbering a known hub in its printed order

Mobile knows some hubs and the order their ports are printed in, for example the Sipolar 20-port charging hub. For such a hub the setup shows **Detected hub:** with the hub's name, and two choices:

- **Number the ports in the order printed on the hub** - Mobile numbers the ports as printed on the hub. You do not have to plug a phone into each port. This choice is selected when only one known hub fits.
- **Map the ports myself** - you plug a phone into each port in turn, as described under Mapping the ports by hand below.


© 2026 Securaze GmbH

If more than one known hub fits, the setup shows **Detected hub - one of these** and lists them. Choose the one in front of you.

The printed order also works with phones still on the hub. The setup then says **The phones on this hub get the numbers printed on it when you continue.** The phones get their new numbers at once.

Click **CONTINUE**. Mobile goes straight to the last page and asks for one phone to check the order, for example **Plug a phone into the port printed USB1 to check the order.** Plug a phone into that port and read the answer:

• **The phone is on the hub's first port - the order fits.** Click **LOOKS GOOD**.

• **The phone is on port 4 of the predefined order, not the first - it does not fit this hub.** The hub looks like a known one, but its ports are in another order. Click **START OVER** and choose **Map the ports myself**.

• **That port is on hub B, not on this one.** Plug the phone into the hub you are setting up.

If the port printed first already has a phone, look at that phone's tile. If it shows the number printed next to the port, the order fits: click **LOOKS GOOD**.

## A hub with two USB cables

The Sipolar 20-port charging hub has two USB cables, so Mobile sees two 10-port hubs: the ports printed USB1 to USB10, and the ports printed USB11 to USB20. Each half gets its own letter and its own sticker, and you set up each half on its own.

Plug in the cable of the USB1-USB10 half first and set it up, then the cable of the USB11-USB20 half. If this is the station's first hub, its ports are then numbered 1 to 20, as printed.

If you set the halves up in the other order, the check with one phone notices it. When Mobile asks for a phone in USB1 and you plug it into the other half, it says that the port is on the other half of the box and asks for a phone in the first port of this half instead. If the USB1-USB10 half has the later letter, Mobile also says that the two halves swap letters with **LOOKS GOOD**, so USB1-USB10 comes first. Swap the two stickers too. The halves swap letters once no phone is on either half.

With two or more of these hubs on one station, Mobile cannot tell which halves belong together and does not swap them. Set up the halves in order.

## A hub moved to another USB port

Mobile recognizes a hub by the USB port of the PC it is plugged into. If you plug a hub into another USB port, Mobile first sees a new hub. If a hub that is no longer connected had a layout for the same kind of hub, the setup asks **Is this hub A, moved to another USB port?** If several hubs fit, choose the letter on the hub's sticker.

• **YES, IT IS HUB A** - the hub gets its letter, port numbers and port names back. Unplug all phones from it first.


© 2026 Securaze GmbH

• **NO, IT IS A NEW HUB** - the setup goes on for a new hub.

On Windows, adding or removing a USB card or a dock can renumber the PC's USB controllers. Mobile then moves the layouts of the hubs behind them by itself when it starts, and the hubs keep their letters.

## Mapping the ports by hand

Use this for a hub Mobile does not know, or when you chose **Map the ports myself**.

1. Unplug all phones from the hub. While a phone is plugged in, the first page says **Disconnect all devices plugged into the hub.** and lists what is still plugged in, and **CONTINUE** stays gray. Click **CONTINUE**.

2. **Managing cables**: plug the USB cables into the hub's ports, with no phones on them. Click **CONTINUE**.

3. **Managing cables**: attach the numbered tags to the free ends of the cables, in order (1, 2, 3 ...). Click **CONTINUE**.

4. **Connect devices in order**: plug a phone into each cable, one by one, in the order of the tags. Each phone gives its port the next number. The page shows how many ports are still open, for example **Ports left: 3. Plug a phone into each one, or click a port to deactivate it.**

• A port you do not use: click it and choose **Deactivate**. **Activate** takes it back.

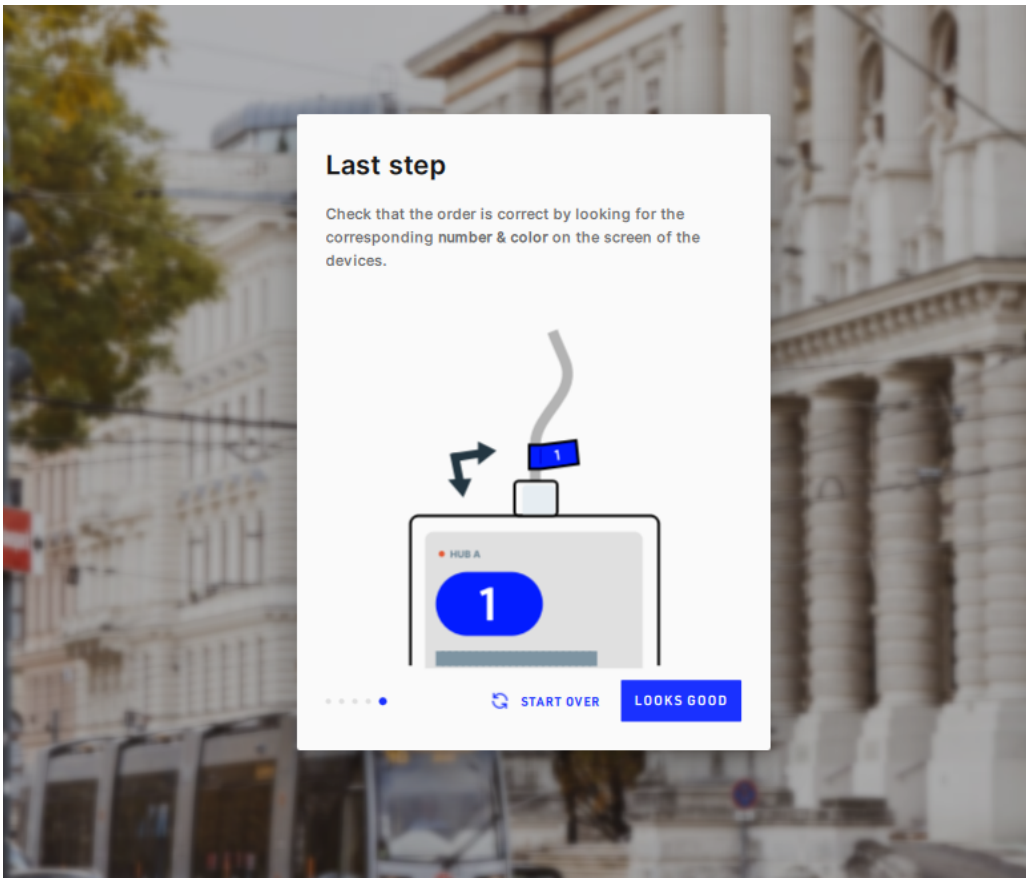
• A phone in the wrong port: unplug it, click the port and choose **Map again**. Then plug the phone into the right port - it takes the lowest free number.

• **CONTINUE** becomes available when every port is mapped or deactivated.

• **RESET PORTS** starts the mapping of this hub over. Before the first phone, this button is **CANCEL**: it closes the setup and leaves the hub without a layout.

5. **Last step**: check that each phone's screen shows the number and color of its cable's tag. Click **LOOKS GOOD**, or **START OVER** to map the hub again.


© 2026 Securaze GmbH




### 8.2.2.3 Managing hubs

Open **Options & Settings** > **General**. Under **Hubs**, click **MANAGE HUBS**. The list shows each hub of the station with its color, letter and name, the USB port it is on (or **Not connected**), how many ports it has and how many are mapped, and how it is numbered: **ports in the printed order**, **mapped by hand** or **no layout yet**.

Each hub has the buttons that fit it:

• **SET UP AGAIN** - for a connected hub: removes its layout and opens the setup for it (see Setting up a USB hub 191). The hub keeps its letter. **Remap Hub** in the menu you get by right-clicking an empty port of the hub does the same.

• **PRINTED ORDER** - for a connected hub Mobile knows that was mapped by hand: numbers its ports in the order printed on the hub. Confirm with **NUMBER IN PRINTED ORDER**. The hub keeps its letter, and phones on it get their new numbers at once.

• **FORGET** - for a hub that is no longer connected: removes its layout. Use it for a hub you no longer use. The other hubs keep their letters.

To start over with all hubs, unplug all phones and hubs, then click **RESET PORT LAYOUT** under **Reset EasyIDs. (Port layout)** in **Options & Settings** > **General**. Mobile removes all layouts and sets up each hub again as you plug it in.


© 2026 Securaze GmbH

### Giving a port a name of its own

If your bench has its own names for its slots, give a port a name such as Bay 3 / Slot 12. Labels and the Securaze Dashboard then show this name instead of the letter and number, and the empty port's tile shows it too.

1. Unplug the phone from the port. Only a mapped port can have a name.

2. Click the three dots in the top right corner of the empty port and choose **Name this port**.

3. Type the name, up to 32 characters, and click **SAVE**.

To go back to the letter and number, clear the name and click **SAVE**. The name stays with the physical port and is kept with the hub's layout.

### Port numbers without hub letter

Turn on **Port numbers without hub letter** in **Options & Settings** > **General** if labels and the Securaze Dashboard should show a port by its number only, for example 13 instead of B13. A port with a name of its own keeps its name.

### When a hub or port shows a warning

When a hub no longer matches its layout, Manage hubs shows a warning under it, and so does the first page of the hub's setup:

• **Hub A shows 8 of its 10 ports - check its power and cable.** Part of the hub did not start. Check its power supply and cable. The layout stays, and the missing ports work again when they come back.

• **Hub A has 10 ports, its layout 7** or **Hub A is not the hub its layout was made for** - click **SET UP AGAIN** for the hub.

An alert icon on an empty port's tile means phones do not come up there, for example because of not enough power, an overcurrent, or phones that dropped several times within seconds. Hover over the icon to read why, then check the cable and the hub's power supply.

### Where the layouts are kept

Mobile keeps each hub's layout in a file of its own, in the layout folder of its storage folder. The file usb.json in the installation folder is no longer used. Do not edit layouts by hand - use Manage hubs.

## 8.2.3 Device details

With **UI Card View** set to **Standard** (**Options & Settings**, tab **General**), click a tile to see the device details at the bottom of the screen. With **Detailed** tiles, the details are on the tile


© 2026 Securaze GmbH

itself.

The details show the device's data, for example **SECURAZE ID**, **MODEL NUMBER**, **SERIAL NUMBER**, **OS VERSION**, **IMEI**, **BATTERY HEALTH**, **EXTERNAL ID**, **INVENTORY NUMBER**, **SKU CODE** and **COLOR** - marked **set by hand** if you picked the color yourself.

For an iPhone, **BATTERY HEALTH** is the Maximum Capacity that the iPhone itself shows in its Settings under Battery - also on iOS 27.

The details of an iPhone also show **STORAGE CHIP**: the vendor and cell type of its storage, for example Hynix TLC. The same value goes to the Securaze Dashboard and the erasure report as the model of the storage.

For an Android phone, **VENDOR ACCOUNT** shows whether it is signed in to a Xiaomi, Huawei, Honor, vivo or OPPO account - for example Xiaomi signed in, None, or Not checked. A detailed tile shows the same as its **Vendor account** flag: **None signed in**, or for example **Xiaomi signed in - may lock the phone after the erasure**. See Data erasure 197.

The icon buttons in the details open the **GRADE SUMMARY**, where you set the grade under **Set grade** and add issues with **ADD ISSUE** - each issue shows the letter of the grade it results in - and the **REGISTRATION**, **ERASURE SUMMARY**, **DIAGNOSE SUMMARY** and **WORKFLOW** views.

For grading on the tile, the color, **All tiles** and **Grade on device**, see Enter Device details 77.

## 8.3 Data erasure

This chapter is the reference for the erasure of phones and tablets. To start an erasure, see Perform erasure 81. The erasure solutions - Data Clear, Smart Erasure and Advanced Erasure - and the **Erasure Settings** window are described in Erasure Methods 82.

### Before the erasure starts

When you click **ERASE SELECTED**, Securaze Mobile checks the selected devices. Where it needs your decision, it shows a window for each case, with the port numbers of the devices concerned. **Continue** (Enter) erases these devices, **Cancel** (Esc) leaves them out. The other selected devices are erased in either case.

• **FMiP ON** - Apple devices with Find My (FMiP) on. Find My stays on after the erasure, so the device stays locked to its Apple account, and the erasure takes about 10 minutes longer. To avoid that, turn off Find My on the device before the erasure.

• **GOOGLE FRP ON** - Samsung devices in Samsung Non-ADB mode with the Google reactivation lock (FRP) on. FRP stays on after the erasure. To remove it, erase the device with USB debugging on.

• **VENDOR ACCOUNT SIGNED IN** - Android phones signed in to a Xiaomi, Huawei, Honor, vivo or OPPO account. If the vendor's "Find device" is on, the phone stays locked to that


© 2026 Securaze GmbH

account after the erasure. Sign out of the account on the phone before the erasure. Securaze Mobile reads the accounts again when the erasure starts: if one is still signed in, the erasure report and the Securaze Dashboard record the phone as locked, as with Google FRP. An automatic erasure - started by the preset or after the diagnose - does not start on such a phone; its tile says, for example, **Not erased automatically: Xiaomi account signed in. Sign out on the phone, then start the erasure.**

• **MDM ON** - devices under company management (MDM). They cannot be used after the erasure.

• **External ID missing** - devices without an external ID, when your Securaze Dashboard asks for one. See External Systems 34.

• **Erase SD cards** - devices with an SD card inserted. **Continue** erases them with their SD cards, **Don't erase** leaves these devices out.

• **Wipe Only Devices** - devices that cannot get Smart Erasure or Advanced Erasure, for example Samsung devices in Samsung Non-ADB mode and Macs (see Erase a Mac 86). **Continue** wipes them with the Data Clear solution (the window calls it Data Wipe).

**Don't show again** in **FMiP ON** and **MDM ON** skips that window until Securaze Mobile is closed; your last answer then applies.

### iOS and Android

What the device needs, what happens during the erasure and what to do when something goes wrong:

• iOS 198 - Requirements 199, Erasure process 200, Problem solutions 201

• Android 203 - Requirements 203, Developer mode and USB debugging 204, Install via USB 205, Erasure process 205, Problem solutions 206

• macOS only: Macs - Erase a Mac 86

Which iOS and Android versions are supported: see Supported Device OS 24.

## 8.3.1 iOS

This section covers the erasure of iPhones and iPads, and of Macs with Apple silicon:

• Requirements 199 - what the device and the station need.

• Erasure process 200 - what happens during the erasure.

• Problem solutions 201 - messages on the tile and what to do.

To connect an iOS device, see Connect iOS Device 58. To start the erasure, see Erase iOS device 85.

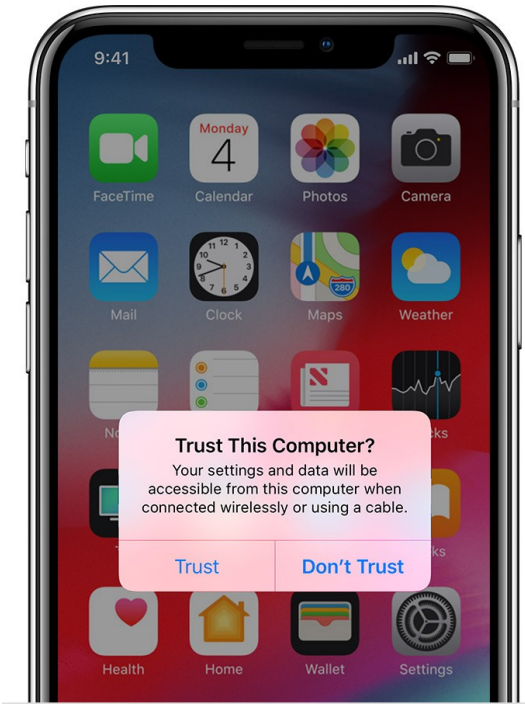

© 2026 Securaze GmbH

#### 8.3.1.1 Requirements

### The device

• Connect the device to the station with a USB cable that carries data, directly or through a USB hub.

• If the device has been set up, unlock it and confirm **Trust This Computer?** with **Trust**; enter the device passcode if it asks. Until then the tile shows **Trust this PC - on device screen**.




Trust This Computer (Source Apple Inc.)

• Find My (FMiP) and MDM: Securaze Mobile reads both. A device with Find My on can be erased, but it stays locked to its Apple account. A device under MDM cannot be used after the erasure. Turn off Find My on the device before the erasure. See the warnings in Data erasure 197.

• macOS only: Macs are erased on macOS stations, in DFU mode and with Data Clear only - see Erase a Mac 86.

• Supported iOS versions: see Supported Device OS 24.

### The Securaze app and Wi-Fi

For Advanced Erasure and for the diagnose, Securaze Mobile installs the Securaze app on the device by itself and connects the device to Wi-Fi. For this, the Mobile preset in the


© 2026 Securaze GmbH

Securaze Dashboard needs a Wi-Fi network (see Set presets 44). If there are several, **Preferred Wifi** in **Options & Settings** > **Processing** picks one.

Without a Wi-Fi network in the preset, Securaze Mobile warns at login (**Wi-Fi Preset Missing**), and Advanced Erasure overwrites the device directly, which is slower. See Erase iOS device 85.

Data Clear and Smart Erasure need neither the app nor Wi-Fi on the device.

### The station

• An internet connection - for the Securaze server and to download iOS firmware. Firmware is needed, for example, for a device with Find My on, for a device in recovery mode and when **Update iOS Devices to latest version** is on. The station also needs enough free disk space for the firmware.

• Windows only: the Apple driver that the Securaze Mobile installer brings. If Windows uses Microsoft's driver instead, Securaze Mobile warns - see Microsoft Apple Driver 67.

• macOS only: Apple Configurator, free from the Mac App Store. Securaze Mobile needs it to erase a device in DFU mode. If it is missing, Securaze Mobile shows **Apple Configurator required** when it starts; **OK** opens Apple Configurator in the Mac App Store.

• macOS only: **Allow accessories to connect** set to **Automatically allow when unlocked** - see Connect iOS Device 58.

## 8.3.1.2 Erasure process

Select the device and click **ERASE SELECTED** - see Perform erasure 81. What Securaze Mobile then does depends on the erasure solution:

• **Data Clear** - resets the device to factory settings and checks that the data is gone.

• **Smart Erasure** - checks a device that is already empty, still on its setup (hello) screen and not diagnosed last, and certifies it; any other device gets a Data Clear.

• **Advanced Erasure** - resets the device, overwrites its storage, resets it again and checks the result.

The details are in Erase iOS device 85 and Erasure Methods 82. With **Update iOS Devices to latest version** in **Erasure Settings**, the device also gets the latest iOS, which takes about 10 minutes more.

The tile shows the progress. After a successful erasure the device is switched off if **iOS device shutdown behavior** is set to **Automatic Shutdown** (**Options & Settings** > **Processing**). A device that still needs a grade stays on, and on a station that runs workflows the workflow decides.

Messages during the erasure: see Problem solutions 201.


© 2026 Securaze GmbH

### 8.3.1.3 Problem solutions

These messages can appear on the tile of an iOS device, and this is what to do. If a problem stays, send a system report from Help 171 and contact support.

| Problem | What to do |
|---|---|
| The device does not appear on its tile. | Unplug it and plug it in again, or try another cable or port. Restart the device.<br>Windows only: open **Help** (Ctrl+H) and click **Re-detect iPhones and iPads** (Ctrl+I). If the filter **Microsoft Driver** appears, see Microsoft Apple Driver 67. |
| **Trust this PC**<br>**Device unauthorized: Please press trust on the device.**<br>**Device cannot be paired. Please click on the 'Trust' button on your device!** | Unlock the device, tap **Trust** and enter the passcode if it asks. If **Don't Trust** was tapped, unplug the device and plug it in again to get the question again. |
| **Device is locked** | Unlock the device. Until then Securaze Mobile reads only part of its details. |
| **Failed to activate**<br>**Device activation failed** with a reason | Do what the reason says - for example remove the SIM card, insert a SIM card, or finish the setup assistant on the device. Then click **Retry** on the tile. |
| **Could not read the device**<br>**Replug and/or reboot device** | Click the refresh icon on the tile, or unplug the device and plug it in again. Restart it if needed. If a reason is shown instead, for example no licenses left, resolve it and plug the device in again. |
| **Failed to connect** | The connection to the Securaze server failed for this device. Click **Retry** on the tile, or **Retry All** in the sidebar for all such devices. If a reason is shown instead, resolve it first. |
| **Device storage full: Please factory reset device manually and retry.** | Reset the device to factory settings on the device itself, then plug it in again. |


© 2026 Securaze GmbH

| Problem | What to do |
|---|---|
| **FMiP detected**<br>**MDM detected** | Find My stays on after the erasure; turn it off on the device first. A device under MDM cannot be used after the erasure. See Data erasure 197. |
| **Verification data found after erasure.**<br>**Device didn't start factory reset within given time. Device may be faulty.** | Start the erasure again. If it fails again, reset the device by hand and erase it again. If that fails too, the storage of the device may be defective. |
| **Apple firmware prohibits automatic factory reset [manual factory reset required]** | Reset the device to factory settings on the device itself, then erase it again. |
| **iOS Firmware Download failed - please restart erasure.**<br>No firmware, not enough disk space, model not supported yet<br>**The firmware could not be downloaded** with a reason | Start the erasure again. Check the station's internet connection and free disk space. The station also lists these problems under Infrastructure issues 73 with what to do.<br>The reason in brackets says why the download failed, for example the server's answer or a download that stalled. |
| **Replug device - to continue its erasure** | The device was unplugged while its erasure waited for the firmware download. Plug it in again; the erasure goes on. |
| **RECOVERY MODE**<br>**DFU MODE**<br>on the tile instead of **READY** | The device is in recovery mode or in DFU mode. Every erasure solution then restores its firmware at once, which erases the device - Advanced Erasure without the overwrite by the app. The station needs the firmware for it (see Upload iOS Firmware 162).<br>macOS only: to restart a device in recovery mode normally, right-click its tile and choose **Leave Recovery Mode** - see Connect iOS Device 58. For devices in DFU mode, see Erase iOS device 85. |


© 2026 Securaze GmbH

| Problem | What to do |
|---|---|
| **Apple device support outdated**<br>in Infrastructure issues 73 | macOS only: the station's Apple device support is too old to restore a Mac. Apple's updater opens by itself; **Install now** in the issue opens it again. Install the update - it asks for the station's password - or update macOS, then start the erasure again. See Erase a Mac 86. |
| The Securaze app cannot be installed, or the tile shows the snail icon. | Advanced Erasure then overwrites the device directly, which is slower. The tooltip of the snail icon says why - see Erase iOS device 85. Repeated install problems are listed under Infrastructure issues 73; contact support. |

## 8.3.2 Android

This section covers the erasure of Android phones and tablets:

- Requirements 203 - what the device needs.
- Developer mode and USB debugging 204 - how to turn on USB debugging by hand.
- Install via USB 205 - devices that block installing the Securaze app.
- Erasure process 205 - what happens during the erasure.
- Problem solutions 206 - messages on the tile and what to do.

To connect an Android device, see Connect Android device 60. To start the erasure, see Erase Android device 86.

### 8.3.2.1 Requirements

#### The device

- Android 5.0 or later - see Supported Device OS 24.
- Connect it to the station with a USB cable that carries data, directly or through a USB hub.
- If the tile says **Unlocking screen [manual interaction required]**, unlock the device.

#### Connection

Securaze Mobile must be able to talk to the device. How depends on the device - see Connect Android device 60:

- Android 16 and later on the setup screen: nothing to do while **Android Express Mode** is on (the default).


© 2026 Securaze GmbH

• All other devices: USB debugging - with the QR code (Android USB-Debugging bypass with QR-Code 60) or by hand (Developer mode and USB debugging 204). When the device asks **Allow USB debugging?**, tap **Allow**.

• Samsung devices can also be erased without USB debugging, with **Samsung Non-ADB communication** - then with Data Clear only and without the FRP check.

## The Securaze app

Securaze Mobile installs the Securaze app on the device over USB by itself, or updates it, and works through it - to read the device, for the diagnose and for the erasure. Some devices, for example from Xiaomi, block installing over USB - see Install via USB 205.

The device needs no internet connection for the erasure. Only the QR code method needs Wi-Fi, to download the app.

## Google account (FRP)

Securaze Mobile shows whether the Google reactivation lock (FRP) is on. To remove FRP with the erasure, the device needs USB debugging. In Samsung Non-ADB mode FRP can neither be checked nor removed - see **GOOGLE FRP ON** in Data erasure 197.

### 8.3.2.1.1 Developer mode and USB debugging

Most Android devices need USB debugging so that Securaze Mobile can talk to them. Two ways need no settings on the device: **Android Express Mode** for Android 16 and later on the setup screen, and the QR code, which turns on USB debugging by itself. See Connect Android device 60 and Android USB-Debugging bypass with QR-Code 60.

## Turn on USB debugging by hand

1. On the device, open **Settings** > **About phone**. On some devices it is under **System**; on Samsung devices tap **Software information** as well.

2. Tap **Build number** seven times. The device says that developer mode is on.

3. Go back. **Developer options** are now in **Settings**, on some devices under **System**.

4. Open **Developer options**, check that they are on, and turn on **USB debugging**.

5. Connect the device to the station. When it asks **Allow USB debugging?**, tick **Always allow from this computer** and tap **Allow**.

Securaze Mobile then reads the device. As long as the tile shows **Turn ON and ALLOW USB debugging**, USB debugging is off or not allowed yet.

The names of the menus differ between manufacturers. Some devices have additional settings that must be on as well, for example **Install via USB** - see Install via USB 205.

Problems: see Problem solutions 206.


© 2026 Securaze GmbH

#### 8.3.2.1.2 Install via USB

Securaze Mobile installs its app on Android devices over USB. Some devices block that unless a setting is on - often Xiaomi, but also vivo, OPPO, realme and Honor.

### Install the app on the device

When a device refuses, Securaze Mobile first tries the device's own installer. If that is refused too, it copies the app to the device, and the tile shows **Install Securaze Mobile on phone first!** - **Files app → install APK.** Then:

1. Open the file manager (Files app) on the device.
2. Open the **Securaze** folder and tap the APK file.
3. Confirm the installation on the device.

Securaze Mobile checks every few seconds and goes on by itself as soon as the app is installed. It waits up to 10 minutes.

### Let Securaze Mobile install the app

To avoid the manual step, turn on the setting in the developer options before you connect the device:

1. Open **Developer options** - see Developer mode and USB debugging 204.
2. Turn on **Install via USB**. On Xiaomi devices, also turn on **USB debugging (Security settings)**; the device may ask for a SIM card and a Xiaomi account sign-in first.

The names of these settings differ between manufacturers.

#### 8.3.2.2 Erasure process

Select the device and click **ERASE SELECTED** - see Perform erasure 81. What Securaze Mobile then does depends on the erasure solution:

- **Data Clear** - resets the device to factory settings.
- **Smart Erasure** - an encrypted device gets a Data Clear; a device that is not encrypted, or whose last run was a diagnose, gets the full Advanced Erasure.
- **Advanced Erasure** - clears the content of the device, overwrites its storage with the Securaze app and resets it to factory settings.

The details are in Erase Android device 86 and Erasure Methods 82.

### What you may have to do

- If Securaze Mobile cannot clear the content, it resets the device first and waits for it: go through the setup screen, turn on USB debugging again and allow it.
- Some devices ask on their screen to activate the device admin for the Securaze app and then to confirm a **Control device** screen. The tile then shows **Activate device admin** -


© 2026 Securaze GmbH

**Then confirm erasure**, or **Please confirm device warnings.** Confirm both on the device; the erasure goes on.

• If the tile asks you to unlock the screen, unlock the device.

### The end of the erasure

At the end, Securaze Mobile resets the phone to factory settings. The tile shows **Wipe running on the phone** once the phone has started its wipe, and **Waiting for factory reset to finish** while Securaze Mobile waits for the reset.

With **Wait for restart** off in **Options & Settings** > **Processing** (the default), the erasure ends once the phone has started its wipe, and you can unplug the phone right away. With **Wait for restart** on, the erasure ends only when the phone is back after its reset.

Messages during the erasure: see Problem solutions 206.

## 8.3.2.3 Problem solutions

These messages can appear on the tile of an Android device, and this is what to do. If a problem stays, send a system report from Help 171 and contact support. Problems of the station itself are listed under Infrastructure issues 73.

| Problem | What to do |
|---|---|
| Developer options are not shown. | Tap **Build number** seven times. Some manufacturers put it elsewhere, for example under **Software information**. See Developer mode and USB debugging 204. |
| **Turn ON and ALLOW USB debugging**<br>**Allow USB debugging?** does not appear on the device | Unplug the device and plug it in again. Switch **USB debugging** off and on again while the device is connected. Set the USB mode of the device to file transfer.<br>A device on its setup screen can use the QR code instead (Android USB-Debugging bypass with QR-Code 60), Android 16 and later also **Android Express Mode**. |
| **Device unauthorized: Please press 'Allow USB debugging' the device.** | Tap **Allow** on the device. Tick **Always allow from this computer** so it does not ask again. |
| **Install Securaze Mobile on phone first!** | Install the app from the Securaze folder in the file manager. See Install via USB 205. |
| **Securaze App could not be installed. Please check device debug settings.** | Check that USB debugging and, where the device has it, **Install via USB** are on. Unplug the device and plug it in again. |


© 2026 Securaze GmbH

| Problem | What to do |
|---|---|
| **Securaze App could not be installed** - too old API version, or the app does not match the CPU (ABI) | The device cannot be processed with this version of Securaze Mobile. See Supported Device OS 24 and contact support. |
| **Unlocking screen [manual interaction required]** | Unlock the device. Securaze Mobile then goes on by itself. |
| **Could not read the device**<br>**Replug and/or reboot device**<br>**Auto Blocker is on** | Click the refresh icon on the tile, or unplug the device and plug it in again. Restart it if needed. If a reason is shown instead, for example no licenses left, resolve it and plug the device in again.<br>**Auto Blocker is on**: Samsung's Auto Blocker blocks commands over USB. Turn it off on the phone (Settings > Security and privacy > Auto Blocker) or switch on USB debugging, then click the refresh icon on the tile. |
| **Failed to connect** | Click **Retry** on the tile, or **Retry All** in the sidebar for all such devices. If a reason is shown instead, resolve it first. |
| **Activate device admin - Then confirm erasure**<br>**Please confirm device warnings.** | Confirm the dialogs on the device: activate the device admin for the Securaze app and confirm the **Control device** screen. The erasure then goes on. |
| **Factory reset failed**<br>**Factory reset did not complete** | Start the erasure again. If it fails again, reset the device by hand and erase it again. If that fails too, the storage of the device may be defective. |
| A Samsung device with USB debugging does not appear. | **Samsung Non-ADB communication** is on: in this mode devices with USB debugging are not shown. Switch it off in **Options & Settings** > **Processing**. |
| **FRP detected**<br>**GOOGLE FRP ON** | Erase the device with USB debugging on to remove FRP. In Samsung Non-ADB mode FRP is neither checked nor removed. See Data erasure 197. |


© 2026 Securaze GmbH

# Cheatsheet

# 9 Cheatsheet

Most buttons in Securaze Mobile show their key on the button. The keys below work on Windows, macOS and Linux; a key that works on some of them only says so. Enter means both Enter keys - on the main keyboard and on the keypad.

macOS only: Ctrl is the Control key, as the buttons show - not Cmd. Only Ctrl+click on a filter in the footer is Cmd+click on a Mac.

## On every screen (sidebar)

• Ctrl+H - **Help** (the **Help & Support** dialog)

• F9 - **General settings**

## Dashboard (sidebar)

• Ctrl+A - **All devices**: selects all devices shown. Press it again to clear the selection.

• Ctrl+P - **Print labels**: for the selected phones, or for all shown phones when none is selected

• Ctrl+N - **Add devices manually** (Manual Entry)

• Ctrl+Shift+L - **Change lot**

• Ctrl+Shift+W - **Change workflow**: the workflow for the phones you plug in next. Only on stations where the operator chooses the workflow.

• Ctrl+Shift+G - **All tiles**: shows every tile on its **Grading** tab. Press it again to show each tile on its own. Only with detailed tiles (Ctrl+Shift+V).

• Ctrl+Shift+V - the card view button in the header: switches the tiles between **STANDARD** and **DETAILED**

• Shift+click on a filter in the footer - adds the filter: phones that match any of the chosen filters are shown.

• Ctrl+click on a filter in the footer - phones that match all chosen filters are shown.

## Grading

• Enter - **ADD ISSUE** on the **Grading** tab of the tile you picked: opens the typical problems list.

In the typical problems list:

• Type - searches by issue code or description

• Up / Down - moves through the list

• Enter - ticks the highlighted issue

• Ctrl+Enter - **Confirm**


© 2026 Securaze GmbH

In a workflow's grading step on the tile:

• Enter - **ADD ISSUE**

• Ctrl+R - removes the last issue

• Ctrl+Enter - **CONFIRM**

## Add devices manually (Manual Entry)

• Enter - **Add device** (not while a list of typical problems, brands or models is open)

• Ctrl+G - **Generate**: makes a serial number for a device without a readable one

• Tab / Shift+Tab - next / previous field

• Arrow keys - change the choice in a row of choices, such as **Capacity** or **Color**. Space or Del clears it.

• Ctrl+Shift+L - **Change** the lot

## Print labels

• S - **Selected phones**, A - **All shown phones** (offered only when phones are selected)

• Enter - **Start printing**

• Esc - **Close**

• 1 to 9 - picks a printer in the open **Preferred Printer** list (General settings - Printer)

## Starting an erasure or a diagnosis

• Warnings before an erasure, such as **FMiP ON**: Enter - **Continue**, Esc - **Cancel**

• **Erasure Settings**: Enter - **Start erasure**

• **Diagnose Settings**: Space - ticks or clears the highlighted test

• **Custom Test** (**CUSTOMIZE** in **Diagnose Settings**): Alt+S - opens the search

## Lot selection

• Up / Down - moves the selection, Enter - confirms it

• 1 to 9 - chooses one of the first nine lots in the list

• Left / Right - previous / next page

• Ctrl+A - number of lots per page (10, 20 or 50)

• F5 - refreshes the list

• Esc - **Keep** the lot in use (when you change the lot)

## Workflow selection

• Up / Down - moves the selection, Enter - chooses the workflow


© 2026 Securaze GmbH

• 1 to 9 - chooses one of the first nine workflows

• Esc - continues without a workflow, or keeps the workflow in use when you change it

## Hub setup

• Enter - **Continue** (**Looks good** on the last page), when the button can be used

• Esc - **Skip configuration** or **Cancel**. Esc never resets the ports or starts over.

## Help dialog

• Ctrl+H - **support** (Knowledge Base)

• Ctrl+D - **Dashboard**

• Ctrl+S - **Send system report**; in that dialog Ctrl+Enter sends the report, Esc closes it

• Ctrl+Shift+R - **Start remote session**

• Windows only: Ctrl+I - **Re-detect iPhones and iPads**

• Ctrl+T - **Support Access** (Securaze support staff only)

• Alt+R - **Retry** when a system report could not be sent

## Device screen window

• Alt+Left - Back on the phone, Alt+Home - Home on the phone, in the **Show device screen** window (only for phones that accept input)

## Import workflows (General settings - Workflows)

Linux only: these keys work in Mobile's own file browser, where you pick the workflows.

• Up / Down - moves the selection, Enter - opens the folder or ticks the workflow

• Space - ticks the workflow, Ctrl+A - ticks all

• Ctrl+Enter - **Import** the ticked workflows

• Backspace - back, F5 - refresh, Esc - back or close

## Login and exit

• Enter in the user name or password field - **LOG-IN**

• Exit dialog (your user name in the sidebar - **Exit**): Ctrl+R - **Reboot**, Ctrl+S - **Shut-down**

• Windows and macOS: Enter in the exit dialog - **Exit**

• Linux only: Enter in the exit dialog - **Logout**

## Wi-Fi

Linux only: click the connection status in the sidebar to open the Wi-Fi list.


© 2026 Securaze GmbH

- Alt+N - adds a hidden network (SSID)
- Alt+A - advanced Wi-Fi configuration
- Enter - **Connect** after the password, Esc - **Back** or **Close**


© 2026 Securaze GmbH

# Securaze Dashboard

# 10 Securaze Dashboard

After logging in to Securaze Dashboard you will be taken to the overview

The following tabs are available in the dashboard

1. Dashboard 282 - shows an overview of deleted devices in the last 24 hours.

2. Logistic - Orders - shows a list of all orders

3. Logistic - Lot - shows a list of all Lots on which the assets where transported to the company

4. Logistic - Sale Lot - shows a list of all Sale Lots with the status of the erasure.

5. Settings - individual settings for Securaze can be made here

6. Download - here you can create a USB stick from which PCs/notebooks can be deleted using Securaze Work.

7. Print queue - shows current and past print jobs

8. Erasure Reports - shows the erasure reports and allows you to download them (see chapter Erasure Reports)

9. Customers - Customer settings and information

10. User - shows a list of all users

11. Licenses - opens license settings (admin users only)

12. Logout - Logging off from Securaze Dashboard


© 2026 Securaze GmbH

**Search bar:**

In the upper area there is the possibility of a simple and efficient search, which searches in all categories and subcategories. You can search for a device model, a Pickup Order, pallet or even a serial number.

The search is also an ideal tool if only parts of the searched information are available.




Simple search:

Enter a word into the input field and press "Enter" to start the search.

Advanced search:

If you do not get any results with the simple search, use the wildcards to search for items: *your word or phrase*

Search by date:

To search for a specific date, use wildcard and the following format: *2021-12-31*;

Multiple search:

To search for several parameters simultaneously, use separator " ; " e.g. => my_word; my_word2; *my_word3*.

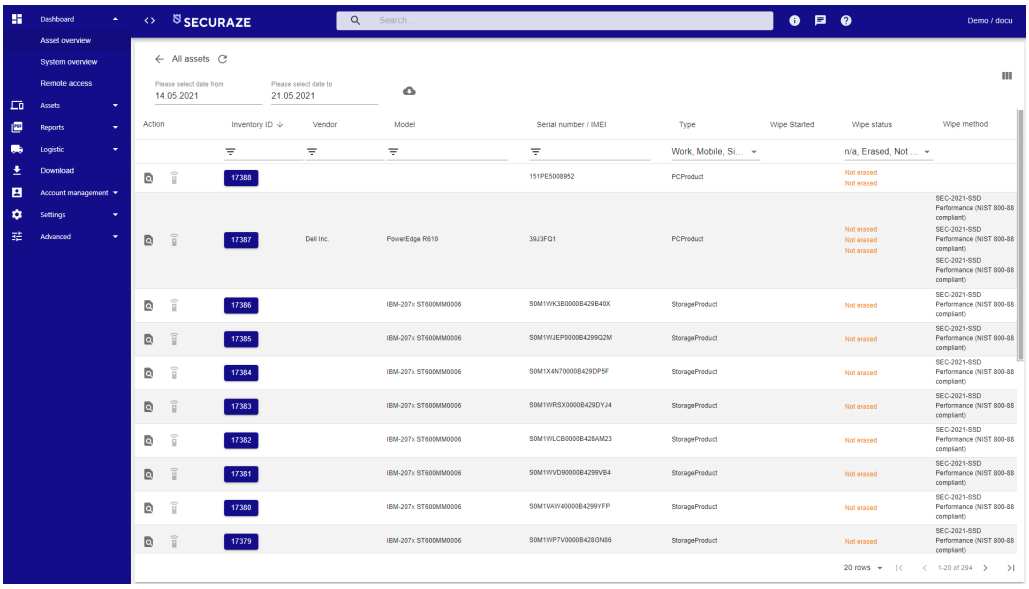
## 10.1 Menu items

### 10.1.1 Dashboard

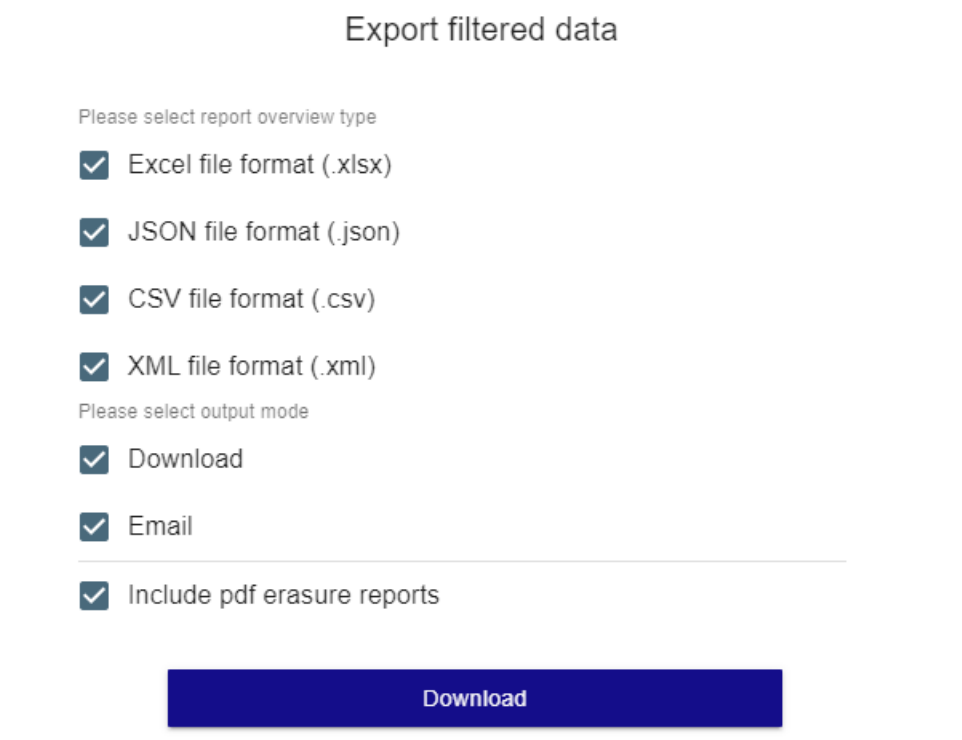
#### 10.1.1.1 Asset overview

In the Asset Overview menu you can see an overview of all assets and select them by date.


© 2026 Securaze GmbH




By clicking on **export filtered data,** you can select the format in which you want to download the erasure report or receive it as an e-mail.






In the area on the right you will see the **show columns** option.


© 2026 Securaze GmbH

Here you can select the columns to be displayed by placing the check mark next to the corresponding column heading.

Confirm your entry by clicking SAVE.

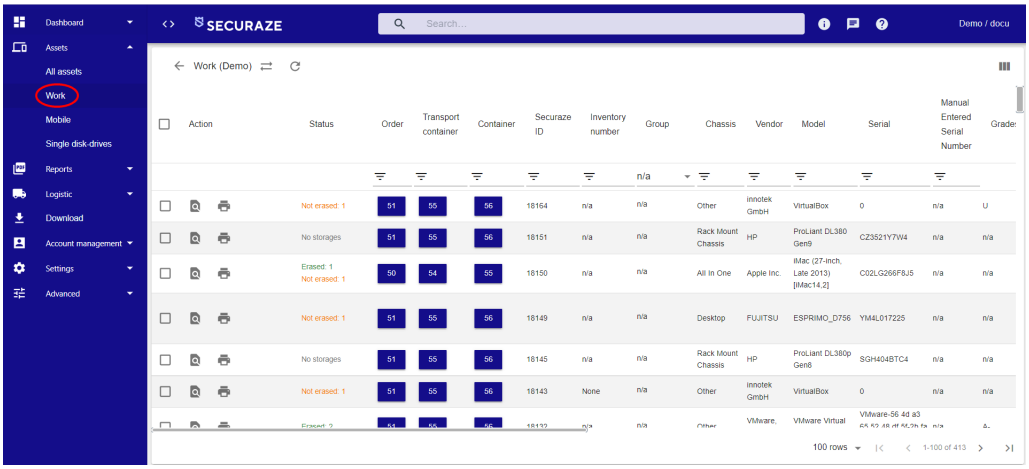
## 10.1.2 Assets

In the **Assets** menu you can see all devices, divided into Work, Mobile and Single disk-drives.

In addition to Work, Mobile and Single disk-drives, the Assets menu also contains the Watch and Headphone categories for processed Apple Watch and audio devices (e.g. AirPods). They offer the same functions as the Mobile list.

### 10.1.2.1 Work

In the **Assets - Work** menu you can see an overview of all Work devices.






In the area on the right you will see the **show columns** option.

Here you can select the columns to be displayed by placing the check mark next to the corresponding column heading.

Confirm your entry by clicking SAVE.

To select all devices, check the **Action** box.

To generate an erasure report for all devices, click on  **Download erasure report.**

In the middle of the page you can see the Work devices with the related information. Here you have the following options:


© 2026 Securaze GmbH



**Product details**

To open the Product details in a new tab, hold down the control button while clicking on it with your mouse. To open the Product details in a new window hold down the shift button while clicking on it with your mouse.

You can also select the desired option by right-clicking on Product details.



**Print label**

### Drive health

In the Product details, the **Storages** tab lists every drive of the device with its **SMART Overall** state and its **Health** - the SMART score from 0 to 100.

Securaze Work records further values per drive. Open a drive with **Edit storage** and go to **Advanced info**:

• **Life remaining percent** - the remaining life of an SSD or NVMe drive

• **Helium level percent** - the helium level of a helium-filled hard disk; a low value means the drive is near the end of its life

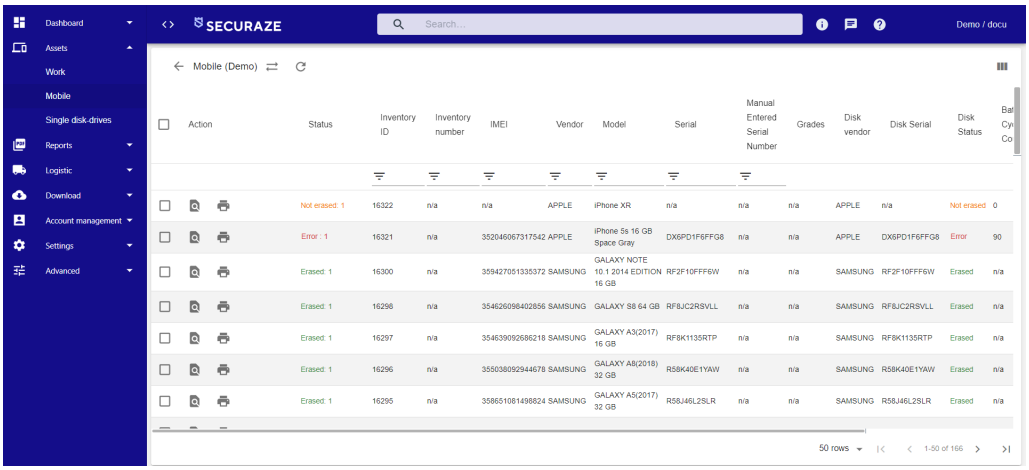
• **Grown defect list count** and **Primary defect list count** - the defects a SAS drive found during use, and the ones it had from the factory

The same values are printed on the erasure certificate, appear as columns in the Excel export of a collection, and can be mapped in the export to an external system (ERP). A drive that does not report a value shows N/A on the certificate.

## 10.1.2.2 Mobile

In the **Assets - Mobile** menu you can see an overview of all Mobile devices.


© 2026 Securaze GmbH




In the area on the right you will see the **show columns** option.

Here you can select the columns to be displayed by placing the check mark next to the corresponding column heading.

Confirm your entry by clicking SAVE.

To select all devices, check the **Action** box.

To generate an erasure report for all devices, click on **Download erasure report.**

In the middle of the page you can see the Mobile devices with the related information. Here you have the following options:

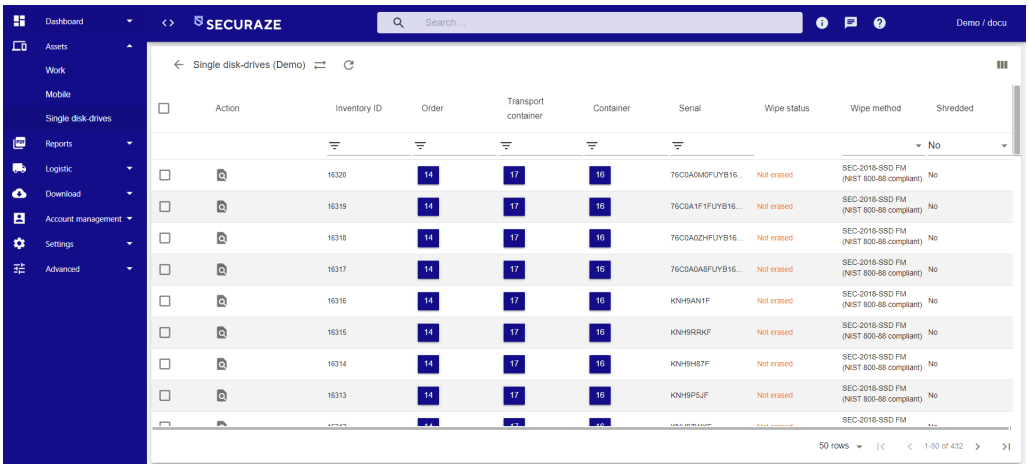
**Product details**

**Print label**

### 10.1.2.3 Single disk-drives

In the **Assets - Single disk-drives** menu you can see an overview of all Single disk-drives devices.


© 2026 Securaze GmbH




In the area on the right you will see the **show columns** option.

Here you can select the columns to be displayed by placing the check mark next to the corresponding column heading.

Confirm your entry by clicking SAVE.

To select all devices, check the **Action** box.

To generate a deletion report for all devices, click on **Download erasure report.**

In the middle of the page you can see the Workp devices with the related information. Here you have the following options:

**Product details**

## Drive health

In the Product details, the **Storages** tab lists every drive of the device with its **SMART Overall** state and its **Health** - the SMART score from 0 to 100.

Securaze Work records further values per drive. Open a drive with **Edit storage** and go to **Advanced info**:

• **Life remaining percent** - the remaining life of an SSD or NVMe drive

• **Helium level percent** - the helium level of a helium-filled hard disk; a low value means the drive is near the end of its life


© 2026 Securaze GmbH

• **Grown defect list count** and **Primary defect list count** - the defects a SAS drive found during use, and the ones it had from the factory

The same values are printed on the erasure certificate, appear as columns in the Excel export of a collection, and can be mapped in the export to an external system (ERP). A drive that does not report a value shows N/A on the certificate.

#### 10.1.2.4 Watch & Headphones

The Watch and Headphone pages list all processed Apple Watch and audio devices (e.g. AirPods) with their related information, analogous to the Mobile devices list.

The following options are available:

• Action box - select all devices for bulk operations

• Download erasure report

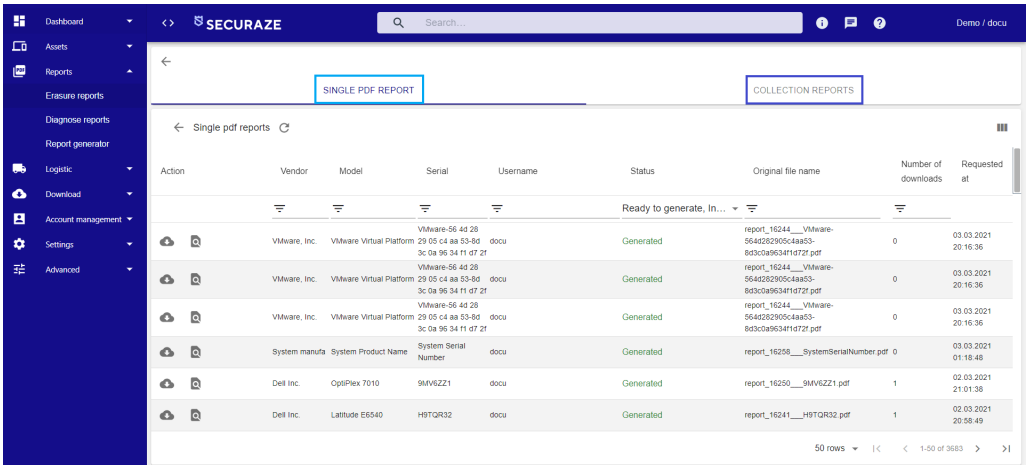
• Product details - open the details of a device

• Print label

Columns can be shown, hidden and saved as in every list.

### 10.1.3 Reports

In the menu **Reports - Erasure reports** you can find the erasure report for one asset (Tab **SINGLE PDF REPORT**) or for all assets of one Sale Lot, one Lot or one whole order (Tab **COLLECTION REPORTS**).

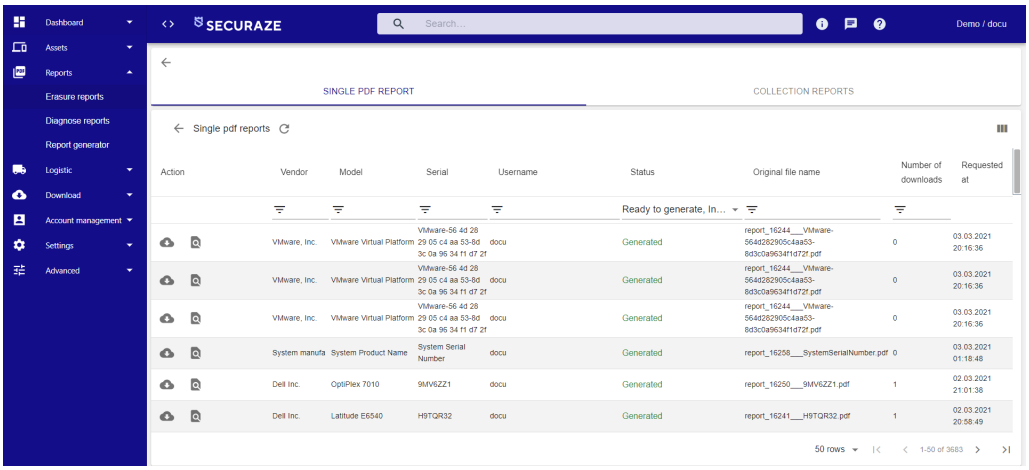



Download an erasure report:

**One asset:**

To download an erasure report of one asset, click on **Reports - Erasure reports** in the Menu section.


© 2026 Securaze GmbH

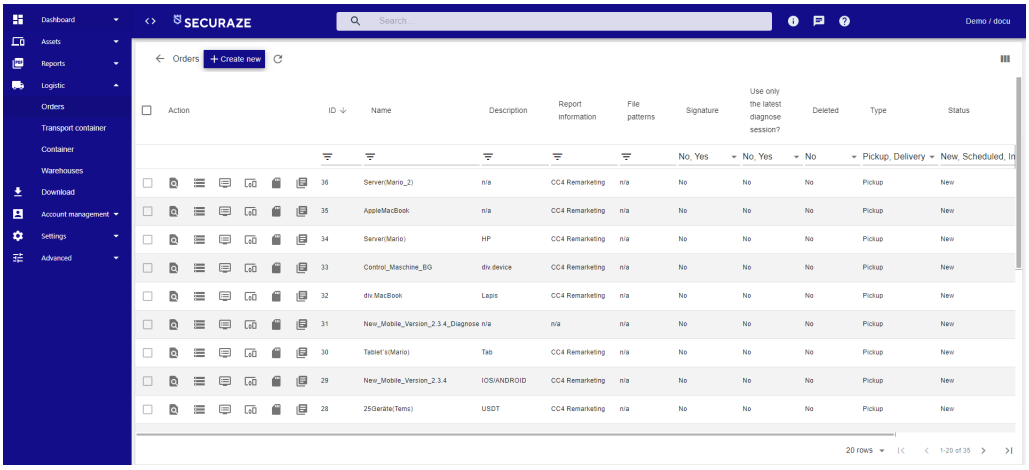



Select the desired report and click Download report(s). The report is downloaded in pdf format.

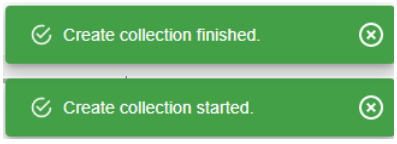
**Order:**

To download an erasure report for all assets of one Order, click on **Logistic - Orders** in the Menu section.

Select the desired Order and click on **Create Collection.**




The erasure report will be generated.




A ZIP file is downloaded containing the reports as a PDF file and a listing of assets as an XLS file. The erasure reports are displayed on **Reports - Erasure reports** in the Menu section.

In the menu **Reports - Erasure reports** you can download the reports again any time by clicking on Download report(s).


© 2026 Securaze GmbH

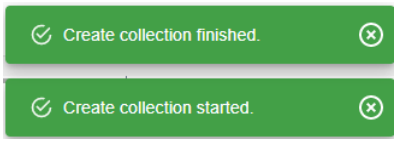
**Lot:**

To download an erasure report of all assets of one Lot, click on **Logistic - Lot** in the Menu section.

Select the desired Order and click on **Create Collection.**



The erasure report will be generated.




A ZIP file is downloaded containing the reports as a PDF file and a listing of assets as an XLS file. The erasure reports are displayed on **Reports - Erasure reports** in the Menu section.

In the menu **Reports - Erasure reports** you can download the reports again any time by clicking on Download report(s).

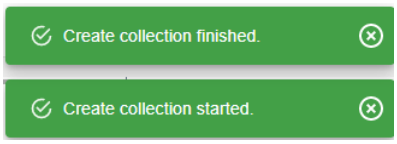
**Sale Lot:**

To download an erasure report of all assets of one Sale Lot, click on **Logistic - Sale Lot** in the Menu section.

Select the desired Order and click on **Create Collection.**



The erasure report will be generated.




A ZIP file is downloaded containing the reports as a PDF file and a listing of assets as an XLS file. The erasure reports are displayed on **Reports - Erasure reports** in the Menu section.

In the menu **Reports - Erasure reports** you can download the reports again any time by clicking on Download report(s).

The erasure report contains all the information about the erased device and the date and time of the erasure.


© 2026 Securaze GmbH

Besides erasure reports, the Reports menu also provides Diagnose reports, Verification reports and User reports. They are accessed the same way and can also be downloaded individually or as collections.

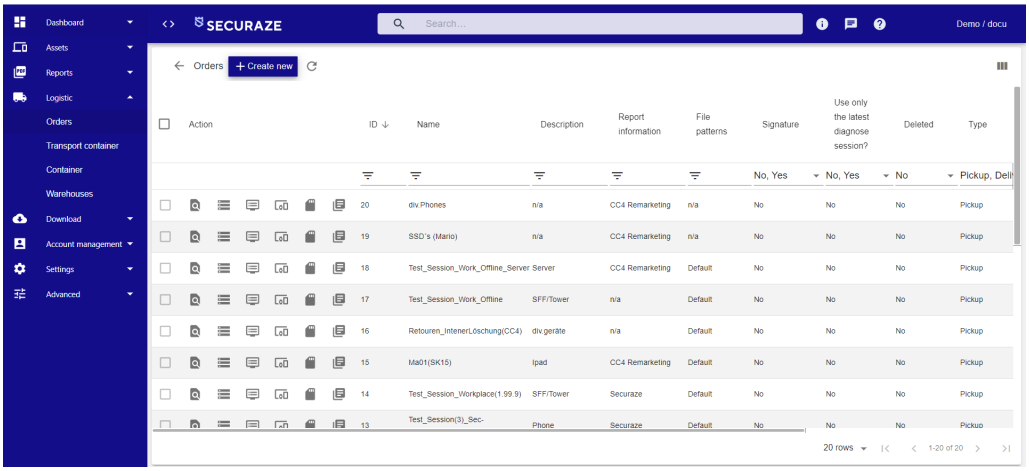
### 10.1.4 Logistic

In the **Logistic** menu you can create, edit or remove orders, Lots and Sale Lots.

#### 10.1.4.1 Orders

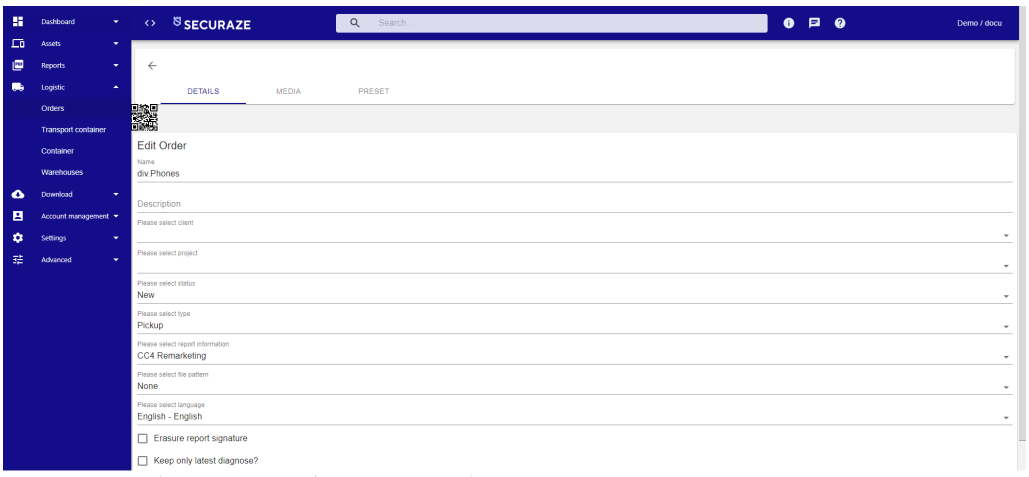
The **Orders** menu allows you to create new Order, edit existing ones and delete them.

There you see a list of all orders.




By selecting the option **Go to Work Products** you can access the list of work devices. By selecting the option **Go to Mobile Products** you get to the list of mobile devices of this order.

By selecting **Order Details** you can see more details for the order.



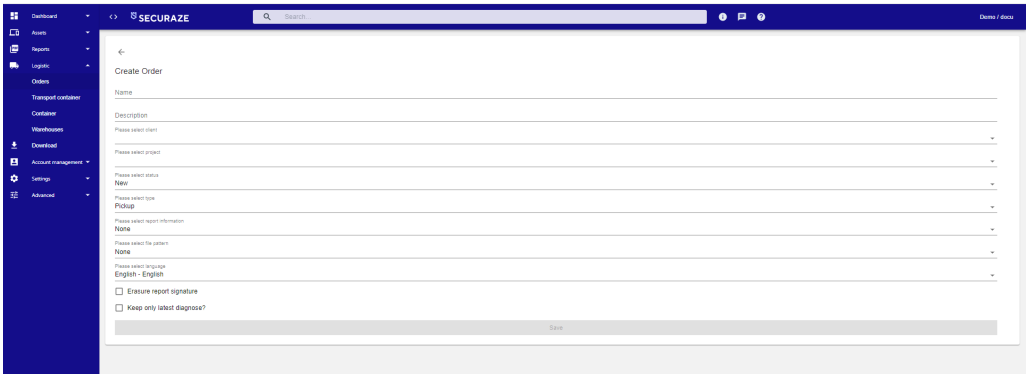


© 2026 Securaze GmbH

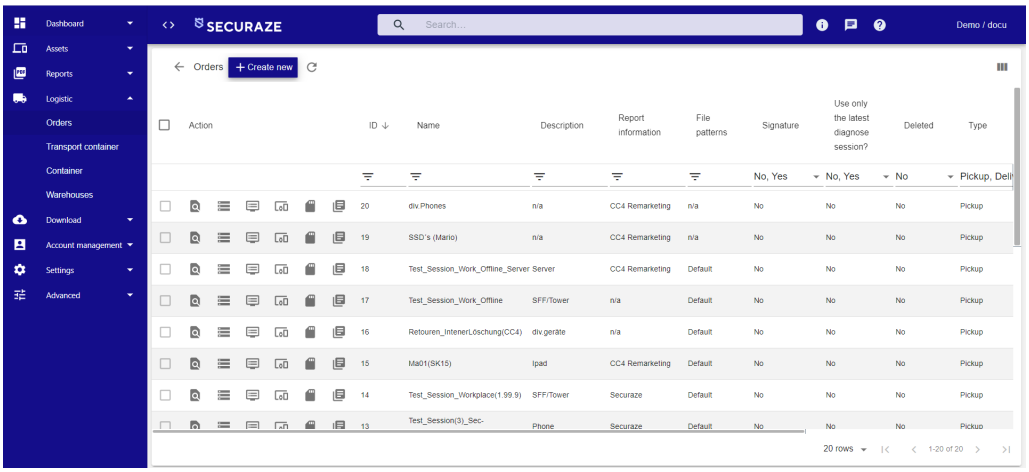
### 10.1.4.1.1 Create new Orders

To create a new Pickup Order, click **Pickup Orders** in the Menu section, then click **Create New**.

Enter the name and description of the pickup order and select the report information and file name pattern you entered.




After confirming the selection by clicking **SAVE**, the newly created order is displayed in the **Order** menu**.**

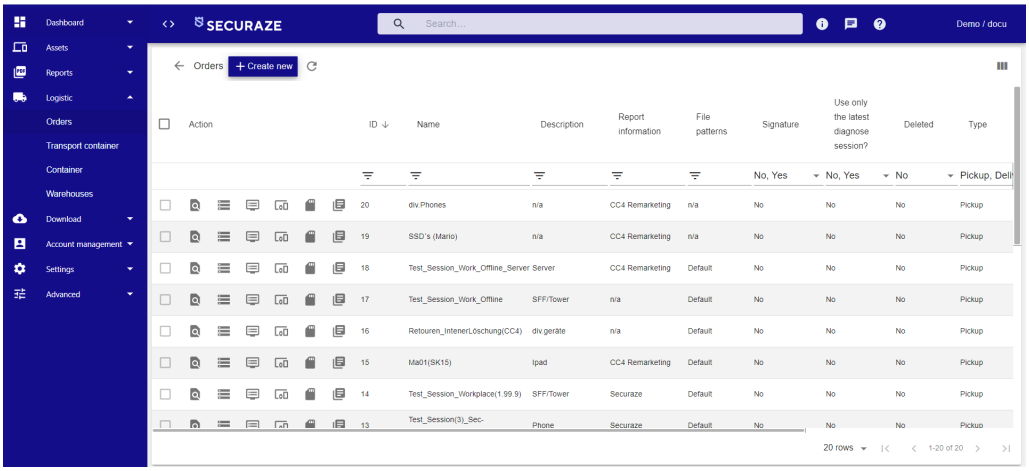



### 10.1.4.1.2 Edit Orders

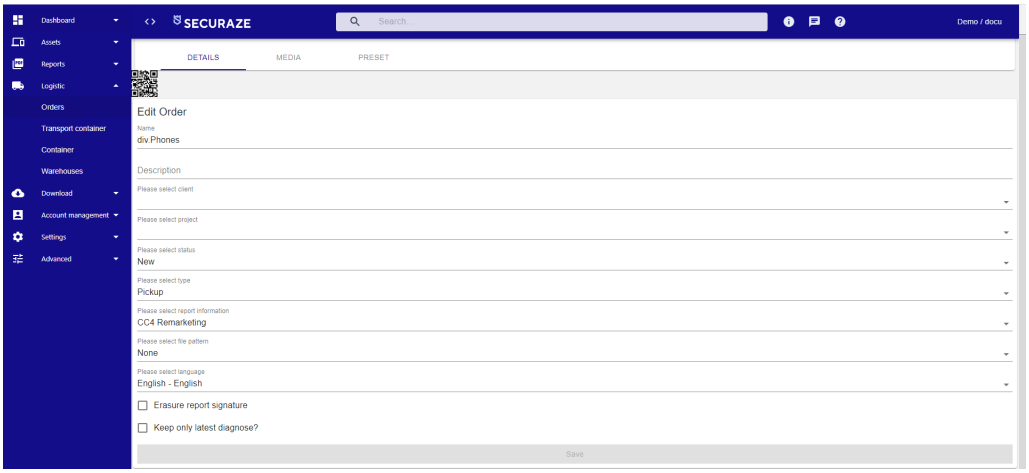
To edit a Pickup Order, select the Pickup Order and click Order Details .

.


© 2026 Securaze GmbH



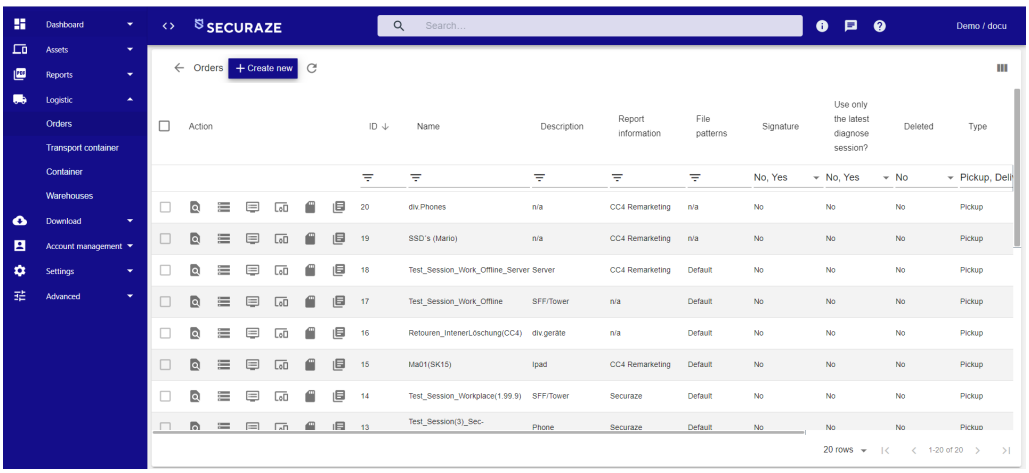

Make the desired changes and confirm them by clicking **SAVE**.




### 10.1.4.1.3 Delete Orders

To delete an Order, select the Order and click Remove all selected Orders .

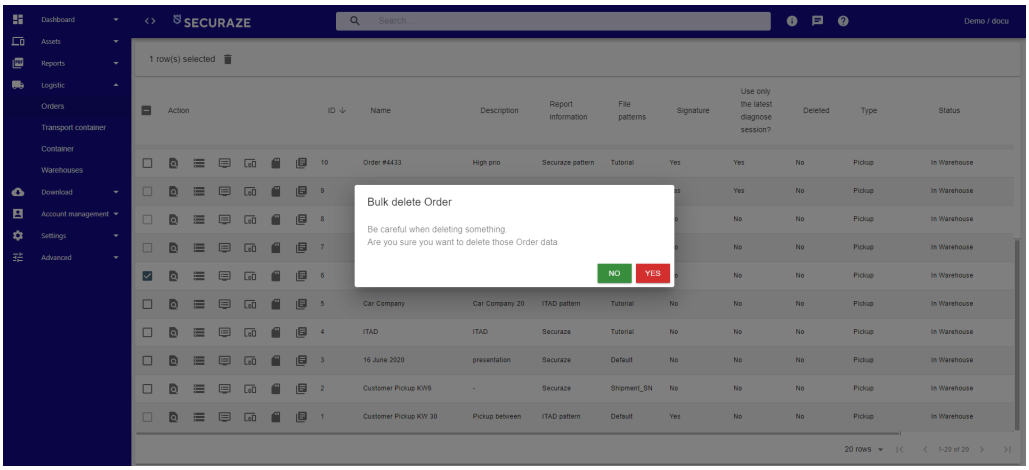
.





© 2026 Securaze GmbH

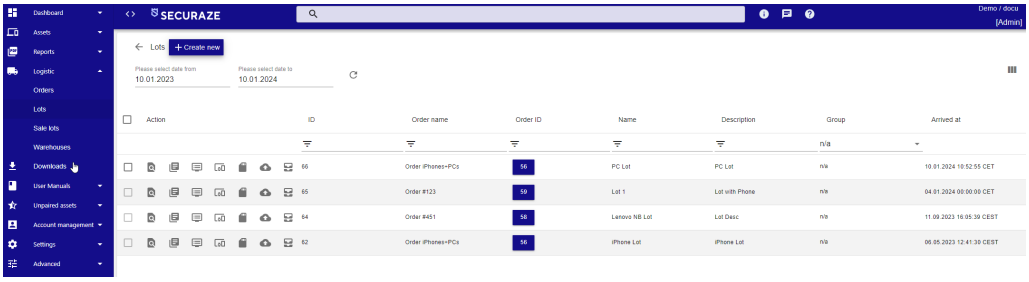
Confirm the erasure by clicking on **YES**.




### 10.1.4.2 Lot

In the menu **Logistic - Lot** you can create new Lots, edit and delete existing ones.

There you see a list of all Lots.




By selecting the option **Go to Work Products** you can access the list of work devices. By selecting the option **Go to Mobile Products** you get to the list of mobile devices of this Lot.

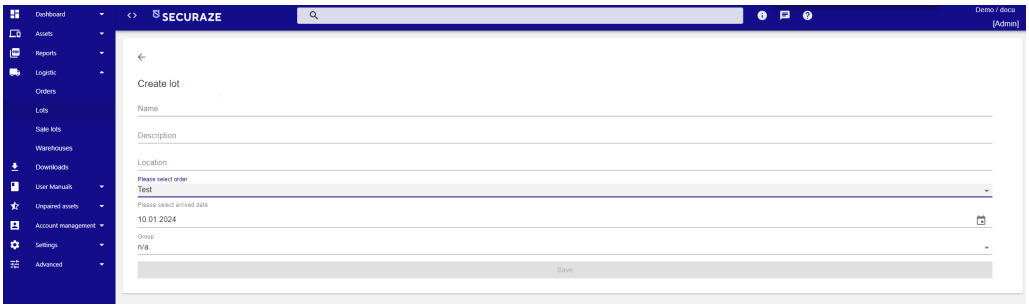
By selecting **Lot Details** you can see more details for the Lot.

#### 10.1.4.2.1 Create new Lot

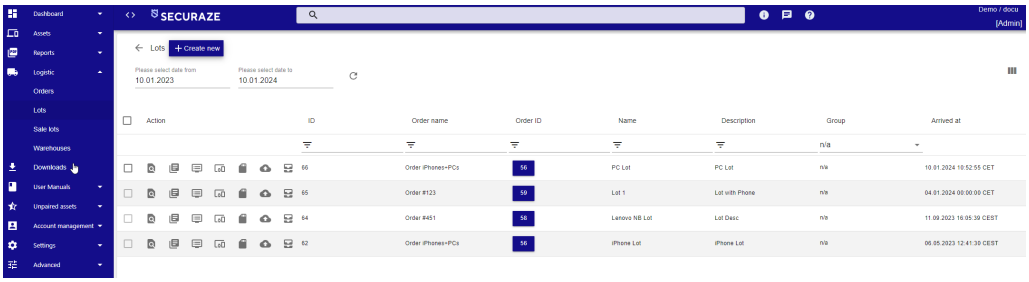
To create a new Lot, click on **Logistic - Lot** in the Menu section and then on **Create New**.

Here you enter the name, description, and location of the Lot and select the order and arrival date.


© 2026 Securaze GmbH

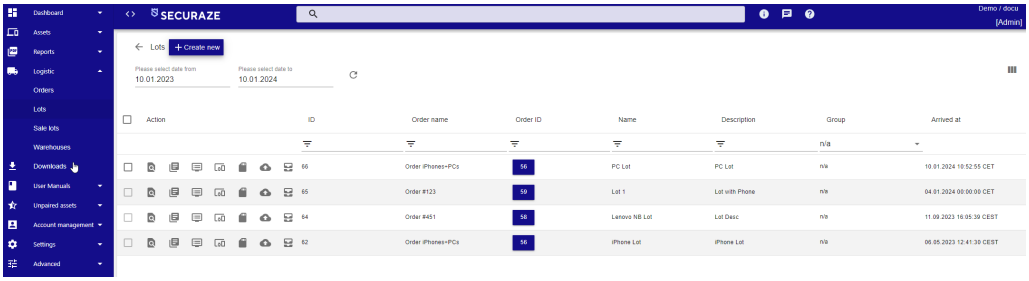



After confirming the selection by clicking **SAVE**, the newly created Lot is visible in the menu **Logistc - Lot**.



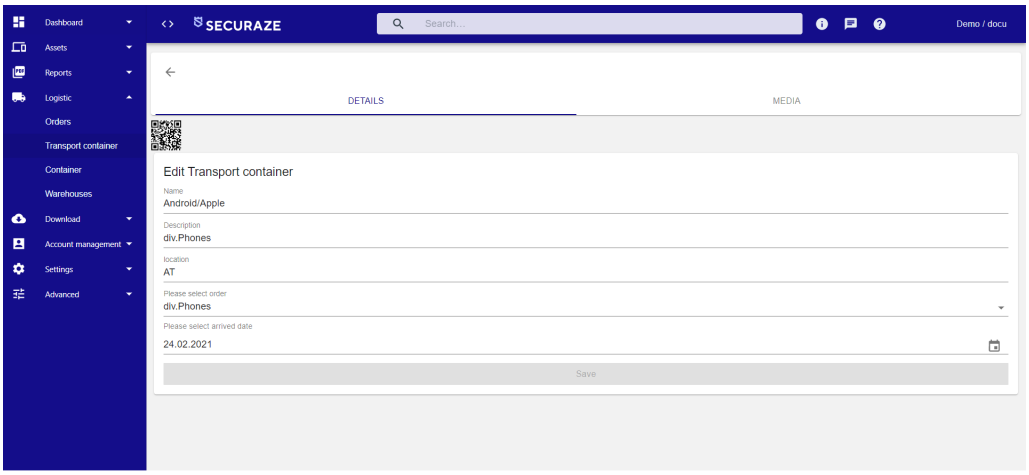

### 10.1.4.2.2 Edit Lot

To edit an incoming pallet, select the relevant Lot and click Lot Details .



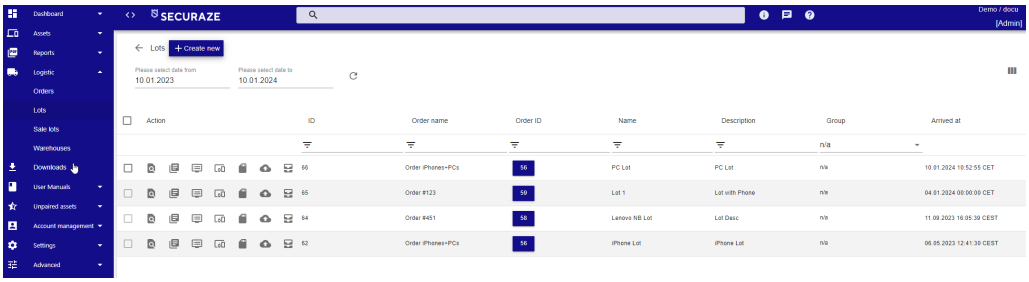

Make the desired changes and confirm them by clicking **SAVE**.


© 2026 Securaze GmbH




### 10.1.4.2.3 Delete Lot

To delete an Lot, select the Lot and click Delete **Lot**




Confirm the erasure by clicking on **YES**.



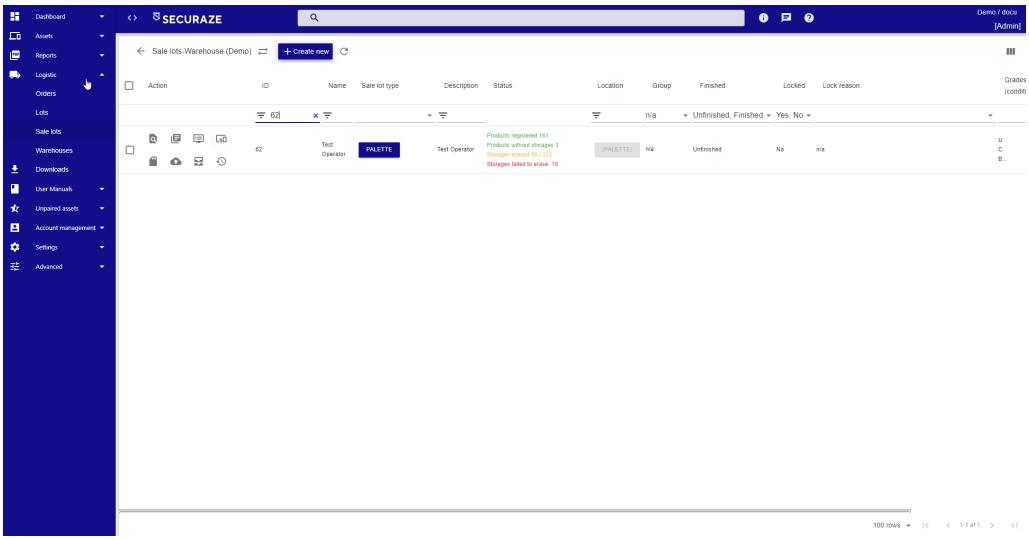
### 10.1.4.3 Sale Lots

In the menu **Logistc - Sale Lots** you can create new Sale Lots, edit and delete existing ones.

There you see a list of all Sale Lots with the status of the erasure.

The Status field displays a brief overview of the content and status of the devices on the Sale Lot.


© 2026 Securaze GmbH




By selecting the option **Go to Work Products** you can access the list of work devices. By selecting the option **Go to Mobile Products** you get to the list of mobile devices of this Sale Lot. Here you can see some details about the devices and the status of the deletion.

Under **history** you can call up an overview, which shows when the device was deleted and what the result was.

By selecting **Sale Lots Details** you can see more details for the Sale Lot.

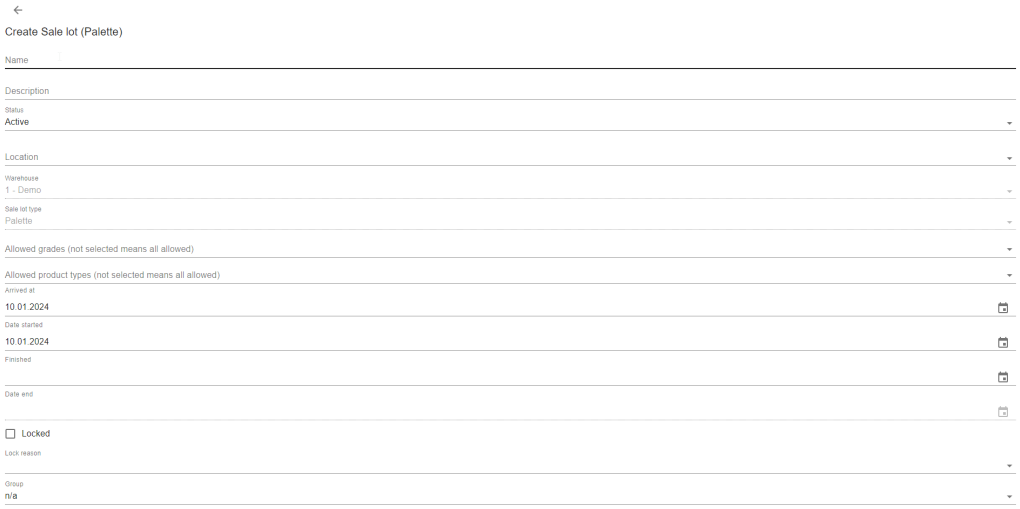



### 10.1.4.3.1 Create new Sale Lot

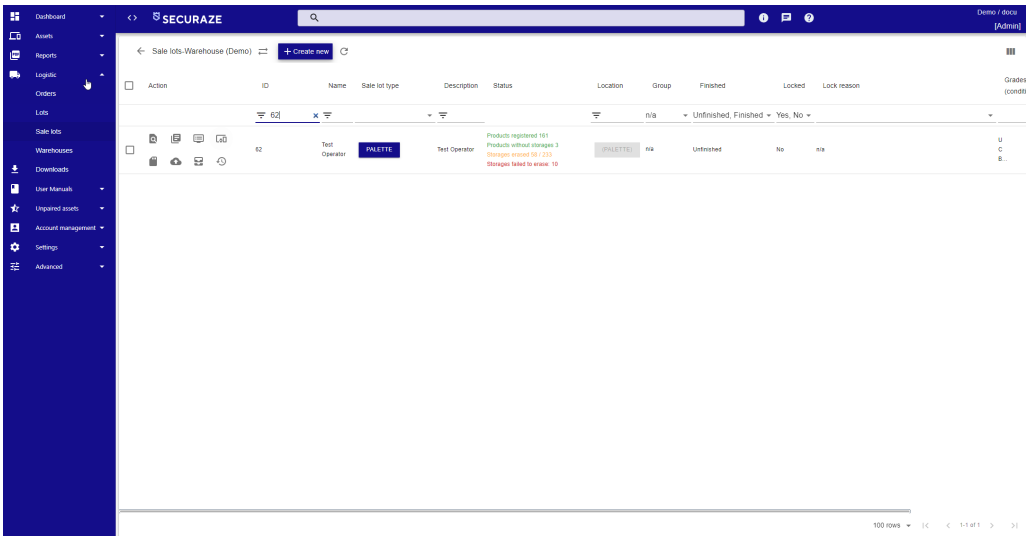
To create a new Sale Lot, click on **Sale Lots** in the Menu section and then on **Create New.**

Here you enter the name, description and location of the Sale Lot and select the date.


© 2026 Securaze GmbH



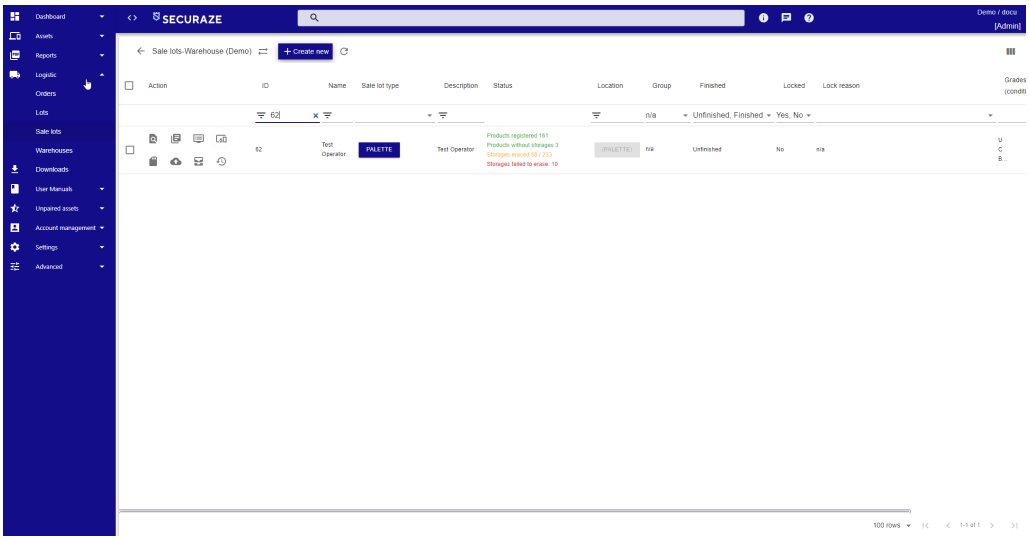

After confirming the selection by clicking **SAVE**, the newly created Sale Lot is visible in the **Sale Lots** menu.



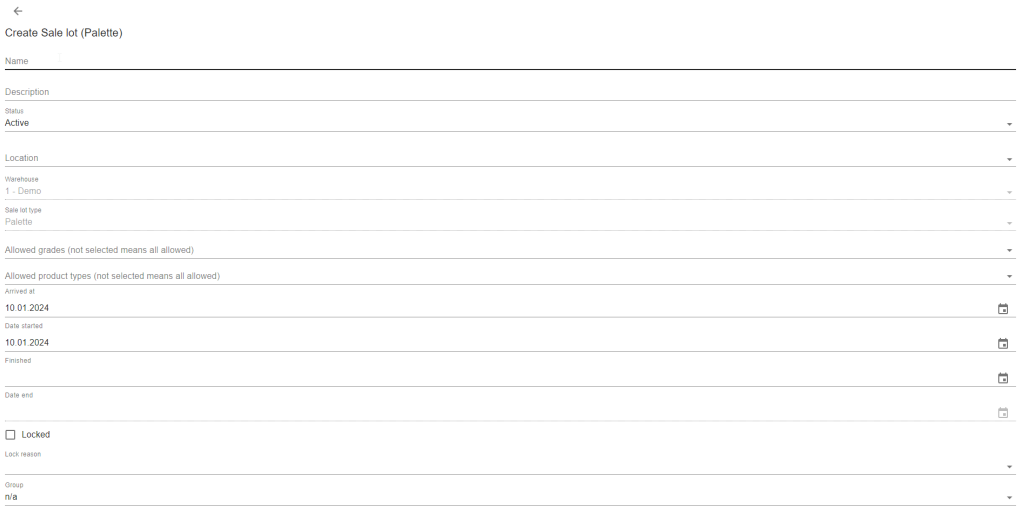

### 10.1.4.3.2 Edit Sale Lot

To edit a Sale Lot, select the Sale Lot and click Sale Lot Details .


© 2026 Securaze GmbH



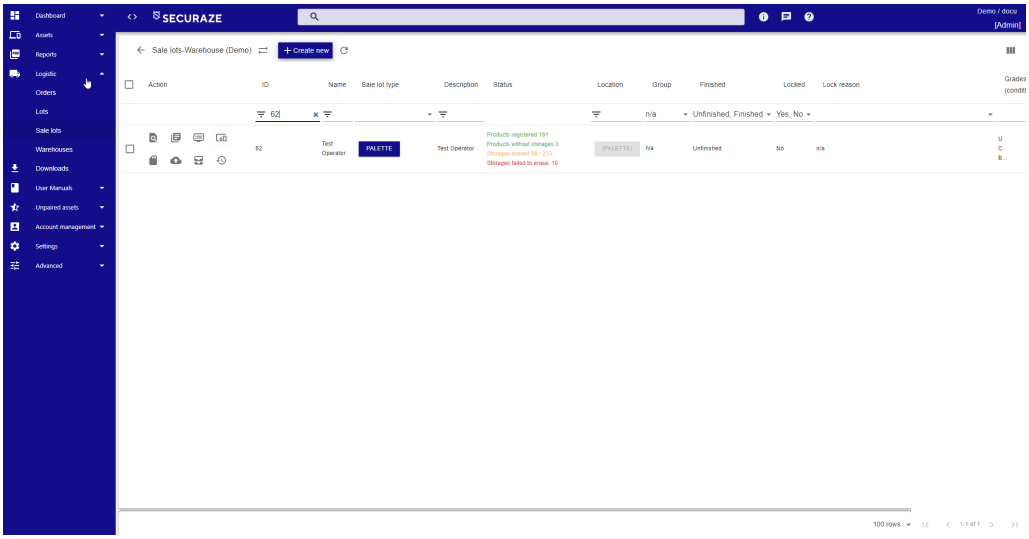

Make the desired changes and confirm them by clicking on **SAVE**.




### 10.1.4.3.3 Delete Sale Lot

To delete a Sale Lot, select the respective Sale Lot and click on Delete **Sale Lot** .

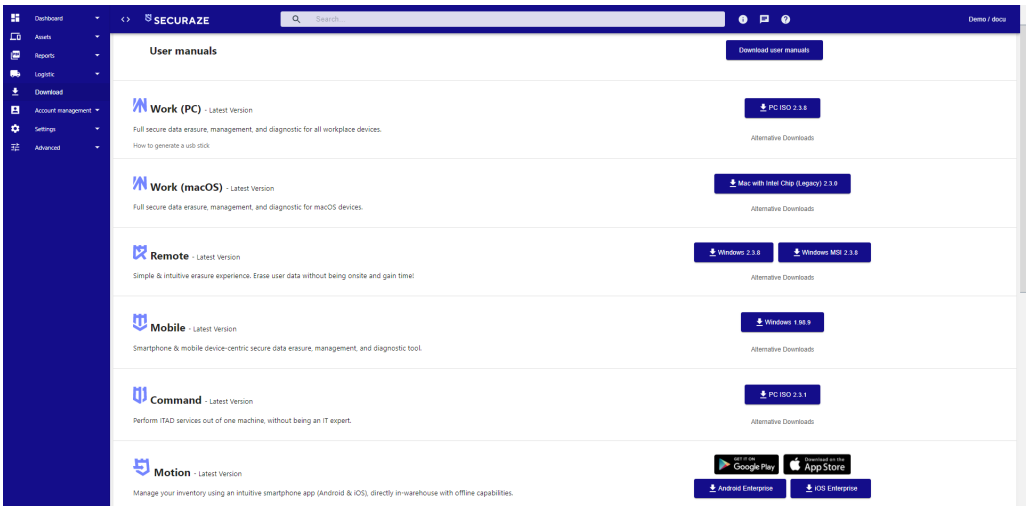

© 2026 Securaze GmbH




## 10.1.5 Download

In the menu **Downloads** you can download the Securaze software and the User manuals.

You will always find the current version of the software and alternative downloads




Start the download by clicking on the corresponding button.

In this section you can also find the download for Securaze Creator, a tool that is used for creating a bootable USB stick, which is needed to boot Securaze Work.

## 10.1.6 Account Management

In the **Account Management** menu you can create, edit or remove users, roles and customers.

### 10.1.6.1 User

In the **Users** menu you can create new Users, edit existing ones and delete them.

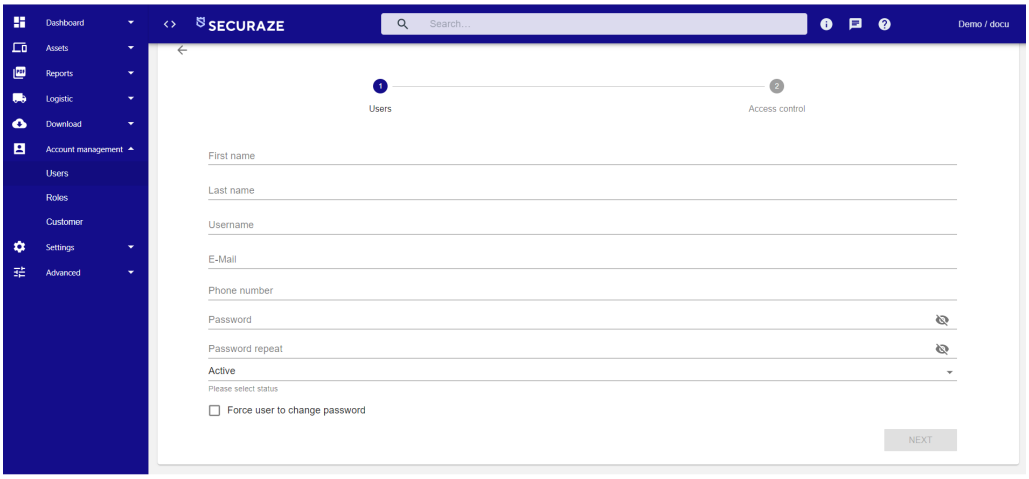

© 2026 Securaze GmbH

### 10.1.6.1.1 Create new Users

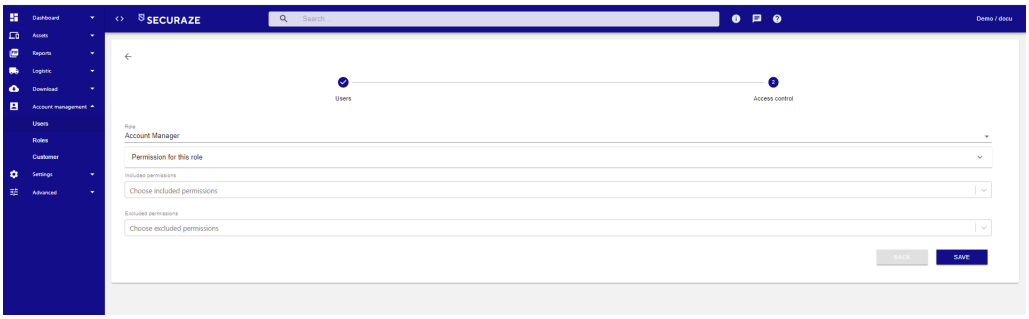
To create a new user, click on **Users** in the Menu section and then on **Create New**.

Here you enter the data of the new user and set a password.

By selecting the item **Force user to change password**, you assign a temporary password which the user must change after the first login.




Confirm the entry of your data with **NEXT**.




In the next step, select the authorization level of the user:

Admin

Operator

Supervisor

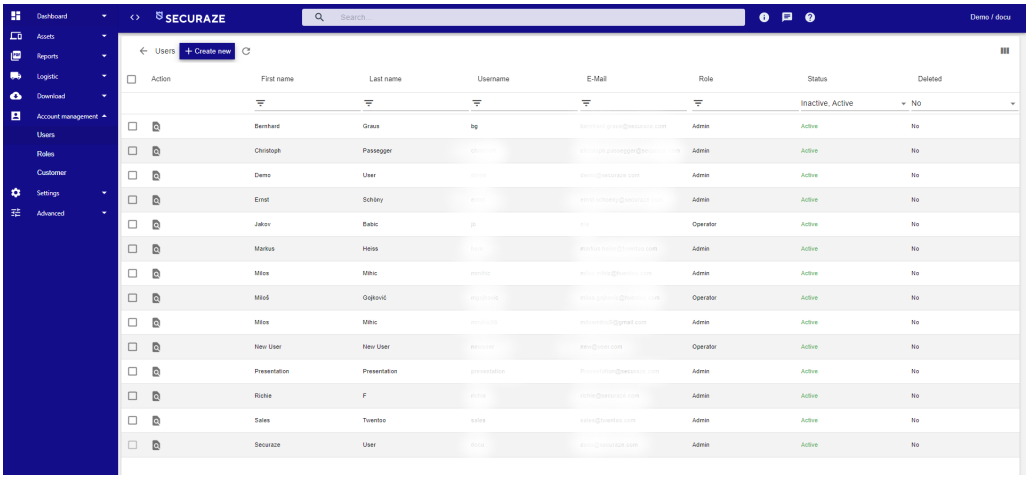
Restricted

EndUser

Below that you can assign permissions under **Included Permissions** and withdraw permissions under **Excluded Permissions**. To do so, click on the respective pull-down menu and select the desired permissions.


© 2026 Securaze GmbH

After confirming the selection by clicking on **SAVE**, the newly created user is visible in the **User** menu.




The created user has 3 different possibilities to log in:

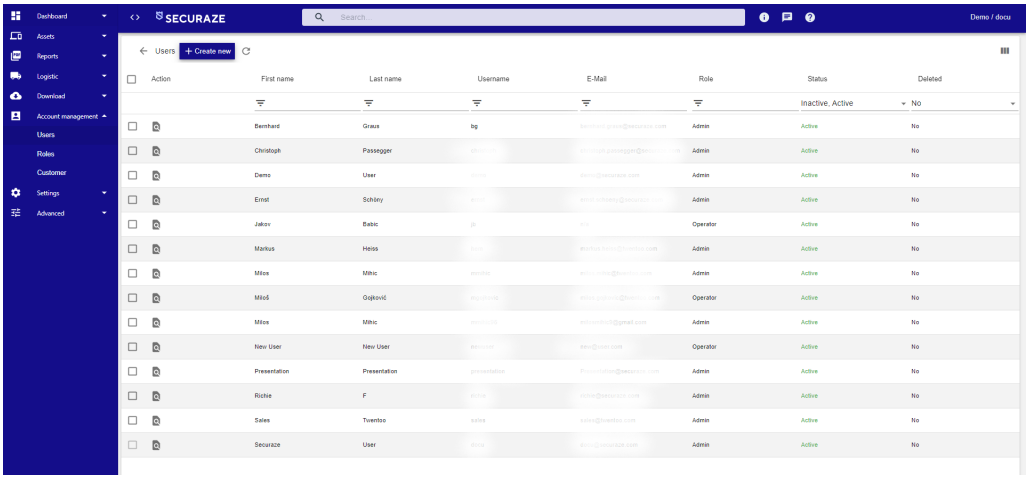
Login with complete username: Enter *username* @ *namespace* 242

Login with e-mail address: Enter your registered e-mail address.

Login with user name: This is only possible if you are in a created network zone 274 and the authorization has been given that you can log in using a user name.

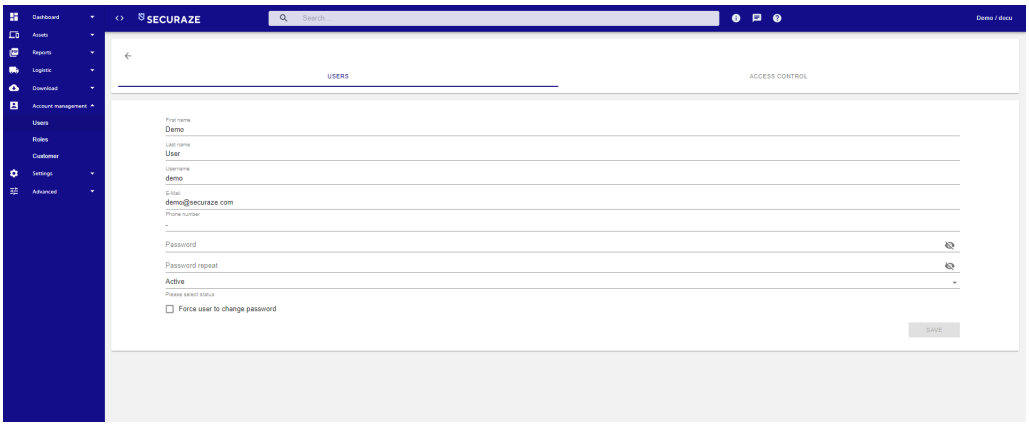
### 10.1.6.1.2 Edit User

To edit a user, select the respective user and click **User details**



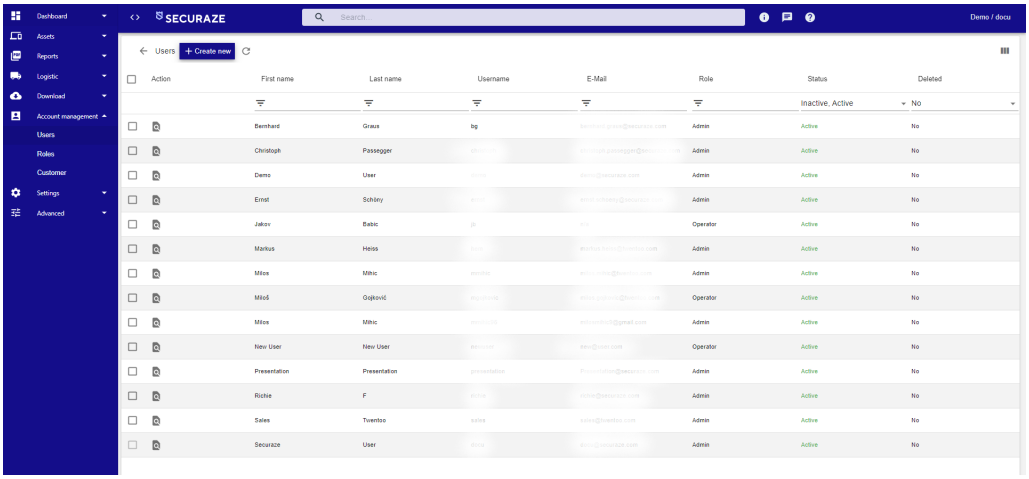

Make the desired changes and confirm them by clicking **SAVE**.


© 2026 Securaze GmbH

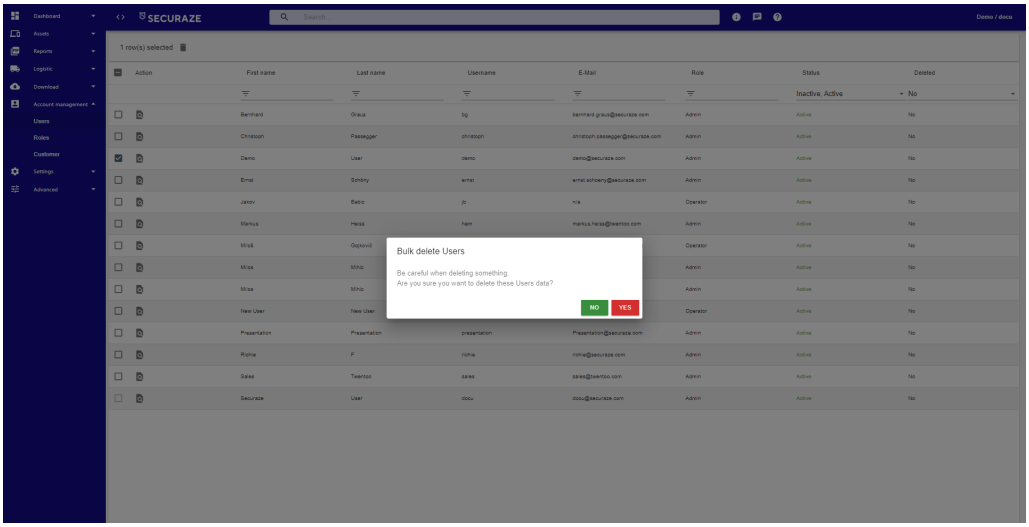



### 10.1.6.1.3 Delete User

To delete a user, select the respective user and click **Remove all selected Users**.




Confirm the erasure by clicking on **YES**.





© 2026 Securaze GmbH

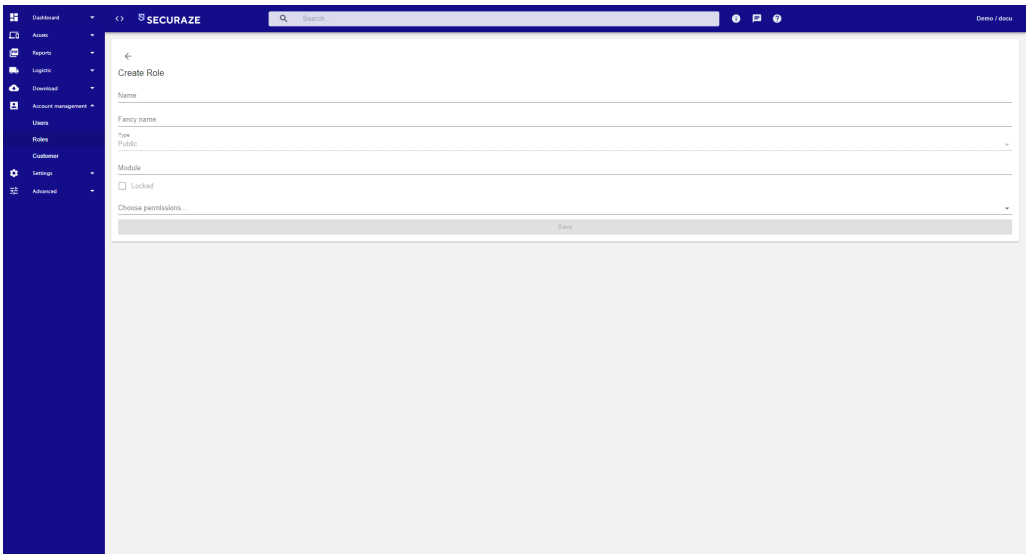
### 10.1.6.2 Roles

In the **Roles** menu you can create new roles, edit existing ones and delete them.

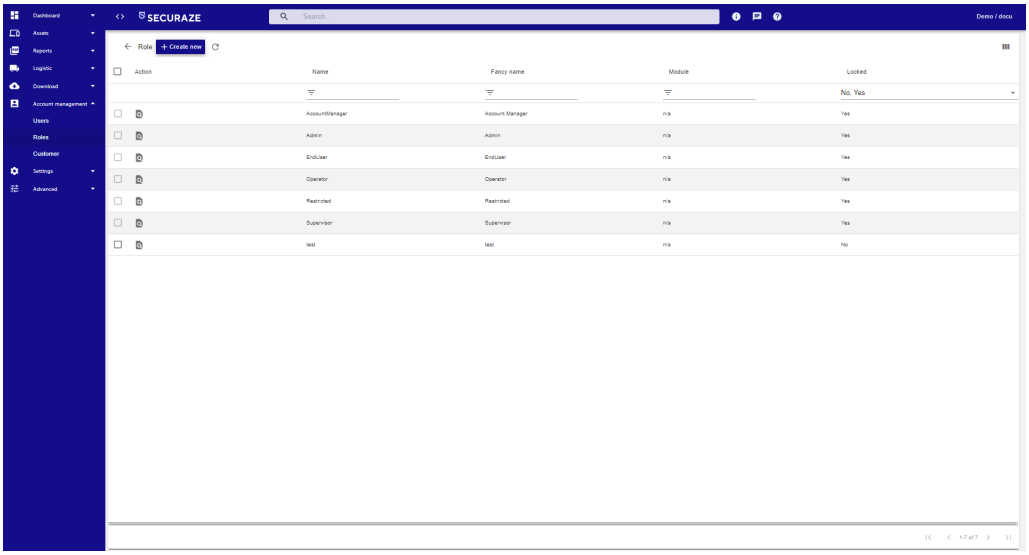
#### 10.1.6.2.1 Create new Role

To create a new role, click on **Roles** in the Menu section and then on **Create New**.

Here you enter the data of the new role.



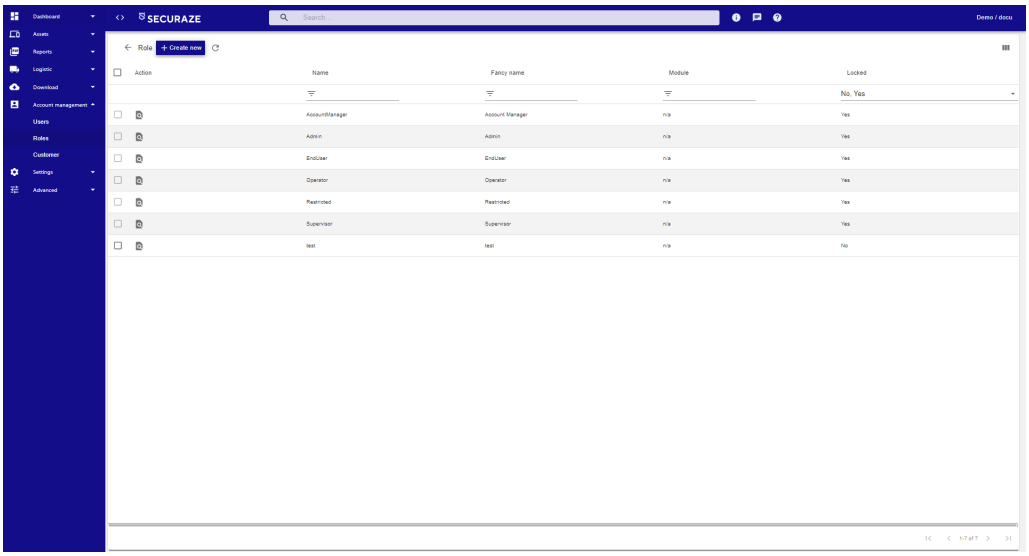

After confirming the selection by clicking on **SAVE**, the newly created user is visible in the **Roles** menu.



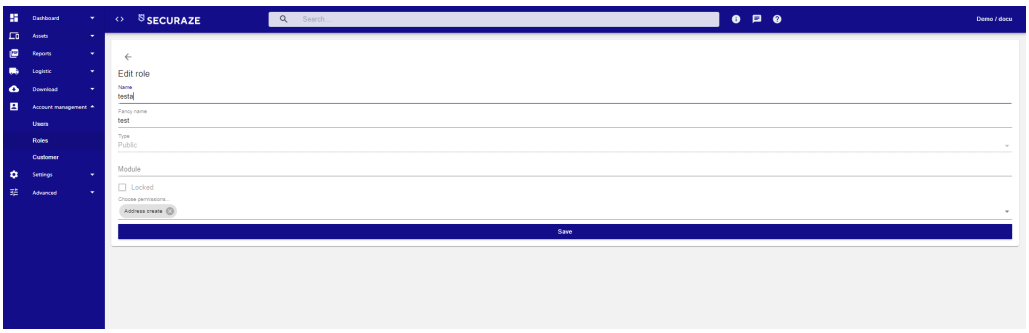

#### 10.1.6.2.2 Edit Role

To edit a user, select the respective user and click **Role details**


© 2026 Securaze GmbH



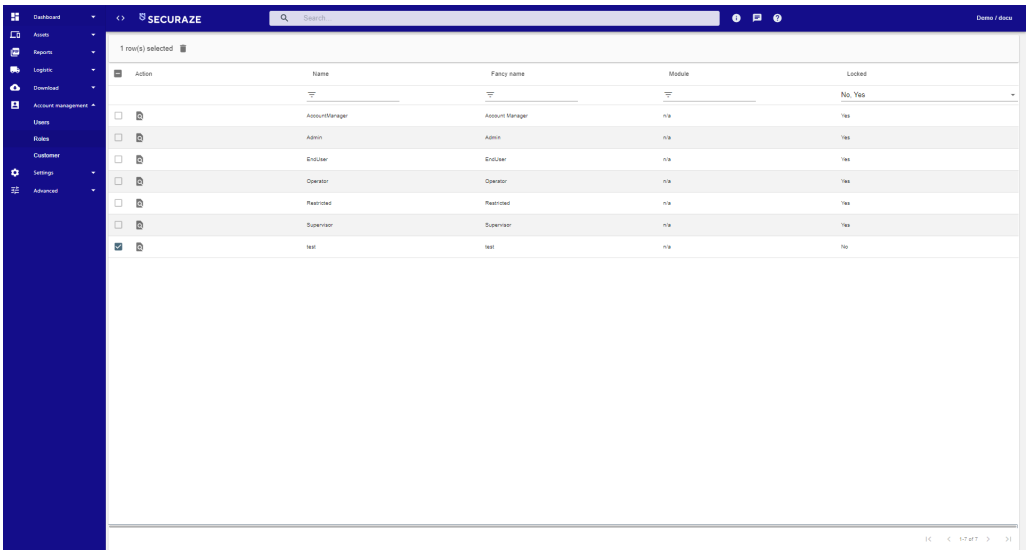

Make the desired changes and confirm them by clicking **SAVE**.



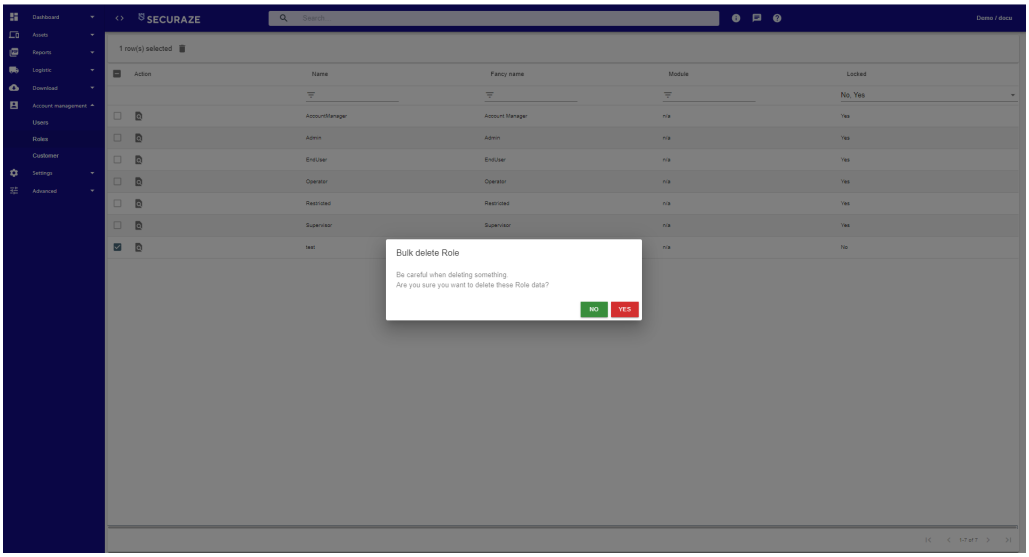

### 10.1.6.2.3 Delete Role

To delete a user, select the respective user and click **Remove all selected Roles**.


© 2026 Securaze GmbH



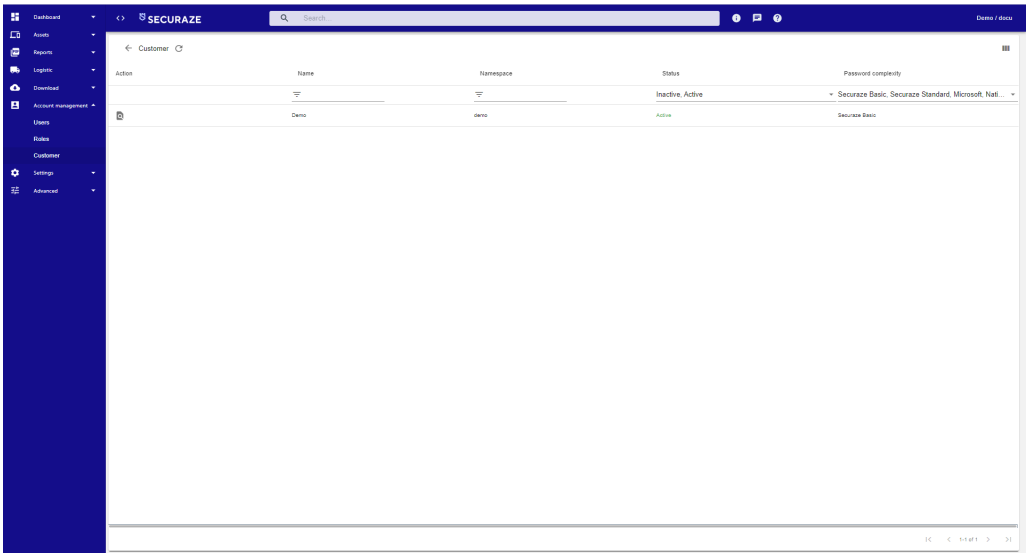
Confirm the erasure by clicking on **YES**.



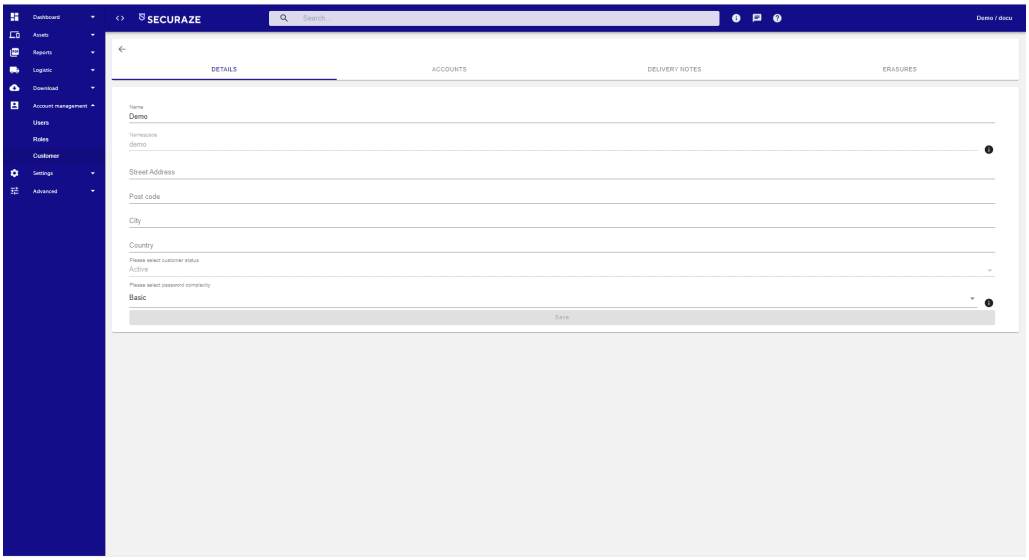

### 10.1.6.3 Customer

In the **Customer** menu you see an overview of the customers created.


© 2026 Securaze GmbH




By clicking on **customer details** you will get to the detailed view.




Here you can choose from the following tabs:

DETAILS

ACCOUNTS

DELIVERY DOCUMENTS

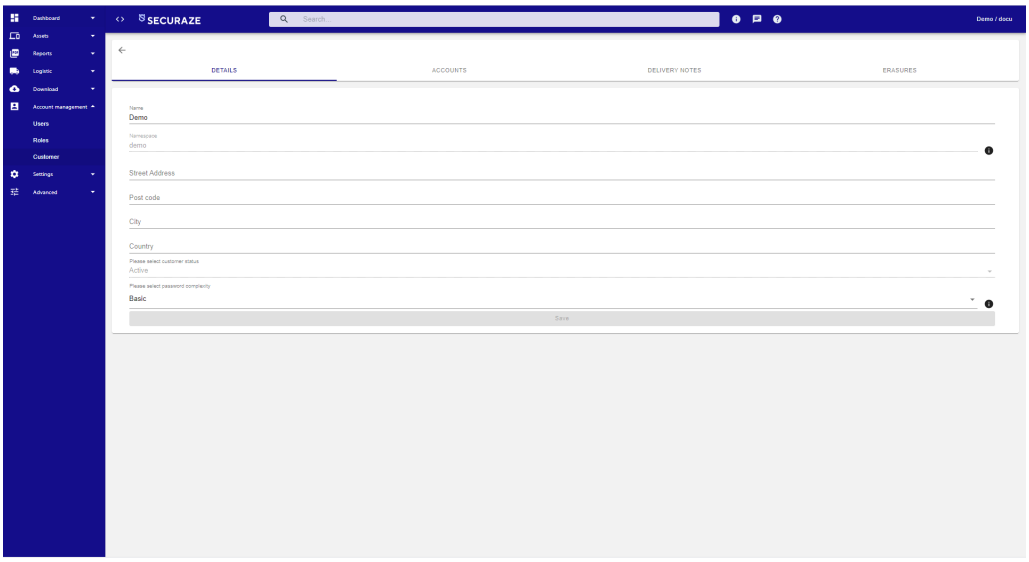
ERASURES

Select the desired tab by clicking on the respective word.

### 10.1.6.3.1 Details

Here you get an overview of the data of the selected customer.


© 2026 Securaze GmbH




First of all you will see the name and address of the customer.

**Namespace:**

Each customer is assigned a unique namespace, which is defined when the customer is created. The selected namespace is valid in combination with the selected user name (*user name@namespace)* as the complete user name for the login 236.

Only lower case letters, numbers and underscores are allowed for the namespace. The selected namespace should be as short, simple and unique as possible.

The namespace can only be changed afterwards by using a support ticket.

**Status**:

Here you have 2 options to choose from:

active

inactive

Choose the status of the customer by selecting it in the drop-down menu.

**Password complexity:**

Here you have 4 options to choose from:

Securaze simple

Securaze Standard

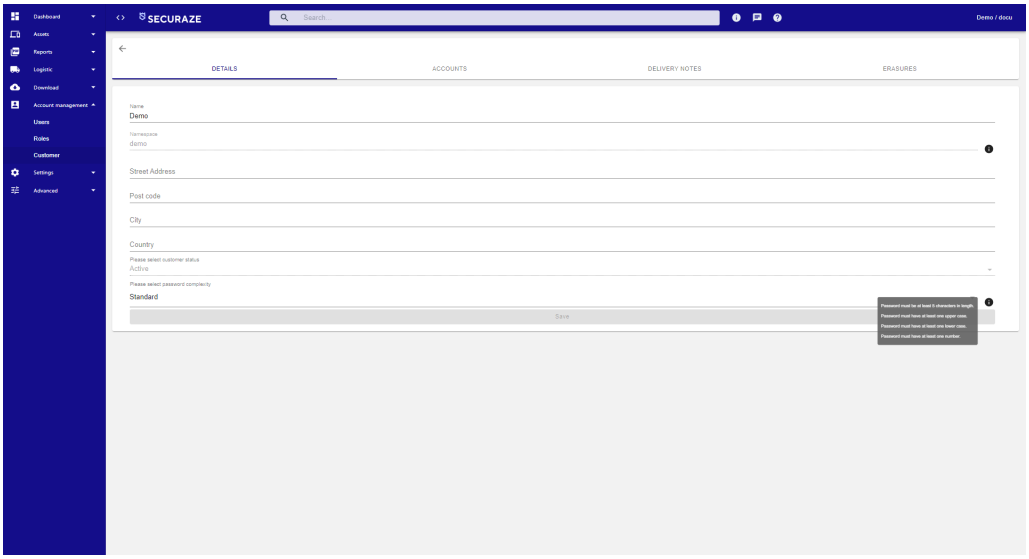
Microsoft

National Institute of Standards and Technology


© 2026 Securaze GmbH

Select the desired password complexity for the customer by selecting from the drop-down menu.

After selecting the password complexity, you can see the requirements for the selected option by placing the mouse pointer over the icon.




## 10.1.7 Settings

In the **Settings** menu you can make settings for Presets, Grades, Report Customizations, Printers, Network Zone, Erasure Methods and External System Settings.

### 10.1.7.1 Presets

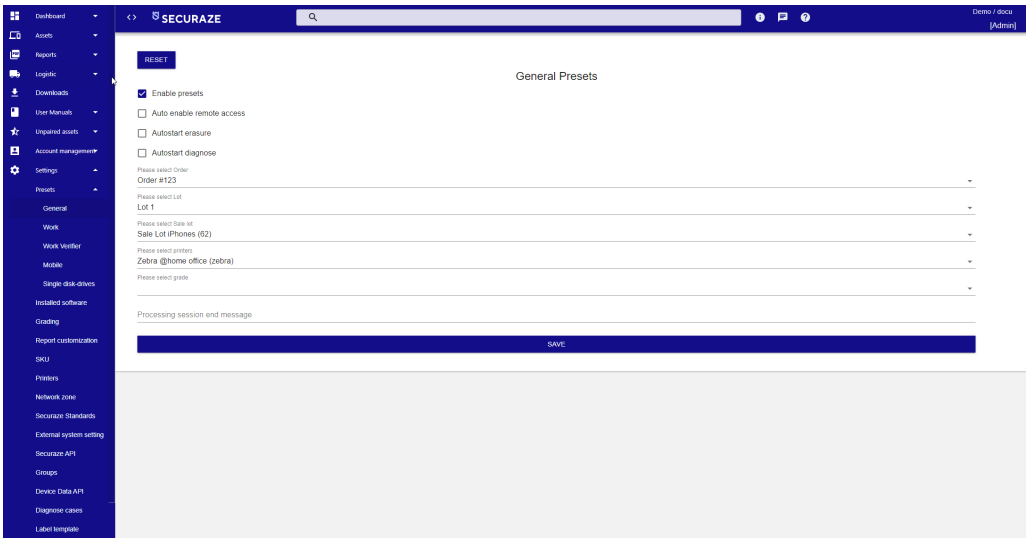
To define specific settings that Securaze should execute immediately after login, click on the **Presets** tab.

The presets are splitted in sections for General settings and settings for the individual clients.

#### 10.1.7.1.1 General

The general settings are valid and used by all Securaze products.


© 2026 Securaze GmbH




Before you can make the desired settings, click **Enable Presets.**

You can make the following settings:

| Setting | Description |
|---|---|
| Enable presets | Enable the presets or diable them at all. (just defined Wifis will be used) |
| Auto shut down after successful erasure (Work) | Check this box to specify that the system will automatically shut down after erasure process finished successfully.In case the erasure failed, the device will keep running. |
| Auto enable remote access | Check this box for starting remote support for each started device. |
| Autostart erasure | Check this box for auto start erasure. |
| Automatic unfreeze | Automatically unfreeze disks for erasure |
| Autostart diagnose | Check this box for auto start diagnostic. |
| Select Order | Select the desired default-order from the list. |
| Select Lot | Select the desired default-Lot from the list. |
| Select Sale Lot | Select the desired default Sale Lot from the list. |
| SSD Securaze Standard | Select the desired method for SSD / flash storages from the list. |
| SSD verification method | Select the desired verification method for SSD / flash storages from the list. |


© 2026 Securaze GmbH

| Setting | Description |
|---|---|
| HDD Securaze Standard | Select the desired method for HDD storages from the list. |
| HDD verification method | Select the desired verification method for HDD storage from the list. |
| Don't erase drives with worse SMART score than: | Allows Securaze to warn the operator based on a bad SMART score of the storage that the erasure could possibly fail.<br>The calculated SMART score ranges from 0 to 100 and maps to the drive health grade shown per drive:<br>**Excellent** - score 81-100.<br>**Good** - score 70-80.<br>**Fair** - score 50-69.<br>**Acceptable** - score 25-49.<br>**Critical** - score 1-24.<br>**Failure Predicted** - score 0, or when the RAID controller reports a predictive failure.<br>The check is off by default: Securaze only warns when a score is set here.<br>The operator can set the SMART score below which a drive is marked as a Bad Disk. Securaze then warns before erasing it; the operator can still continue. The score is set in the Presets for HDD erasure: |
| Disk Health Calculation | This setting changes the calculation method of the SMART Health score.<br><br>Currently supported:<br>**Securaze proprietary method**<br>Securaze proprietary method (typically the most rigorous calculation method) [Default]<br><br>**Hard disk sentinel (HDSentinel)**<br>Hard disk sentinel method, based on public available documentation of the algorithm<br>https://www.hdsentinel.com/help/en/52_cond.html<br>https://www.hdsentinel.com/smart/index.php<br><br>**Acronis Drive Monitor** |


© 2026 Securaze GmbH

| Setting | Description |
|---|---|
| | Acronis Drive Monitor method, based on public available documentation of the algorithm https://kb.acronis.com/content/9264 |
| Please select normal screen brightness (e.g. after login, while entering data) | Available for both Work macOS and Work Linux, working for PC, macOS Native and also Mac booting WorkPC.<br><br>Normal Brightness can be set to any value between 20 and 100. |
| Please select reduced screen brightness (during screensaver mode) | Reduced Brightness can be set to any value between 0 and 100, for when screensaver is displayed during erasure (allowing the screen to be black, if max. power saving is required)<br>If Diagnose is started, the Brightness goes to 100 until Diagnose is finished, then it is returning to configured Normal Brightness. |
| Please select printers | Preselect the default printer. |
| Please select grade | Preselect the default grade. |
| Please select operating system | Preselect the default operating system. |
| Processing session end message | Message which should appear after processing a device. |
| Different erasure solution for Android and iOS | Enable to select different default values for iOS and Android devices. |
| Print upon connection | Print a label on connection of a device. |
| Print upon successful erasure | Print a label on successful erasure. |
| Print upon failed or aborted erasure | Print a label on failed or aborted erasure. |
| Print upon diagnose | Print a label on diagnose of a device. |
| Remove app after diagnose | Remove Securaze application after diagnose. |


© 2026 Securaze GmbH

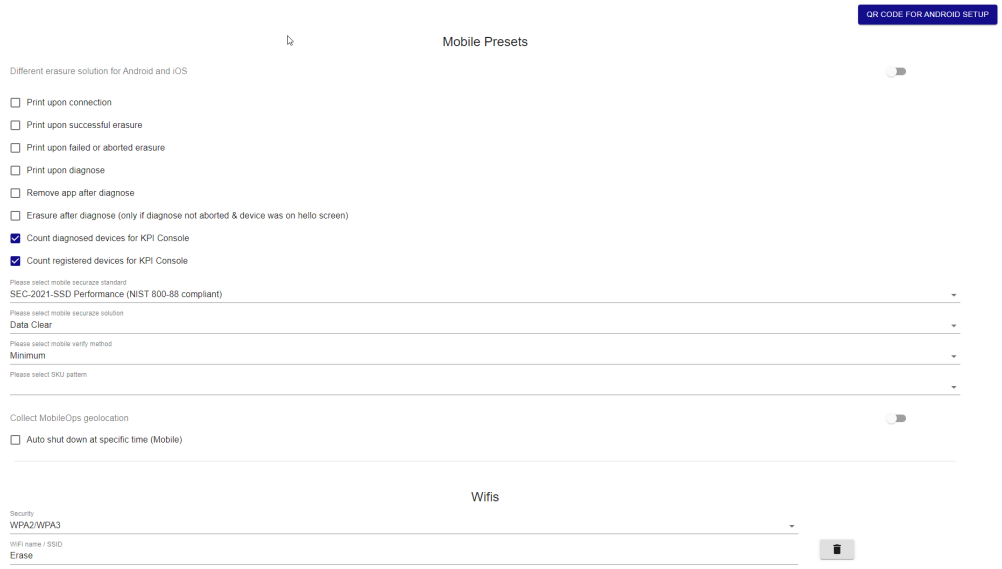
| Setting | Description |
|---|---|
| Erasure after diagnose (only if diagnose not aborted) | Erase the device after diagnose. Only if diagnose was not aborted. |
| Count diagnosed devices for KPI Console | Count diagnosed devices for the KPI Console. |
| Count registered devices for KPI Console | Count registered devices for the KPI Console. |
| Please select mobile securaze standard | Default value for the Securaze Standard. |
| Please select mobile securaze solution | Default value for the Securaze Solution. |
| Please select mobile verify method | Select the desired verification method from the list. |
| Collect MobileOps geolocation | Collects the geolocation of the device in the moment of processing the device. |
| Wifis | Define the wifi(s) which should be used when processing the devices.<br>It is mandatory for iOS diagnose and iOS Advanced erasure.<br>And it can be used for generating QR-Codes for faster Android USB-Debugging bypass. |
| | |
| | |
| | |

Make your settings and confirm them with **SAVE.**

### 10.1.7.1.2 Mobile

You can make the following preset settings for Mobile in Menu section **Settings - Presets - Mobile**:


© 2026 Securaze GmbH




| Setting | Description |
|---|---|
| Print upon connection | Print a label on connection of a device. |
| Print upon successful erasure | Print a label on successful erasure. |
| Print upon failed or aborted erasure | Print a label on failed or aborted erasure. |
| Print upon diagnose | Print a label on diagnose of a device. |
| Print upon successful erasure | Print a label on successful erasure. |
| Remove App after diagnose | emove Securaze application after diagnose from the device. |
| Erasure after diagnose (only if diagnose not aborted) | Erase the device after diagnose.Only if diagnose was not aborted. |
| Count diagnosed devices for KPI Console | Count diagnosed devices for the KPI Console. |
| Count registered devices for KPI Console | Count registered devices for the KPI Console. |


© 2026 Securaze GmbH

| Setting | Description |
|---|---|
| Please select mobile securaze standard | Default value for the Securaze Standard. |
| Please select mobile securaze solution | Default value for the Securaze Solution. |
| Please select mobile verify method | Select the desired verification method from the list. |
| Select SKU pattern | Select a custom SKU pattern which can be defined in Settings / SKU in advance. |
| Collect MobileOps geolocation | Collects the geolocation of the device in the moment of processing the device. |
| Auto shut down at specific time | Shutdown the Mobile station at a specific time to save energy after working hours. |
| Wifis | Define the wifi(s) which should be used when processing the devices.<br>It is mandatory for iOS diagnose and iOS Advanced erasure.<br>And it can be used for generating QR-Codes for faster Android USB-Debugging bypass. |
| QR Code for Android Setup | This functionality allows to send the QR-Code for Android setup via mail. |
| | |
| | |

Make your settings and confirm them with **SAVE.**

#### 10.1.7.1.3 Work

You can make the following preset settings for Work in Menu section **Settings - Presets - Work**:


© 2026 Securaze GmbH




| Setting | Description |
|---|---|
| Auto shutdown after successful erasure | Device will shutdown after successful erasure and keep running otherwise. |
| Automatic unfreeze | Device will do a automatic unfreeze before erasure. |
| Please select SSD Securaze standard | Default value for the Securaze Standard. |
| Please select SSD Verify method | Select the desired verification method from the list. |
| Please select HDD Securaze standard | Default value for the Securaze Standard for HDDs. |
| Please select HDD Verify method | Select the desired verification method for HDDs from the list. |
| Don't erase drives with worse SMART score than | Specify the warning level for SMART score. If the SMART score(health) of the storage is below the specified value a warning will appear. |
| Disk Health Calculation | Choose the method for the Disk Health calculation.<br>Default is Securaze. Hard Disk Sentinel and Acronis are also available. |
| Please select normal screen brightness | Screen brightness (e.g. after login, while entering data) |
| Please select reduced screen | Screen brightness (e.g. during screensaver mode) |

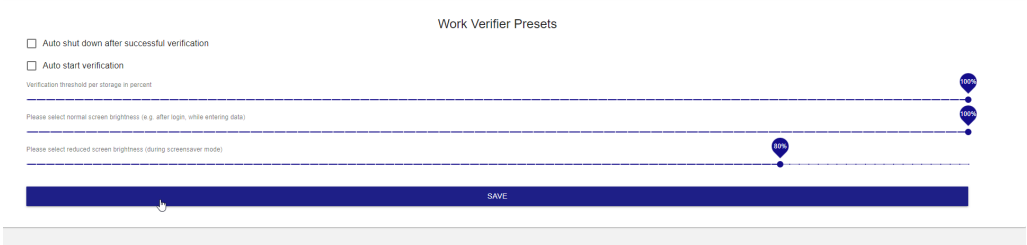

© 2026 Securaze GmbH

| Setting | Description |
|---|---|
| brightness (during screensaver mode) | |
| Please select operating system | Default operating system for all devices. |
| Please select SKU pattern | Used SKU pattern. |
| Remove BIOS/UEFI Passwords | Specify BIOS/UEFI passwords which are getting removed. Supported are Dell, HP and Lenovo devices. |

Make your settings and confirm them with **SAVE.**

### 10.1.7.1.4 Work Verifier

You can make the following preset settings for Mobile in Menu section **Settings - Presets - Work Verifier**:




| Setting | Description |
|---|---|
| Auto shutdown after successful verification | Device will shutdown after successful verification and keep running otherwise. |
| Auto start verification | Device will do a automatic verification after login. |
| Verification threshold per storage in percent | How much data of the storage should get verified. (Default 100%) |
| Please select normal screen brightness | Screen brightness (e.g. after login, while entering data) |

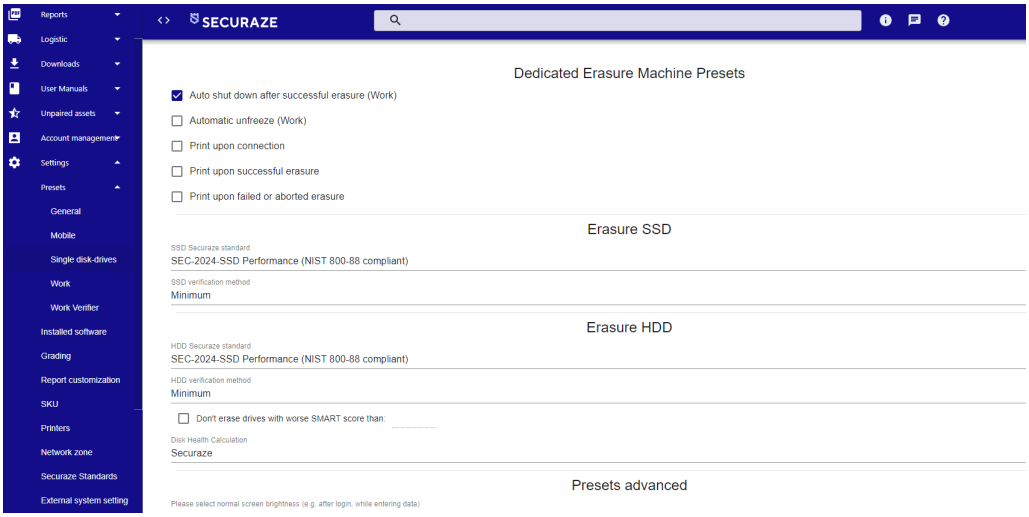

© 2026 Securaze GmbH

| Setting | Description |
|---|---|
| Please select reduced screen brightness (during screensaver mode) | Screen brightness (e.g. during screensaver mode) |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |

Make your settings and confirm them with **SAVE.**

### 10.1.7.1.5 Single Disk-Drives

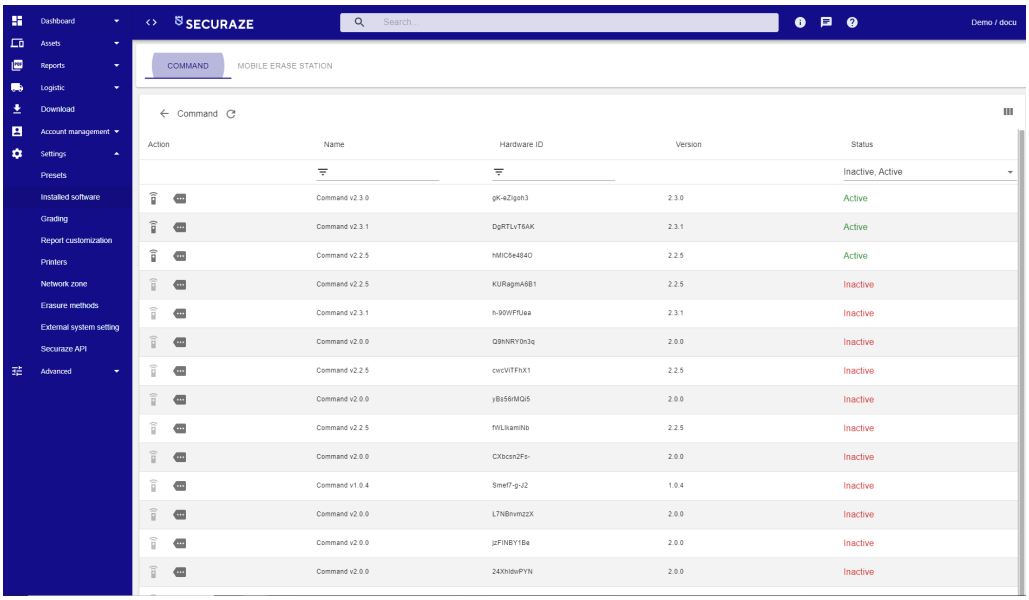
Single Disk-Drive presets are settings applied only when Securaze Work is used for erasure of loose drives (disks) in Dedicated Erasure Machine mode.




## 10.1.7.2 Installed software

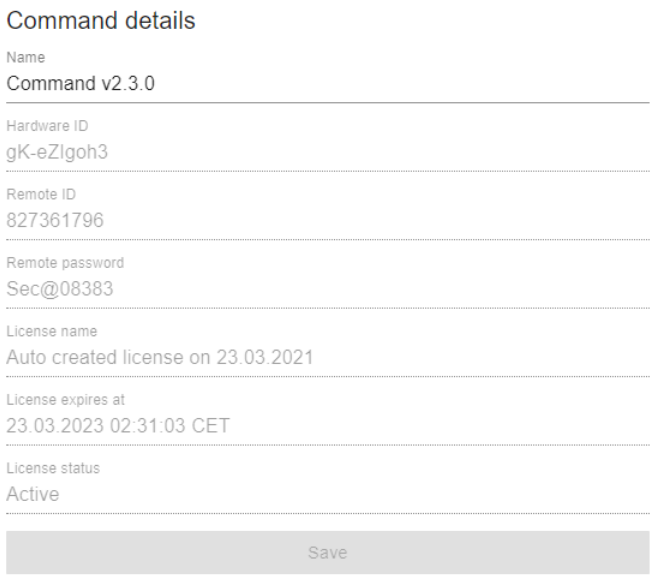
In the menu **Installed software** you can see the different versions of the software that are installed.


© 2026 Securaze GmbH



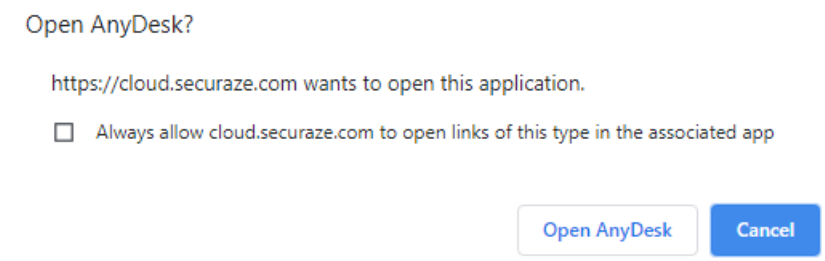

Here you can find the information about which version it is and if the software is active.

If you click on Command details, a new window will open showing the details.




If you click on the icon **Open Securaze Remote**, you can establish a remote connection via RustDesk (Securaze Remote). Make sure RustDesk is installed on your computer; AnyDesk remains available as a legacy fallback.

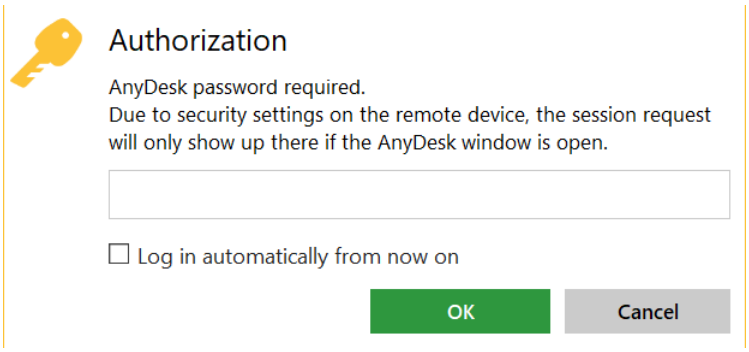

© 2026 Securaze GmbH




The password will be copied to clipboard automatically.




When RustDesk opens, paste the copied password here with CTRL+V and confirm.




After that, a remote connection to the device will be established.

### 10.1.7.3 Grading

In the **Grading** menu you can see 4 tabs:

GRADES

TYPICAL PROBLEMS

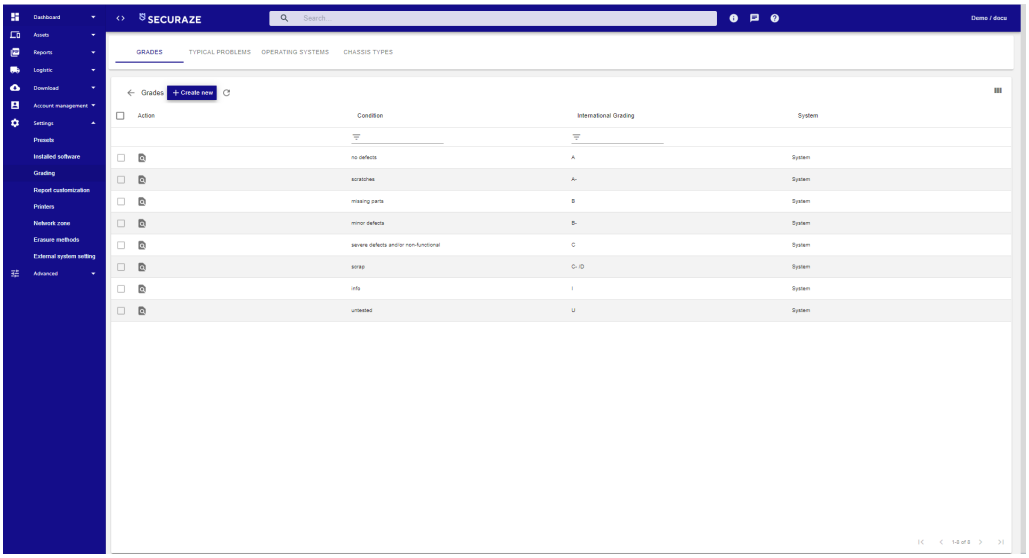
OPERATING SYSTEMS

CHASSIS TYPES


© 2026 Securaze GmbH

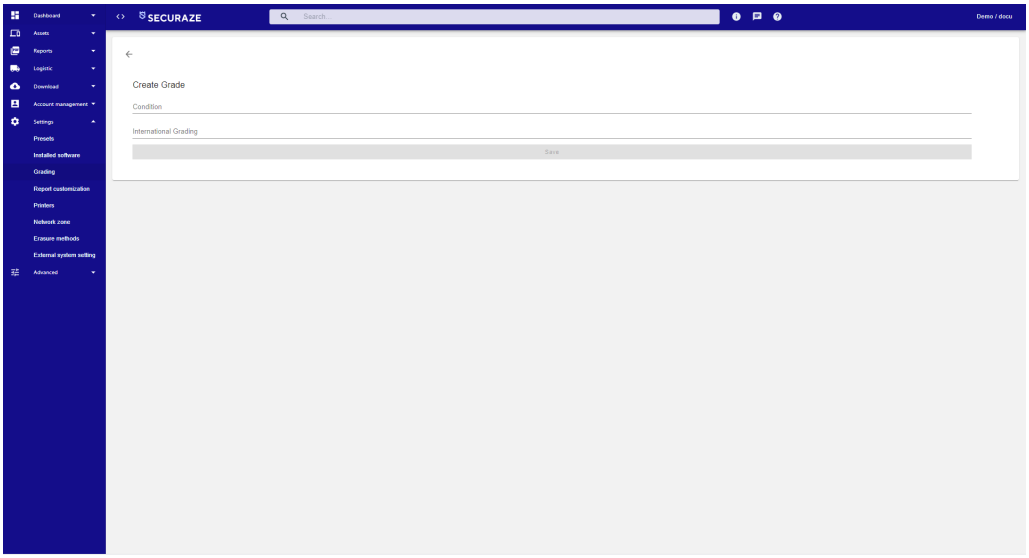
### 10.1.7.3.1 Grades

Here you can see a list of all grades.




To create a new grade, click on **Grading** in the Menu section and then on the **Tab Grades**. Then choose **Create New**.

Here you enter the data of the new grade.

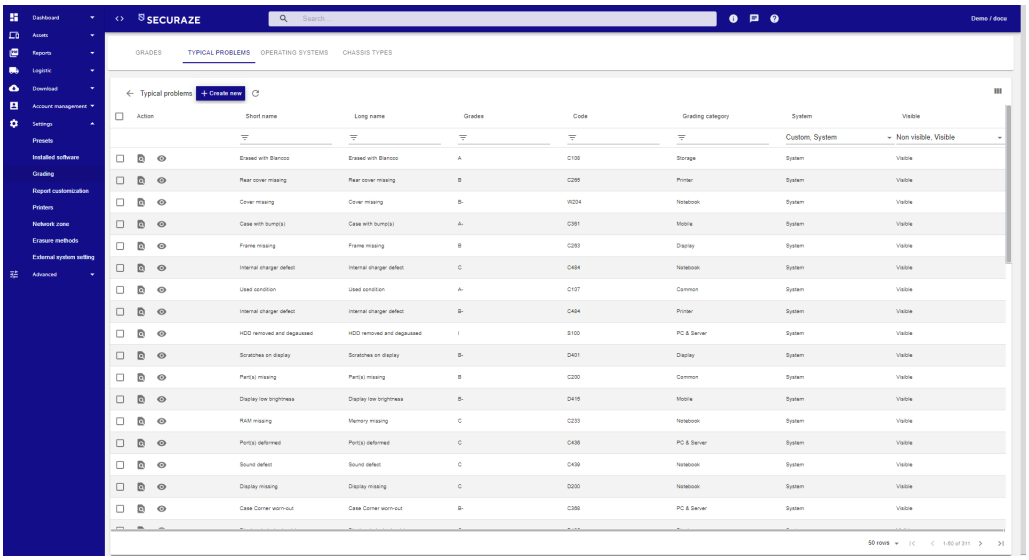



After confirming the selection by clicking **SAVE**, the newly created grade is displayed in the **Grades** menu.


© 2026 Securaze GmbH

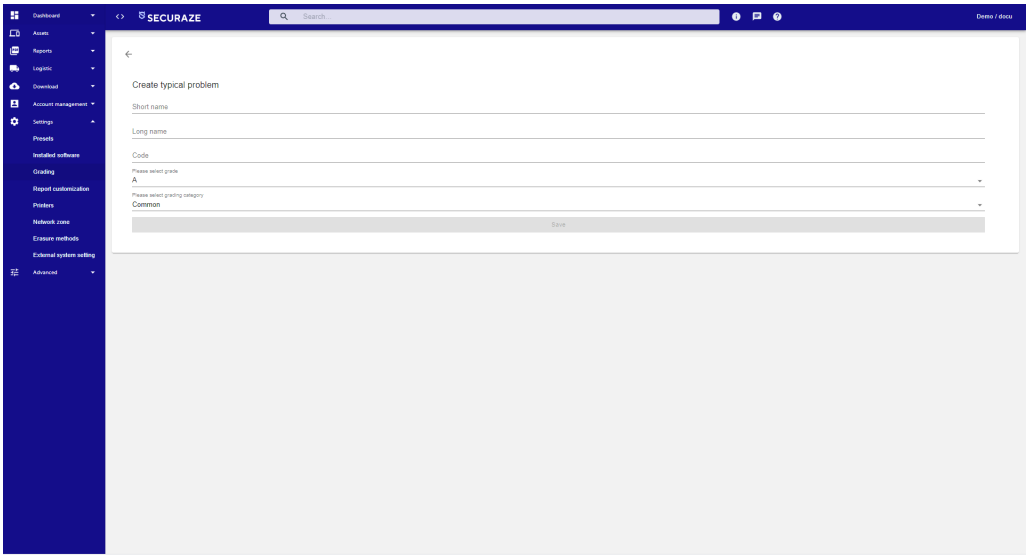
### 10.1.7.3.2 Typical problems (Optional)

Here you can see a list of all typical problems.




To create a new typical problem, click on **Grading** in the Menu section and then on the **Tab Typical Problems**. Then choose **Create New**.

Here you enter the data of the new typical problem.

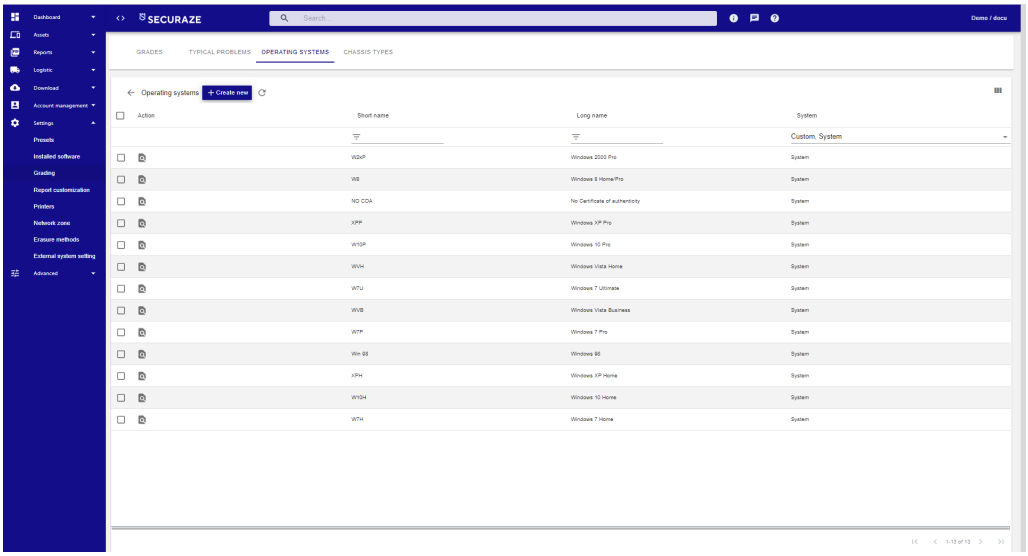



After confirming the selection by clicking **SAVE**, the newly created grade is displayed in the **Typical Problems** menu.

### 10.1.7.3.3 Operating Systems

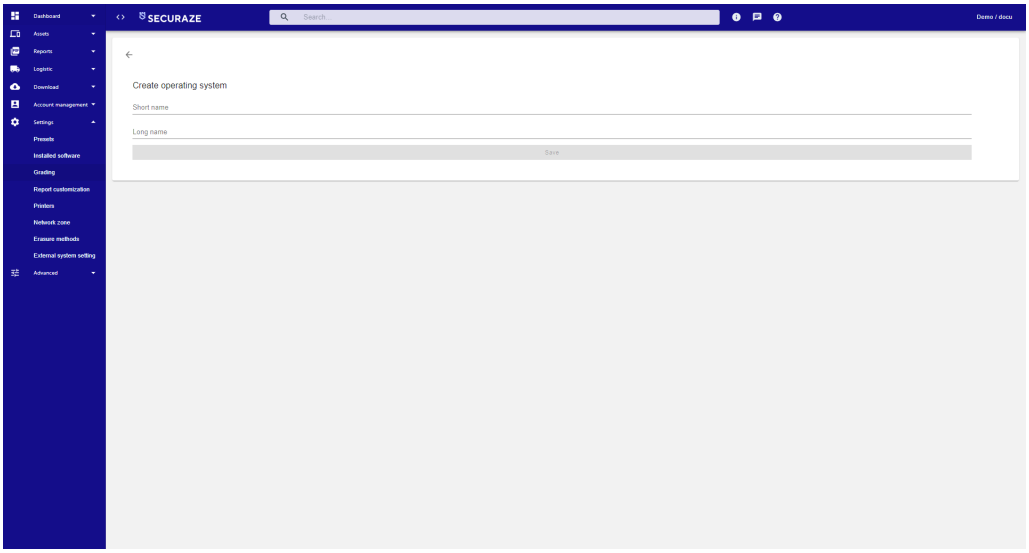
Here you can see a list of all Operating Systems.


© 2026 Securaze GmbH




To create a new operating system, click on **Grading** in the Menu section and then on the **Tab Operating Systems**. Then choose **Create New**.

Here you enter the data of the new operating system.

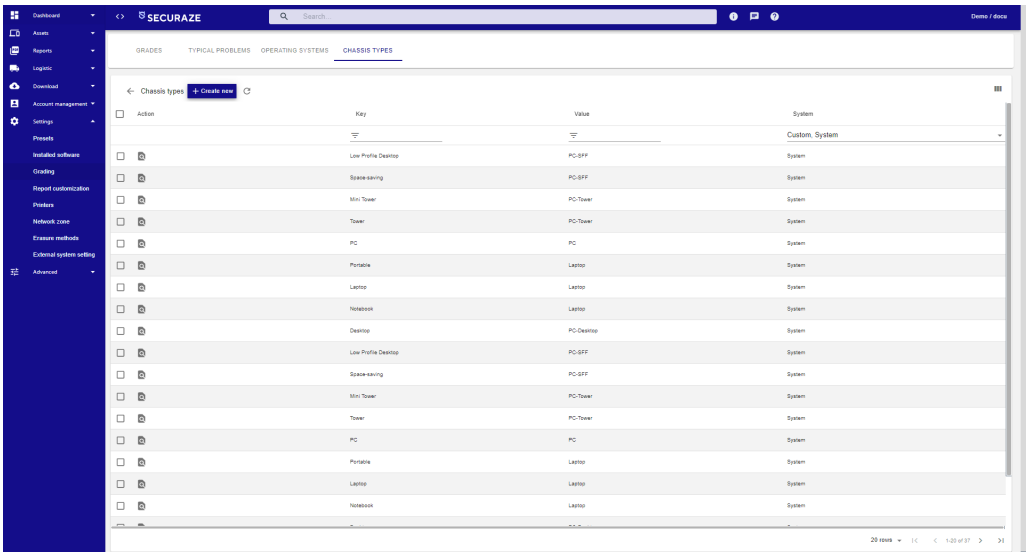



After confirming the selection by clicking **SAVE**, the newly created grade is displayed in the **Operating Systems** menu.

### 10.1.7.3.4 Chassis Types

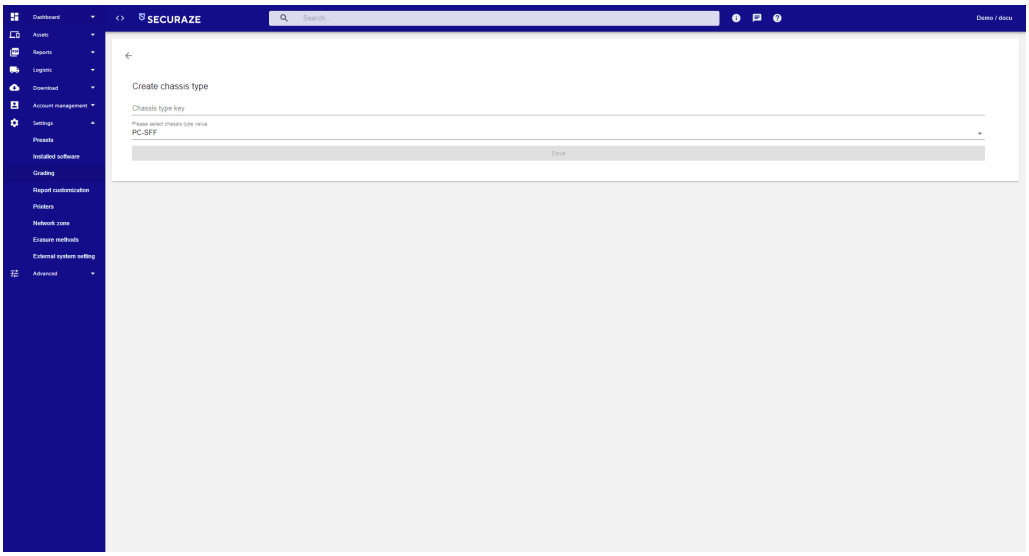
Here you can see a list of all Chassis Types.


© 2026 Securaze GmbH




To create a new chassis type, click on **Grading** in the Menu section and then on the **Tab Chassis Types**. Then choose **Create New**.

Here you enter the data of the new chassis type.




After confirming the selection by clicking **SAVE**, the newly created grade is displayed in the **Chassis Types** menu.

### 10.1.7.4 Report Customization

Geben Sie hier den Text ein.

#### 10.1.7.4.1 Logos

In the menu **Settings - Report Customization**, Tab **Logos** you can create new logos, edit existing ones and delete them.


© 2026 Securaze GmbH

### 10.1.7.4.1.1 Create new Logo

To create a new logo to be displayed on the deletion report, click **Settings - Report Customization** in the Menu section and then on the Tab **LOGOS.** There you choose **Create New**.

Here you upload the desired logo by kicking on **UPLOAD** and assign a name.

**Recommended size of the logo:**

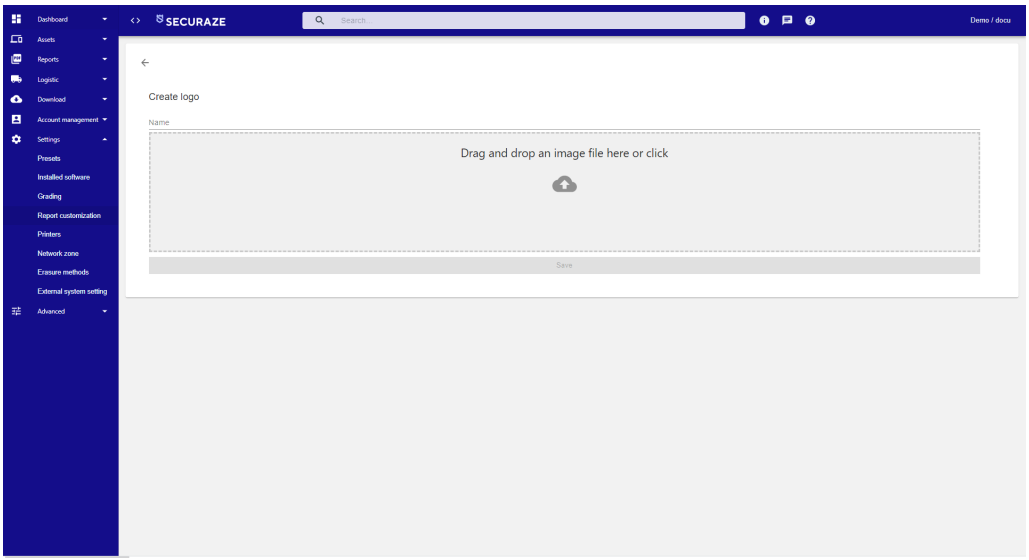
Square shaped: 512 x 512 pixel



Rectangular shaped:

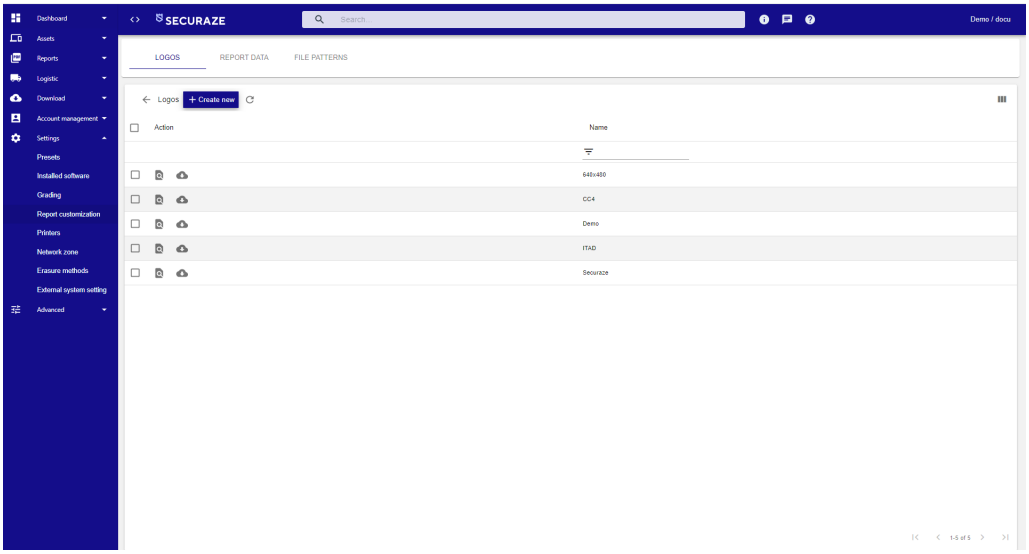
600 x 400 pixel



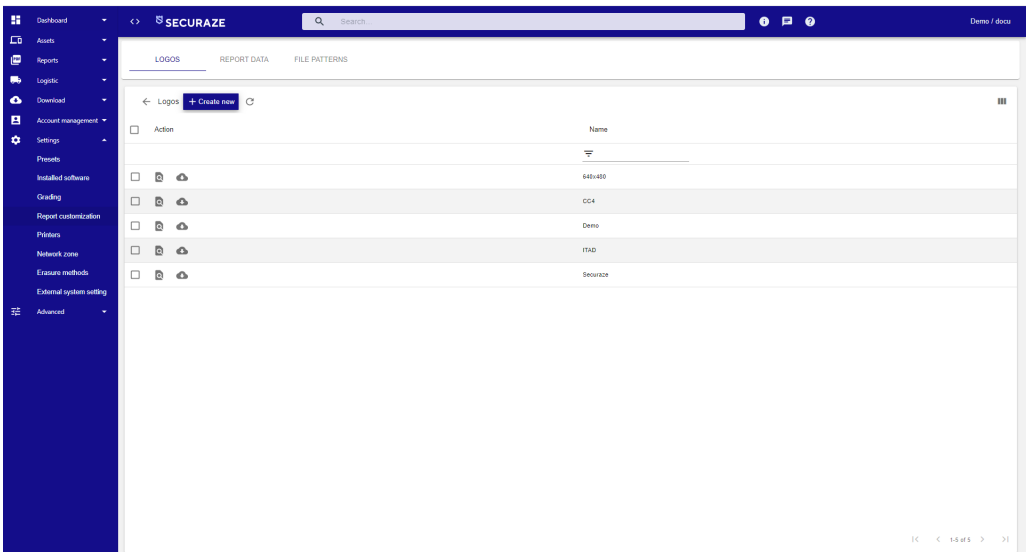

After confirming the selection by clicking **SAVE**, the newly created logo is visible in the Tab **Logos**


© 2026 Securaze GmbH



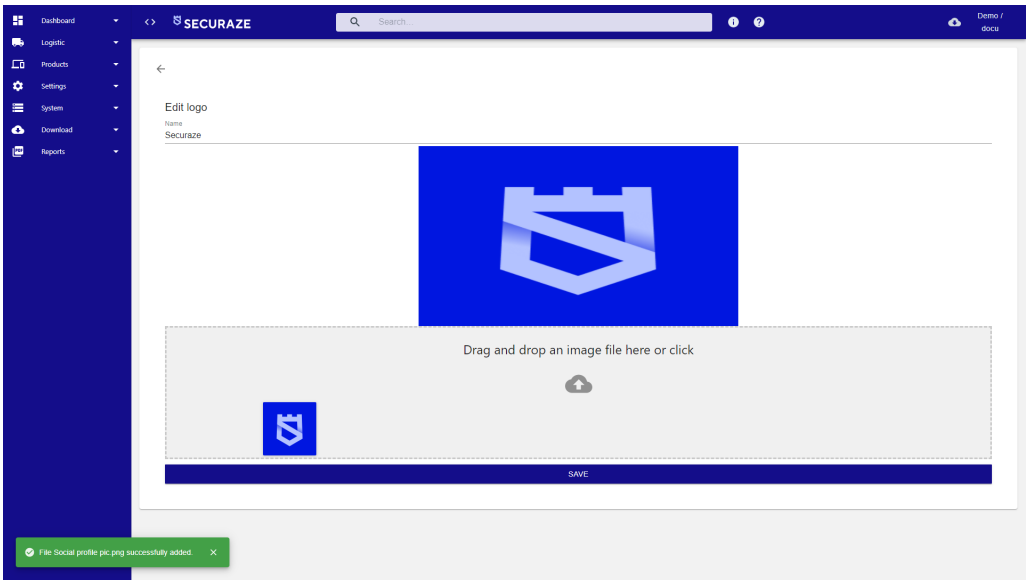

### 10.1.7.4.1.2 Edit Logo

To edit a logo, select the respective logo and click on **Logo details** .



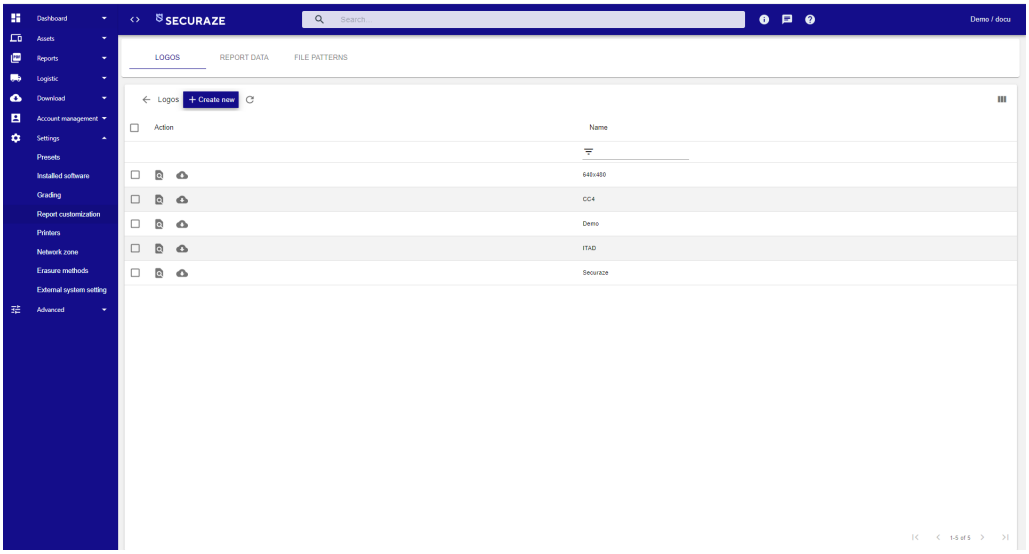

Make the desired changes and confirm them by clicking **SAVE**.


© 2026 Securaze GmbH



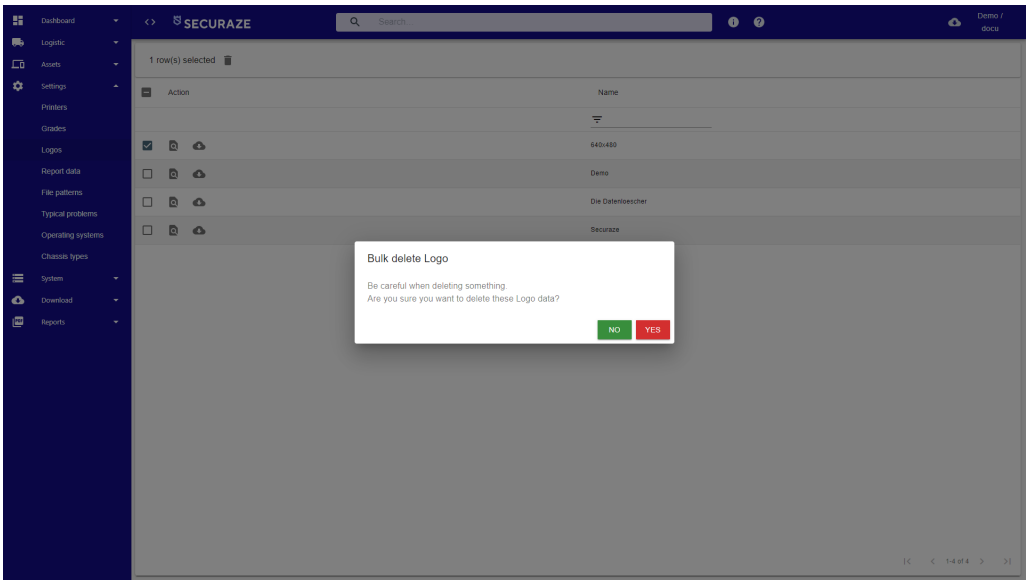

### 10.1.7.4.1.3 Delete Logo

To delete a logo, select the respective logo and click on **Remove all selected Logos**.




Confirm the erasure by clicking on **YES**.


© 2026 Securaze GmbH



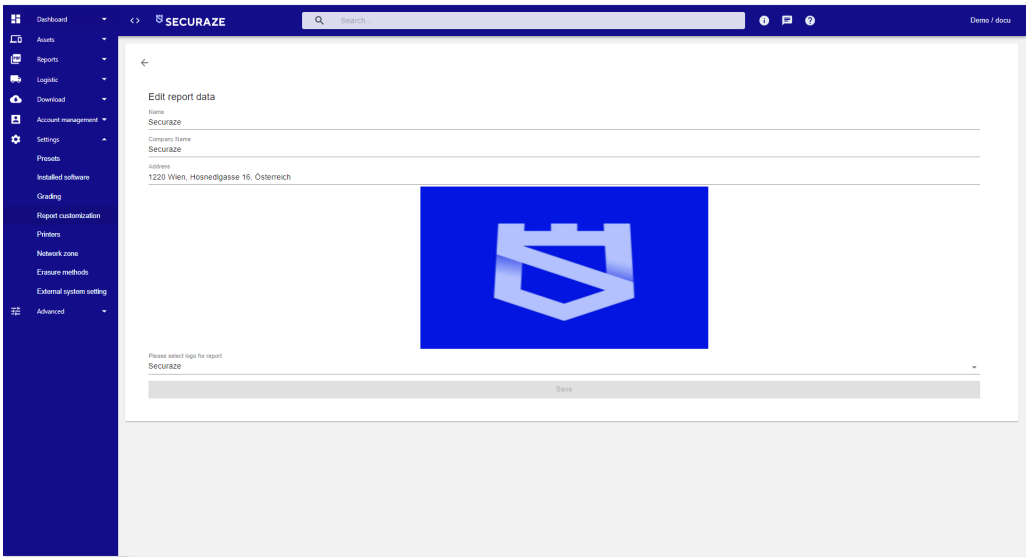

### 10.1.7.4.2 Report Data

In the **Settings - Report Customization** menu, Tab **REPORT DATA**, you can create new report data, edit existing report data, and delete report data.

#### 10.1.7.4.2.1 Create new Report Data

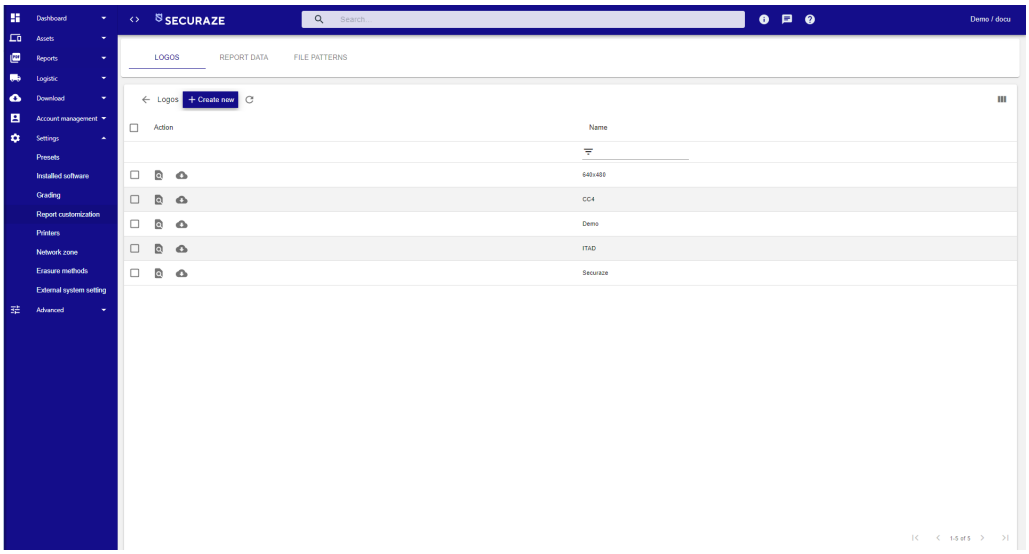
To create new report data, click **Settings - Report Customization** in the Menu section and then on the Tab **REPORT DATA.** There you choose **Create New**.

Here you enter the data to appear on the deletion report and select the logo.




After confirming the selection by clicking **SAVE**, the newly created report data can be viewed in the Tab **Report data.**

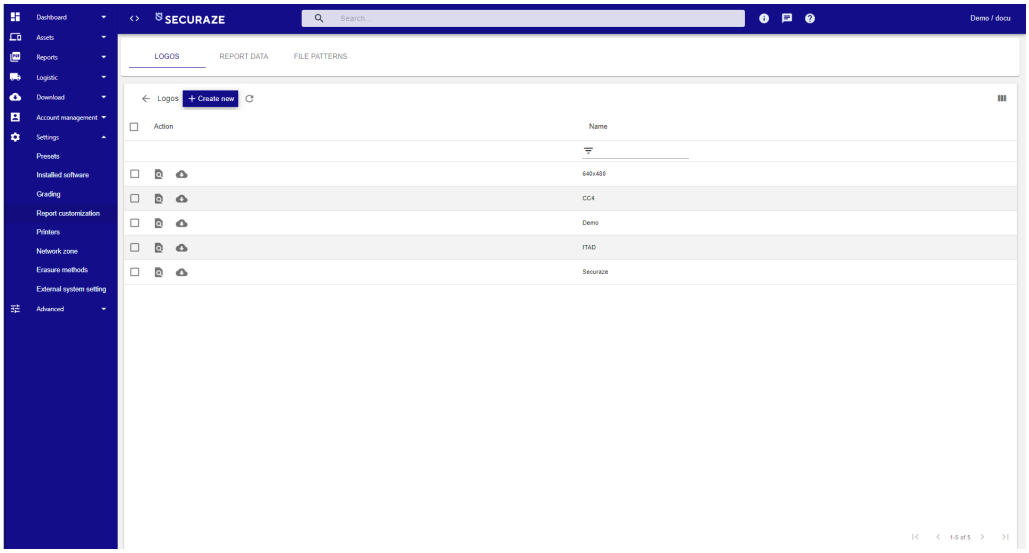

© 2026 Securaze GmbH




### 10.1.7.4.2.2 Edit Report Data

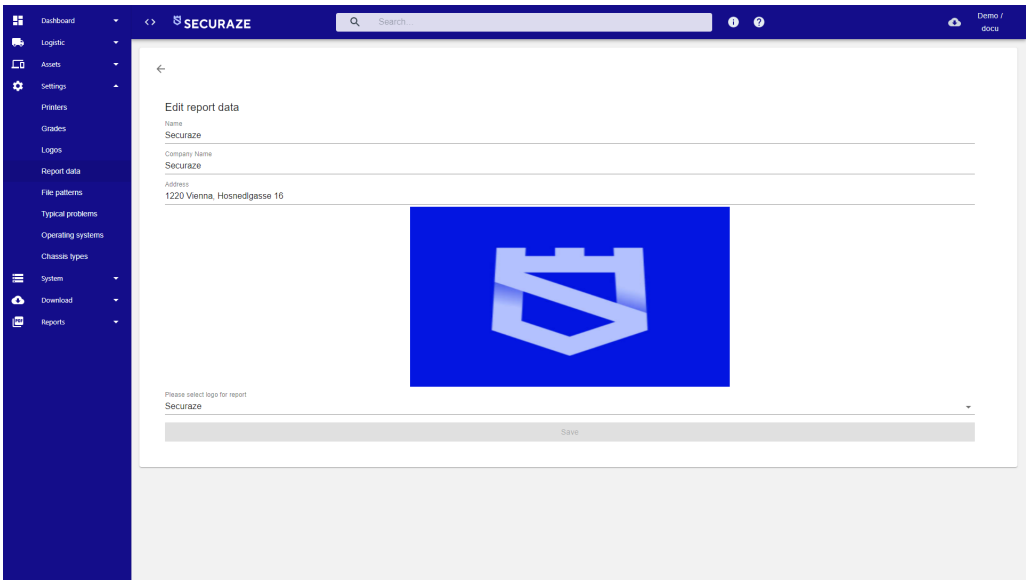
To edit report data, select the respective report data and click on **Report Data details**

.



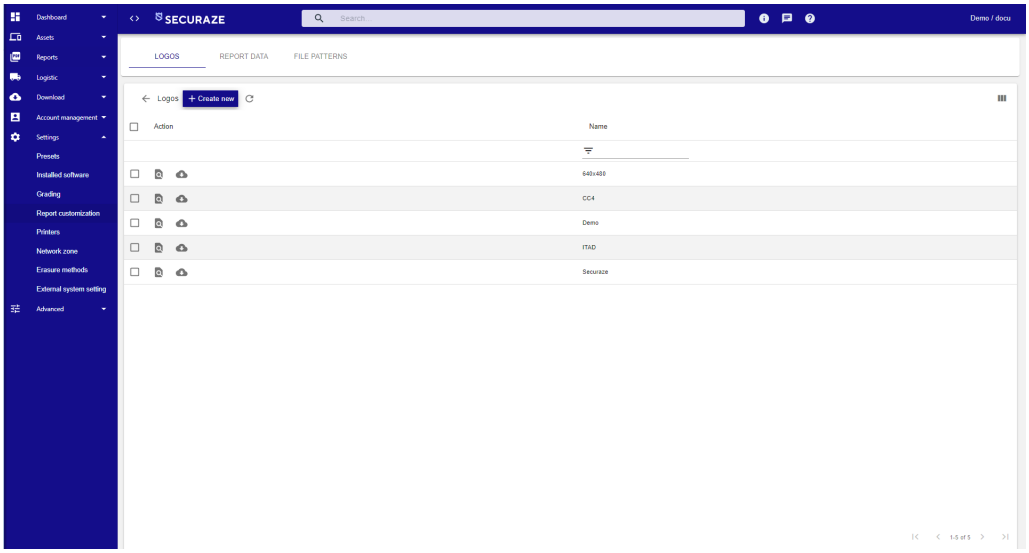

Make the desired changes and confirm them by clicking **SAVE**.


© 2026 Securaze GmbH



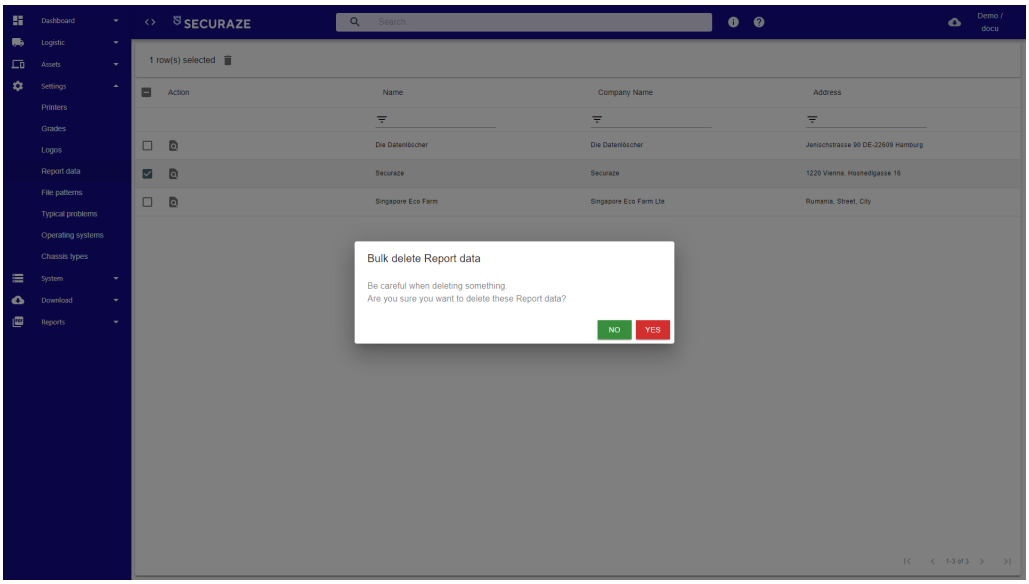

### 10.1.7.4.2.3 Delete Report Data

To delete report data, select the relevant report data and click **Remove all selected Report Data** .




Confirm the erasure by clicking on **YES**.


© 2026 Securaze GmbH



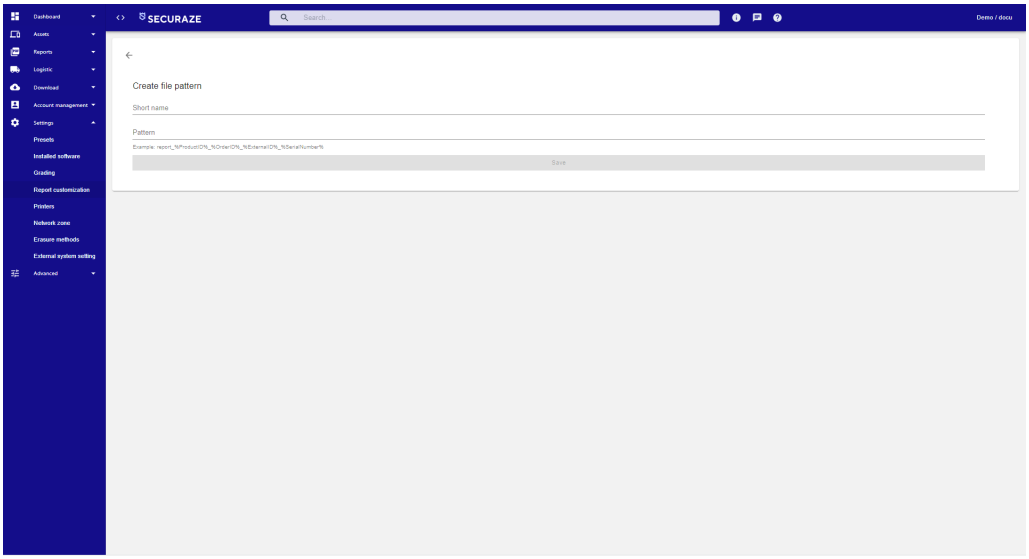

### 10.1.7.4.3 File Patterns

In the **Settings - Report Customization** menu, Tab **FILE PATTERNS**, you can create new file patterns, edit existing report data, and delete report data.

#### 10.1.7.4.3.1 Create new File Pattern

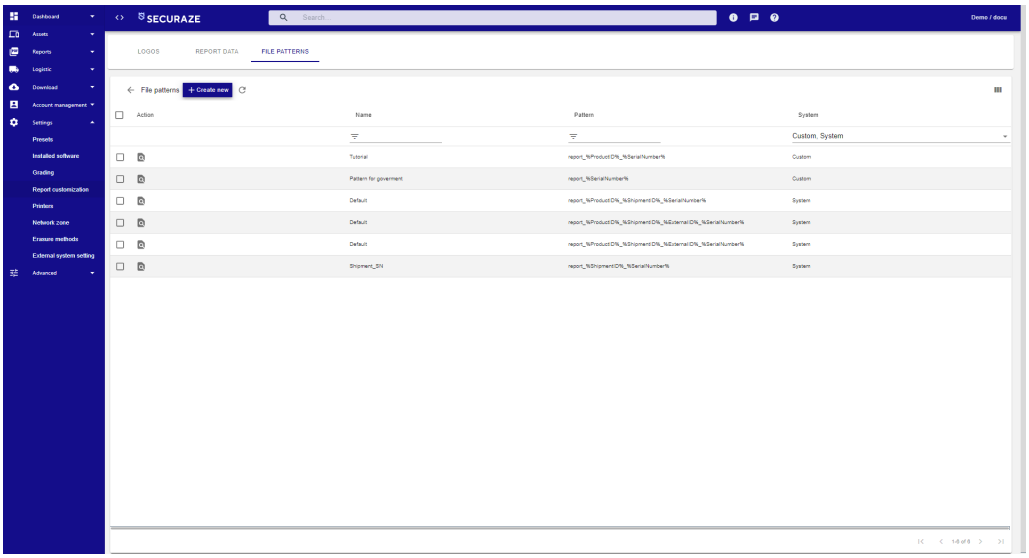
To create new file patterns, click **Settings - Report Customization** in the Menu section and then on the Tab **FILE PATTERN.** There you choose **Create New**.

Here you enter the desired file name pattern.



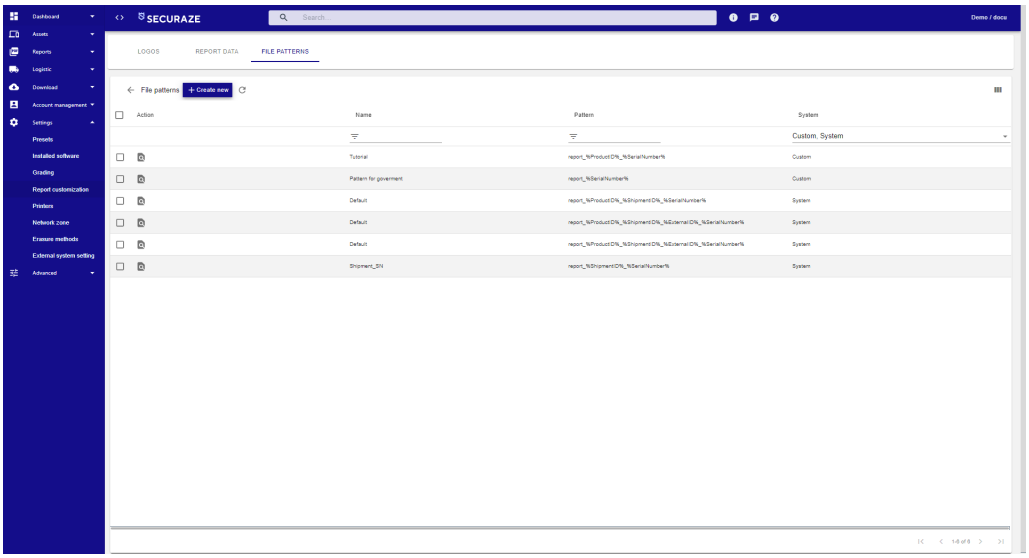

After confirming the selection by clicking **SAVE**, the newly created file pattern can be viewed in the Tab **File Pattern.**


© 2026 Securaze GmbH



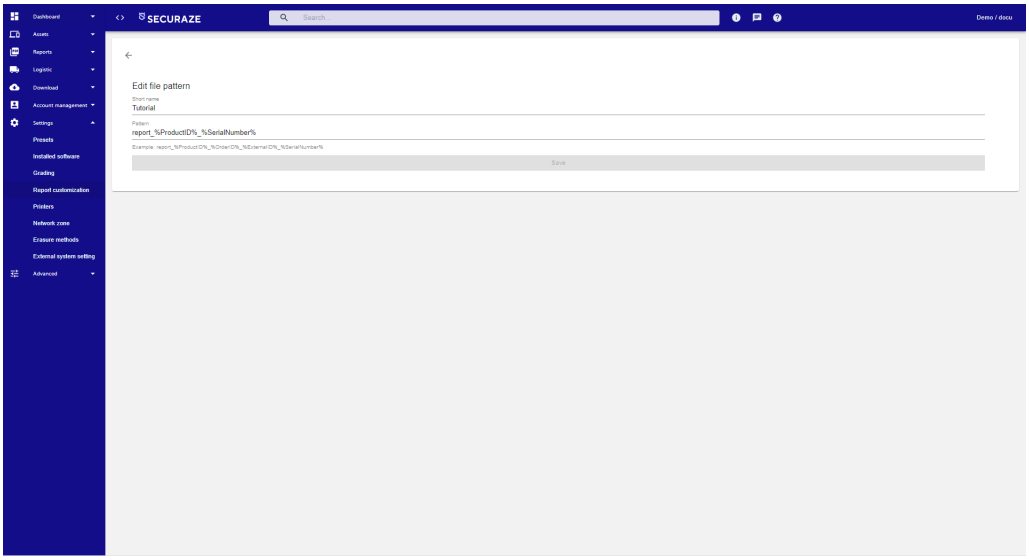

### 10.1.7.4.3.2 Edit File Pattern

To edit file patterns, select the respective file name patterns and click on **File Pattern details.**



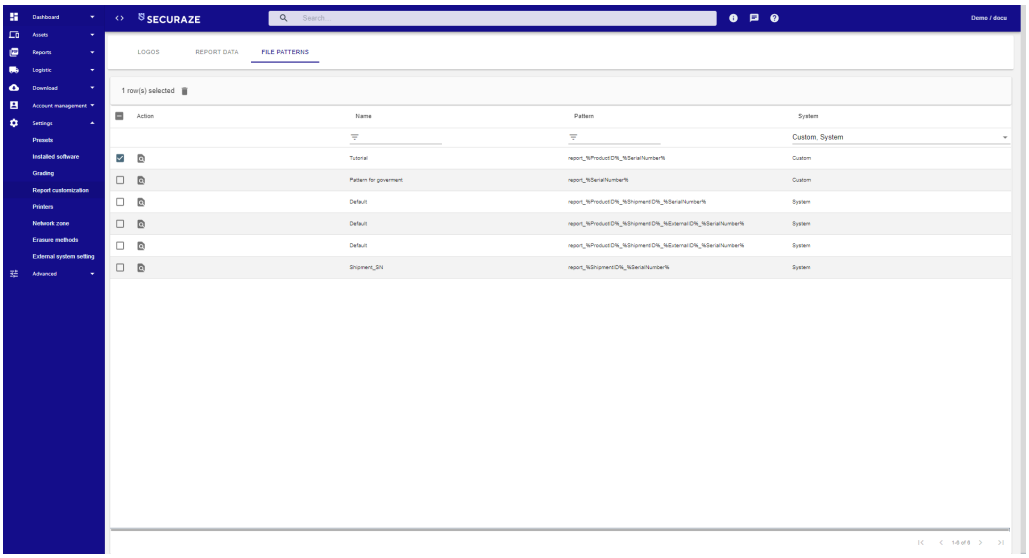

Make the desired changes and confirm them by clicking **SAVE**.


© 2026 Securaze GmbH



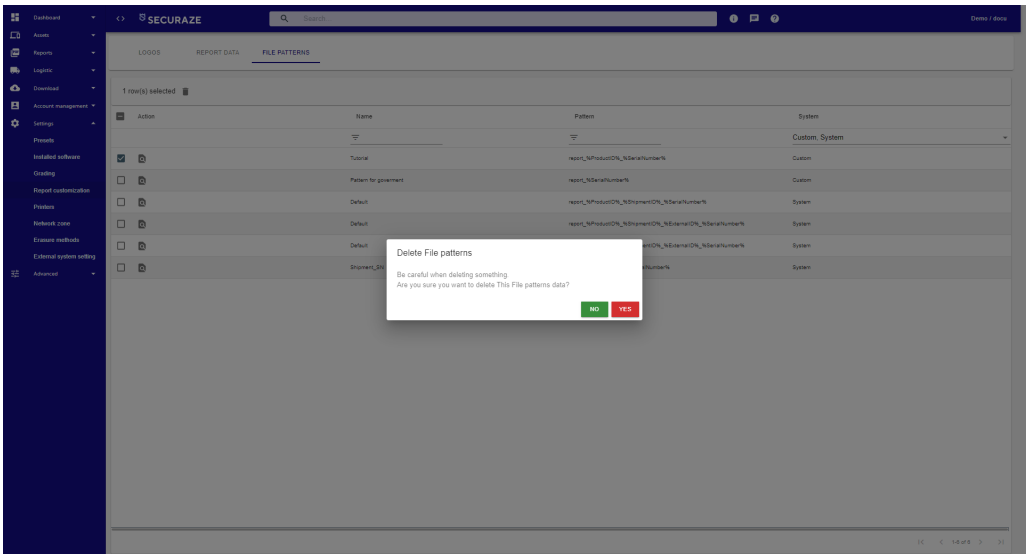

### 10.1.7.4.3.3 Delete File Pattern

To delete file patterns, select the file name patterns and click **Remove all selected File Pattern.**




Confirm the erasure by clicking on **YES**.


© 2026 Securaze GmbH




### 10.1.7.5 SKU

In the **SKU** menu you can see 2 tabs:

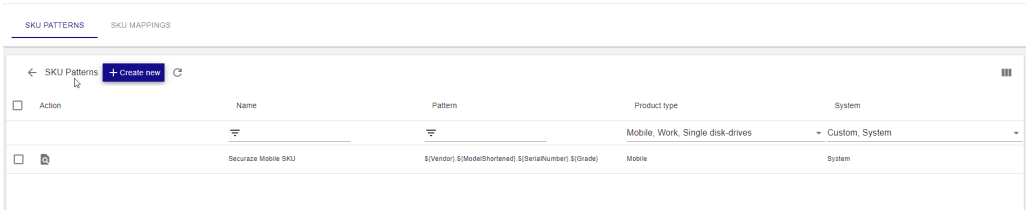
SKU Pattern for defining and editing SKU patterns.

SKU Mapping for uploading and editing SKU Mappings

#### 10.1.7.5.1 SKU Pattern

Here you can see a list of all SKU patterns.

After the pattern was created it can be selected in **Settings / Presets / Mobile or Work** (depending on the product type of the pattern)



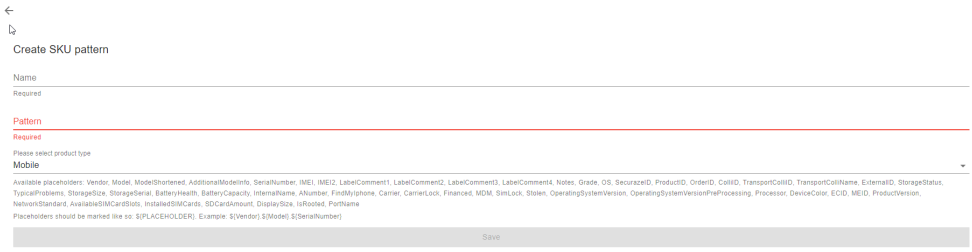

To create a new SKU pattern, click on **SKU** in the Settings-Menu section and then on the **Tab SKU Pattern**. Then choose **Create New**.

Here you enter the data of the new pattern.

After choosing a product type the list of possible usable keywords is visible.

A pattern may look like this and can use any seperator between the keywords: ${Vendor}.${ModelShortened}.${SerialNumber}.${Grade}


© 2026 Securaze GmbH

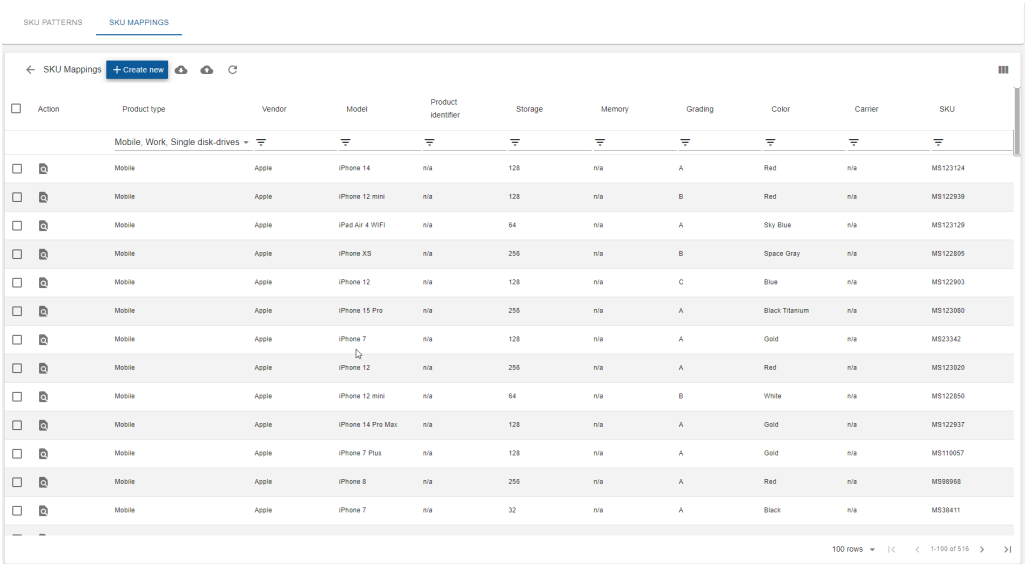



After confirming the selection by clicking **SAVE**, the newly created grade is displayed in the **SKU Patterns** menu.

### 10.1.7.5.2 SKU Mapping

Here you can see a list example SKU mappings which can be exported and imported via Excel-File or .json file.

As soon the SKU Mapping was imported or created manually it will be used after the next restart of the client.




To create a new SKU Mapping, click on **SKU** in the Menu section and then on the **Tab SKU Mapping**. Then choose **Create New**.

Its also possible to bulk import initial mappings from an prepared Excel-File.

The entries can also be edited afterwards:


© 2026 Securaze GmbH




After confirming the selection by clicking **SAVE**, the newly created grade is displayed in the **SKU Mapping** menu.

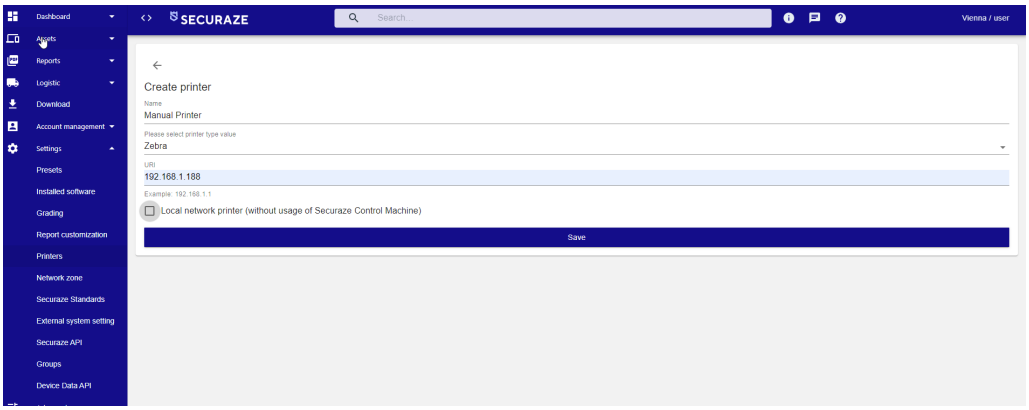
### 10.1.7.6 Printer

In the menu **Settings - Printers** you can create new printers, edit and delete existing ones.

#### 10.1.7.6.1 Creating a new printer

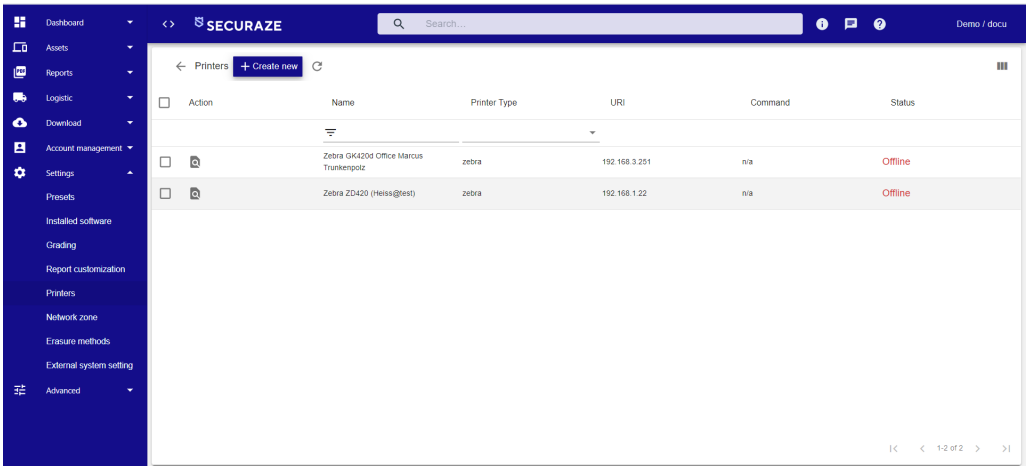
To create a new printer, click on **Printers** in the Menu area and then on **Create New**.

Here you enter the name of the printer and select the printer type from the list.




After confirming the selection by clicking on **SAVE**, the newly created printer can be seen in the menu **Settings - Printer**


© 2026 Securaze GmbH




### 10.1.7.6.1.1 Printer Type

The following GoDex printers are supported:

RT700 / RT730

RT700x / RT730x

RT700i / RT730i

RT700iW / RT730iW

RT200 / RT230

RT200i / RT230i

RT863i

GE300 / GE330

G500 with Ethernet / G530 with Ethernet

DT2x / DT4x

Most Zebra printers are supported excluding Zebra ZSB series (small office / home printers), due to their limitations.

Very common used Zebra printers are ZD420, GK420 and ZD230.

Most Brother label network printers are supported.

### 10.1.7.6.1.2 Printer network adress (URL)

IP address of the printer.

For Godex printer the Port-number needs to be specified

e.g.

```
192.168.1.10:9100
```

For Zebra printers just the IP-Adresss needs to be specified


© 2026 Securaze GmbH

e.g.

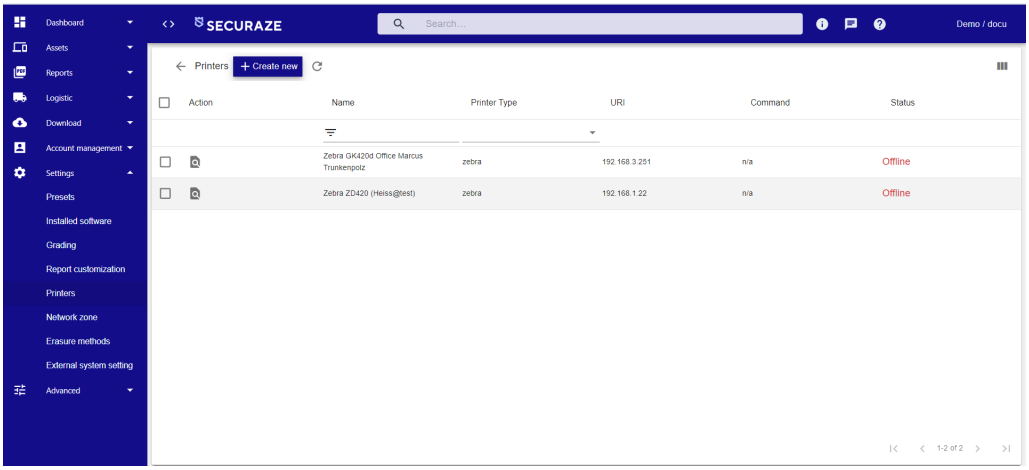
192.168.1.215

### 10.1.7.6.1.3 Direct connected USB printer

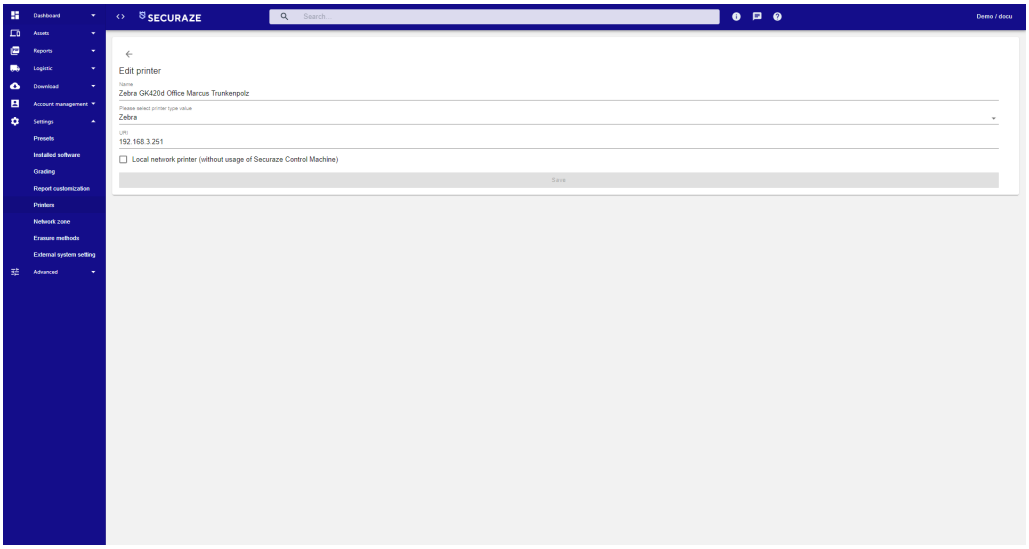
Directly connected printers.

### 10.1.7.6.2 Edit printer

To edit a printer, select the respective printer and click on **Printer details.**



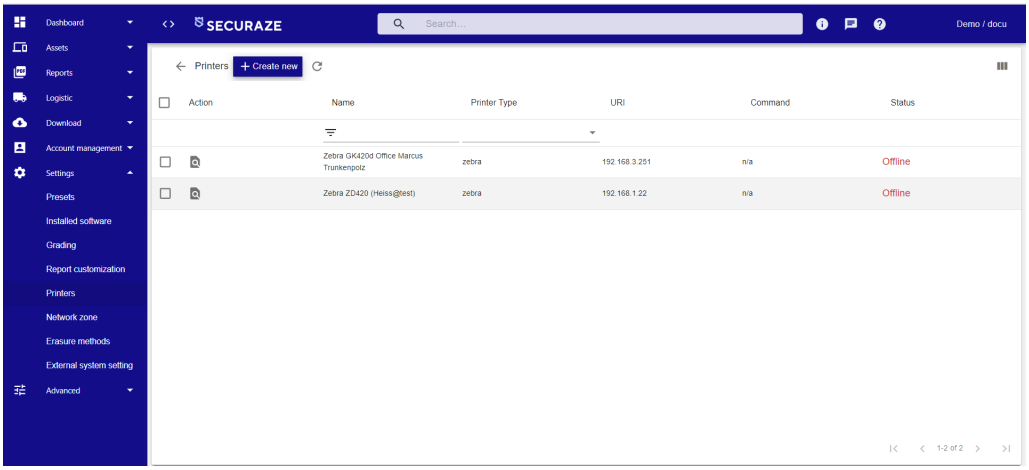

Make the desired changes and confirm them by clicking **SAVE**.



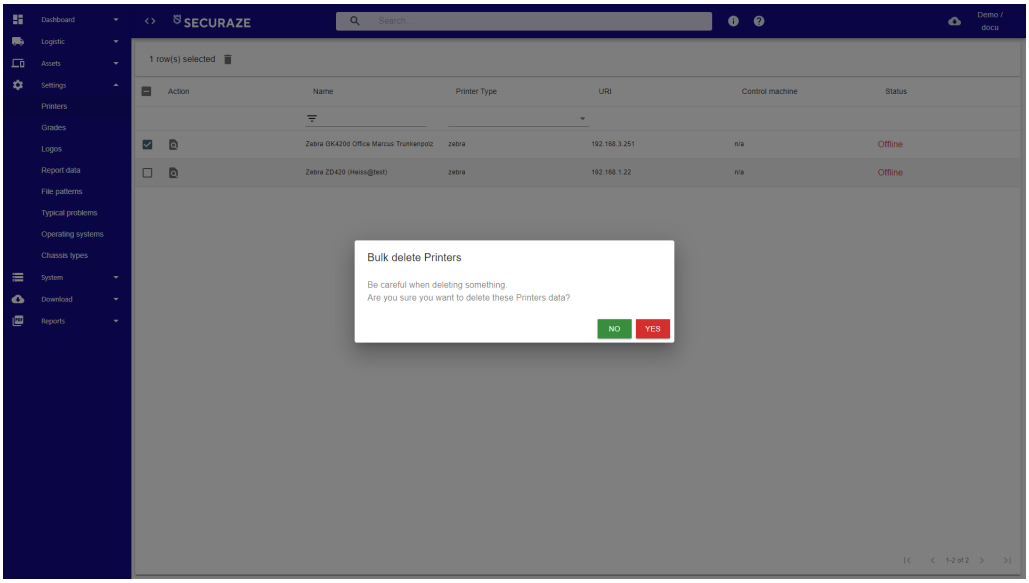

### 10.1.7.6.3 Delete printer

To delete a printer, select the printer and click **Remove all selected Printer**.


© 2026 Securaze GmbH




Confirm the erasure by clicking on **YES**.




### 10.1.7.7 Network Zone

Creating a Network Zone has several advantages:

- Time saving for the operator during login process: reduce the length of the usernames.

If the login happens within a network zone users can omit the namespace/domain - so instead of user@company.com / user@company-securaze-namepsace they just write "user"

- It is possible to allow or deny logins from specific IP addresses:

customers can e.g. choose that the login is only allowed from within their facilities

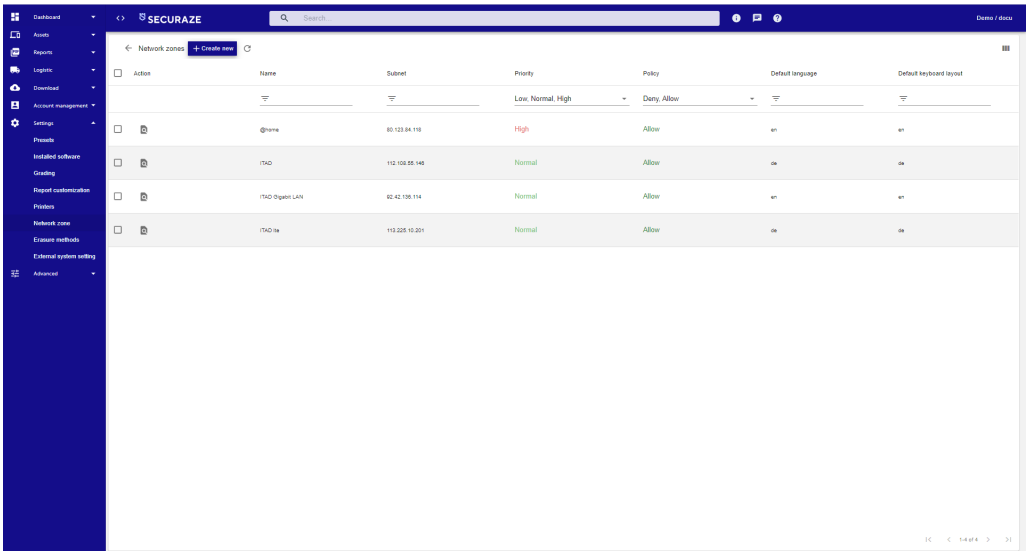
this can be also limited or extended per user

- You can define the default language per network zone region (e.g. one facility in English, another in Chinese)
- If a device is booted within network zone, remote support is possible before login.


© 2026 Securaze GmbH

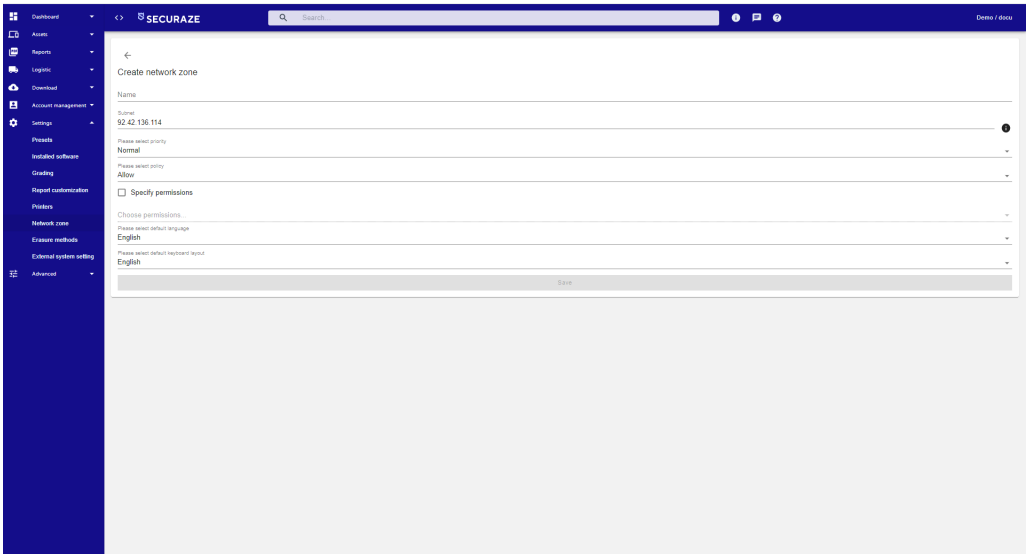
- Chromebook erasure requires network zone a pre-requesite to find the chromebooks within the company network

Here you can see an overview of all Network Zones.




To create a new network zone, click in the Menu area on **Settings - Network Zone** and then on **Create New**.

First enter the name of the new network zone.

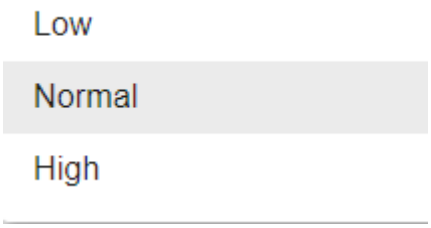



Then define the IP address or the network area including subnet of the network zone. The IP address of your external network connection is already stored here by default.

Here you can see in the right area the **note**: The network zone only works properly if a static IP address or a subnet is assigned.

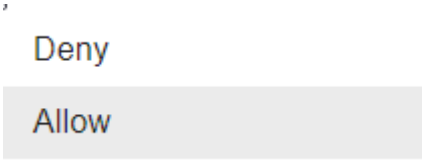

© 2026 Securaze GmbH

Set the priority of the network zone by opening the pull-down menu at **Please select priority**. Here you have 3 options to choose from:




If you create multiple network zones, the rules will be processed in this order.

Define whether the network zone should allow or prevent connections by opening the pull-down menu at **Please select rule**. Here you have 2 options to choose from:



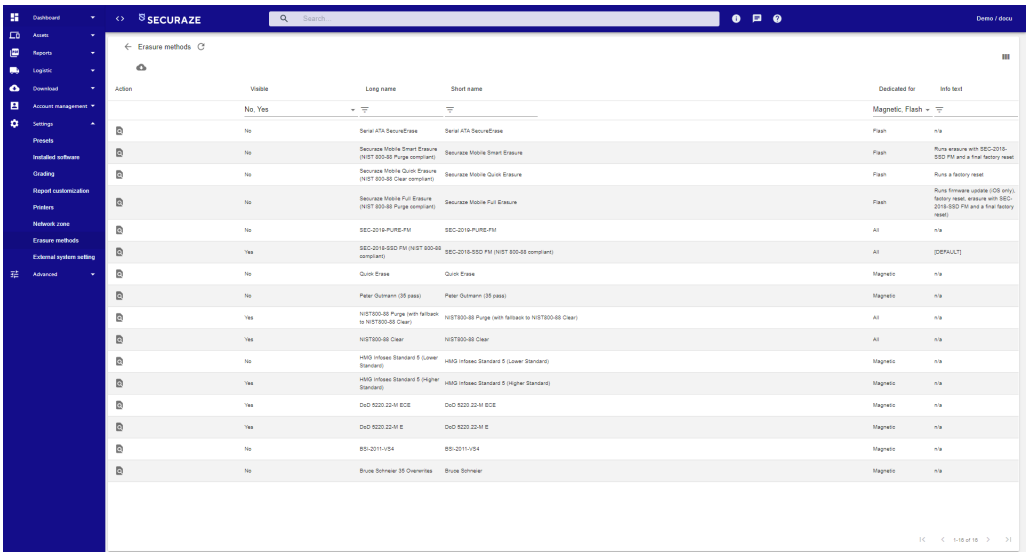

Finally, you can optionally specify permissions that should apply in this network zone.

To do this, check the box **Specify permissions** and then select the desired permissions from the pull-down menu.

Click on **Save** in the bottom right area to confirm your entries.

### 10.1.7.8 Securaze Standards

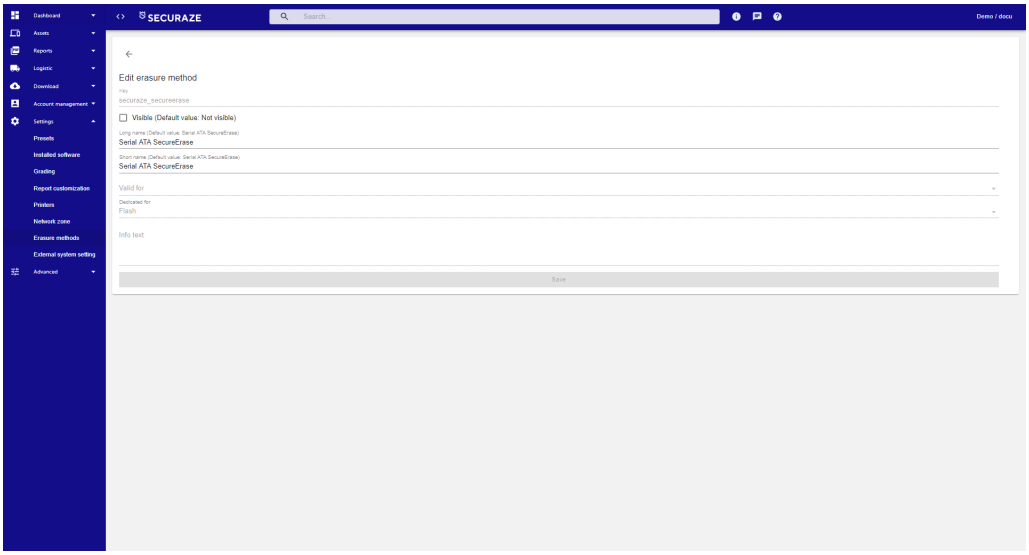
Here you can see an overview of all Erasure Methods.





© 2026 Securaze GmbH

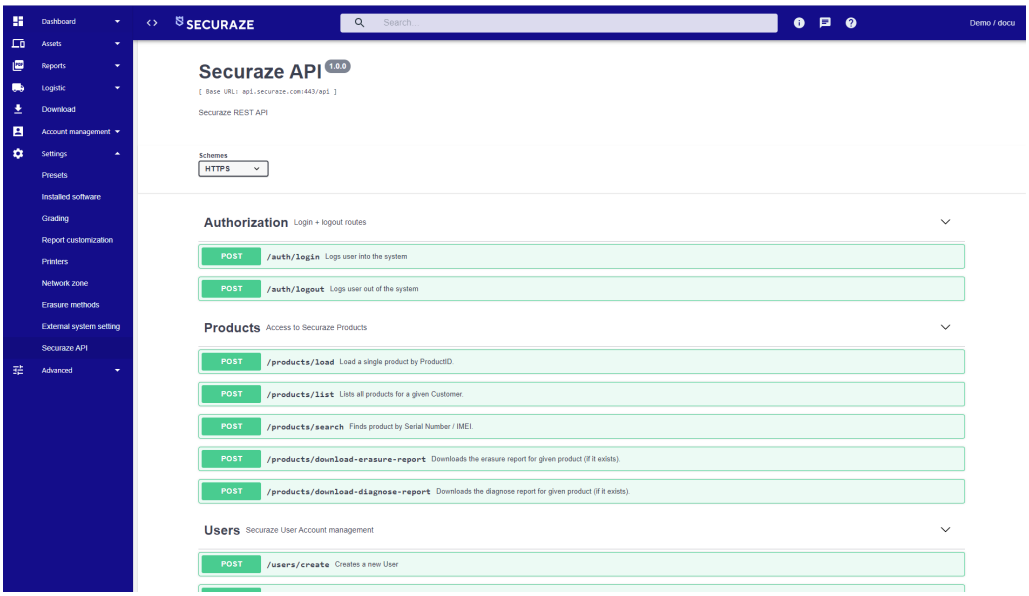
To edit an erasure method, select the respective erasure method and click Erasure Method Details.




Make the desired changes and confirm them by clicking **SAVE**.

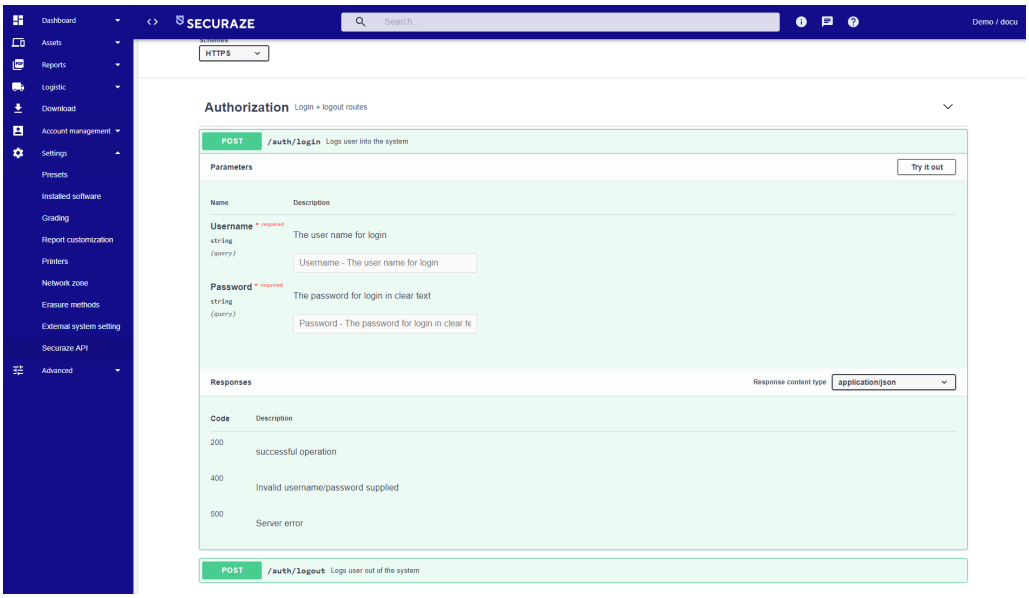
### 10.1.7.9 Securaze API

In the menu **Securaze API** you can find a list of all API calls and the documentation.




To open the details, click on the desired API.


© 2026 Securaze GmbH




Here you have the possibility to try out the API by entering the respective parameters and clicking on **Try it out**.

First you have to log by entering your username and password and click Execute.

You will then receive a token in the code that will be automatically inserted in the rest of the APIs.

To use the APIs, you need your customer ID, which you can request from the Securaze support team.

There are APIs in the following categories:

**Authorization**: Here you can login and logout.

**Products**: Here you can load, list and search for products and also download erasure reports.

**Users:** Here users can be created, listed, updated and deleted.

**Complete reference document:** a comprehensive, portable reference of all external API endpoints ("Securaze External API — Complete Reference", English and German, including authentication, all endpoint groups, worked examples and testing guidance) is available from Securaze. The interactive documentation on this page is always authoritative for your environment.


© 2026 Securaze GmbH

### 10.1.7.9.1 Authentication & conventions

All external API endpoints are POST and accept/return JSON. Parameters can be sent as JSON body (recommended) or as query-string - both work for every endpoint.

#### Base URL

The base URL of the standard Securaze cloud is https://api.securaze.com/api. Dedicated environments use their own base URL - you find the correct one together with the interactive documentation in your Dashboard under Settings > Securaze API.

#### Authentication

Every request must contain:

• ActiveCustomerID - your Securaze customer id (always required)

• ApiKey - your license API key (server-to-server), OR

• Token - a session token from POST /auth/login (Username + Password); invalidate with /auth/logout

#### Conventions

• Response envelope: { status, message, succeeded, error, result }

• List endpoints support Page/PageSize, Filters (same structure as the Dashboard grids) and, where supported, OrderField/OrderDirection

#### Naming (logistics)

The API paths use internal names. Mapping to the product terminology:

• logistic/order = Pickup Order

• logistic/transport-colli = Lot (incoming)

• logistic/colli = Sale Lot

The aliases /logistic/lot/list and /logistic/sale-lot/list exist but are deprecated - prefer the primary paths.

### 10.1.7.9.2 Products

Endpoints for devices and their reports:

• /products/load - load a single product by ProductID

• /products/list - list products (Filters, paging, ProductType, sorting)

• /products/search - find a product by serial number / IMEI (SearchInput)

• /products/download-erasure-report - download the erasure report (PDF)

• /products/download-diagnose-report - download the diagnose report (PDF)


© 2026 Securaze GmbH

• /products/download-xls-report - upload an Excel file with conditions, receive the matching product list as XLS

• /products/check-esn - run an ESN/IMEI check (e.g. GSMA, Apple GSX, Samsung). Note: billed per check.

### Typical problems

Manage the typical problems flagged on a device (identify by ProductID or SerialNumber; problems by TypicalProblemIDs and/or Codes):

• /products/typical-problem/list - current problems

• /products/typical-problem/add - add (idempotent)

• /products/typical-problem/remove - remove, e.g. after repair

• /products/typical-problem/set - replace the whole set (empty = clear all)

Problems are matched only within the device's own category.

## 10.1.7.9.3 Users

User administration via API:

• /users/create - create a user (FirstName, LastName, Email, Username, Password, PhoneNumber, Status, optional SendEmailNotification)

• /users/list - list users (Filters, paging)

• /users/load - load by UserID

• /users/save - update a user

• /users/delete - delete by UserID

• /users/update-balance - per-user licensing: IndividualLicensingEnabled, WorkBalance, MobileBalance, RemoteBalance, CurrencyBalance

## 10.1.7.9.4 Logistics

Pickup Orders (/logistic/order/…): create, load, list, save, delete. Fields: Name, Description, Type, Status, DefaultLanguage.

Lots (/logistic/transport-colli/…): create, load, list, save, delete. Fields: Name, Description, Location, Order (assignment), ArrivedDate.

Sale Lots (/logistic/colli/…): create, load, list, save, delete. Fields: Name, Description, ColliTypeID, HolderColliID, WarehouseID, GradeIDs, AllowedProductTypeIDs, Status.

Typical intake chain: create a Pickup Order, then create the Lot with Order set to the new OrderID and the ArrivedDate.


© 2026 Securaze GmbH

### 10.1.7.9.5 Integrations & webhooks

Manage external-system connections - the same records as Settings > External system setting:

• /integration/list - list integrations / webhooks

• /integration/load - load by ExternalSystemSettingID

• /integration/create - create (Name, Direction, Type, ServiceType, Settings, Active)

• /integration/save - update

• /integration/delete - delete

An Outbound integration with a URL in Settings acts as a webhook and receives processing events.

### 10.1.7.9.6 Testing & errors

#### Testing your integration

• Use the interactive documentation in the Dashboard (Settings > Securaze API) first: log in there and execute each endpoint with try-it-out - the token is inserted automatically. Then copy the working request into your code.

• Start read-only: validate search / list / load before any create / save / delete.

• List first to see the real Codes / IDs of your account before writing.

• typical-problem/add is idempotent; create endpoints are not - guard against retries.

• products/check-esn consumes credits - test with a single device.

#### Errors

All errors use the standard envelope with succeeded: false and an error object:

• 200 - success

• 400 - malformed request / missing required field

• 401 - authentication failed (invalid ApiKey / expired Token)

• 404 - object not found (unknown id, serial, or out-of-category match)

• 5xx - server error; retry with backoff, contact support if persistent

### 10.1.7.10 Further settings

The Settings menu contains further areas:

• Groups - group users for shared permissions and easier administration (Settings > Group).

• Label templates - define the layout and placeholders of printed device and lot labels (Settings > Label template).


© 2026 Securaze GmbH

• External system settings - connect external systems such as ERP integrations (Settings > External system setting).

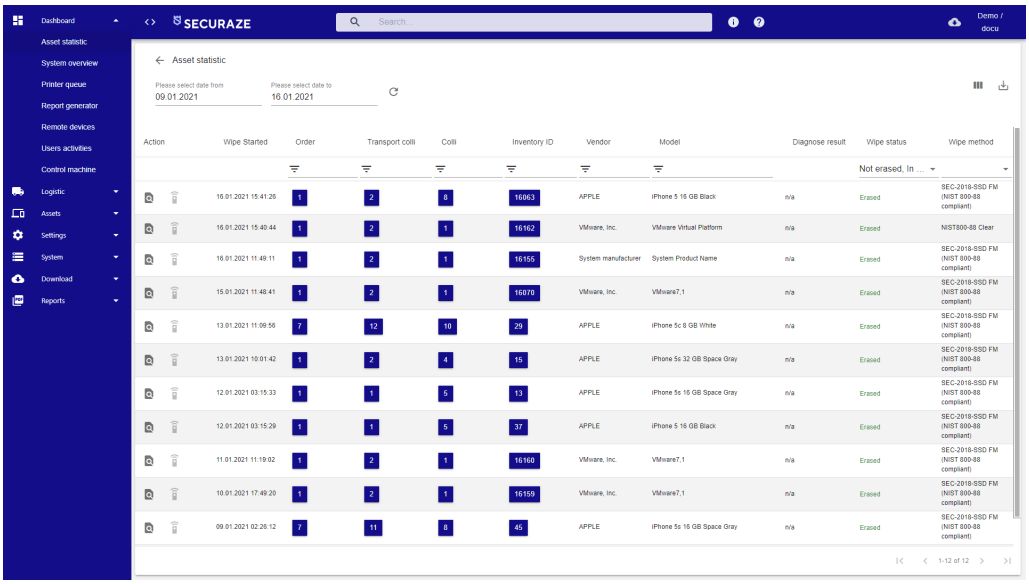
• Device Data API - configure the API used to look up device data by identifier (Settings > Device Data API).

The print queue (Print queue menu) shows all label print jobs with their status.

### 10.1.8 Statistic

The dashboard shows an overview of deleted devices in the last 24 hours.

The buttons can be used to navigate directly to the respective devices, Sale Lots or orders.





© 2026 Securaze GmbH




© 2026 Securaze GmbH