Work

SECURAZE

Administration

1 Administration

1.1 System environment

Securaze Work can be used in the following system environment.

System requirements

	Minimum Configuration	Recommended Configuration	Production Configuration (Dedicated Erasure Machine)
Dedicated for	**processing devices with 1-2 drives**	**processing devices with 1-10 drives**	**processing up to 100 drives simultaneously**
CPU	64Bit CPU	64Bit Quad-Core CPU	Dual 64Bit Quad-Core CPU (5th gen or newer)
Memory (RAM)	512 MB	1 GB	16 GB
Storage requirements	None	None	None
Resolution	1024 * 768 resolution or higher	1280 * 1024 resolution or higher	1920 * 1080 or higher
Network-Connection	1 network-port or Wifi-Module	1 network-port or Wifi-Module	1 network-port
Storage Connection	Internal, USB	Internal, USB	Internal, USB, PCI express SAS controller Card
Internet	Internet-Connection or Offline-Mode	Internet-Connection or Offline-Mode	Internet-Connection or Offline-Mode
Inputs	Keyboard and/or Mouse/Trackpad	Keyboard and/or Mouse/Trackpad	Keyboard and/or Mouse/Trackpad

Software settings

Firewall settings	
Internet connection	Permanent Internet connection is required
Securaze servers	The firewall must not block any of the Securaze pages: • https / http to *.securaze.com • https://cdn.securaze.icu • https://securazeeu.blob.core.windows.net
Remote Support	The firewall may have to be modified. To allow AnyDesk for incoming connections, add AnyDesk to the Whitelist: · *.net.anydesk.com · TCP-Ports 80, 443 and 6568
Local DNS	if local dns is used, it has to be correctly propagated · ssh port 22 in case of support issues · icmp enabled to outside world (currently 8.8.8.8 is used; will be changed to

1.2 Deployment

Securaze Work can be deployed using the following methods:

Server based:
In this case, the image of the Securaze installation is provided by PXE boot using DHCP and TFTP. (PXE boot is not available for macOS, see chapter Apple devices 91)
This deployment method allows efficient erasure of many devices in parallel.

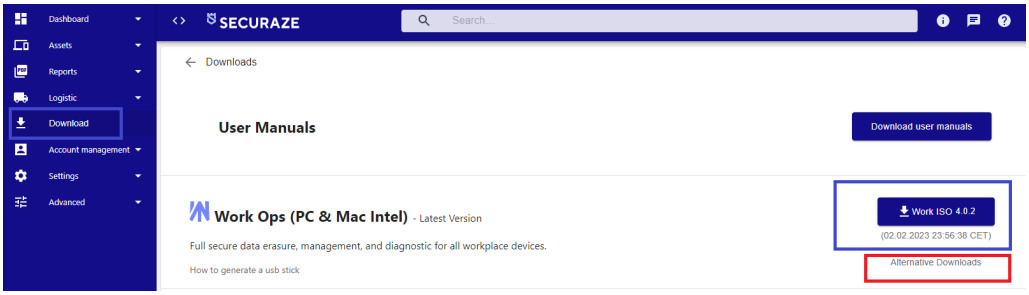
Please find details on Securaze Command in the chapter Command 25.

Portable:
In this case, the image of the Securaze installation is written to any USB stick.

1.2.1 Burning Securaze Images

Step 1: Download Securaze Work

In the menu **Download** you can download the latest Securaze Work image.
You will always find the **current version** of the software and **alternative downloads**

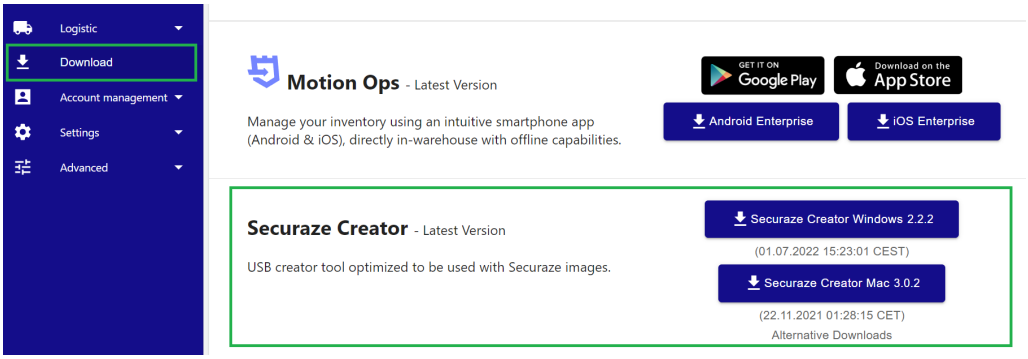


Start the download by clicking on the corresponding button.

Step 2:

In order to install the downloaded Securaze image on your operating system, you can use Securaze Creator, an application to format and create bootable USB flash drives.

Click on Downloads in the menu and on **Securaze Creator.**

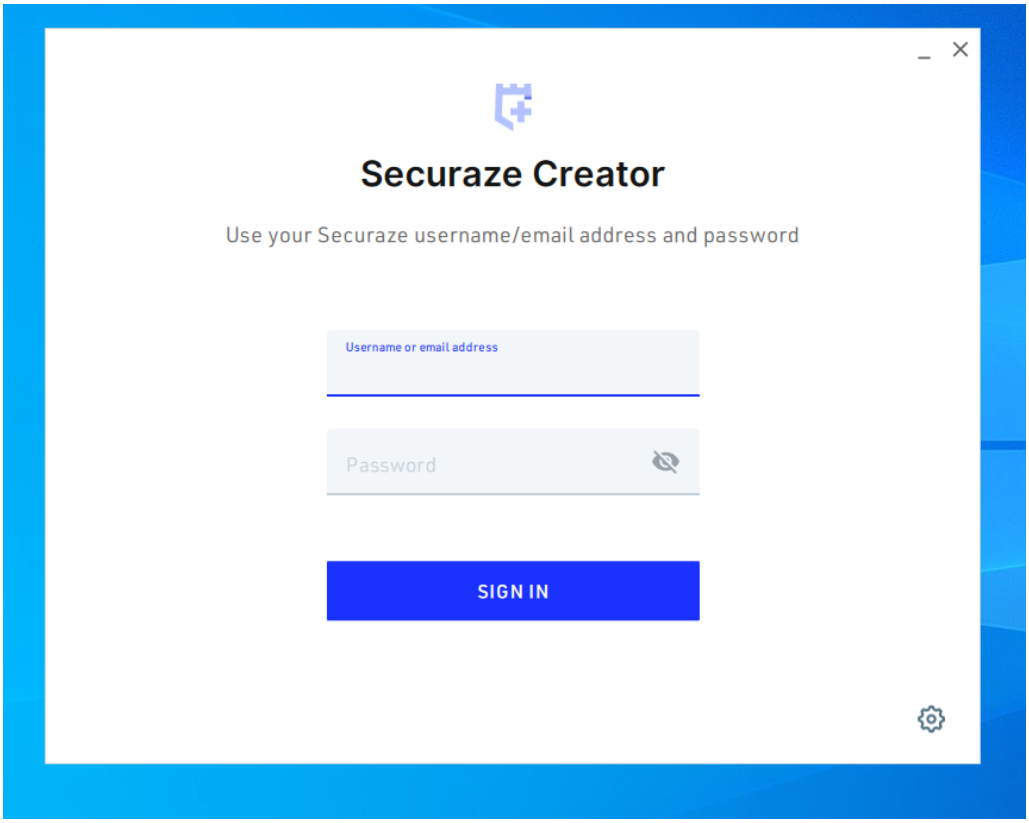


Start the download by clicking on the corresponding button.

Please note that the Securaze Creator Mac is currently supported only on Intel-based macs (M1-based macs cannot run Securaze Creator).

Securaze Creator will be downloaded to you system and installed.

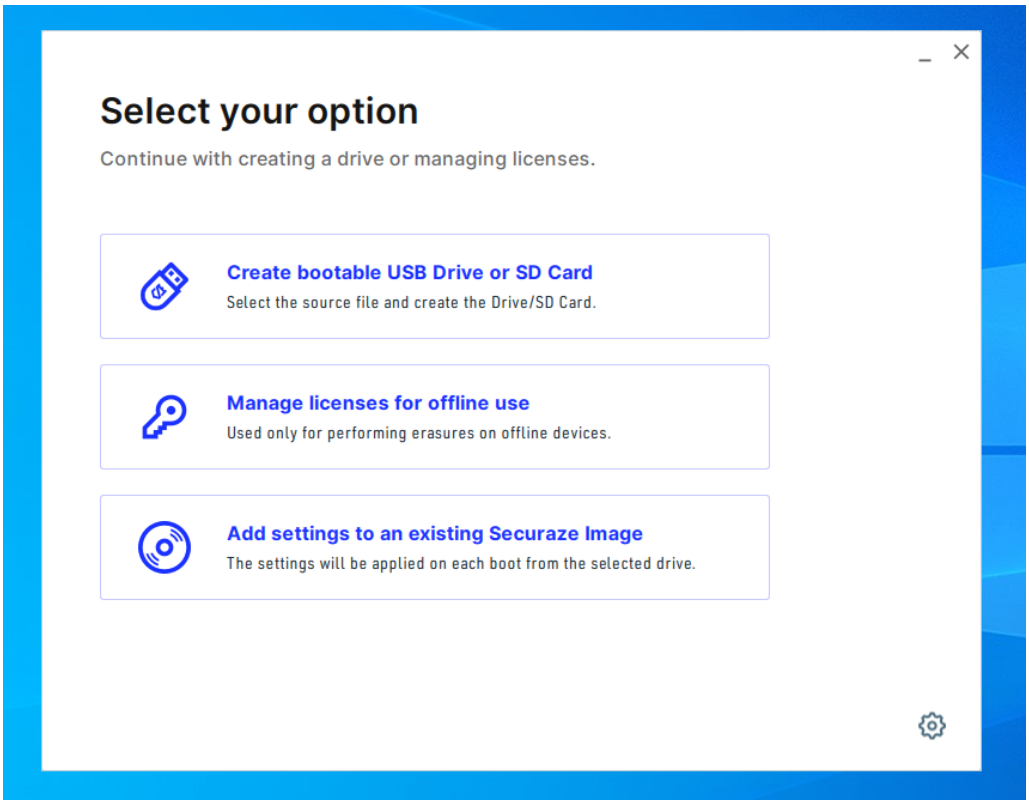
Open Securaze Creator and login with your credentials.



In the lower right corner you will see a settings icon.
This button will take you to settings, where you can change the language or the URL of the backend server (we advise you not to change this settings unless you are told otherwise by your Administrator).

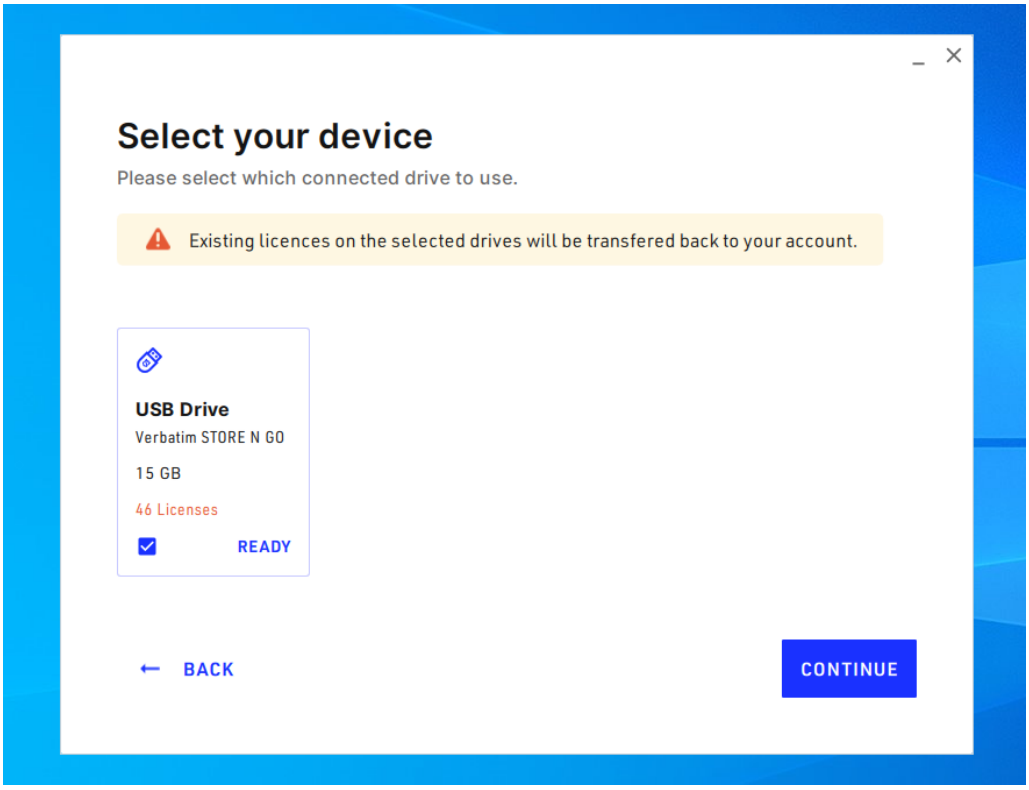
After you type in your login credentials, click on **SIGN IN** to get to the next step.

You can now choose what you want to do with your USB drive:



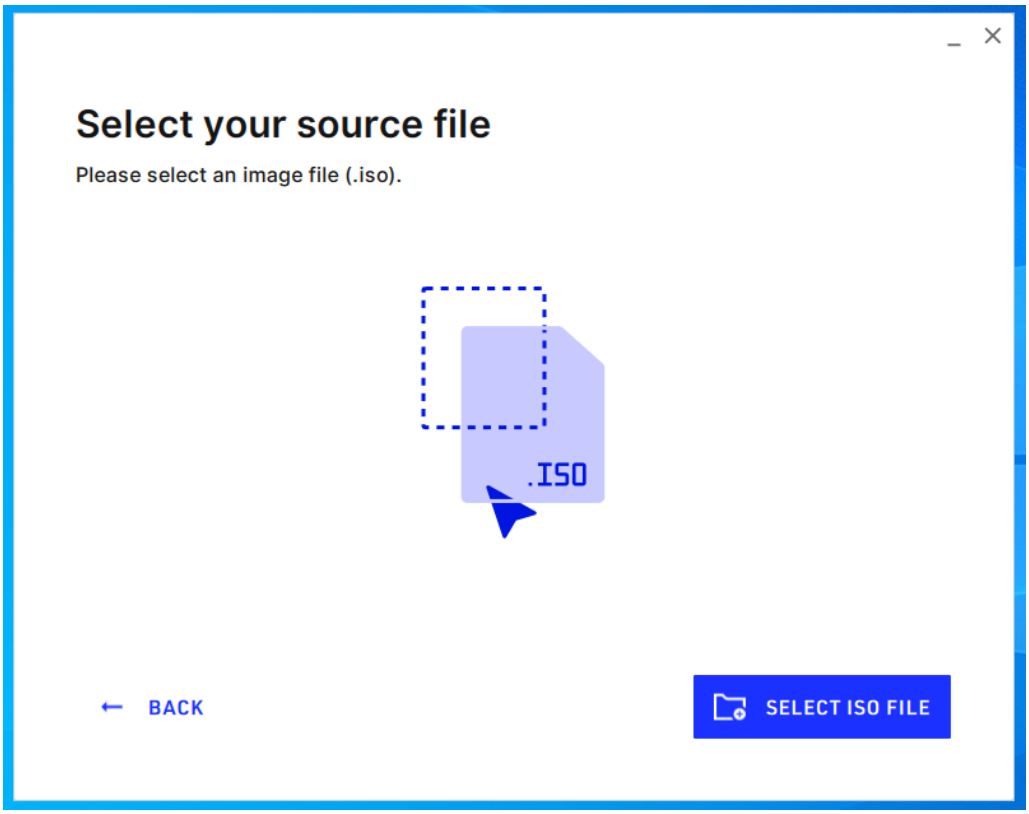
1) Create bootable USB drive or SD card

If you choose this option, in the next window you will be prompted to select the drive to which you want to burn the Securaze image:

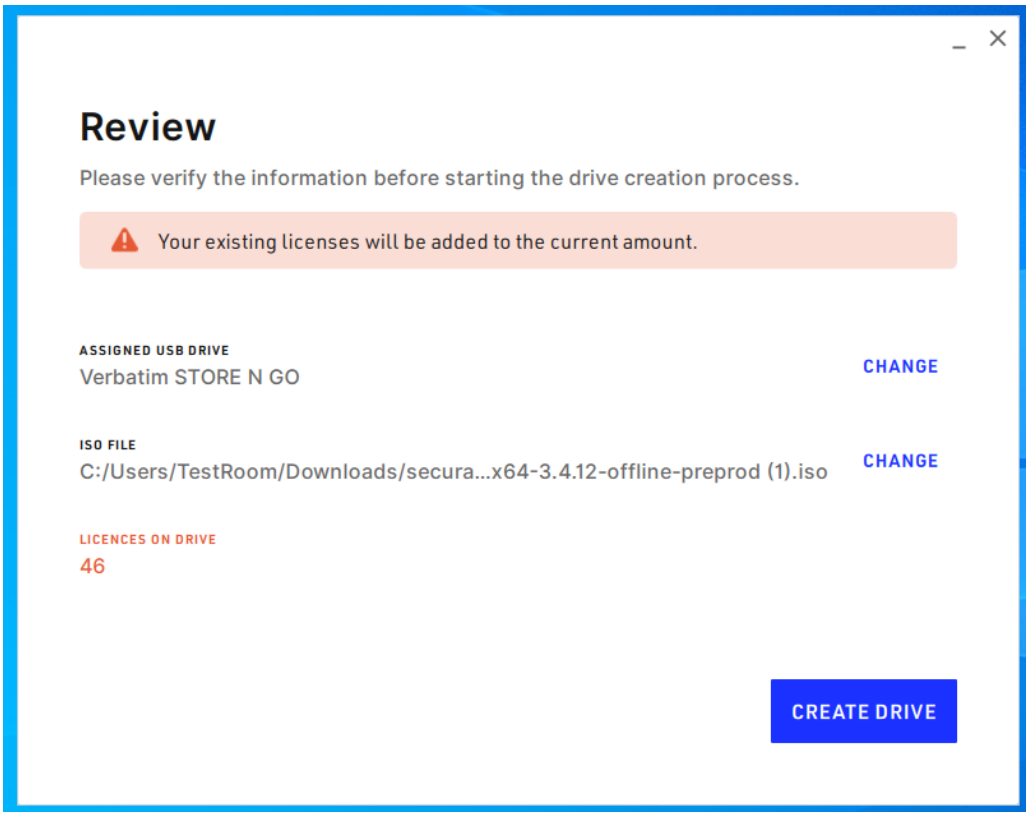


Please note that in case you already used this USB drive / SD card to burn Securaze image and added erasure licenses to it, the existing licenses will be transferred back to the account that was used for creating that USB drive / SD card. After you have selected the drive, click on **CONTINUE**.

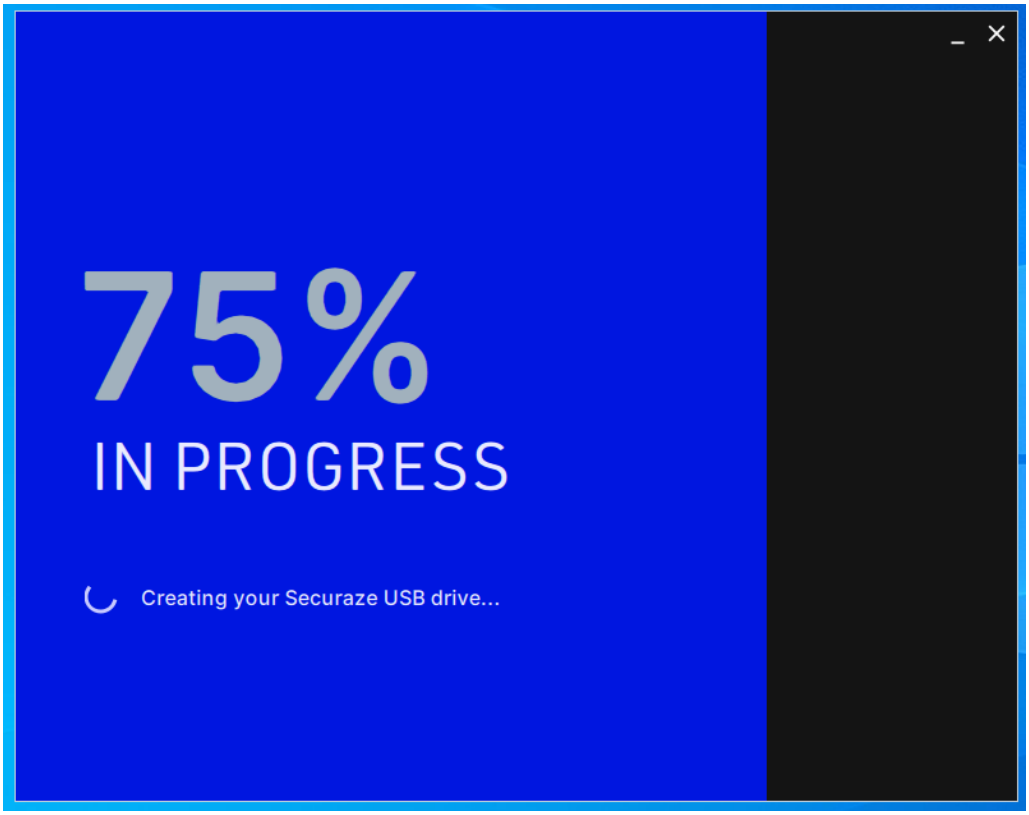
Next step is to select the Securaze image you previously downloaded from the Dashboard:



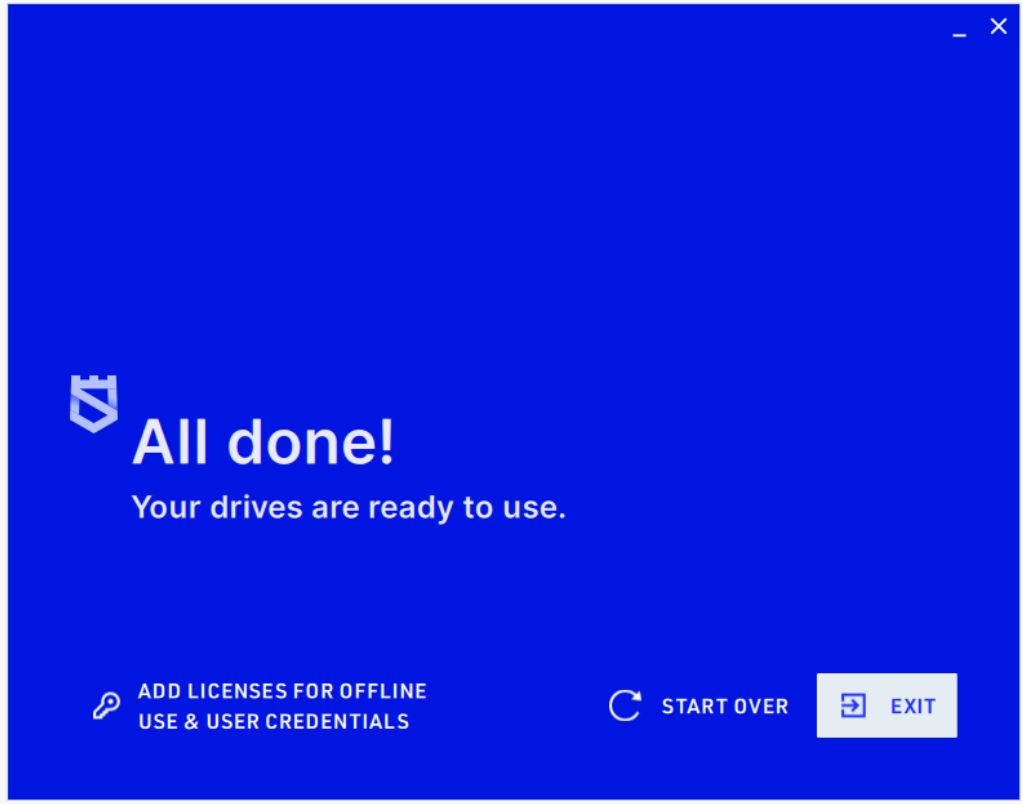
After you have selected the image, you will be asked to verify the information before starting the drive creation process.



After you have reviewed the information, click on **CREATE DRIVE** and start the process.



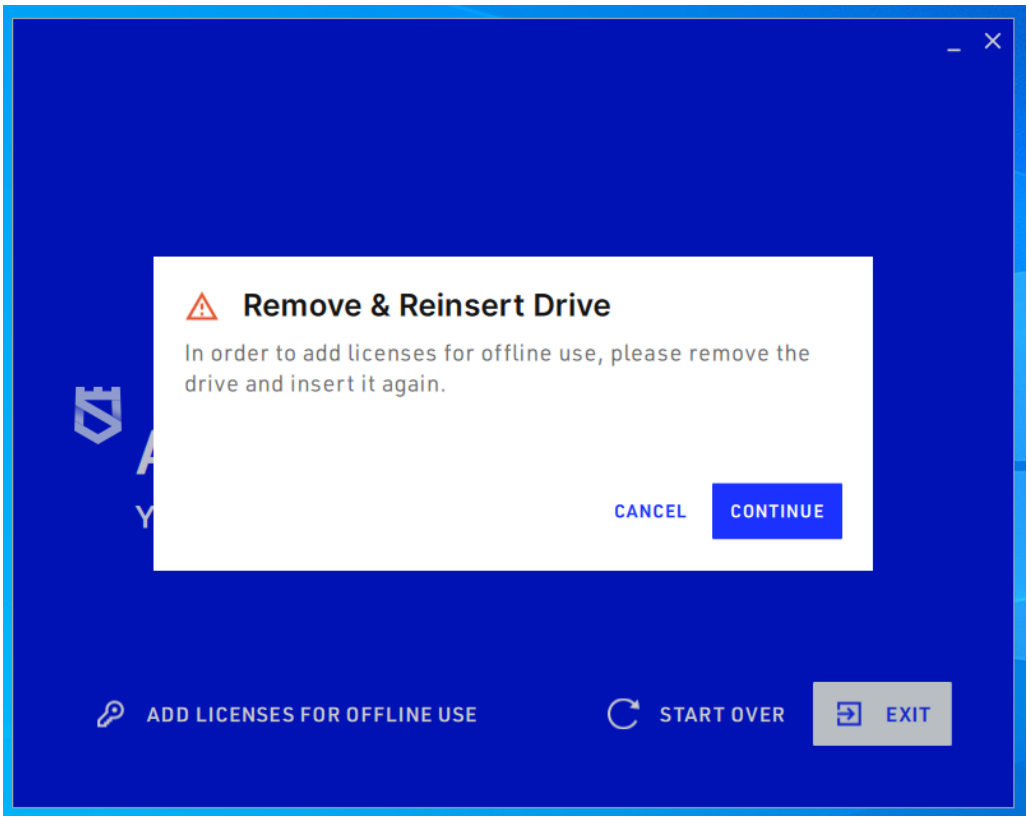
You will be able to follow the progress of drive creation. After it is completed, you will be notified.



Your drive is now ready for use.

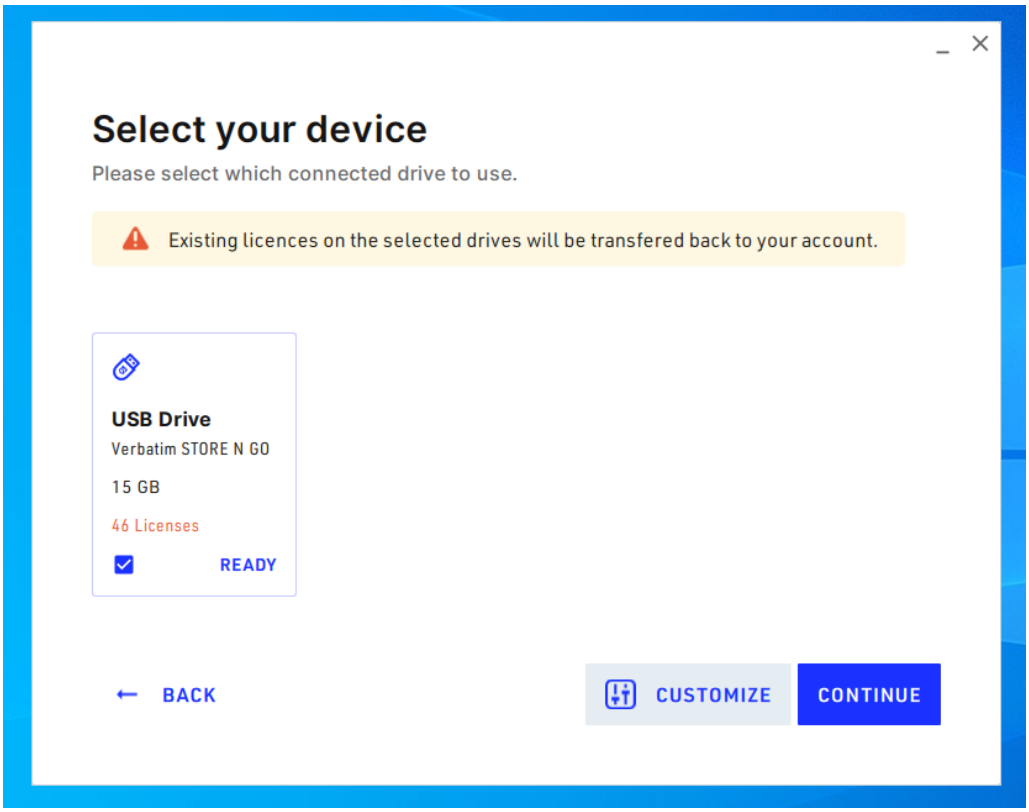
In case you wish to add the erasure licenses for offline erasure, or user credentials for auto-login, click on **ADD LICENSES FOR OFFLINE USE & USER CREDENTIALS.**

After you click on this button, you will be asked to remove the USB stick / SD card, plug it back in and click on **CONTINUE**.



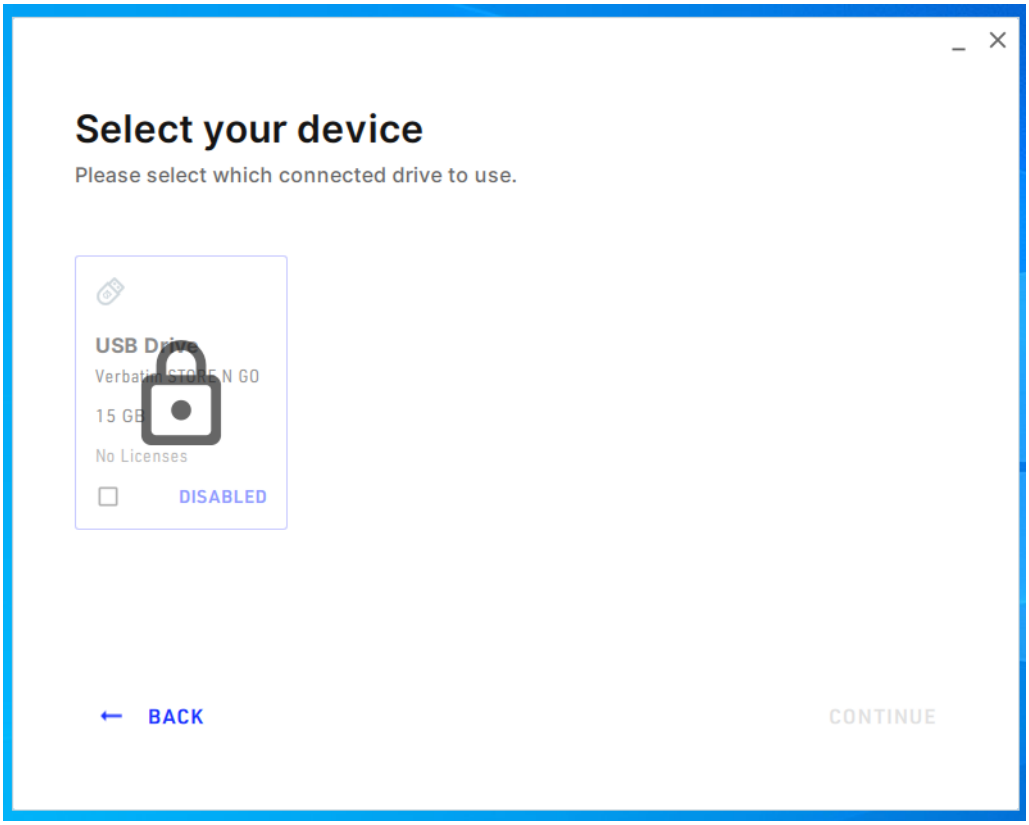
2) Manage licenses for offline use

If you choose this option after you log in to Securaze Creator, in the next window you will be prompted to select the drive you wish to use:

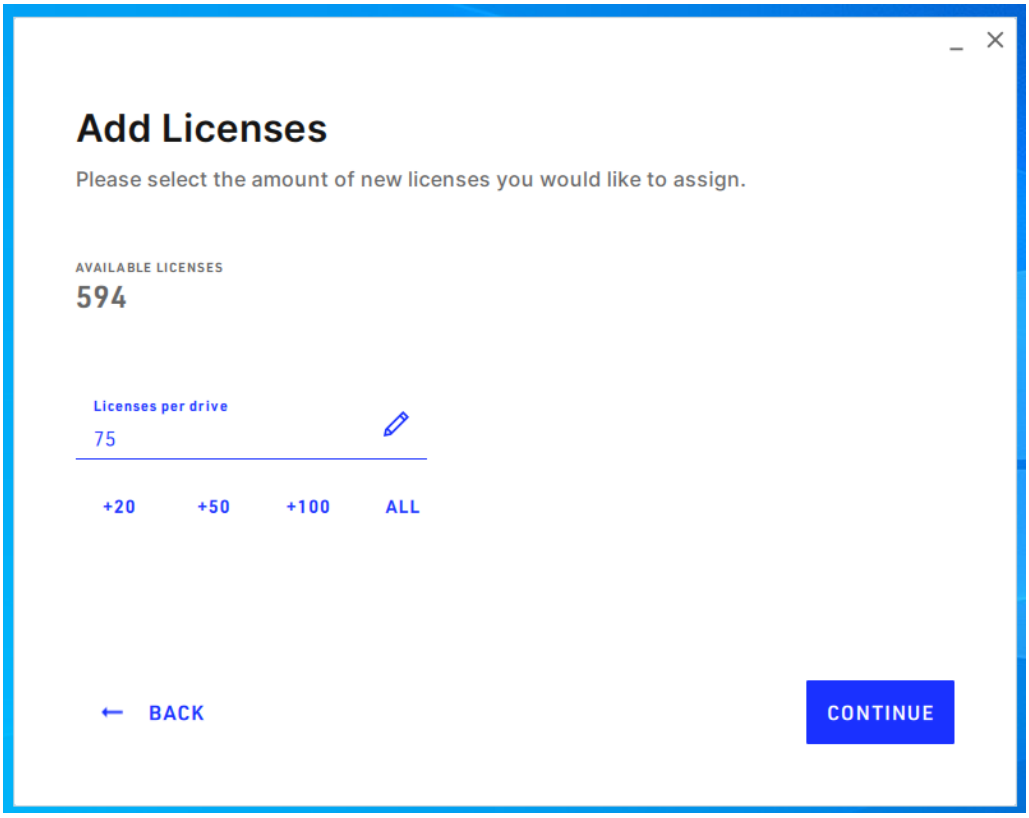


Please note that in case you already used this USB drive / SD card to burn Securaze image and added erasure licenses to it, the existing licenses will be transferred back to the account that was used for creating that USB drive / SD card. After you have selected the drive, click on **CONTINUE**.

In case there is no Securaze Image on the USB drive / SD card you plugged in, you won't be allowed to continue.

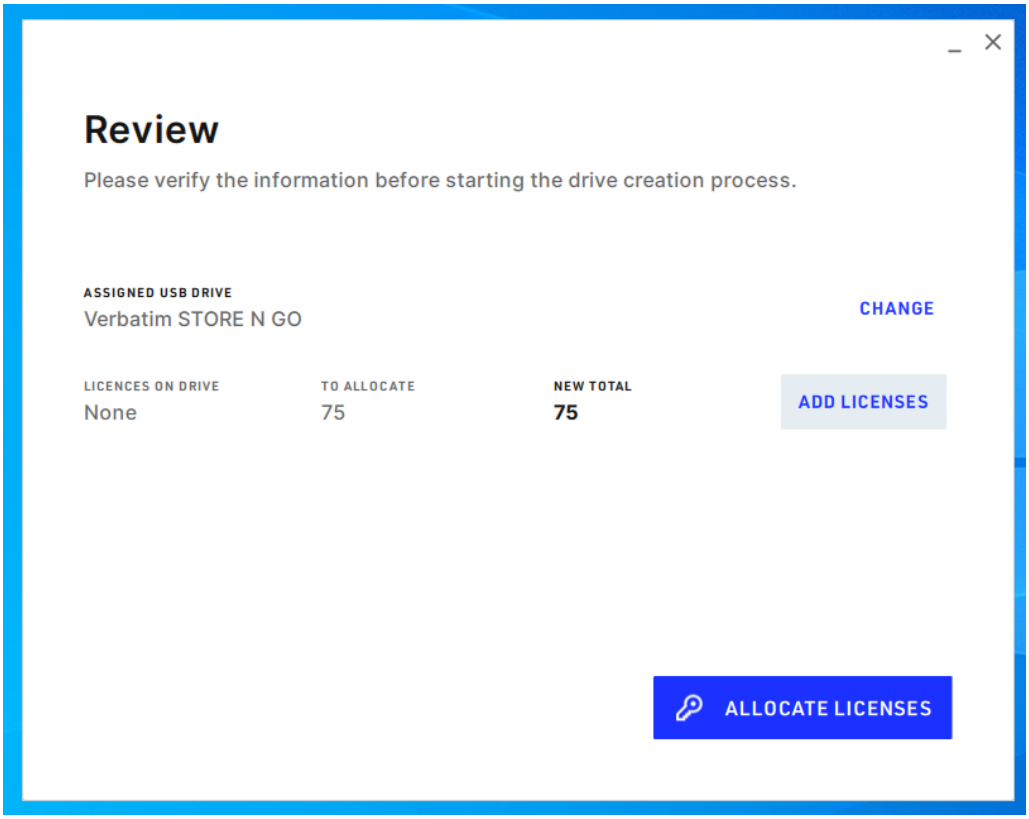


In this case, you will be required to burn the Securaze image on the USB drive / SD card first, and then you can add the licenses.

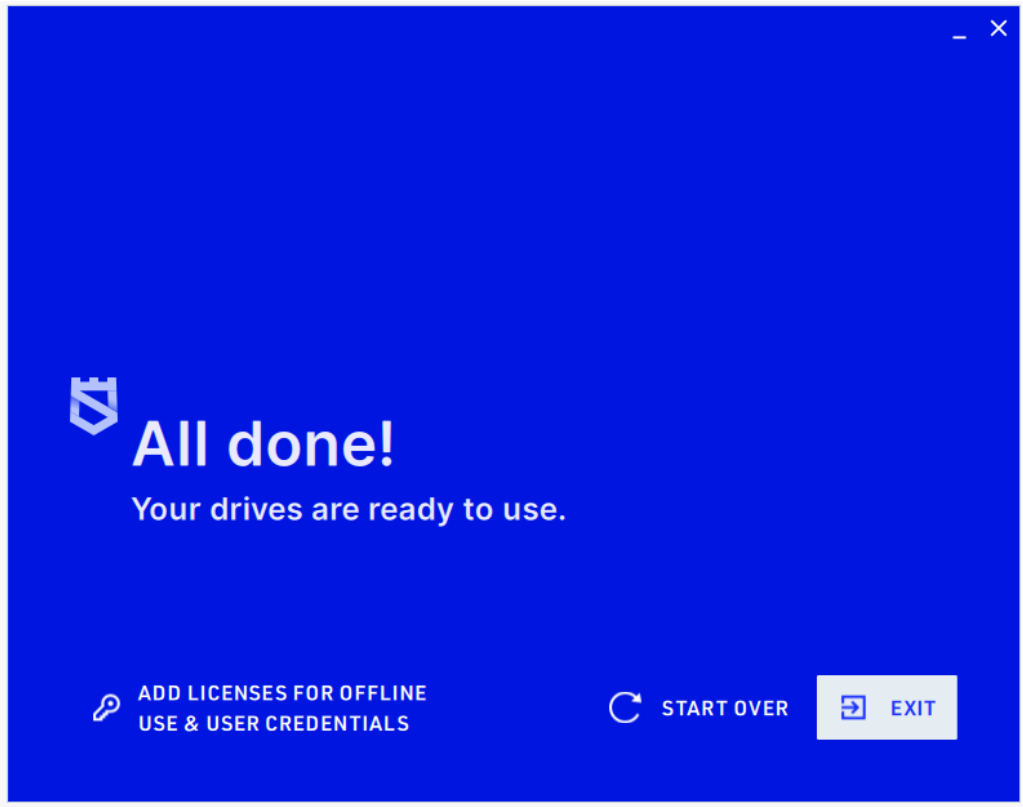


The number of available licenses is displayed first, so that you are able see what is the maximum number of licenses you can add to the drive.
You can type in the number of licenses you wish to add manually, click on buttons "**+20**", "**+50**", "**+100**", or, if you want to instantly add all the available licenses, click "**ALL**". After you have selected the number of licenses, click on **CONTINUE**.

In the next window, you will be asked to review the information before you add the licenses to the drive. If everything is correct, click on **ALLOCATE LICENSES**.

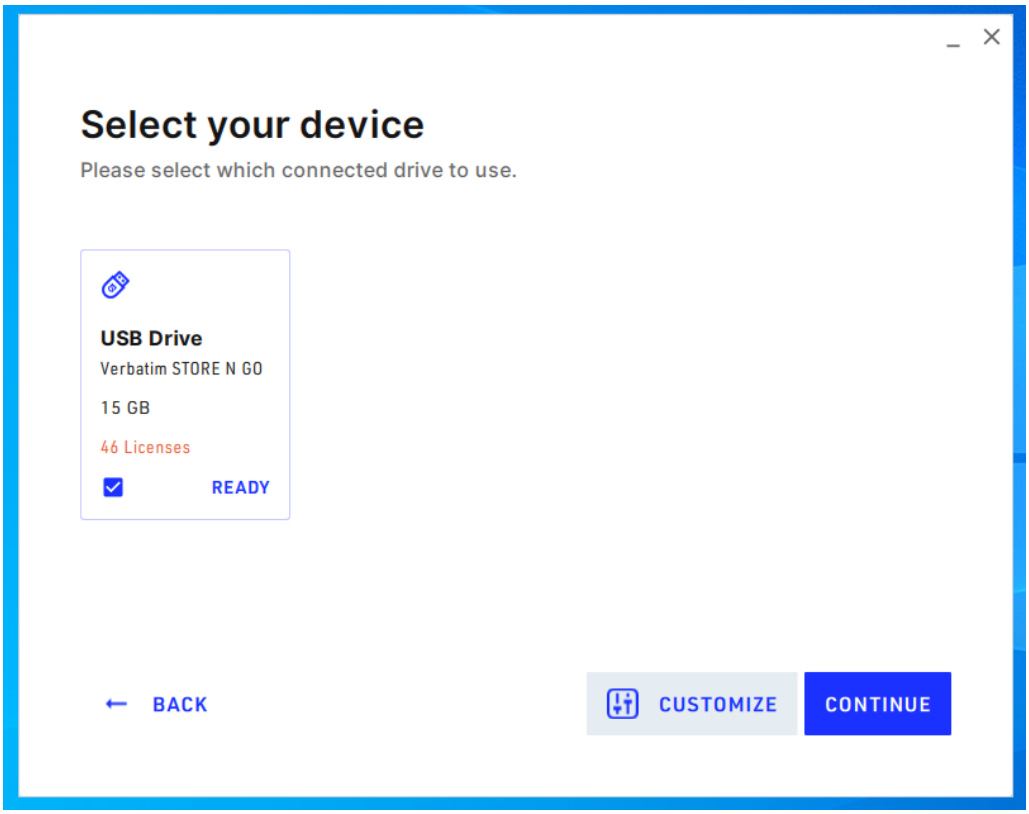


After the licenses are added, you will be taken to the last screen.

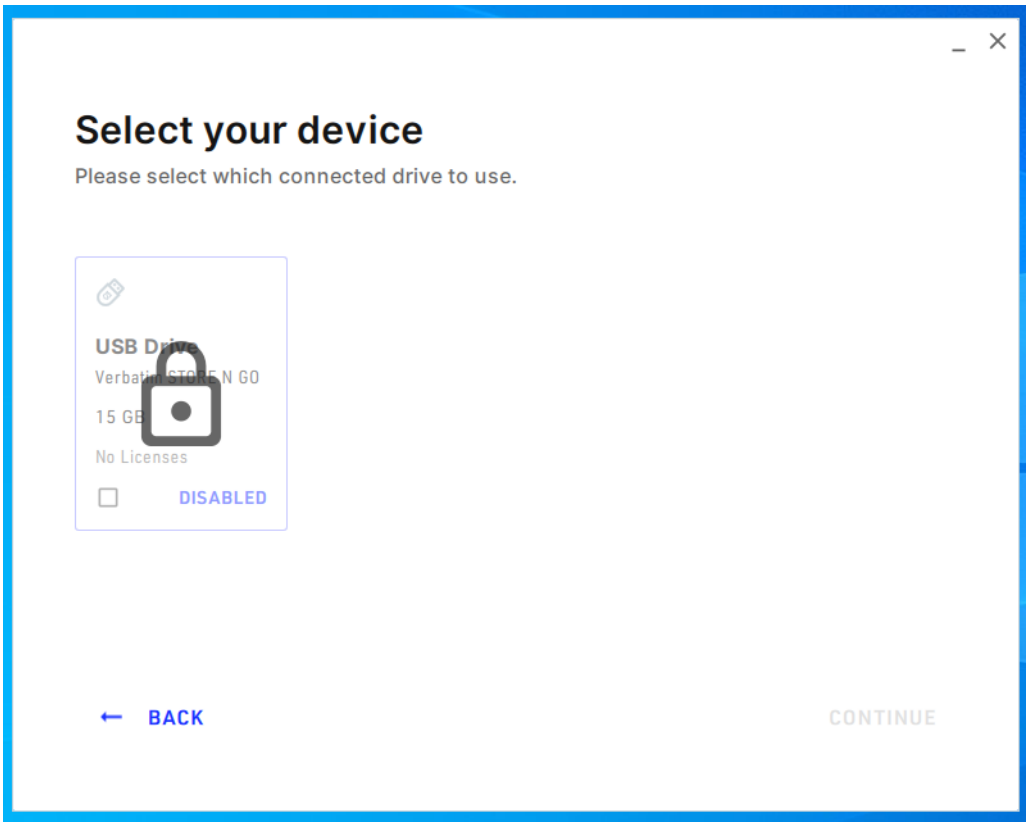


3) Add settings to an existing Securaze image

If you choose this option after you log in to Securaze Creator, in the next window you will be prompted to select the drive you wish to use:

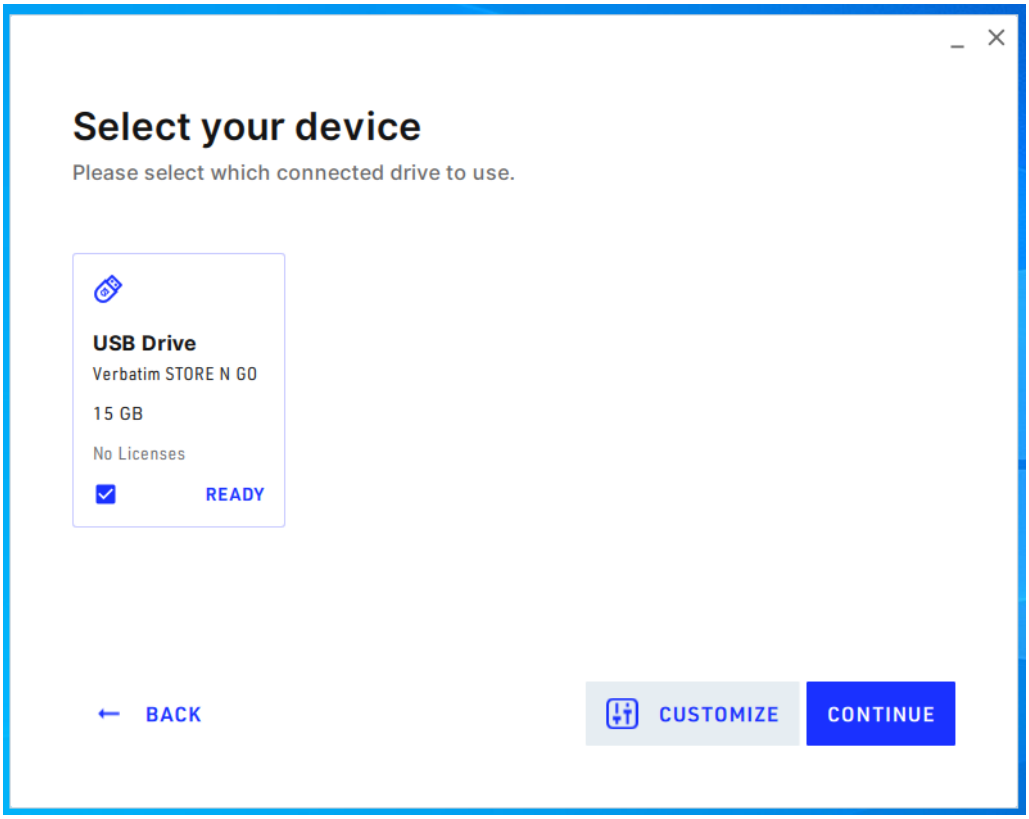


In case there is no Securaze Image on the USB drive / SD card you plugged in, you won't be allowed to continue.



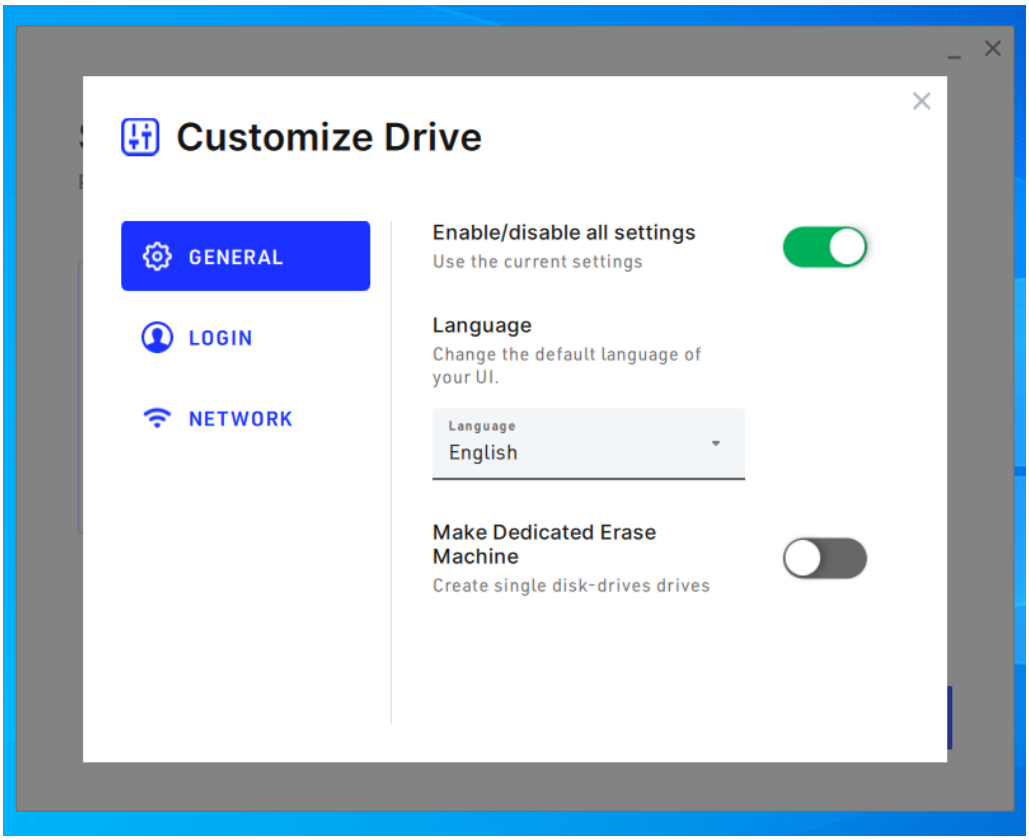
In this case, you will be required to burn the Securaze image on the USB drive / SD card first, and then you can change the settings.

Start by selecting you drive and clicking on CUSTOMIZE button.

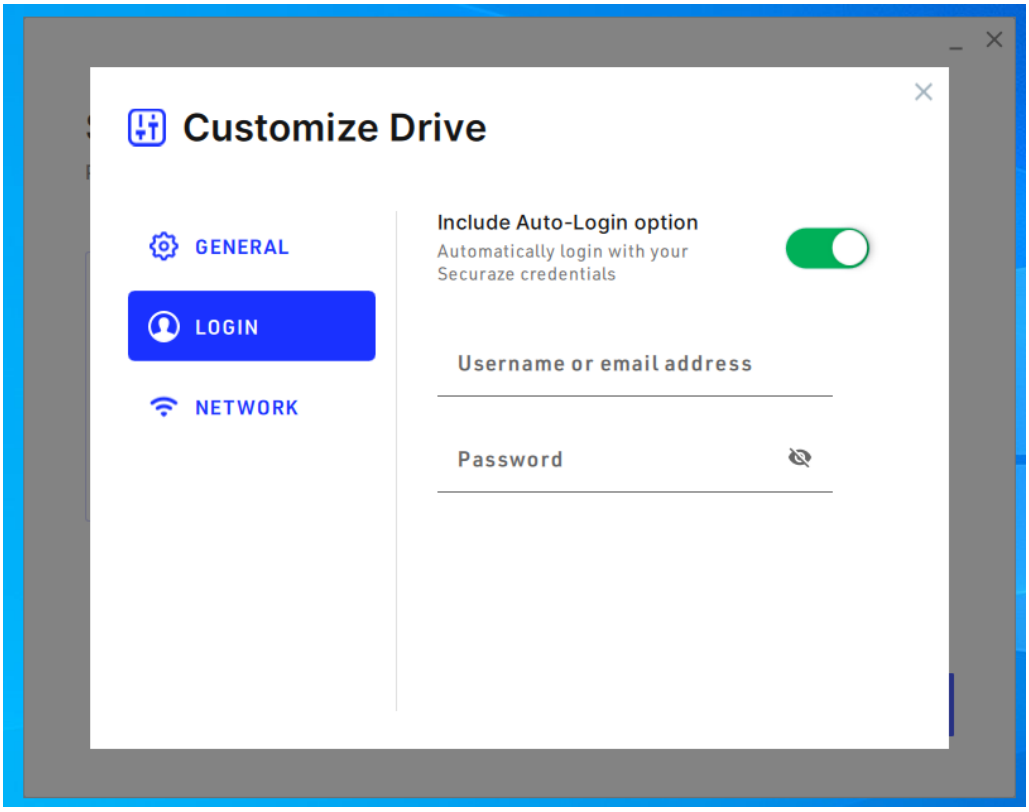


A new window will open, with the available settings. In the first tab, you can edit GENERAL settings.

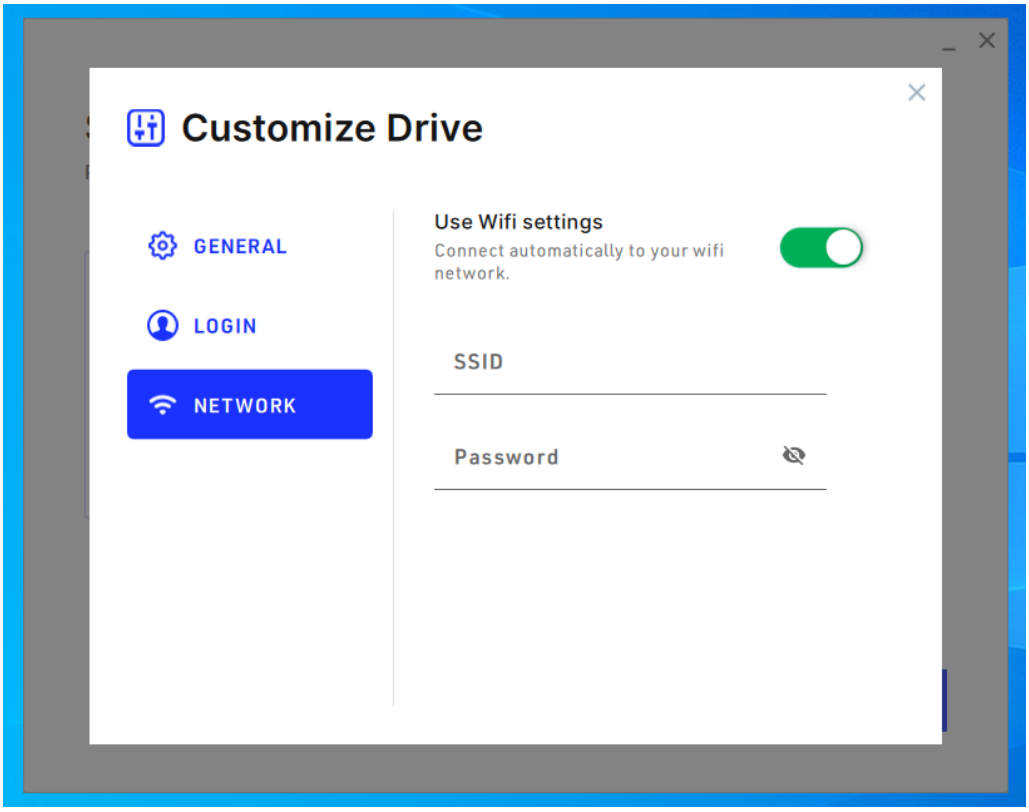
Enable/disable all settings allows you to control whether or not settings are available or not.
Language setting allows you to change the default language of the user interface.
Make Dedicated Erasure Machine setting enables the Dedicated Erasure Machine mode, for erasure of loose drives.



In the tab LOGIN, you can setup the credentials for auto-login.

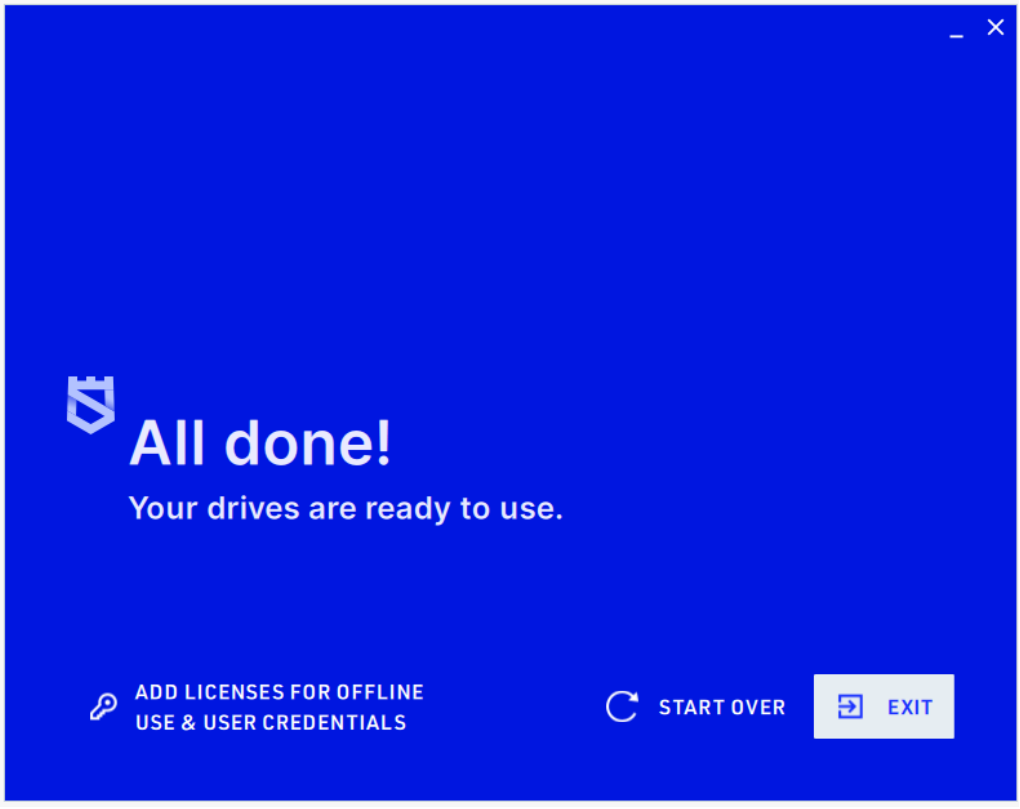


In the tab NETWORK you can setup your Wi Fi, so that you get automatically connected if that Wi Fi network is available.



After you have made the necessary changes, click on **X** in the upper right corner of the settings window, and then click on **CONTINUE** button.

You will be taken to the exit screen after the changes are saved.



After you completed the image burning and settings setup, you may click on **EXIT** button.

If the message "You need to format the disk in drive X: before you can use it" appears, this is completely normal and the message can simply be ignored.

To continue to erasure process, plug out your USB drive / SD card and take it to the device you wish to erase.
Insert the USB stick into an open USB slot and press the power button on your device.
During the startup, press F1, F2 or Del to open the Boot Menu selection (**different brands** have **different keys** - see here which key you need for your brand - chapter BIOS Boot Up Keys 251)
Select the USB drive you want to boot from.

Your computer will now boot and start Securaze Work.

1.3 Command

1.3.1 System environment

Securaze Command can be used in the following system environment.

System requirements

	Minimum Configuration	Recommended Configuration	Production Configuration
Dedicated for	**processing 1-10 devices simultaneously**	**processing more then 20 devices simultaneously**	**processing up to 500 devices simultaneously**
CPU	64Bit CPU	64Bit Quad-Core CPU	Dual 64Bit Quad-Core CPU (5th gen or newer)
Memory (RAM)	512 MB	2 GB	8 GB
Storage requirements	HDD; 100GB free space	SSD; 256GB free space	SSD; 512GB free space
Resolution	1280 * 1024 resolution	1280 * 1024 resolution or higher	1280 * 1024 resolution or higher
Network-Connection	1 Network-port and Wifi-Module or (for production usage 2 Network-ports are highly suggested) Alternative: use a supported USB Ethernet-Dongle instead of the Wifi-Module	2 Network-ports	2-4 Network-ports
Network Hardware	Standard 100/1000mbit RJ45-Network-Hub	Professional grade 24 port 1000mbit RJ45-Network-Hub	Professional grade 48 port 1000mbit RJ45-Network-Hub
Internet	Internet-Connection is mandatory	Internet-Connection is mandatory, 5 Mbps or higher	Internet-Connection is mandatory, 25 Mbps or higher

	Minimum Configuration	Recommended Configuration	Production Configuration
Inputs	Keyboard and/or Mouse/Trackpad	Keyboard and Mouse	Keyboard and Mouse

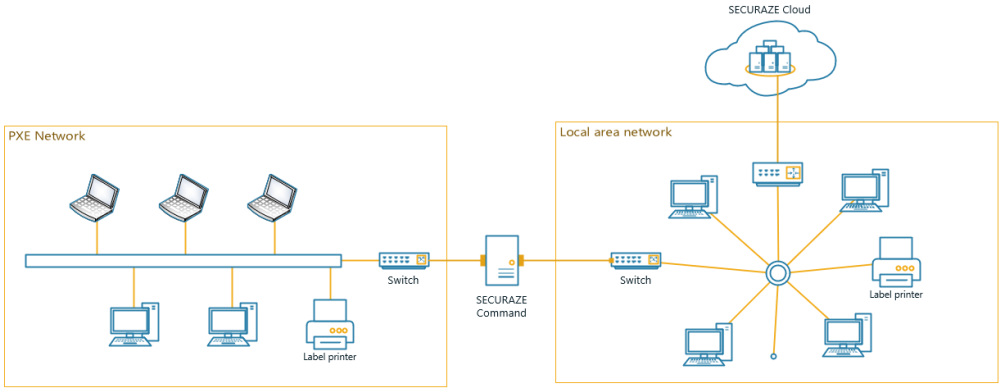
Software settings

Firewall settings	
Internet connection	Permanent Internet connection is required
Securaze servers	The firewall must not block any of the Securaze pages: • https / http to *.securaze.com • https://cdn.securaze.icu
Remote Support	The firewall may have to be modified. To allow AnyDesk for incoming connections, add AnyDesk to the Whitelist: · *.net.anydesk.com · TCP-Ports 80, 443 and 6568
Local DNS	if local dns is used, it has to be correctly propagated · ssh port 22 in case of support issues · icmp enabled to outside world (currently 8.8.8.8 is used; will be changed to

1.3.2 Network Topology

For an optimal network setup, Securaze Command requires two network interfaces:

- One network interface for the PXE network with a separate switch, where Securaze Command provides DHCP. This part should not be connected to LAN.
- One network interface (or optionally WiFi) to connect Securaze Command to the office network and through it to the internet.



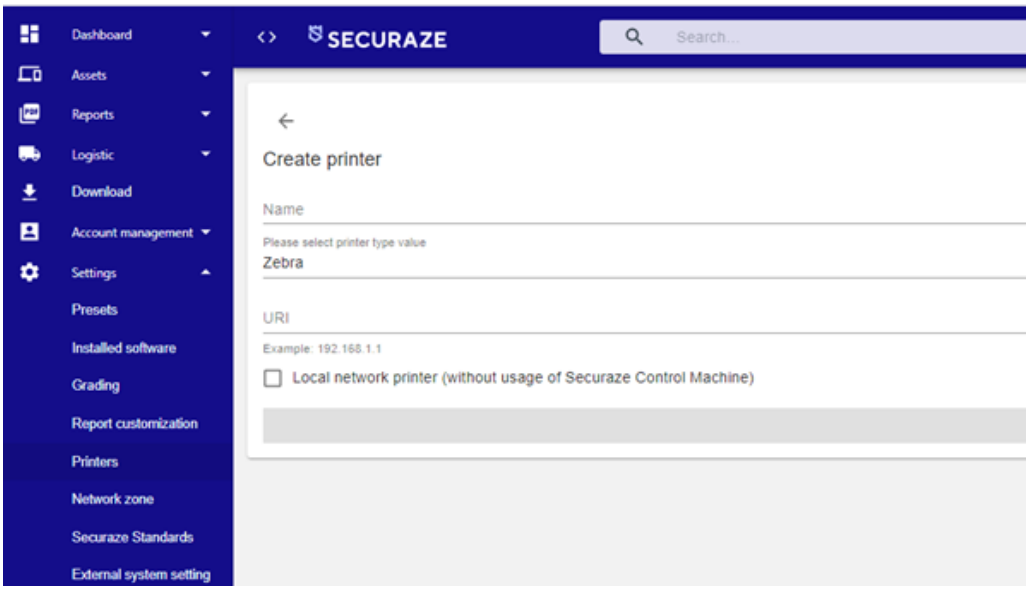
You can connect a label printer to either PXE network or LAN.
If there are multiple Command machines in a workspace, only one of them can have the Print agent turned on (for more information see Settings - Print Agent 43).

Supported printer brands are GoDex and Zebra, excluding Zebra ZSB series, 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

Printing labels from the cloud (Securaze Dashboard):
The printer does not need to be connected to the PXE network, it can be connected to the Command machine directly, or any other device, as long as it's included in the local network.
The printer has its own IP address, which you enter in Securaze Dashboard under Settings - Printers.



Start the print job in the client using the created printer. The print request is submitted to the cloud and passed to Securaze Command. The label is printed by Securaze Command on a local printer.

1.3.3 Deployment

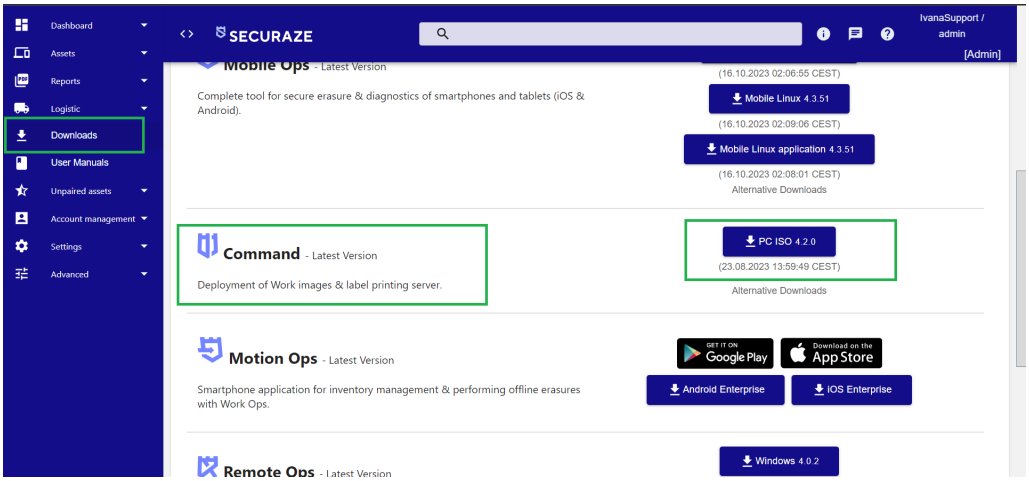
Securaze Command must be deployed using a USB stick.
To do this the image of the Securaze installation is written to any (supported) USB stick.

The following steps must be performed to install Securaze Command.

Open Securaze Dashboard and login with your username and password, which you received in your welcome mail.

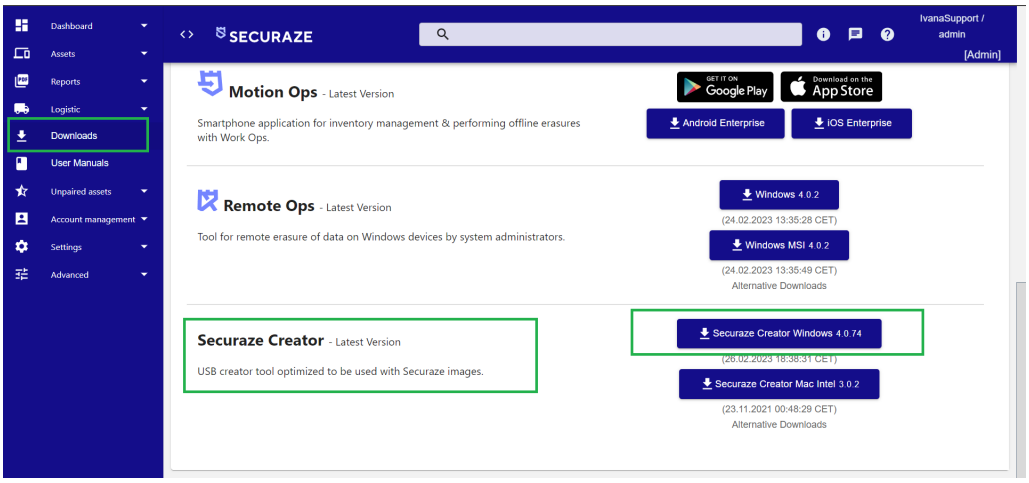
Ensure that the sleep mode on your computer is disabled before starting the download and burning process!

Step 1: Download Securaze Command
In the left tab menu **Downloads** you can download the Securaze Command **PC ISO** image.



Start the download by clicking on the corresponding button.

Step 2: Download Securaze Creator
In order to install the downloaded Securaze image on your operating system, please download Securaze Creator Windows, which is optimized to create bootable USB drives.



Step 3: Install Securaze Creator Windows on your Windows computer

Run the Securaze Creator installation file, allow the program to make changes to your computer, follow the installation path by clicking Next / Continue, and once it is finished, launch Securaze Creator.

Step 4: Create bootable drive in Securaze Creator Windows:

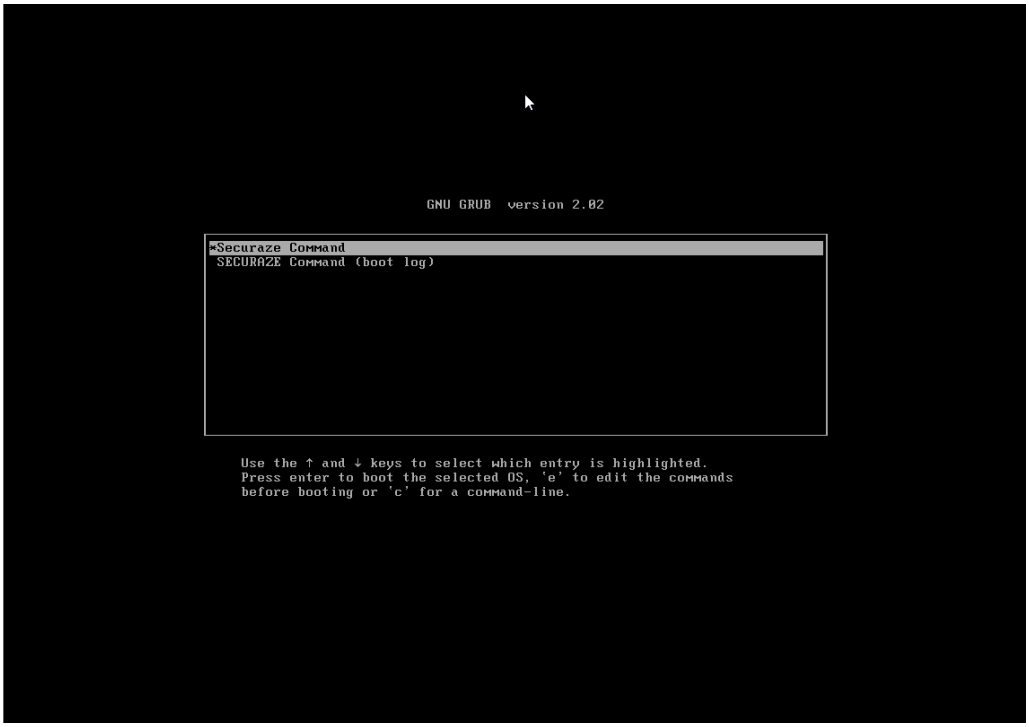
Plug in the USB stick you want to use to create the bootable drive.
Log into the Securaze Creator by using your Securaze credentials (the same as for Dashboard), select the USB drive you plugged in. Make sure it is empty, before proceeding, because the content on the USB drive will be wiped, during formating and creation of Securaze Command.
Select Option 1: Create bootable USB drive or SD card
Select Command ISO file
Continue until process is complete.

With this USB stick you can now install Securaze Command on the dedicated machine.
Insert the USB stick into an open USB slot and press the power button on the computer you will use as Command server.
During the starting progress press F1, F2 or Del to get to Boot Menu selection.
Select the USB drive you want to boot from.

Your computer will now boot and start Securaze Command.

1.3.4 Installation

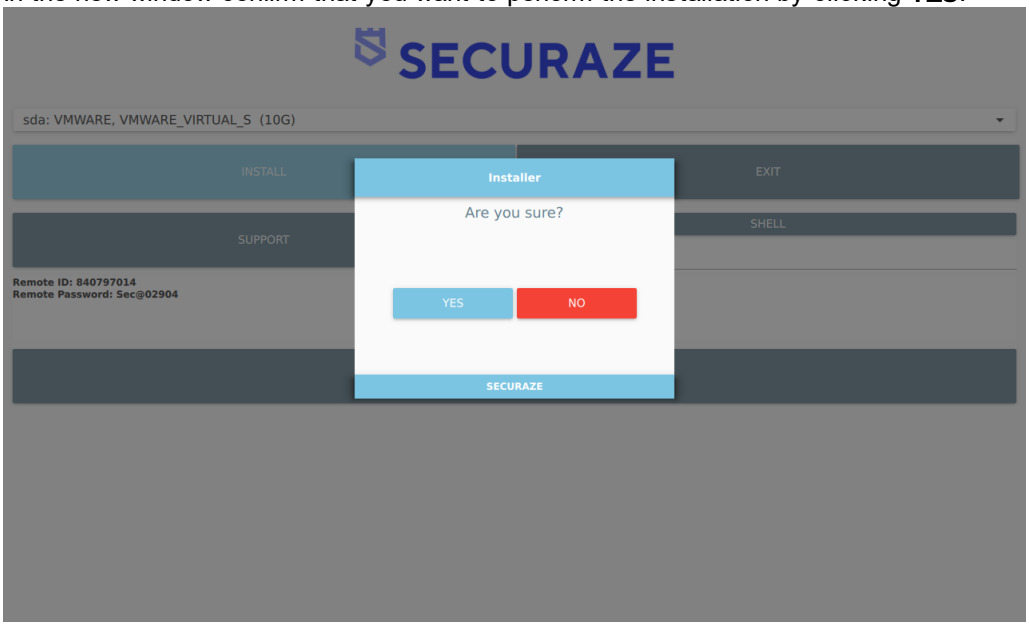
To start Securaze Command, boot the device from the prepared USB stick. During the boot process the Securaze Command boot menu will appear.



Once Securaze Command boots, select the local target SSD on the device from the drop down at top.

Click the **Install** button.

In the new window confirm that you want to perform the installation by clicking **YES**.



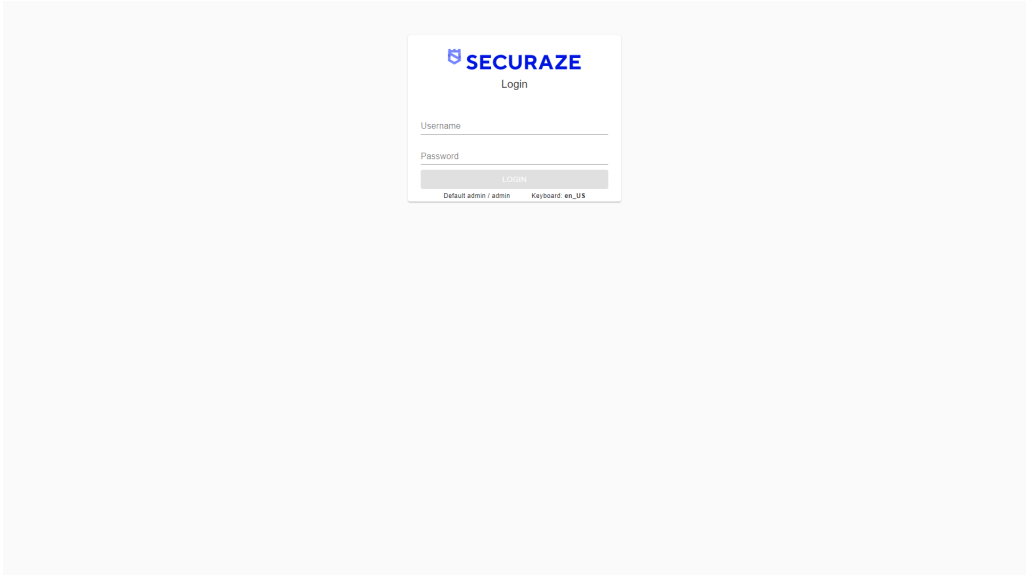
Now the installation will start.

After installation, the system will restart. Upon system reboot, the USB stick can be removed. Please make sure the Boot Order on the Command station is set to the local drive.

Once booted from the local system, the setup of the PXE network will start.

1.3.5 Configuration

After installing Securaze Command, configure it in Securaze Command WebUI.
You can later access this WebUI in the entire company network via the browser and the IP address assigned to the Securaze Command, found in the Status screen.

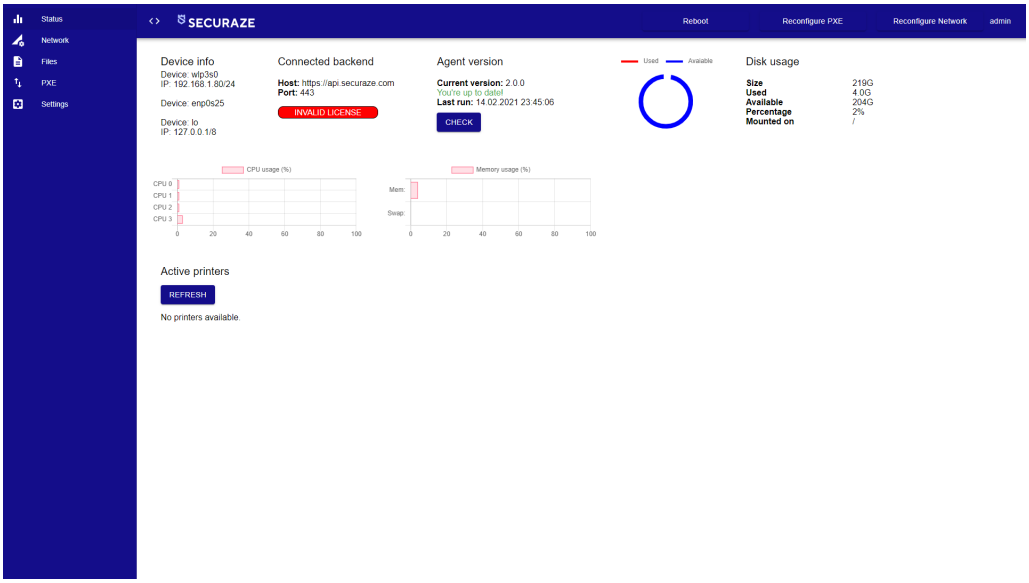


Enter your username and password and confirm with **LOGIN**. The default username and password are *admin / admin.*

Note: Currently only the English keyboard layout is supported. Please be aware of this when entering your password.

Upon Admin log-in, it will prompt you to setup the network. The setup-wizard guides you through Network, License and PXE-Setup.

Status Page
On the Status page you get a brief overview about the installed Securaze Command.

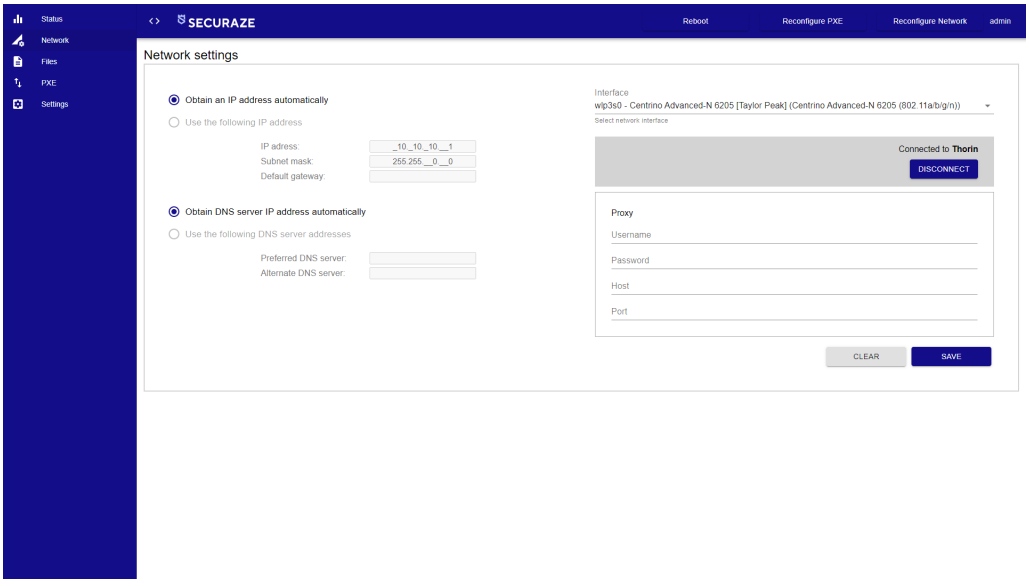


License:
As long now valid license is installed on Securaze Command the automatic image download service is disabled.

Check:
By pressing "Check" a manual check for new Securaze images is triggered. The check is done automatically in regular intervals.

1.3.5.1 Network

First you carry out the network configuration. To do this, click on **Network** on the left.

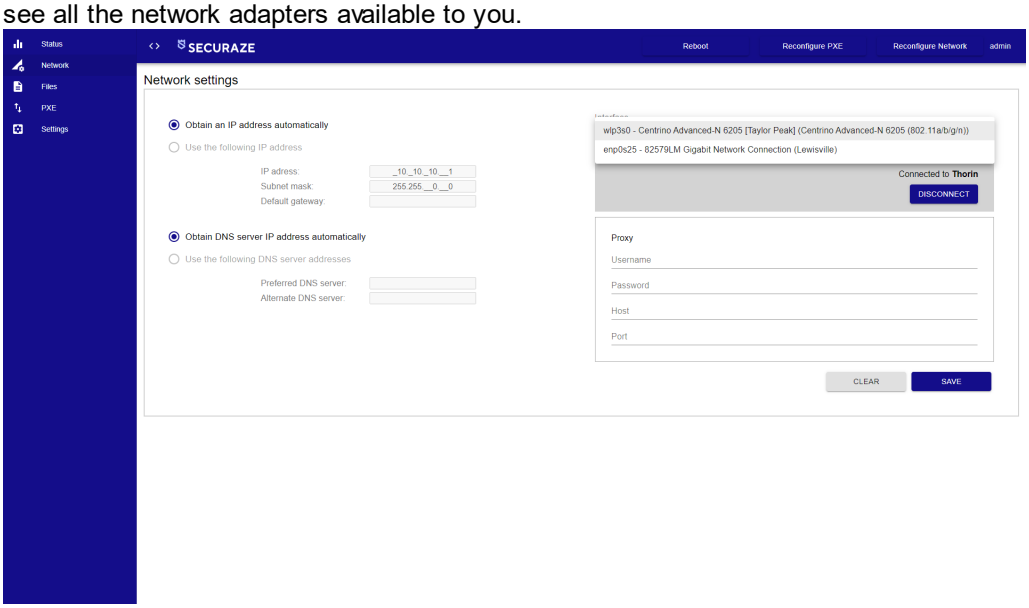


On the left side you can make network settings.

Check the box **Obtain an IP address automatically** to automatically obtain an IP address from the DHCP server.
Check the box **Use the following IP address** to enter a specific **Static IP** address.

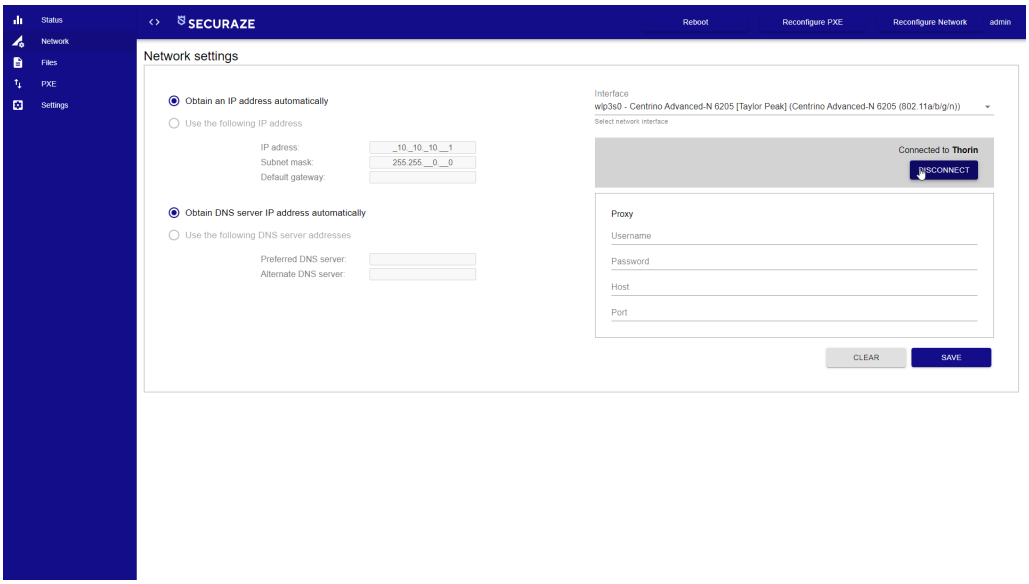
Below this you can also have the DNS server address set automatically or enter a specific DNS server address by checking the boxes as described above.

On the right side, select the network interface you want to use to connect to the Internet.
To do this, click the arrow next to **Interface** to open the drop-down menu. Here you can see all the network adapters available to you.

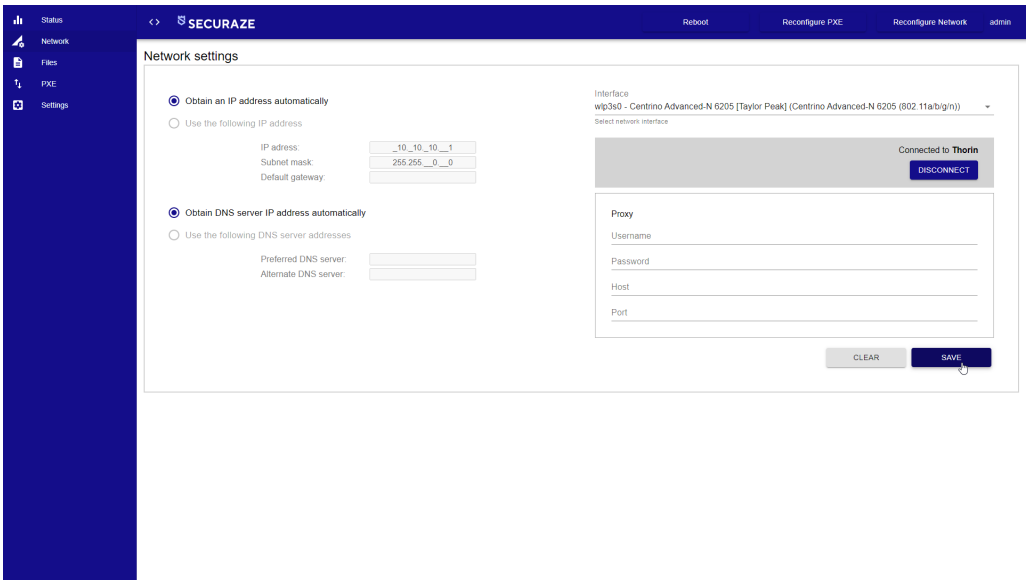


Select the desired interface and establish the connection.

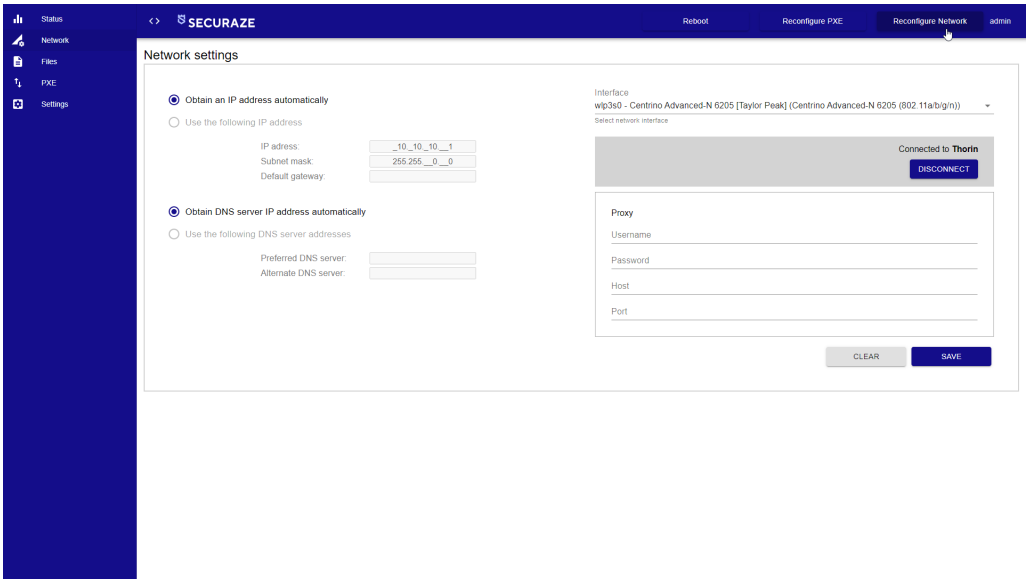
Alternative if only one network interface is installed
If a WLAN module is installed, you will also see it in the list.
Select the WLAN SSID, enter the WLAN password and confirm your entry with **CONNECT**.
Note: Currently only the English keyboard layout is supported. Please be aware of this when entering your password.



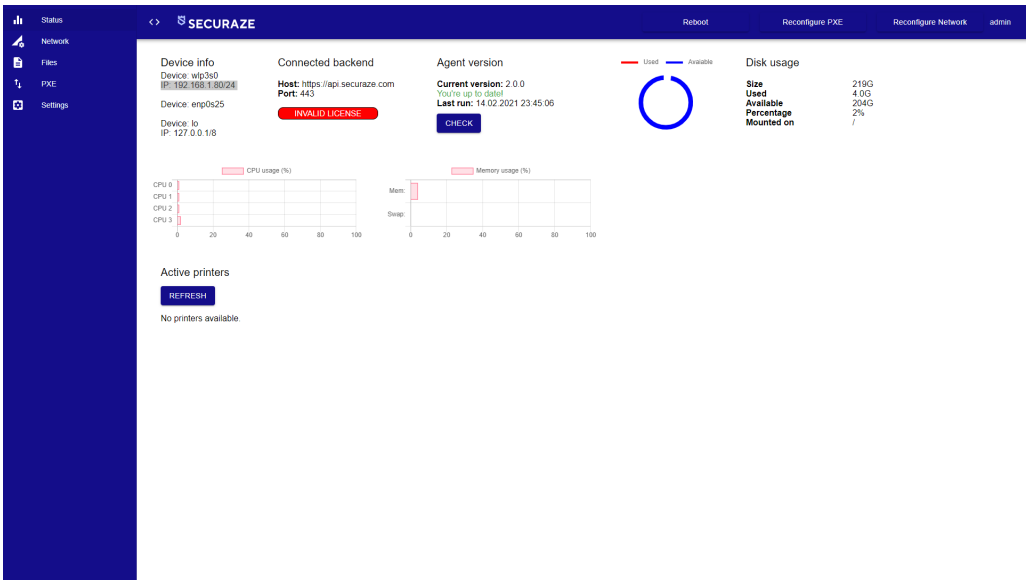
Save your settings by clicking on **SAVE**.



To apply the network settings live to the system, click **Reconfigure Network** in the upper right corner.



Select the **Status** menu item to return to the dashboard, where you can check whether an IP address has been obtained from the system.

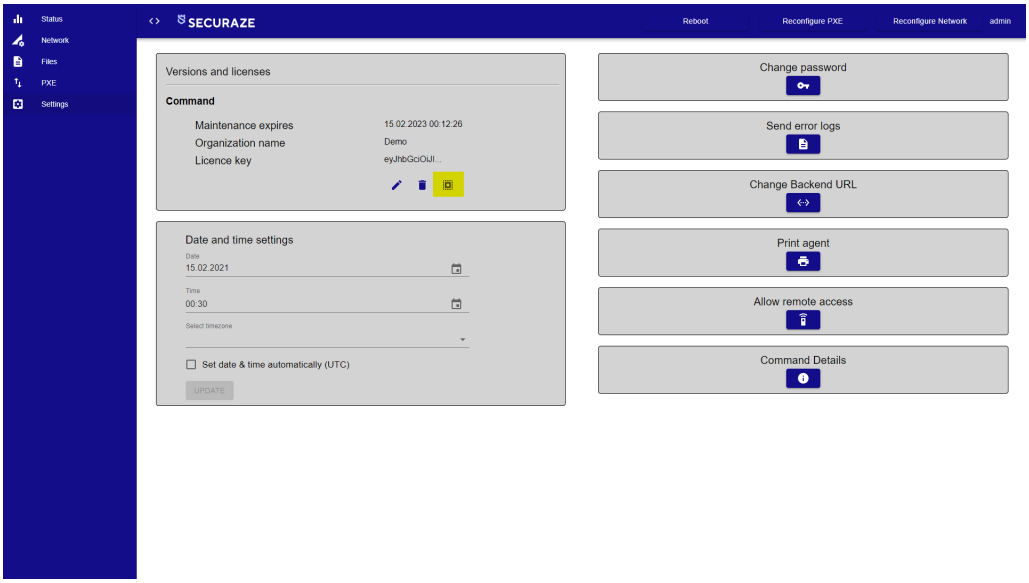


In case no IP address could be retrieved check the following things:
- Network connection of the device. A typical problem is that the Internet-Port and the PXE-Port are connected in reverse order.
- Ensure a DHCP-server is available in the network if "Obtain an IP address automatically" is selected.
- Ensure that the given IP address is not yet used if "Use the following IP address" is selected.

1.3.5.2 Licenses

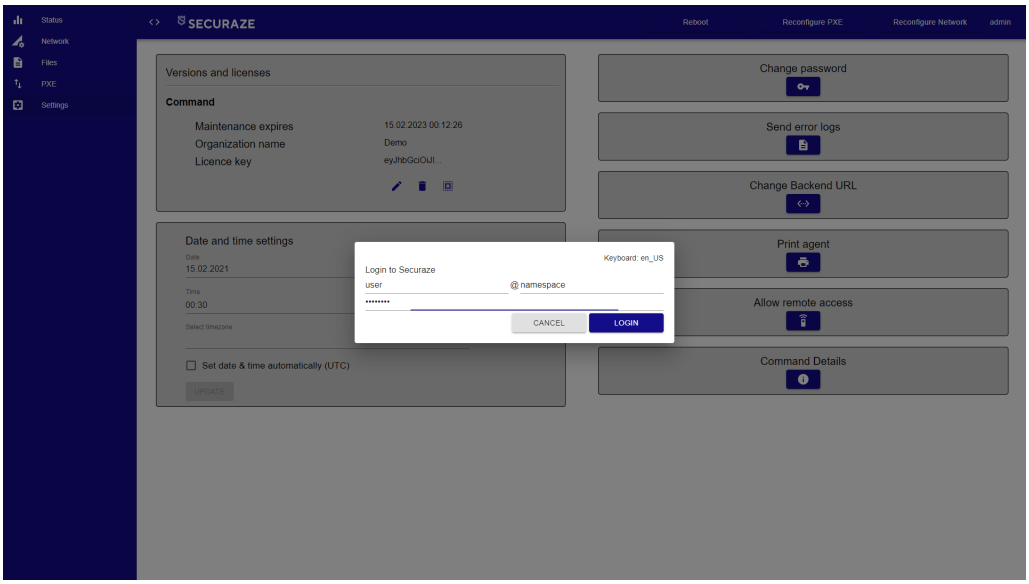
In the next step you configure the licenses.

Select the menu item **Settings** and Click on **Load Licenses** in the grey box **Versions and licenses**.



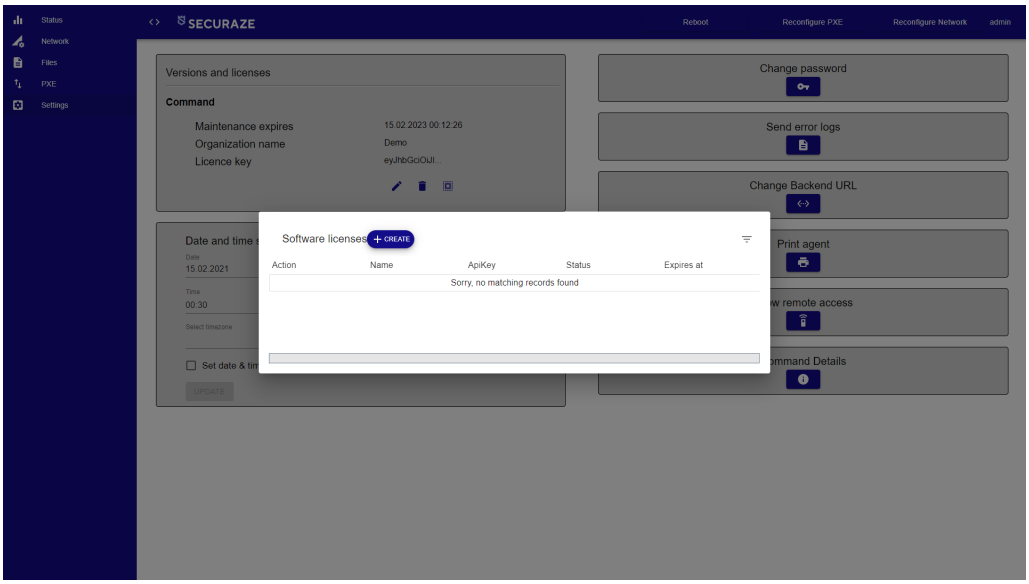
Enter your Securaze user credentials (username and password) here and the licenses will be loaded automatically by the system.

Note: Currently only the English keyboard layout is supported. Please be aware of this when entering your password.

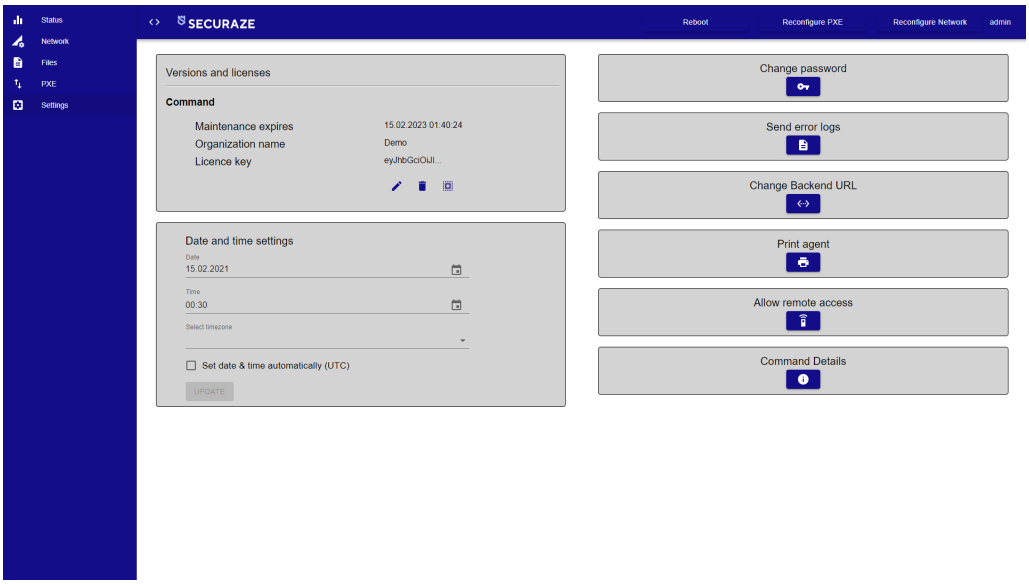


Now you create a new Software license for the installed Securaze Command.
This action connects the installed Command with your account.

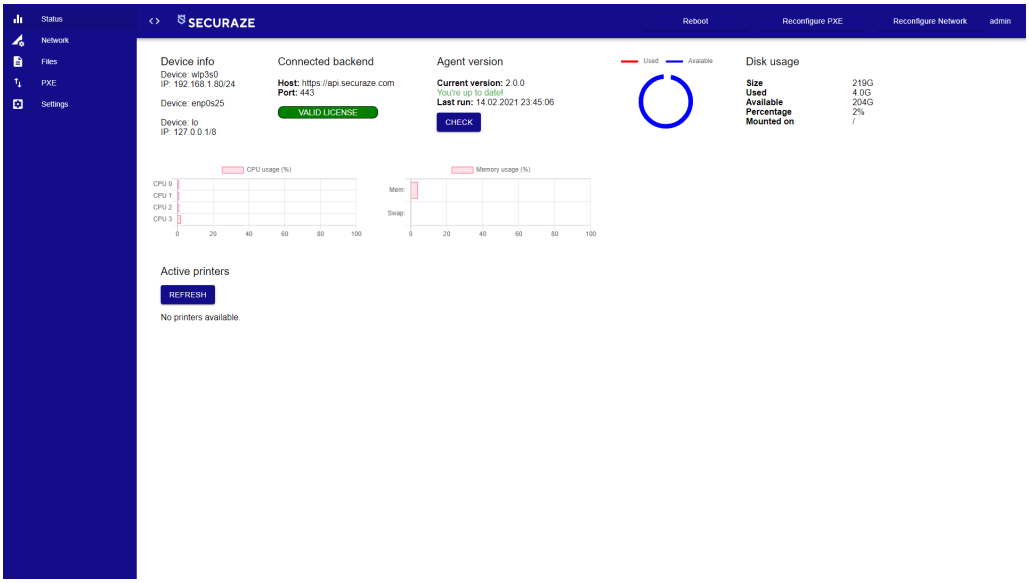
Click on **Create** on the header and the license will be created.



The installed linces are shown below **Versions and licenses**.

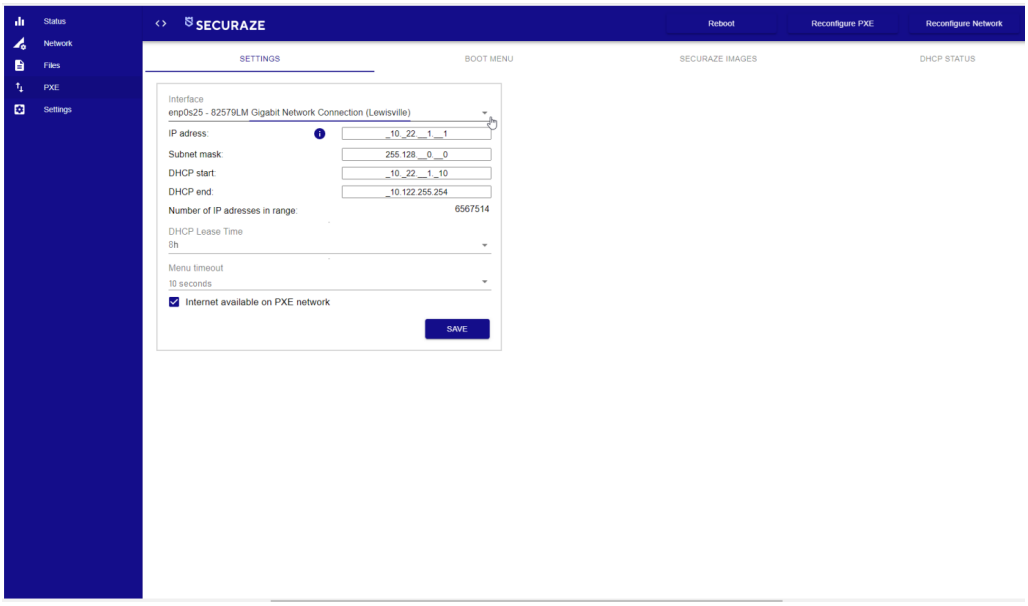


Select the **Status** menu item to return to the dashboard where you can check if a valid license is available.



1.3.5.3 PXE

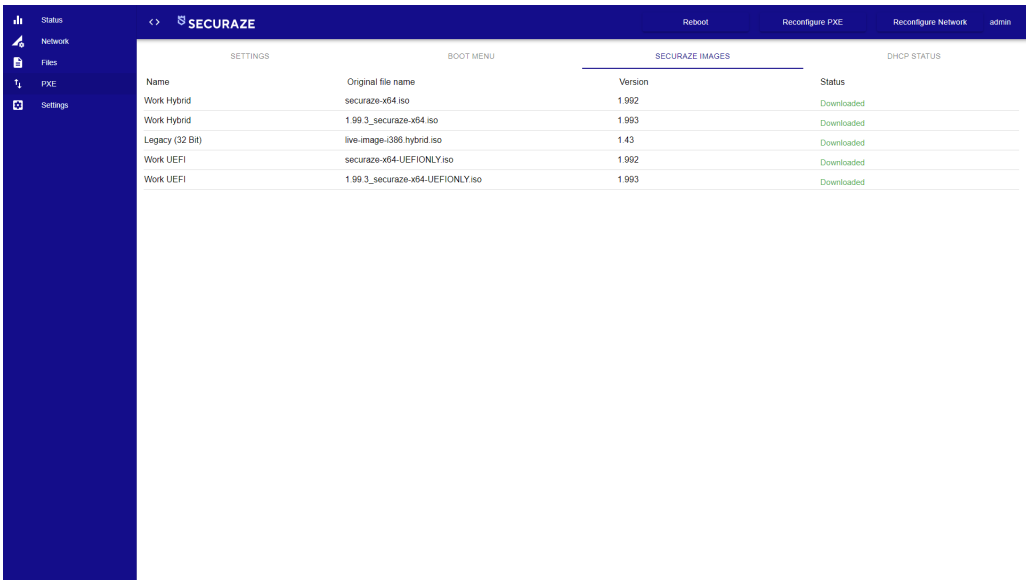
To configure the PXE, select the menu item **PXE**.
Select one of the available network interface you want to use for the PXE network by clicking the arrow next to **Interface** to open the drop-down menu. .



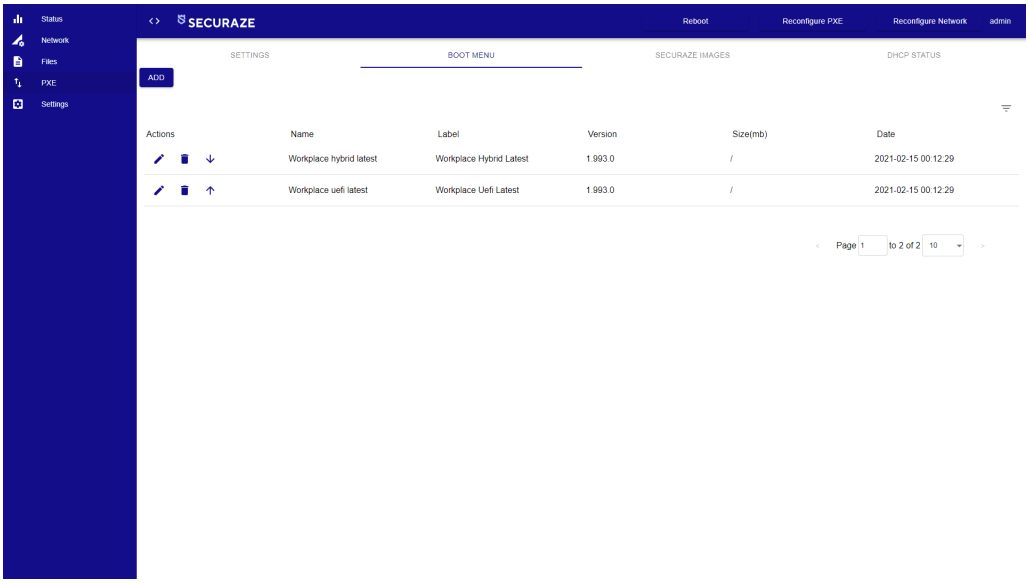
Select the desired network interface and, if necessary, change the configuration of the PXE network. These changes are not recommended, since the default settings are optimized for errorless workflow of the Securaze Command.
Click on **SAVE** to save your entries.

PXE IP address range
The default setup of the PXE network should only be changed if you want to differentiate you PXE IP addresses from the ones used in your company's network, or if you want to increase the number of simultaneously booted devices in the PXE network.
The PXE network is a standalone network and won't conflict with your company's local network.

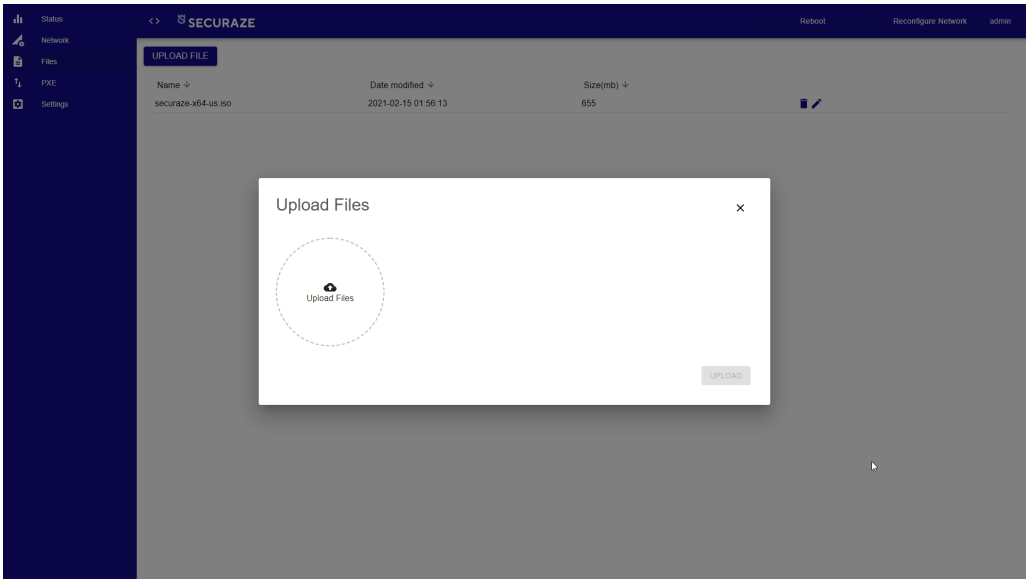
As soon PXE configuration is done and a valid license has been entered, Securaze Command will automatically start downloading the Securaze images.
These can be found under the **Securaze IMAGES** tab at the top right.
Here you can see the available images.



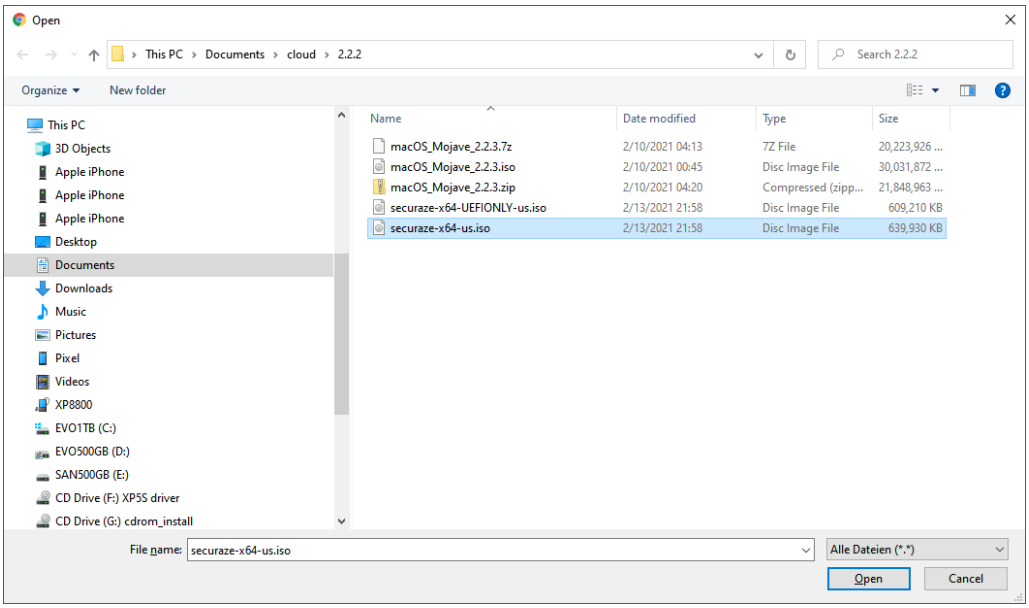
Once the Securaze images are downloaded, you can select them in the boot menu.
To do this, click on the **BOOT MENU** tab in the top center.



By default 2 images are preconfigured, the latest version of Securaze Work Hybrid and Securaze Work UEFI.
However, additional images such as custom images can be added.
To do this, click on the menu item **Files**. Here you click on **UPLOAD FILE** in the upper area.

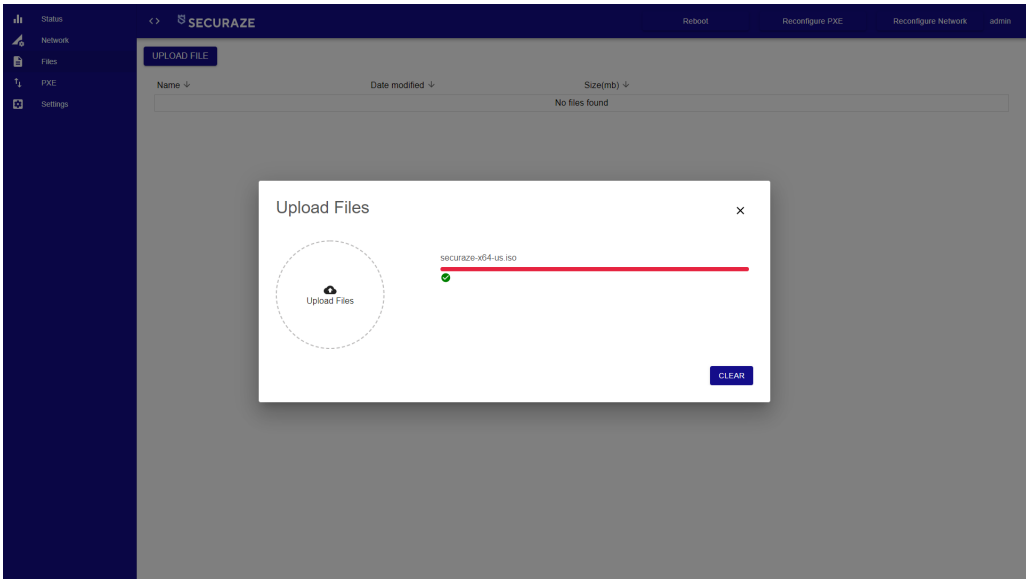


In the new window click on **Upload Files** to select a saved image.

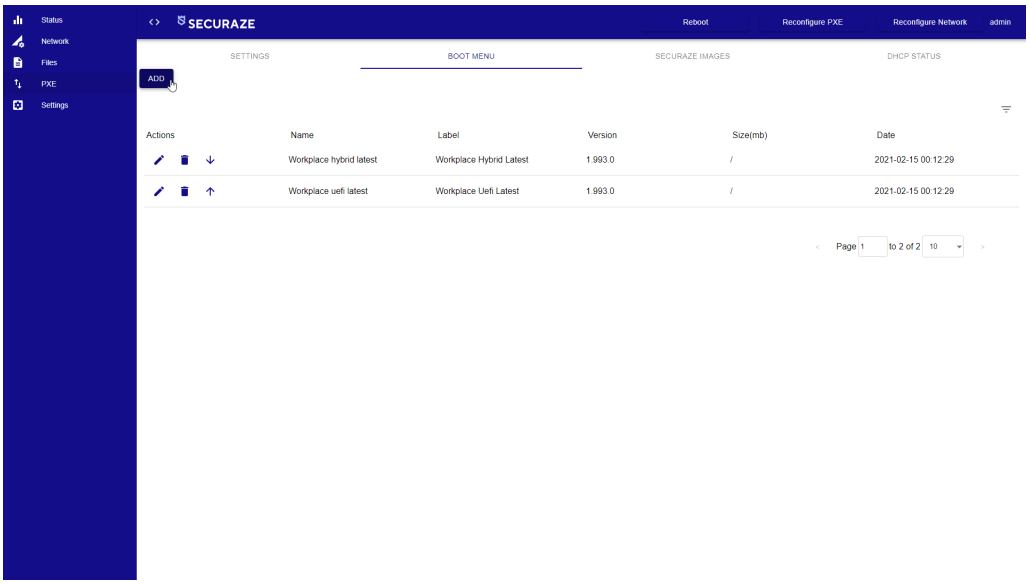


Select the desired image and click on **Open**.

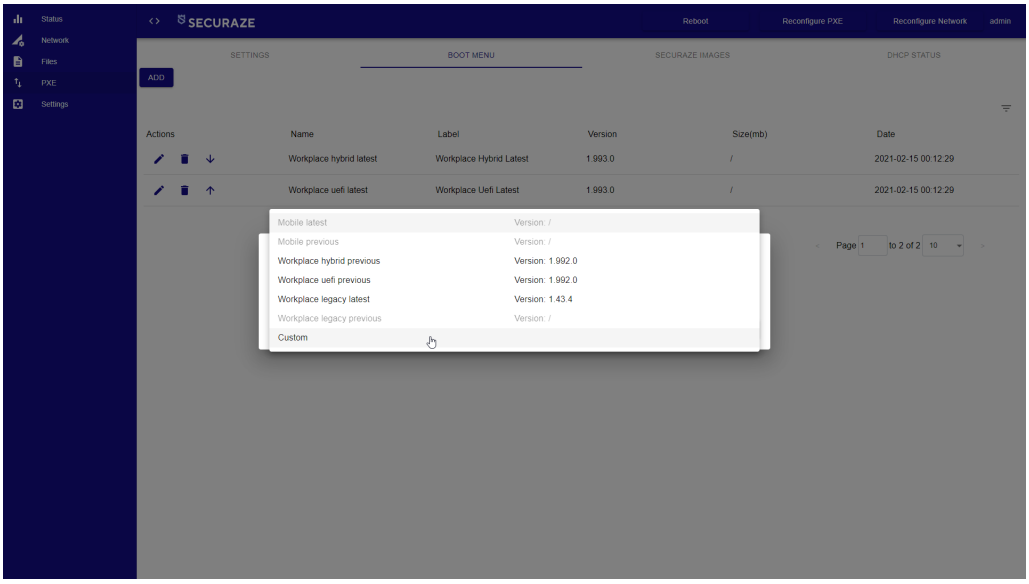
Confirm your selection by clicking **UPLOAD** and the image will be uploaded.



After uploading, the image file is available and you can add it to the boot menu.
To do this, select the menu item **PXE** again and the tab **BOOT MENU.**



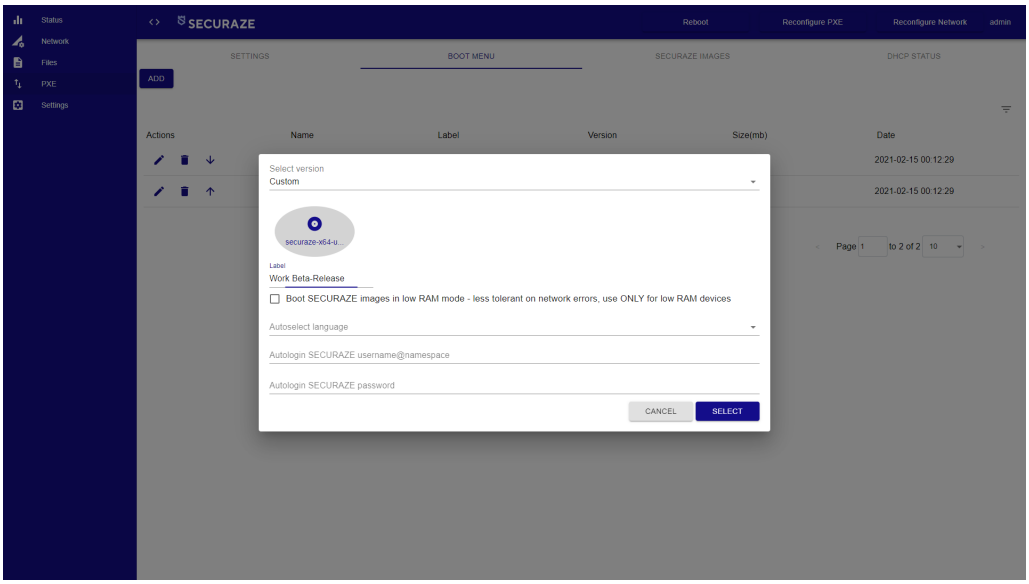
Click **ADD** and select Custom in the new window if you want to use an uploaded file or choose any of the predefined entries to use a provided Securaze image.



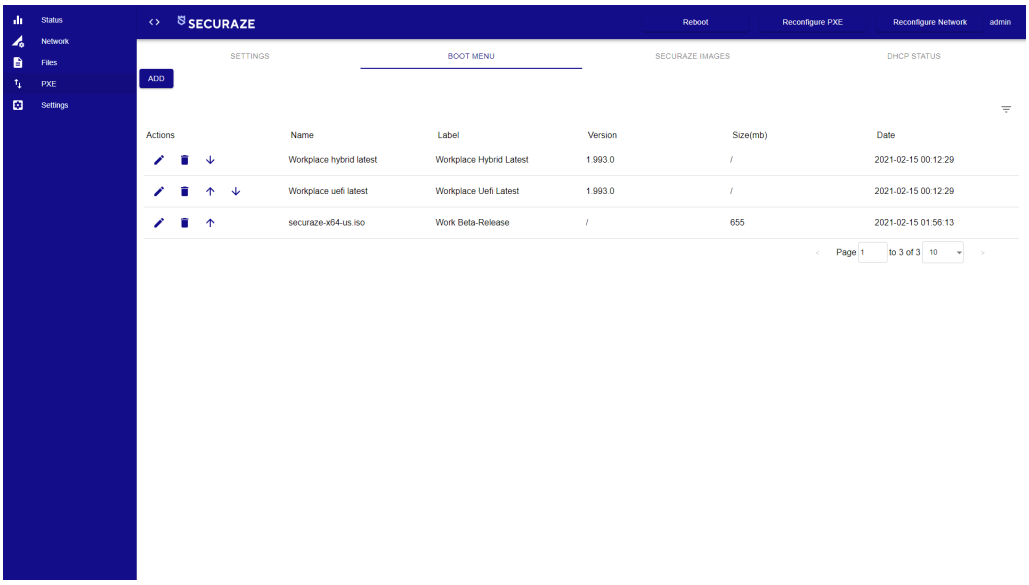
After choosing Custom, enter a name for the PXE menu at **Label** and select the image file by clicking on it.
You can choose the default language which should be used for Securaze Work by selecting a language.
Further you can assign a default Securaze username and password which will be used by Securaze Work.

Note: Currently only the English keyboard layout is supported. Please be aware of this when entering your password.

Confirm your selection by pressing **SELECT**.



Now you will see the image file in the **BOOT MENU** display and you can change the order by clicking on the red arrows.

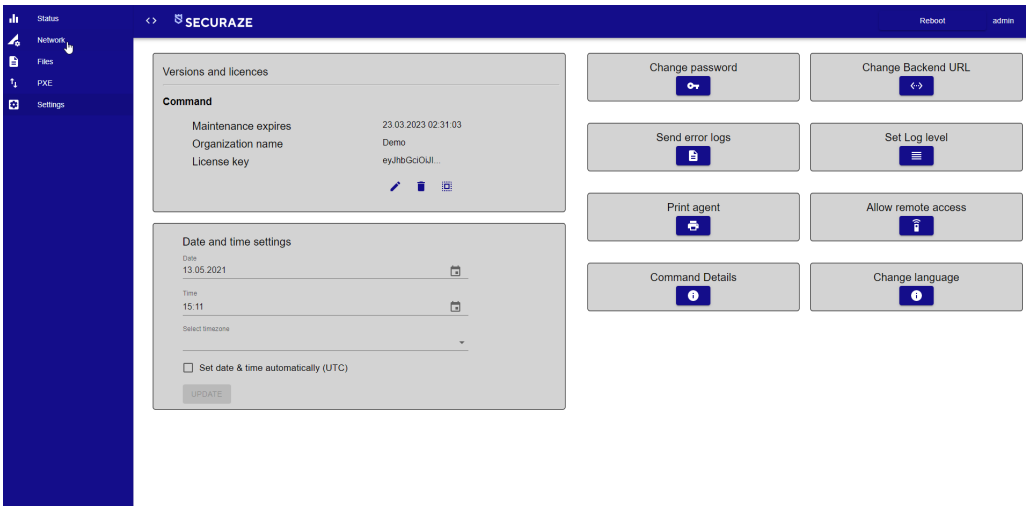


To activate the PXE settings in the system, click on **Reconfigure PXE** in the upper right corner.

To complete the initial configuration, a restart is necessary. To do this, click on **REBOOT** in the upper area.

1.3.5.4 Settings

In the Settings menu you can make various adjustments.



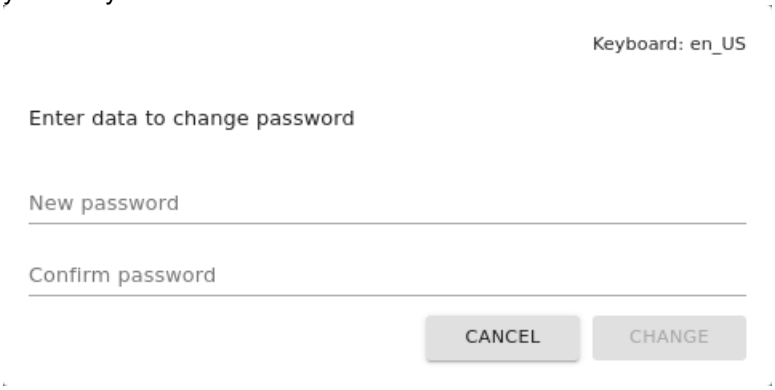
On the top left you will find information about versions and licenses. In this box you can see when the maintenance expires and your license key.

In the box below you can set the date and time or choose to set it automatically.

In the right area you can make various settings:

- **Change password**

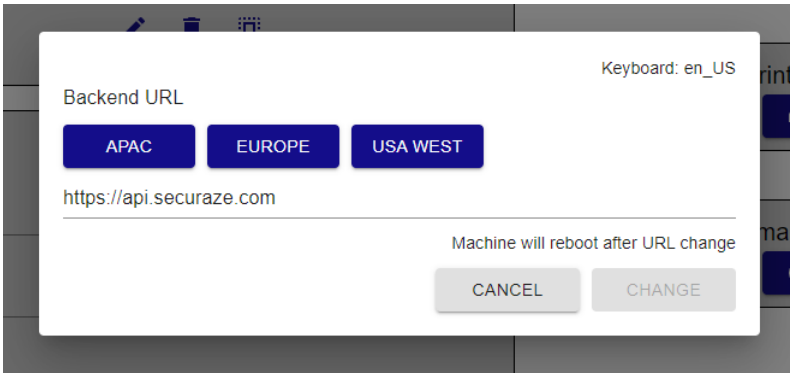
Here you can change the password. To do this, enter the new password and confirm your entry.



Press CHANGE to confirm your entry.

- **Change Backend URL**

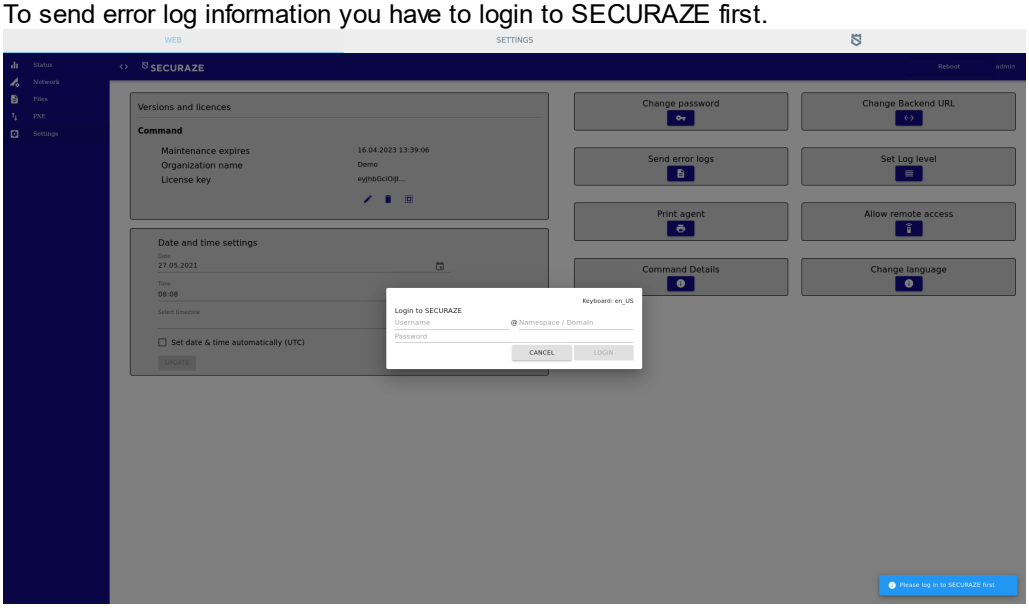
Here you can change the server by selecting the desired region.



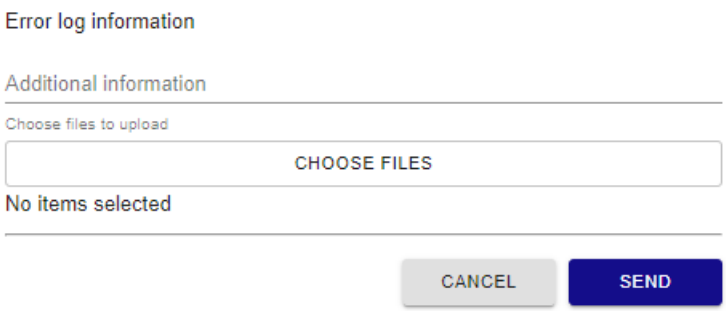
Press CHANGE to confirm the selection.

- **Send error logs**

To send error log information you have to login to SECURAZE first.



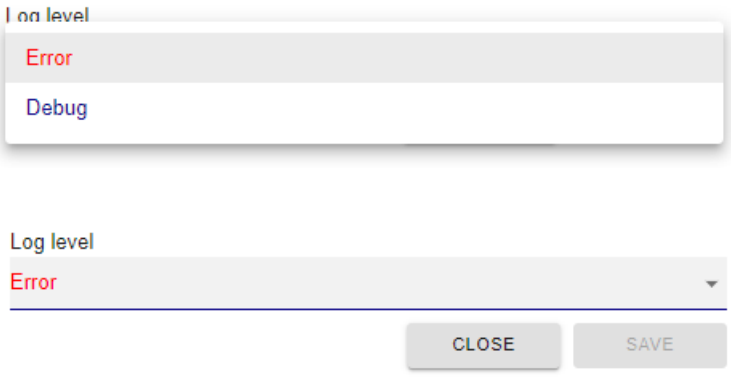
After the login you can enter the error log information and upload a file.



Press **SEND** to send the information.

- **Set Log level**

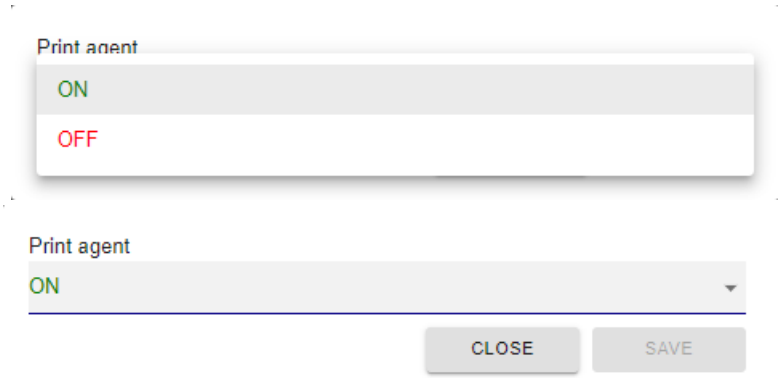
Here you can set the log level.



Press **SAVE** to confirm the selection.

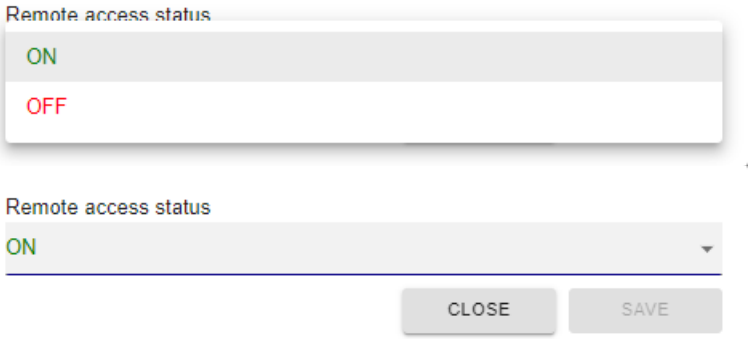
- **Print agent**

If there are multiple Command machines in a workspace, only one of them can have the Print agent turned on. To see if the Print agent is on, just click on the setting and it'll show the status:



Press **SAVE** to confirm the selection.

- **Allow remote access**



Press **SAVE** to confirm the selection.

- **Command details**
- **Change language**

Press **SAVE** to confirm the selection.

Getting started

2 Getting started

Before you can start with the first erase operations, please make some basic settings in Securaze Dashboard.

Under Preparations 48 you will find an explanation of the settings that you need to make once before the first use of the erasure software.

The Recurring Tasks 57 section covers the settings that you will make more often during the course of the application. It also gives you an overview of the options for storing customer-specific requests for erasure, which Securaze Work executes immediately after login.

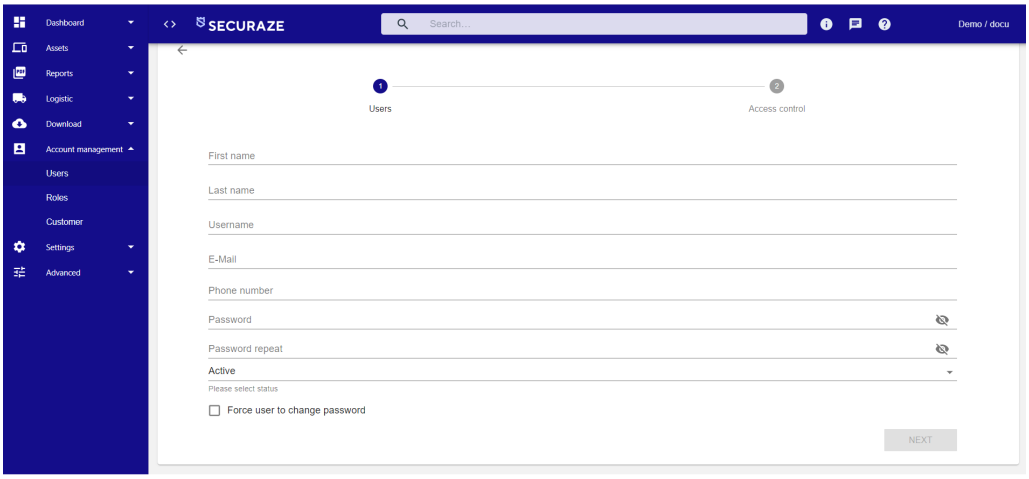
2.1 Preparations

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

2.1.1 Creating a new user

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

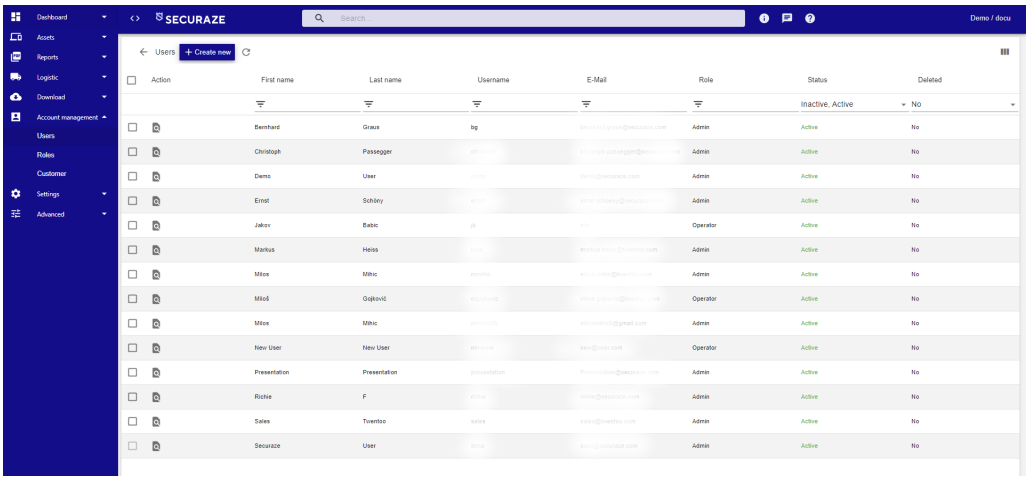
Here you enter the data of the new user and define a password.
By selecting the item **Force user to change password**, you assign a temporary password which the user must change after the first login.



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

In the next step you select the authorization level of the user.

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



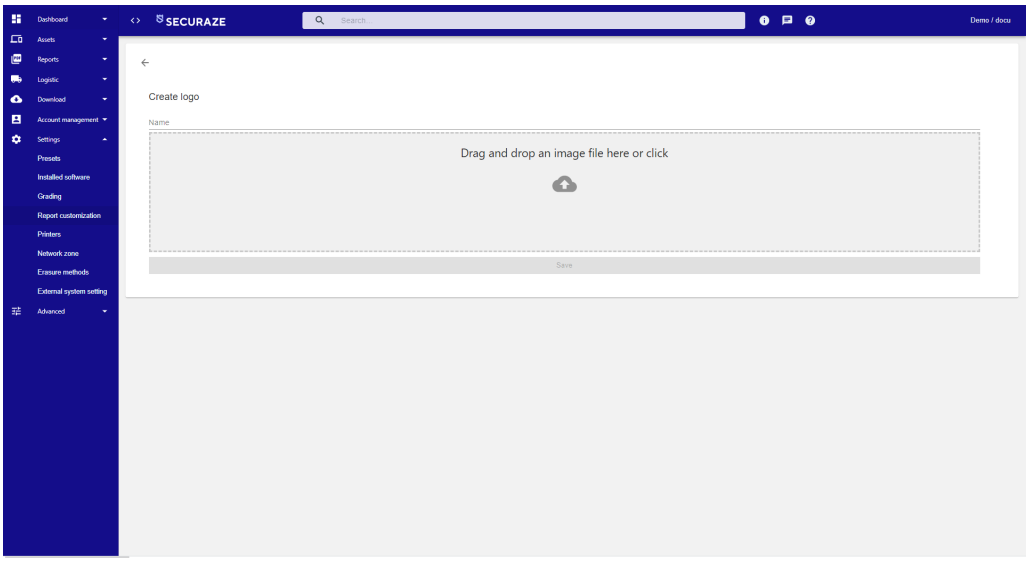
For information on editing or deleting an existing user, see Securaze Dashboard - Menu Items - Users 196.

2.1.2 Create a 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

Upload the desired logo by kicking on **UPLOAD** and assign a name.

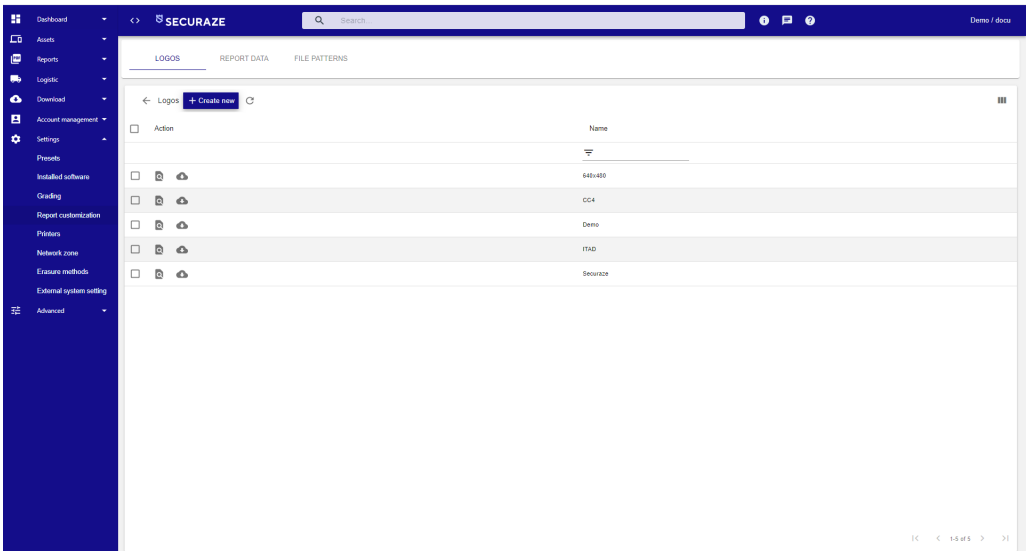


Recommended size of the logo:
Square shaped: 512 x 512 pixel

Rectangular shaped:
600 x 400 pixel

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.**



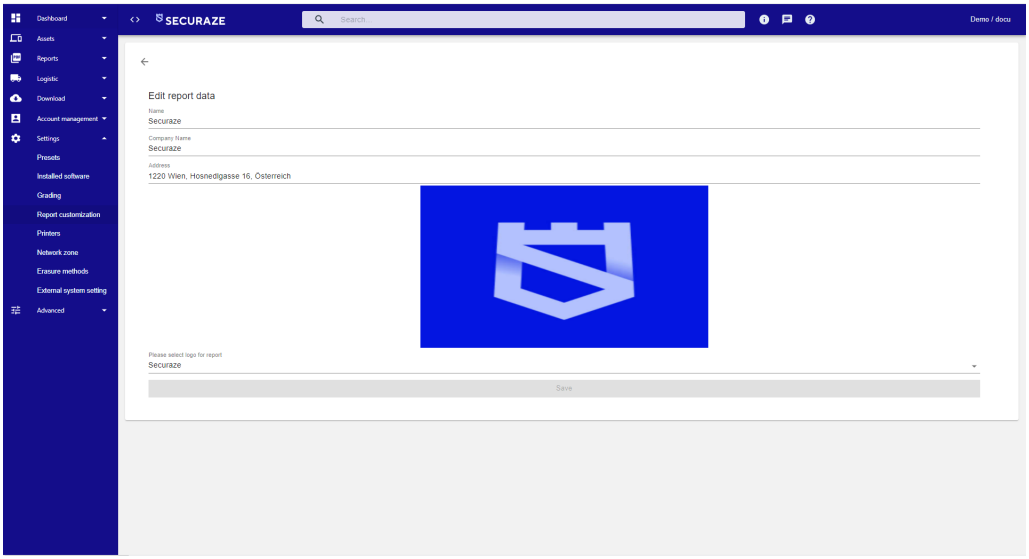
For information on editing or deleting an existing logo, see Securaze Dashboard - Menu Items - Settings - Logos 216.

2.1.3 Create new report data

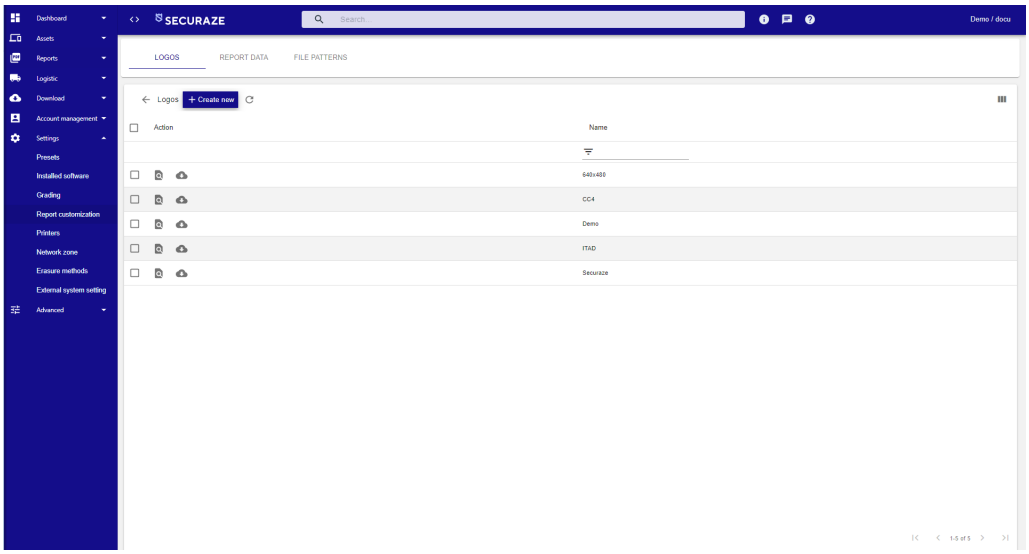
To create new report data, click on **Settings - Report customization** in the Menu section and then on the tab **REPORT DATA.**

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.**



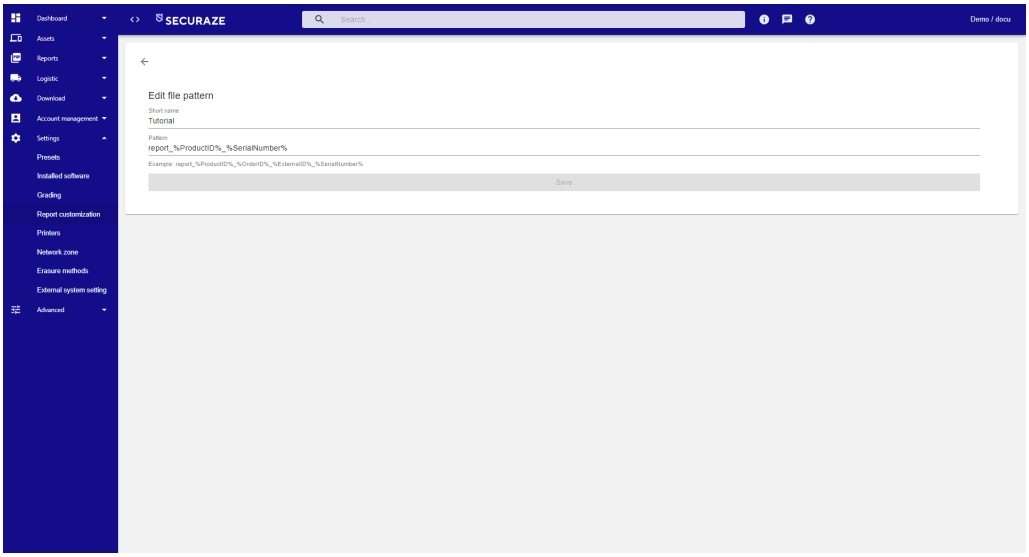
For information on editing or deleting already created report data, see Securaze Dashboard - Menu items - Settings - Report data 219.

2.1.4 Create a new file pattern

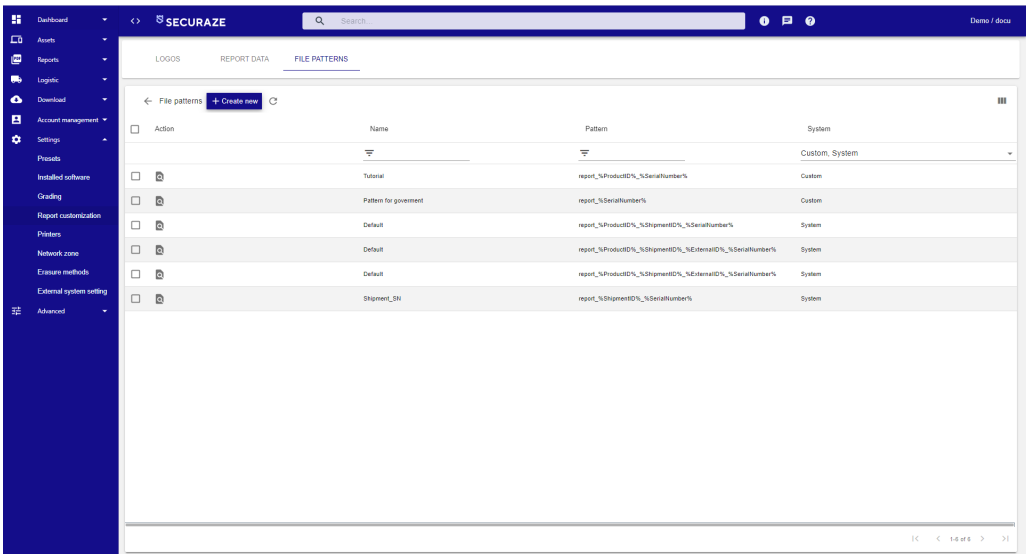
To create a new file pattern, click on **Settings - Report customization** in the Menu section and then on the tab **FILE PATTERNS.**

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**.



2.1.5 Creating a new printer

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

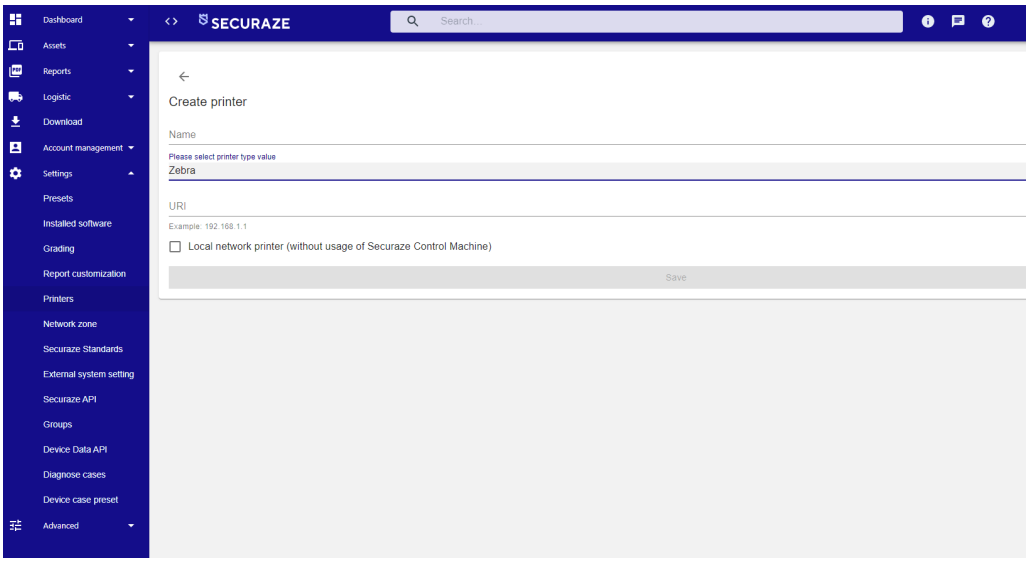
Here you enter the name of the printer and select the printer type from the list.
For the name, you can choose any name you find most suitable.
Currently supported printer types are **Zebra** and **GoDEX,** excluding Zebra ZSB series (small office / home printers), due to their limitations.

The following GoDex printers are supported:

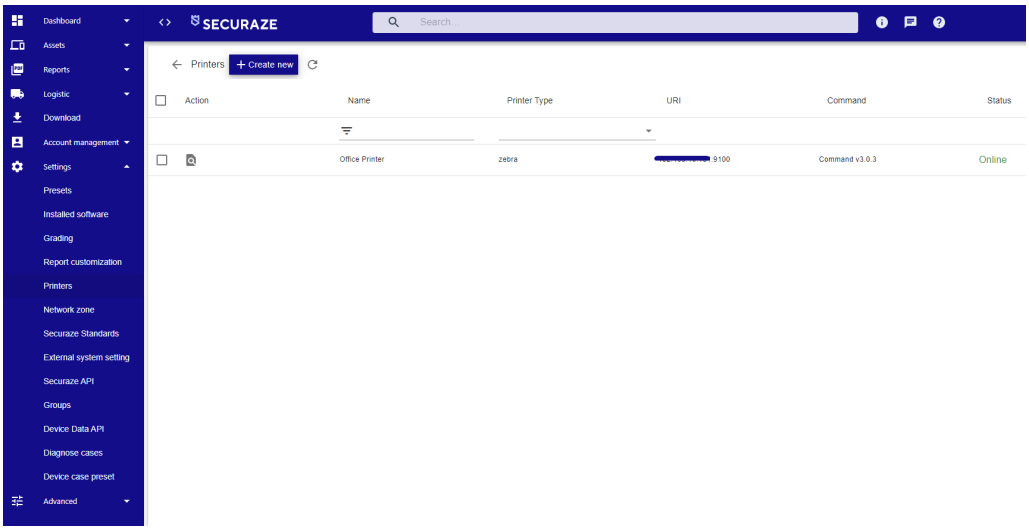
RT700 / RT730
RT700x / RT730x
RT700i / RT730i
RT700iW / RT730iW
RT200 / RT230
RT200i / RT230i
RT863i
GE300 / GE330
G500 with Ethernet / G530 with Ethernet
DT2x / DT4x

The URI of the Zebra printer can be determined in the following way:
1. Ensure the printer is powered on.
2. Press and hold the feed + cancel buttons at the same time for about 2 seconds.
3. A settings sheet will print showing the IP address of the printer.

It is important to add the port :9100 at the end of the URI of the Zebra printer, like in this example: "192.168.1.1:9100"



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



For information on how to edit or delete an already created printer, see Securaze Dashboard - Menu Items - Settings - Printers 227.

2.2 External Systems

Enter topic text here.

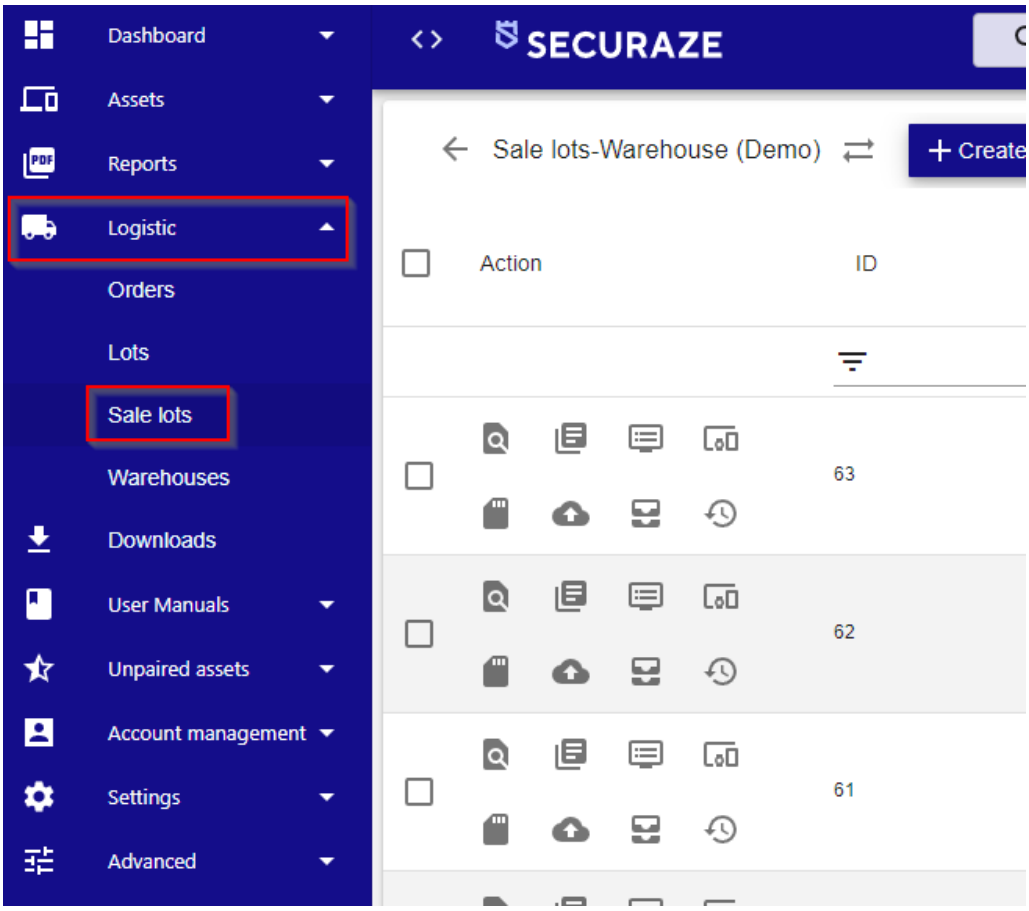
2.2.1 Re-trigger data sending

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.

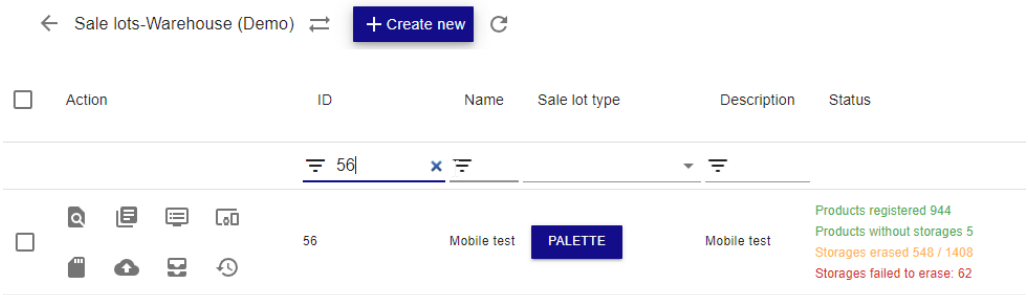
This can be done by asset (you can find the exact asset in Securaze Dashboard in the tab Assets - Work / Mobile / Single-disk drives) or by Container (so erasure data for all the assets from a particular Container can be re-sent to the external system).

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

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

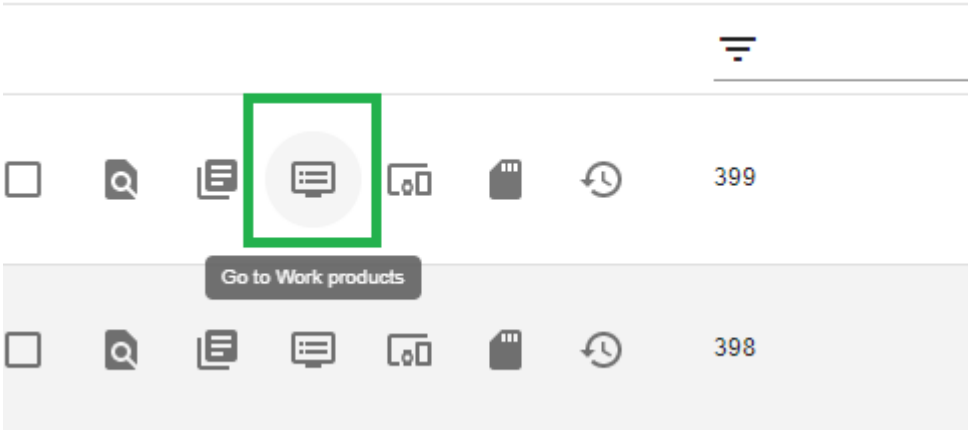


2. Search for the Container by ID, Name or Description.

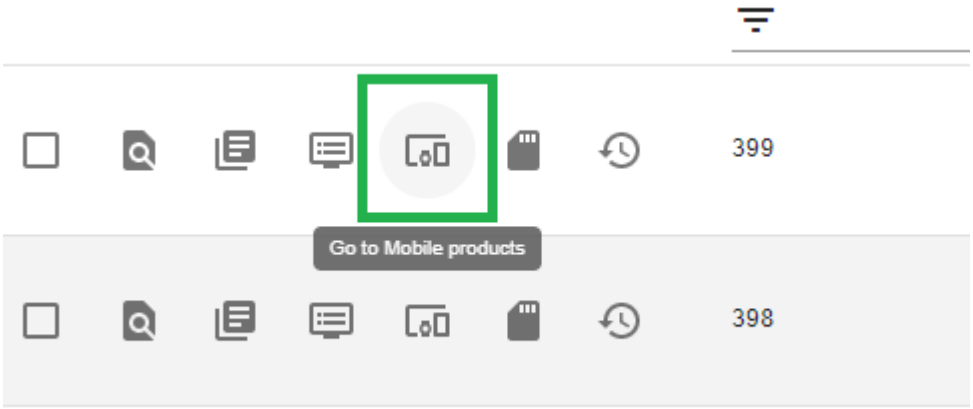


3. After you have found the Container, depending on what assets are included, select the button to go to:

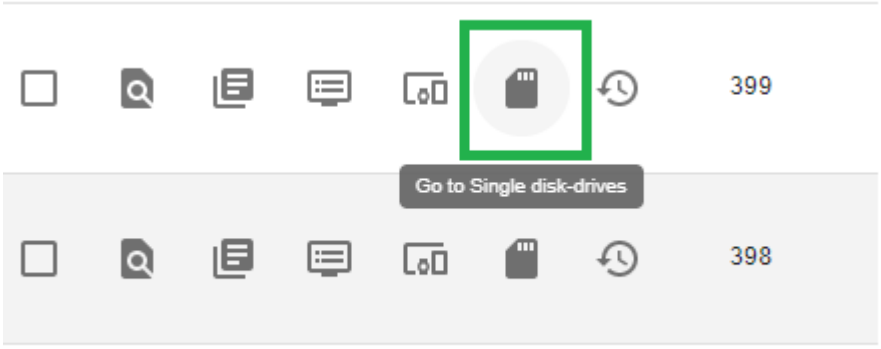
a) Work products (PCs, laptops etc.):



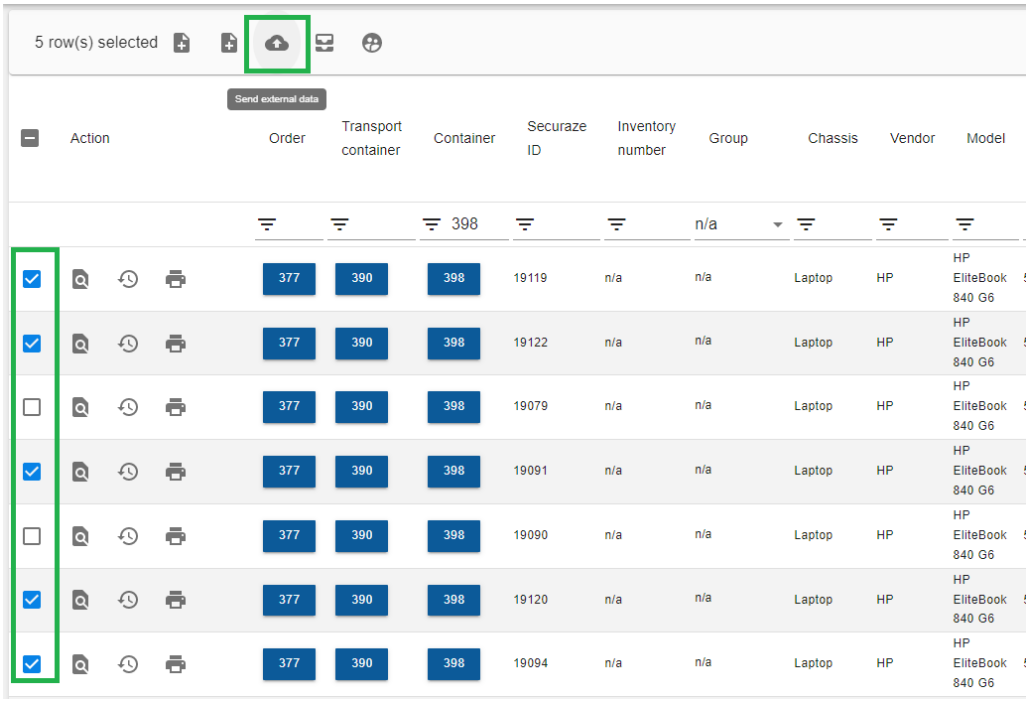
b) Mobile products (Smart phones, tablets etc):



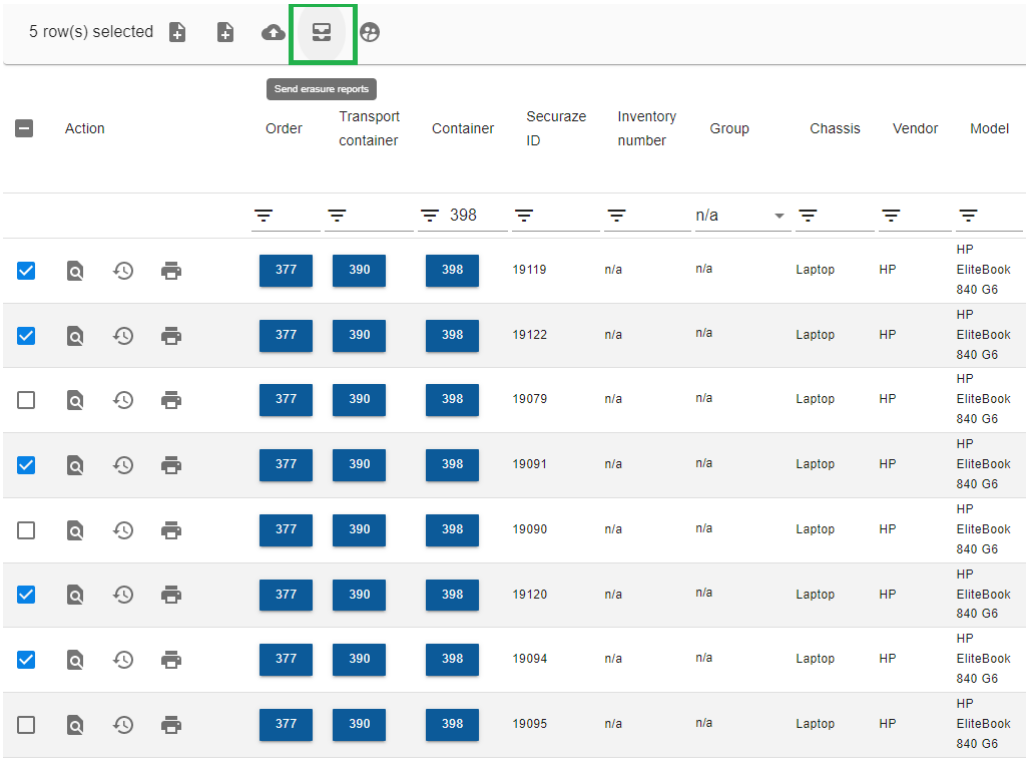
c) Single disk-drives (single disks):



4. In case you have selected Work product, you will be taken to a list of these assets within the selected Container, 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.



This may take a few minutes, depending on the number of assets in the Container. 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.

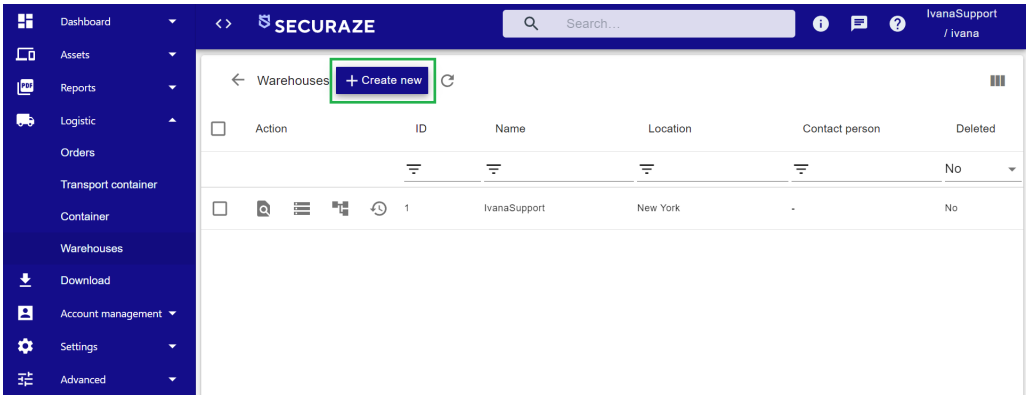
2.3 Recurring operations

While Securaze Work is running, some recurring tasks are performed in Securaze Dashboard.

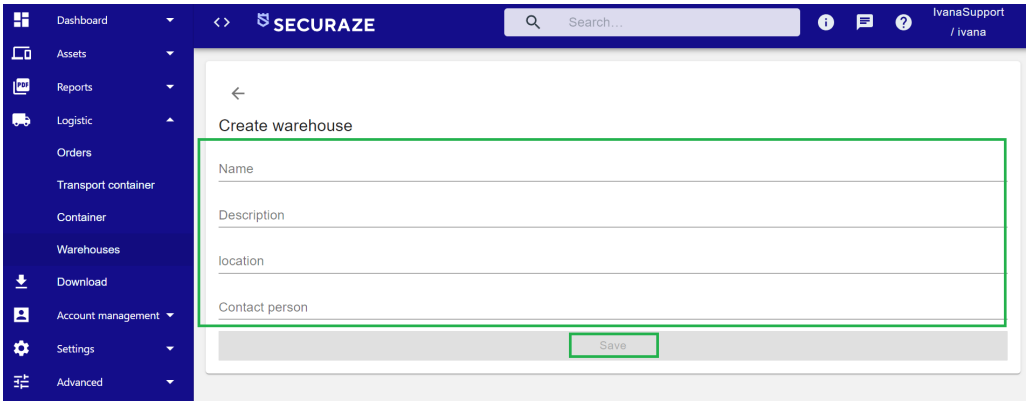
2.3.1 Create a new Warehouse

Warehouses

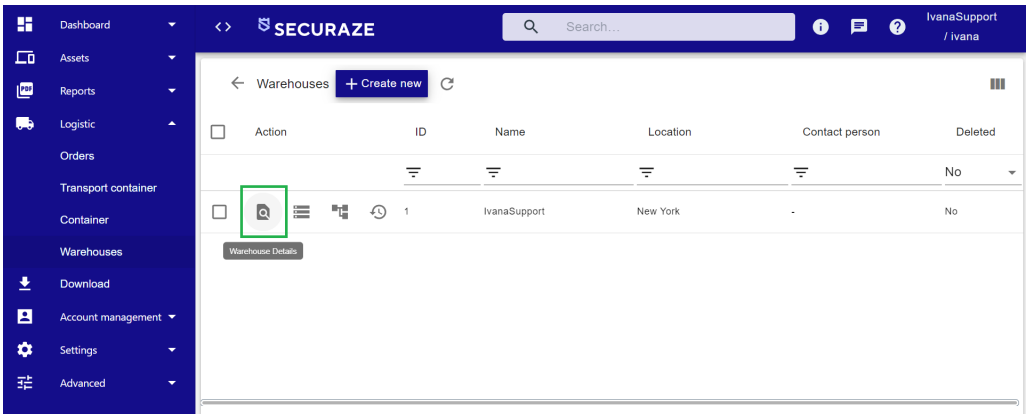
The first component needed in the logistics section to allow a clean workflow of receiving, processing, storing and sending out assets is a warehouse.
This tab can be found in the Dashboard, in the left sidebar menu, under Logistics.



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.



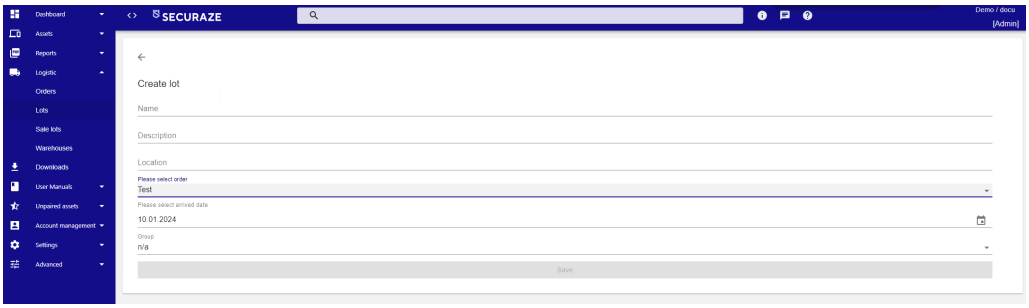
In case you want to edit the information about any warehouse, you can simply click on **Warehouse Details** button, and you will be taken to the details page.
When editing is completed, you should click on **Save** button.



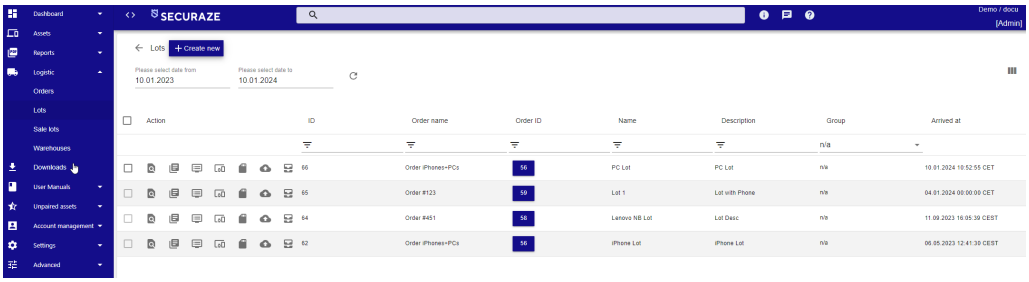
2.3.2 Create a new Transport Container

Each time you start an erasure or diagnostic session, you will be asked to select the Point of origin. This point of origin is the transport container to which the asset in question was assigned.
The transport container is the container on which the assets were delivered to you. These transport containers can be created in Dashboard, under Logistics – Transport container.
By using the concept of transport container 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 Incoming Pallet, click on **Logistic - Transport Container** in the Menu section and then click + Create new

Here you enter the name, description and location of the transport container and select the pickup order and arrival date.



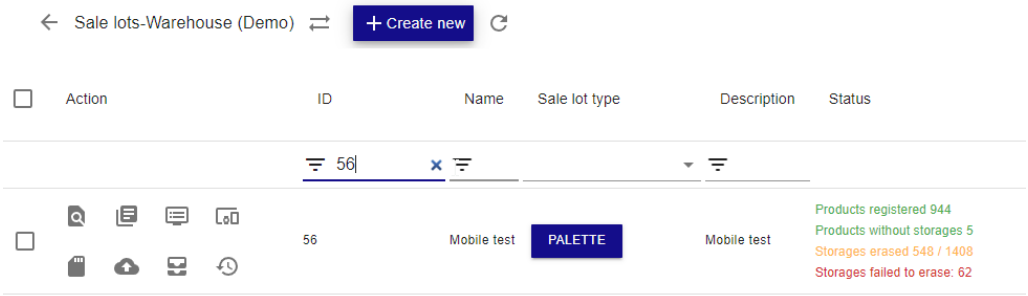
After confirming the selection by clicking **SAVE**, the newly created Incoming Pallet is visible in the menu **Logistic - transport container**.



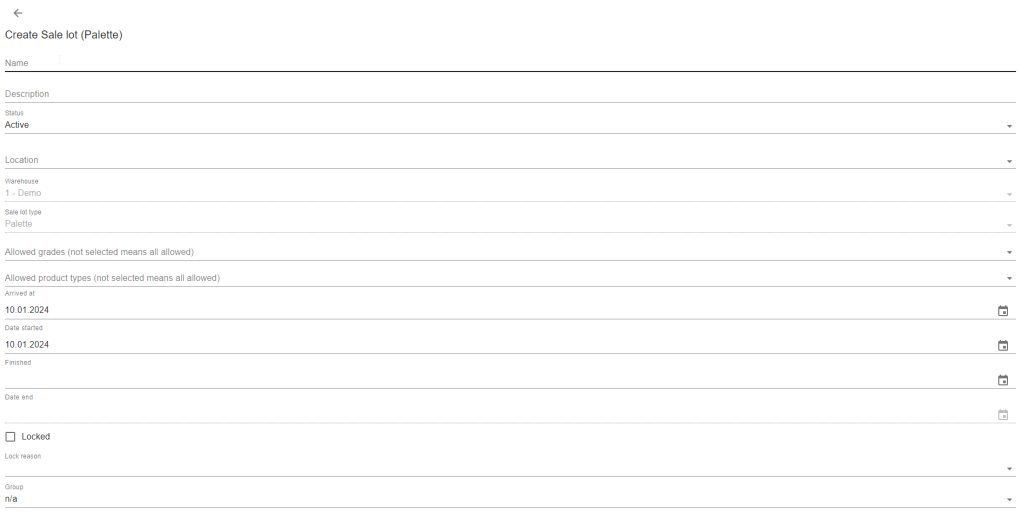
For more information on Incoming Pallets, see Securaze Dashboard - Menu Items - Transport Container 190.

2.3.3 Create a new Container

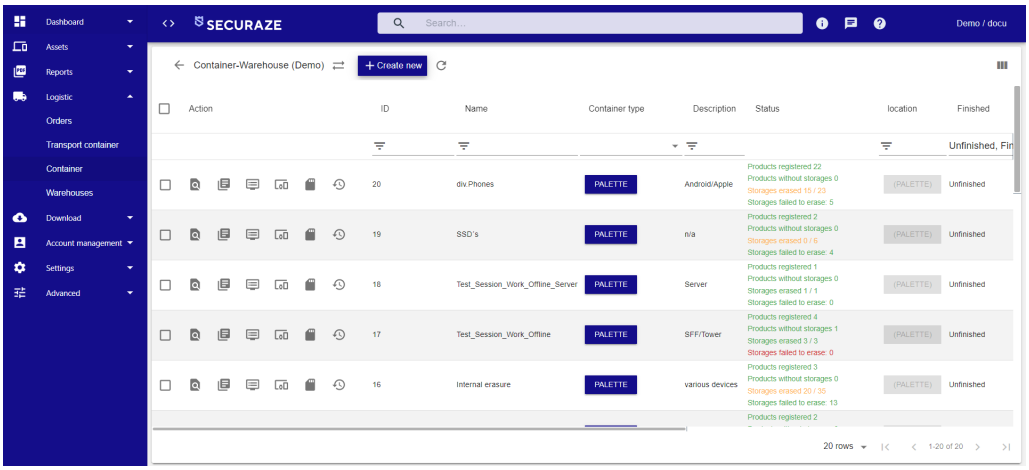
To create a new container, click on **Logistic - Container** in the Menu section and then on + Create new



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

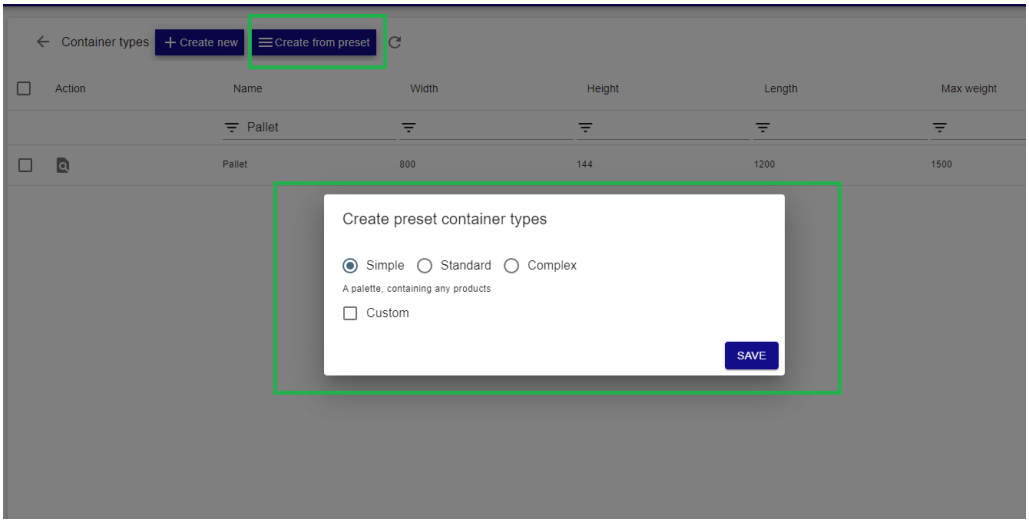


After confirming the selection by clicking **SAVE**, the newly created container is visible in the menu **Logistic - Container**.

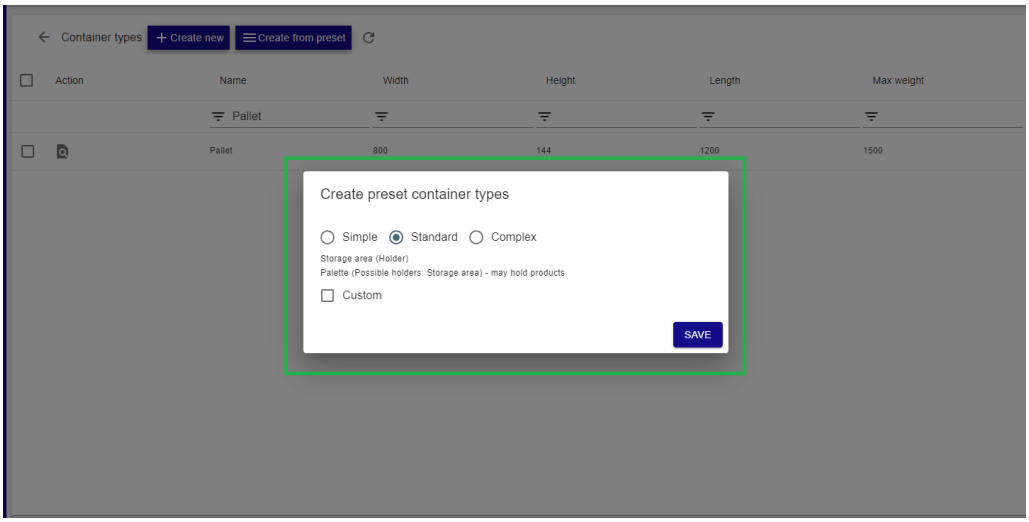


If you want to create a new container type from preset, you can click on Create from preset button.
You will then be prompted to select the type of preset you want to have when creating your containers.

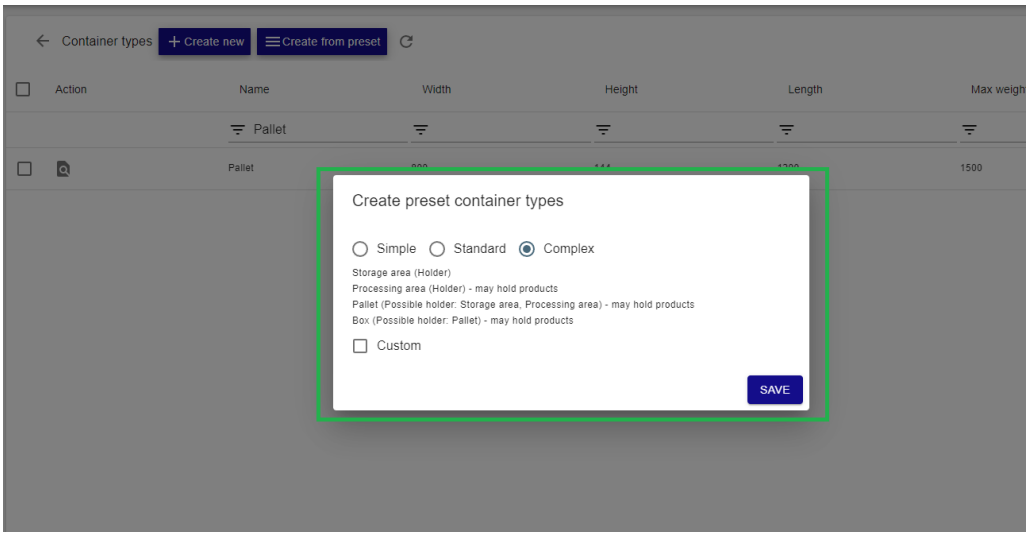
If you select **Simple**, you will be able to create a new container with just a Pallet as allowed container holder.
A Pallet can contain products only.



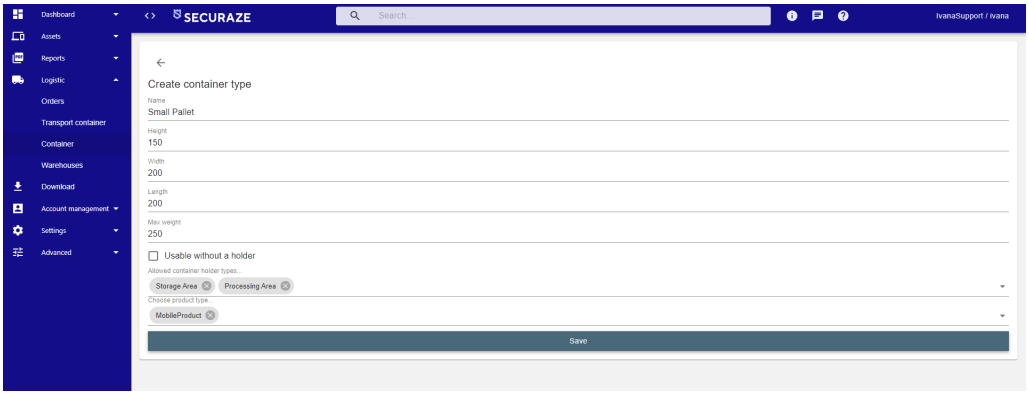
If you select **Standard**, you will be able to have Storage area as holder, and a Pallet as product holder.



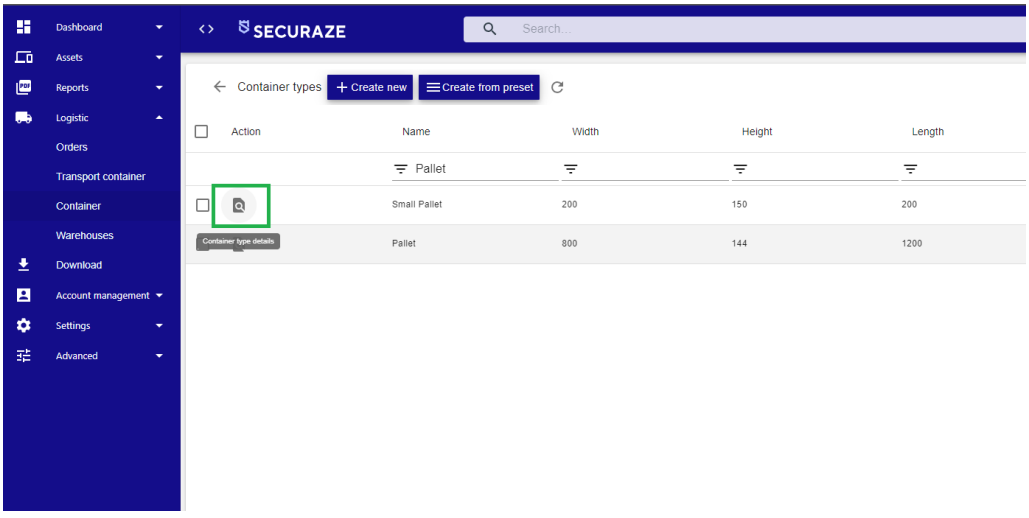
If you select **Complex**, you will be able to have Storage area as holder, Processing area as holder (it can also contain Products), Pallet as product holder and Box as product holder.



Once you are sure what kind of preset suits your needs, you select it and click on SAVE button.
You may now click on **+ Create new** container type and fill in the information.
Under Allowed container holder types, you will be able to select the name for your container, size (length, width, height), weight, holder type and product type (specify which products will be stored in such container).
As an example, we created one called “Small pallet”:



You can edit details about the container at any point, by clicking on Container details:

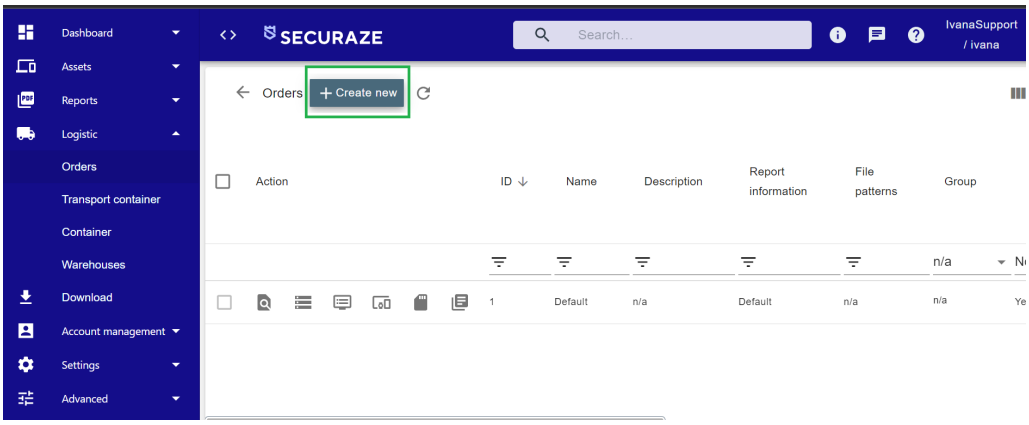


For more information on Stock container, please refer to Securaze Dashboard - Menu items - Container 192.

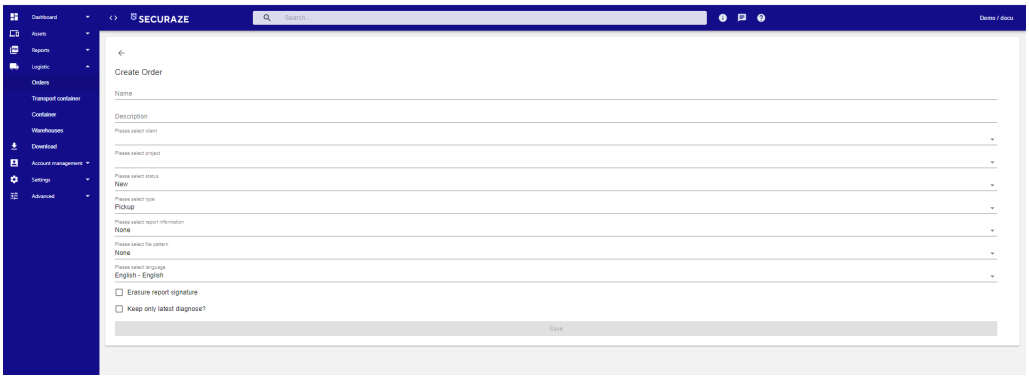
2.3.4 Create a new Order

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

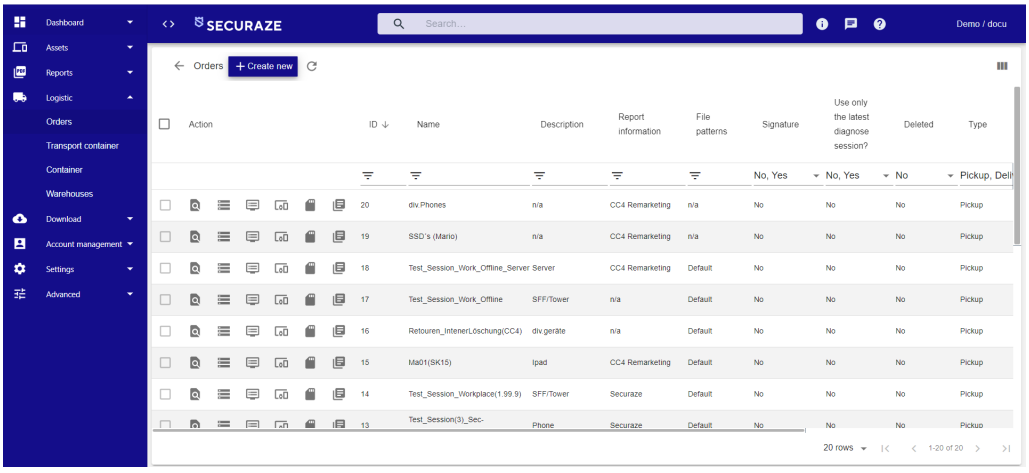
+ Create new



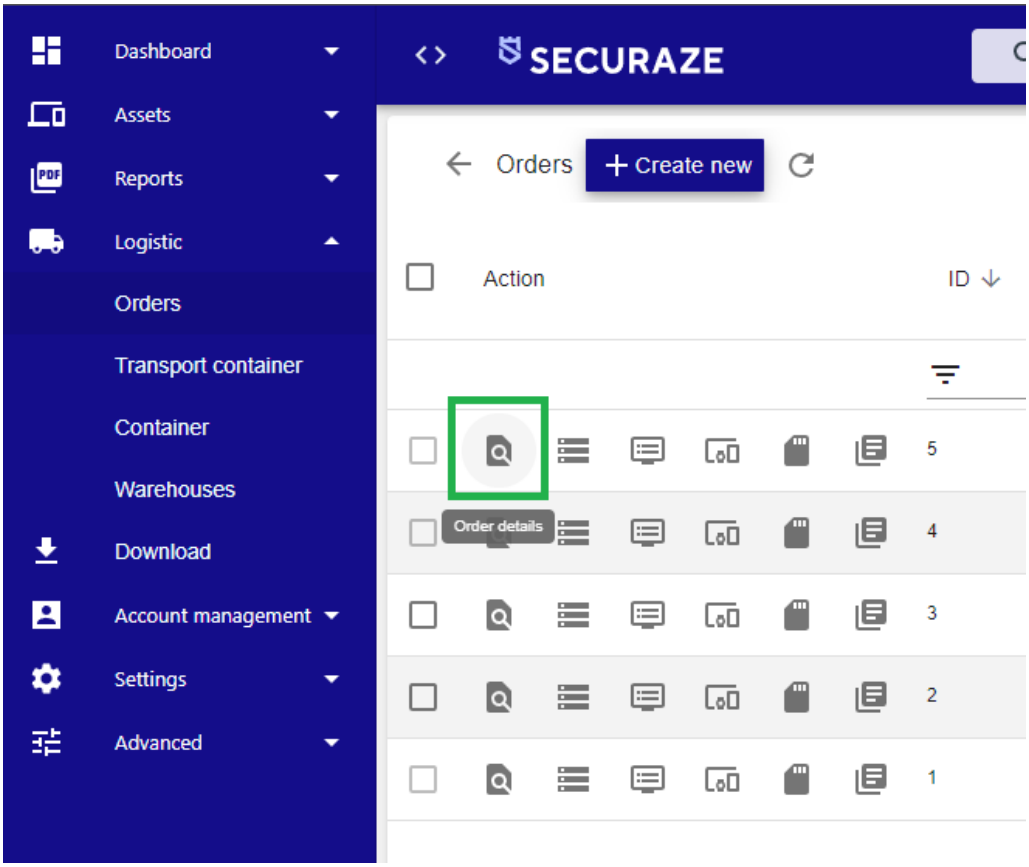
Enter the name and description of the pickup order and select the report information and file name pattern you entered.



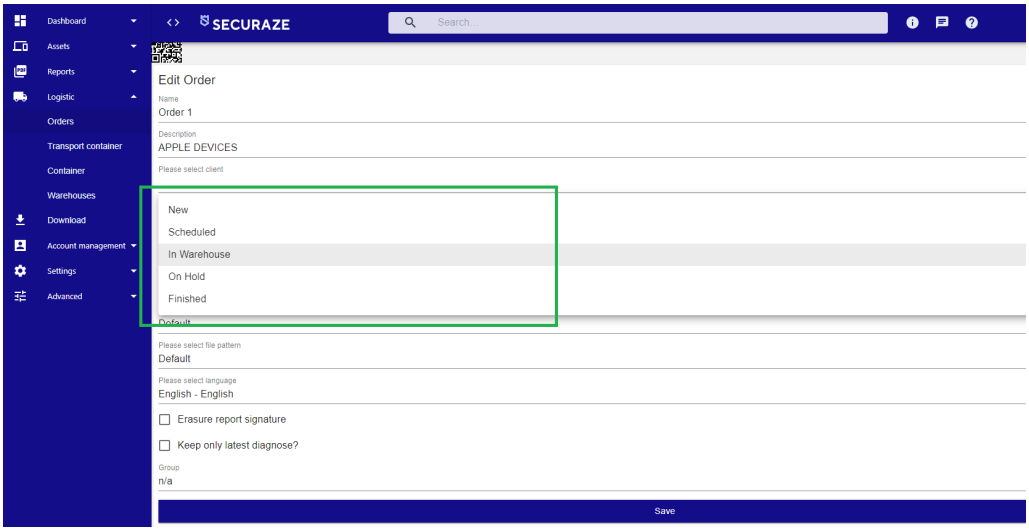
After confirming the selection by clicking on **SAVE**, the newly created pickup order can be seen in the menu **Orders.**



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



Most common change you will make is the status:

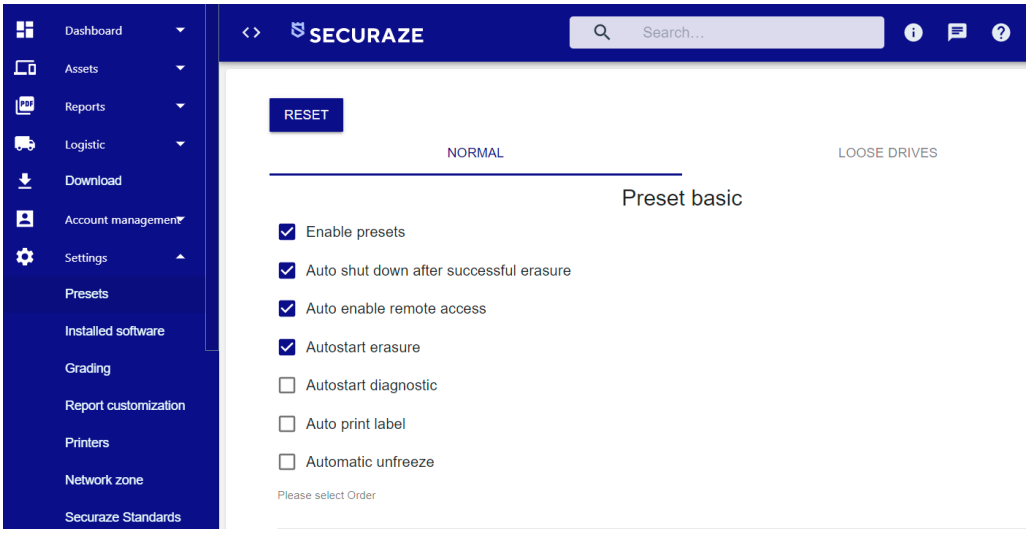


For more information on Pickup orders, see Securaze Dashboard - Menu Items - Orders 187

2.3.5 Set presets

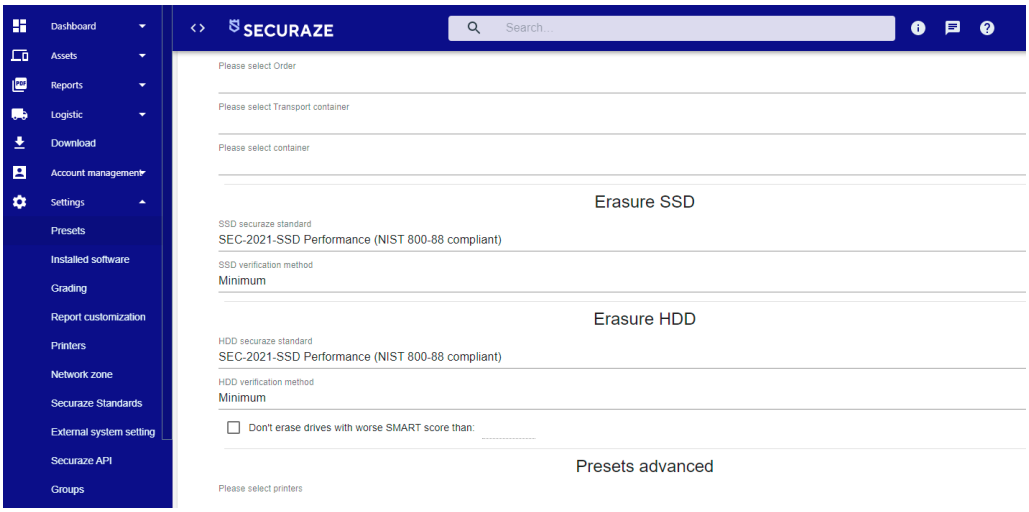
To define specific settings that Securaze should execute immediately after login, click on **Settings - Presets** in the Menu section.

Before you can make the desired settings, click **Enable preset** under **Preset basic:**

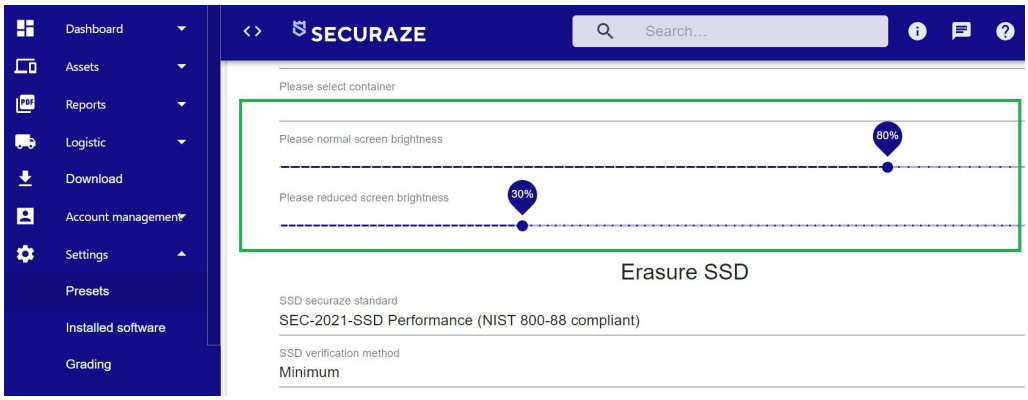


You can make the following settings:

Auto shut down - 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.
Auto start erasure - Check this box for auto start erasure.
Auto start diagnostic - Check this box for auto start diagnostic.
Auto print label - Select this checkbox to automatically print a label.
Automatic unfreeze - Automatically unfreeze disks for erasure



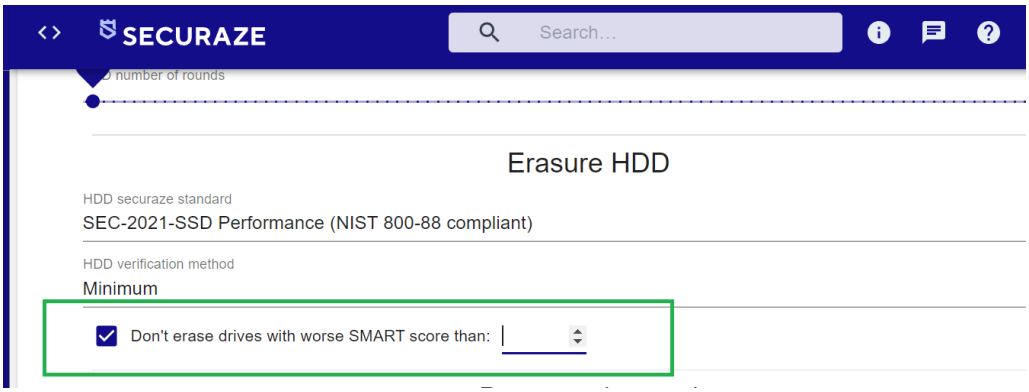
Order - select the desired order from the list.
Transport Container - select the desired transport container from the list.
Container- select the desired stock container from the list.



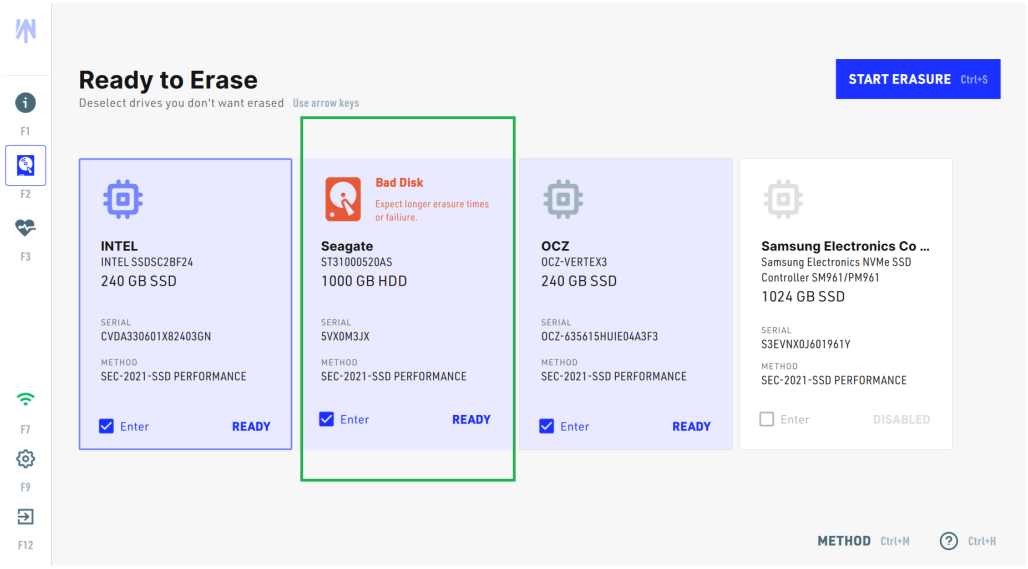
Display brightness adjustment
Available for both Work macOS and Work Linux, working for PC, macOS Native and also Mac booting WorkPC.
The built-in defaults are: normal: 80%, reduced 30%.
Normal Brightness can be set to any value between 20 and 100.
Reduced Brightness can be set to any value between 0 and 100, for when screensaver is displayed during erasure (allowing the screen to be black, if max. power saving is required)
If Diagnose is started, the Brightness goes to 100 until Diagnose is finished, then it is returning to configured Normal Brightness.

SSD securaze standard - select the desired erasure method for SSD drives from the list.
SSD verification method - select the desired verify method for SSD drives. Last verifies the last erasure round, All verifies each round and custom allows to choose a percentage value of the storage size.
HDD securaze standard - select the desired HDD erase method from the list.
HDD verification method - select the desired verify method for HDD drives. Last verifies the last erasure round, All verifies each round and custom allows to choose a percentage value of the storage size.
SMART score - allows Securaze to warn the operator based on a bad SMART score of the storage that the erasure could possibly fail.

If the calculated SMART score is 80-100, the disk is considered to be in good condition. The score of 40-79 describes used condition, and if it's less than 40, a failure is possible.
The operator can set the SMART score bellow which the disks should not be processed in the Presets for HDD erasure:



Preview of a Bad Disk warning in Securaze Work erasure session:



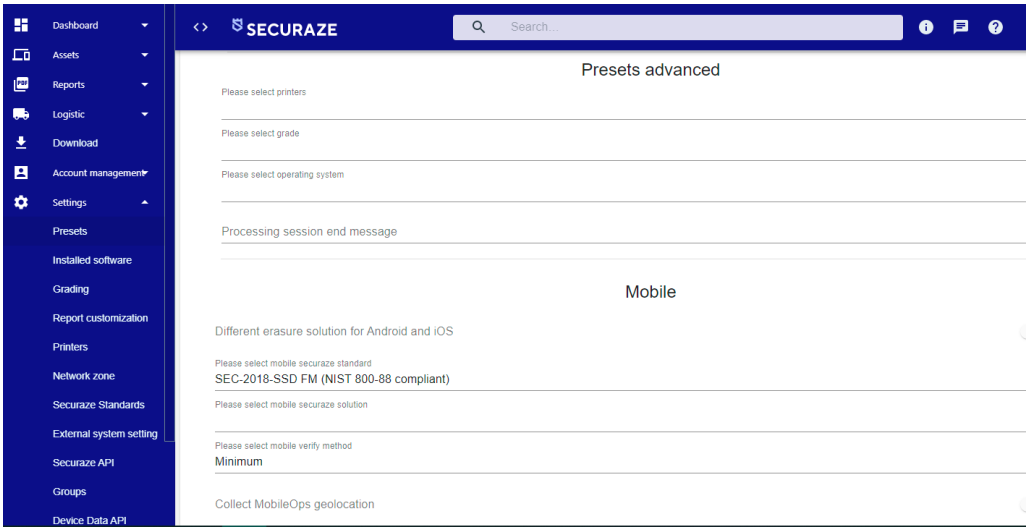
Disk Health Calculation- This setting changes the calculation method of the SMART Health score.

Currently supported:
Securaze proprietary method
Securaze proprietary method (typically the most rigorous calculation method) [Default]

Hard disk sentinel (HDSentinel)
Hard disk sentinel method, based on public available documentation of the algorithm
https://www.hdsentinel.com/help/en/52_cond.html
https://www.hdsentinel.com/smart/index.php

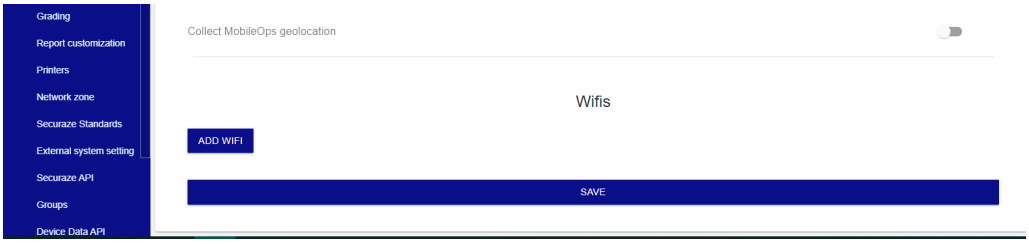
Acronis Drive Monitor
Acronis Drive Monitor method, based on public available documentation of the algorithm
https://kb.acronis.com/content/9264

Preset advanced:



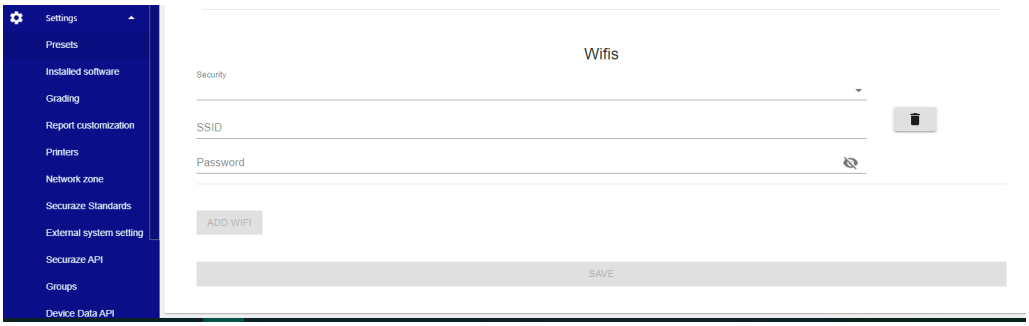
Printer - select the desired printer from the list.
Grades - select the desired grade from the list.
Operating System - select the desired operating system from the list.
Processing session end message - Add a custom message at the end or processing session

Mobile securaze standard - select the desired erasure type for mobile devices.
Mobile securaze solution - select the desired erasure method for mobile devices from the list.
Mobile verify method - select the desired verify method for mobile devices. Minimum verifies 10% of the disk, Last verifies the last erasure round, All verifies each round, and custom allows to choose a percentage value of the storage size to be verified.



Collect MobileOps geolocation - collects the geolocation of the device in the moment of erasure

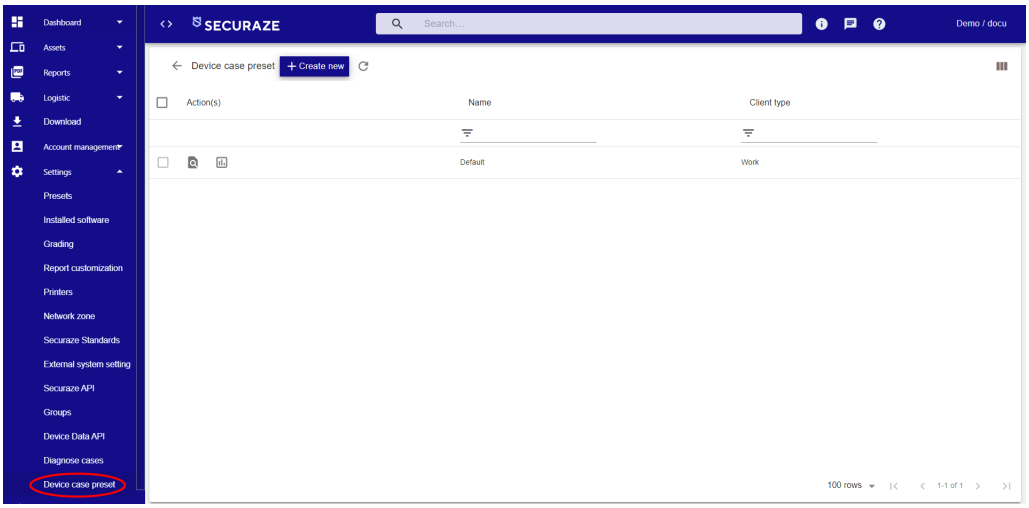
ADD WiFi - preset a WiFi connection



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

2.3.6 Set Device Case Presets

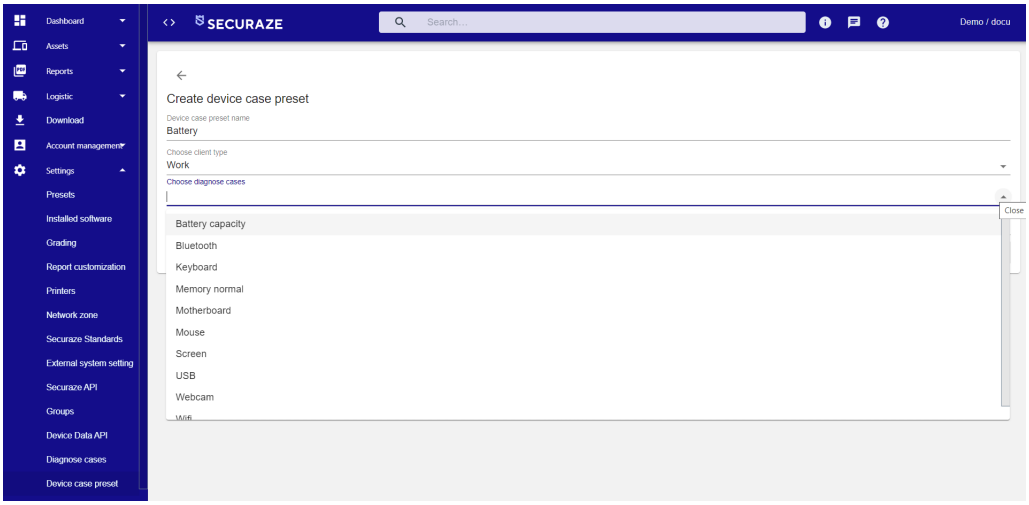
To define specific test cases that Securaze Diagnostics should execute immediately after booting Securaze Work, click on **Settings - Device Case Presets** in the Menu section.

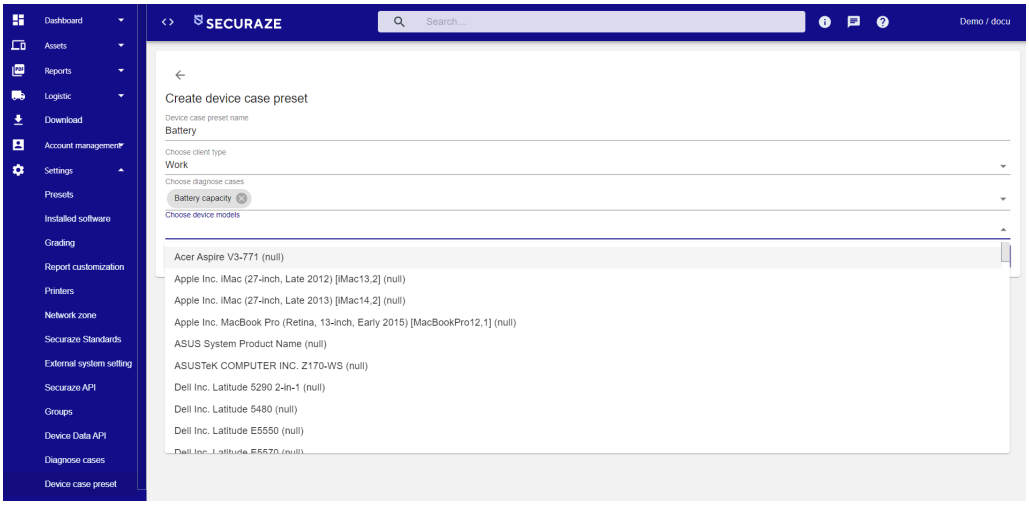


You can use these presets to select which diagnose cases to run on which device models after booting Securaze Work.

To create a new device case preset klick on click + Create new .

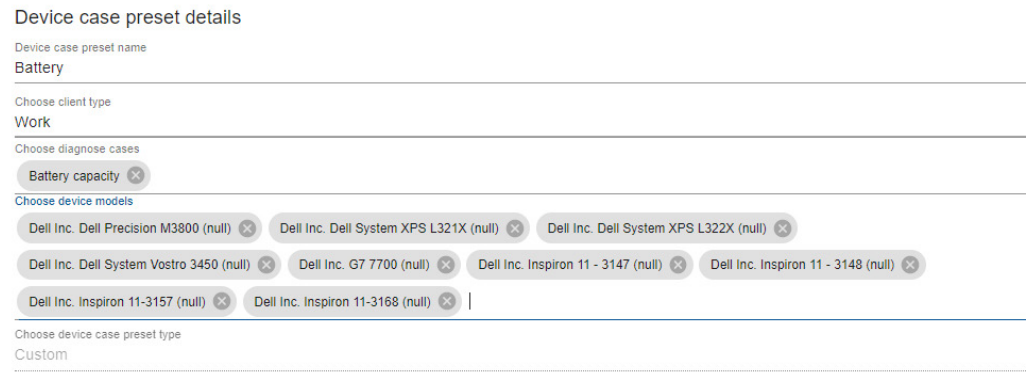
There you can choose a name for your preset, the client type, the diagnose cases and the device models.





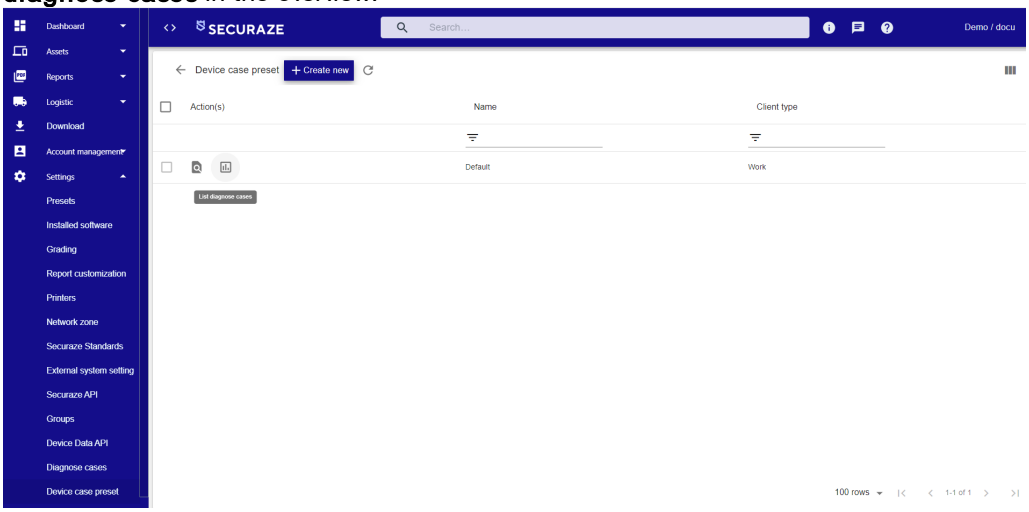
Click on **SAVE** when you are done.

Please make sure that you do not include the same devices in two different device case presets, because then the system will randomly select one of them.

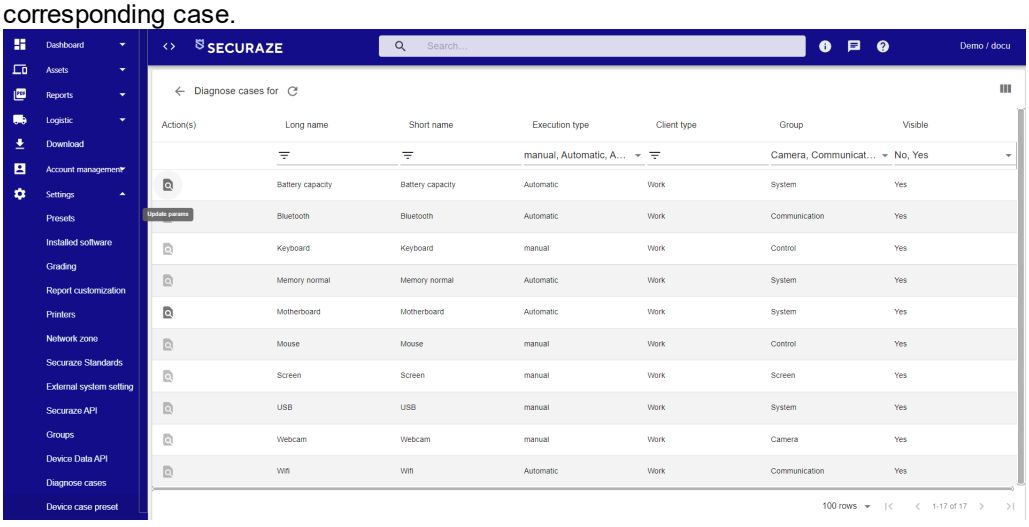


In this case, a preset has been defined to run the Battery capacity diagnose case when one of the listed devices is booted with Securaze work.

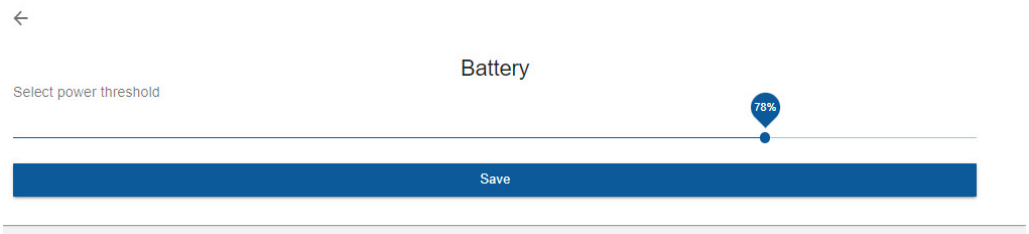
If you want to update the parameters of the chosen diagnose cases, just select **List diagnose cases** in the overview.



There you will find the selected diagnose cases. Select **update params** on the corresponding case.



Here you can select the pass levels for the cases.



Click on **Save** when you are done.

Operation

3 Operation

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

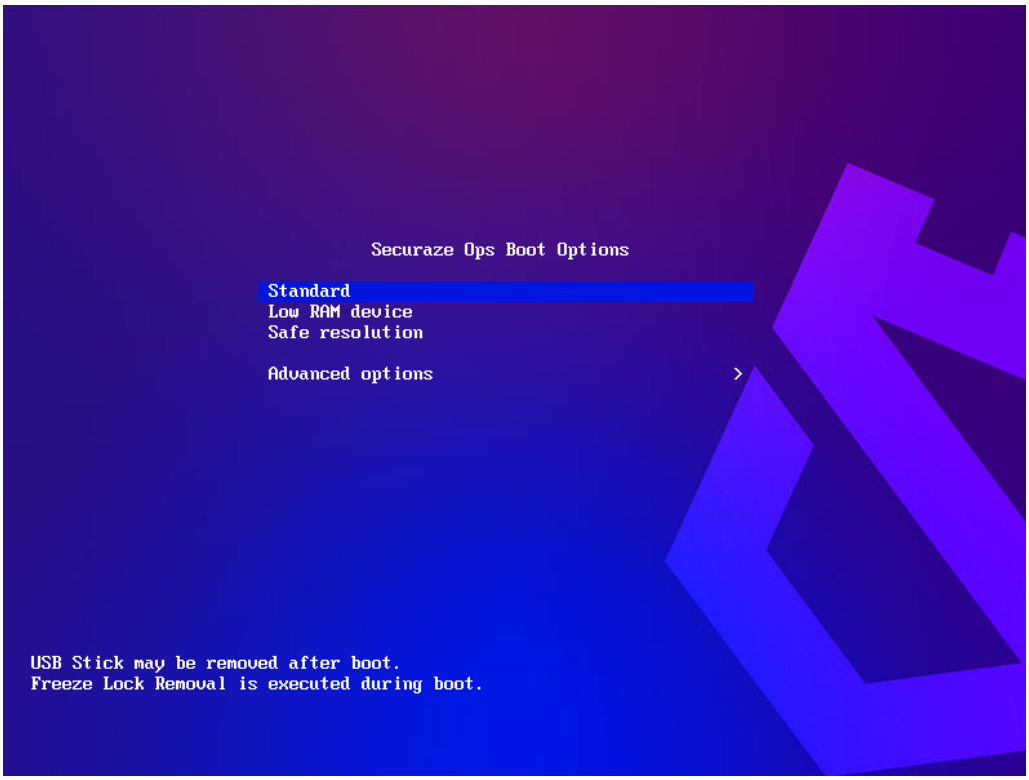
3.1 Starting Securaze Work

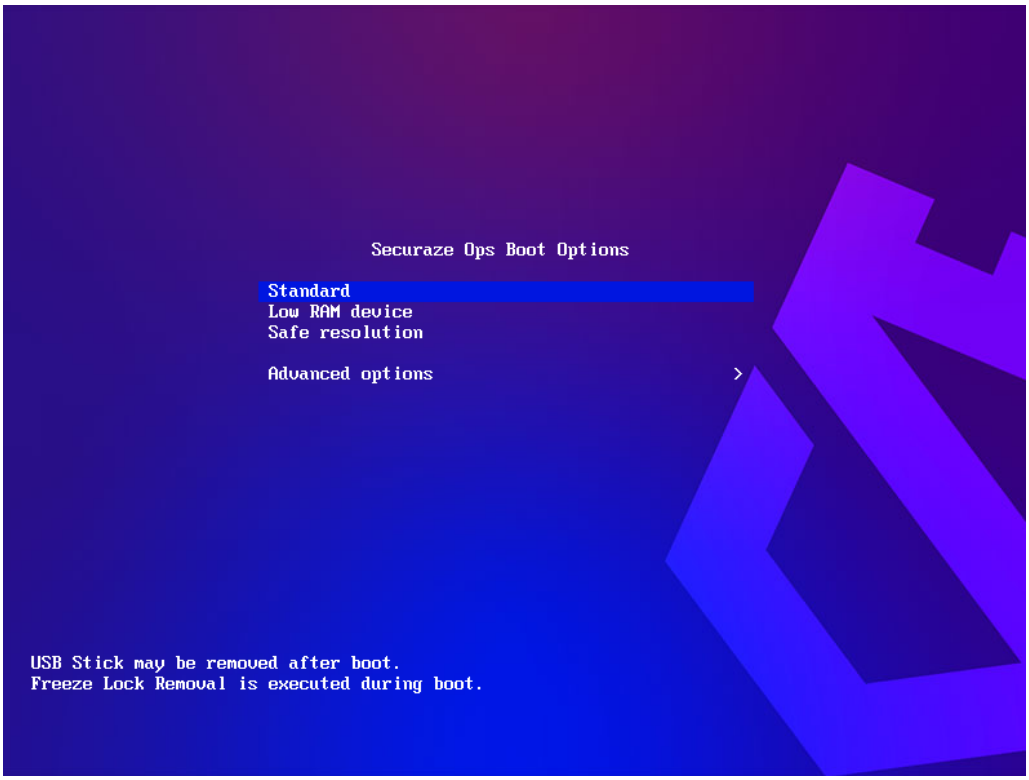
After the Securaze image has been written to the USB stick (for further information see chapter Administration - Installation) 29, the system can be booted with this USB stick.
During the booting process the Securaze Work boot menu will appear.

It depends on if the device has enabled SecureBoot or running on legacy BIOS which Boot-Menu will appear.
The content of both Boot-Menus are similar but not identical.

The suggested options is to choose **Standard** and press enter or wait for the automatic boot.

SecureBoot version

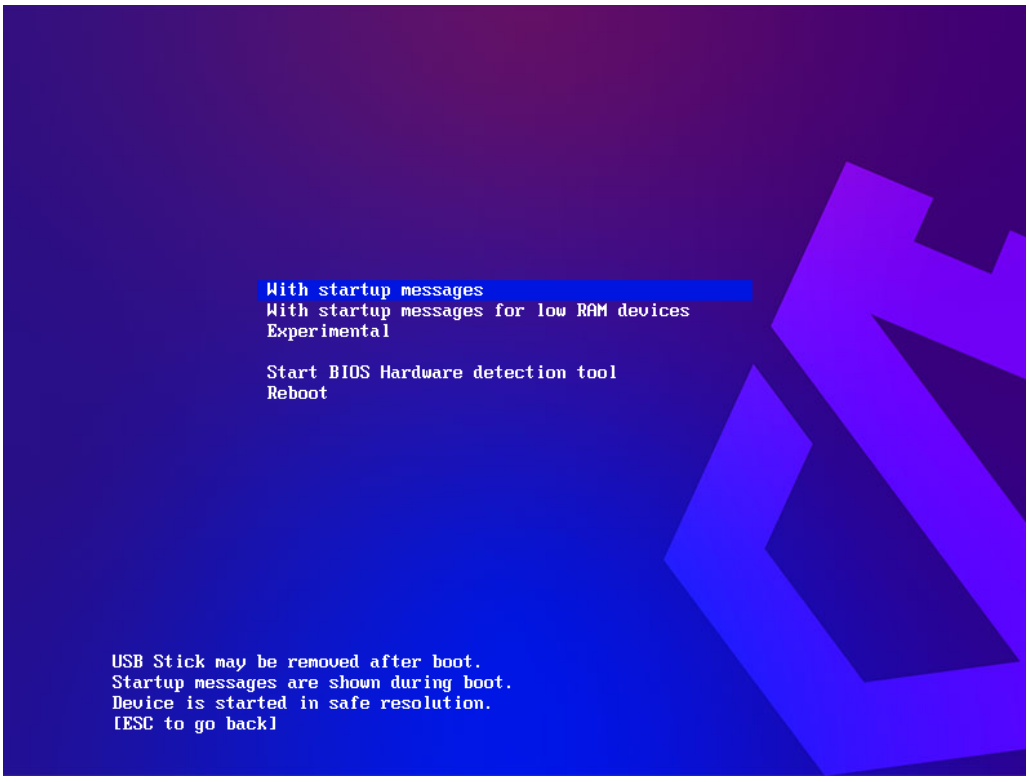




Boot options:

- Standard (USB Stick can be removed after boot)
- Low RAM device (USB Stick must stay connected)
- Safe resolution (starts the device in a safe resolution mode)
- Apple devices (can be used for booting older Apple devices from 2015 and older without T2-chip)

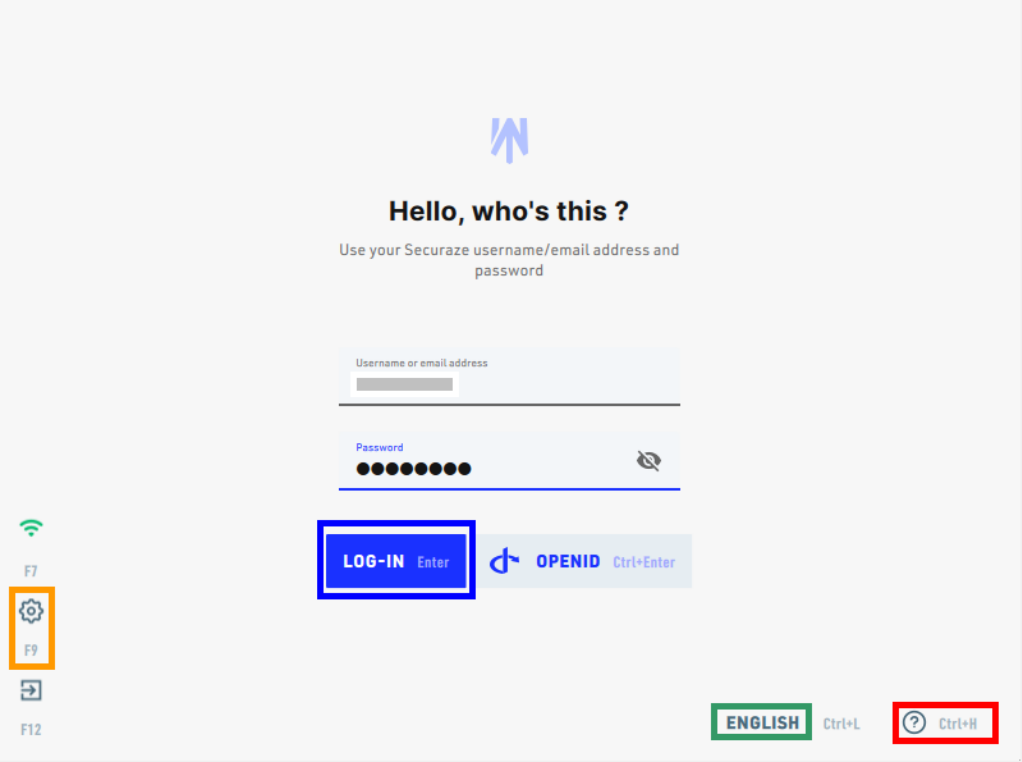
Advanced



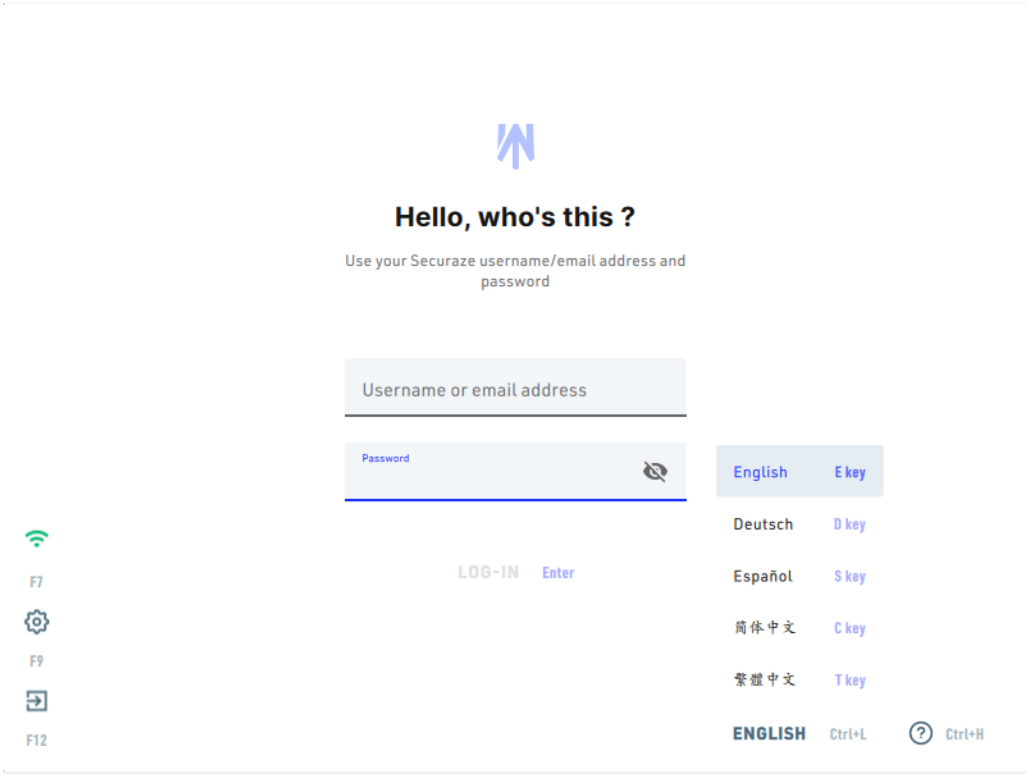
- Non-Secureboot kernel (alternative Kernel with doesn't support SecureBoot, but contains additional drivers)
- Startup message (shows startup messages)
- Experimental (uses experimental settings which may be introduced in upcoming versions into the Standard boot setting)
- BIOS Setup (Opens BIOS setup)

3.2 Login

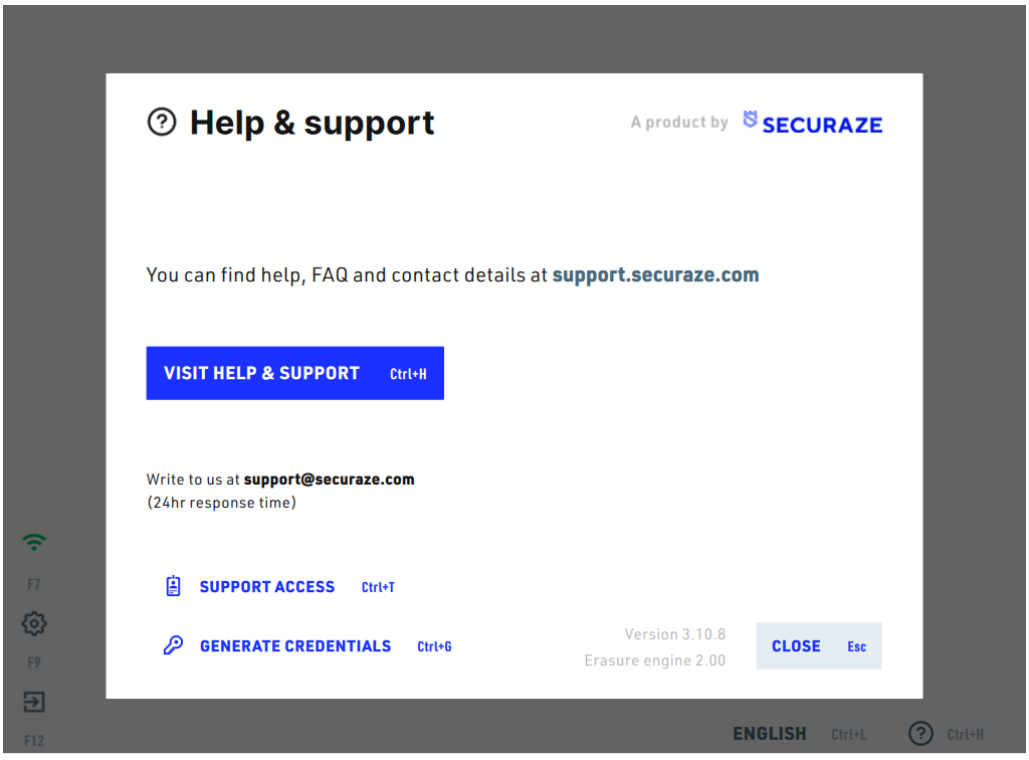
After starting Securaze Work you will be taken to the login screen.



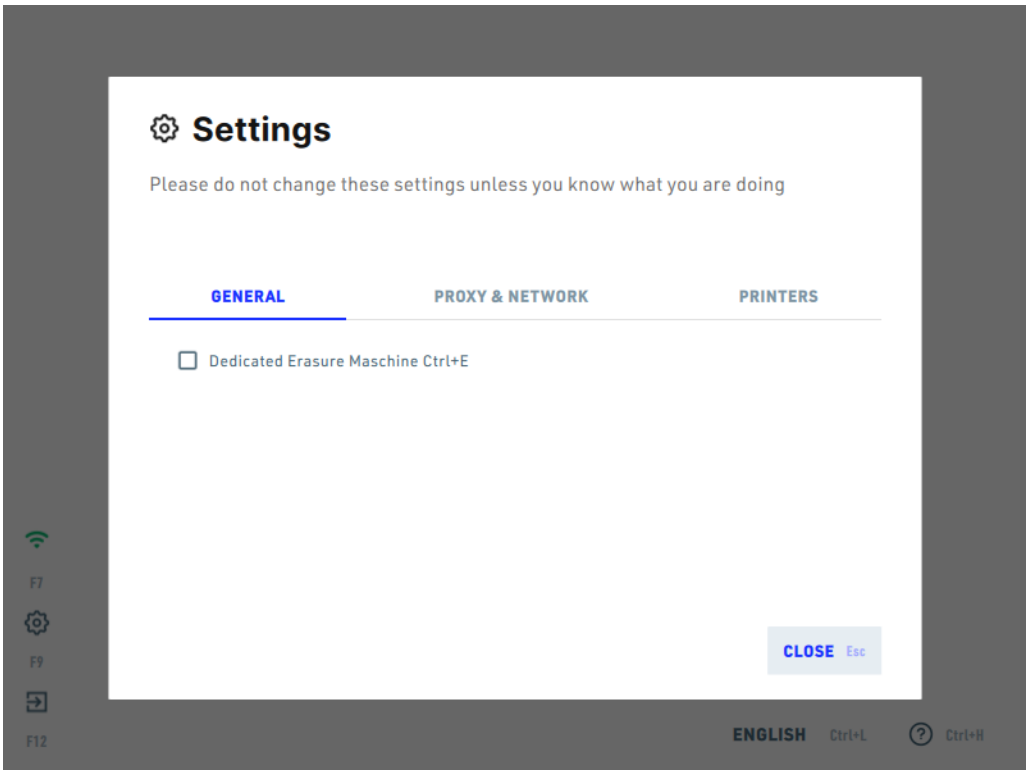
You can select the **language** in the lower right corner. Click on the language or press Ctrl+L and select the desired language.



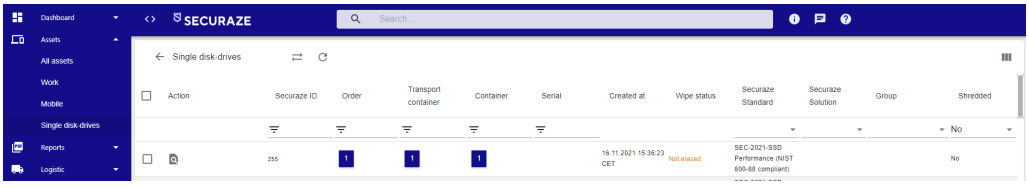
The current version of the Securaze Engine is shown in the **Help menu** in the right corner. Click on the **?** or press Ctrl+H to open the Menu.



To open the Settings menu, click on **general settings** or press F9.



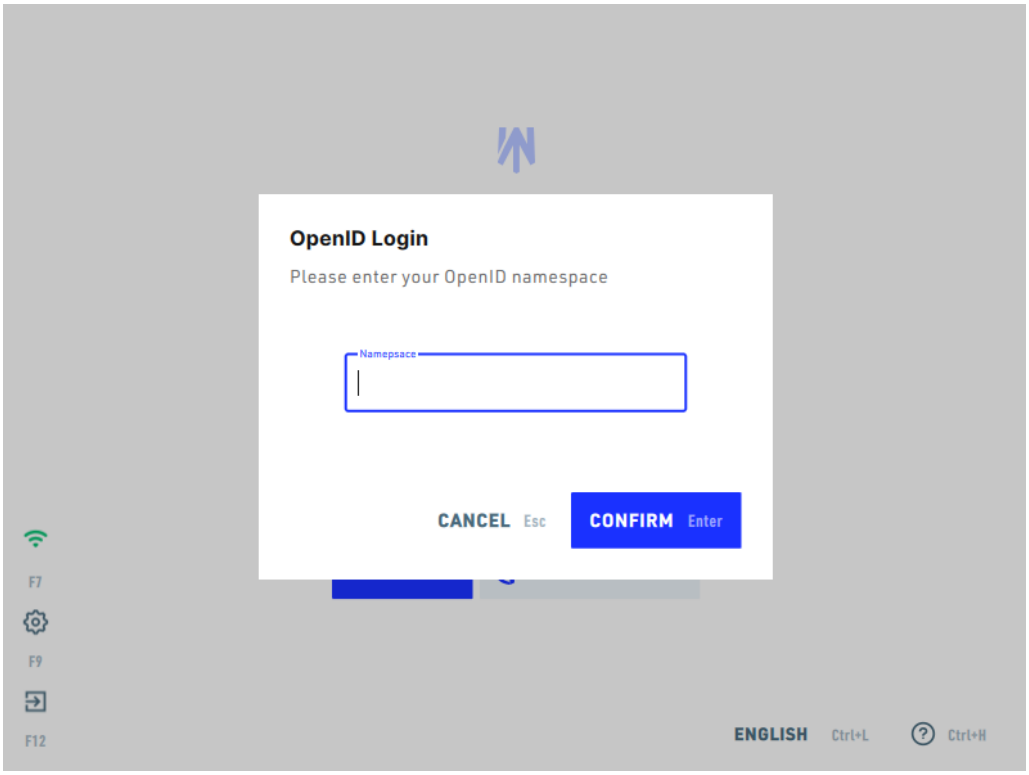
In the tab **GENERAL** you can set the device to behave as **Dedicated Erasure Machine** by checking the checkbox or pressing Ctrl+E.
If this option is enabled, only the information about the erased storages will be gathered, and no information about the system will be captured on erasure reports.
This option is most needed by customers who are performing loose drive erasure and need to keep audit trails about disk drives separately. In this mode, DIAGNOSE IS NOT POSSIBLE.
Securaze will not show anything about "Missing drives - are they shredded?" when the same machine boots up with different drives under these conditions, because the drives are expected to be swapped as the processing continues.
The processed storages (disks) can be found in the Securaze Dashboard, under **Assets - Single Disk Drives:**



The option for dedicated erasure machine is retained when the device is rebooted, so it is possible to use the computer as an erasure machine until the option is deactivated again.

To start processing, enter your Securaze *username@namespace* or full email address, and password and confirm with **LOG IN** to get to the Securaze Work start screen.
Your administrator will provide you with your username and password.

Securaze Work also supports OpenID Connect, an interoperable authentication protocol. Just click on the OpenID login button that will forward you to your system where you enter your OpenID namespace and login to your account.

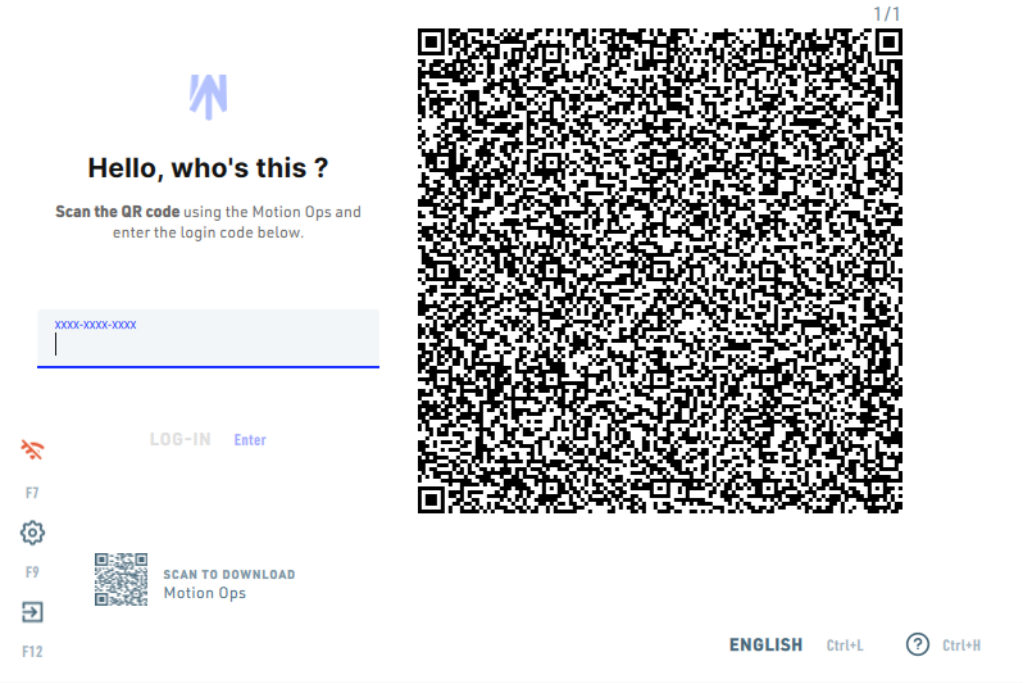


If the login was successful, you will be redirected back to Securaze with the appropriate user information.
If we already have a registered account with these user details, we will simply log you in. If not, we will create an account with these data and then log you in.
The newly created user will receive a role of "EndUser", which can be changed by the user with the role of "Admin".

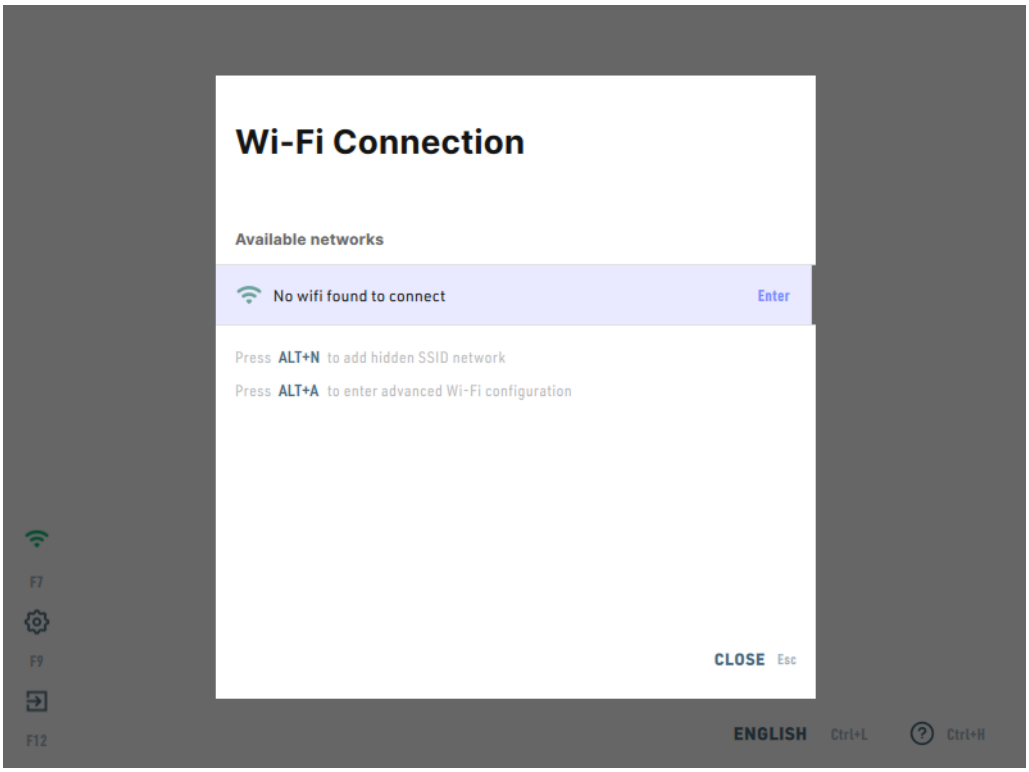
Login withing Network Zone
If the log-in happens within a defined Securaze Network Zone, you can omit the customer namespace, e.g. if your customer namespace is "@example" your full username would be "myusername@example".
Within a Network Zone you can omit the namespace and use just the username to login, e.g. "myusername".

If no Internet-Connection is available the Offline-Mode is started which uses Securaze Motion from AppStore.
Find details regarding working Offline in the chapter Work Offline 142.

No cabled connection available
If no cabled connection is possible with the device (e.g. broken LAN port, no LAN port available, not LAN cable available) an alternative Wifi connection may be used.
The connection state is shown on the lower left corner, either connected or disconnected.

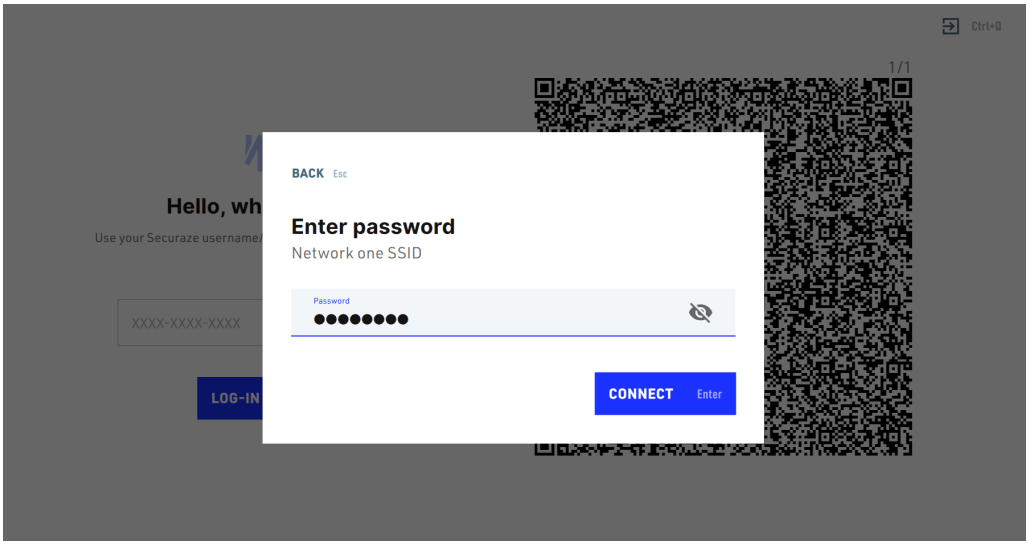


To establish a Wifi connection either click on the Disconnected symbol or press Shortcut F7.

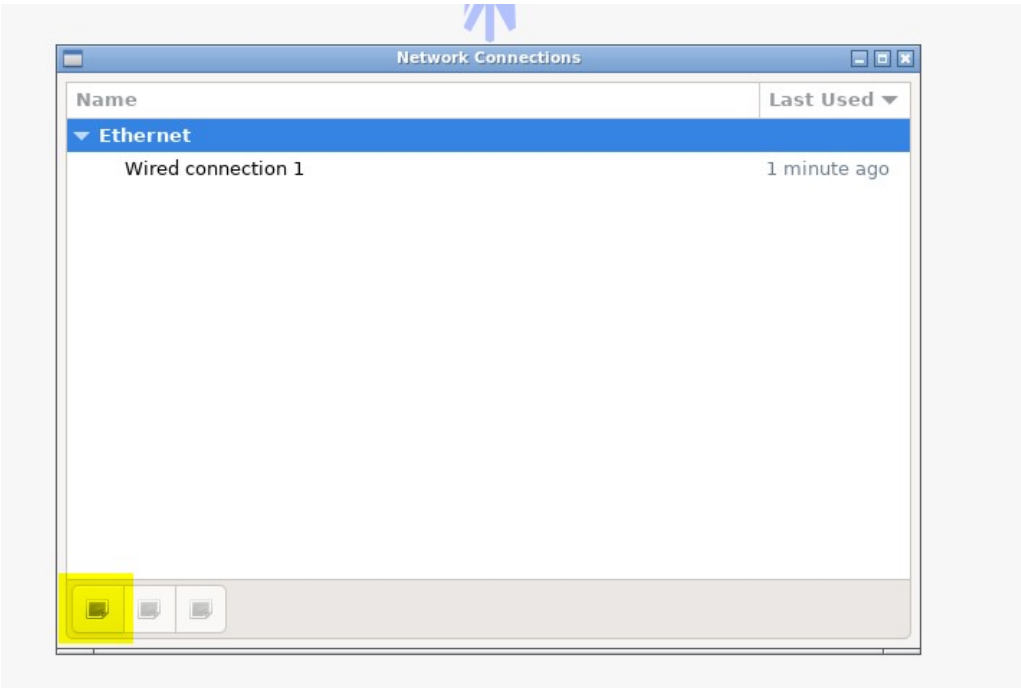


Select one of the available networks and choose with **ENTER** to enter the password for the network.

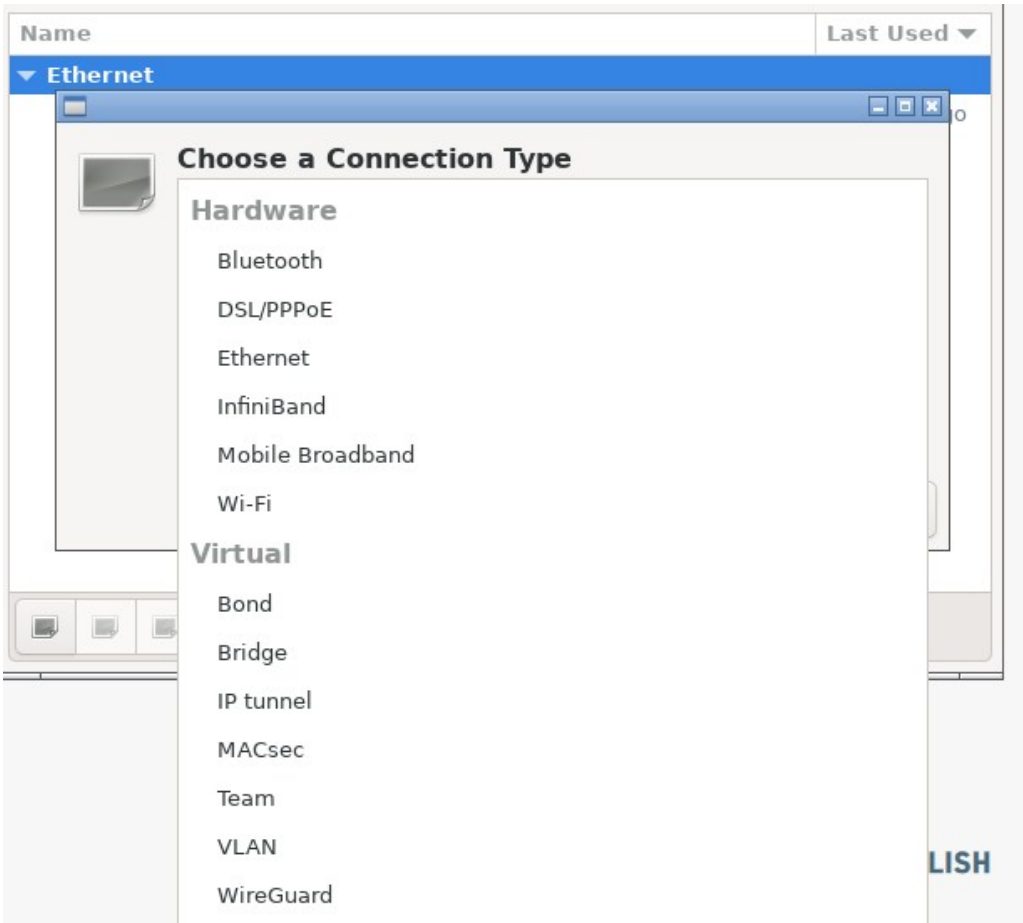
After entering the password for the selected network press **CONNECT** to establish the connection.



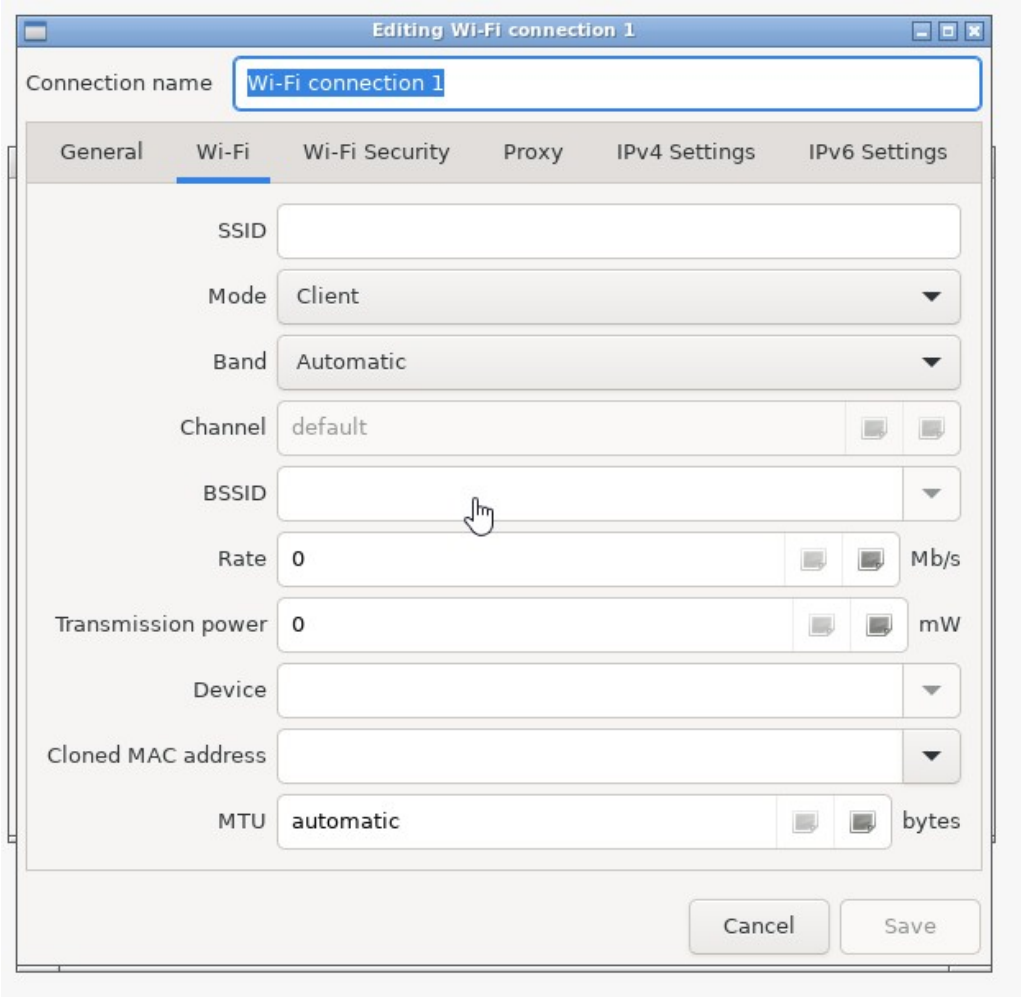
In case you wish to change configuration for an existing Wi Fi, or create a new Wi Fi connection, press ALT + A (advanced Wi Fi settings).
In the upper right corner, a red ⛔ icon will appear. Right click on it and then select "Edit connections".
To add a new connection, select "Add a new connection":



Next, select "Wi Fi" in the drop-down menu:



Fill in the settings in the window:



Connection name: Add the name for your Wi Fi connction

SSID: The SSID (Service Set Identifier) is the name of your wireless network, also known as Network ID. This is viewable to anyone with a wireless device within reachable distance of your network, and is configurable.

Mode:

- Client: Devices such as computers, tablets, and phones are common Clients on a network. When you are accessing a wireless hotspot, or the router in your home or office, your device is the client. This client mode is also known as “station mode” as well.
- Hotspot: Most wireless networks are made using Access Points - devices that host and control the wireless connection for laptops, tablets, or smart phones. If you use Wi-Fi in your home or office, it is most likely through an Access Point. When a router is set up as an Hotspot, or AP, it is said to be in “Master” or “Infrastructure” mode.
- Ad Hoc: Devices configured for ad hoc functionality require a wireless network adapter or chip, and they need to be able to act as a wireless router when connected. When setting up a wireless ad hoc network, each wireless adapter must be configured for ad hoc mode instead of infrastructure mode. All wireless devices connecting to an ad hoc device need to use the same service set identifier (SSID) and wireless frequency channel number.

Band: Wi Fi frequency bands are frequency ranges within the wireless spectrum that are designated to carry Wi Fi: A (5 GHz) and B/G (2.4 GHz), automatic

Channel: A Wi Fi channel is the medium through which wireless networks can send and receive data. For routers made in the U.S., the 2.4 GHz band has 11 channels and the 5 GHz band has 45 channels. Selecting the proper Wi-Fi channel can significantly improve your Wi-Fi coverage and performance. In the 2.4 GHz band, 1, 6, and 11 are the only non-overlapping channels.

BSSID: Basic Service Set Identifier is the identifier used to identify access points and their associated clients. It's the Layer 2 MAC physical address of the access point or wireless router that is used to connect to the Wi Fi and is provided by the hardware manufacturer.

Rate: Rate at which data bits are transferred withing Wi Fi network (mb/s).

Protocol	Frequency	Channel Width	MIMO	Maximum data rate (theoretical)
802.11ax	2.4 or 5 GHz	20, 40, 80, 160 MHz	Multi User (MU-MIMO)	2.4 Gbps
802.11ac wave2	5 GHz	20, 40, 80, 160 MHz	Multi User (MU-MIMO)	1.73 Gbps2
802.11ac wave1	5 GHz	20, 40, 80 MHz	Multi User (MU-MIMO)	866.7 Mbps2
802.11n	2.4 or 5 GHz	20, 40 MHz	Multi User (MU-MIMO)	450 Mbps
802.11g	2.4 GHz	20 MHz	N/A	54 Mbps
802.11a	5 GHz	20 MHz	N/A	54 Mbps
802.11b	2.4 GHz	20 MHz	N/A	11 Mbps
Legacy 802.11	2.4 GHz	20 MHz	N/A	2 Mbps

Transmission power: The most accurate way to express Wi Fi signal strength is with milliwatts (mW).

Device: Device selection.

Cloned MAC address: Cloned MAC address selection.

MTU: Maximum Transmission Unit, is the largest size packet that can be delivered in bytes without fragmentation. The largest size allowed over Ethernet and most of internet service providers is 1500 bytes.

Once you are done with configuring the connection settings, click on "Create..." button.

3.3 Select transport container

On the Securaze Work start screen you will see an overview of the transport containers. The transport container is the container on which the assets where delivered to you.

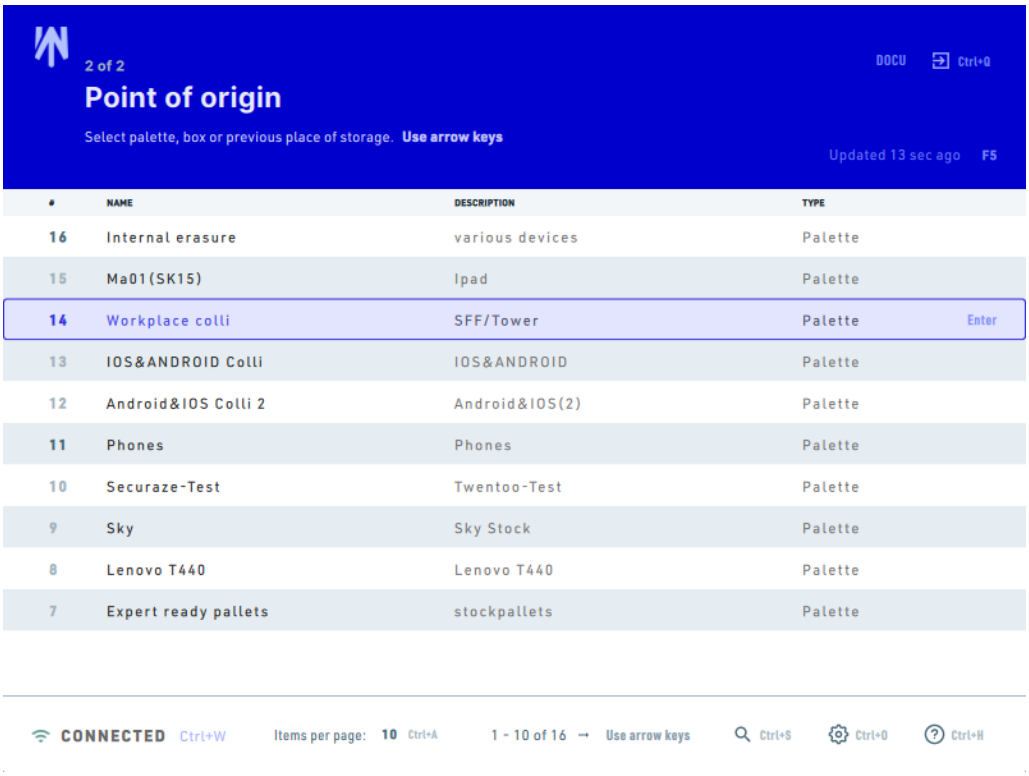
By using the concept of transport container 190 and orders 187 you are able to split the assets into smaller pieces so they are easier to handle and track during daily operation. (e.g. generate erasure reports just for whole transport container or orders)

Select the desired transport container and confirm your selection with Enter.

3.4 Select container

Select the desired container within your company or warehouse and confirm your selection with Enter.

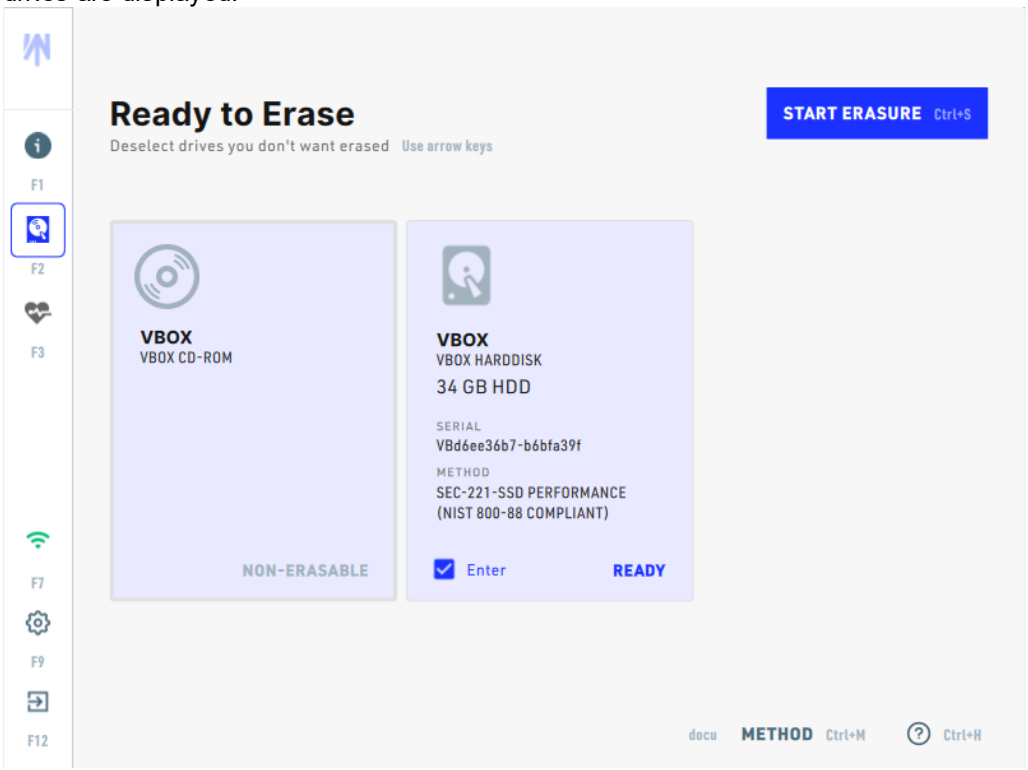
This is the container on which the asset should be put within your company or warehouse.
By using the concept of container 192 you are able to group assets together by logical and/or logistical aspects.



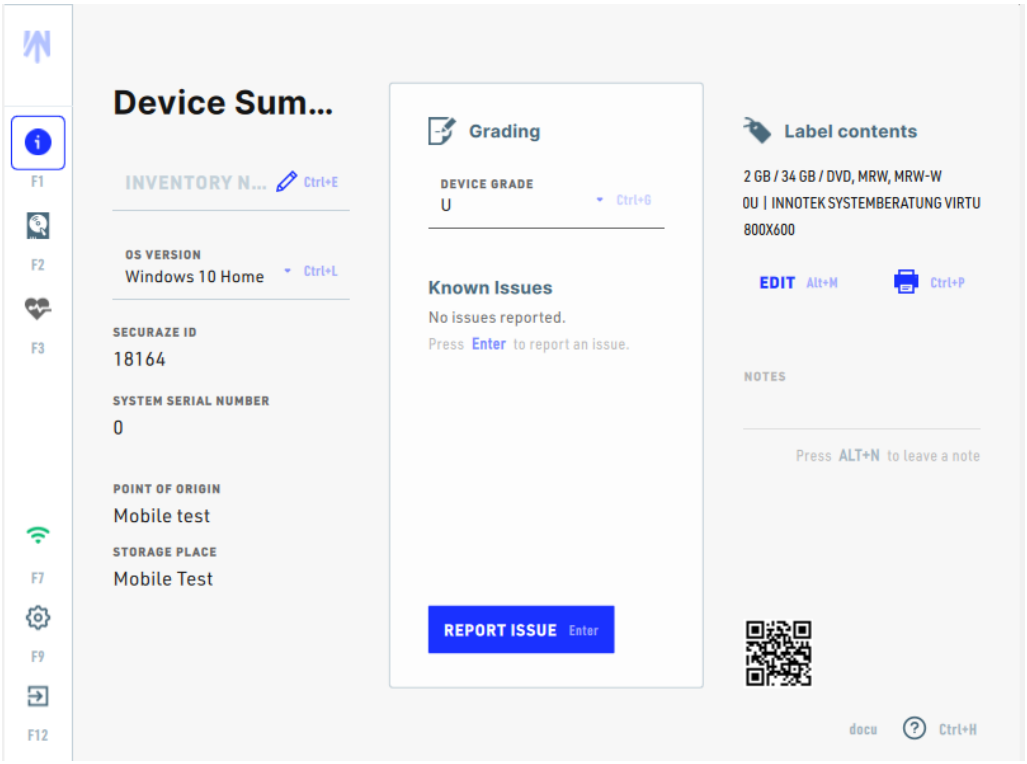
Select the desired container and confirm your selection with Enter.

3.5 Perform Grading

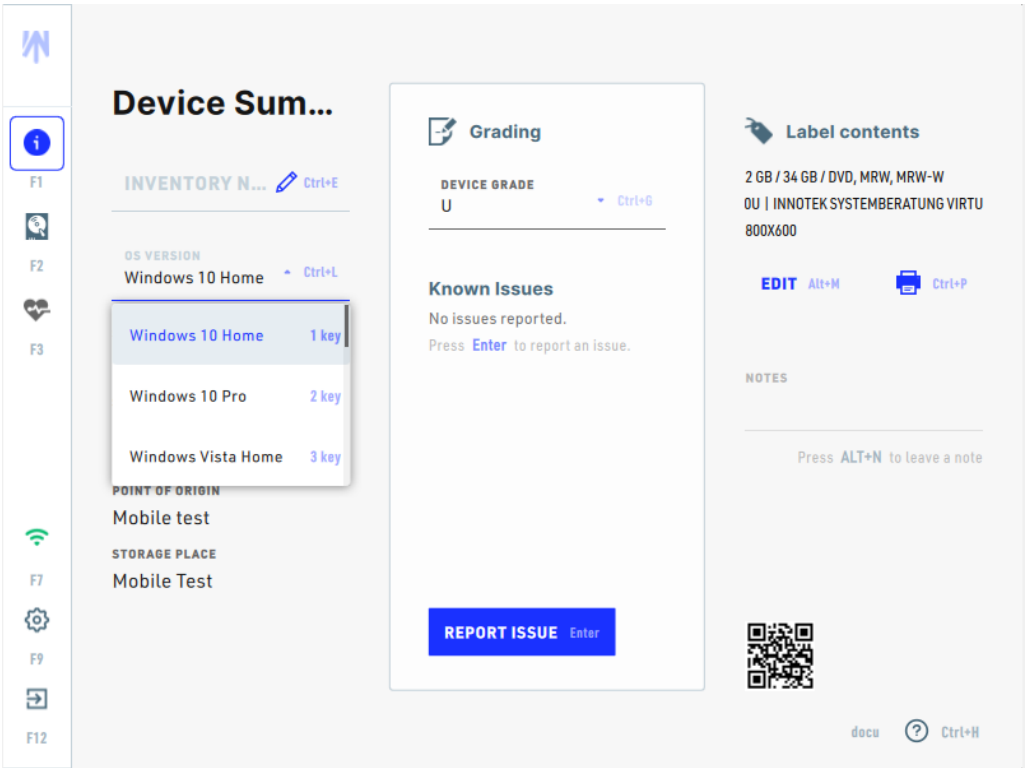
After you have selected the respective containers, you will get to the overview where the drives are displayed.



To enter the Device Summary press F1 or click the **i** icon in the menu on the left side of the screen.



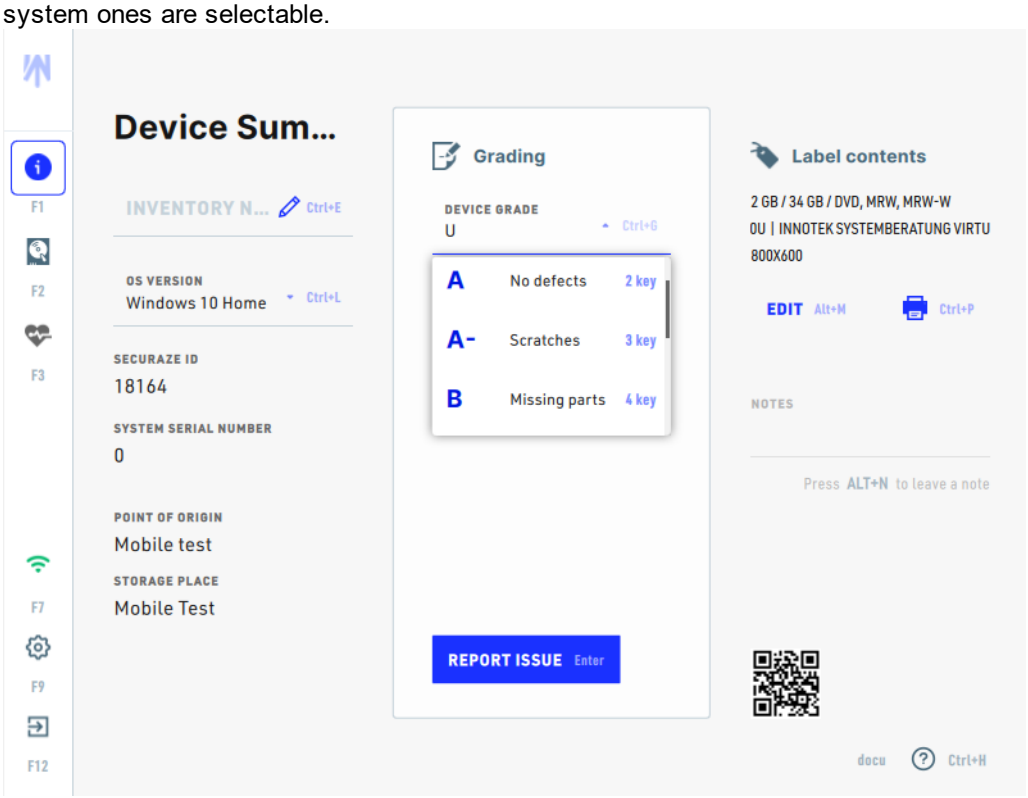
Here you can enter information about the device, such as **INVENTORY NUMBER** and **OS VERSION**.



Simply click on the relevant line and enter the desired information or select the desired option from the menu.

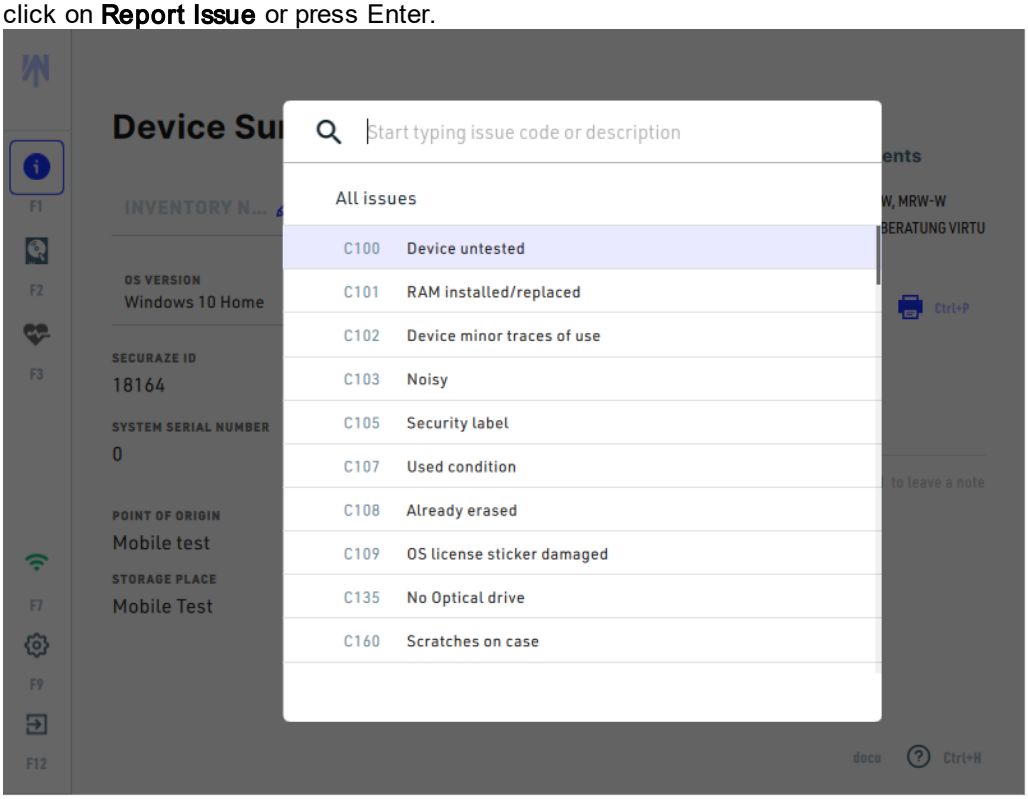
In the **Grading** section you can rate the condition of the device and **REPORT ISSUES**.

The possible grades can be configured in Securaze Dashboard, as default the Securaze system ones are selectable.



Simply select the desired grade from the pull-down menu or press the corresponding hotkey.

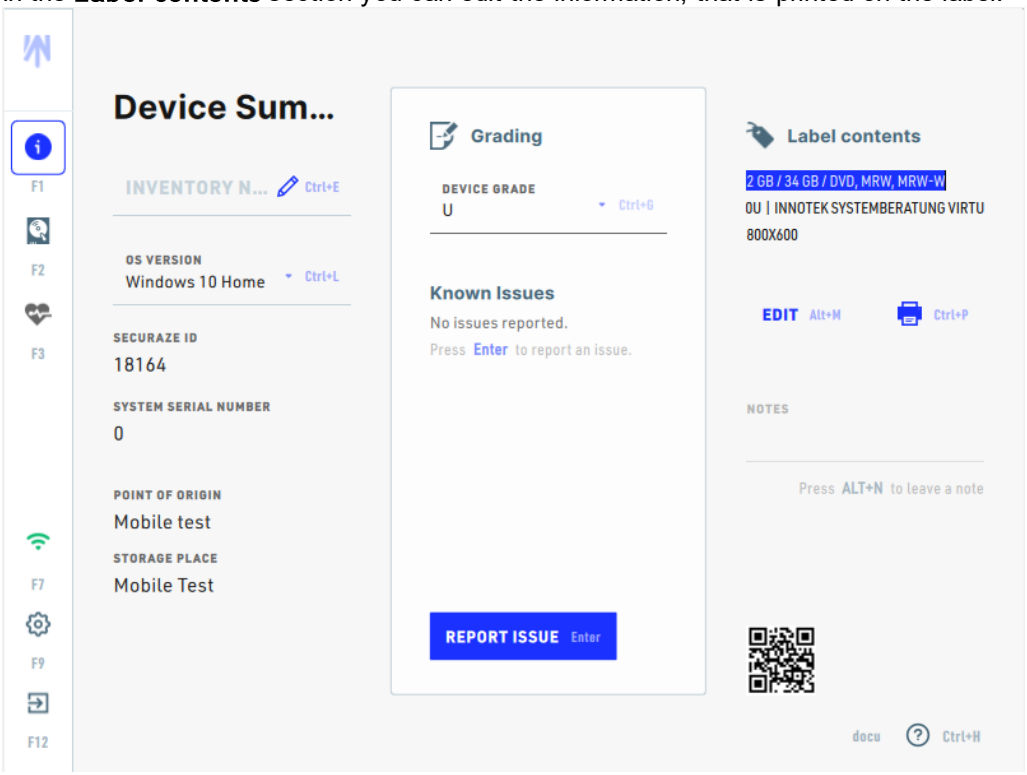
With **REPORT ISSUE** you can add details about the condition of the device. To do this, click on **Report Issue** or press Enter.



Now you select the issue by entering the description or issue code or clicking on the corresponding issue.

You can find information on this under Menu Items - Report Issue 175.

In the **Label contents** section you can edit the information, that is printed on the label.



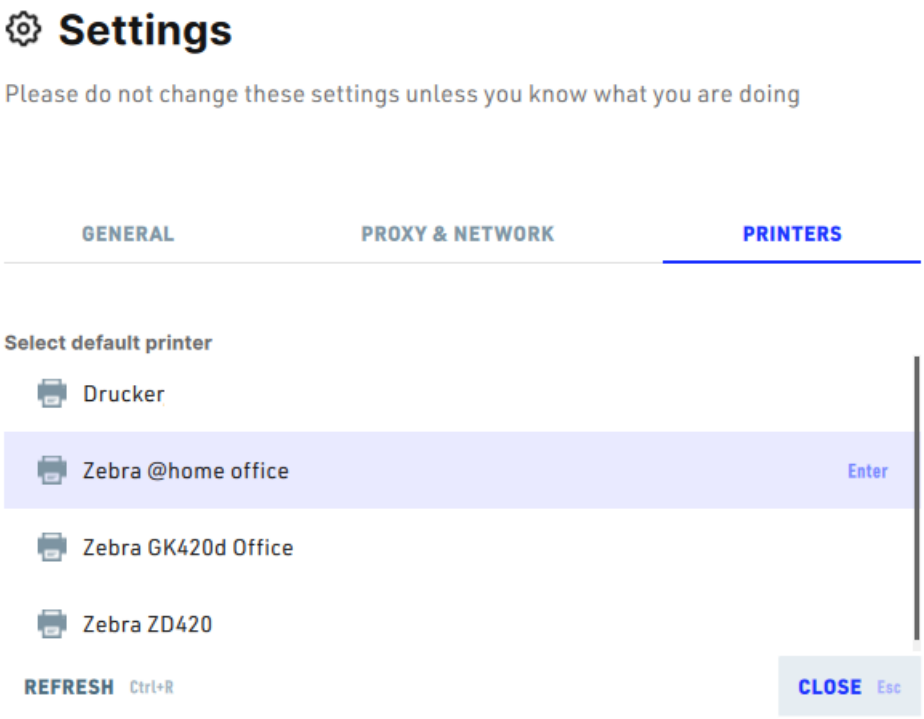
Simply click on **EDIT** or press Alt+N to edit the first row of the label information.

To print the label click on the printer icon or press Ctrl+P.

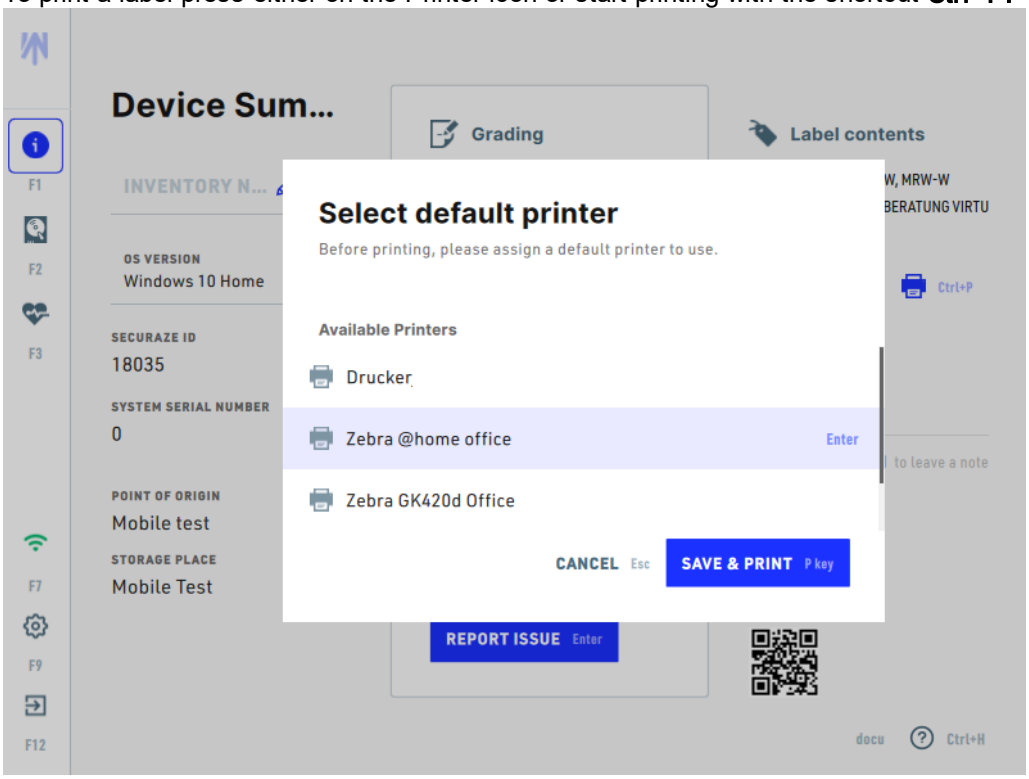
If you want to leave a Note about the device press Alt+N.

3.6 Print label

In the Settings, you can choose a printer to print on.
Select the relevant printer and confirm your selection with **ENTER.**

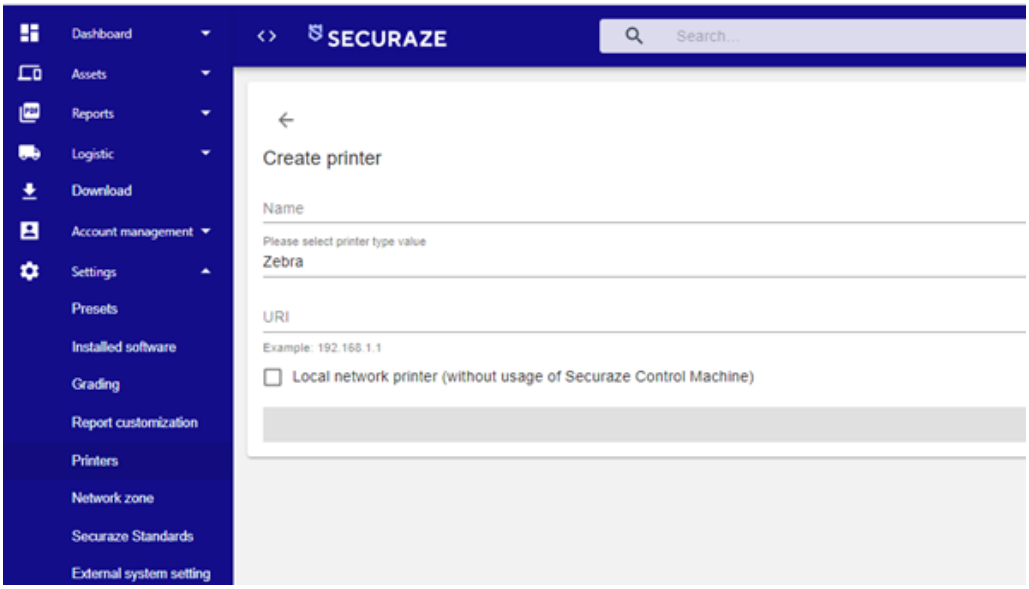


To print a label press either on the Printer icon or start printing with the shortcut **Ctrl+P.**



Printing labels from the cloud:
Securaze Command is required to print labels from the Cloud (Securaze Dashboard).

The printer does not need to be connected to the PXE network, it can be connected to the Command machine directly, or any other device, as long as it’s included in the local network.
The printer has its own IP address, which you enter in Securaze Dashboard under Settings - Printers.



Start the print job in Securaze Work using the created printer. The print request is submitted to the cloud and passed to Securaze Command. The label is printed by Securaze Command on a local printer.

3.7 Apple devices

Securaze Work supports Apple devices of different ages and builds, the following table helps to identify the right method for the specific device.

Age of device	CPU Architecture	Compatible models	Securaze version to use
2020 and newer	Apple Silicon	MacBook Air M1 (2020) MacMini M1 (2020)	Latest Work macOS application.*
2012 until today	Intel CPU **with** T2-chip	MacBook (Early 2015 - 2017) MacBook Air (Mid 2012 - 2020) MacBook Pro (Mid 2012 - 2020) Mac mini (Late 2012 - 2018) iMac (Late 2012 - 2020) iMac Pro (2017) Mac Pro (Late 2013 - 2019) Details per model 112	Latest Work macOS (Catalina) image. Use either External boot macOS from USB Stick or boot from internal recovery partition 110.
2010 to 2020	Intel CPU **with / without** T2-chip	MacBook (Early 2015 or newer) MacBook Air (Mid 2012 or newer) MacBook Pro (Mid 2012 or newer) Mac mini (Late 2012 or newer) iMac (Late 2012 or newer) iMac Pro (2017) Mac Pro (Late 2013; Mid 2010 and Mid 2012 with specifc graphic cards)	Latest Work macOS (Mojave) image. Use either External boot macOS from USB Stick or boot from internal recovery partition 110.
2006 - 2015	Intel CPU **without** T2-chip	MacBook Pro (2010) Mac mini (2009) iMac (2010) Mac Pro (2010) MacBook Air (2012)	Latest Work macOS application. Use External Securaze Image boot 29 from USB stick.
1994 - 2006	PowerPC	iMac G3/G4, iBook G3/4, PowerBook G3/G4	Not supported
1982 - 1995	Motorola	Macintosh PowerBook	Not supported

* Securaze Mobile is also able to detect and erase Apple Silicon devices in DFU mode - but no Diagnose available in that case.

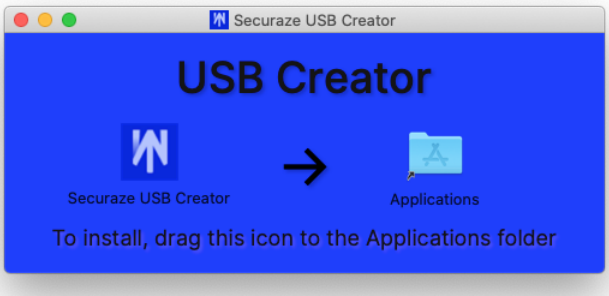
3.7.1 Apple T2 erasure

This is the suggested way how to erase an Apple device with T2 or Intel chip.
This method is compatible with all devices supporting macOS Mojave or macOS Catalina.

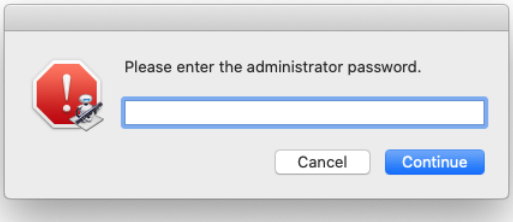
Prerequisites: Machine
Ensure internet connection either via LAN cable or Wi-Fi.
Ensure that the machine is connected to power for the entire duration of the erasure process.
Ensure that the USB or external SSD (preferred) remains connected to macOS throughout the entire erasure process.
Ensure that the sleep mode on your computer is disabled before starting the download and burning process.

Preparations: USB / external SSD
Download **Securaze Creator** from Securaze Dashboard in the menu **Downloads**.

Download the file, double click the image, drag it into the Applications Folder and run it from there.

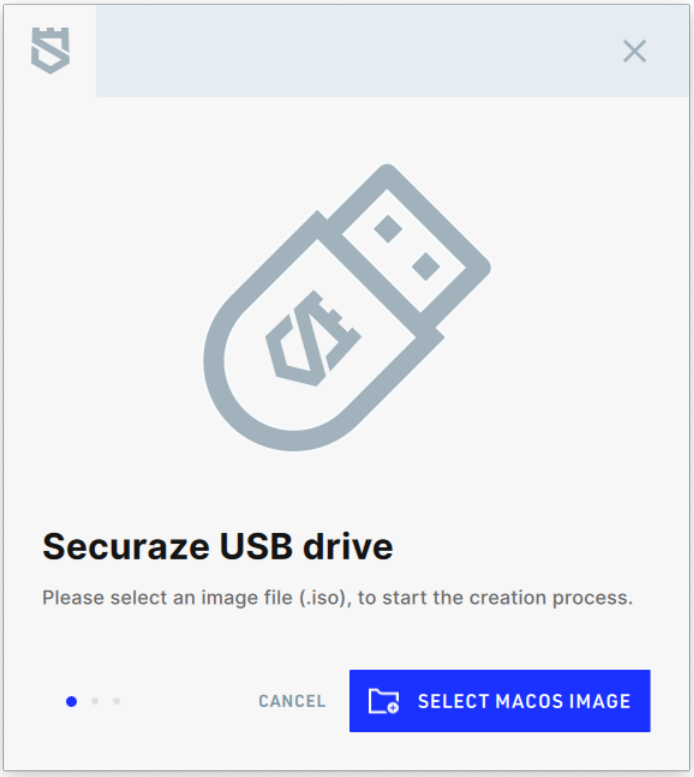


Start the Securaze Creator from the Applications folder. You will be asked for administrator password. This is your Mac password, that you use to access your Mac user account. Make sure this Mac user has Administrator rights on the Mac.

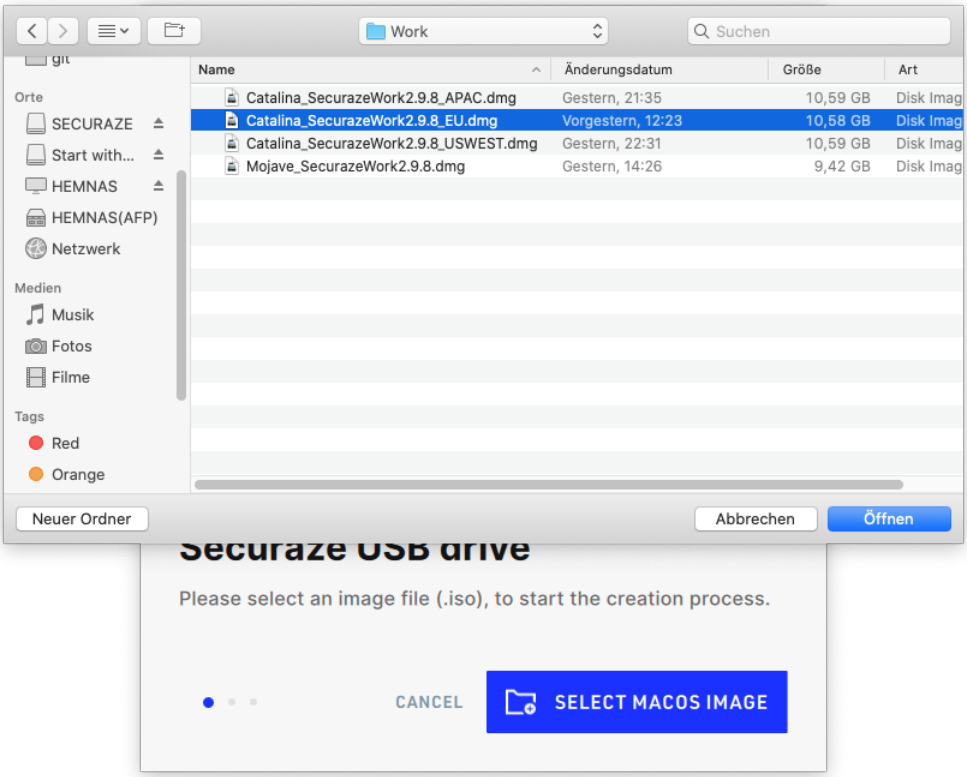


In Securaze Dashboard in the menu **Download** you can download the Securaze Work macOS image.

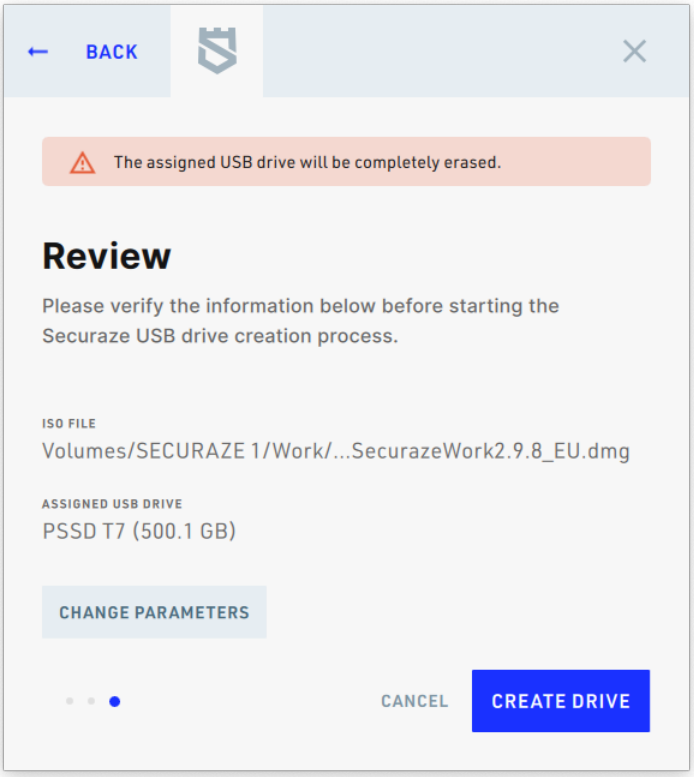
Find and select the downloaded Securaze image by clicking on **SELECT MACOS IMAGE**.



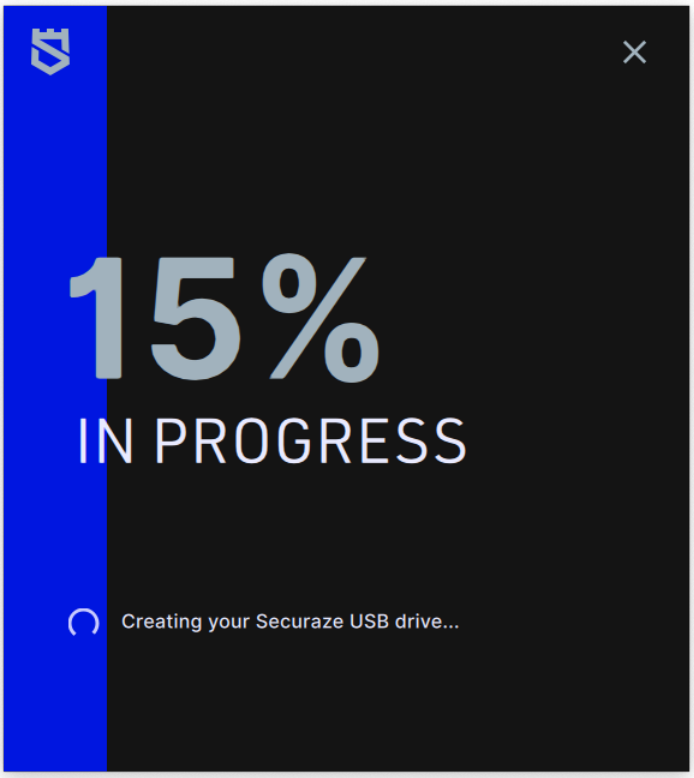
Choose the downloaded image (.dmg file).



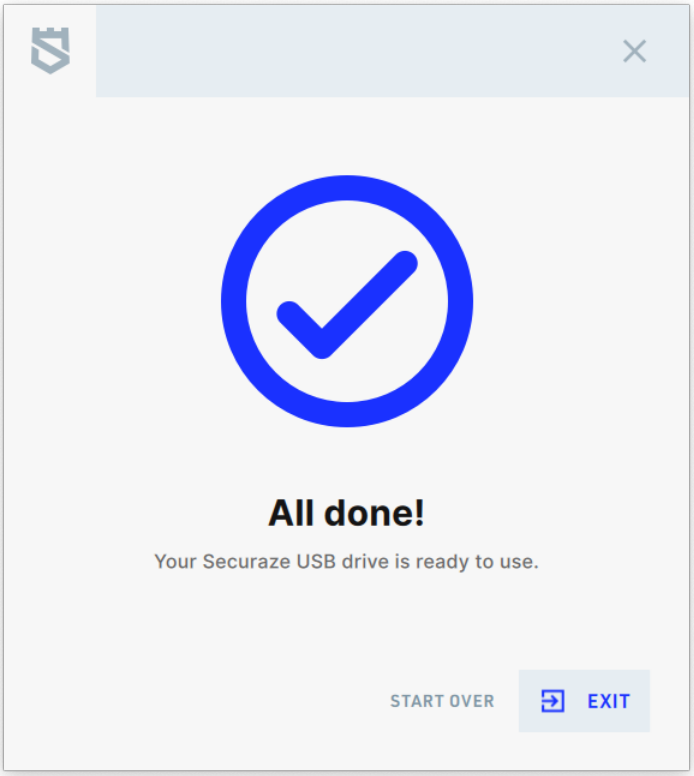
Plug in either an external SSD or a USB-C drive to your system and click on **CREATE DRIVE**



The Securaze image is now being burned onto the stick. You can monitor the progress in the opened window.



After the image has been burned to the external SSD / USB drive, you can use it to boot Securaze.



If this workflow fails, please use Disk Utility 252.

First boot of the new generated external SSD / USB stick

Only for macOS Mojave image:
On the first boot, a dialog appears asking which region the external SSD / USB stick should be used for.
Select the region where your customer is located (currently APAC, EU, USA).
This selection is permanent and will not be asked again for further boots with this external SSD / USB stick.

It is also possible to pre-configure Wifi connections for example, these are also persistent on the external SSD / USB stick.

General workflow

Download
Download the macOS version with integrated Securaze Work Client from the Dashboard or the given download link.
Follow the instructions above to generate a bootable external SSD / USB stick which contains as well macOS as the Securaze Work application.

Erasure process
Connect the external SSD / USB stick to the Apple device.
Boot from the external storage by pressing Option Key immediately after powering on the device.
If booting from external storage is disabled you need to enable it - see chapter Exceptions in Workflow 111.

Process within Securaze Work
Log-in with your Securaze credentials (username@namespace + password).
Depending on your pre-defined customer presets, you need to choose a transport container and warehouse container.
Depending on your pre-defined customer presets, the erasure starts automatically or needs to be started manually.

System compatibility

- macOS Monetrey
- macOS BigSur
- macOS Catalina (latest updates required to start burning)
- macOS Mojave (supports only Mojave images, Catalina images are not possible on Mojave - as Mojave doesn't support Catalina)
- all older macOS versions are not compatible

3.7.2 Apple Silicon erasure

Prerequisites:

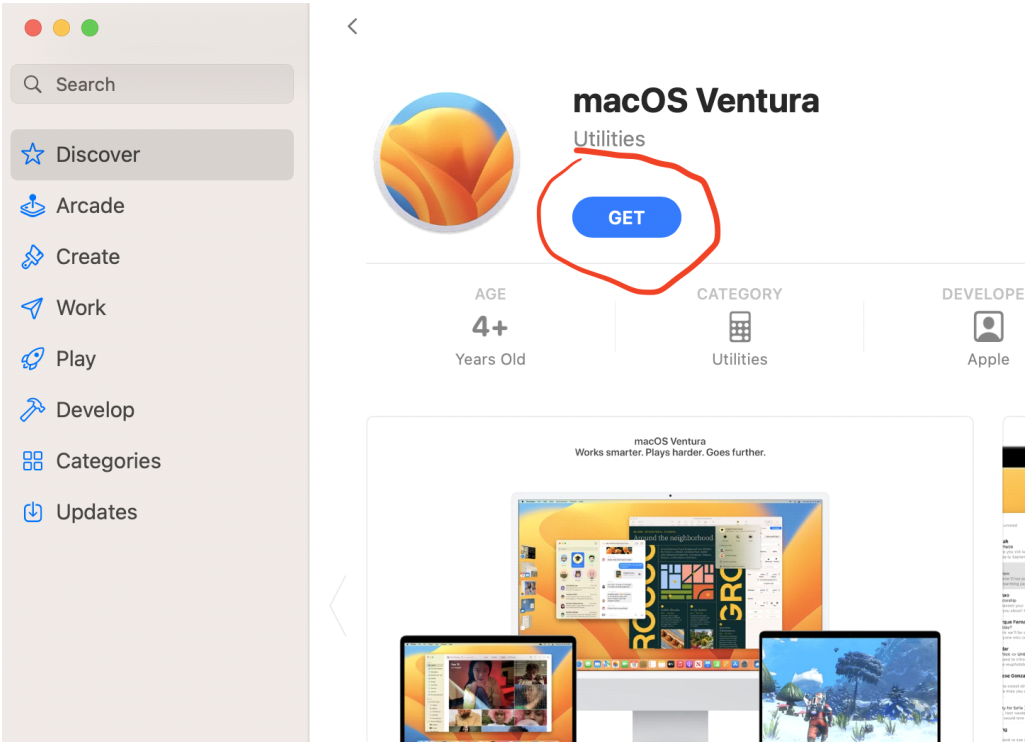
1. An Apple Silicon device running on macOS Ventura 13.1 (at time of writing this the latest one) or newer
2. An external SSD to install macOS on (we can recommend Samsung T7 series SSDs as great performers)
3. An adapter from USB-C to USB-A

Example:

Step 1:

Download the macOS Ventura Installer on the machine - open the following URL:

https://apps.apple.com/de/app/macos-ventura/id1638787999?mt=12



Click on “GET” button (and grab a coffee while the 12 GB image is being downloaded).

Step 2:

Plug in the external USB SSD.

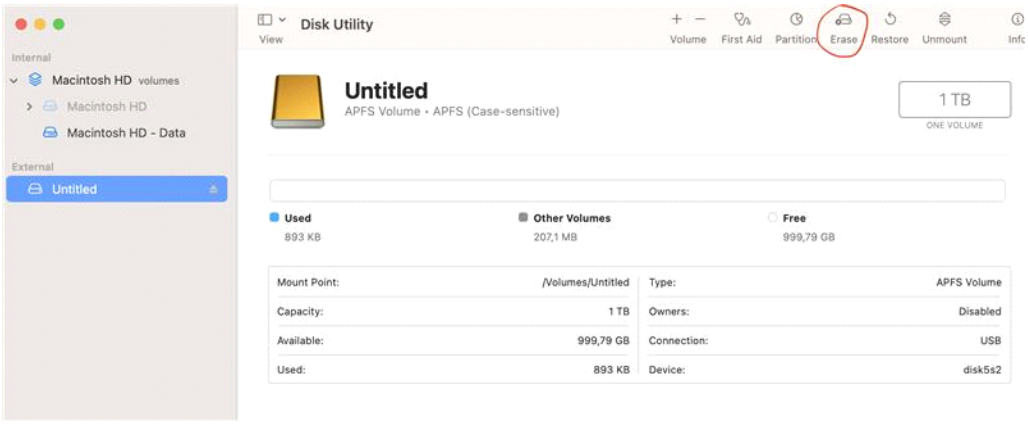
⚠ DO NOT USE A USB-C to USB-C cable, use the adapter to connect the SSD via the USB-C to USB-A adapter!

Step 3:

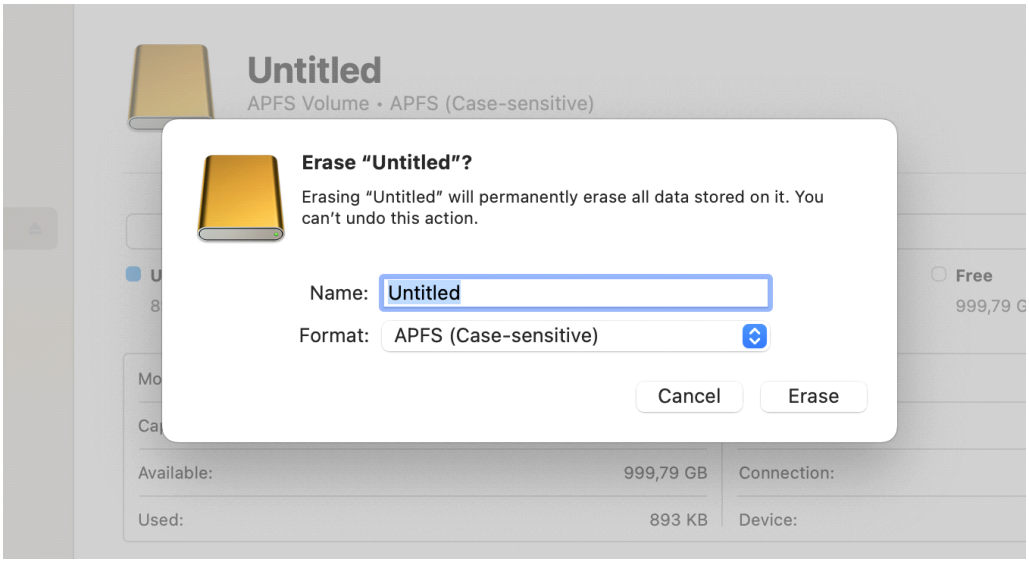
Open "Disk Utility".

It will show the connected external USB SSD on the bottom of the left-pane (In example, named “Untitled”).

Click on the External drive, and then “Erase”.

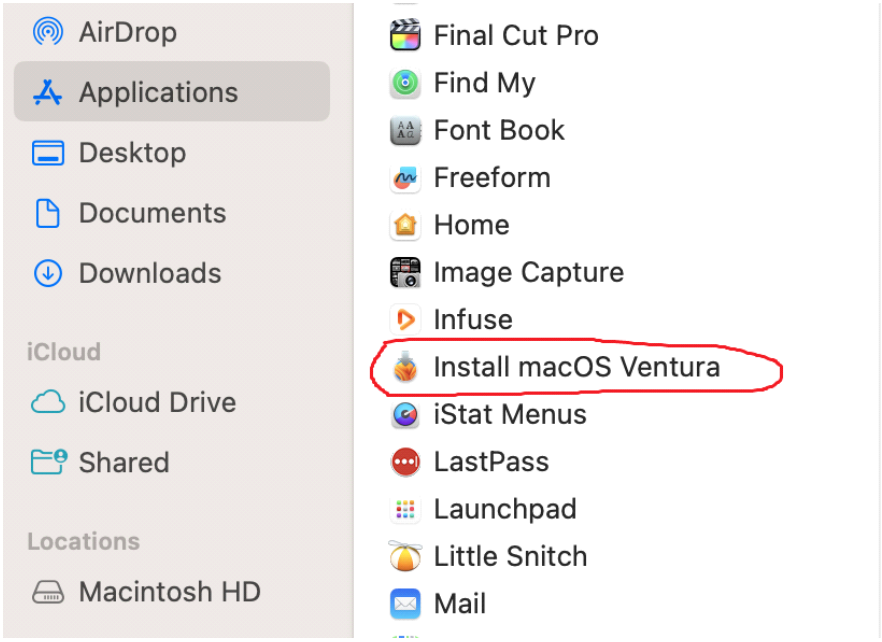


Select Format "APFS (Case-sensitive)" and click on “Erase”.



Step 4:

Once the download of macOS Ventura has been completed, open the “Applications” folder and start the “Install macOS Ventura” application.

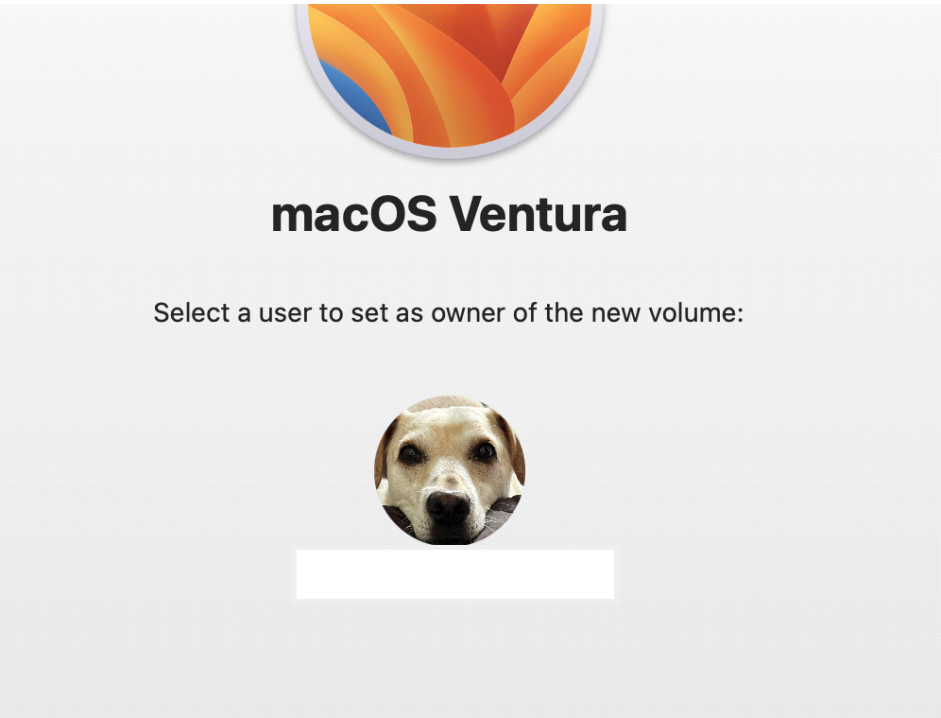


Click on “Continue” button.

Click on "Show All Disks..." button.

A new external SSD will be shown as well. Select the external drive and click “Continue”.

Select your current user as the new owner.

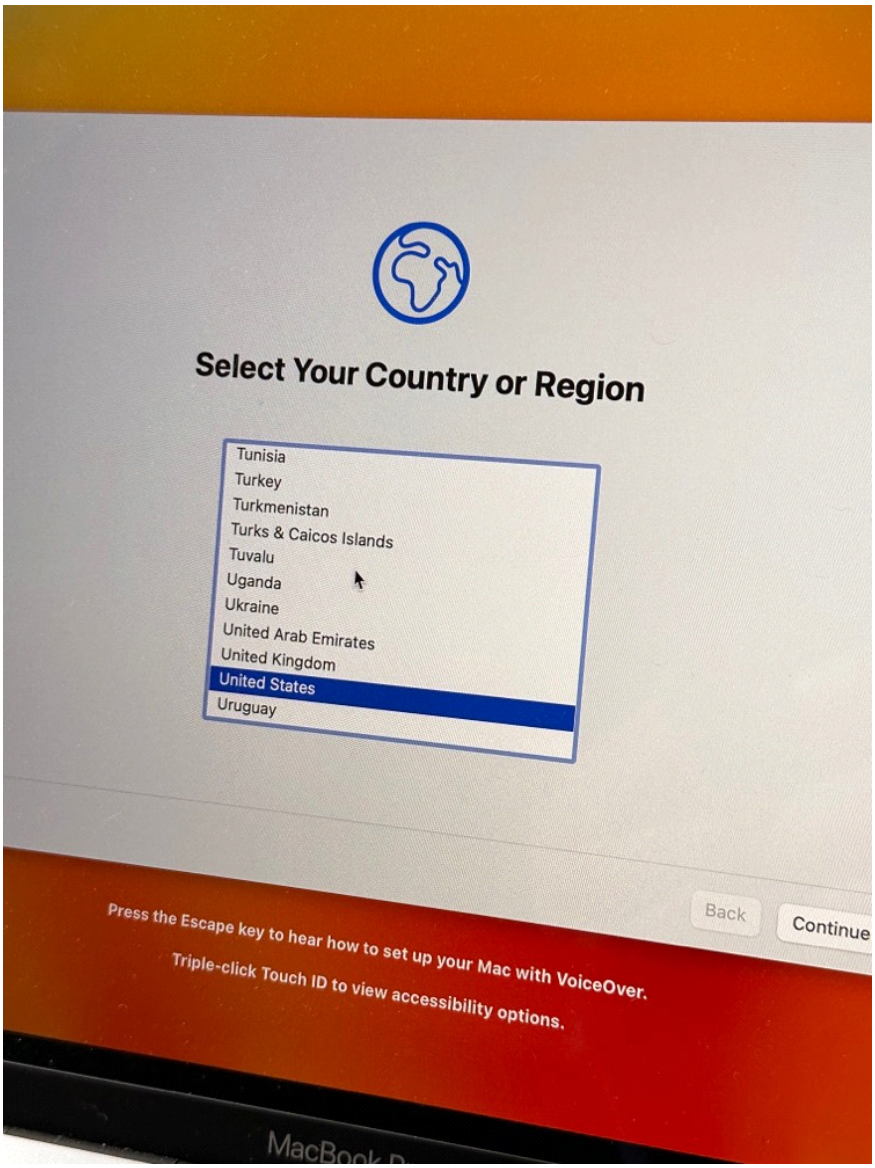


Wait for the installation to be complete.

After the installation is complete, you will be asked to restart your Mac.

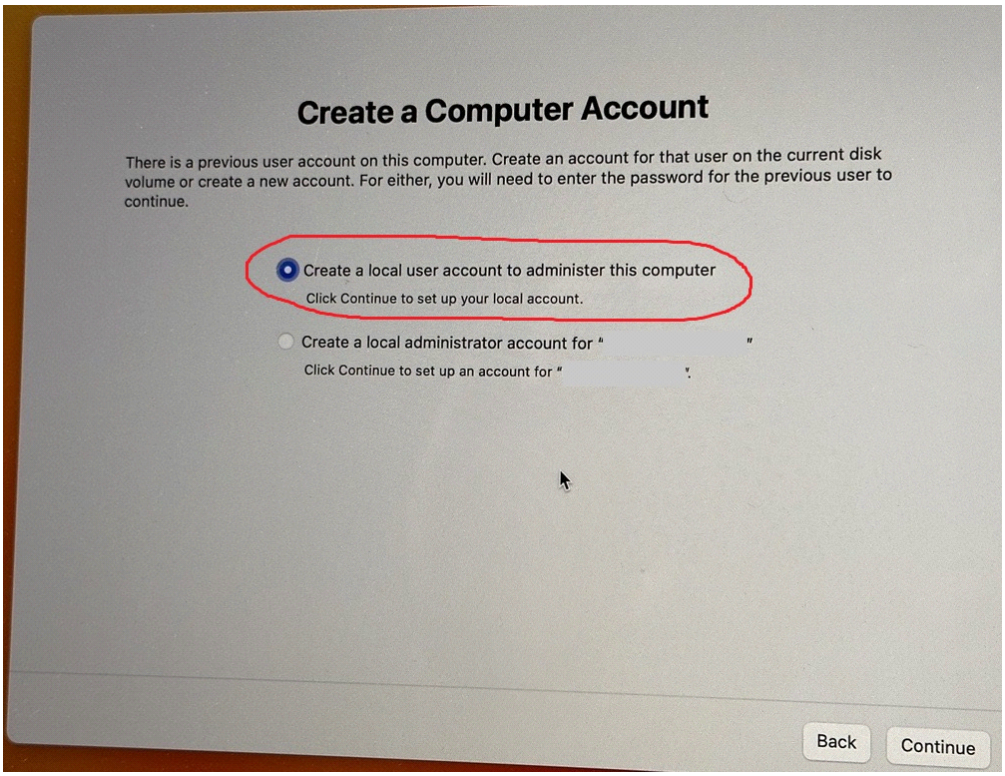
Step 4:

Upon restart, select your country or region.



Continue setup.

Select “Create a local user account to administer this computer”. Click Continue.



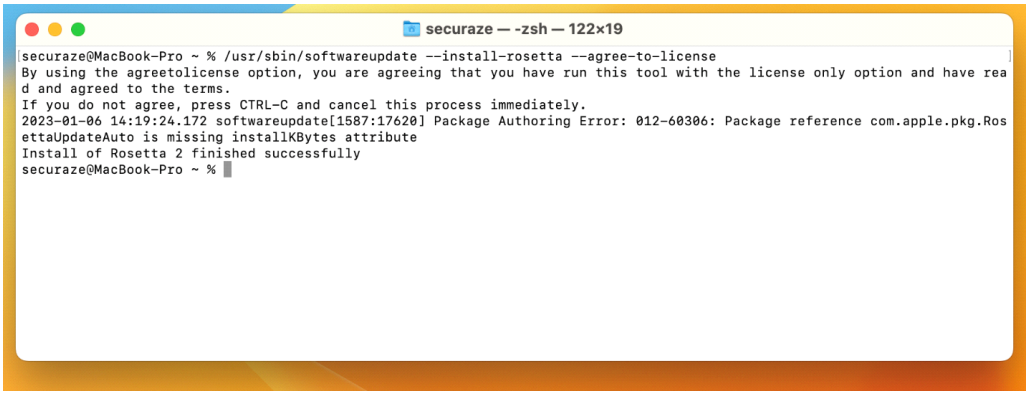
You will be asked to create a computer account, fill in the fields in the following way:

Full name: securaze
Account name: securaze
Password: admin

Continue the setup process till finished.

Step 5:

Open the Terminal, and enter the following command to install Rosetta 2:

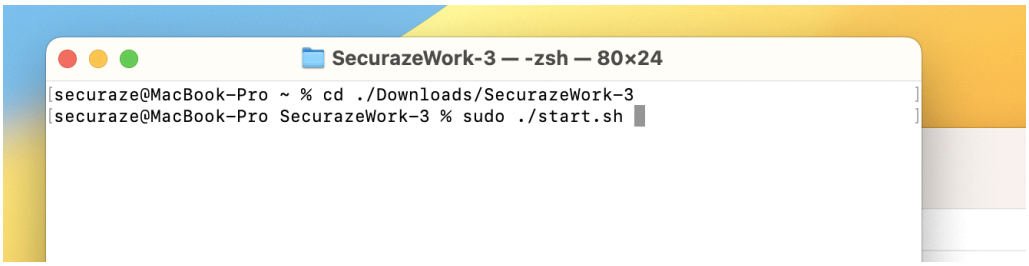


Step 6:

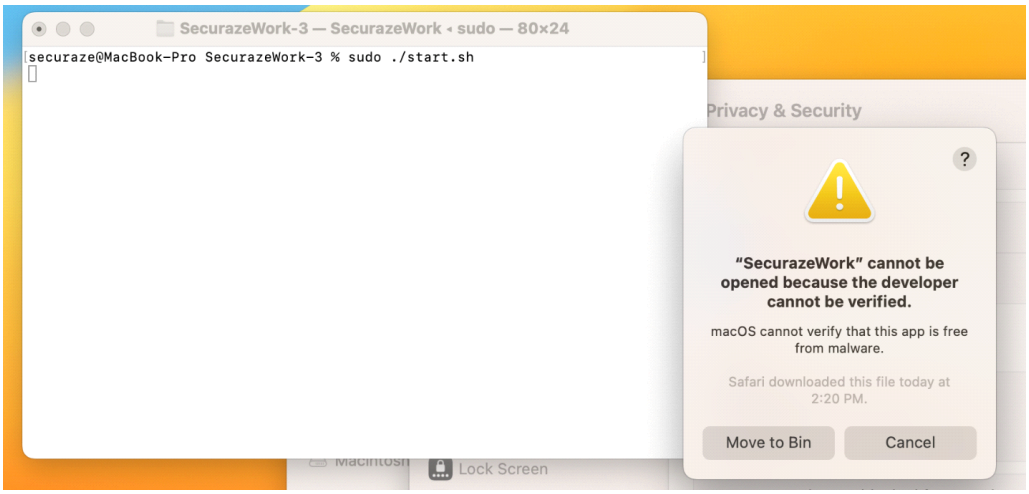
Once finished, download latest Securaze application for macOS from the Dashboard.

To start the application, open the Terminal. Change to the directory where you unpacked the zip and start the app with „sudo ./full.sh“

Enter the admin password you used during setup.



You will be greeted with a one-time error message.



Go to System settings, then to Privacy & security, and accept there to open Securaze work. (This needs to be done only once per disk created!)

After the process is complete, your external SSD is ready to be used to boot Securaze Work on M1/M2 machines and you can perform diagnose and erasure according to the instructions:

Erasure process
Connect the external SSD to the Apple device.
Boot from the external storage by pressing Option Key immediately after powering on the device.

If booting from external storage is disabled you need to enable it - see chapter Exceptions in Workflow 111.

Process within Securaze Work
Log-in with your Securaze credentials (username@namespace + password).
Depending on your pre-defined customer presets, you need to choose a transport container and warehouse container.
Depending on your pre-defined customer presets, the erasure starts automatically or needs to be started manually.

3.7.3 Using Apple recovery mode

This is the suggested way how to erase an Apple device without T2 chip or if macOS Mojave cannot be booted anymore.

Prerequisites: Machine
Ensure internet connection either via LAN cable or Wi-Fi.
Ensure that the machine is connected to power for the entire duration of the erasure process.
Ensure that the Pendrive with SecurazeWork stays connected during the entire erasure process.

Preparations: Pendrive
Format a pendrive with Mac OS Extened (Journaled) filesystem and name the pendrive "Securaze" (so that it is not listed as storage in Securaze Work).
Copy SecurazeWork.app and the shell scripts "start.sh" and "cmd.sh" to the pendrive.
Set the file permissions with "chmod +x *.sh" in case the execution permissions are lost during the download.
Connect the drive to the Apple device which should be erased.

General workflow

Download
Download SecurazeWork Client and unzip the .zip file to a location on a Mac.
If you want to use the Command Line version, update "cmd.sh" with the Securaze credentials you intend to use.

Erasure process
Boot into Recovery Mode by pressing Command-R before/during startup (up to 3 Minutes) and start the Terminal in Recovery Mode "Utilities -> Terminal.
If a password is needed to continue, you need to disable it - see chapter Exceptions in Workflow 111.
Change directory towards Securaze Work content on pendrive by entering:

GUI-Mode:
cd /Volumes/Securaze [ENTER]
Start Securaze Work by entering: ./start.sh [ENTER]

Command-Line-Mode:
cd /Volumes/Securaze [ENTER]
Start Securaze Work by entering: ./cmd.sh [ENTER]

Process within Securaze Work
Log-in with your Securaze credentials (username + password).
Depending on your pre-defined customer presets you need to choose an transport container and warehouse container.
Depending on your pre-defined customer presets the erasure starts automatically or needs to be started manually.

3.7.4 Exceptions in workflow

Firmware password set or Filevault Encryption active
If a firmware password or Filevault Encryption is activated, it must be removed to keep the value of the device.
To remove it either the Administrator password needs to be entered or the storage needs to be erased and OSx reinstalled from scratch.

Administrator Password known
Start "Startup Security Utilities" from "Utilities -> Startup Security Utilities"
-> Turn off firmware password
-> Set Secure Boot to "No security"
The FileFault encryption will be removed during erasure in Securaze Work.

Reinstall
Boot into Recovery Mode by pressing Command-R before/during startup (up to 5 Minutes)
Goto Disk Utility and erase the storage with Apple "Erase" functionality
Boot into Internet Recovery Mode by pressing Command-R before/during startup (up to 30 Minutes)
Boot into Recovery Mode by pressing Command-R before/during startup (up to 5 Minutes)
Start "Startup Security Utilities" from "Utilities -> Startup Security Utilities"
-> Turn off firmware password
-> Set Secure Boot to "No security"

Duration
The duration of the general workflow (boot into recovery mode + erasure) takes on a typical Macbook Air with 128 GB SSD about ~15 minutes including secure erasure with Securaze Work.
After the erasure an Internet Recovery needs to be done to reinstall OSx on the device. This takes up to 30 minutes, depending on the speed of the internet connection.

3.7.5 macOS Catalina compatibility

Securaze Work supports Apple devices of different ages and builds, the following table helps to identify the right method for the specific device.

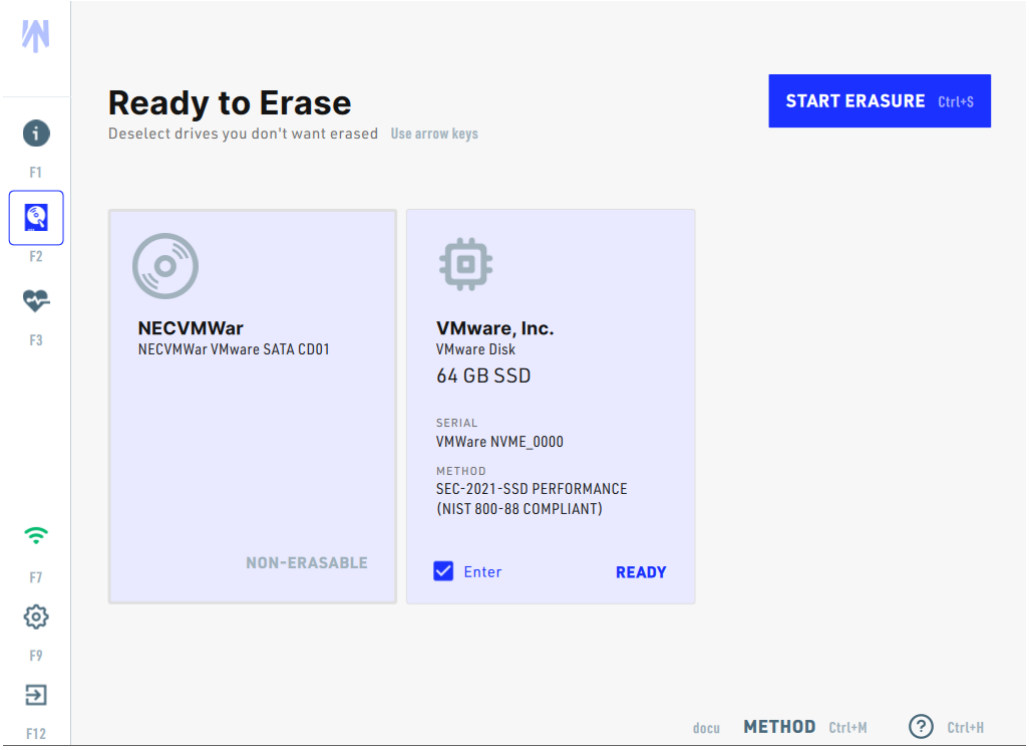
Device	Compatible models
MacBook Pro	MacBook Pro (13-inch, Mid 2021 - 2020) MacBook Pro (16-inch, 2019) MacBook Pro (15-inch, Mid 2012 - 2019) MacBook Pro (Retina, 15-inch, Mid 2012 - Mid 2015) MacBook Pro (Retina, 13-inch, Late 2021 - Early 2015) MacBook Pro (15-inch, Mid 2012) MacBook Pro (13-inch, Mid 2012)
MacBook Air	MacBook Air (Retina, 13-inch, 2018-2020) MacBook Air (13-inch, 2017) MacBook Air (13-inch, Early 2015) MacBook Air (11-inch, Early 2015) MacBook Air (13-inch, Early 2014) MacBook Air (11-inch, Early 2014) MacBook Air (13-inch, Mid 2013) MacBook Air (11-inch, Mid 2013) MacBook Air (13-inch, Mid 2012) MacBook Air (11-inch, Mid 2012)
MacBook	MacBook (Retina, 12-inch, 2017) MacBook (Retina, 12-inch, Early 2016) MacBook (Retina, 12-inch, Early 2015)
iMac Pro	iMac Pro (2017)
iMac	iMac (Retina 5K, 27-inch, Late 2014-2020) iMac (Retina 4K, 21.5-inch, Late 2015 - 2019) iMac (21.5-inch, Late 2012 - 2017) iMac (27-inch, Late 2012 - Late 2013)
Mac mini	Mac mini (2018) Mac mini (Late 2014) Mac mini (Late 2012)
Mac Pro	Mac Pro (2019) Mac Pro (Late 2013)

3.8 Perform erasure

You can now perform the erasure.

3.8.1 Drive Erasure

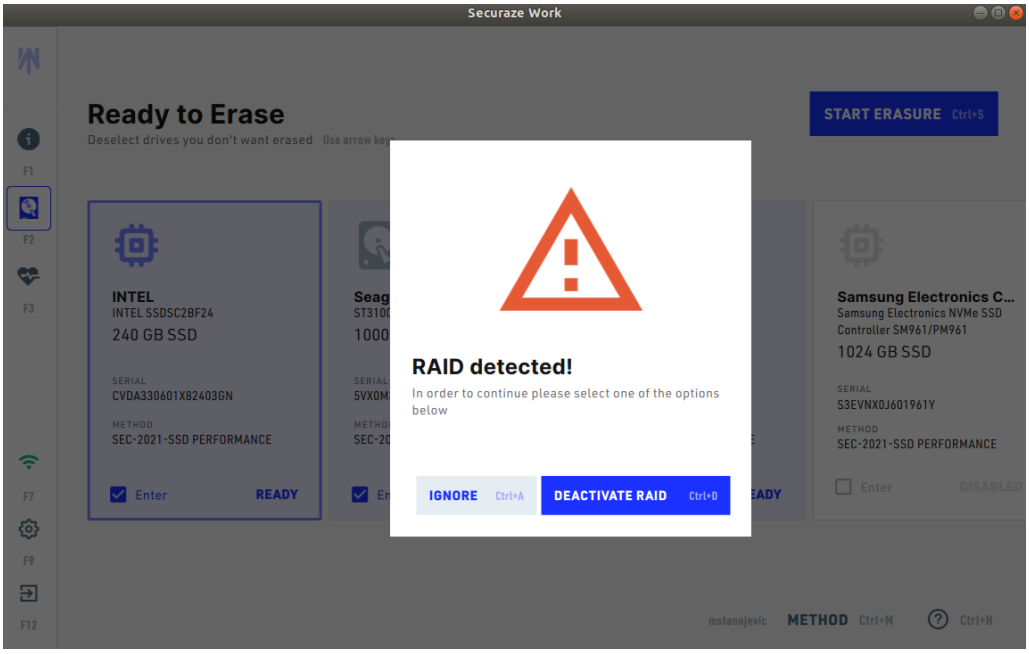
In the Drive Erasure section, you will see an overview of all hard drives available for erasure.

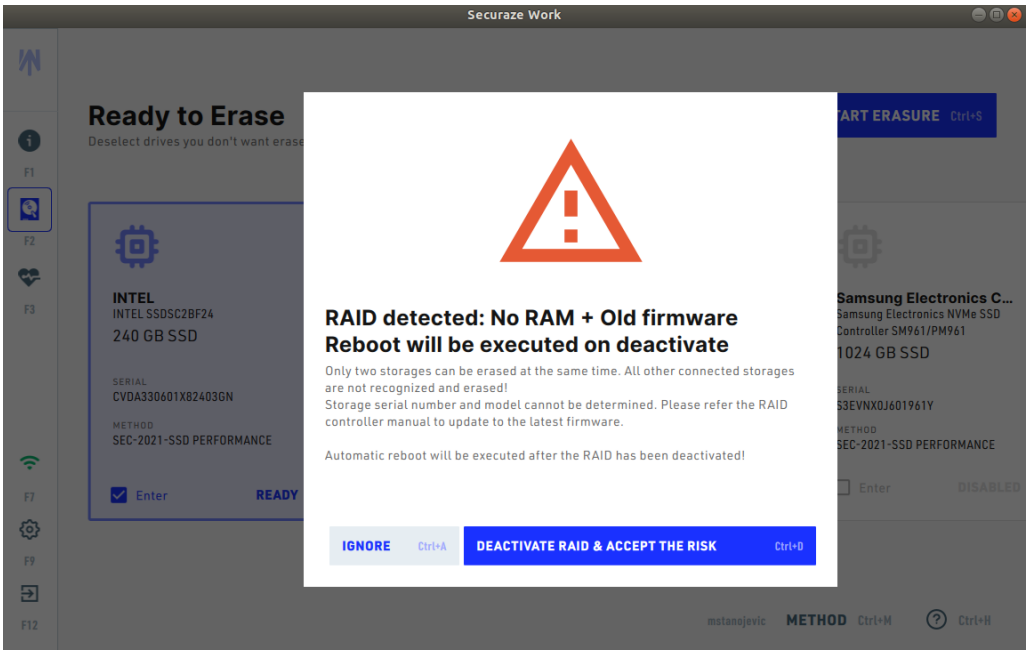


Detecting RAID controller on servers

Since it is necessary for Securaze software to access each and every physical disk to wipe it, the removal of that virtual drive is necessary, before the full wipe is completed and deemed as successful. We have implemented features in Work that will automatically turn off the RAID functionality on the server RAID controller – but warn the operator upfront, because even that first step of turning it off will cause loss of data.

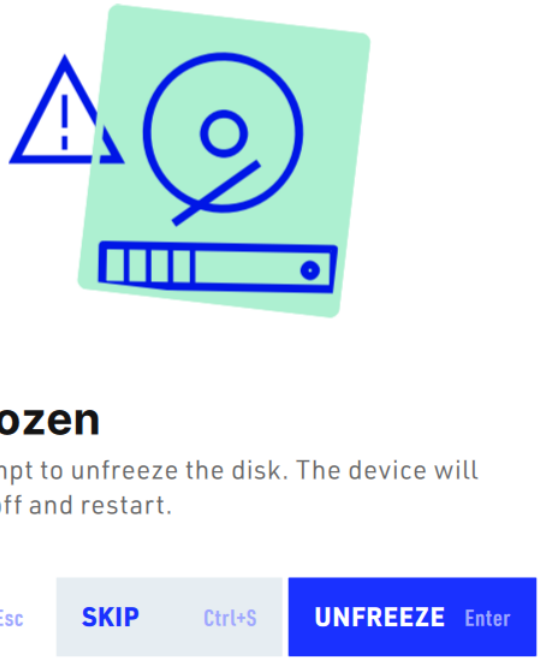
By confirming, the user allows Securaze to destroy RAID setup and provide information about each disk (serial number, capacity etc.) in the erasure report.





Click on the hard disk(s) you want to erase and select **START ERASURE** Ctrl+S.

If the storage needs unfreezing, the unfreeze dialog appears.

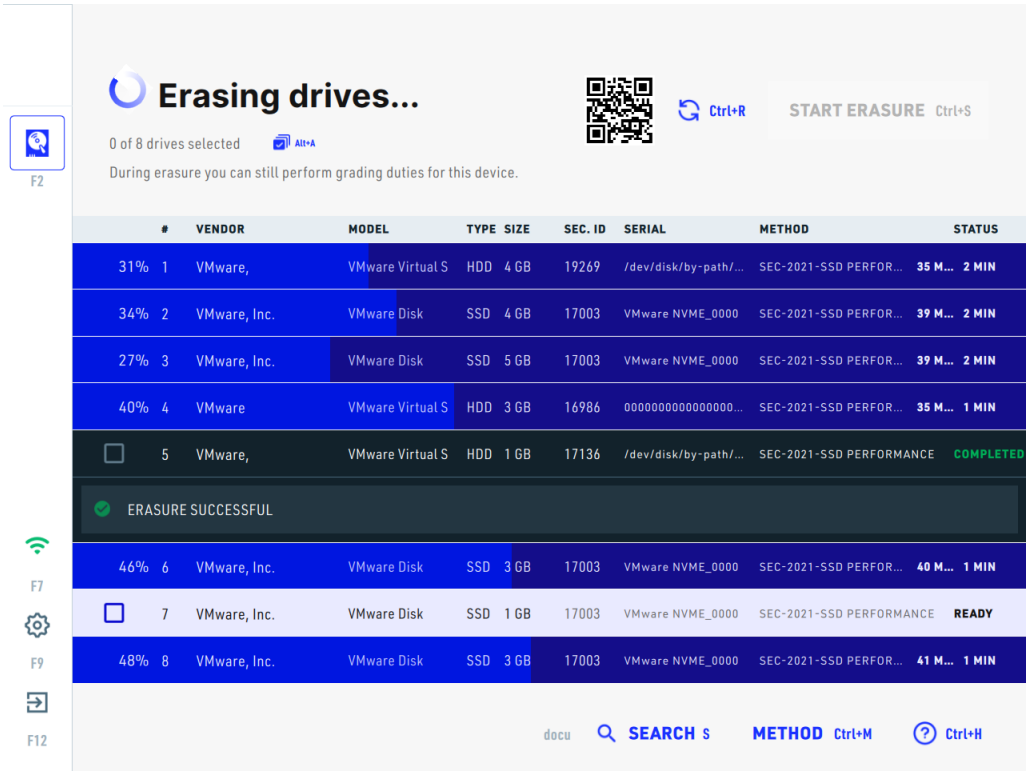


If you want to skip the attempt to unfreeze, select **SKIP**.
Erasure methods which are based purely on firmware based erasure will fail subsequently.
If the unfreeze process fails, the erasure will fail.

We recommend not to skip the process at the first attempt, but to try to unfreeze the disk.

The optimal erasure method is automatically used for the specific type of storage medium.
For information on changing the erasure method, see Menu Items - Erasure 173.

If more then 4 disks are found in the device a table-view is shown which provides a good overview about all storages.
To select/deselect all discs, simply press ALT + A (by default all are selected).
Below each disc you will see additional status info like "Erasure in progress/ finished", etc..



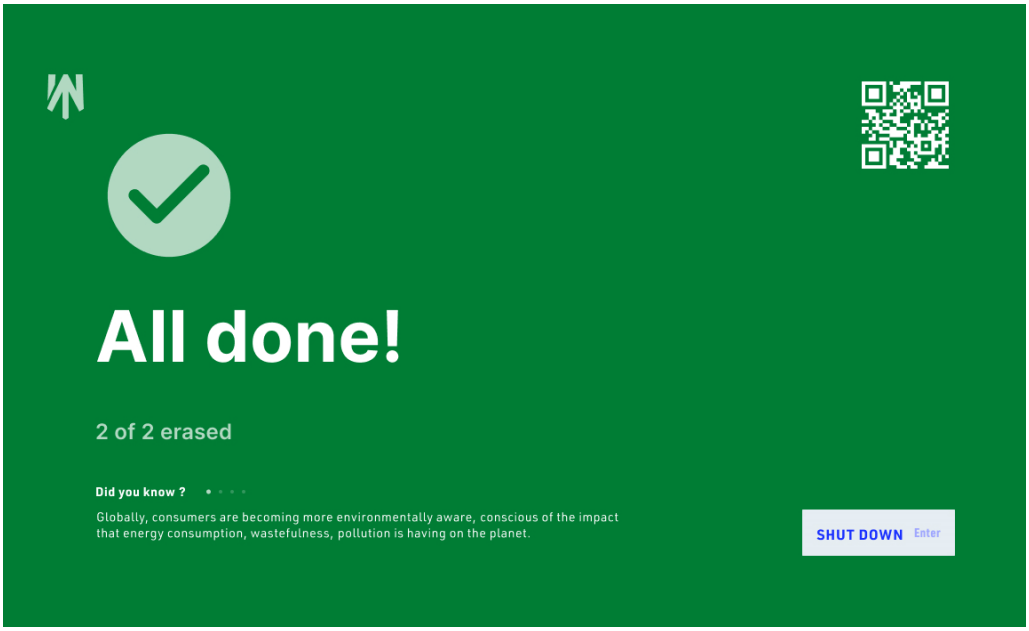
To show the screensaver immediately, press CTRL+W.

You can monitor the progress at any time during the erasure process on the screensaver.

Successful erasure

For progress with no errors, the display will be blue:

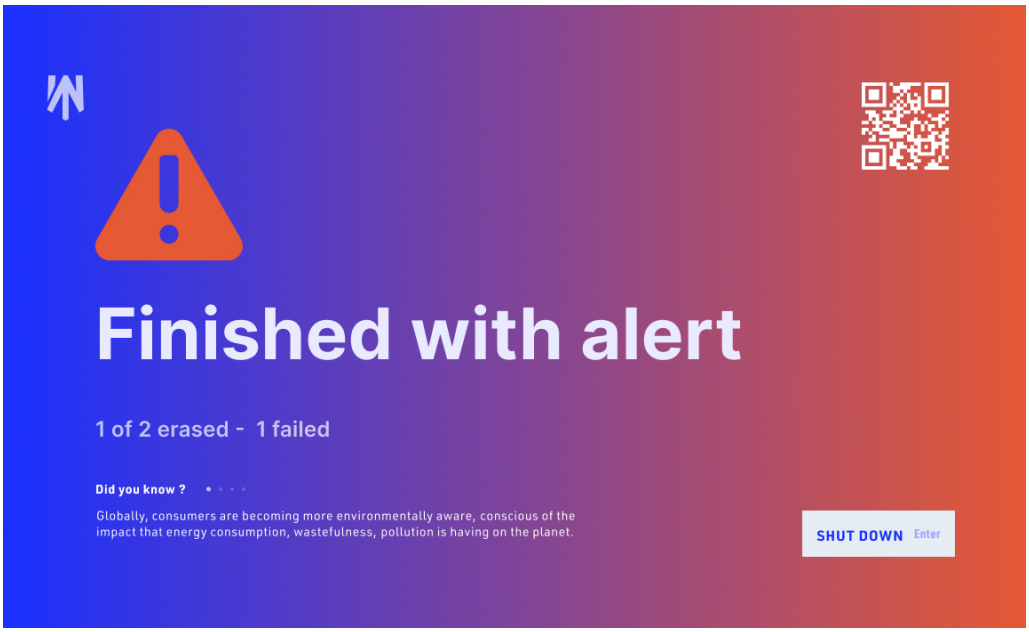
For successfully completed erasure, the screen will be green:



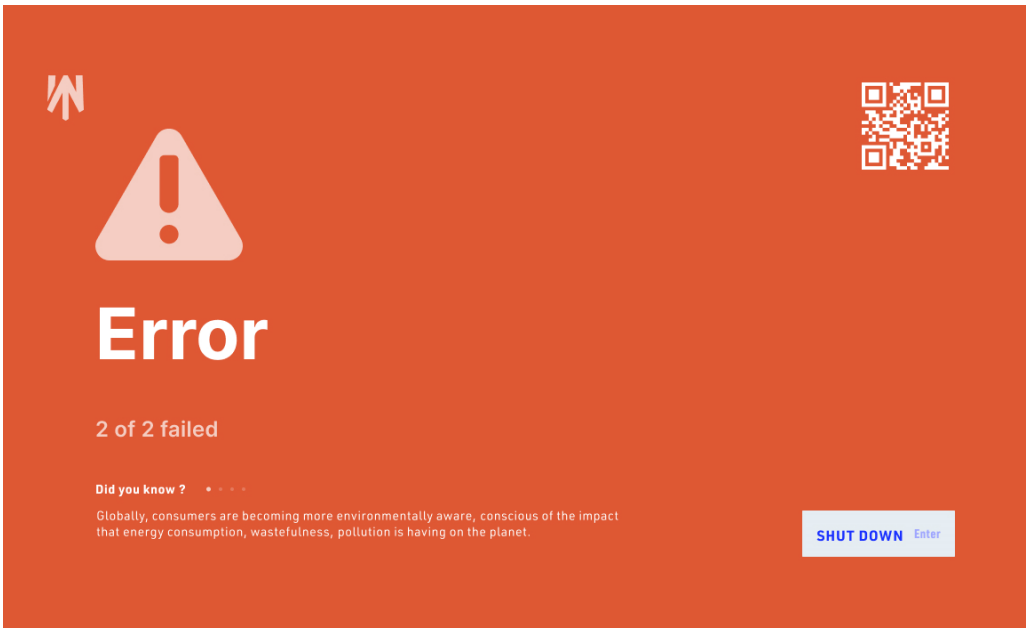
Error during erasure

If an erasure fails, you will see the warning icon and the screen will turn partially red.

If the erasure process failed for some assets, the screen will be red-blue:



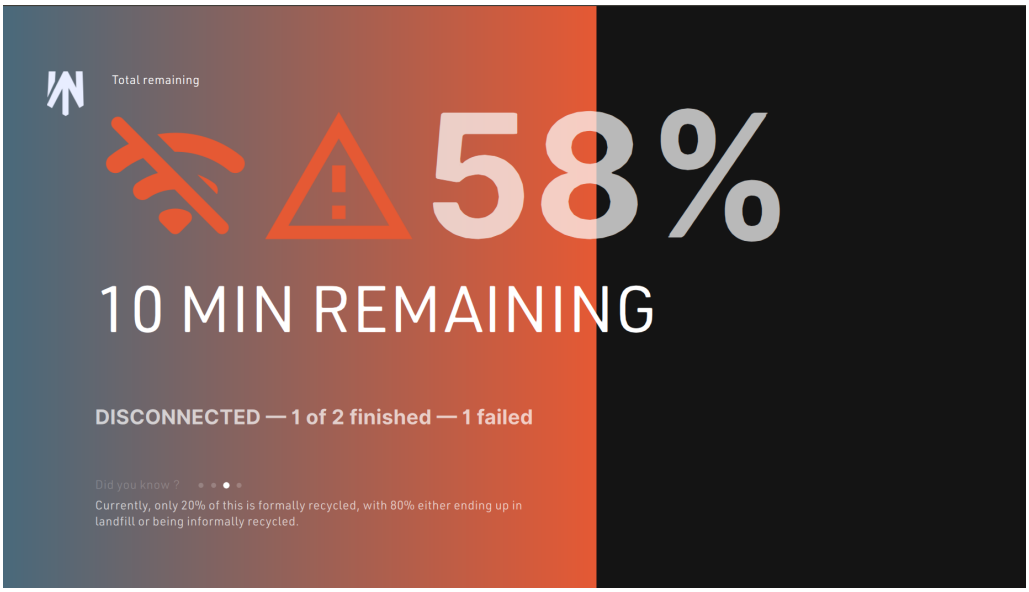
If the erasure process failed for all assets, the screen will be red:



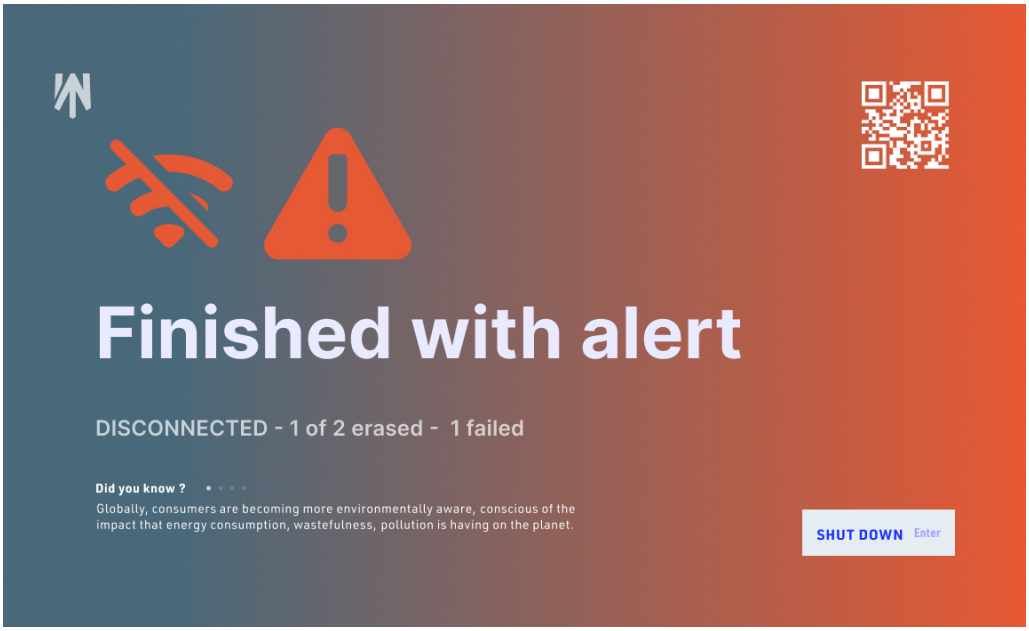
Offline during erasure

If the device goes offline during the erasure process, you will see the disconnected icon and the screen will turn partially gray.

If the device goes offline during the erasure process and the erasure fails, you will see both the disconnected and the warning icon and the screen will turn partially gray and red.



When the erasure process is complete, but the device is still disconnected (erasure report could not be uploaded to the Dashboard automatically), the screen will be gray-red:



If the internet connection is stable, at the end of the erasure you will receive a report in the Securaze Dashboard, regardless of whether the erasure was successful or failed.

Information about erasure reports can be found under Reports - Download erasure Report 152

Offline at the end of erasure

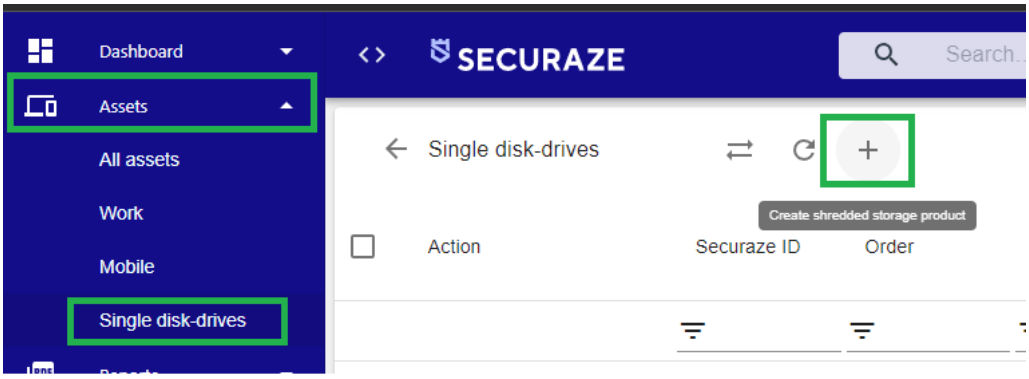
If the device is still offline at the end of erasure, you have two options:

- Reconnect network-cable or WiFi-Connection and Securaze Work will automatically detect the reconnected network and will upload the asset and erasure data. No additional steps are needed.
- Use Securaze Motion App to upload the asset and erasure data. (for Details see Work Offline 142)

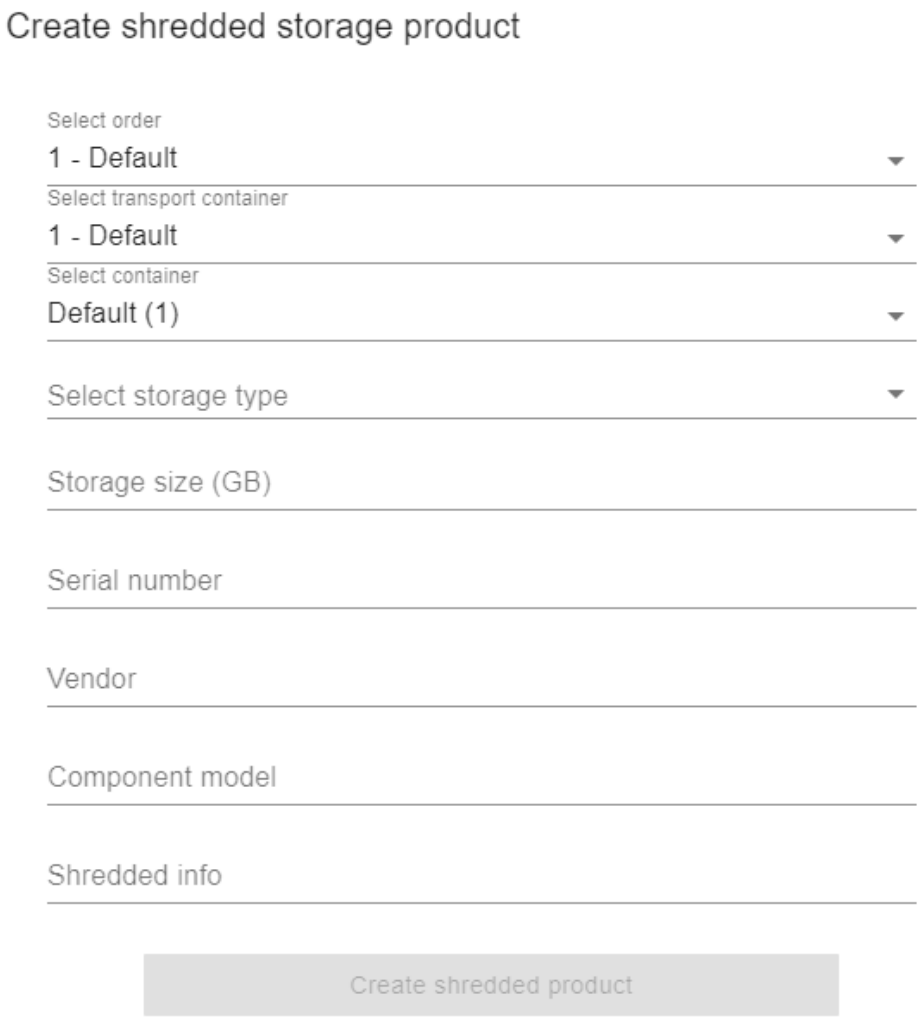
3.8.2 Schredded Storage Product

In case you cannot erase a disk, meaning either the erasure fails, or the disk is not even registered by Securaze Work, so simply said - it is a bad piece of hardware that is deemed to be destroyed (shredded), there is a way of saving the disk information within Securaze Dashboard. This way, all of the disks you are trying to process will be accounted for.

To create a shredded storage product, log in to the **Dashboard** in your browser, in the left sidebar menu click on **Assets**, then on **Single disk-drives**.
You will see a plus button in the upper area, and when you hover over it with mouse pointer, a message "Create shredded storage product" will be displayed.
Click on the button to add a new shredded disk.



A pop-up window will appear, where you can choose the logistics details, storage type (HDD / SDD) and then type in the rest of data manually.
Important note: If you set in Presets (Settings menu) the logistics (Order, Container and Transport Container), it will also be automatically selected during the creation of the shredded storage products.
You can still change it if you want to.

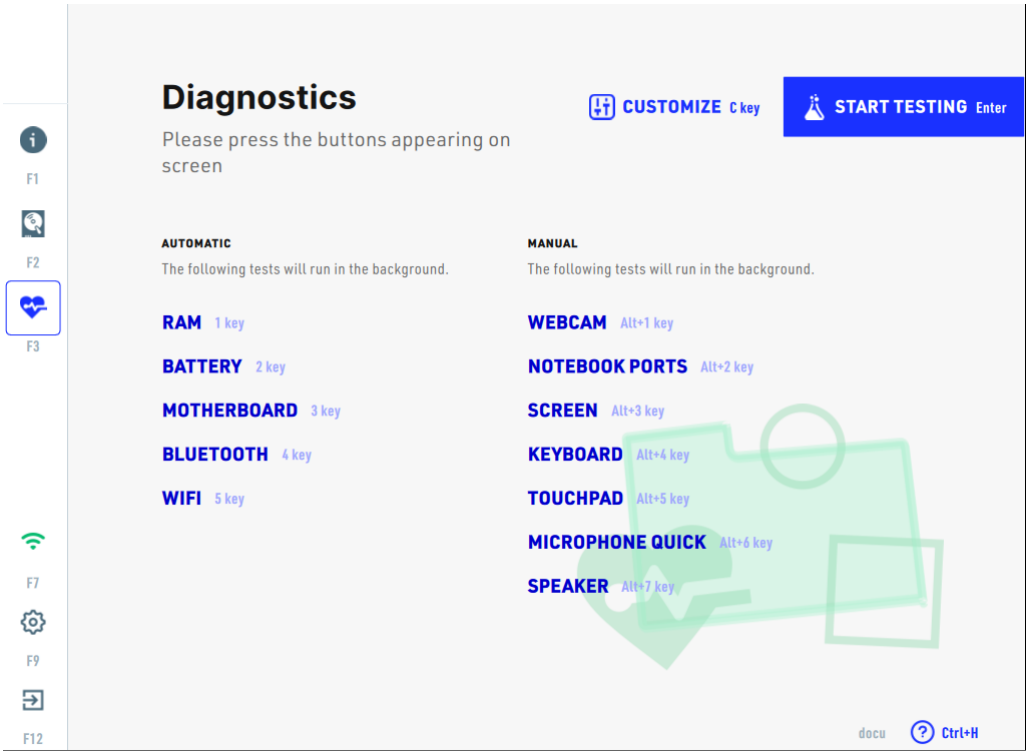


After all the information is stored, click on "Create shredded product".

This shredded disk will now be visible in the Single disk-drive section of the Dashboard. You can click on **Storage details** icon to check, add or edit the information of each disk, or download the shredded storage product report (found in the REPORTS tab).

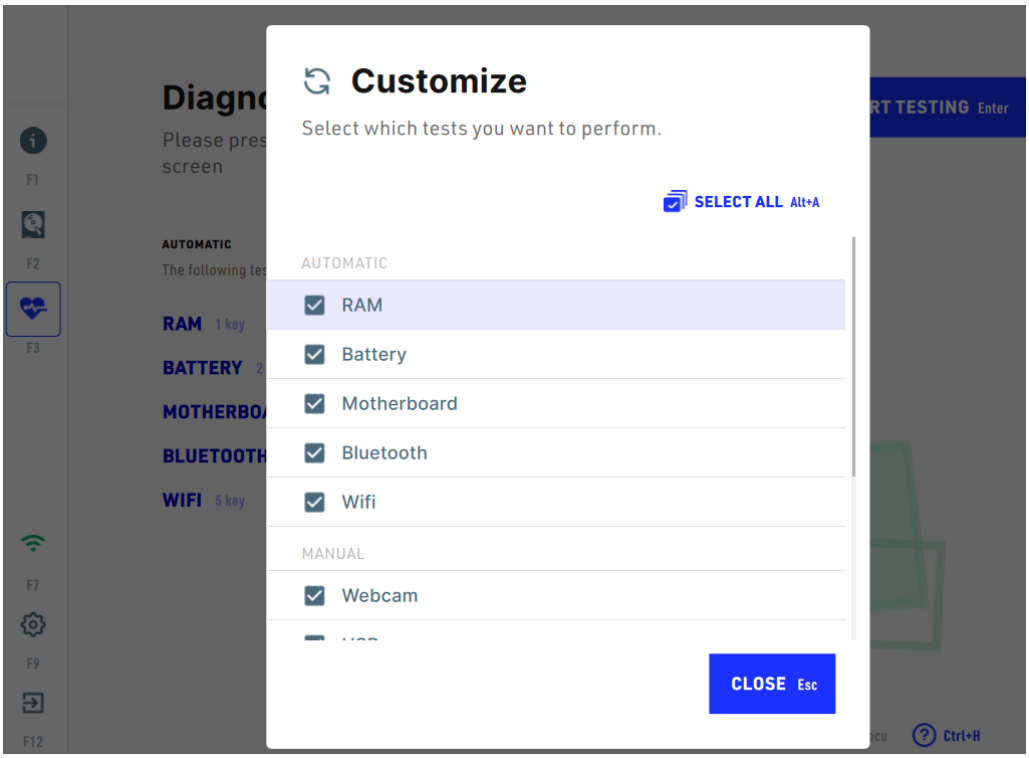
3.9 Diagnostics

To enter Diagnostics press F3 or click the heart icon in the menu on the left side of the screen.



In the Diagnostics overview you can see the tests that are performed by default. These are divided into automatic tests, where everything is executed automatically, and manual tests, where an action from the operator is required

To customize which tests should be performed, click on **CUSTOMIZE** in the upper area of the screen and a new window will open.



Here you can select which tests should be performed by checking the corresponding checkbox (you can also select or deselect all) and then clicking on **CLOSE**.

You can start each test separately using the respective keys on keyboard (e.g. 1 key for Battery, 3 key for Bluetooth, alt + 0 key for USB, alt + 2 key for Keyboard etc).
The session starts by pressing Enter key on the keyboard or clicking on **START TESTING** in the upper right corner.

Below you will find an **overview** of **all diagnostic cases**, which are divided into categories.

Camera

Name	Automatic	Manual	Short description	Link
Webcam		x	In this test the webcam is turned on and the operator has to see if the image is clear and alright.	Webcam 127

Communication

Name	Automatic	Manual	Short description	Link
Bluetooth	x		In this test, the device searches for other devices nearby. The operator has to make sure that there is a device nearby that sends out a permanent Bluetooth signal.	Bluetooth 126
WiFi	x		In this test, the device searches for a WiFi signal. The operator therefore has to ensure that a WiFi signal is available.	WiFi 126

Control

Name	Automatic	Manual	Short description	Link
Keyboard		x	In this test, the operator must press all the keys on the keyboard and it will be displayed if all the keys are reacting to the key press.	Keyboard 131
Trackpoint		x	In this test, the operator has to swipe their finger	Trackpoint 132

Name	Automatic	Manual	Short description	Link
			over the trackpoint and thereby move the mouse.	
Touchpad		x	In this test, the operator should slide their finger on the touchpad to the left and right and click the left and right mouse buttons.	Touchpad 131

Screen

Name	Automatic	Manual	Short description	Link
Screen		x	In this test, the operator has to choose at the beginning if they want to test everything or only certain colors or patterns. With "All tests" the screen changes color from red to green, to blue, to black and white squares, to white only, to black only and then back to screen outputs. The operator must then select if everything was error free or if there were stuck pixels somewhere.	Screen 129

Sound

Name	Automatic	Manual	Short description	Link
Microphone Quick		x	In this test, the operator needs to make a sound and as soon as a sound is perceived by the device, the test is passed.	Microphone Quick 132
Speakers		x	In this test, sound is played on all speakers	Speakers 133

Name	Automatic	Manual	Short description	Link
			one after another and the operator must confirm whether a sound is heard per speaker.	

System

Name	Automatic	Manual	Short description	Link
Battery capacity	x		In this test, the condition of the battery is checked and displayed.	Battery capacity 127
RAM	x		In this test, random data is written to the free areas of RAM and it is checked if all data is valid.	RAM 126
Motherboard	x		In this test, the CMOS checksum, CMOS battery, RTC (Real-Time Clock), UEFI and Desktop management interface are automatically tested for proper functionality.	Motherboard 127
Touchbar		x	In this test, the operator has to move the slider completely, which will show up on the Touchbar.	Touchbar 134
USB		x	In this test, the operator has to connect a device to see if all detected ports are listed.	USB 128

Here you will find the **detailed descriptions** of the various **diagnostic cases**.

3.9.1 Automatic tests

All of the Automatic tests will be performed in the background.
A pop-up window with the information that the tests have been completed (and also if any of them failed for did not meet the requirements) will appear afterwards.

3.9.1.1 RAM

Random data is written to the free areas of RAM (full RAM test not doable on booted device). Securaze checks back to affirm all is valid; if good, Securaze verifies it is working and test is passed. If not, it is failed.

Securaze Work cannot detect the defect RAM bar from software, as there are many different hardware related variables which make it impossible to tell which RAM bar is the defect. There is, however, a workaround, as suggested by memtestx86:

Once a memory error has been detected, determining the failing SIMM/DIMM module is not a clear cut procedure. Different CPUs map memory addresses to physical memory sticks in different ways. Features like dual channel RAM (with interleaving), channel hashing and NUMA make the mapping of addresses to modules, banks & rows very difficult. Due to the large number of CPUs and motherboard vendors and potential combinations of memory slots we do not have a general solution, though in some cases limited decode is possible. However, there are steps that may be taken to determine the failing module. Here are some techniques that you may wish to use:

1) Removing modules

This is simplest method for isolating a failing modules, but may only be employed when one or more modules can be removed from the system. By selectively removing modules from the system and then running the test you will be able to find the bad modules. Be sure to note exactly which modules are in the system when the test passes and when the test fails.

2) Rotating modules

When none of the modules can be removed then you may wish to rotate modules to find the failing one. This technique can only be used if there are three or more modules in the system. Change the location of two modules at a time. For example put the module from slot 1 into slot 2 and put the module from slot 2 in slot 1. Run the test and if either the failing bit or address changes then you know that the failing module is one of the ones just moved. By using several combinations of module movement you should be able to determine which module is failing.

3) Replacing modules

If you are unable to use either of the previous techniques then you are left to selective replacement of modules to find the failure.

3.9.1.2 Bluetooth

During this test, the device goes into scan mode and looks for nearby devices. As such, it is important to have a device around that emits a persistent BT signal. If found, radio works and the test is passed. If not, it is failed.

3.9.1.3 WiFi

During this test, the device goes into scan mode and looks for a WiFi signal. If Securaze Work Ops is connected to internet via WiFi, it passes immediately.

3.9.1.4 Battery capacity

The battery capacity test checks the state of the battery and indicates what condition the battery is in. In the production of each battery a maximum capacity must be set for the battery capacity. This test compares the current maximum capacity with the original maximum capacity and calculates the difference to know how good the battery is.

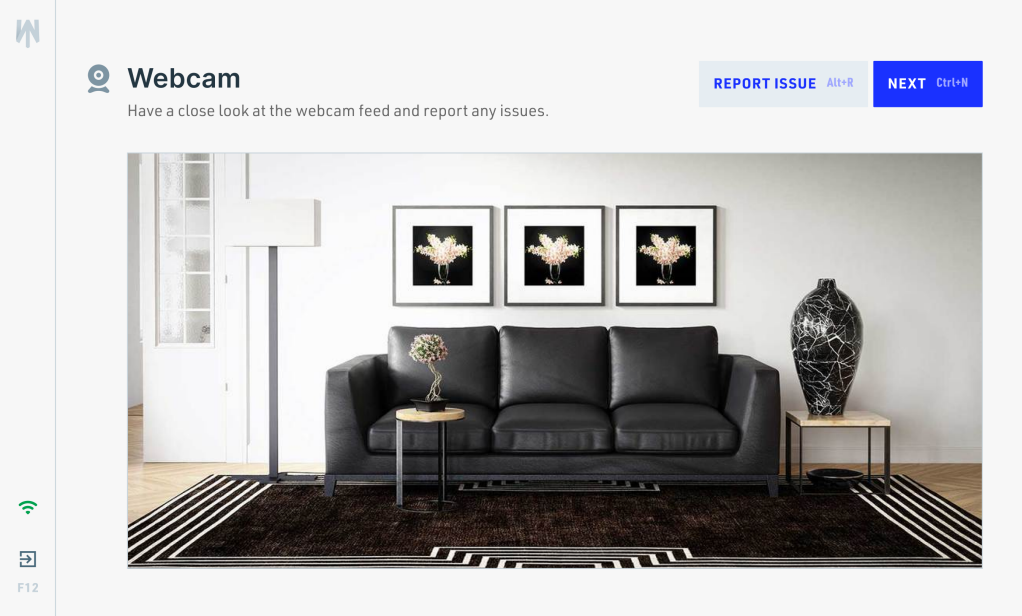
3.9.1.5 Motherboard

The motherboard test checks the CMOS checksum, the CMOS battery, RTC, UEFI and DMI.
The CMOS checksum is tested and checked to see if it is faulty. If the CMOS checksum is valid, the test is passed.
For the CMOS battery, it is tested and evaluated whether it still works well or is already weak and a new battery is needed.
In the RTC part of the motherboard test, it is checked if an Apple Silicon is present or not and if it is present, the RTC (Real-Time Clock) is checked for functionality.
The UEFI part of the test checks if an Apple silicon is present or not, and if it is, UEFI is tested for functionality.
With DMI, seven different properties are tested and at least 5 of the 7 must be detected for the test to be successful. Some of these seven properties that are tested are BIOS date, version, vendor and release as well as board serial.

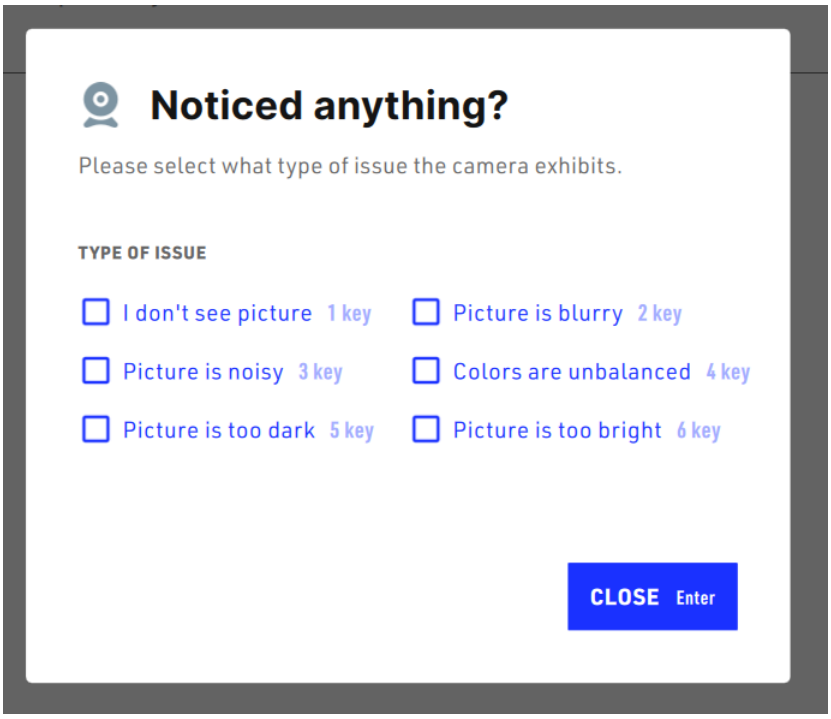
3.9.2 Manual tests

3.9.2.1 Webcam

The webcam is turned on and you just need to check if the picture you see is ok.



If there are any issues click on **REPORT ISSUE** and a pop-up will open.

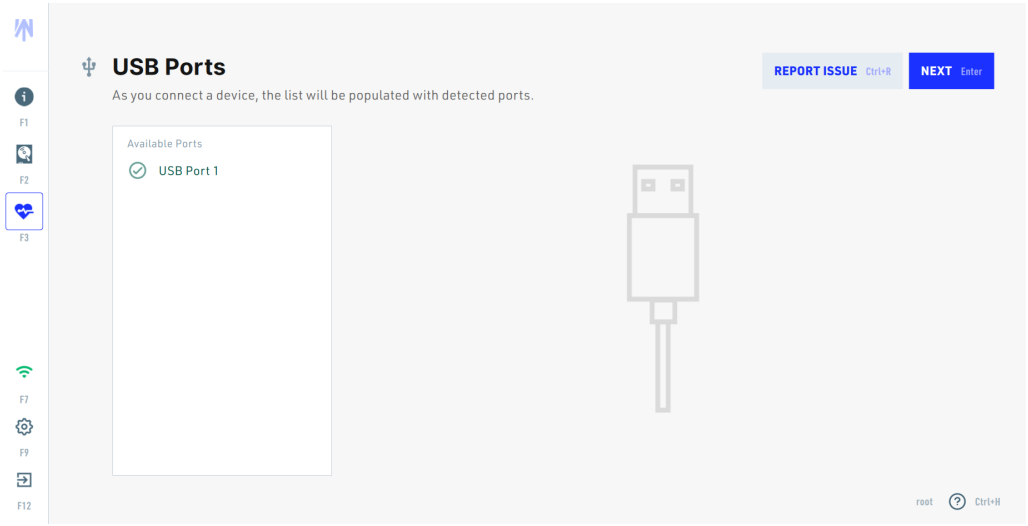


Here you can select what type of issue the camera exhibits by checking the corresponding checkbox and then clicking on **CLOSE**.

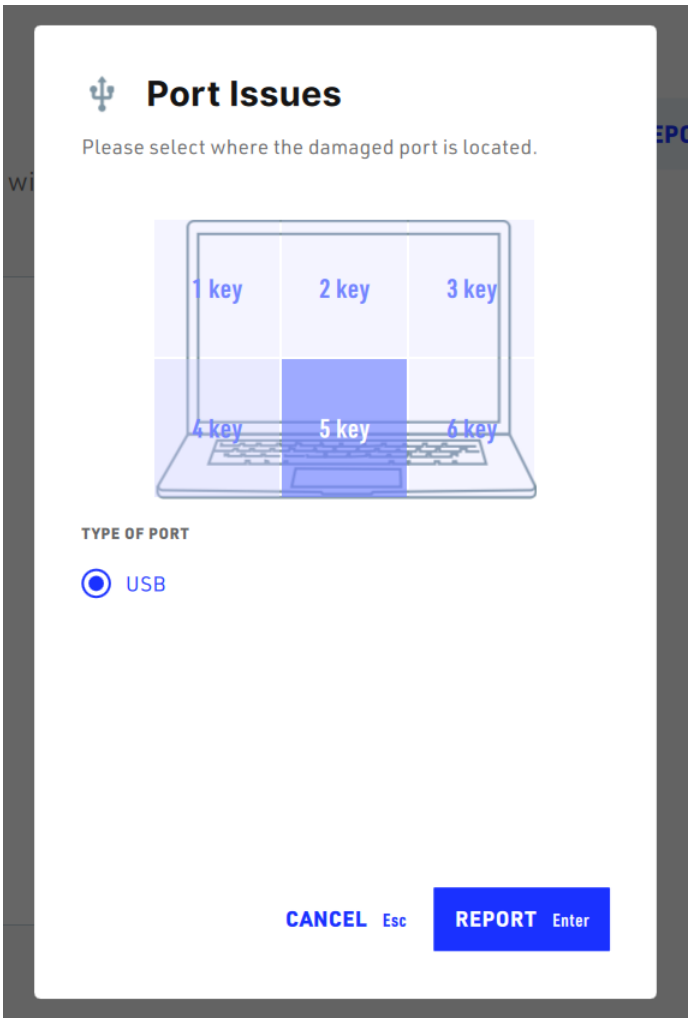
To proceed to the next test, click on **NEXT**.

3.9.2.2 USB

For testing USB ports, Work Diagnostics asks you to connect a device, so it can list all the detected ports.



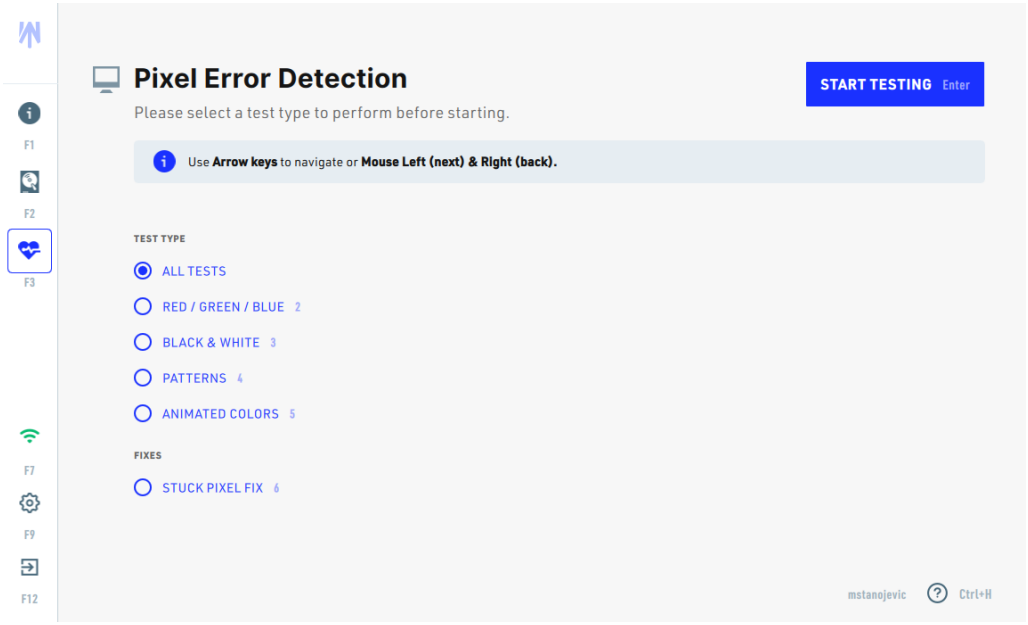
If there are any issues click on **REPORT ISSUE** and a pop-up will open where you can report a damaged port.



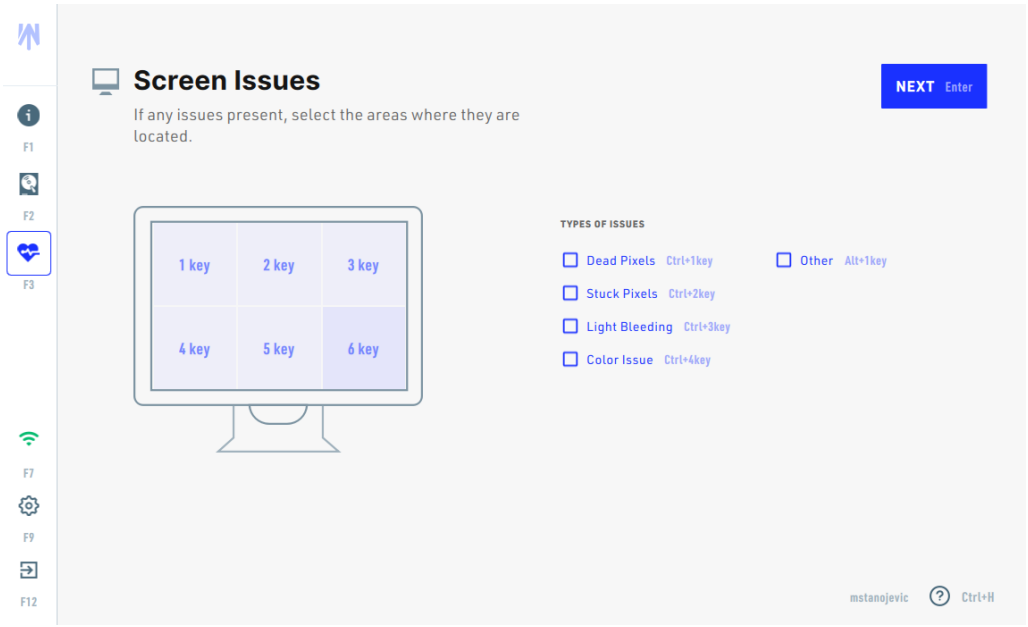
To proceed to the next test, click on **NEXT**.

3.9.2.3 Screen

Before you can start the Pixel error detection, you need to choose a test type.



You can make your selection with arrow keys or mouse left-click (next) and right-click (back).
The test starts and the screen changes colors from red, to green, to blue, to black and white squares, to white only, to black only and then back to Screen issues.

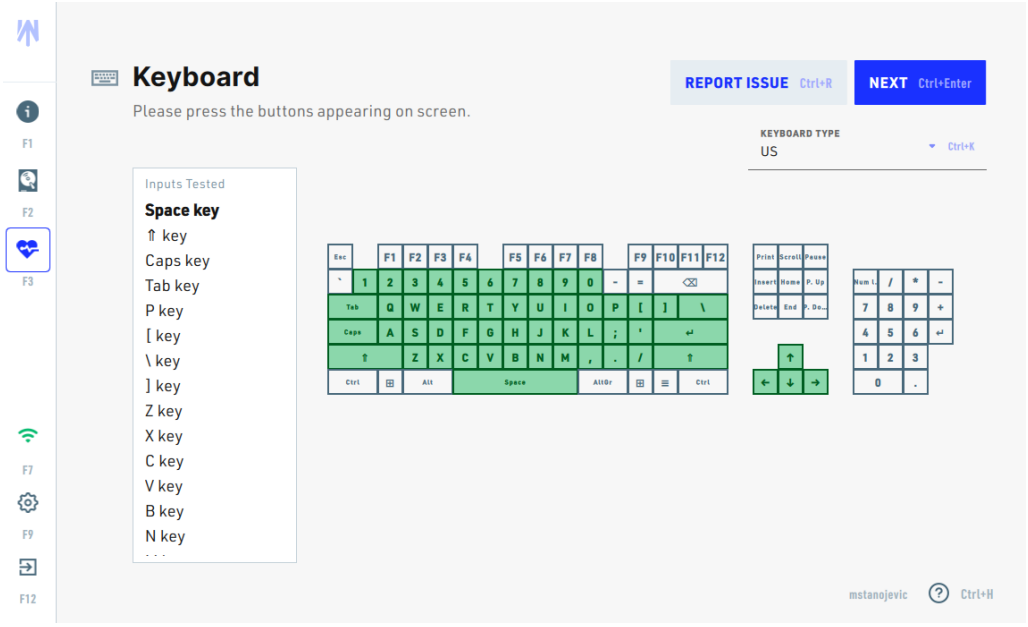


In the screen issues, you can select the screen part that is damaged by clicking on the corresponding field or pressing the corresponding key (1 to 6) and choose the type of damage:
- Dead Pixels (ctrl + 1 key)
- Stuck Pixels (ctrl + 2 key)
- Light Bleeding (ctrl + 3 key)
- Color Issues (ctrl + 4 key)
- Other (alt +1 key)

To proceed to the next test, click on **NEXT**.

3.9.2.4 Keyboard

For the keyboard test, all the keys on the keyboard simply need to be pressed, and if all of them work, the whole keyboard will appear in green on the screen.

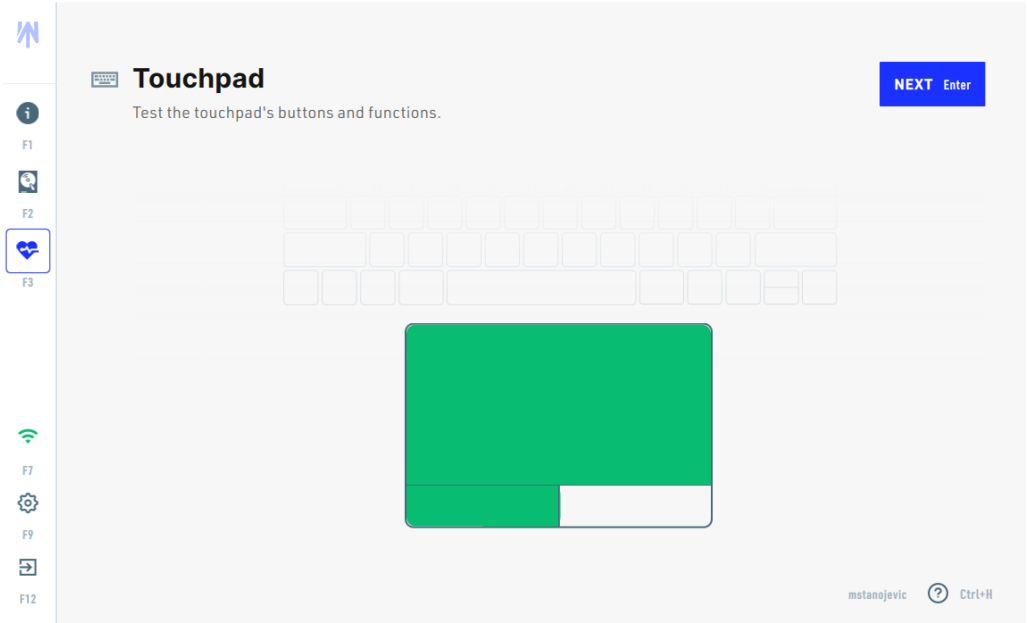


You can select the keyboard type (e.g. US) in the upper right corner.

If there are any issues click on **REPORT ISSUE** and a pop-up will open where you can report a damaged key.
To proceed to the next test, click on **NEXT**.

3.9.2.5 Touchpad

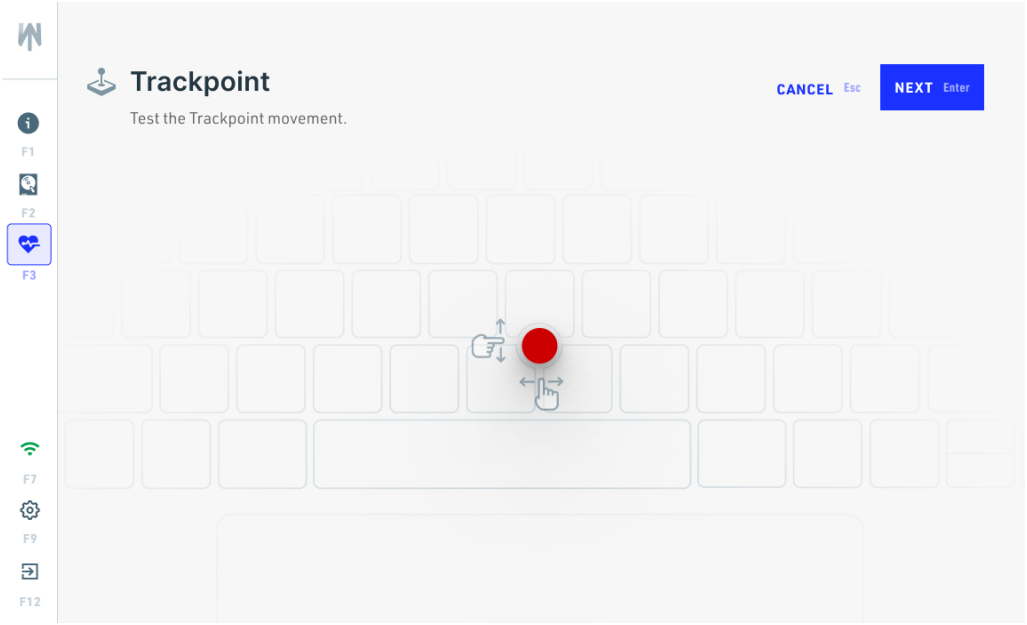
To start it, you slide left and right with your finger on the touchpad and click both left click and right click buttons. The touchpad fields shown on the screen will turn from white to green if they are functional.



To proceed to the next test, click on **NEXT**.

3.9.2.6 Trackpoint

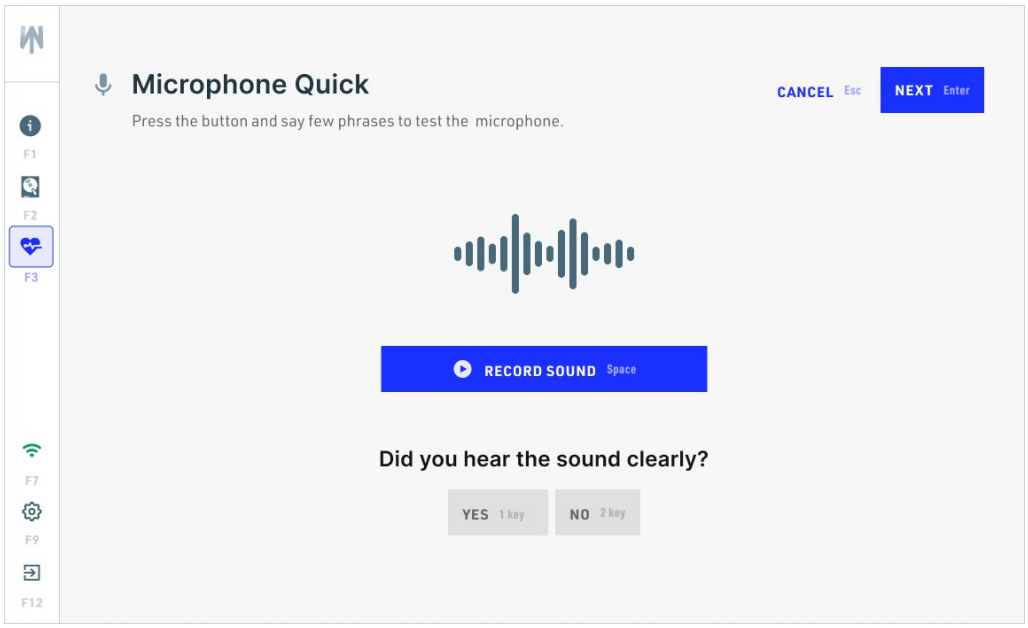
To test the trackpoint, simply move your finger on the trackpoint in all directions and see if the cursor on the screen moves in the respective direction. If the movement is perceived, the test is passed successfully.



To proceed to the next test, click on **NEXT**.

3.9.2.7 Microphone Quick

In the Microphone Quick test, you need to click the "Record Sound" button and then say a few words or make sounds that the microphone will record. After the microphone has perceived the sounds, the sounds you have just recorded will be played and you will have to confirm whether you heard the sound clearly or not by pressing a button. You can also play the sounds again by clicking the "Restart" button.

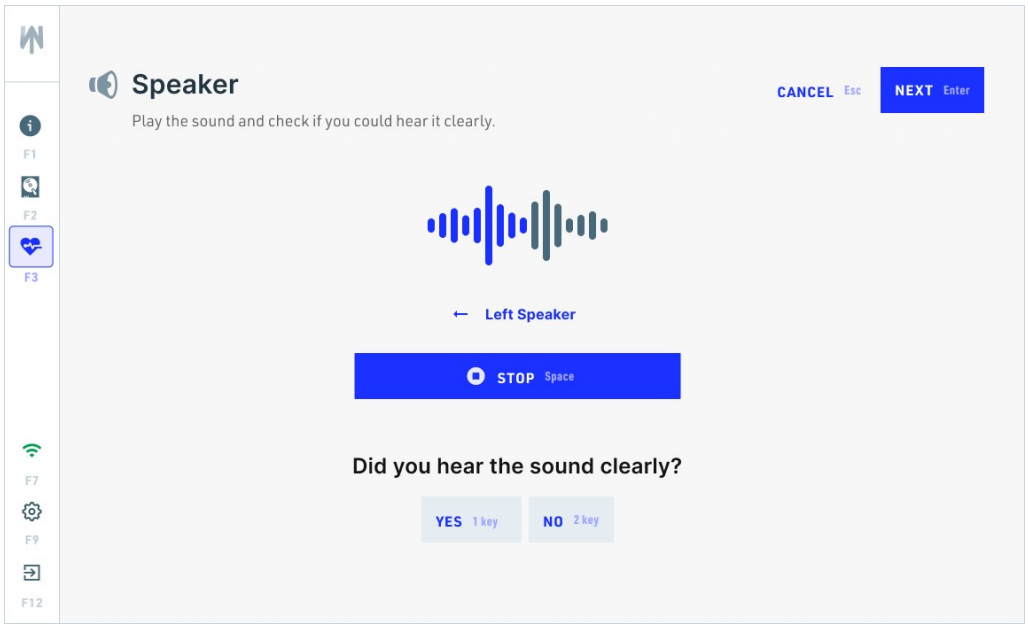


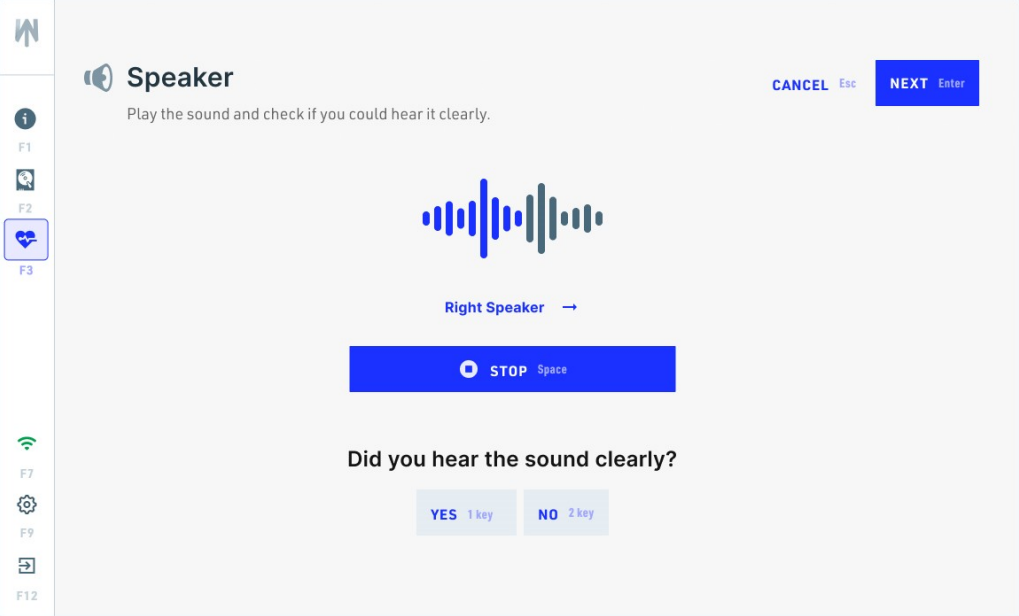
To proceed to the next test, click on **NEXT**.

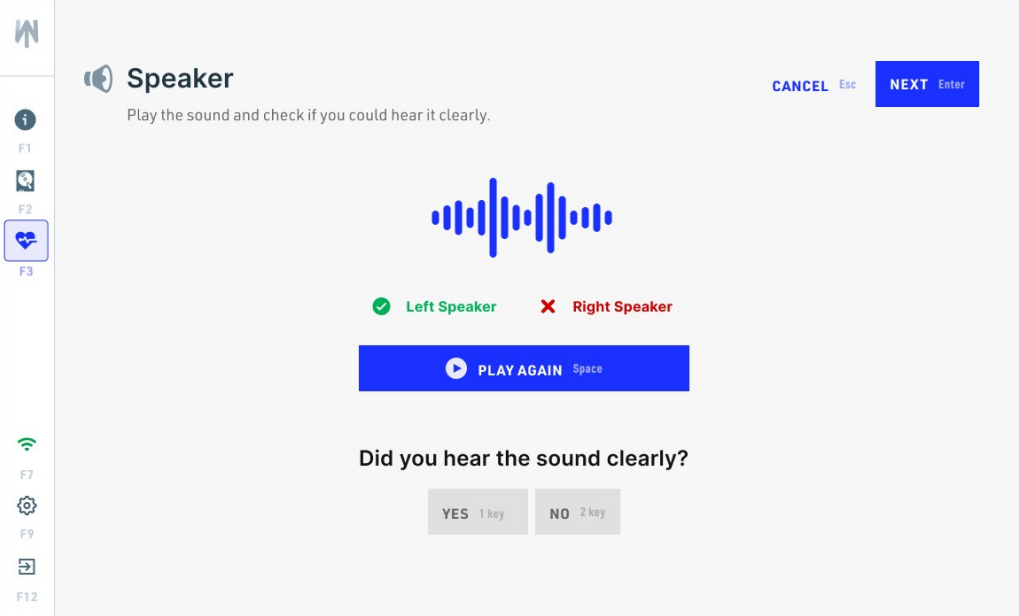
3.9.2.8 Speakers

During the speaker test, a sound is automatically played on the left speaker and you must check whether you can hear the sound clearly. Then confirm with the "Yes" or "No" key whether you could hear the sound clearly. After that, the same is repeated for the right speaker and you have to confirm again if you can hear the sound clearly. After that, an overview appears where you can see how you decided and can repeat the test and play the sounds again.

The shortcuts for the answers are 1 for "Yes" and 2 for "No".



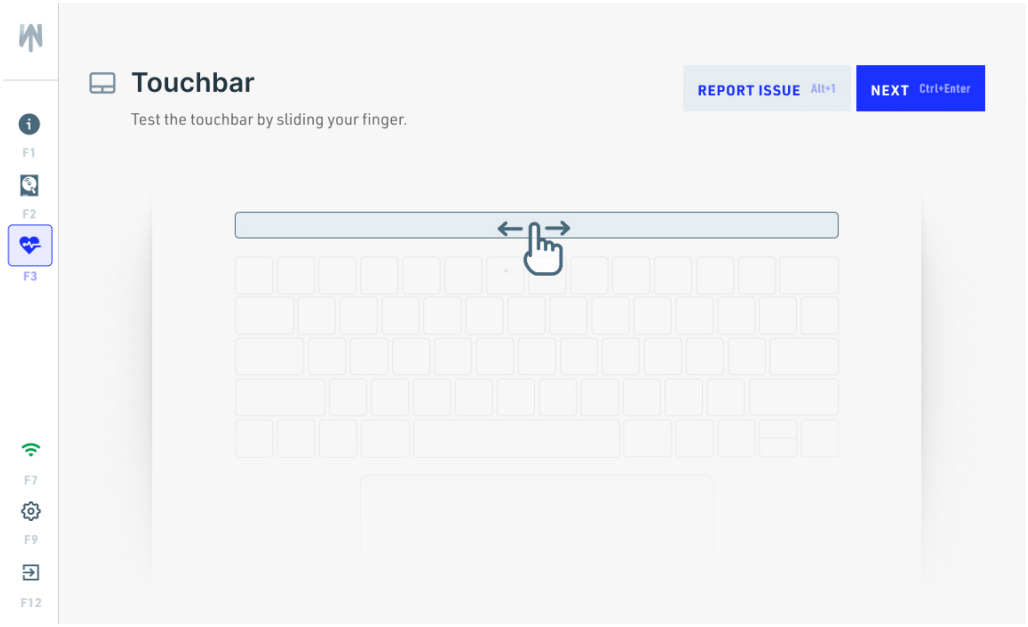




To proceed to the next test, click on **NEXT**.

3.9.2.9 Touchbar

The Touchbar is the bar at the very top of the keyboard on certain MacBooks and Macs. In this test, you have to use your finger to slide the provided slider completely to the left and right. If you manage to move the slider completely, the test is passed successfully.

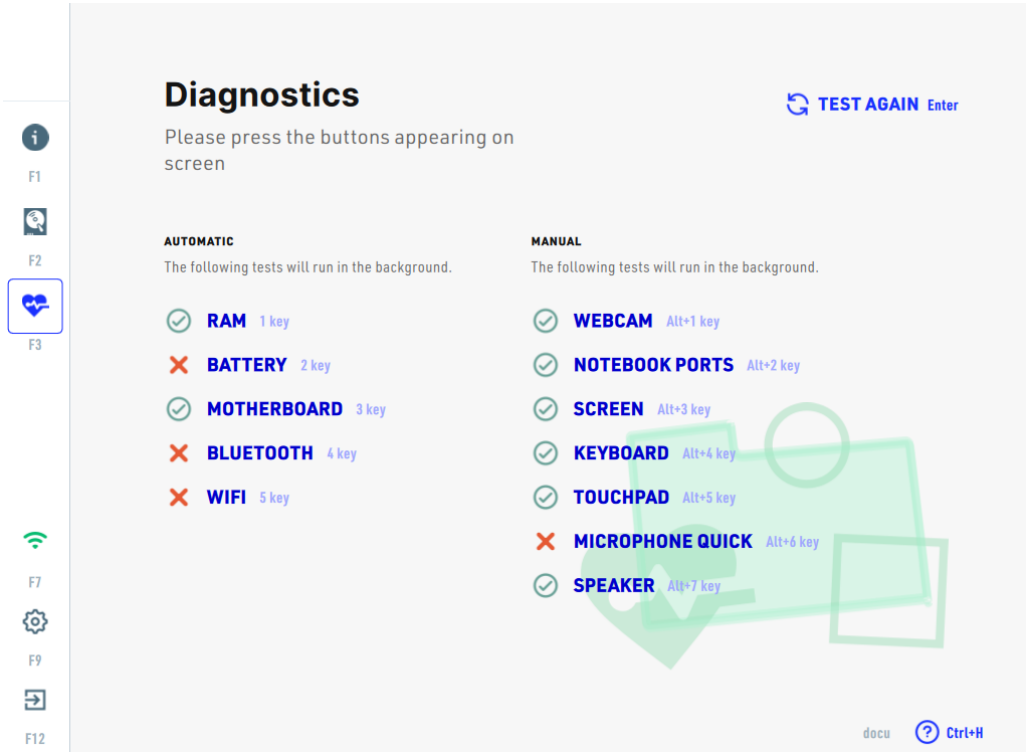


If there are any issues, click on **REPORT ISSUE** and a pop-up will open where you can specify what is not working with the Touchbar. The test is not supported when the device is in Apple Recovery Mode.

To proceed to the next test, click on **NEXT**.

3.9.3 Diagnose completed

You are now back on the Diagnostics page, where the results of the tests are shown.



Green check symbol is next to a successfully completed test and red “x” is next to the failed test.

You may start the tests again with clicking **TEST AGAIN** or by pressing alt + A key on the keyboard. You select / deselect the tests you wish to perform again and start with ENTER on the keyboard or clicking on **START AGAIN** on the lower right part of the screen.

Command Line Usage

4 Command Line Usage

Securaze Work can be controlled by command line.
It is used to securely erase selected files and folders using various rules. The software will erase the files and folders in the background on selected machines.
Command Line is currently only available for macOS.

You can use the following parameters to achieve the desired action:

Options:	
-h, --help	Show help
-n, --nogui	Run client without gui
-u, --username <username>	User to login <securaze username>.
-p, --password <password>	Password to login <securaze password>.
-s, --standard	The erasure standard which should be used for erasure. e.g.
-a, --advanced	Advanced output mode

For File erasure (upcoming feature)	
-o, --aon	Checks if all files can be erased and erases only if all files can be erased [valid for erasefile+erasefolder]
--leave	The file should be erased but not removed from the filesystem. [valid for erasefile+erasefolder]
--force	The file should be removed even a program is currently having it open. [valid for erasefile+erasefolder]
--path	Report file path can be specified as an optional parameter. [valid for erasefile+erasefolder]
-b, --batch	A file containing the files or folders to erase. The file must contain fullpaths. [valid for erasefile+erasefolder]
--olderthen n	Erase only files or folders older than n days/date. (If n < 1900 then n = no of days, else n = YYYYMMDD date) e.g. --olderthen 10 or --olderthen 20201224 [valid for erasefile+erasefolder]

Arguments:	
standards	List all available algorithms
print	Print device configuration
register	Register the system with all hardware informations. [Login required]
erasesystem	To start erasure, specify the storage to erase. [Login required] More storages can be specified and seperated with spaces. e.g. "/dev/disk0" "/dev/disk1"

erasedisk	To start erasure of specific disks, specify the storage to erase. [Login required] More storages can be specified and seperated with spaces. e.g. "/dev/disk0" "/dev/disk1"
erasefile (upcoming feature)	To start erasure of specific files, specify fullpath of the file. [Login required] More files can be specified and seperated with spaces. e.g. "C:\SecretFile\file1.txt" "D:\AnotherLocation\file2.txt"
erasefolder (upcoming feature)	To start erasure of specific folders, specify fullpath of the folder. [Login required] More folders can be specified and seperated with spaces. e.g. "C:\SecretFile" "D:\AnotherLocation"

Work Offline

5 Work Offline

If you want to use Securaze Work Offline, you need to download the Securaze Motion App on your Smartphone from

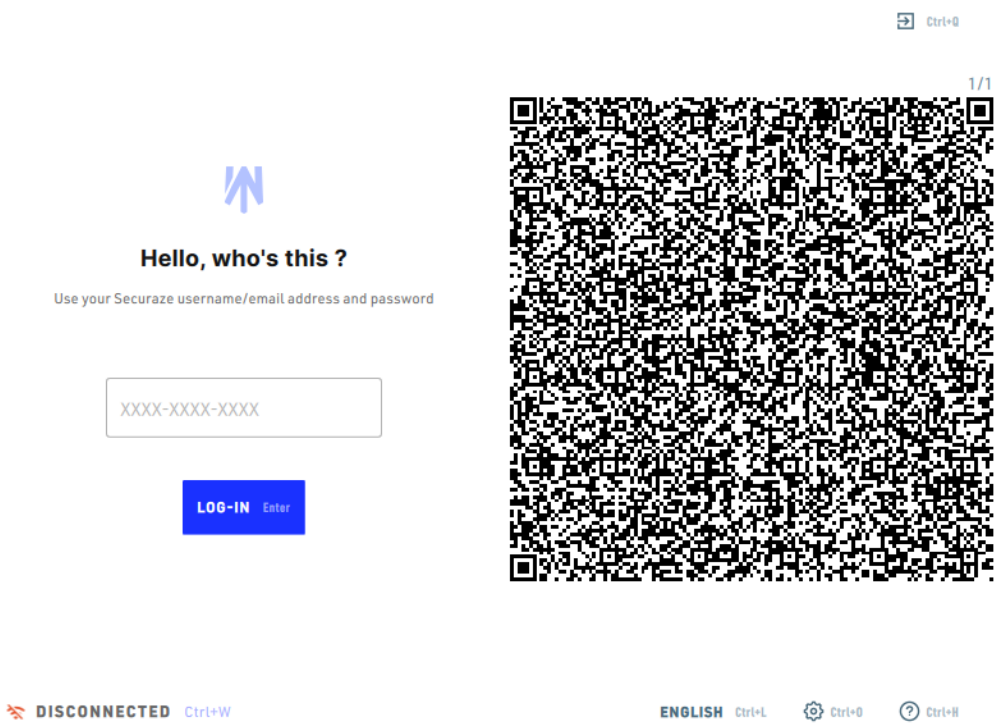
The available downloads are listed on the Securaze Motion Ops product page:
https://securaze.com/motion-operations
and are found on the individual AppStores:

Apple AppStore
https://apps.apple.com/in/app/securaze-motion-app/id1552368203

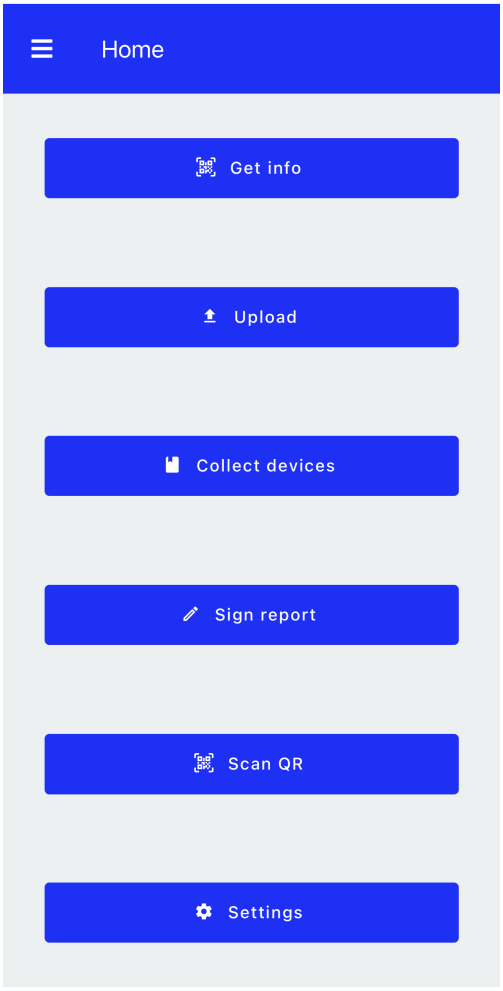
or

Google PlayStore
https://play.google.com/store/apps/details?id=com.securazemotion

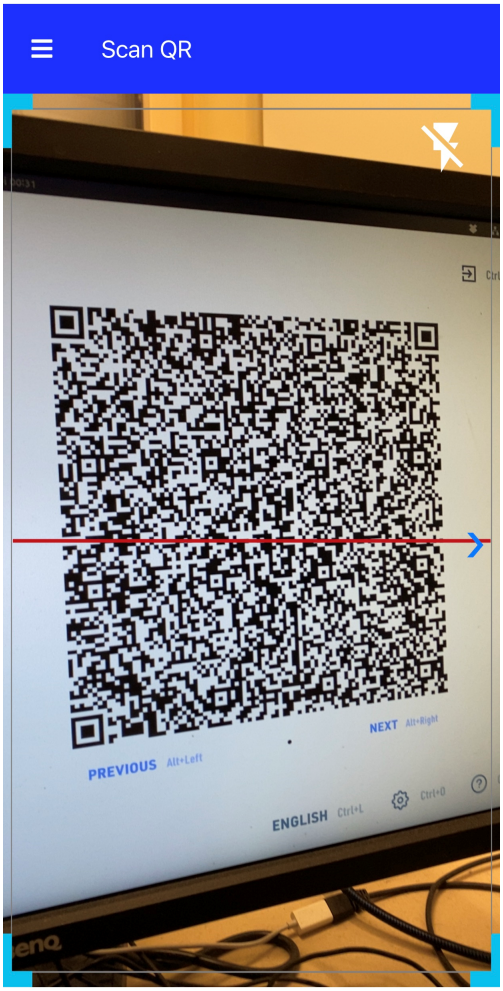
Instead of the login screen, where you enter your username and password, you will see a QR Code.



Scan the QR Code with the Securaze Motion App on your Smartphone by using the functionality "Scan QR".

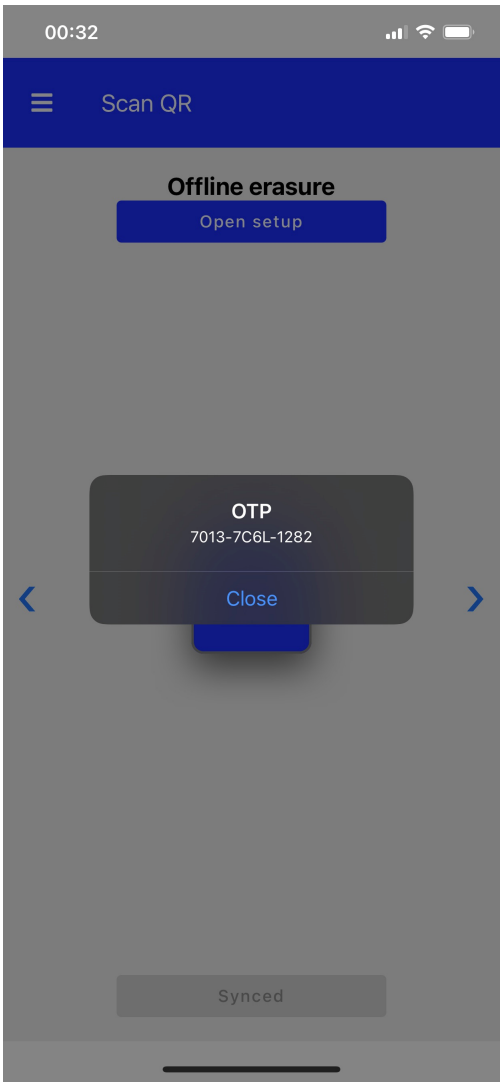


Click on **Scan QR** to start the scanning.

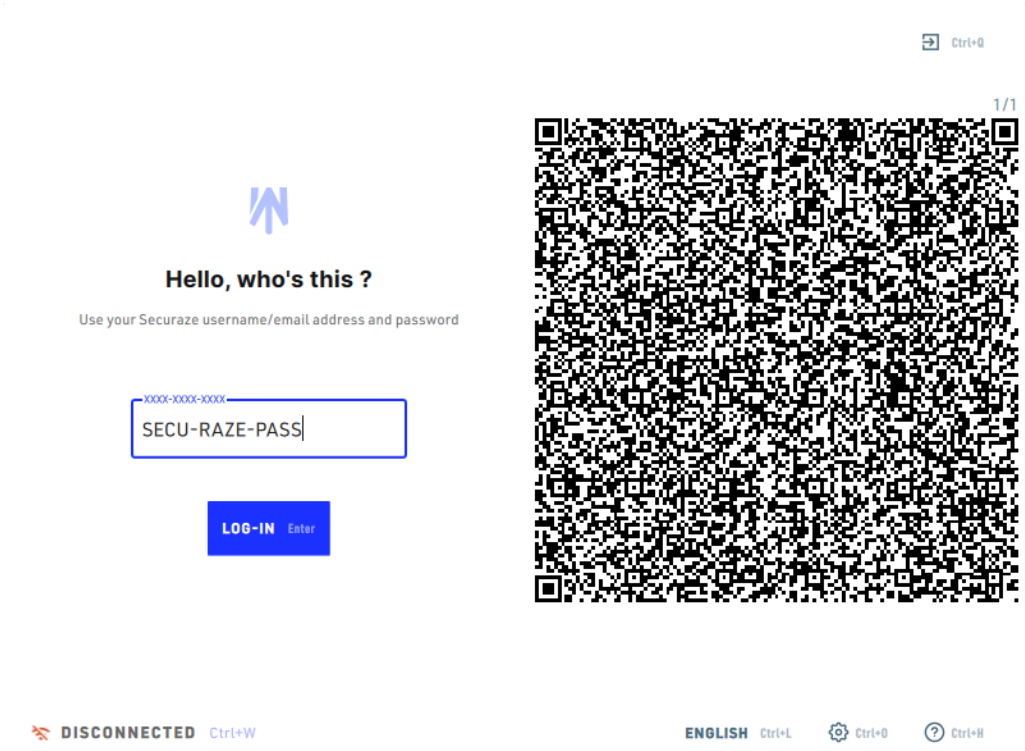


When the scanning is completed, you will receive the message **QR Code scanned successfully** on the App Securaze Motion.

An OTP - One Time Password will be generated.



With this password you can log onto Securaze Work.



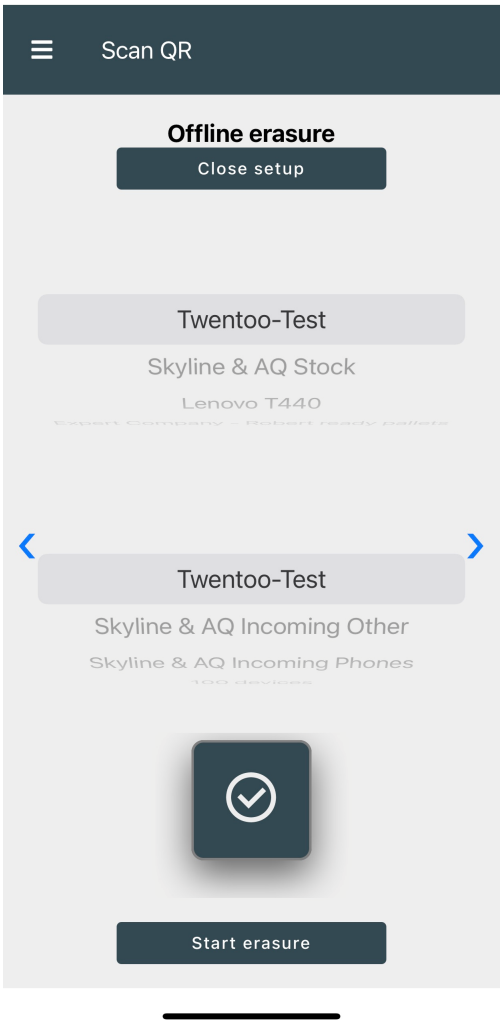
Enter the created password (OTP) in Securaze Work and select **LOG-IN [ENTER]**.

After the Login you proceed as described in chapter Operation 72 with grading and erasure.

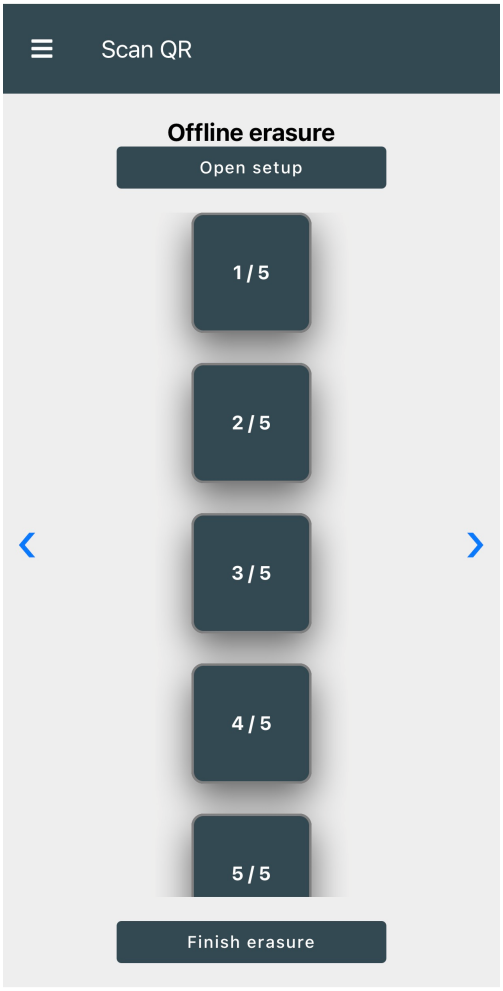
After the erasure Securaze Work shows QR Codes of the erasure.

Now you can scan the QR Codes with the Securaze Motion App by clicking on **Scan QR**. You need to switch after each successful scan to the next QR-Code in Securaze Work.

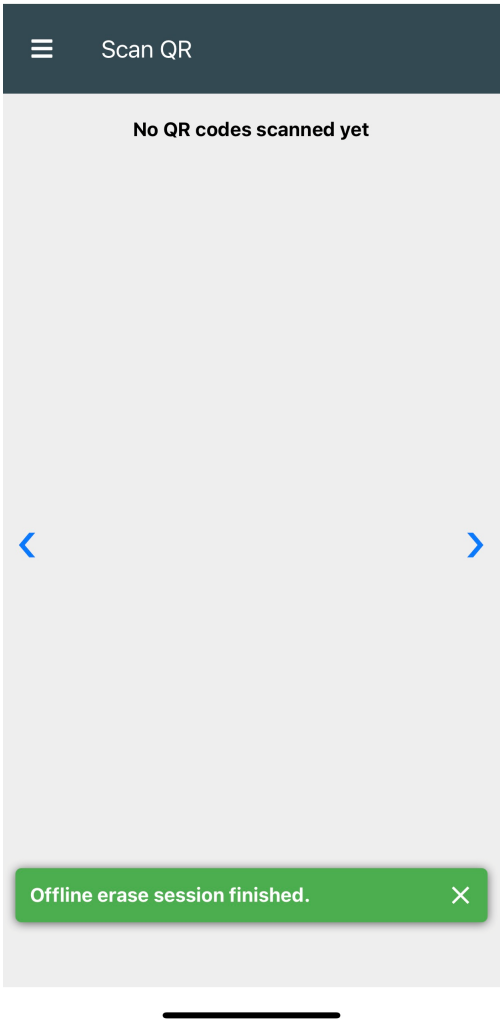
After all QR-Codes are scanned you can choose the logistic data.



You can see all QR Codes in the Securaze Motion App.



Press **Finish erasure** to transfer the erasure data to the cloud.



Reports

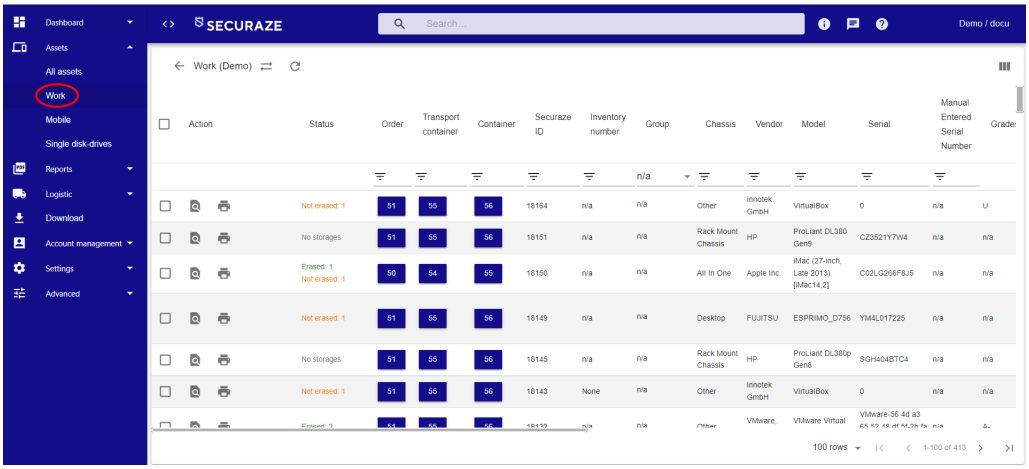
6 Reports

You can find the erasure reports in Securaze Dashboard.

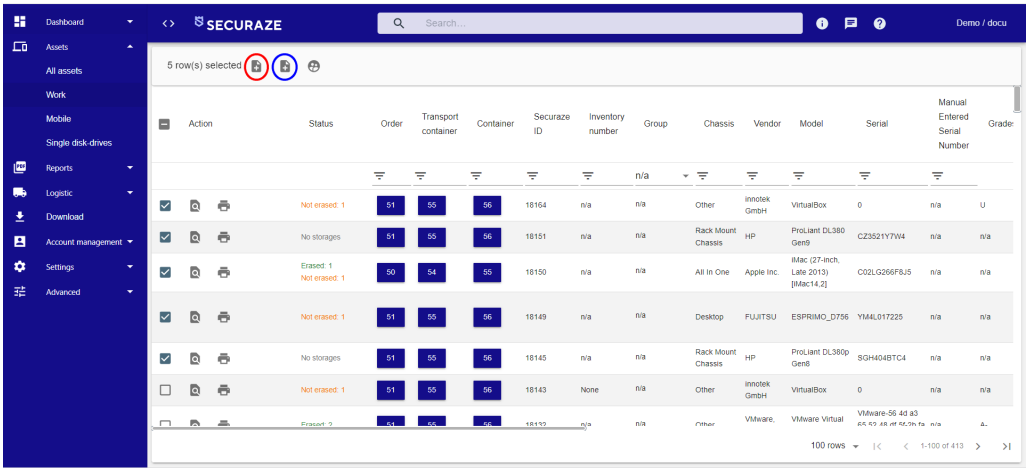
6.1 Download erasure and diagnose report

You have several options to download erasure and / or diagnose reports.

1. You can download reports in the menu **Assets - Work** in Securaze Dashboard.

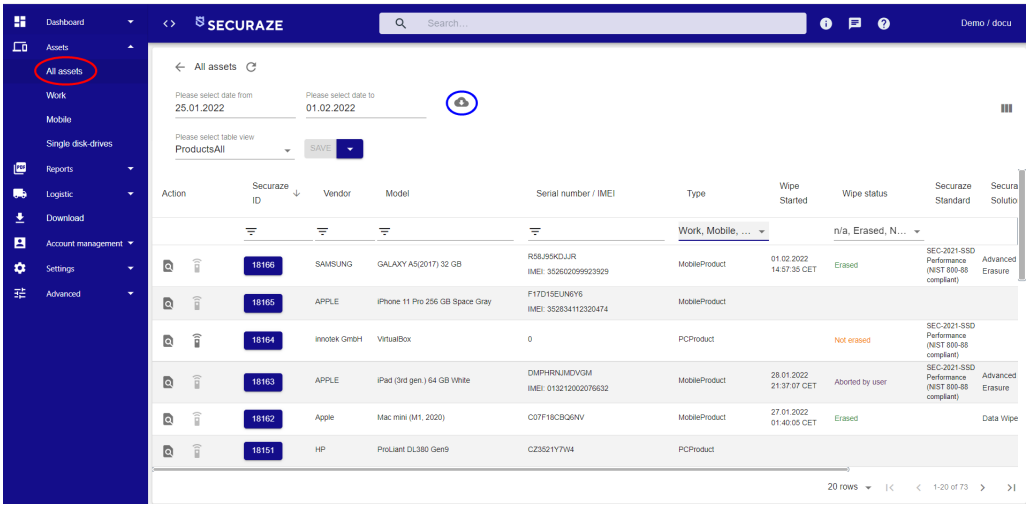


Select the assets for which you want to download the reports by checking the box. You can also select all Assets by checking the box next to **Action** in the upper area. Once you have checked the desired assets, you can select whether you want to download the erasure reports or diagnose reports in the top left section.

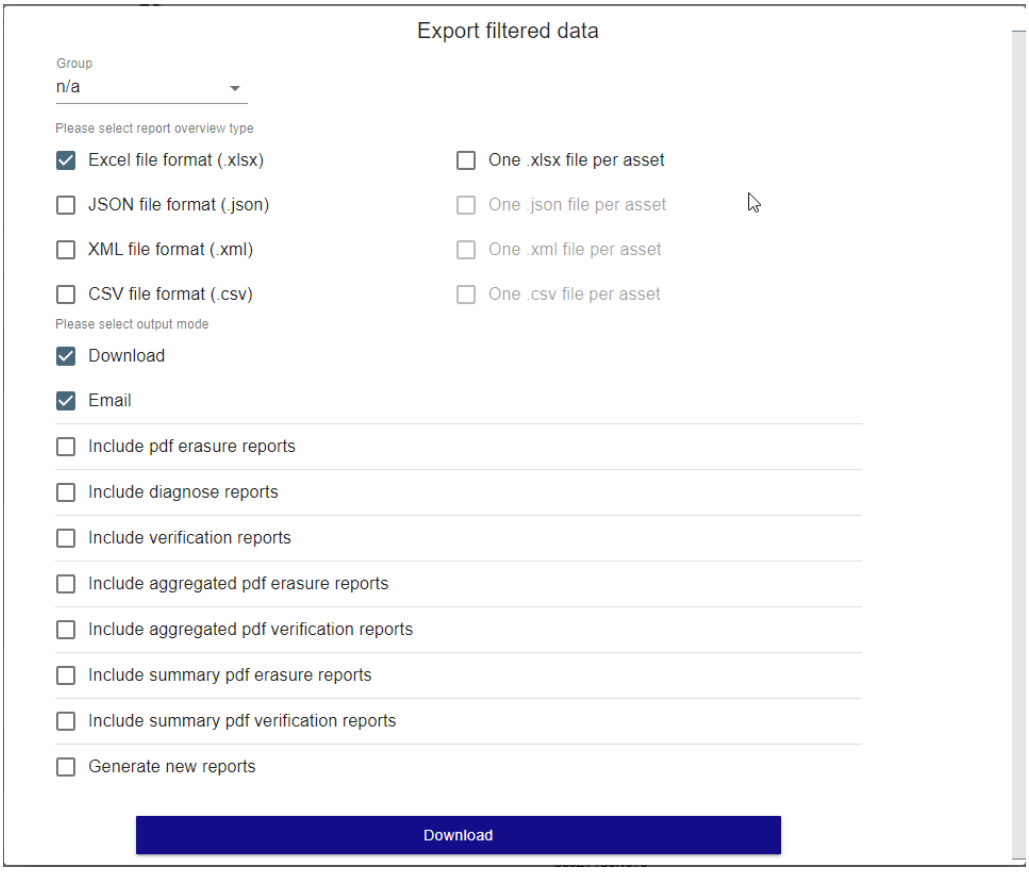


The reports will be downloaded to your download folder.

2. You can download reports based on date of processing in the menu **Assets - All Assets** in Securaze Dashboard.

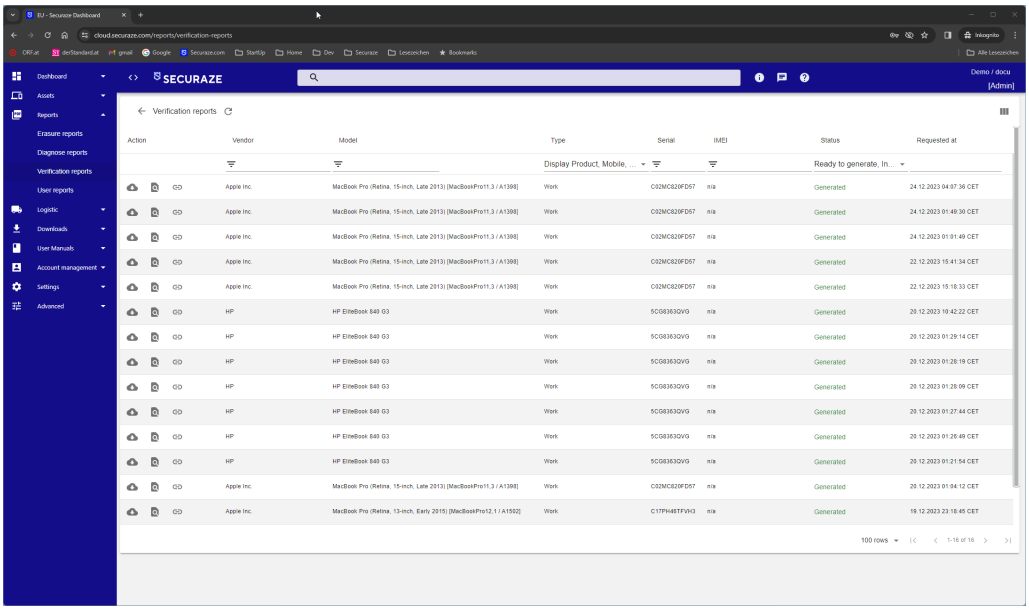


Here you can select the date of the reports you want to download. Click on **Export filtered data** and a new window will open, where you can customize the output.



Choose your desired report overview type and output mode by checking the corresponding boxes and click on **Download**.
You will get a .zip file with the report overview and all erasure reports you download folder.

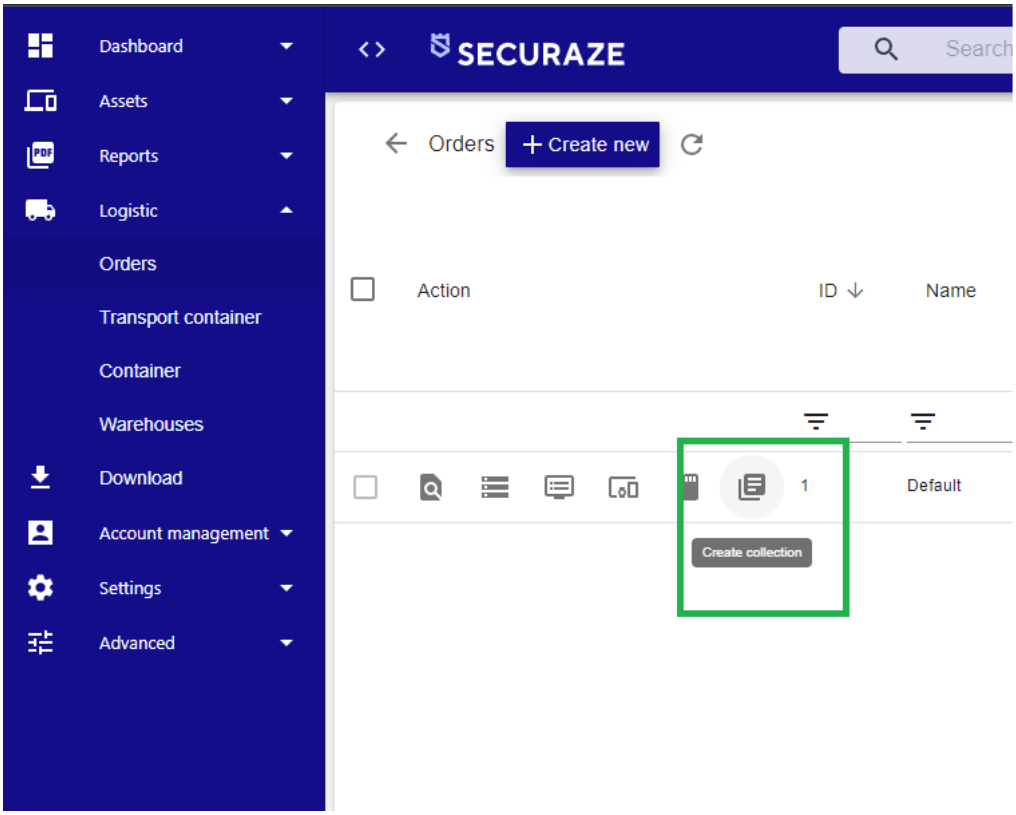
3. You can download reports in the menu **Reports** in Securaze Dashboard.



Click **Download report(s)** to download a single erasure report. The reports will be downloaded to your download folder.

4. You can download reports based on the Order they belong to. In the left sidebar menu, click on **Logistics**, and then on **Orders**.

Find the order for which you wish to generate reports, and click on the button **Create Collection.**



A download of .zip file with single PDF erasure reports, aggregated PDF reports and .xlsx file will commence.

6.2 Upload erasure report

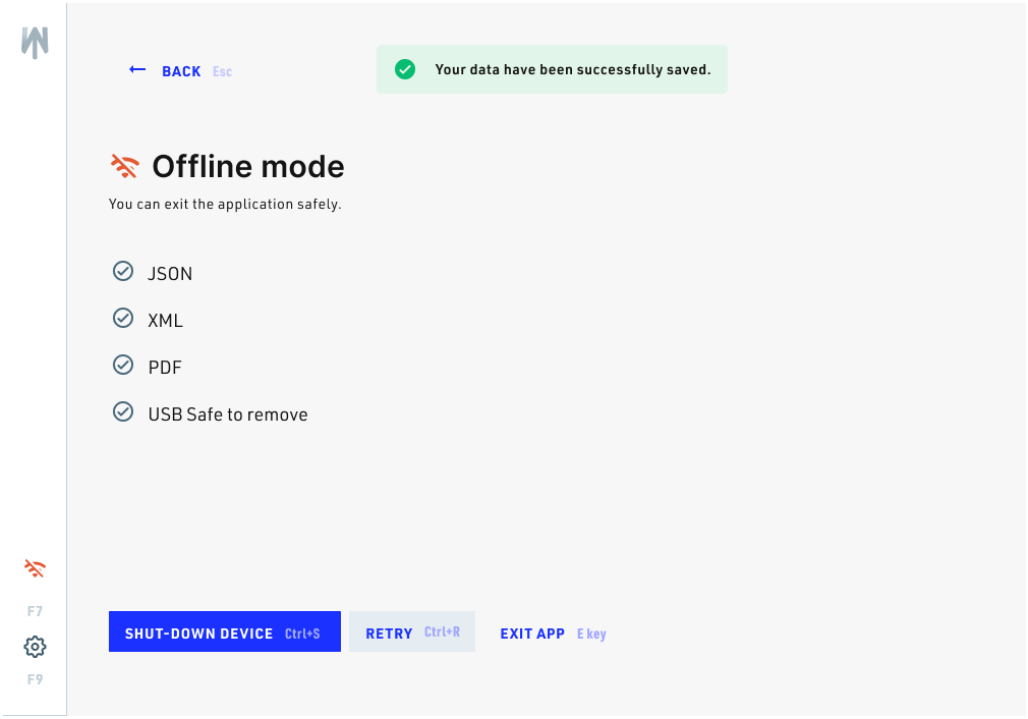
In case you performed an offline erasure, you will have to manually collect the erasure report onto a USB stick, and then upload it to the Dashboard when you have internet access.

The first step is to complete the erasure in the offline mode. To do so, create the bootable USB drive with Securaze Work image on it, and add licences for offline erasure (steps are described in Burning Securaze Images 9 section.
Next, plug in the USB stick to the device you wish to erase, and power on the device. You will be asked to select your timezone and the current time. After that, you will be taken to the erasure screen.

Note: Diagnose is not available in the offline mode.

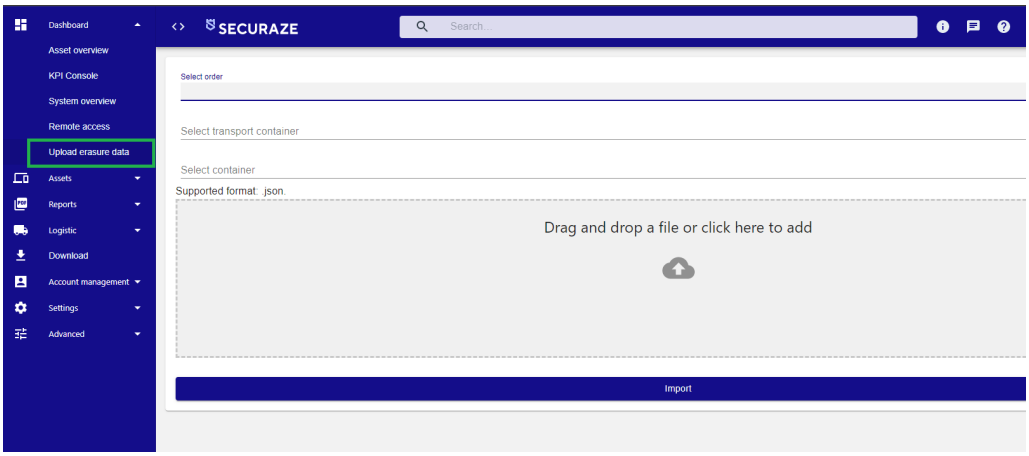
You can now select the drives you want to erase and click on START ERASURE.
A message notifying you that it is now safe to remove the USB stick will be shown.
After the erasure has been completed, click on Settings (F9).

Next, collect the report onto the USB stick, by plugging in the USB stick into the erased asset and clicking on RETRY (ctrl+R).
The reports are now saved onto the USB stick and you may remove the USB stick and shut down the device.

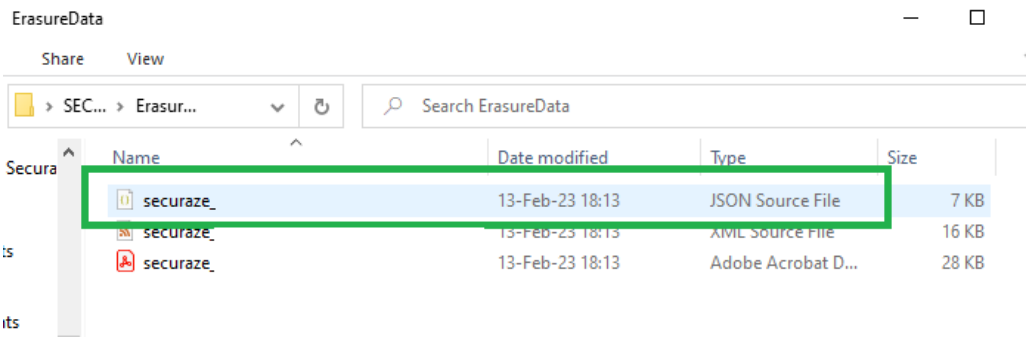


You can use the same USB stick to collect as many erasure reports as you'd like (the total amount depends on the USB storage capacity).

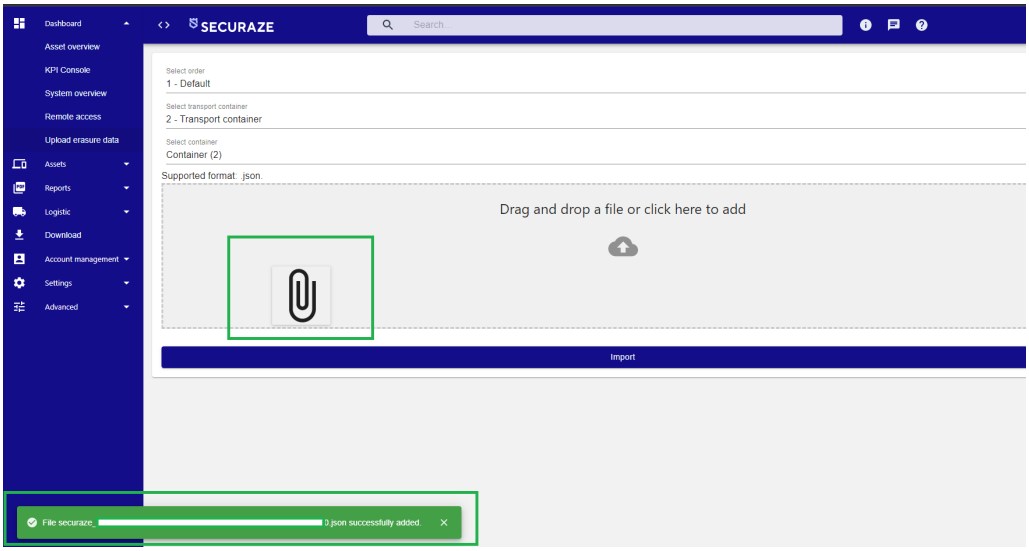
To upload these saved erasure reports, open your browser and log into the Dashboard. In the left sidebar menu click on **Dashboard**, then on **Upload erasure data**.



Here you should select Order, Transport container, and Container, to which the assets you erased in offline mode belong.
After you are done selecting this, plug in the USB stick with the erasure reports, and then open the folder **ErasureData.**
Select all the **.json** formats of the erasure reports you would like to upload.

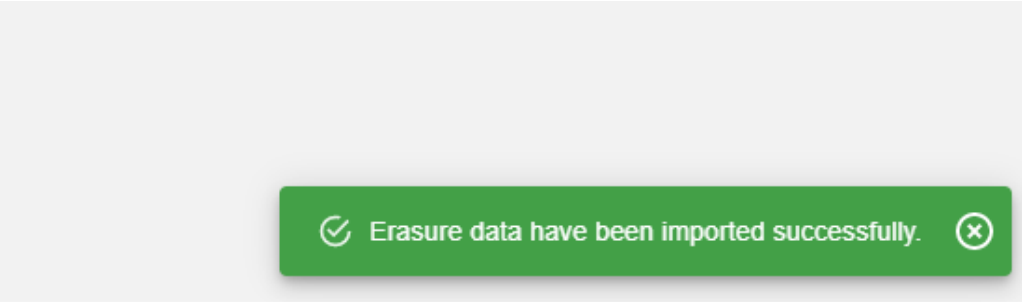


After they have been selected, drag them onto the drag & drop area.
If the file was successfully added, you will see a paperclip icon in the drag & drop area, and a message in the lower left screen area.

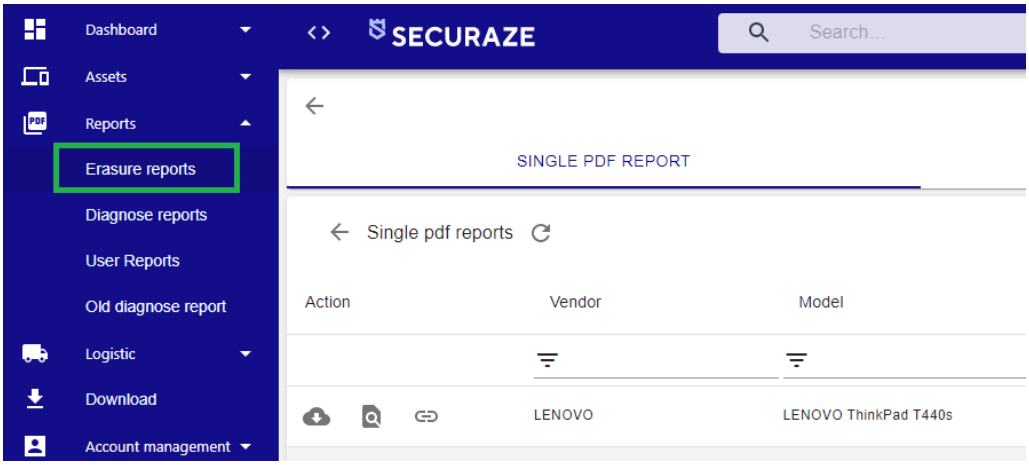


Next, click on **Import**.

After the import was successfully completed, you will see a confirmation message in the lower right corner of the screen.



To check if the reports are stored properly, go to **Dashboard**, then click on **Reports**, then on **Erasure reports** section.



FAQ

7 FAQ

7.1 Chromebook

The erasure of Intel based Chromebooks can be done with the following procedure.

Pre-Condition:
- Prepared pendrive with latest Securaze Work.

1. **Enable Developer mode**
   Turn off your ChromeBook.
   Holding Esc + Refresh (F3) buttons while pressing Power button. Then release Power Button.
   Your screen will display Recovery screen. Here, press Ctrl+D to turn on Developer mode. Then wait for couple of minutes.

2. **Setup Wifi / Internet connection**
   In the Setup-Screen of the Chromebook choose a Wifi connection or establish a cabled internet connection

3. **Install legacy firmware to enable USB-boot**
   Press CTRL+F3 to open terminal and login with user ChromeOS
   To download and run this script under ChromeOS, from a terminal/shell type:
   cd; curl -LO mrchromebox.tech/firmware-util.sh
   sudo install -Dt /usr/local/bin -m 755 firmware-util.sh
   sudo firmware-util.sh
   and press enter. (copy/paste these to avoid typos)

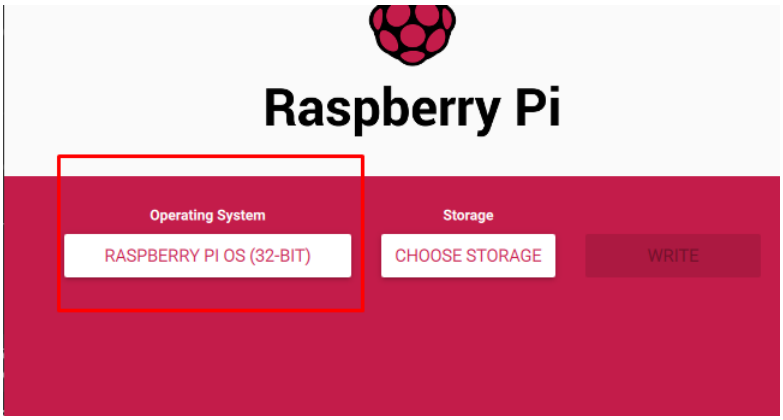
4. **Reboot the device and start it from prepared pendrive with Securaze Work**
   Start or reboot the device
   Plugin the prepared pendrive with Securaze Work
   Press CTRL+L on first screen
   Press ESC to enter boot drive selection
   Choose the pendrive from the shown list

5. **Securaze Work starting**
   After Securaze Work started successfully it can be used.

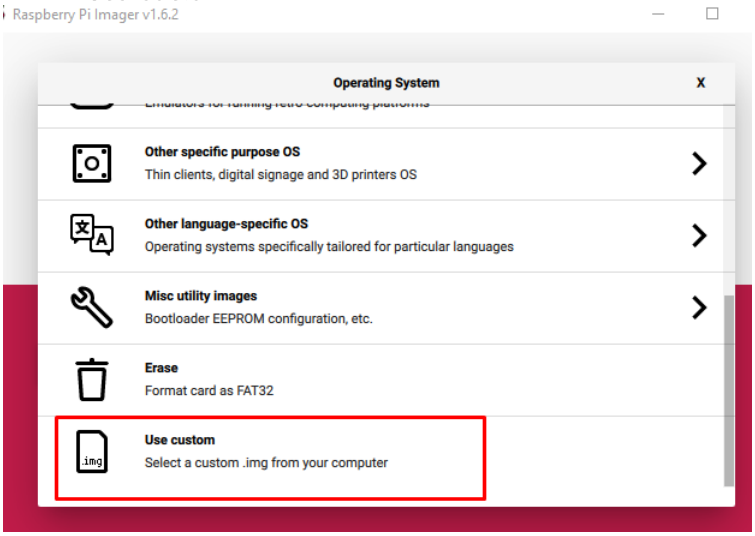
Chromebook erasure with Raspberry Pi (RPi) image

Download official RPi imager from Raspberry Download page.
Windows:
https://downloads.raspberrypi.org/imager/imager_latest.exe
macOS:
https://downloads.raspberrypi.org/imager/imager_latest.dmg

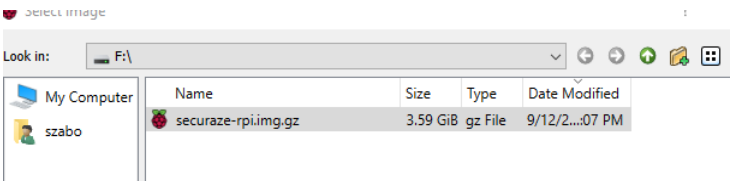
Use the downloaded Raspberry Pi imager (RPi imager) to generate the SD card.
Click on **Operating System**.



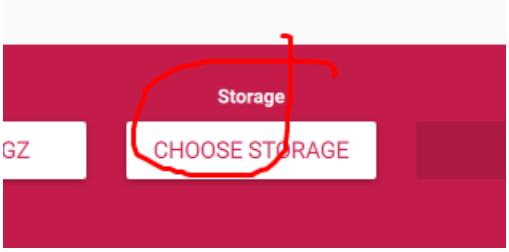
Select **Use custom**



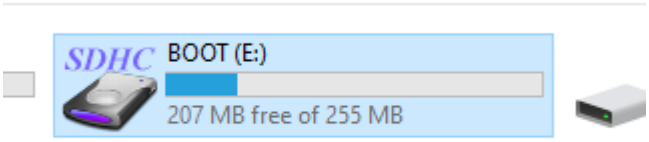
Select the Custom Securaze RPi image.



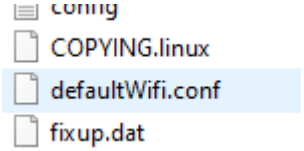
After the previous process is finished, press **Choose storage**, which opens a new explorer window, where you can select the boot partition on the SD card.



There you will find the boot partition.

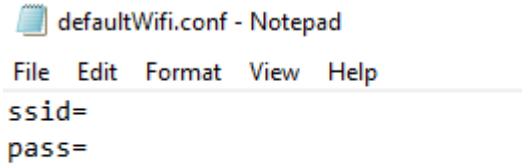


Find "defaultWifi.conf" on the SD card.



Edit the Wi-Fi settings with Notepad or any other similar Text-Editor. (not Word or any other full grown Word-Processor)

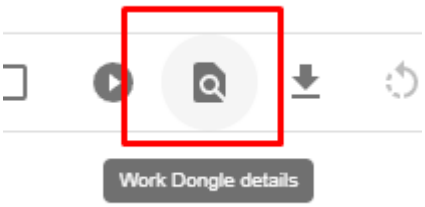
Enter the Wi-Fi SSID and password after the equal signs.



After that place the SD Card in the RPi and boot it.
Please ensure that the Securaze "Network Zone" is configured in Securaze Dashboard correctly (for more information see chapter Network Zone 230) .

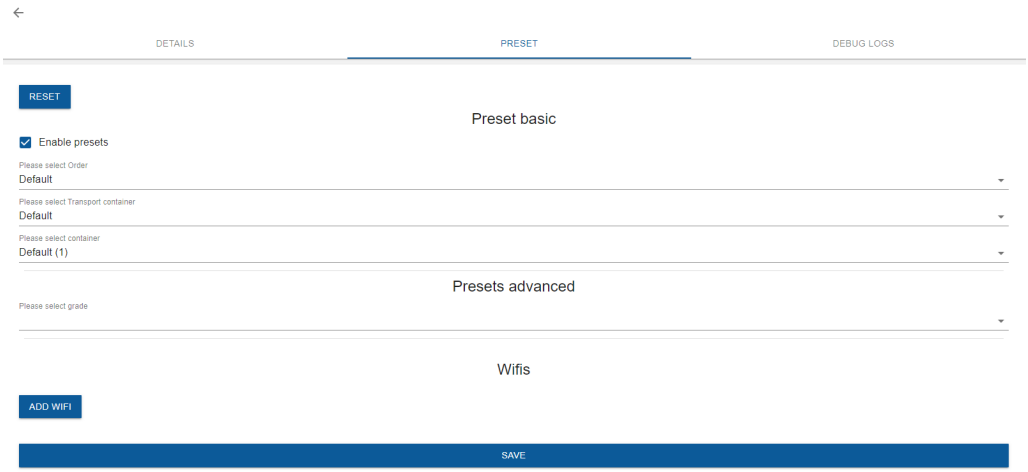
Then select **Settings - Installed Software - Work Dongle** in Securaze Dashboard

Rename the Work Dongle to a meaningful name, so it can be differentiated later during operations.



Change the Name of the Work Dongle

Select the containers you want to use for the erasure in the Customer presets.



Update the presets with your settings, connect Chromebook with root console, then hit **Erase**.

You can optimize to start the erasure process with a Scanner - find the QR Codes in the Appendix.

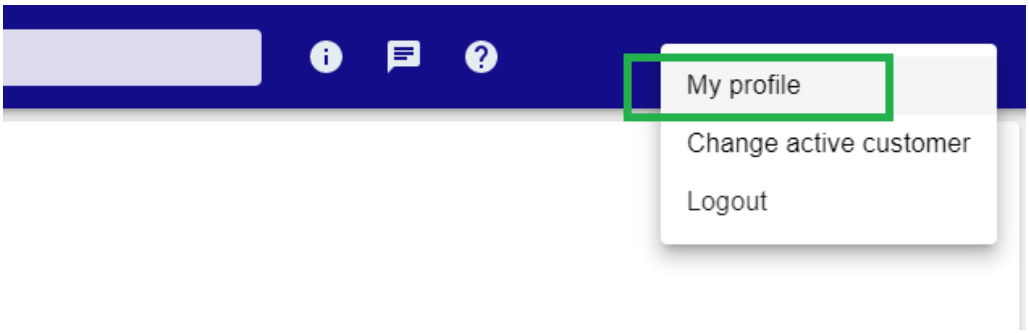
Before Starting the erasure process, please ensure that the Chromebook is in the Developer Mode & in a Root Shell Terminal.

- Power on device and hold the ‘Escape + Refresh Key’
  - Once at the OS Verification page, press ‘Ctrl + d’ to boot into developer mode
- Press ‘Enter’
- Wait until another OS verification page pops up and then press ‘Ctrl + d’ again
- Now wait until the developer OS is booted in
- Once in, press ‘Ctrl+Alt+F3’ to boot into the root terminal

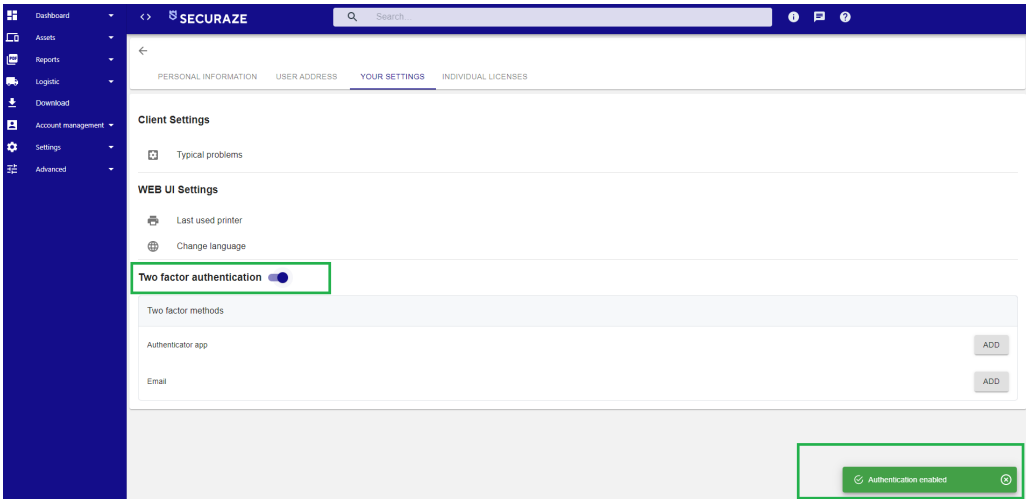
7.2 Two-Factor Authentication (2FA)

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**.

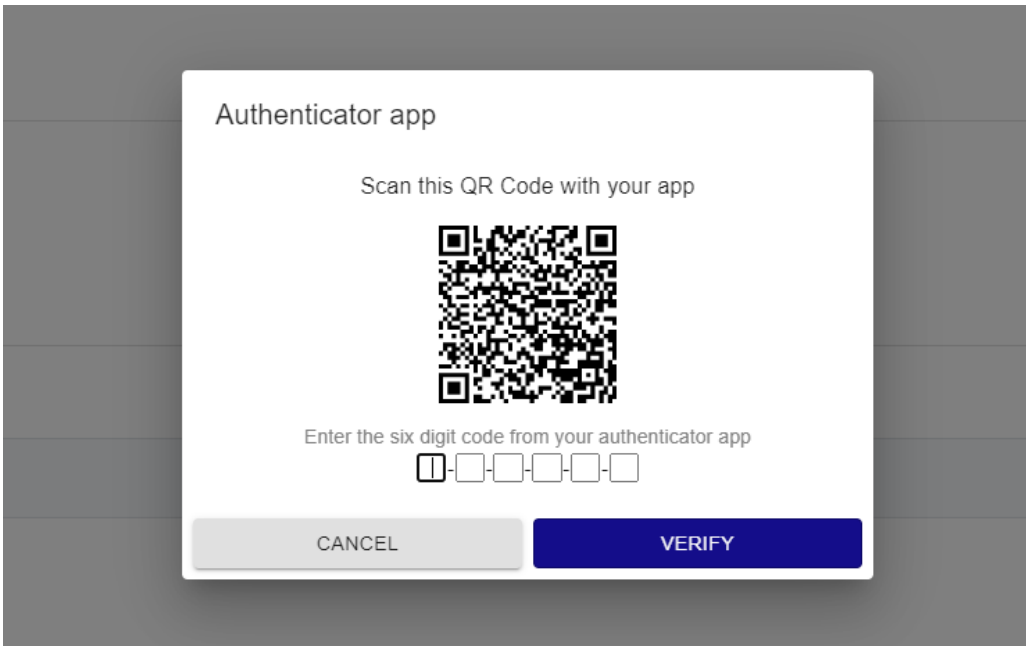


In the My profile section, select tab "**YOUR SETTINGS**". In this tab, you will see the option "**Two factor authentication**" and a toggle button on the right.
Click on the toggle button, and a menu for selecting the authentication method appears.



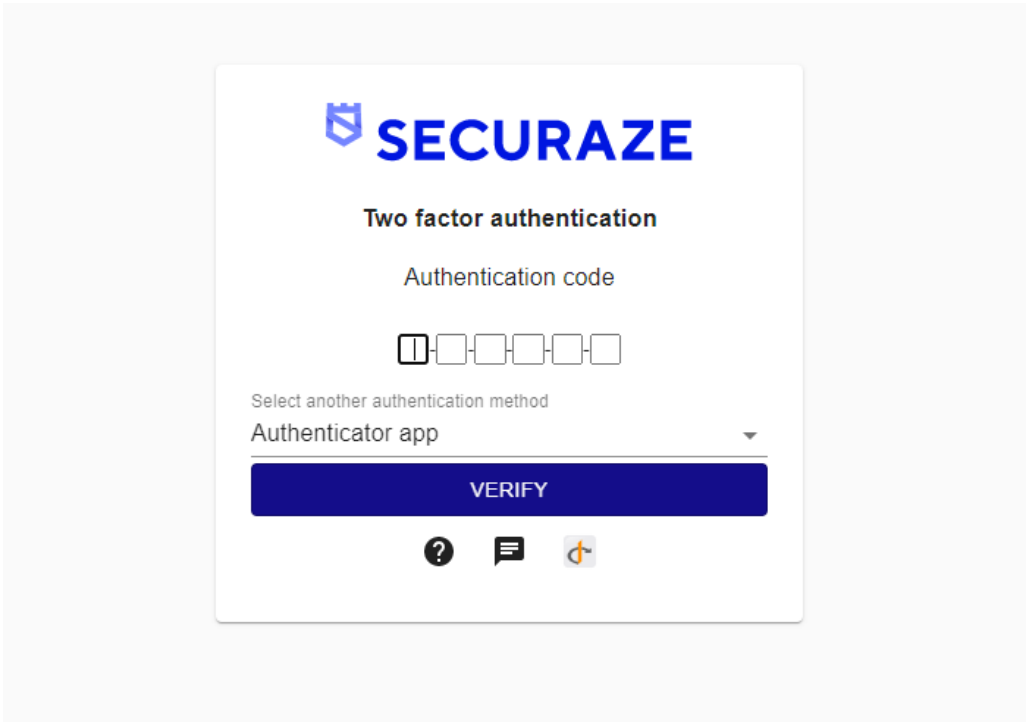
For Authenticator app method, we suggest using Google Authenticator, found in both App Store and Google Play, or Microsoft Authenticator, also found in both App Store and Google Play.

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.

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.

7.3 Screen Mirroring

In case you wish to erase a notebook / laptop with broken screen, Securaze Work has integrated screen mirroring option, available immediately upon booting.
Connect your external display (screen) to you device, and then press CTRL + F7.

After that, you should be able to continue with your erasure process.

Release notes

8 Release notes

The current release notes can be found at:

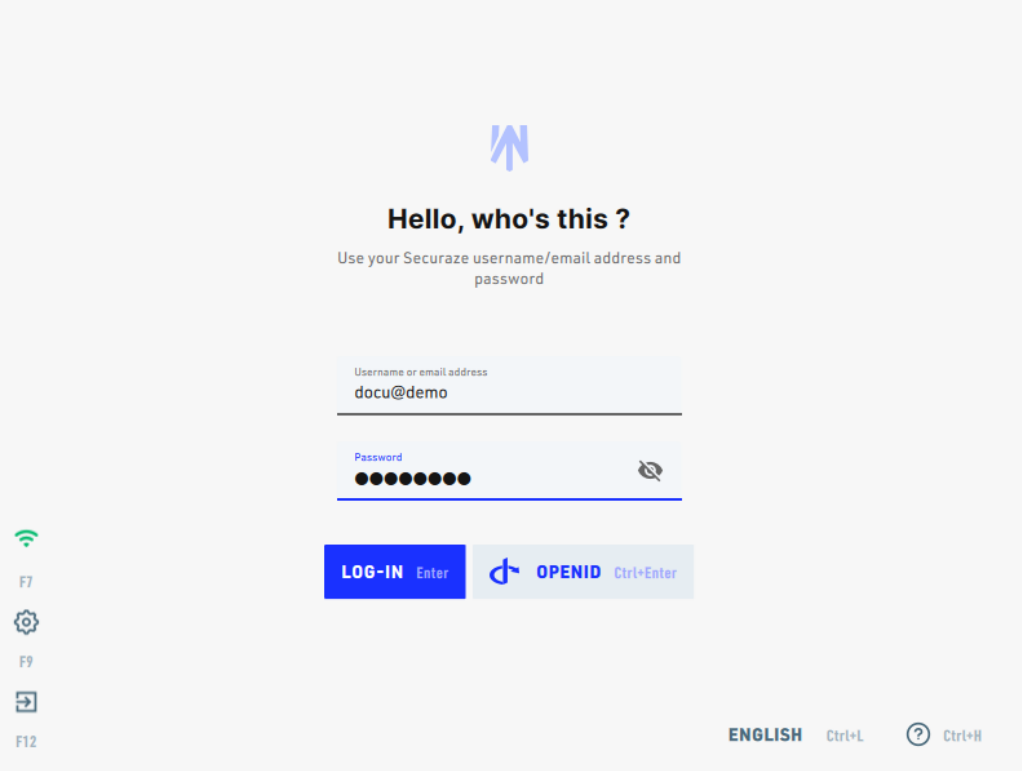
Securaze Work Release Notes

Menu items

9 Menu items

9.1 Overview

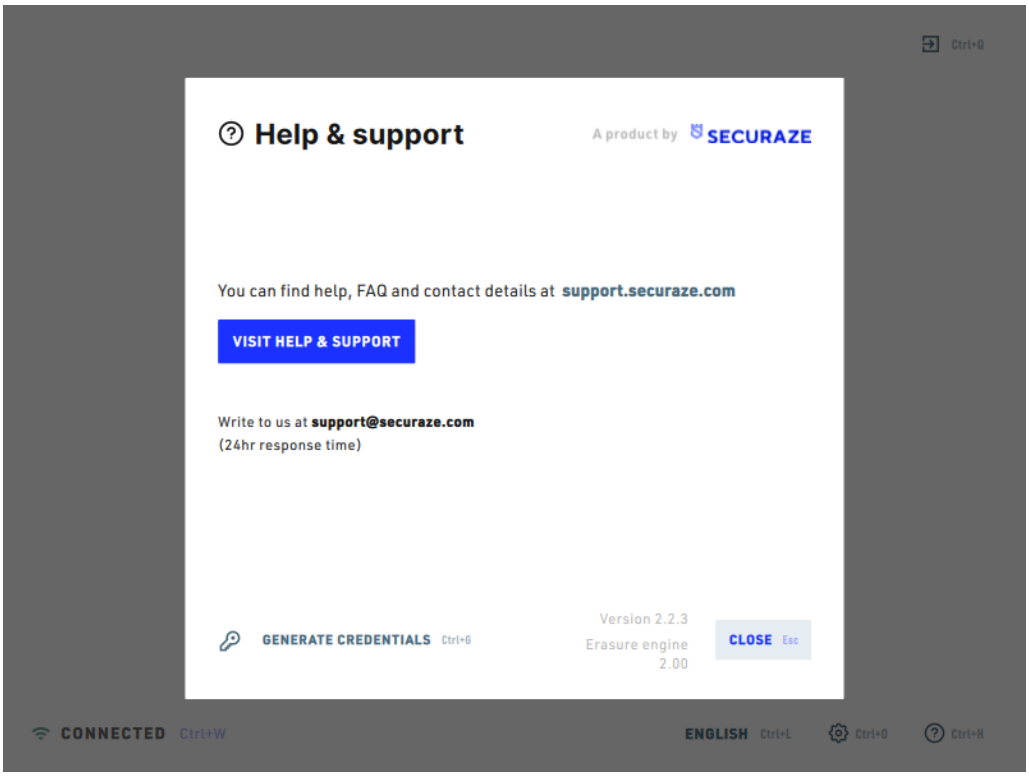
After starting Securaze, you will be taken to the login screen



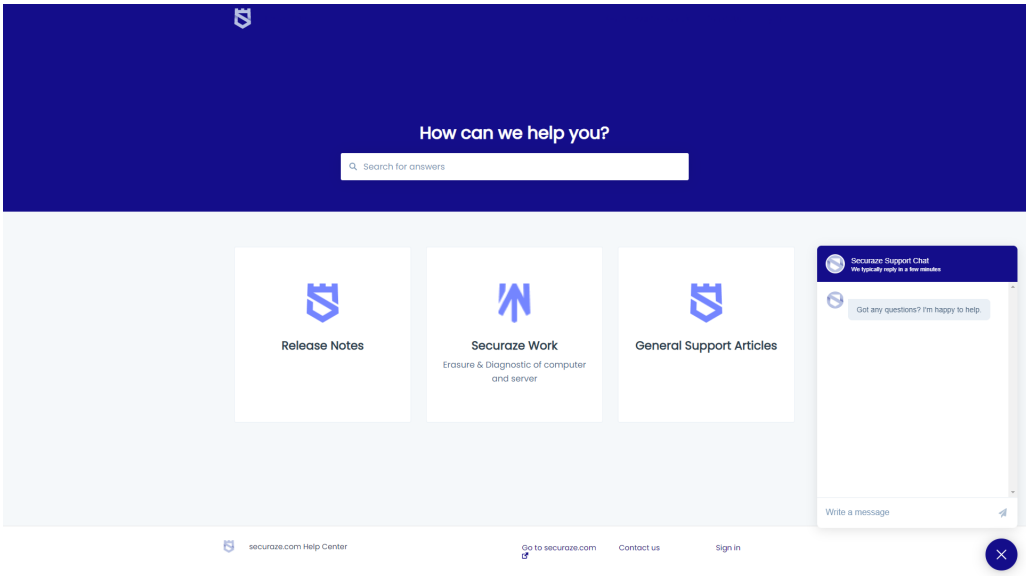
On the bottom left you will see the connection state, either "Connected" or "Disconnected".

In the lower right area the following items are available for selection:
ENGLISH (Ctrl+L) - allows you to change the client language
OPTIONS (Ctrl+O) - allows you to change options within the Work client

HELP+SUPPORT (Ctrl+H) - starts the Help & Support dialog



You can visit the **Securaze Help & Support online Portal** which allows you to create tickets, start support chat and search the knowledge base.



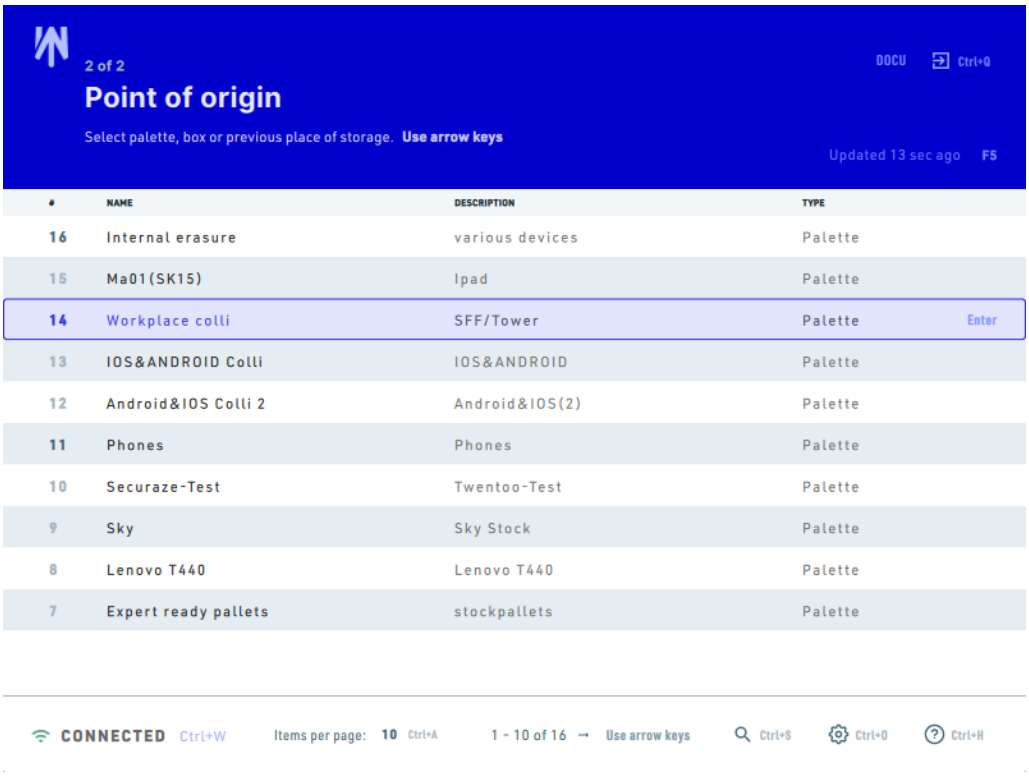
Generate Credentials for Remote Support
You can create manually credentials for remote support, these are automatically transferred to Securaze Dashboard and can communicated also to the Securaze Support team..

Working Offline

If no connection to the server can be established on startup a Ofline QR-Code for usage with Securaze Motion is shown.
Also connecting with a Wifi is possible instead of using a cabled network connection.
Find details regarding working Offline in the chapter Work Offline 142.

After logging in, you will be taken to the Securaze Work start screen where the current input palettes are displayed.

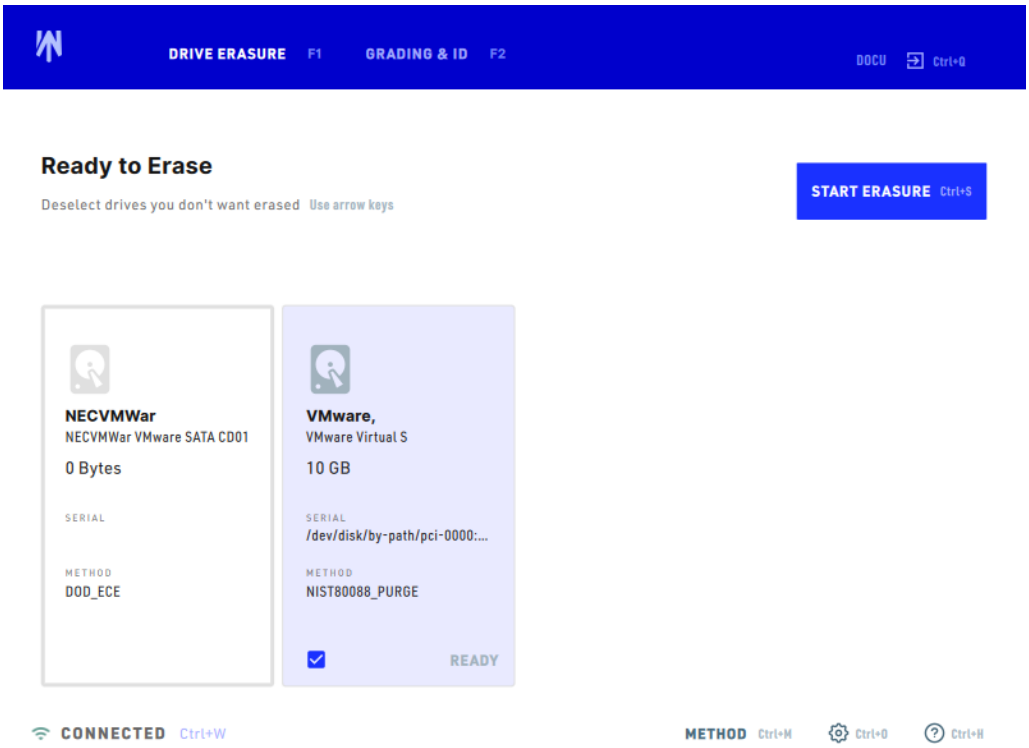
After selecting an input pallet by pressing ENTER, the storage pallets are displayed.



9.2 Drive Erasure [F1]

In the Drive Erasure section you will see an overview of all hard disks available for erasure.

The optimal deletion method is automatically stored with the respective hard drives. For each hard disk, you can also manually specify the deletion method and the verification to be carried out.



First select the erasure method and then the verification level.
To change the erasure method, click on the **METHOD (Ctrl+M)**.

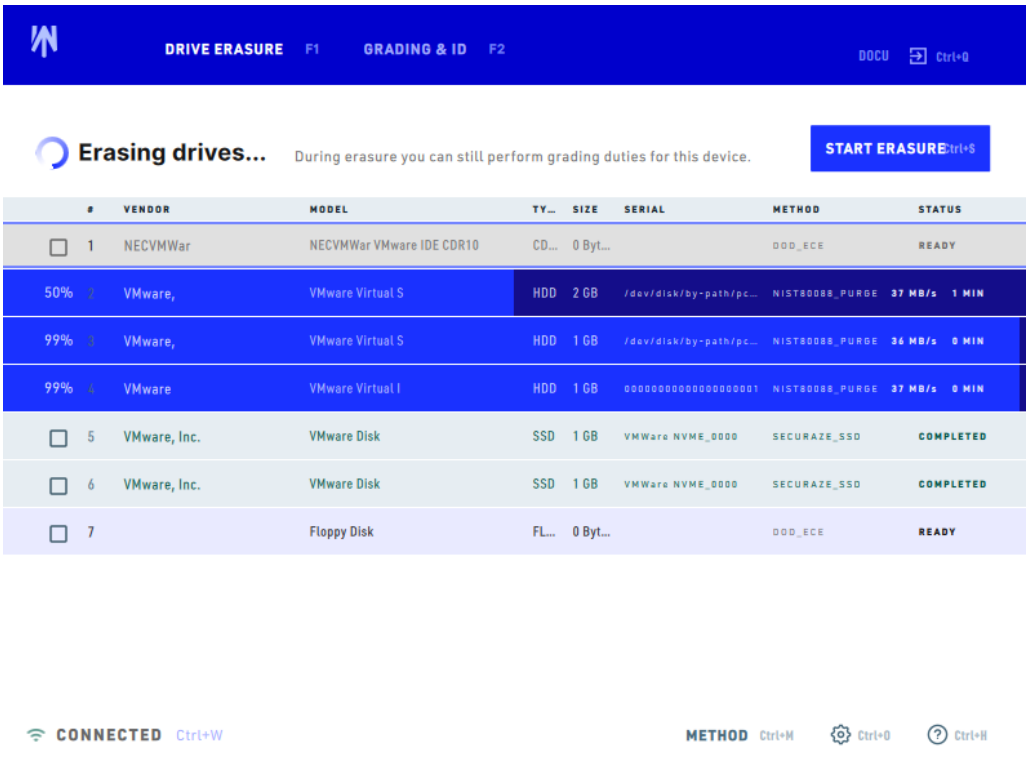
You can find information on the currently supported erasure methods under Erasure Methods 237.

The following options are available for the levels of verification:
Minimum: Default setting (provides sufficient verification)
Last: only the last step is verified
All: every step is verified
Custom: offers an individual setting of the verification level

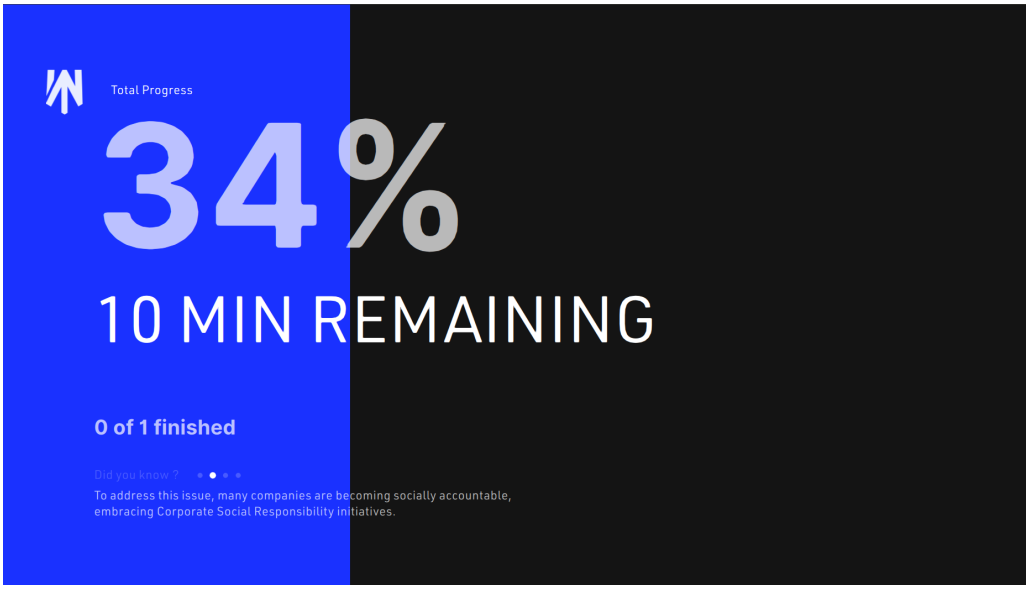
The selection of the verification level affects the duration of the deletion process.

The selected settings can be applied to the hard drives:
ALL: on all hard disks
SELECTED: on the selected hard disks
HDD: only on HDD hard drives
SSD: only on SSD hard drives

You can monitor the progress at any time during the erasure process.



After some minutes the Securaze Work Screensaver appears and shows information about the overall state.

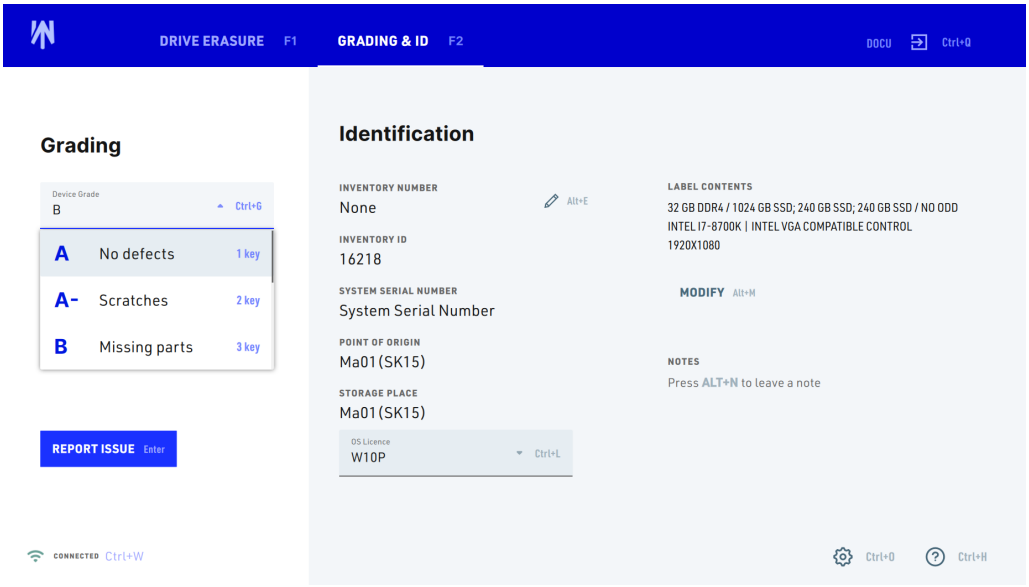


At the end of the erasure you will receive a erasure report in Securaze Dashboard regardless of whether the erasure was successful or failed.

You can find information on erasure reports under Reports - Download erasure report 152

9.3 Grading & ID [F2]

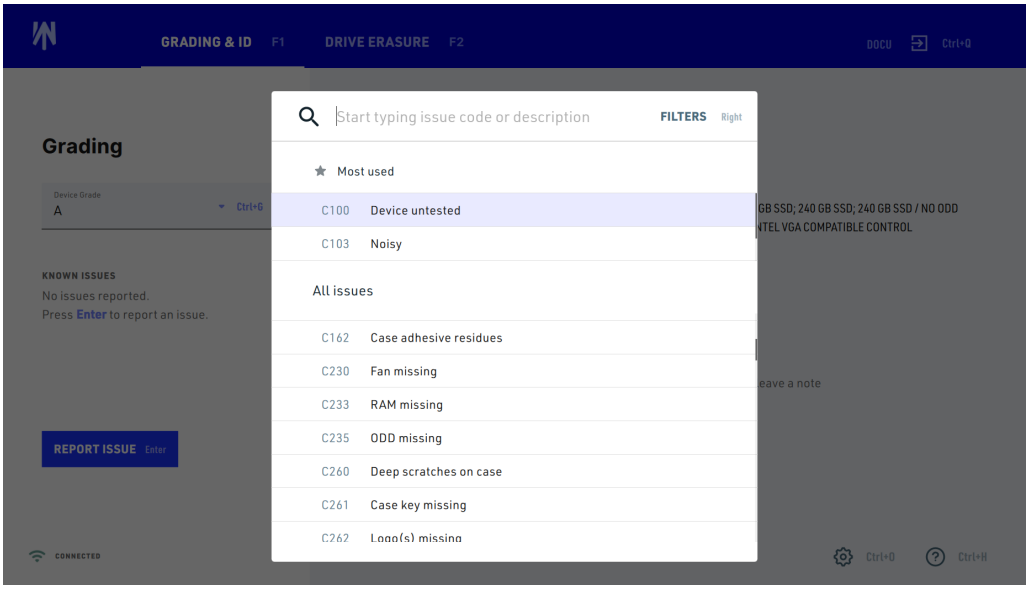
In the **Grading** area on the left side you can set the Device Grade and report known issues of the device.



By Pressing Device Grade (Ctrl+G) the overall device grade can be choosen.
The following assessments of the overall condition are available for this purpose:

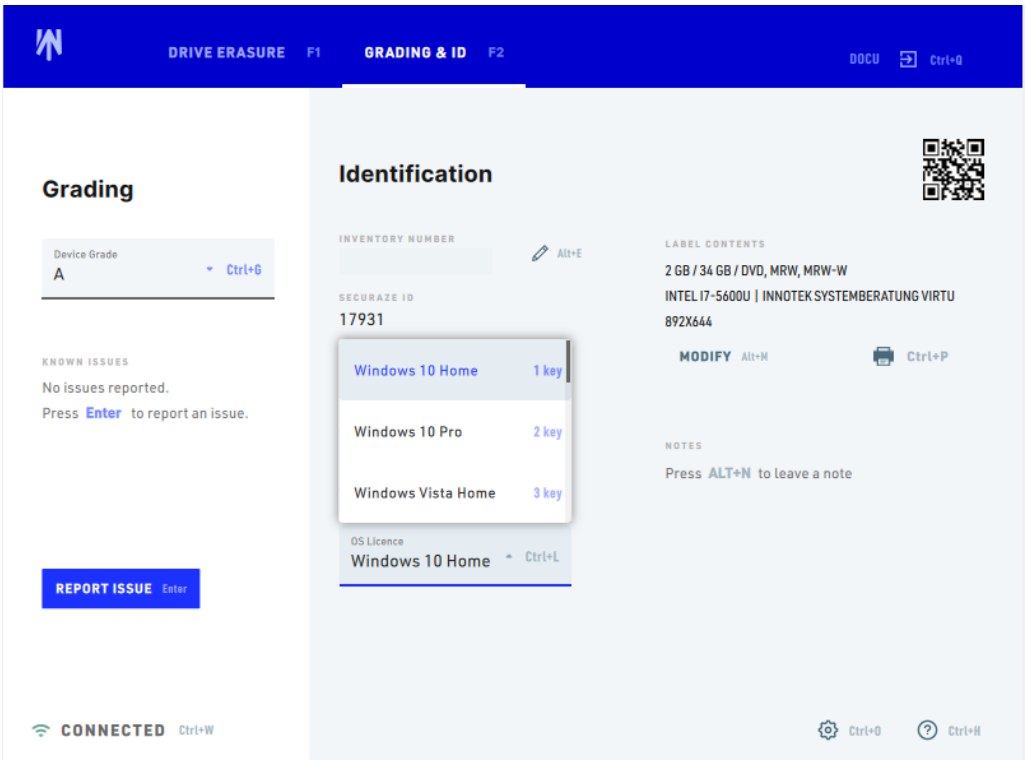
- U (Untested)
- C-/D
- C
- B-
- B
- A-
- A

By Pressing Enter **Issues** can be reported.
Issues can be filtered either by entering the issue short code or the description, and it's assigned by pressing ENTER.



In the **Identification** area on the right side you can set Device Grade, Inventory number, add a Note etc.

By pressing **Inventory Number (ALT+E**) a optional existing inventory number of the device can be entered or scanned.
Under **OS License (Ctrl+L)** you can choose any existing operating system license



By pressing **Modify (ALT+M**) the label comments for label printing can be edited.
By pressing **NOTES (ALT+N**) additional notes for the device can be entered.

Securaze Dashboard

10 Securaze Dashboard

After logging in to Securaze Dashboard you will be taken to the overview

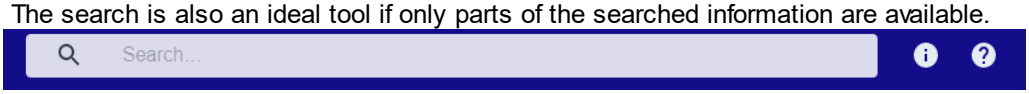
The following tabs are available in the dashboard

1. Dashboard - 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

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:

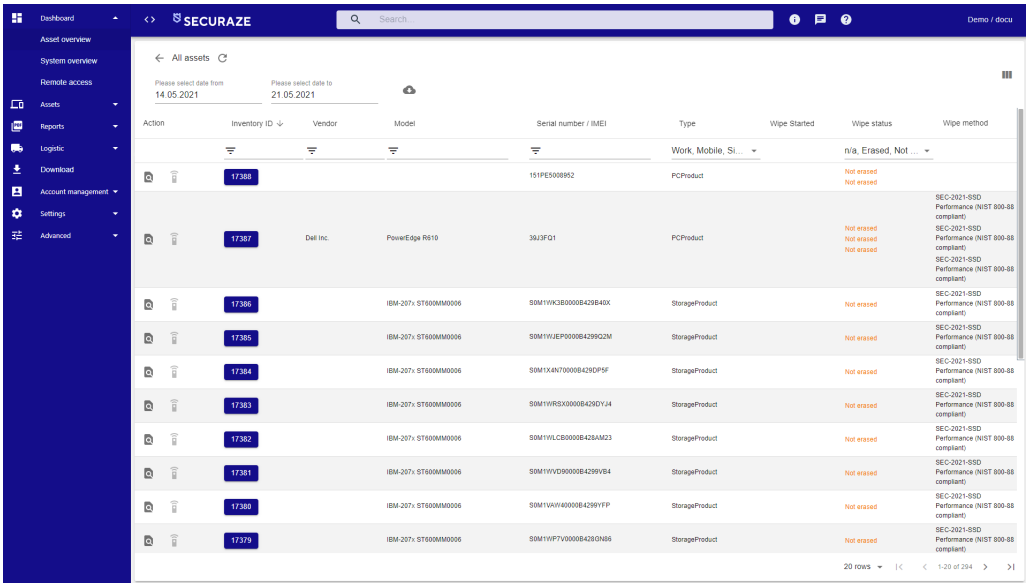
To search for several parameters simultaneously, use separator " ; " e.g. => my_word; my_word2; *my_word3*.

10.1 Menu items

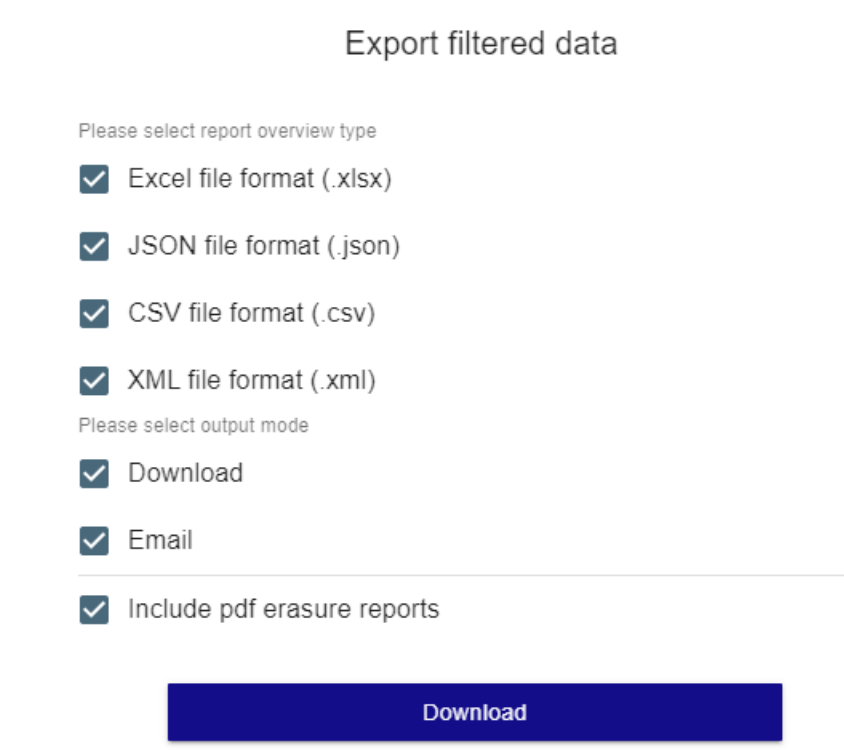
10.1.1 Dashboard

10.1.1.1 Asset overview

In the Asset Overview menu you can see an overview of all assets and select them by date.



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.

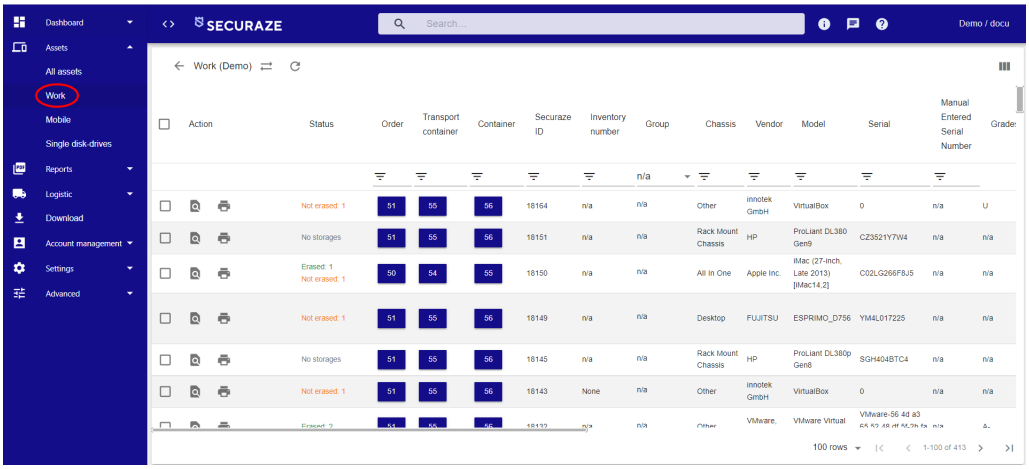
Here you can select the columns to be displayed by placing the check mark next to the corresponding column heading.
Confirm your entry by clicking SAVE.

10.1.2 Assets

In the **Assets** menu you can see all devices, divided into Work, Mobile and Single disk-drives.

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.**

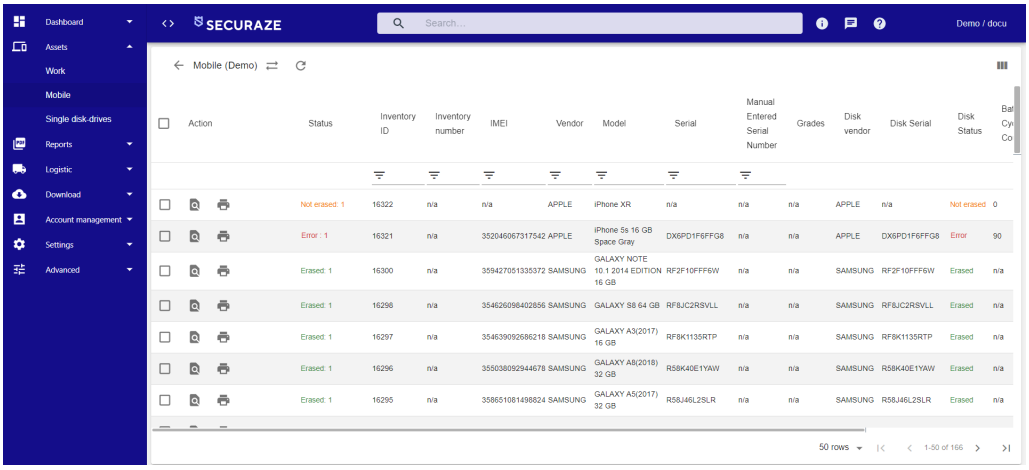
In the middle of the page you can see the Work devices with the related information.
Here you have the following options:

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

10.1.2.2 Mobile

In the **Assets - Mobile** menu you can see an overview of all Mobile 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.**

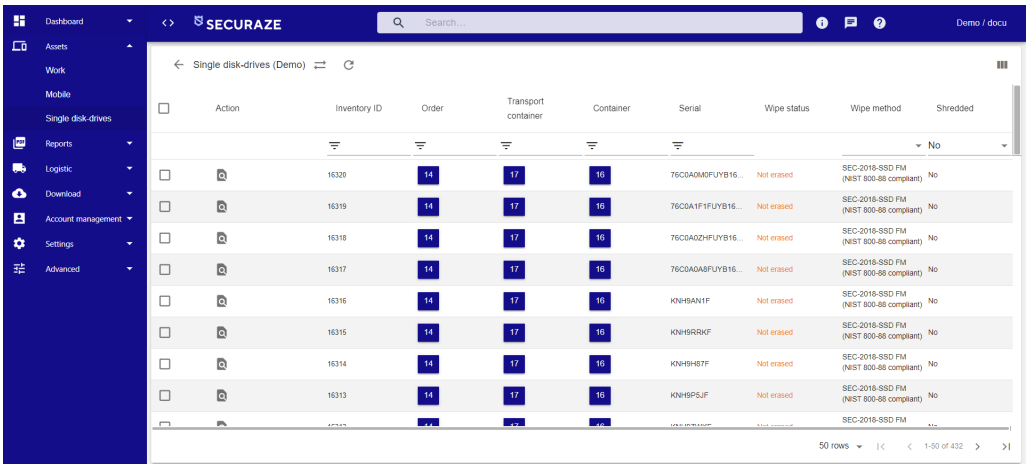
In the middle of the page you can see the Workp devices with the related information.
Here you have the following options:

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.



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.

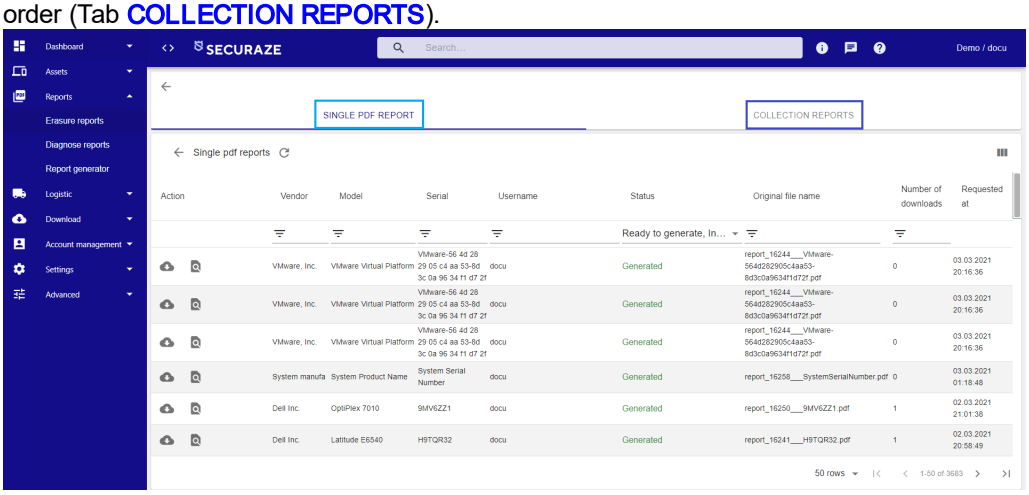
To generate a deletion report for all devices, click on **Download erasure report.**

In the middle of the page you can see the Workp devices with the related information.
Here you have the following options:

Product details

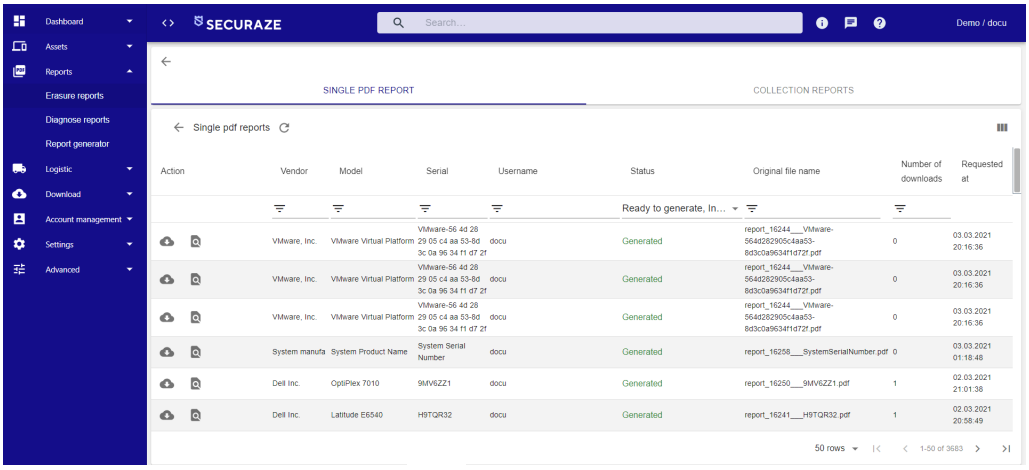
10.1.3 Reports

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.

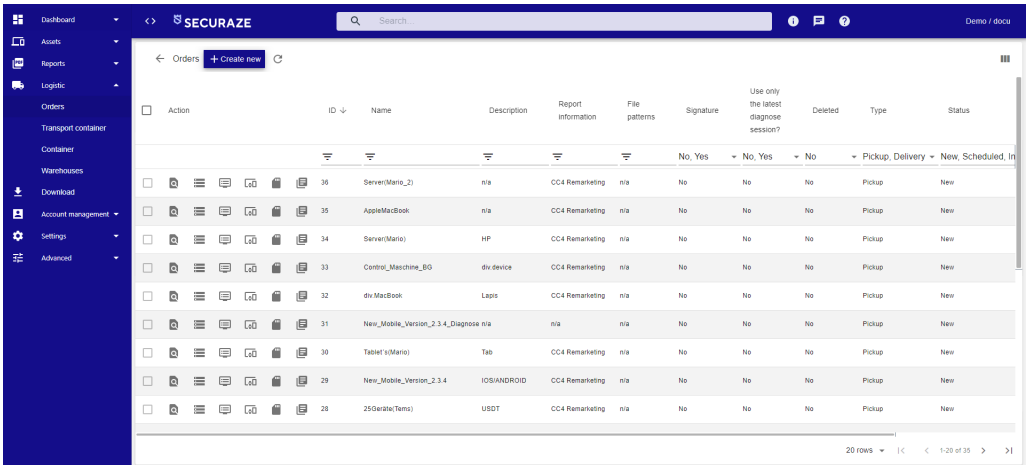


Select the desired report and click **Download report(s).** The report is downloaded in pdf format.

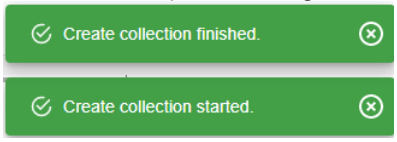
Order:

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.



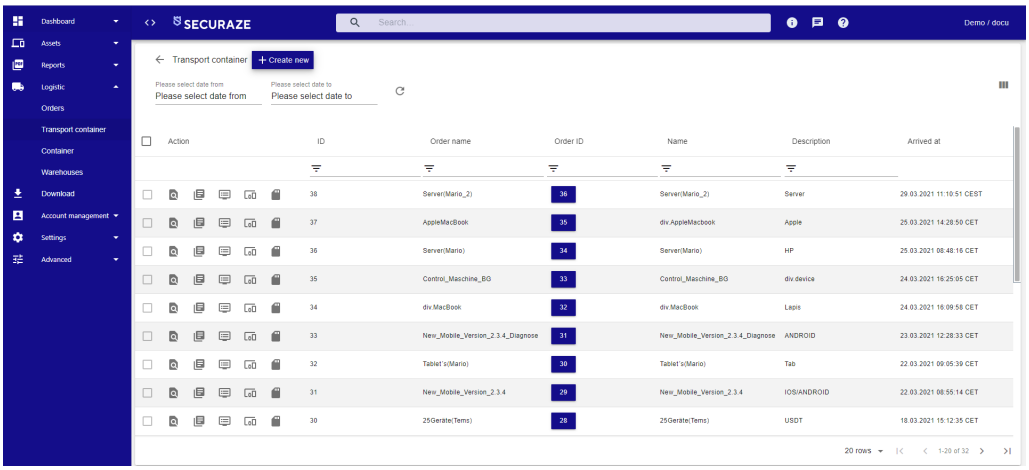
A ZIP file is downloaded containing the reports as a PDF file and a listing of assets as an XLS file. The erasure reports are displayed on **Reports - Erasure reports** in the Menu section.

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

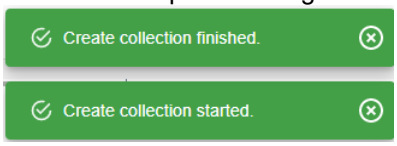
Lot:

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.**



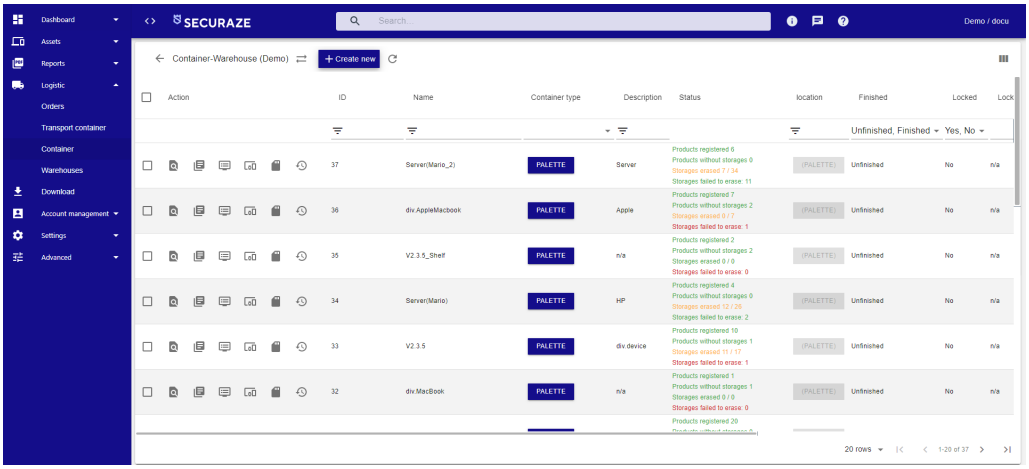
The erasure report will be generated.



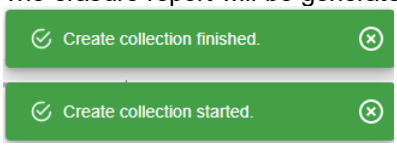
A ZIP file is downloaded containing the reports as a PDF file and a listing of assets as an XLS file. The erasure reports are displayed on **Reports - Erasure reports** in the Menu section.
In the menu **Reports - Erasure reports** you can download the reports again any time by clicking on **Download report(s)**.

Container:
To download an erasure report of all assets of one container, click on **Logistic - Container** 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.

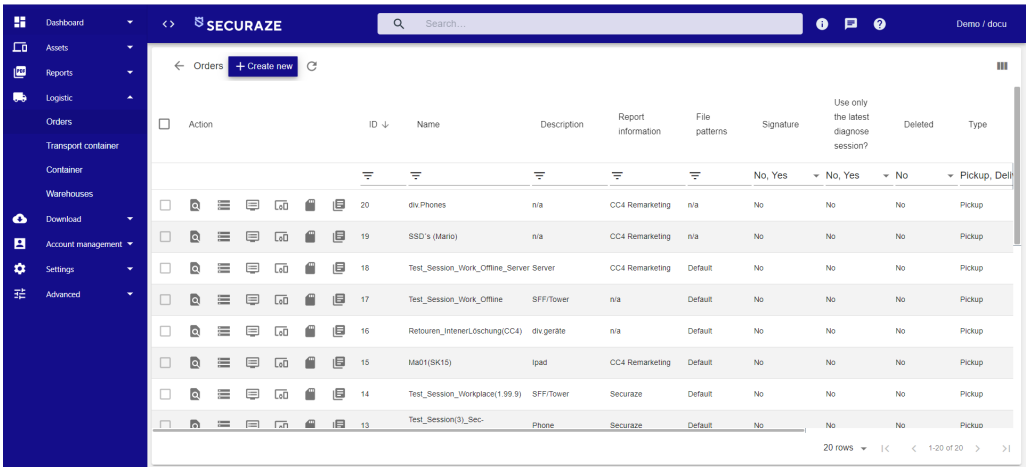
10.1.4 Logistic

In the **Logistic** menu you can create, edit or remove orders, Lots and Sale Lots.

10.1.4.1 Orders

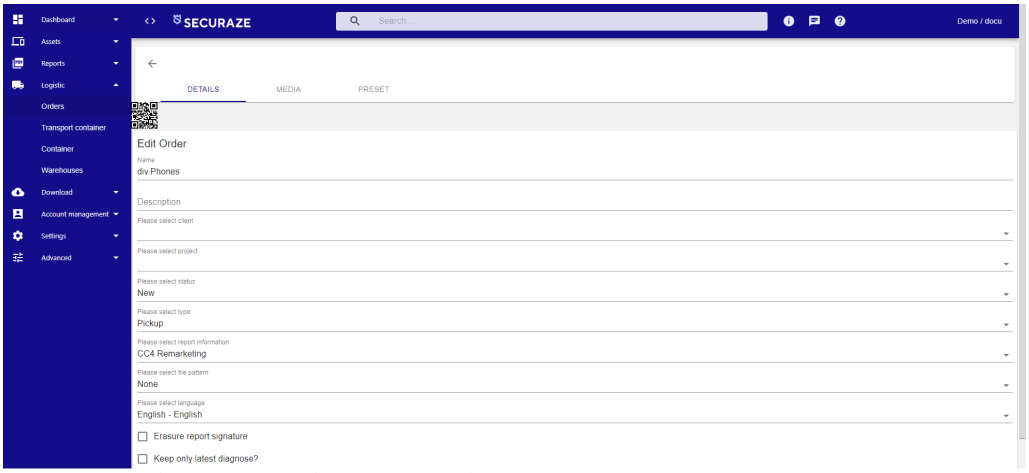
The **Orders** menu allows you to create new Order, edit existing ones and delete them.

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 palette.

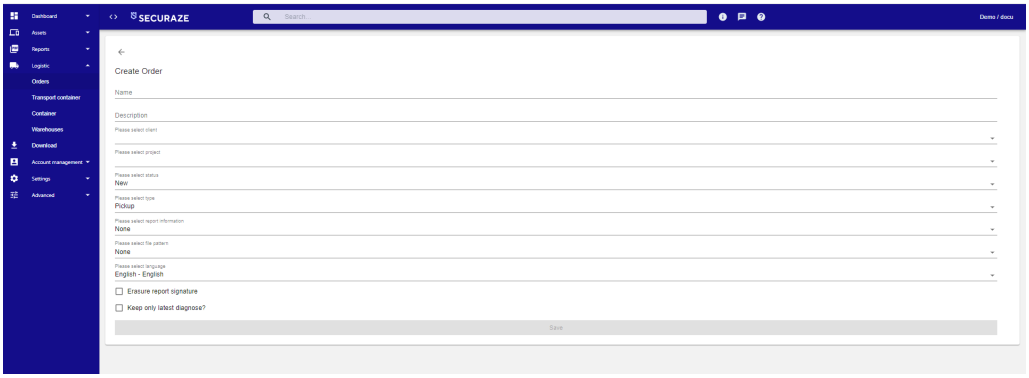
By selecting **Order Details** you can see more details for the order.



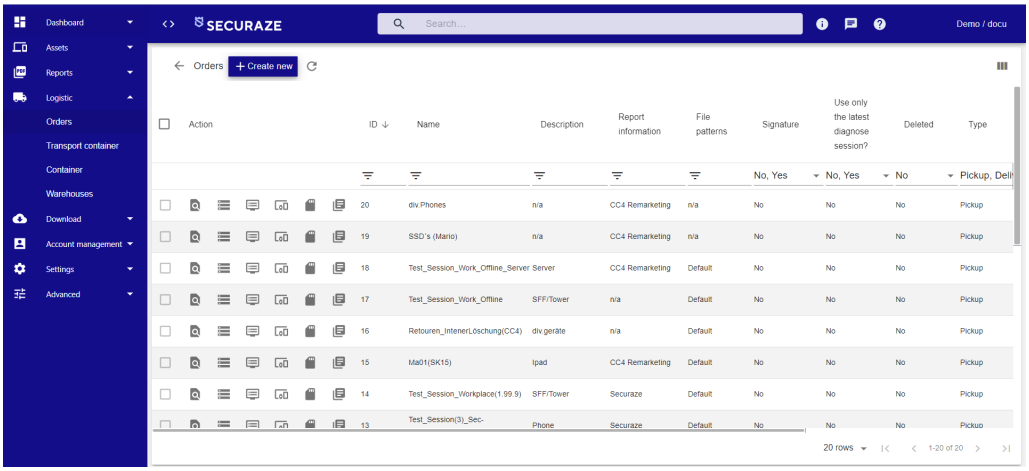
10.1.4.1.1 Create new Orders

To create a new Collection Request, click **Collection Requests** in the Menu section, then click **Create New**.

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



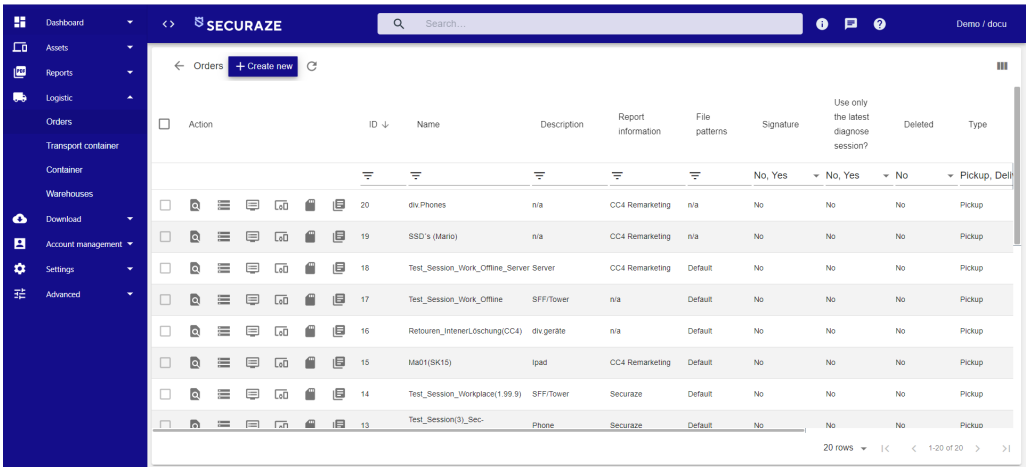
After confirming the selection by clicking **SAVE**, the newly created order is displayed in the **Order** menu.



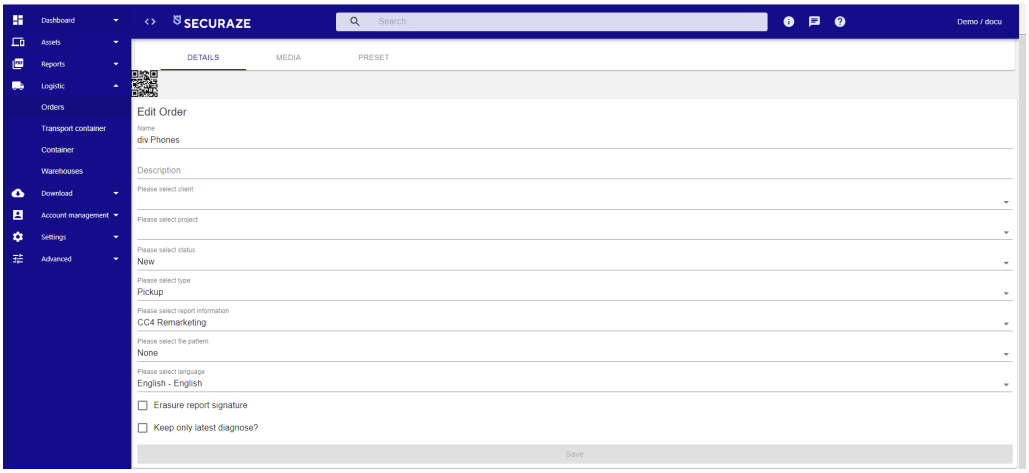
10.1.4.1.2 Edit Orders

To edit a Pickup Order, select the Pickup Order and click **Order Details**.

.



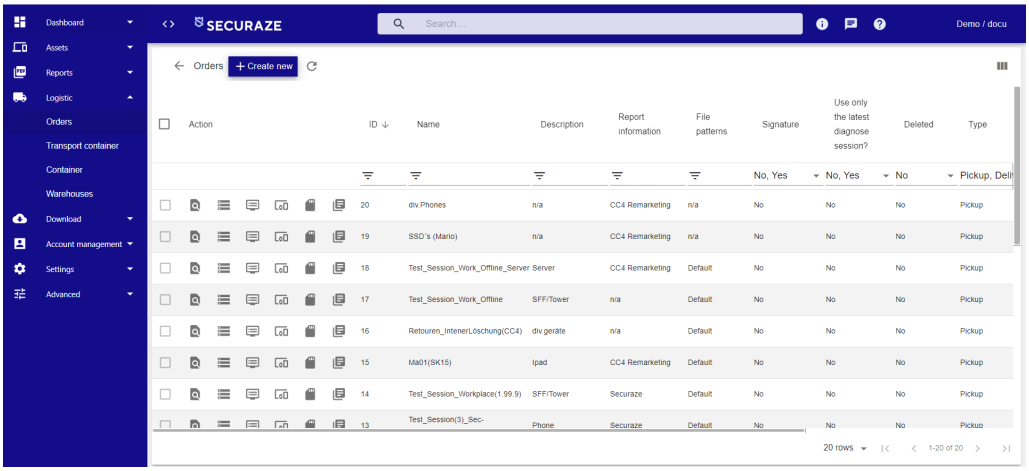
Make the desired changes and confirm them by clicking **SAVE**.



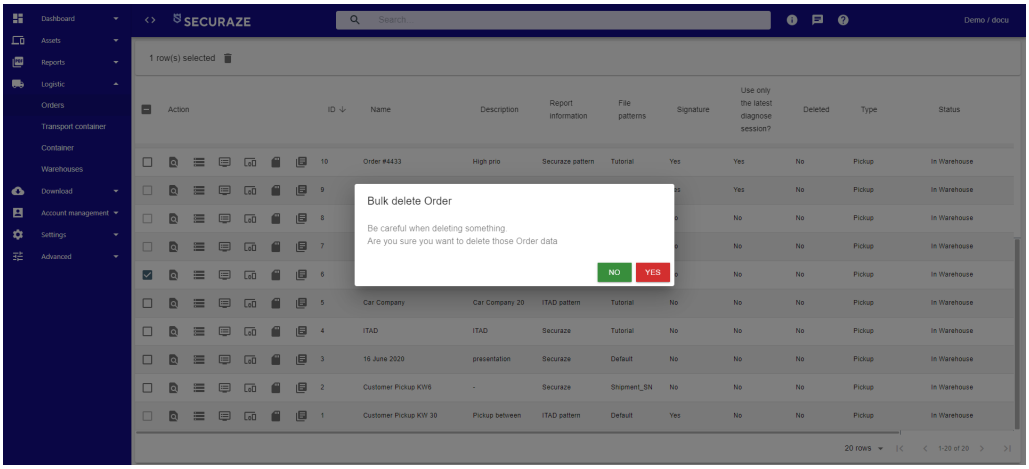
10.1.4.1.3 Delete Orders

To delete an Order, select the Order and click **Remove all selected Orders** .

.



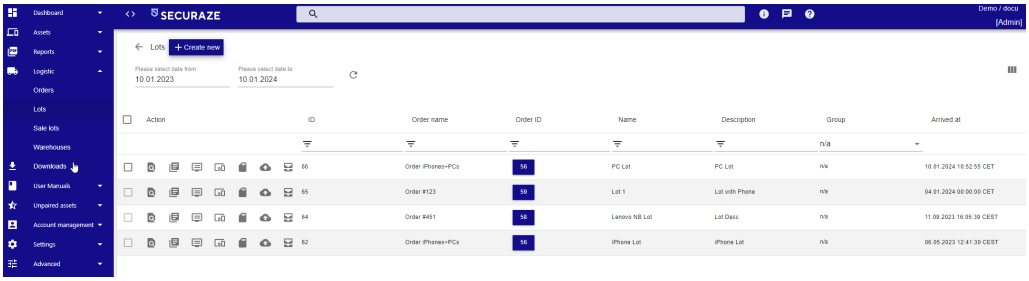
Confirm the erasure by clicking on **YES**.



10.1.4.2 Lot

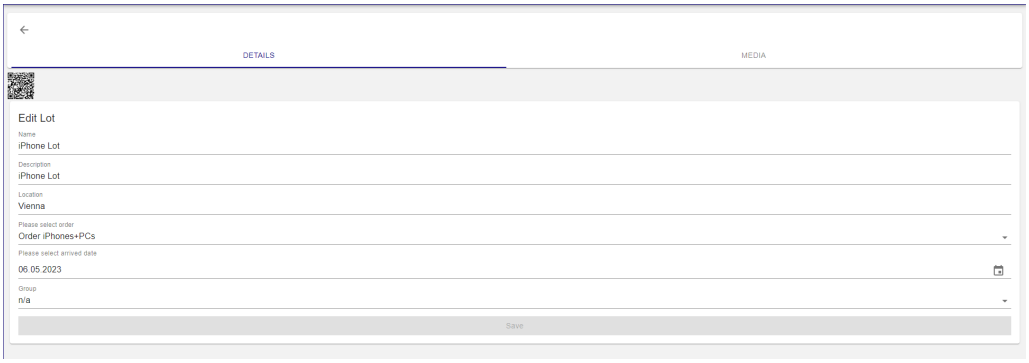
In the menu **Logistic - Lot** you can create new incoming palettes, edit and delete existing ones.

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 palette.

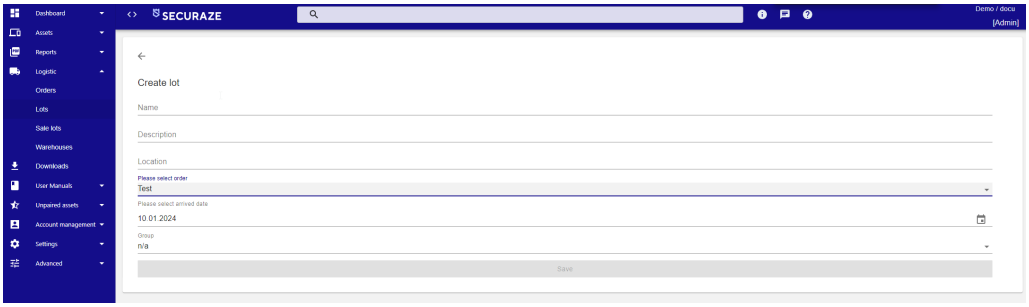
By selecting **Lot Details** you can see more details for the Lot.



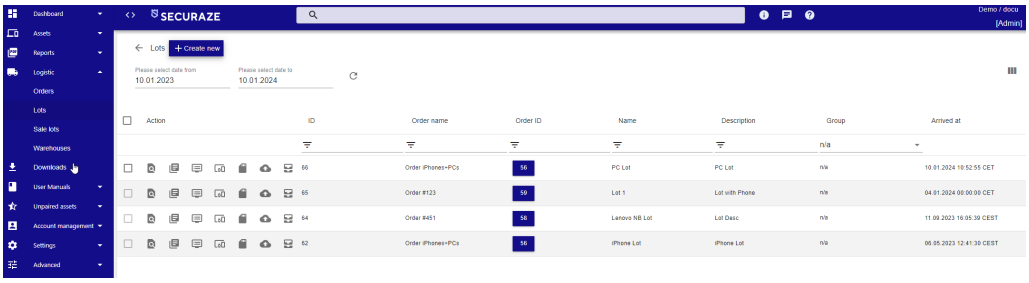
10.1.4.2.1 Create new Lot

To create a new input palette, 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.

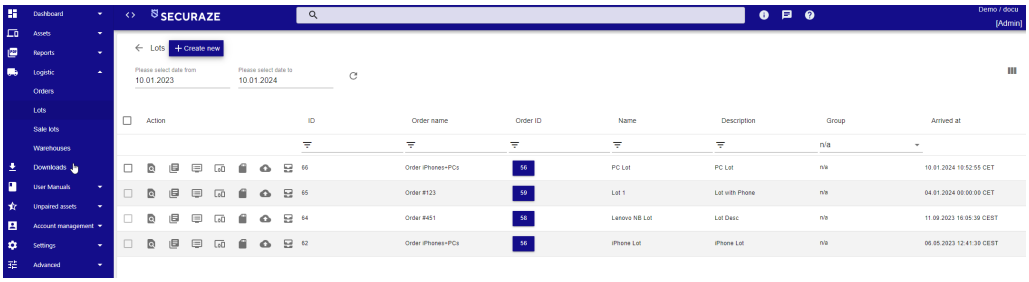


After confirming the selection by clicking **SAVE**, the newly created Lot is visible in the menu **Logistc - Lot**.

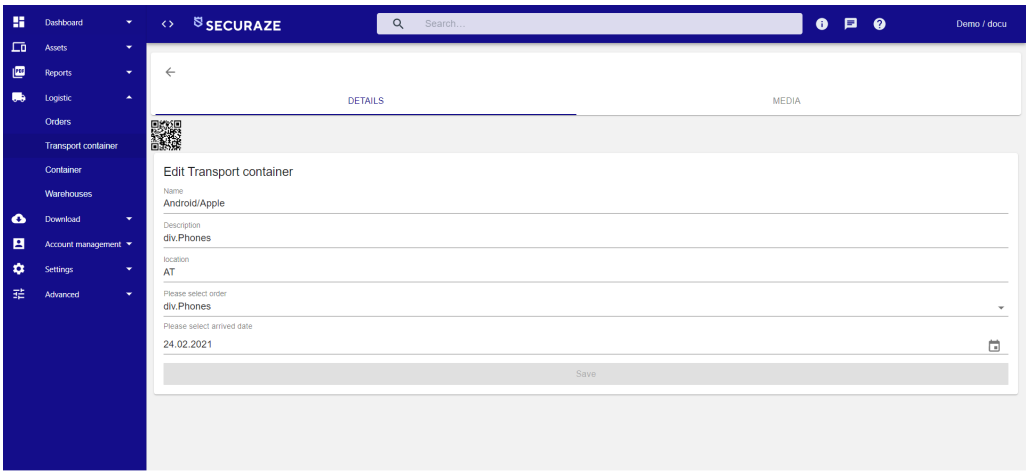


10.1.4.2.2 Edit Lot

To edit an incoming pallet, select the relevant Lot and click **Lot Details**.

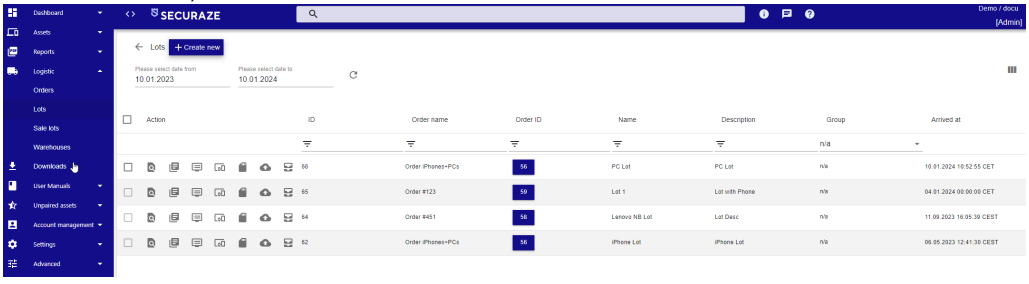


Make the desired changes and confirm them by clicking **SAVE**.

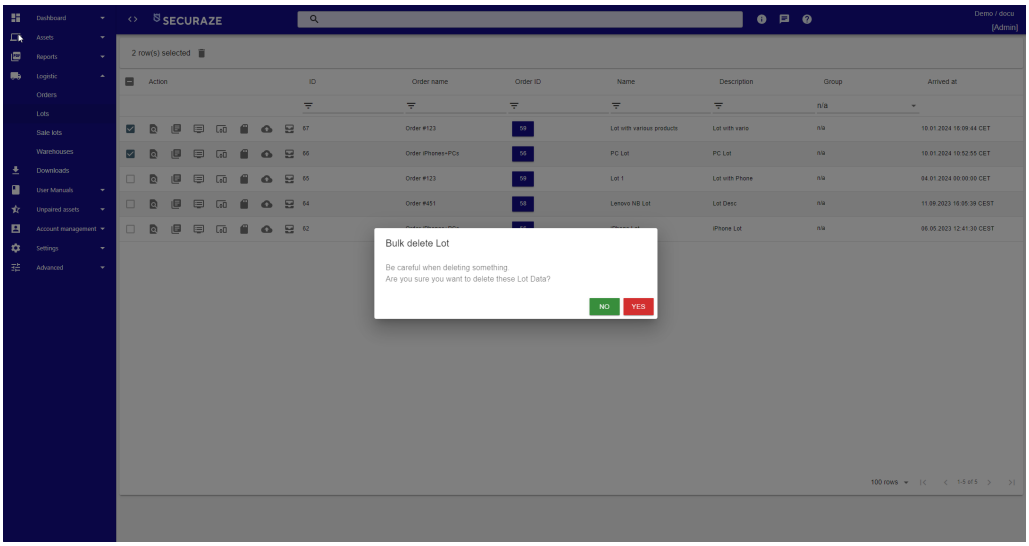


10.1.4.2.3 Delete Lot

To delete an Lot, select the Lot and click **Delete Lot**



Confirm the erasure by clicking on **YES**.

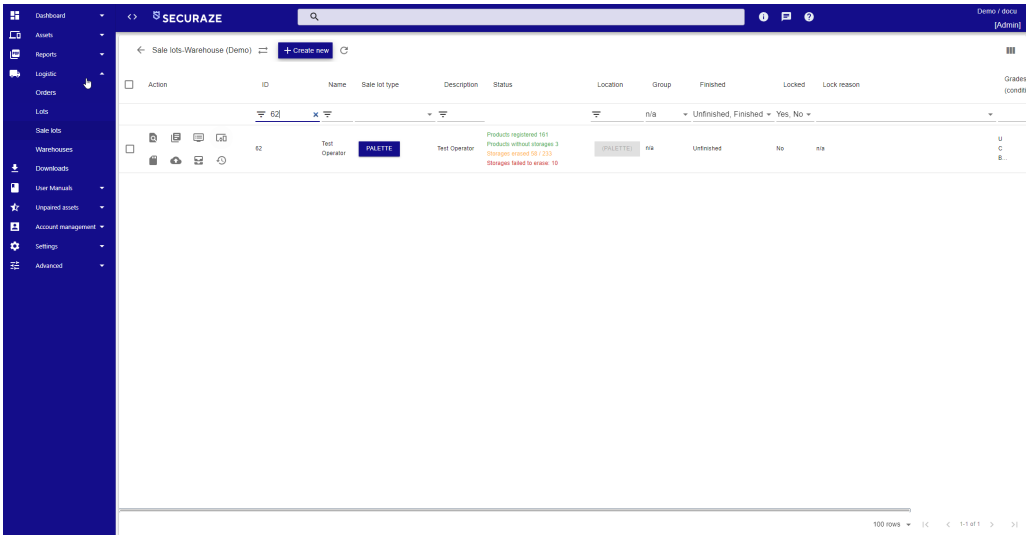


10.1.4.3 Sale Lots

In the menu **Logistc - Sale Lots** you can create new containers, edit and delete existing ones.

There you see a list of all containers with the status of the erasure.

The Status field displays a brief overview of the content and status of the devices on the container.



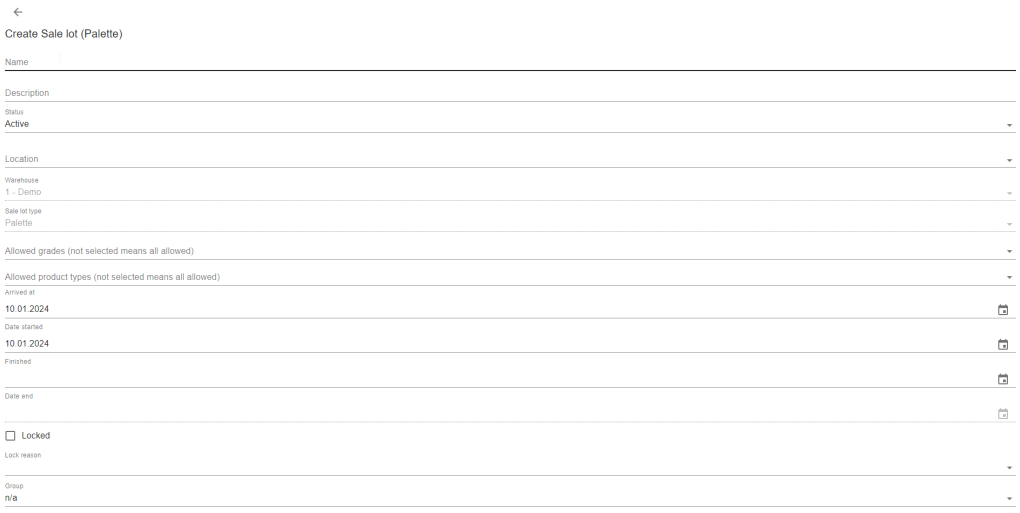
By selecting the option **Go to Work Products** you can access the list of work devices.
By selecting the option **Go to Mobile Products** you get to the list of mobile devices of this palette. Here you can see some details about the devices and the status of the deletion.
Under **history** you can call 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.

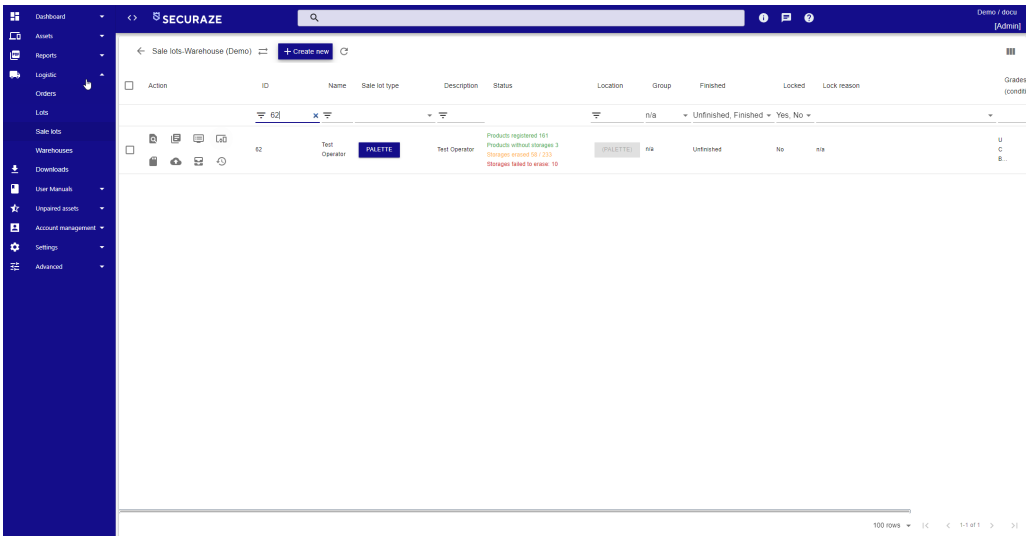
10.1.4.3.1 Create new Sale Lot

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 storage pallet and select the date.

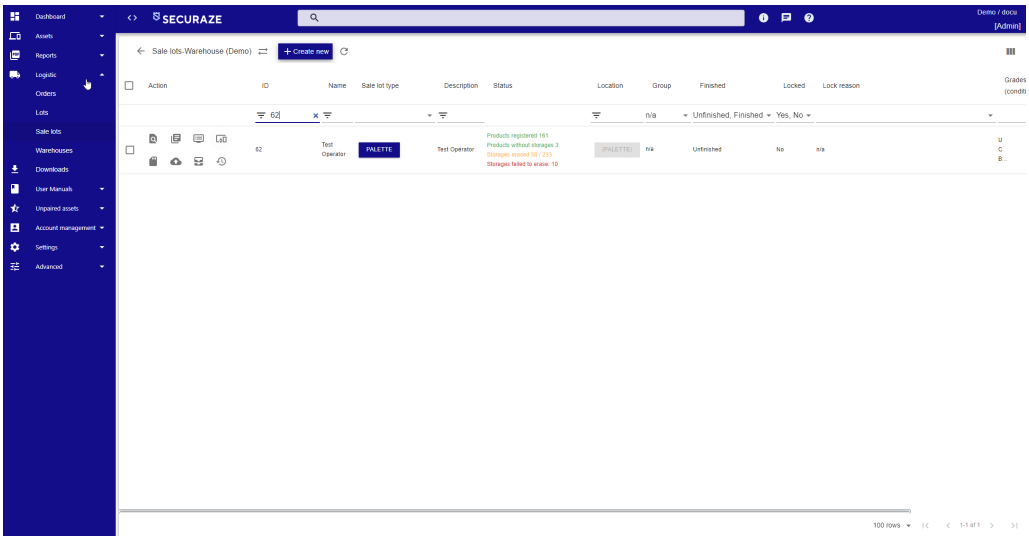


After confirming the selection by clicking **SAVE**, the newly created storage pallet is visible in the **Sale Lots** menu.

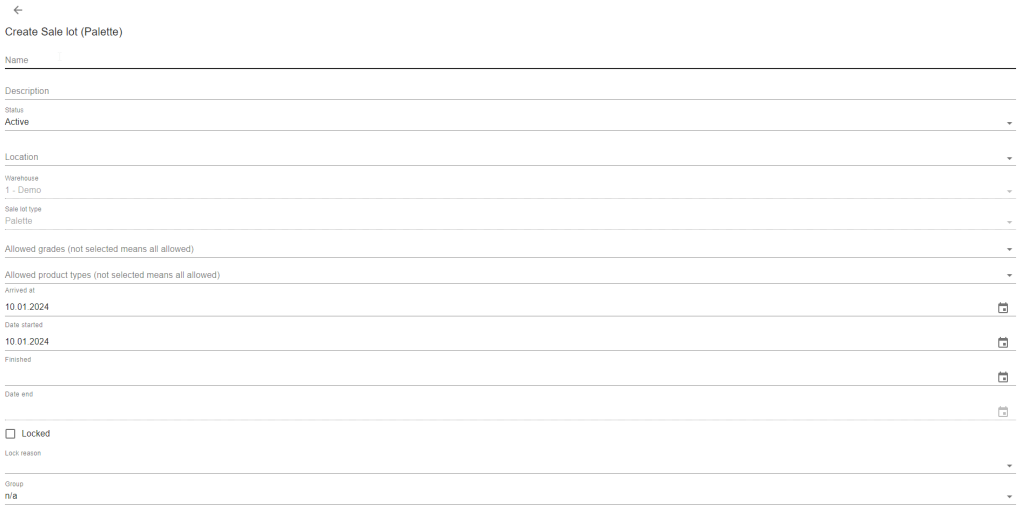


10.1.4.3.2 Edit Sale Lot

To edit a Sale Lot, select the container and click **Sale Lot Details**.

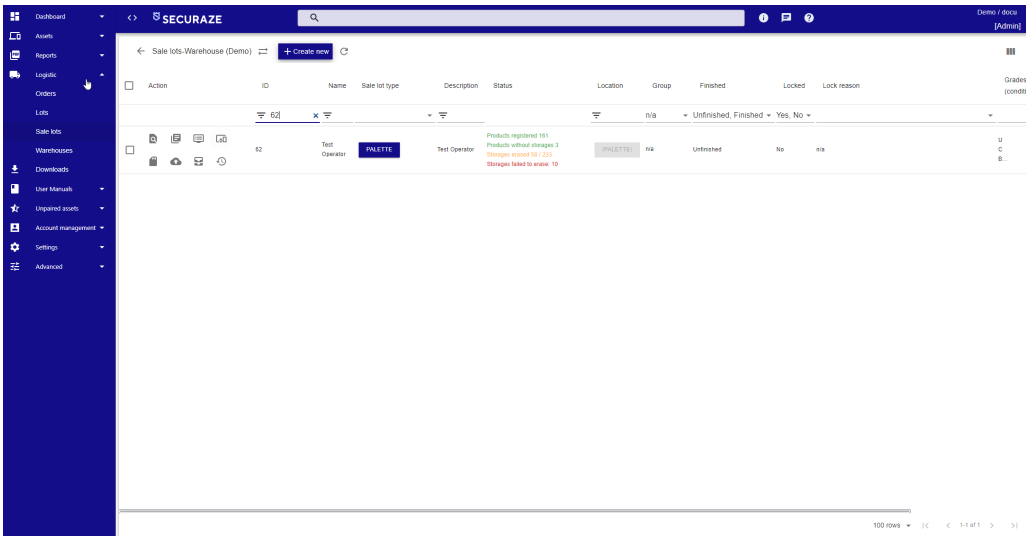


Make the desired changes and confirm them by clicking on **SAVE**.



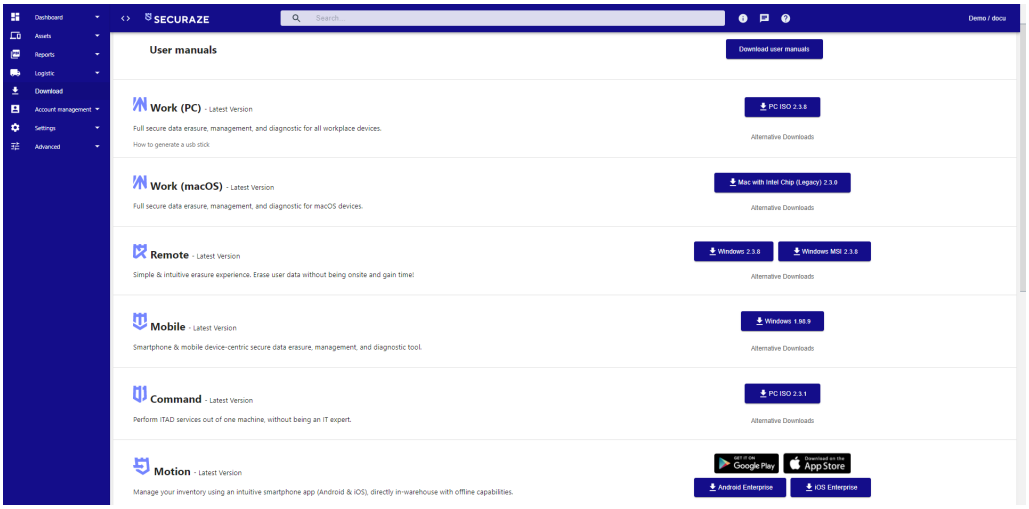
10.1.4.3.3 Delete Sale Lot

To delete a Sale Lot, select the respective container and click on **Delete Sale Lot** .



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.

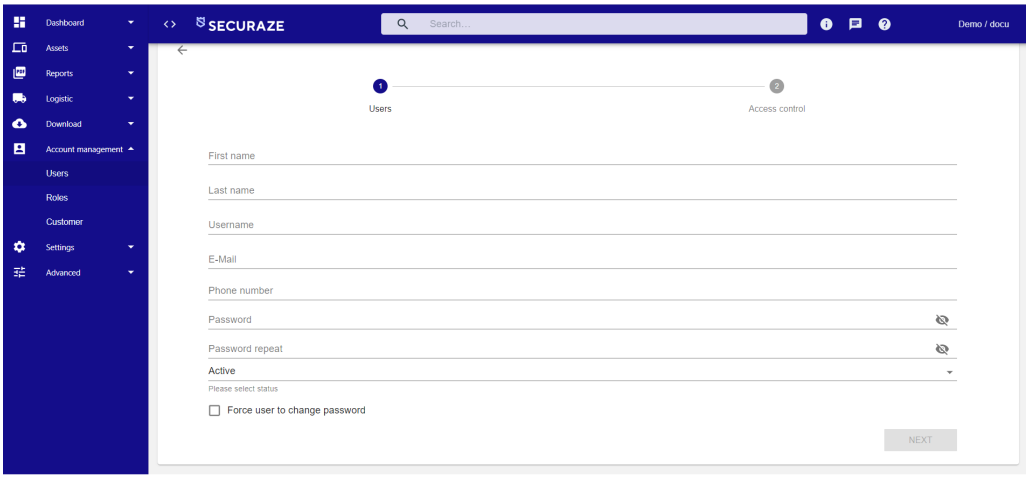
10.1.6.1 User

In the **Users** menu you can create new Users, edit existing ones and delete them.

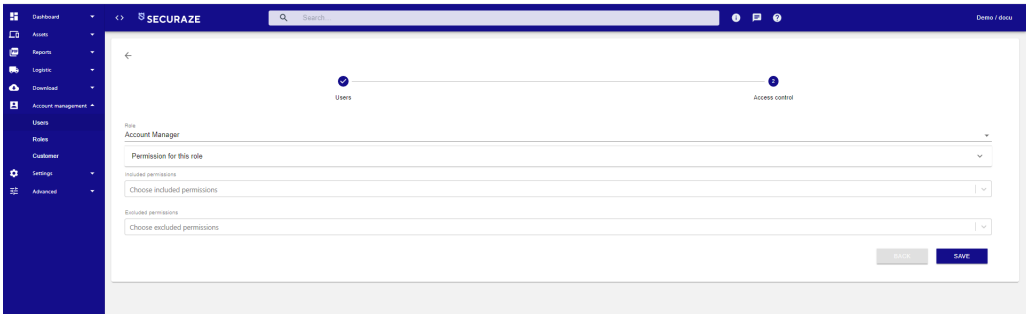
10.1.6.1.1 Create new Users

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.



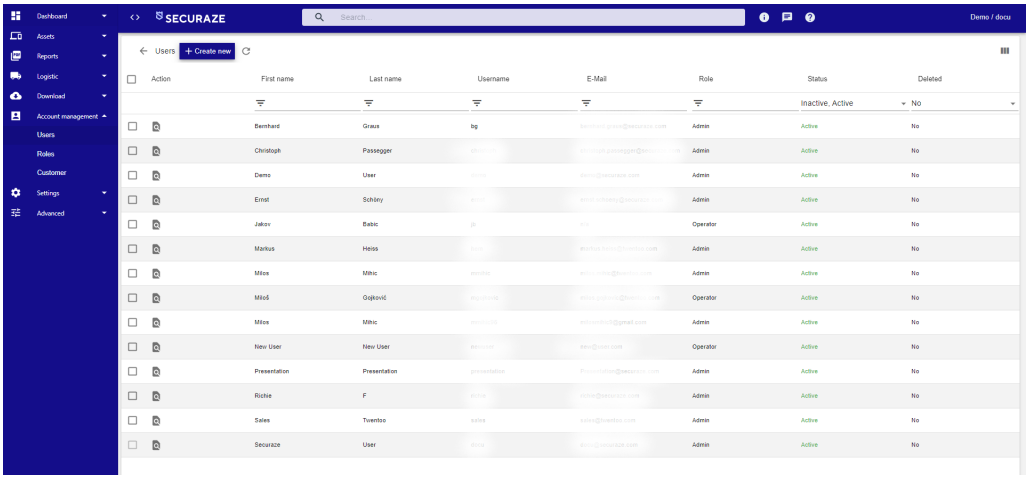
Confirm the entry of your data with **NEXT**.



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.

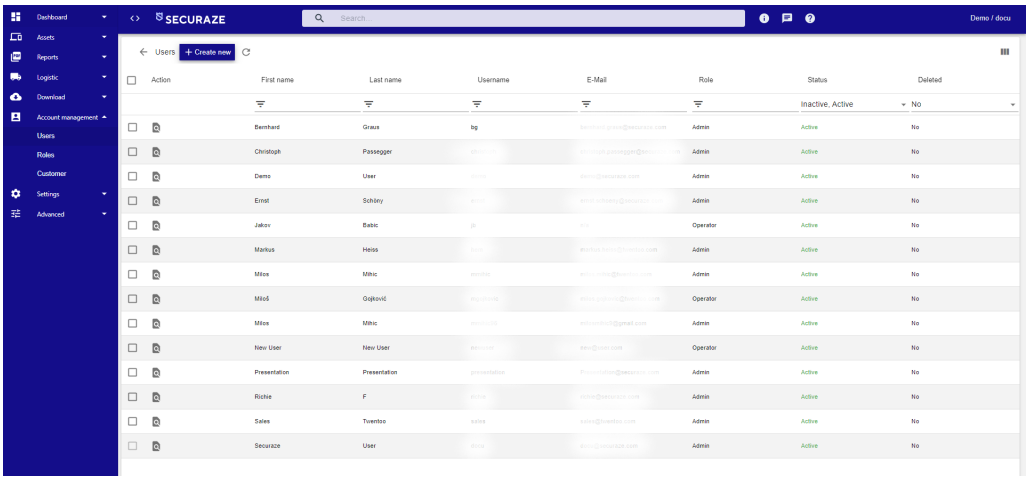
After confirming the selection by clicking on **SAVE**, the newly created user is visible in the **User** menu.



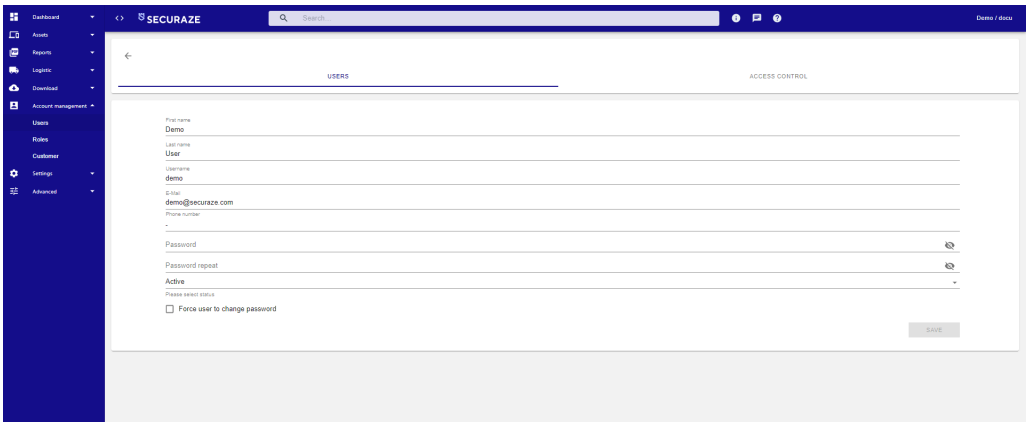
The created user has 3 different possibilities to log in:
Login with complete username: Enter *username @ namespace* 202
Login with e-mail address: Enter your registered e-mail address.
Login with user name: This is only possible if you are in a created network zone 230 and the authorization has been 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**

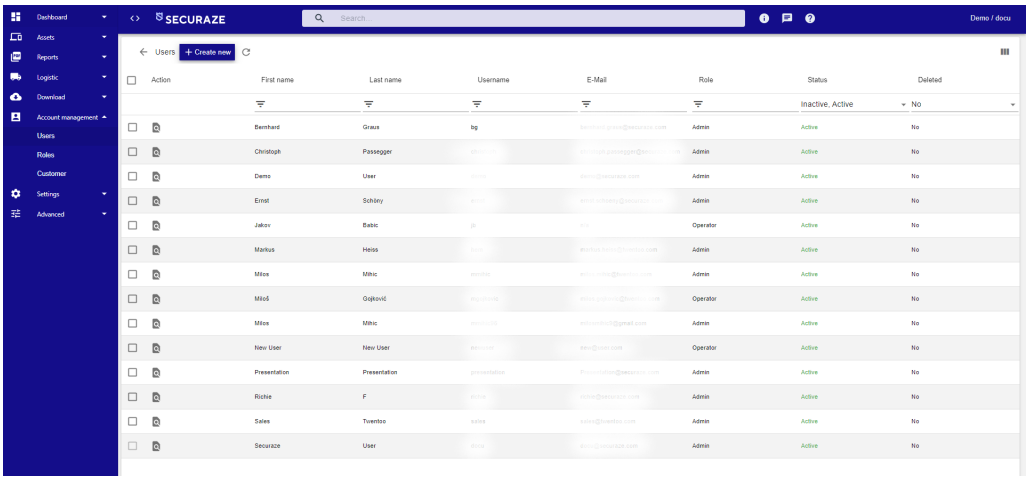


Make the desired changes and confirm them by clicking **SAVE**.

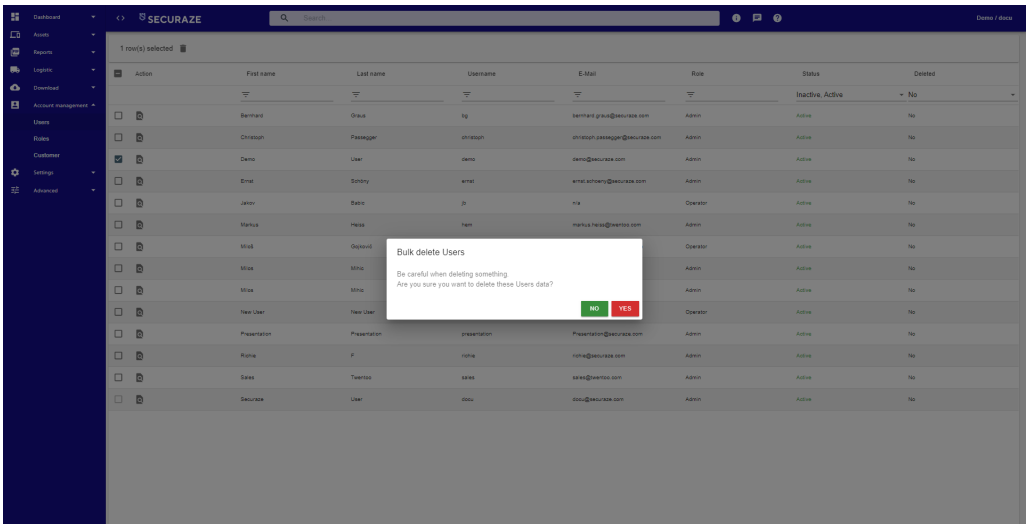


10.1.6.1.3 Delete User

To delete a user, select the respective user and click **Remove all selected Users**.



Confirm the erasure by clicking on **YES**.



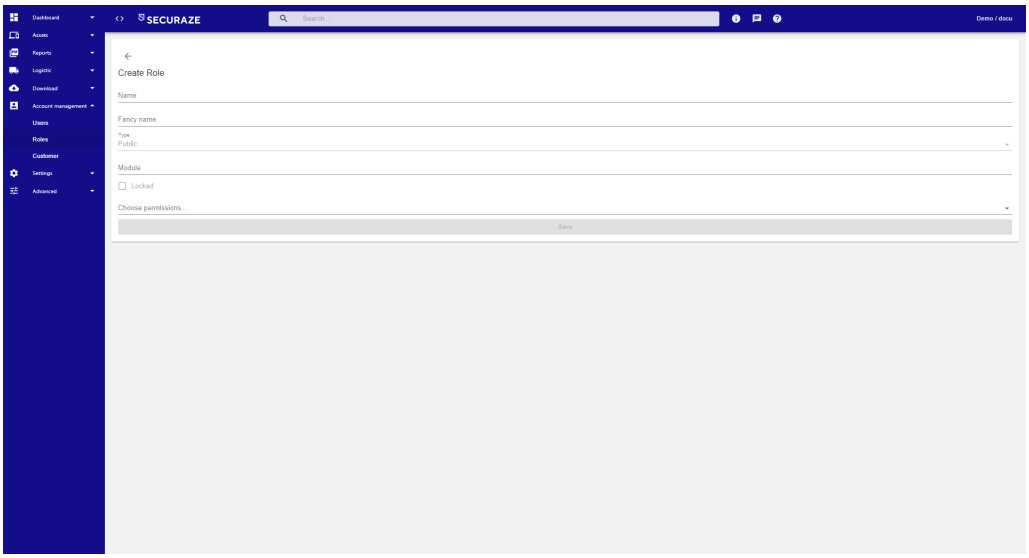
10.1.6.2 Roles

In the **Roles** menu you can create new roles, edit existing ones and delete them.

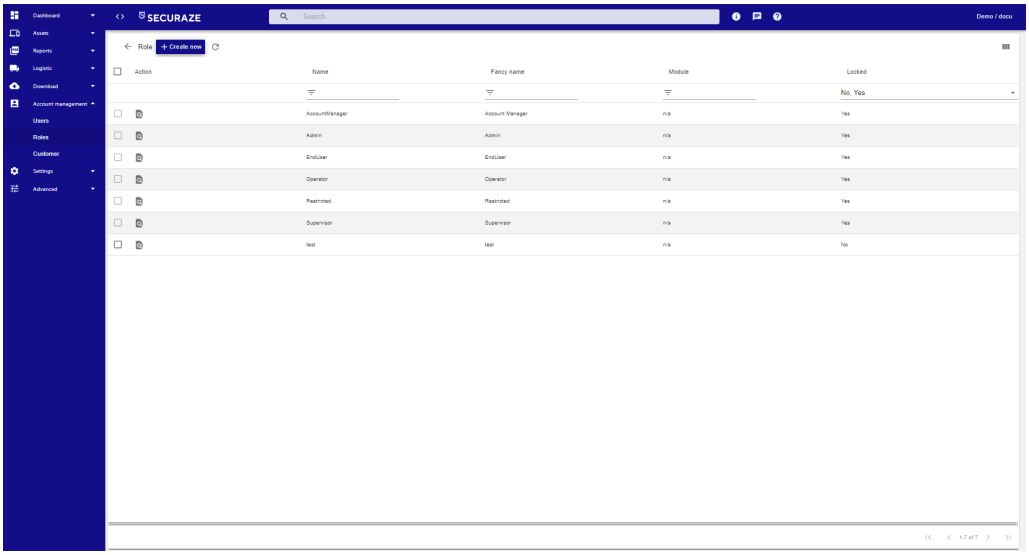
10.1.6.2.1 Create new Role

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.

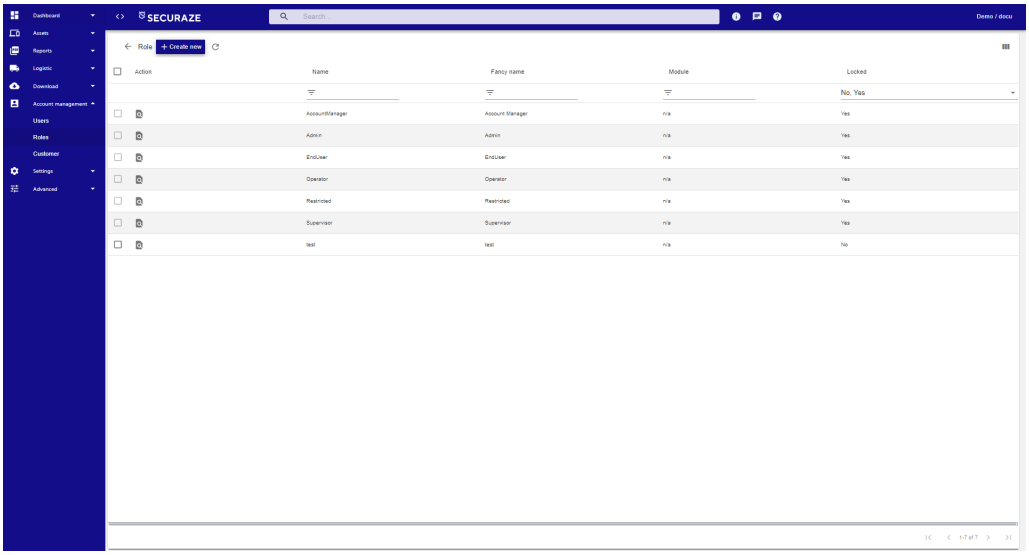


After confirming the selection by clicking on **SAVE**, the newly created user is visible in the **Roles** menu.

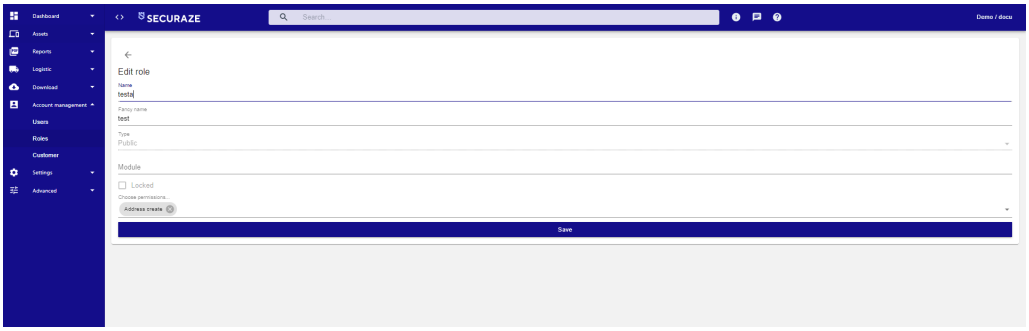


10.1.6.2.2 Edit Role

To edit a user, select the respective user and click **Role details**

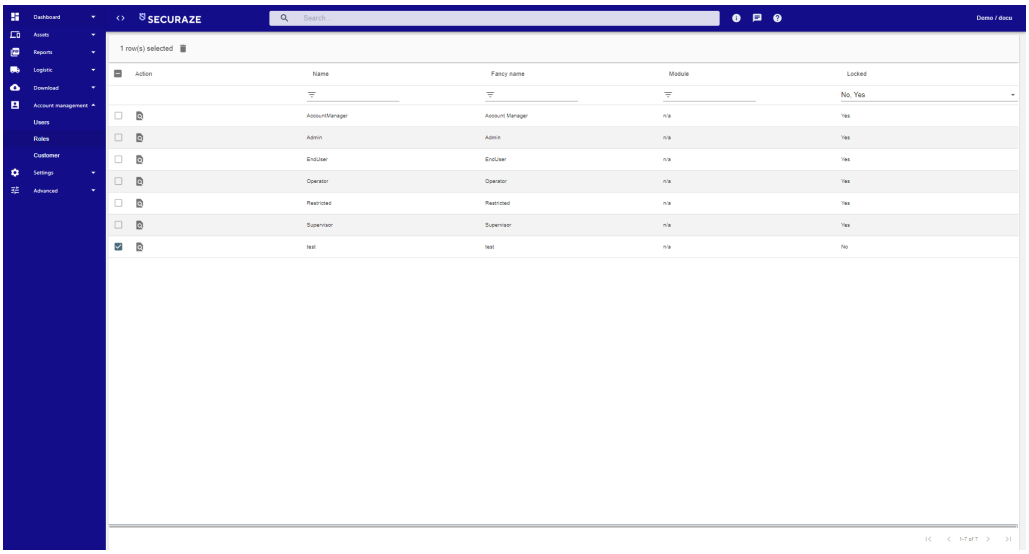


Make the desired changes and confirm them by clicking **SAVE**.

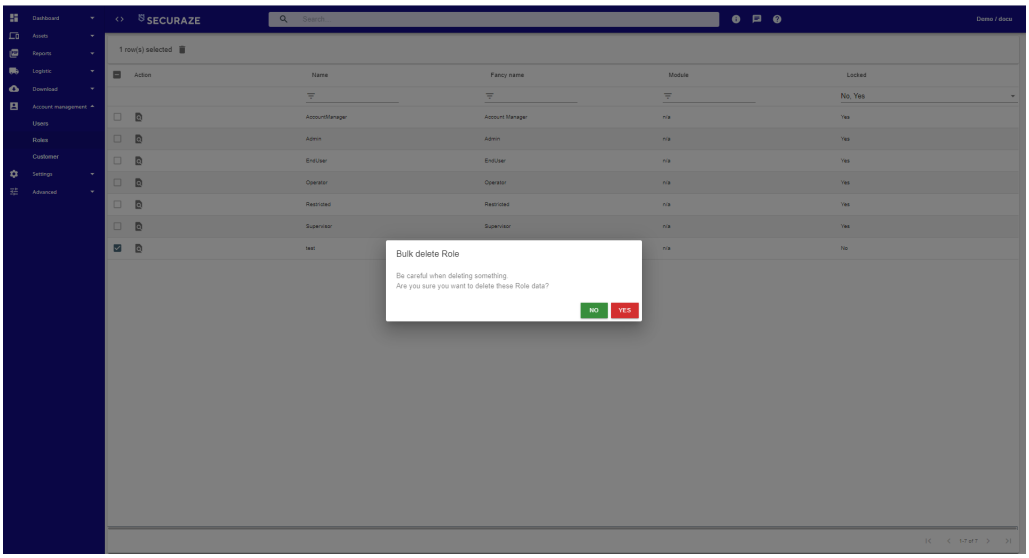


10.1.6.2.3 Delete Role

To delete a user, select the respective user and click **Remove all selected Roles**.

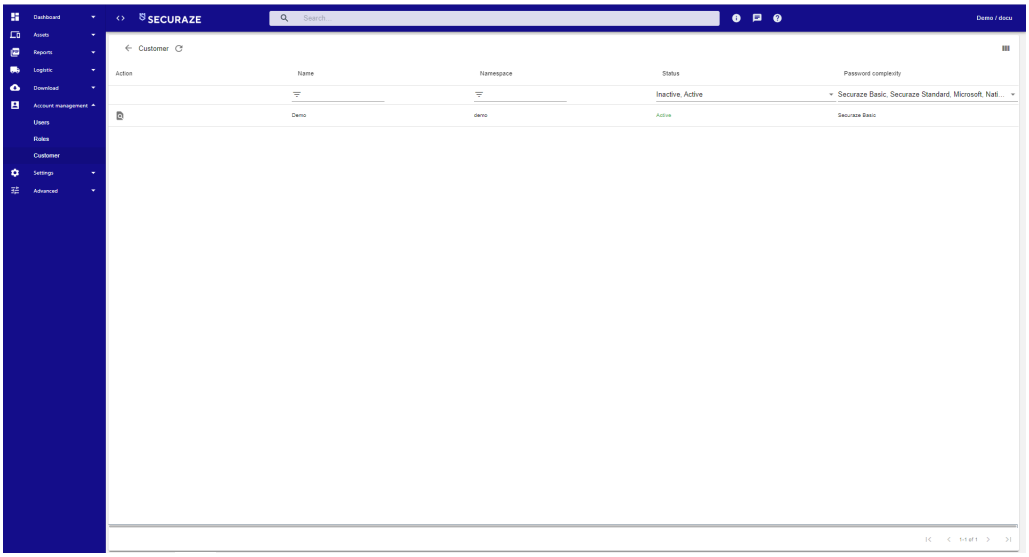


Confirm the erasure by clicking on **YES**.

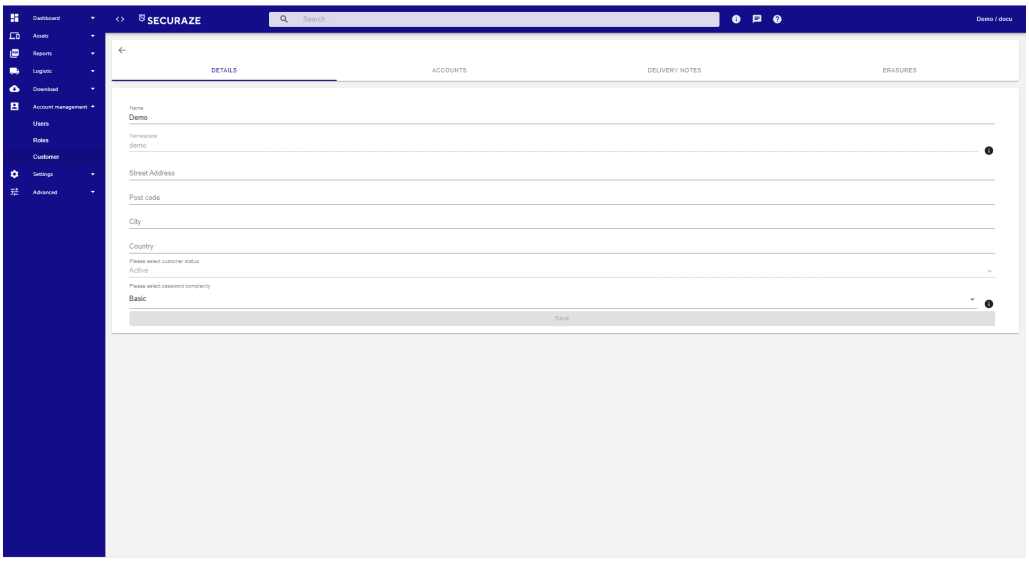


10.1.6.3 Customer

In the **Customer** menu you see an overview of the customers created.



By clicking on **customer details** you will get to the detailed view.

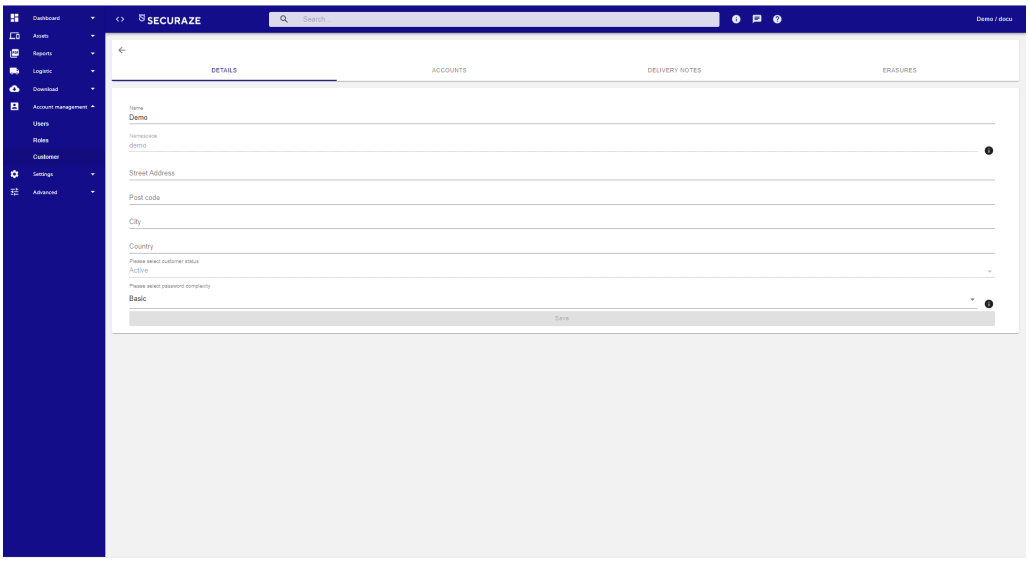


Here you can choose from the following tabs:
DETAILS
ACCOUNTS
DELIVERY DOCUMENTS
ERASURES

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.

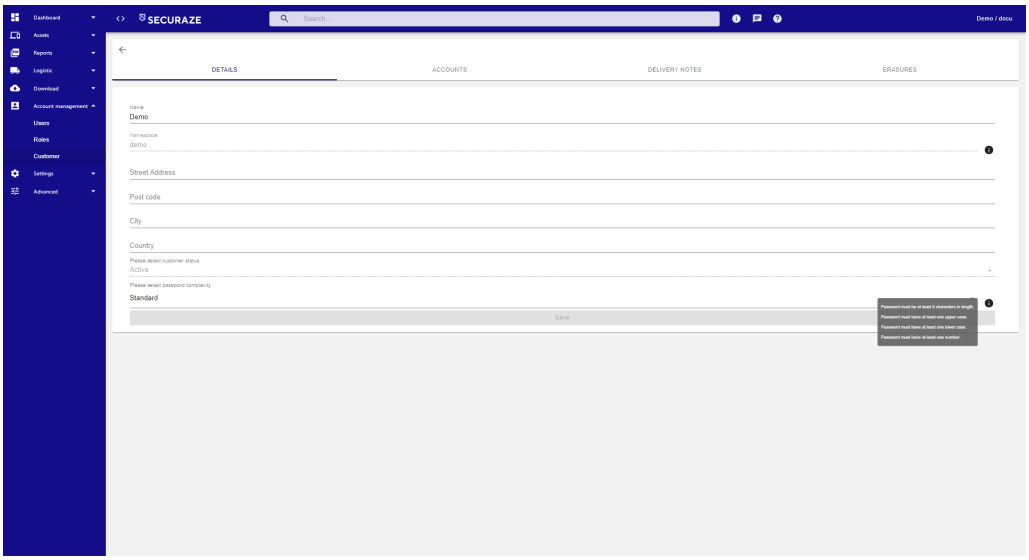


First of all you will see the name and address of the customer.

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 196.
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
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.

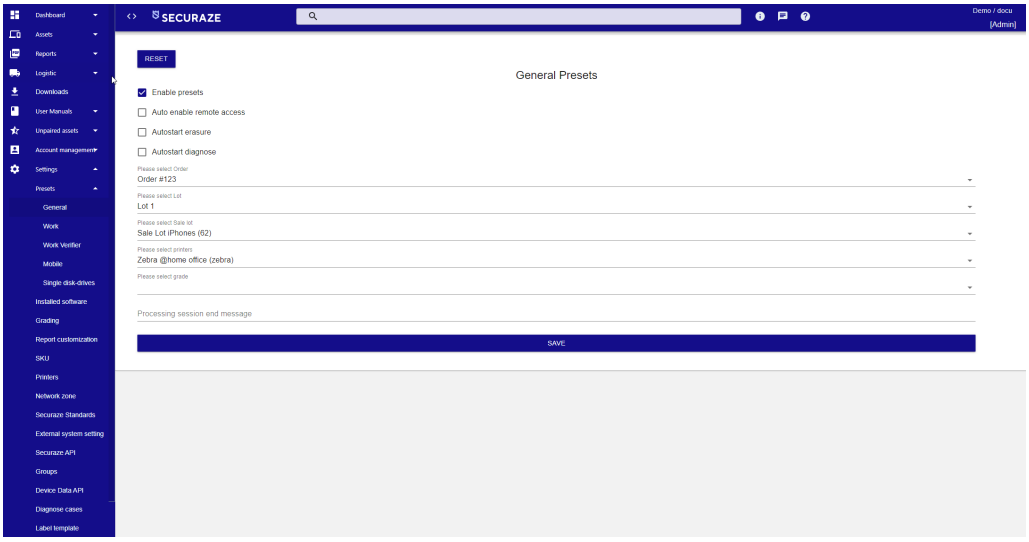
10.1.7.1 Presets

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.



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.
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. Based on the Securaze default value of 80: If the calculated SMART score is 80-100, the disk is considered to be in good condition. The score of 40-79 describes used condition, and if it's less than 40, a failure is possible. The operator can set the SMART score bellow which the disks should not be processed in the Presets for HDD erasure:
Disk Health Calculation	This setting changes the calculation method of the SMART Health score. Currently supported: **Securaze proprietary method** Securaze proprietary method (typically the most rigorous calculation method) [Default] **Hard disk sentinel (HDSentinel)** Hard disk sentinel method, based on public available documentation of the algorithm https://www.hdsentinel.com/help/en/52_cond.html https://www.hdsentinel.com/smart/index.php **Acronis Drive Monitor** 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.	Available for both Work macOS and Work Linux, working for PC, macOS Native and also Mac booting WorkPC.

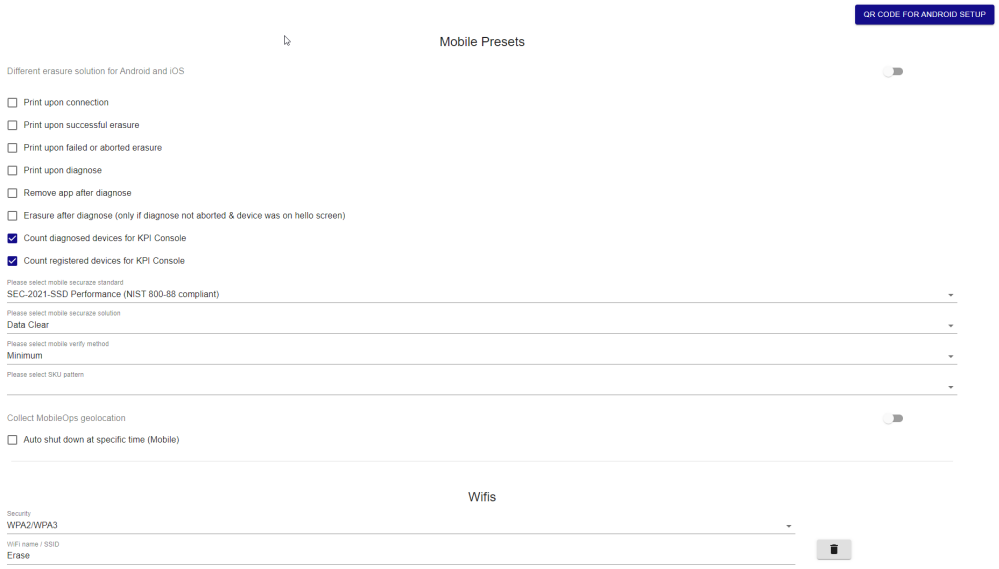
Setting	Description
after login, while entering data)	Normal Brightness can be set to any value between 20 and 100.
Please select reduced screen brightness (during screensaver mode)	Reduced Brightness can be set to any value between 0 and 100, for when screensaver is displayed during erasure (allowing the screen to be black, if max. power saving is required) 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.
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. It is mandatory for iOS diagnose and iOS Advanced erasure. And it can be used for generating QR-Codes for faster Android USB-Debugging bypass.

Setting	Description

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**:



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.
Please select mobile securaze standard	Default value for the Securaze Standard.

Setting	Description
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. It is mandatory for iOS diagnose and iOS Advanced erasure. 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**:

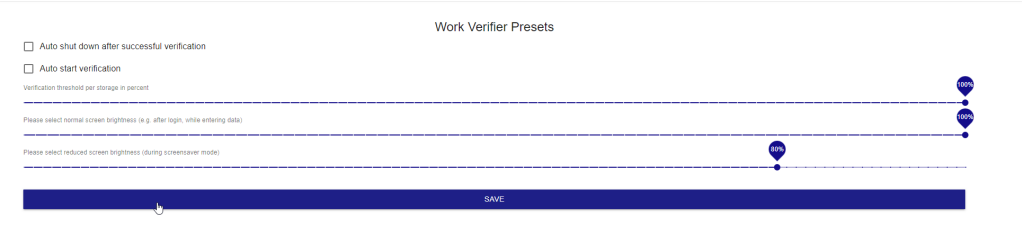
Setting	Description
Auto shutdown after successful erasure	Device will shutdown after successful erasure and keep running otherwise.
Automatic unfreeze	Device will do a automatic unfreeze before erasure.
Please select SSD Securaze standard	Default value for the Securaze Standard.

Setting	Description
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 of Disk Helath calculation method. Default is Hard Disk Sentinel. Available is as well Securaze and Acronis.
Please select normal screen brightness	Screen brightness (e.g. after login, while entering data)
Please select reduced screen brightness (during screensaver mode)	Screen brightness (e.g. 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**:



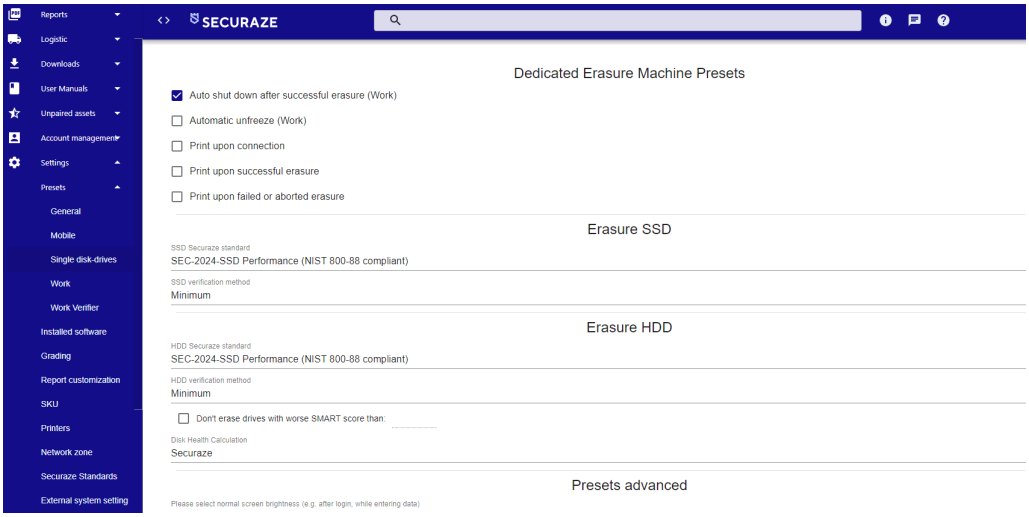
Setting	Description
Auto shutdown after successful verification	Device will shutdown after successful verification and keep running otherwise.
Auto start verification	Device will do a automatic verification after login.
Verification threshold per storage in percent	How much data of the storage should get verified. (Default 100%)

Setting	Description
Please select normal screen brightness	Screen brightness (e.g. after login, while entering data)
Please select reduced screen brightness (during screensaver mode)	Screen brightness (e.g. during screensaver mode)

Make your settings and confirm them with **SAVE.**

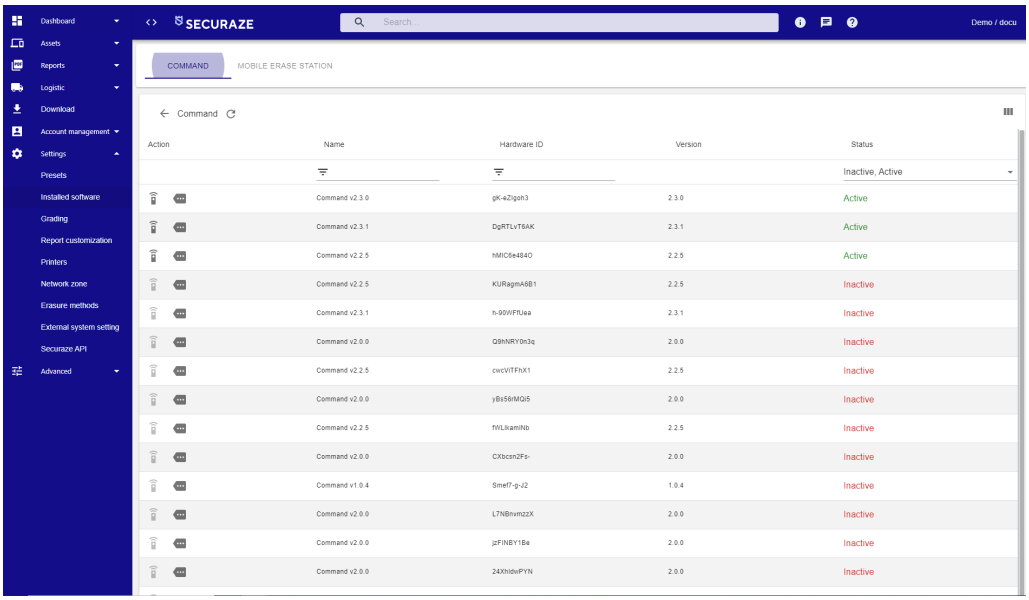
10.1.7.1.5 Single Disk-Drives

Single Disk-Drive presets are settings applied only when Securaze Work is used for erasure of loose drives (disks) in Dedicated Erasure Machine mode.



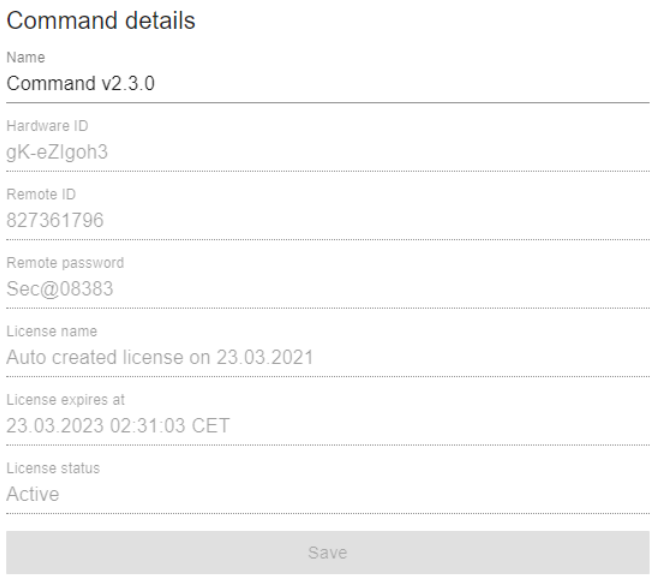
10.1.7.2 Installed software

In the menu **Installed software** you can see the different versions of the software that are installed.

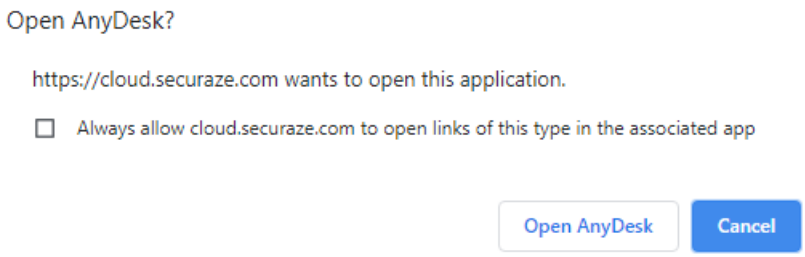


Here you can find the information about which version it is and if the software is active.

If you click on Command details, a new window will open showing the details.

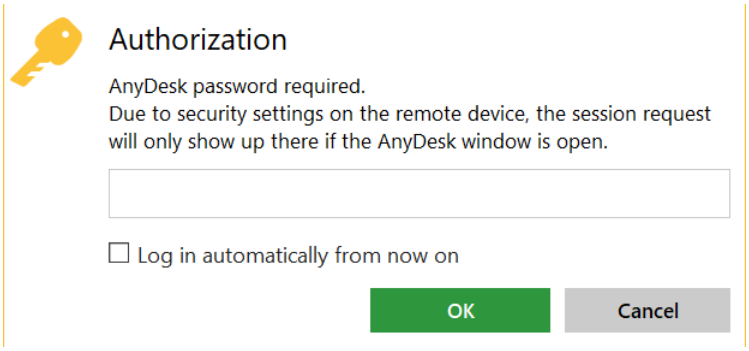


If you click on the icon **Open Securaze Remote**, you can establish a remote connection via Anydesk.



The password will be copied to clipboard automatically.

When Anydesk opens, paste the copied password here with CTRL+V and confirm with OK.



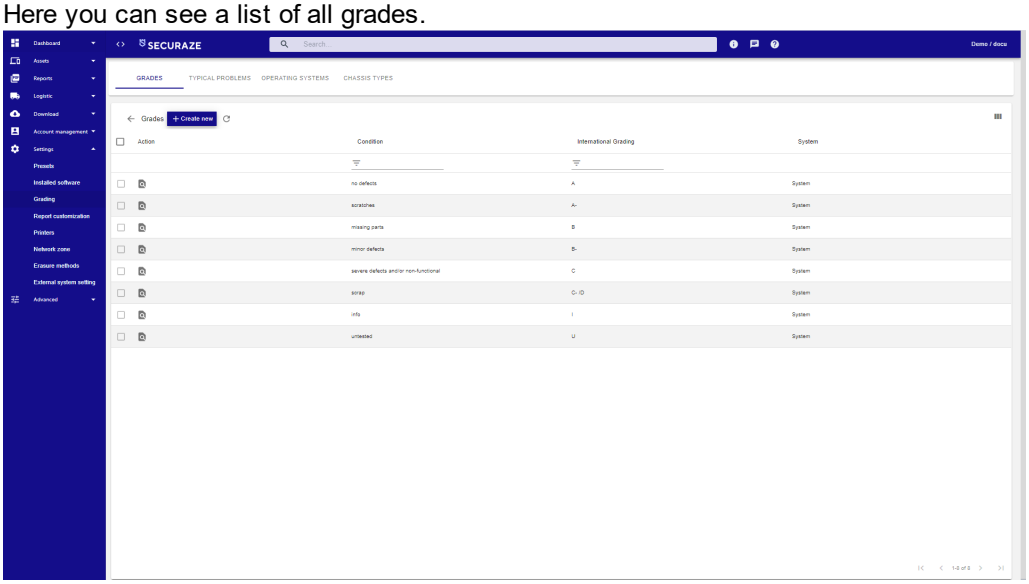
After that, a remote connection to the device will be established.

10.1.7.3 Grading

In the **Grading** menu you can see 4 tabs:
GRADES
TYPICAL PROBLEMS
OPERATING SYSTEMS
CHASSIS TYPES

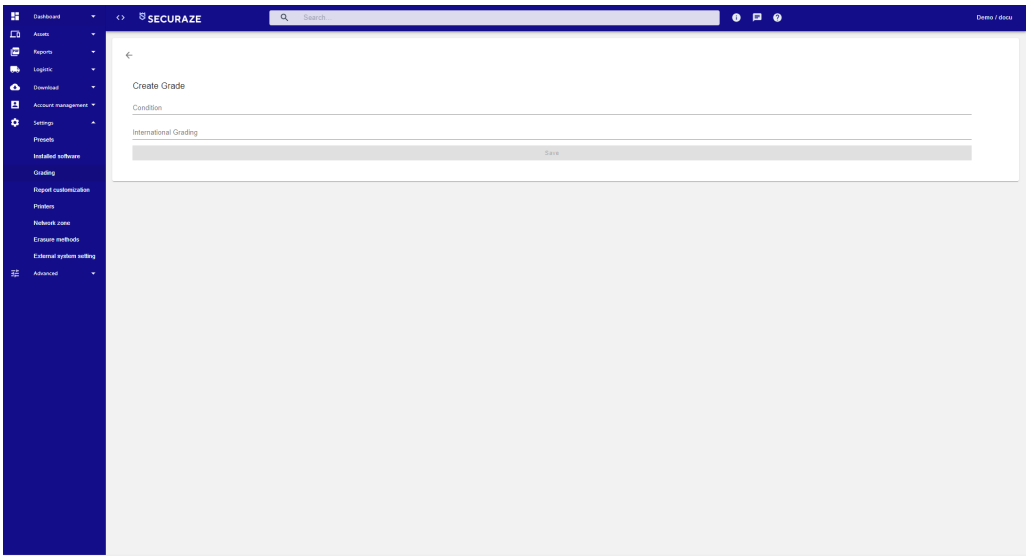
10.1.7.3.1 Grades

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**.

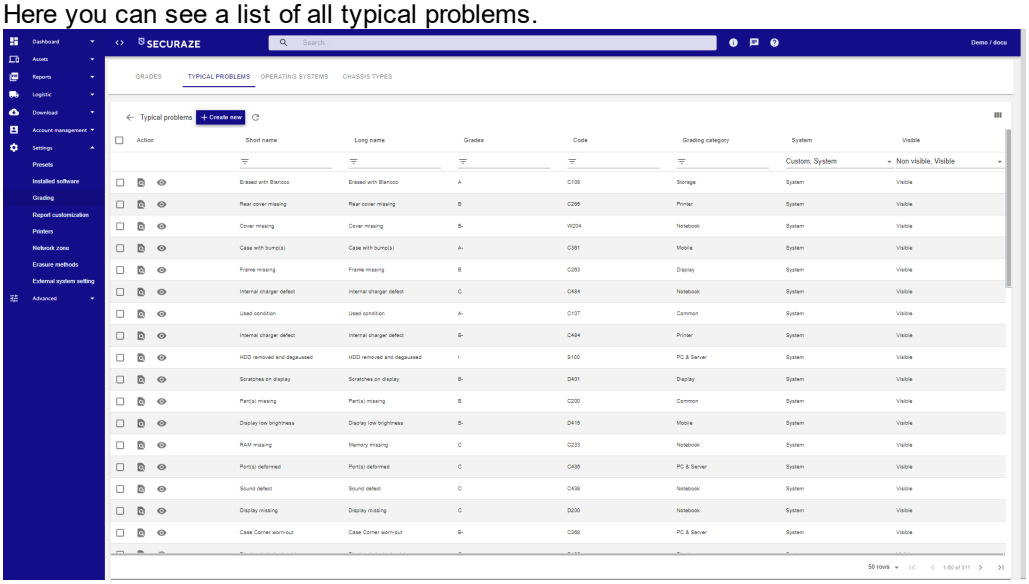
Here you enter the data of the new grade.



After confirming the selection by clicking **SAVE**, the newly created grade is displayed in the **Grades** menu.

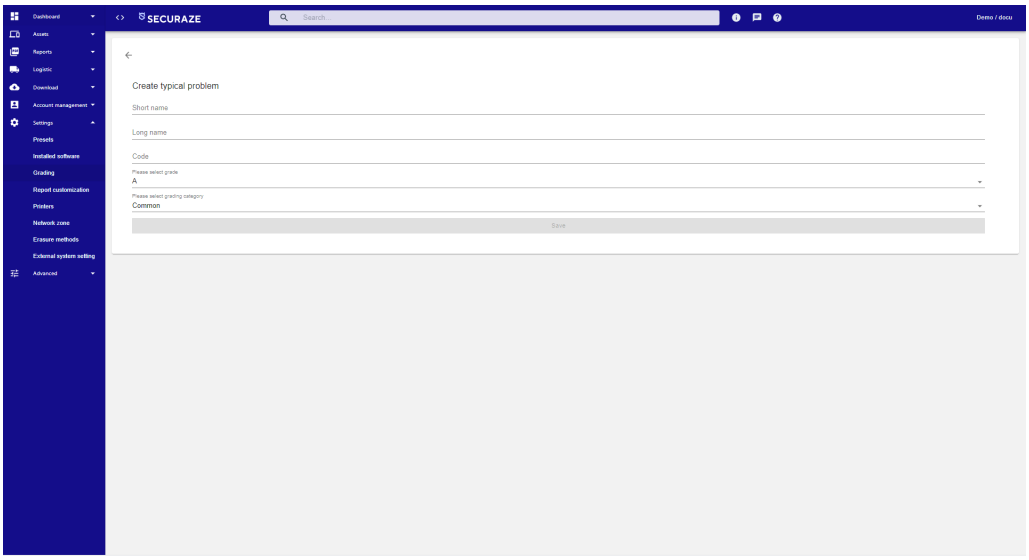
10.1.7.3.2 Typical problems (Optional)

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**.

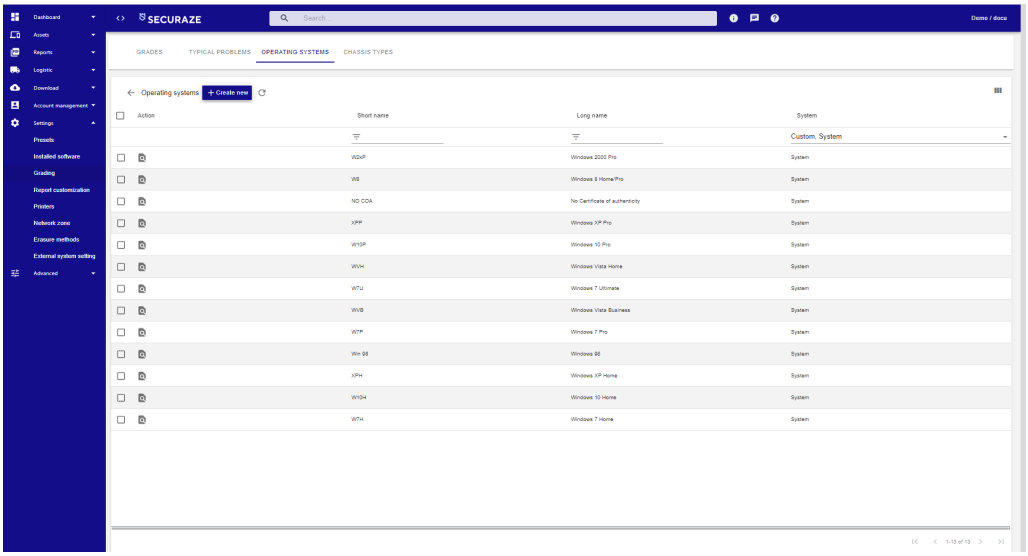
Here you enter the data of the new typical problem.



After confirming the selection by clicking **SAVE**, the newly created grade is displayed in the **Typical Problems** menu.

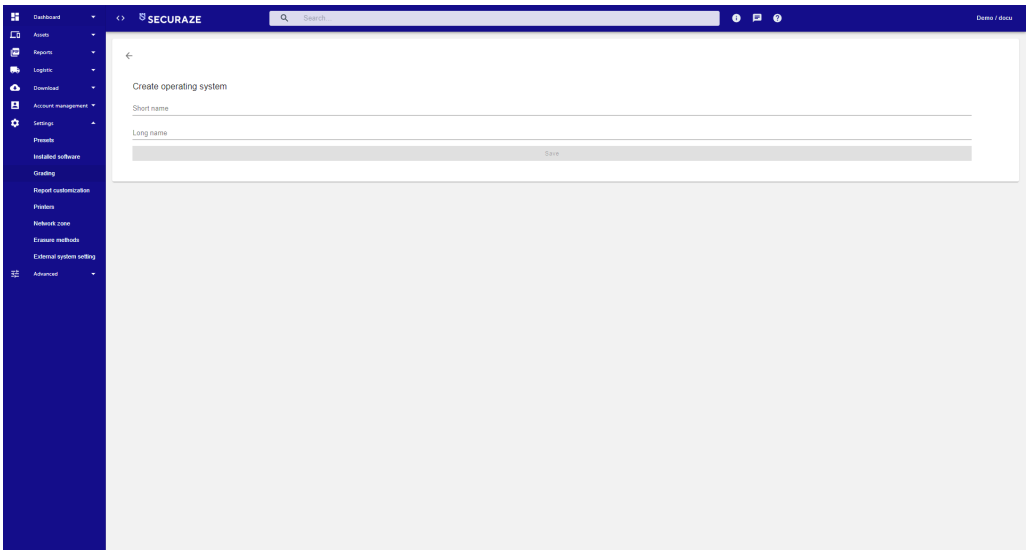
10.1.7.3.3 Operating Systems

Here you can see a list of all Operating Systems.



To create a new operating system, click on **Grading** in the Menu section and then on the **Tab Operating Systems**. Then choose **Create New**.

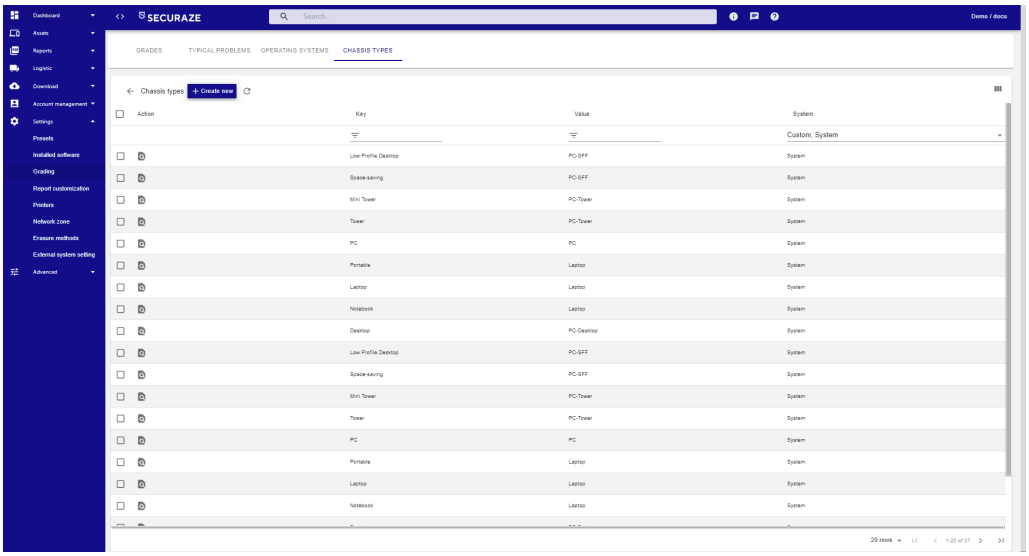
Here you enter the data of the new operating system.



After confirming the selection by clicking **SAVE**, the newly created grade is displayed in the **Operating Systems** menu.

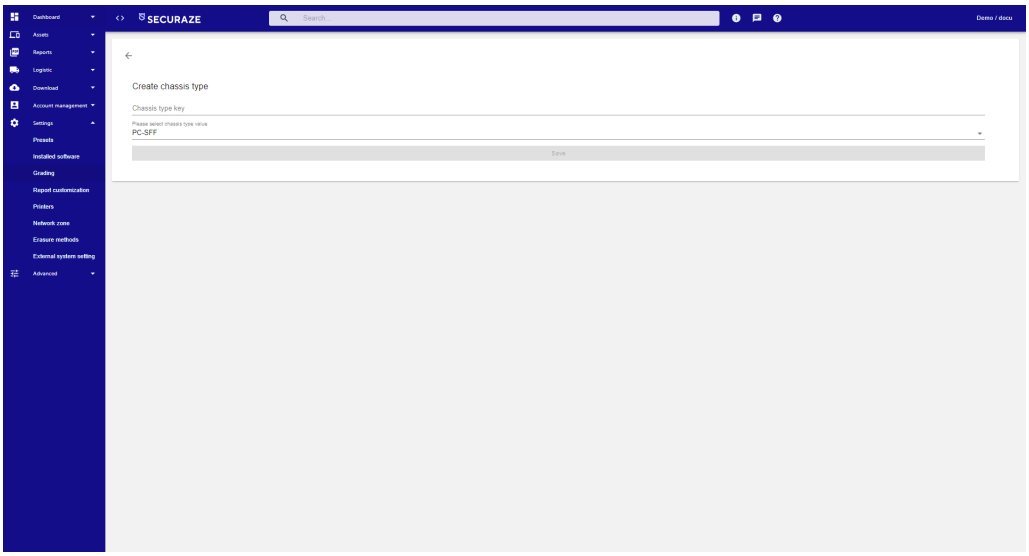
10.1.7.3.4 Chassis Types

Here you can see a list of all Chassis Types.



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.

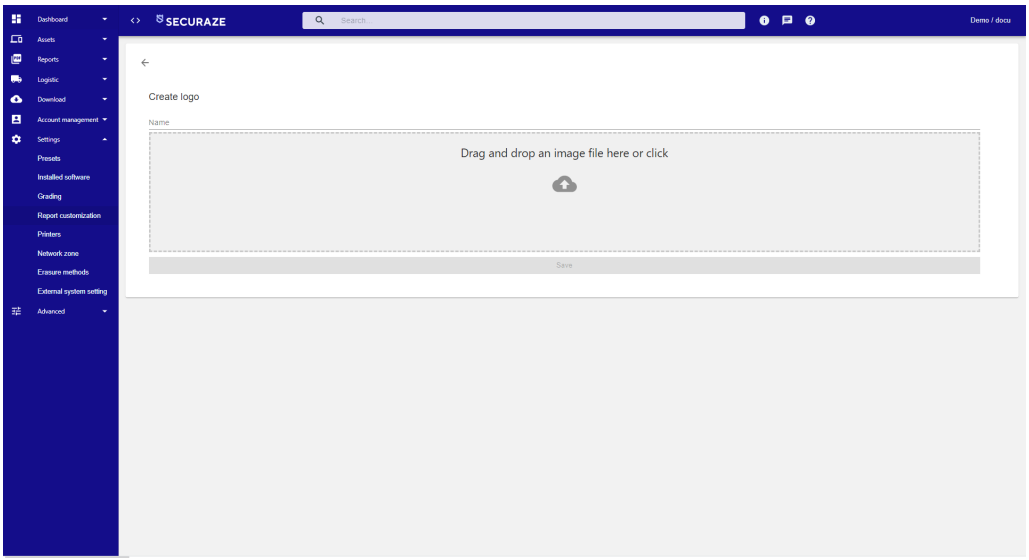
10.1.7.4.1.1 Create new Logo

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**.

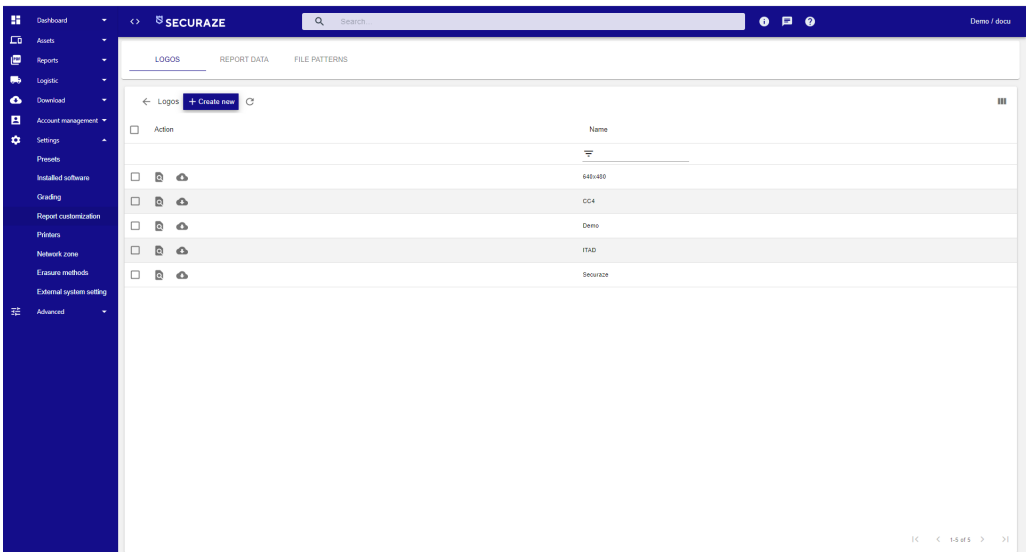
Here you upload the desired logo by kicking on **UPLOAD** and assign a name.

Recommended size of the logo:
Square shaped: 512 x 512 pixel

Rectangular shaped:
600 x 400 pixel

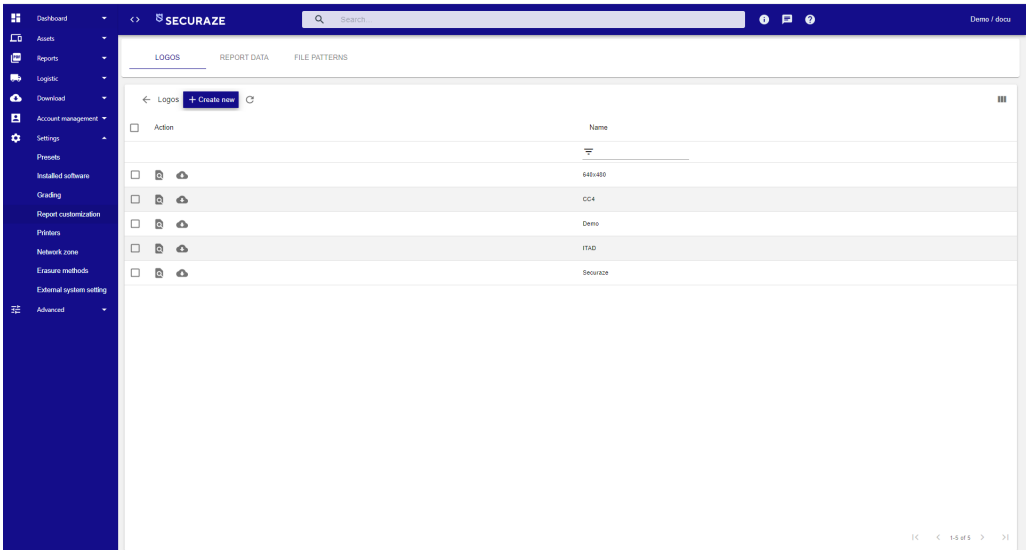


After confirming the selection by clicking **SAVE**, the newly created logo is visible in the Tab **Logos**

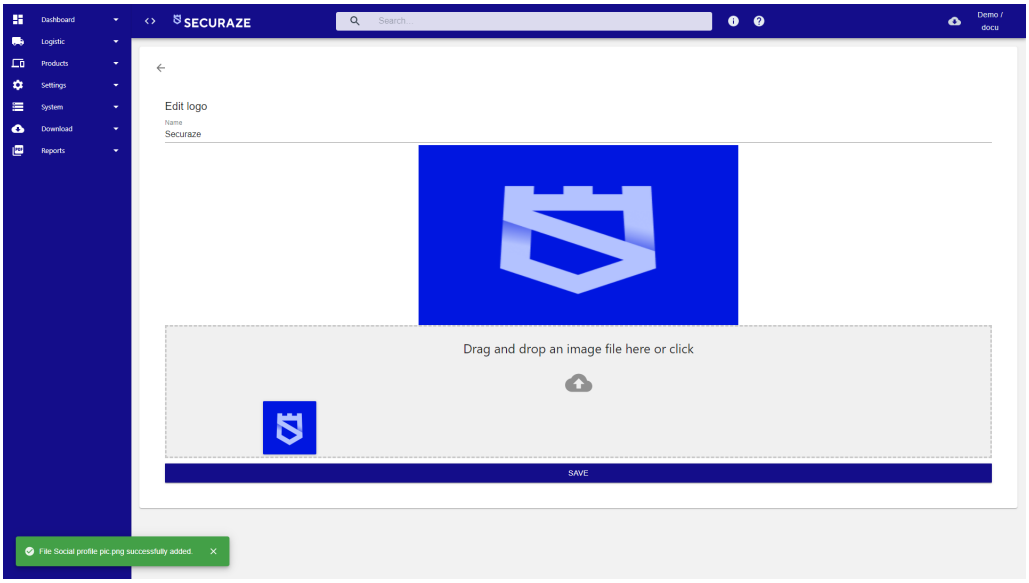


10.1.7.4.1.2 Edit Logo

To edit a logo, select the respective logo and click on **Logo details** .

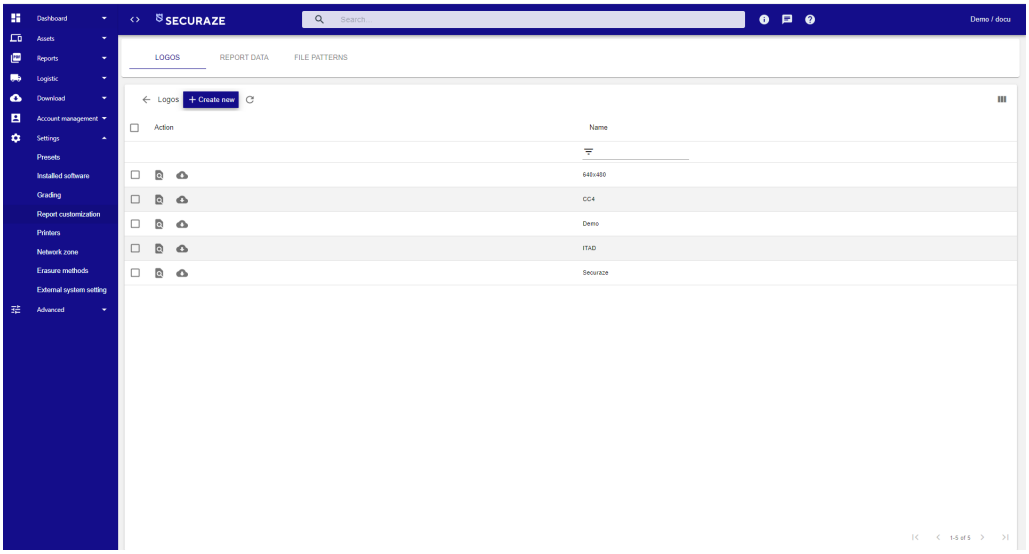


Make the desired changes and confirm them by clicking **SAVE**.

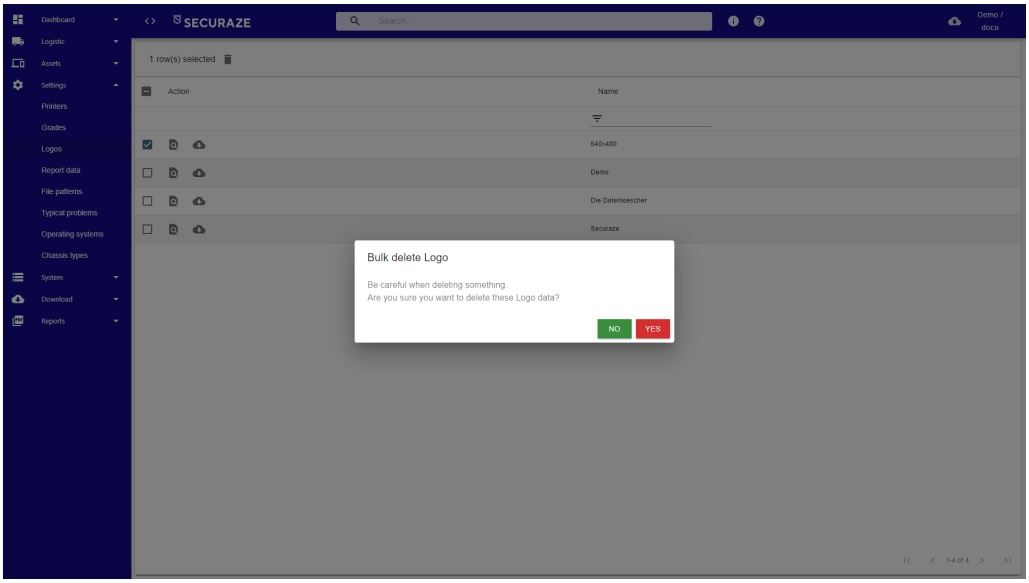


10.1.7.4.1.3 Delete Logo

To delete a logo, select the respective logo and click on **Remove all selected Logos**.



Confirm the erasure by clicking on **YES**.



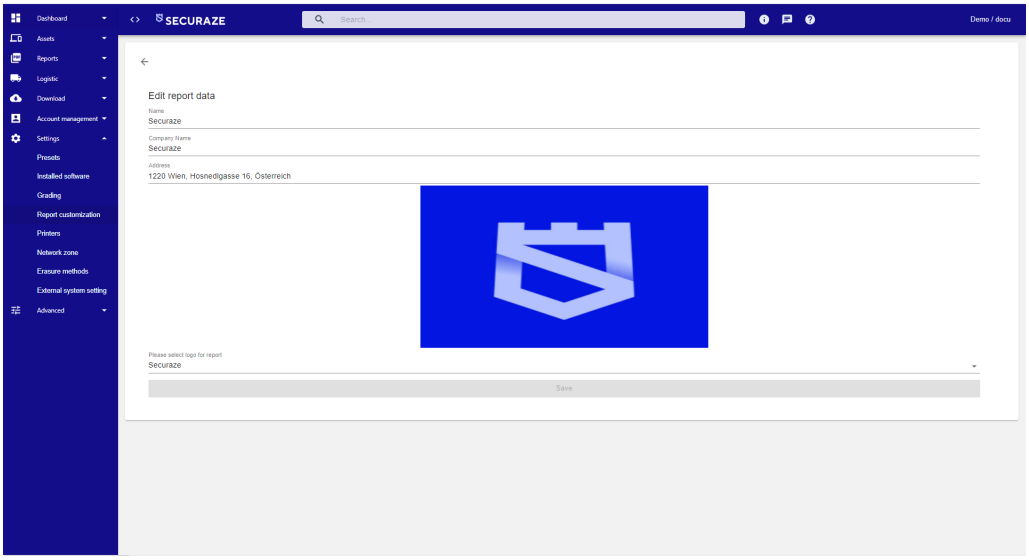
10.1.7.4.2 Report Data

In the **Settings - Report Customization** menu, Tab **REPORT DATA**, you can create new report data, edit existing report data, and delete report data.

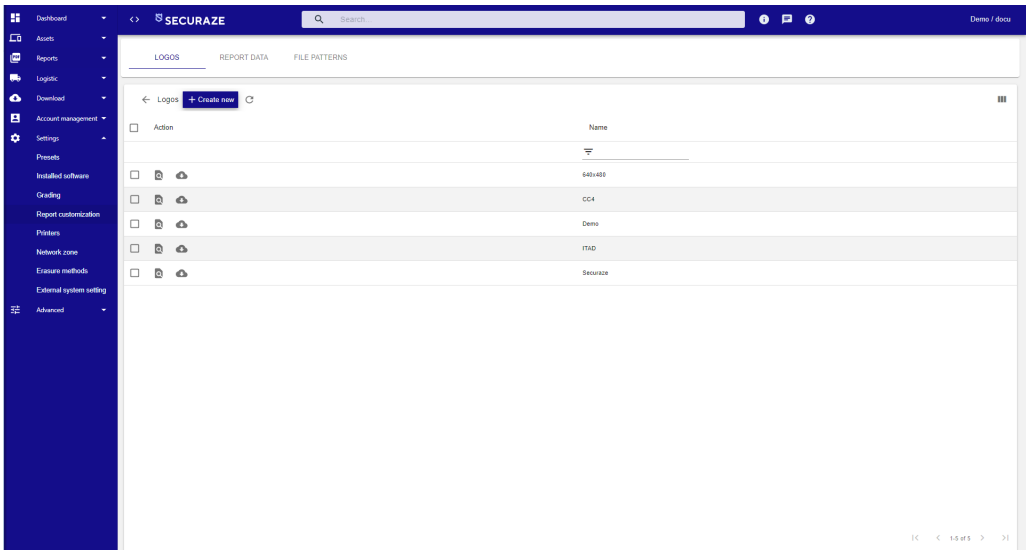
10.1.7.4.2.1 Create new Report Data

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.

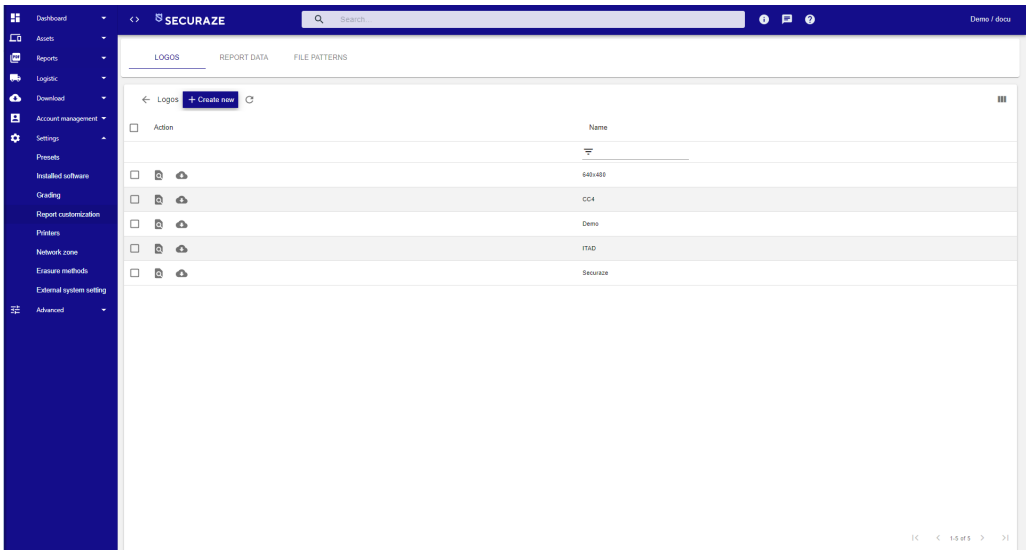


After confirming the selection by clicking **SAVE**, the newly created report data can be viewed in the Tab **Report data.**

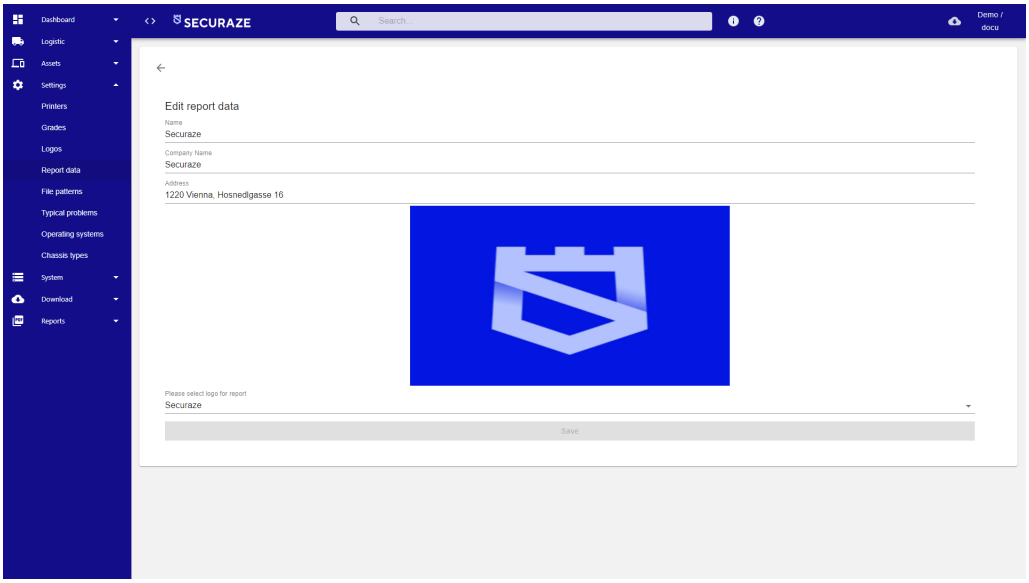


10.1.7.4.2.2 Edit Report Data

To edit report data, select the respective report data and click on **Report Data details** .

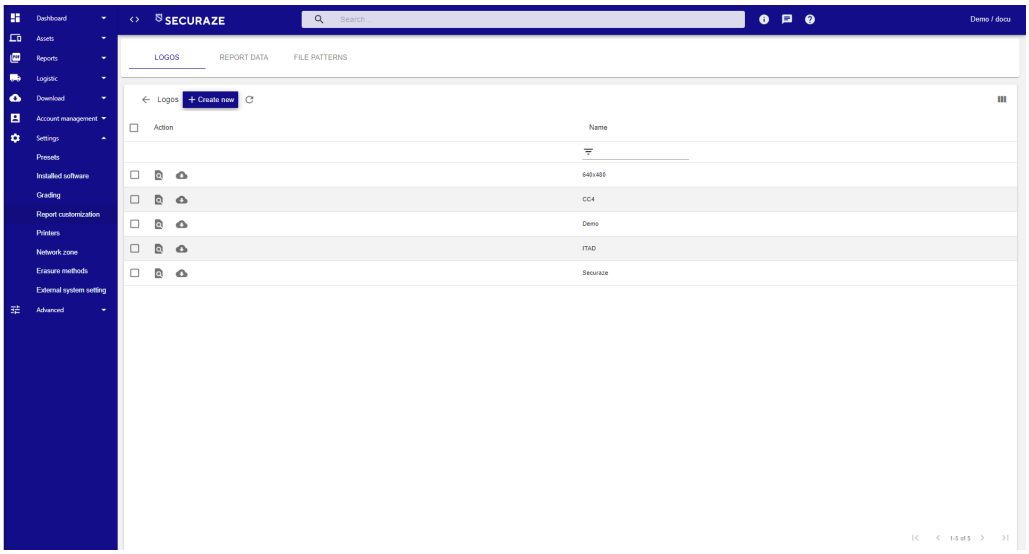


Make the desired changes and confirm them by clicking **SAVE**.

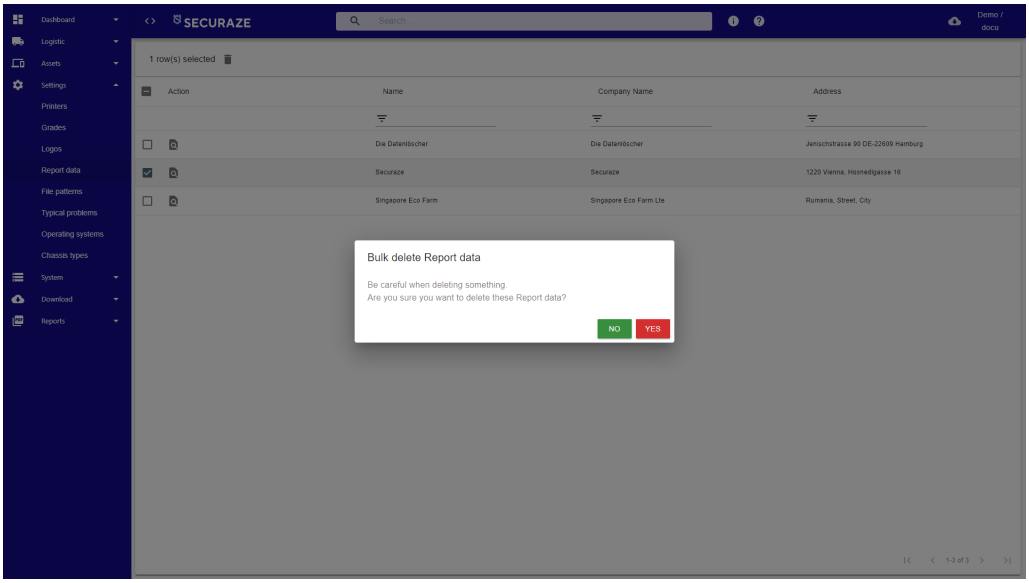


10.1.7.4.2.3 Delete Report Data

To delete report data, select the relevant report data and click **Remove all selected Report Data** .



Confirm the erasure by clicking on **YES**.

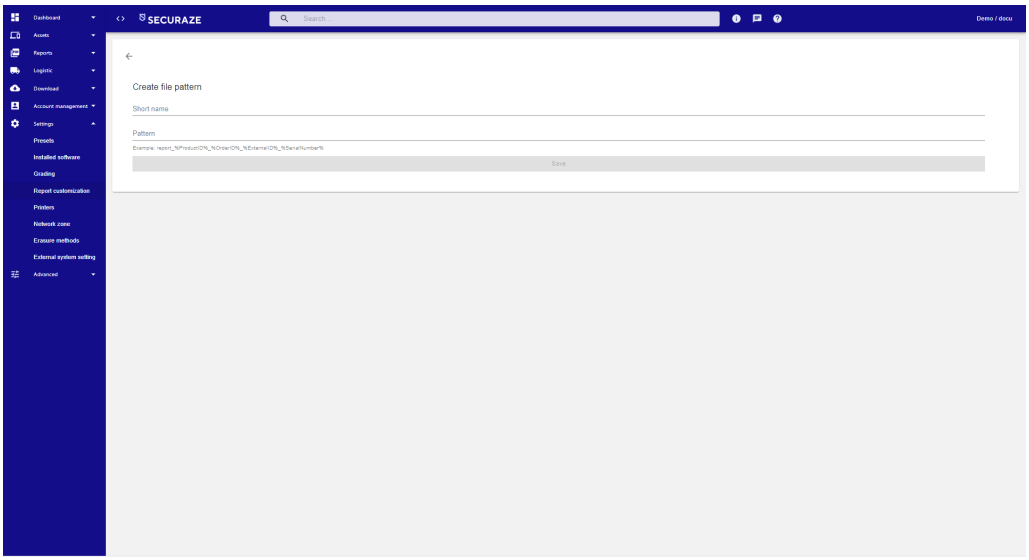


10.1.7.4.3 File Patterns

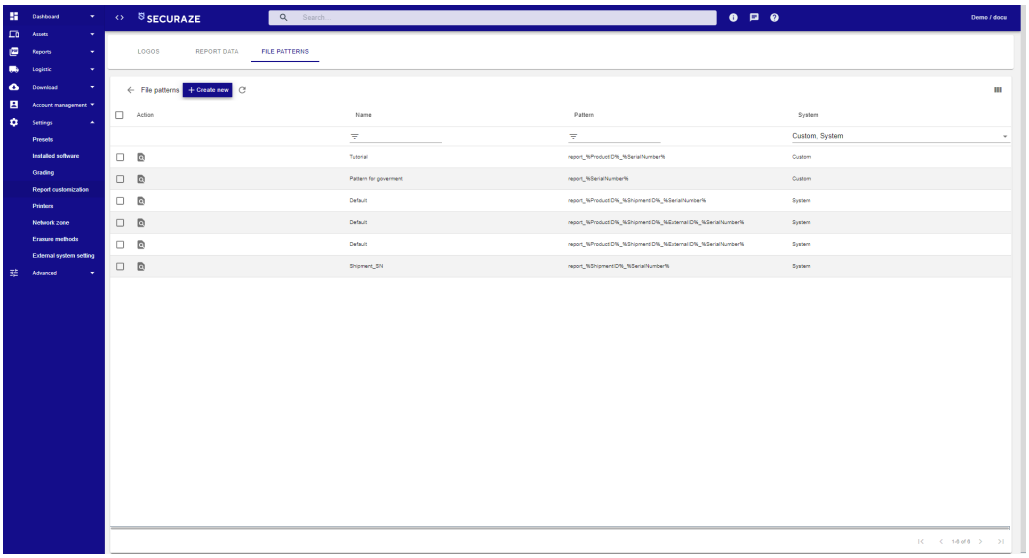
In the **Settings - Report Customization** menu, Tab **FILE PATTERNS**, you can create new file patterns, edit existing report data, and delete report data.

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.

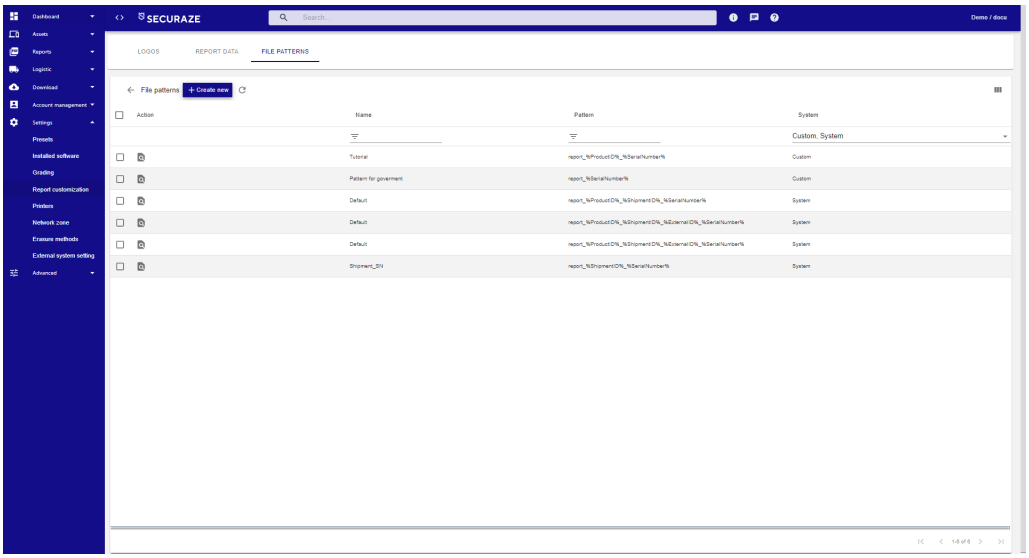


After confirming the selection by clicking **SAVE**, the newly created file pattern can be viewed in the Tab **File Pattern.**

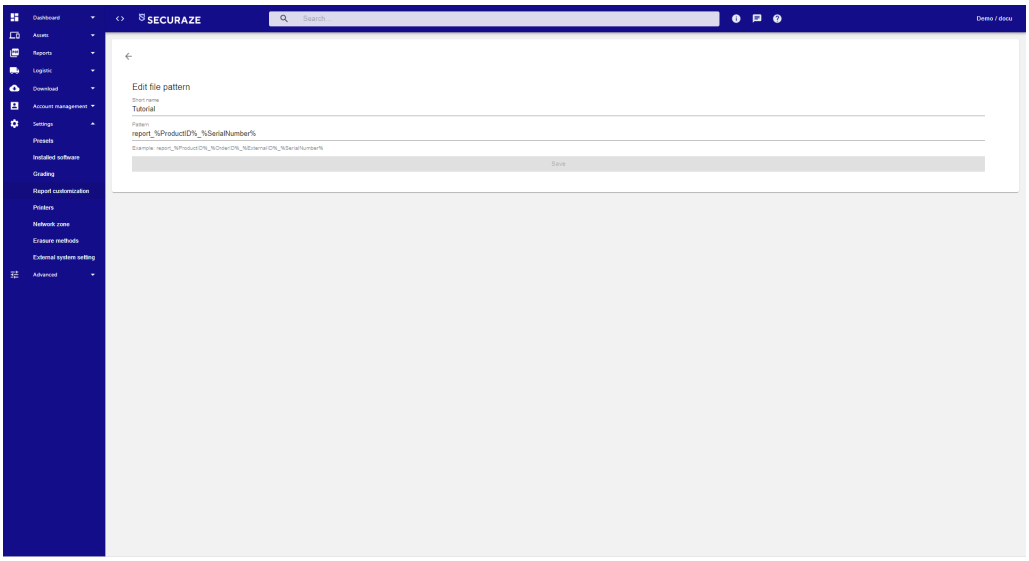


10.1.7.4.3.2 Edit File Pattern

To edit file patterns, select the respective file name patterns and click on **File Pattern details.**

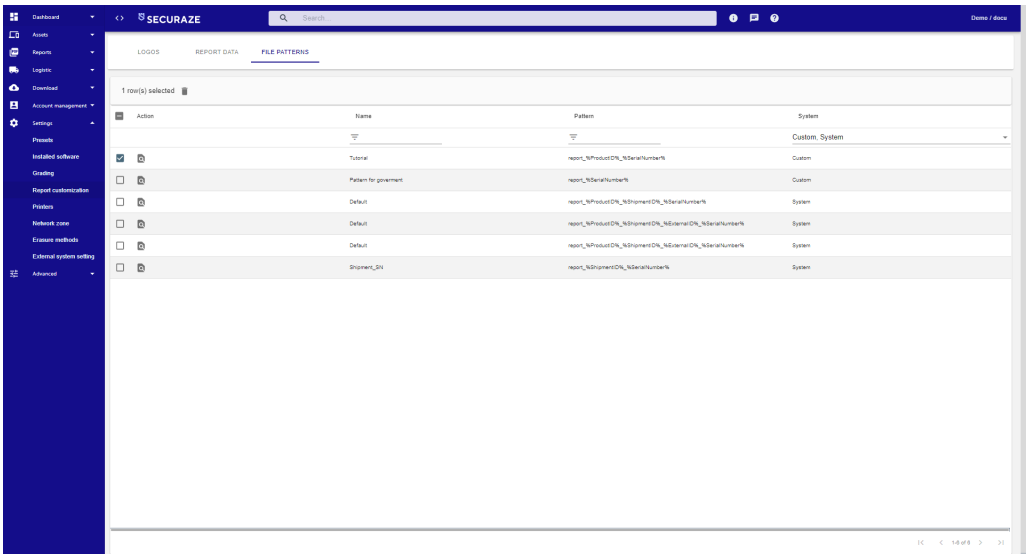


Make the desired changes and confirm them by clicking **SAVE**.

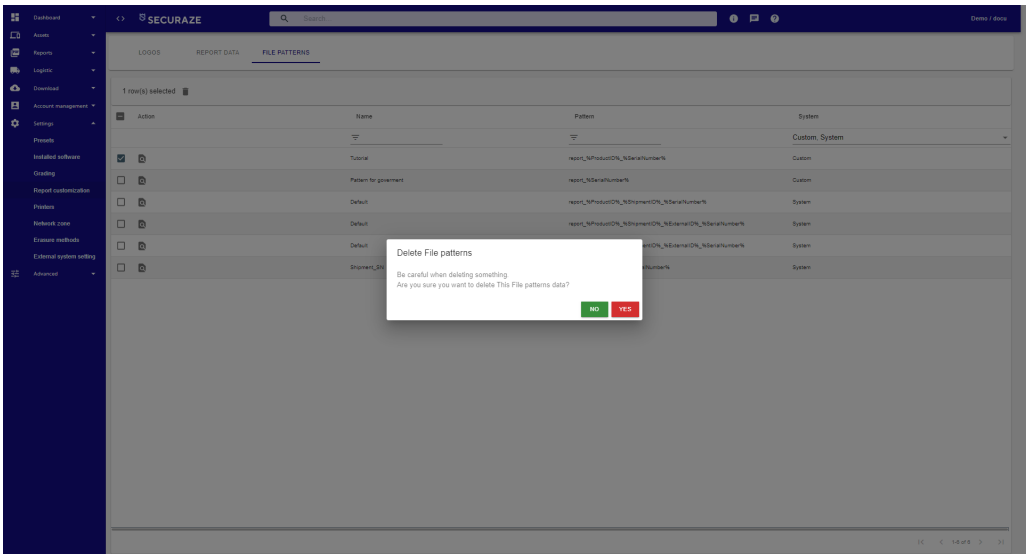


10.1.7.4.3.3 Delete File Pattern

To delete file patterns, select the file name patterns and click **Remove all selected File Pattern.**



Confirm the erasure by clicking on **YES**.



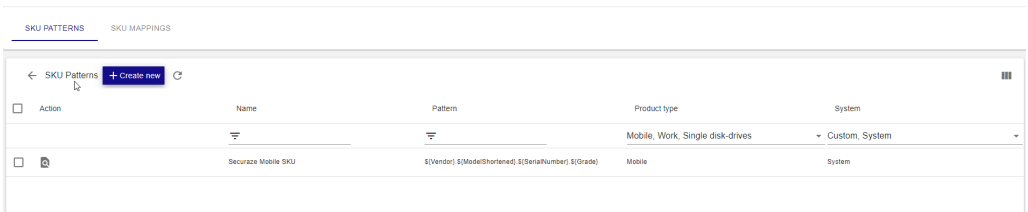
10.1.7.5 SKU

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

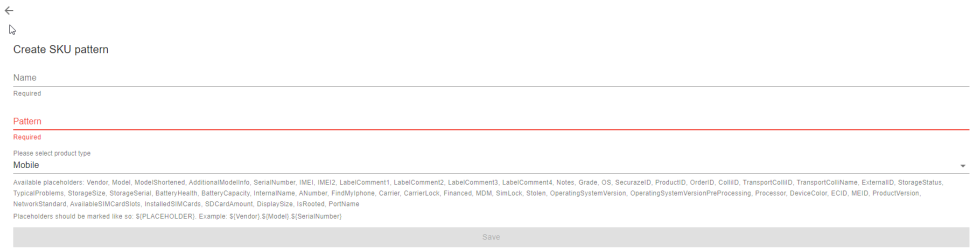
Here you can see a list of all SKU patterns.

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**.

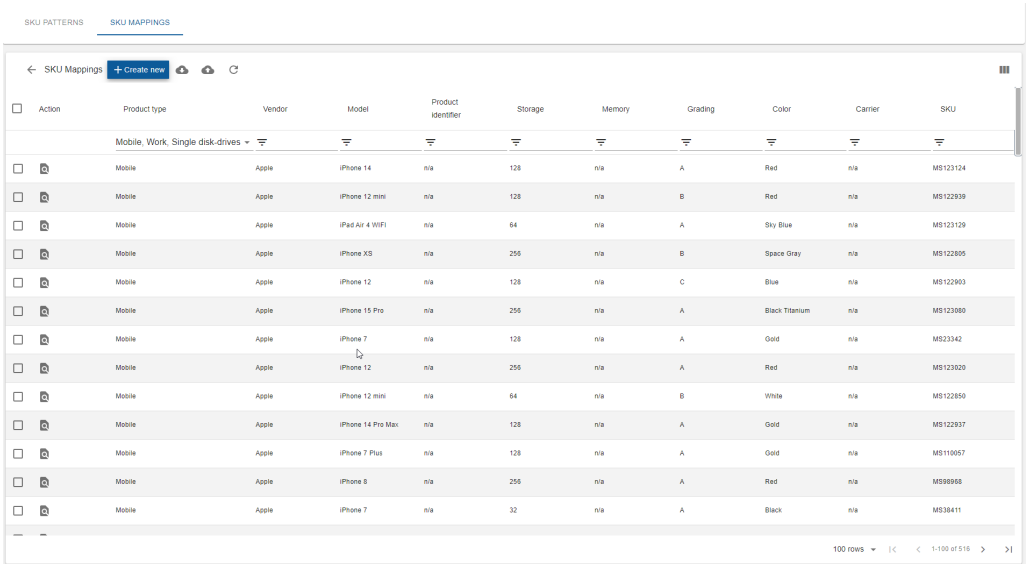
Here you enter the data of the new pattern.
After choosing a product type the list of possible usable keywords is visible.
A pattern may look like this and can use any seperator between the keywords:
${Vendor}.${ModelShortened}.${SerialNumber}.${Grade}



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:

After confirming the selection by clicking **SAVE**, the newly created grade is displayed in the **SKU Mapping** menu**.**

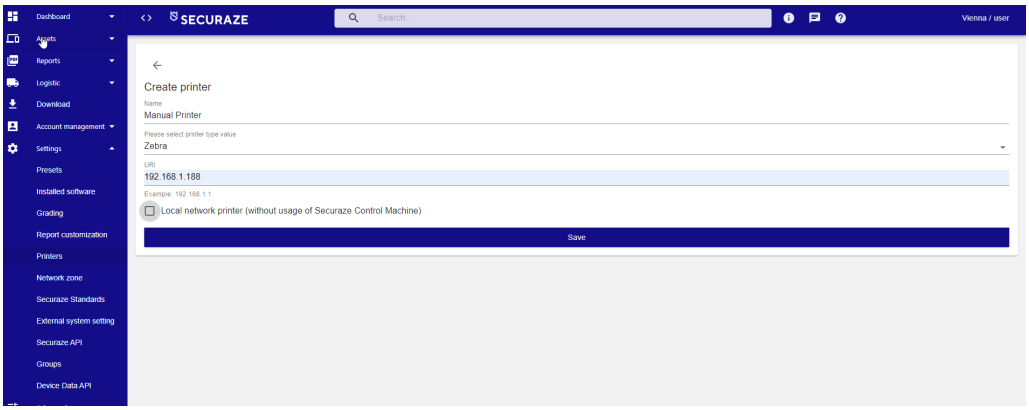
10.1.7.6 Printer

In the menu **Settings - Printers** you can create new printers, edit and delete existing ones.

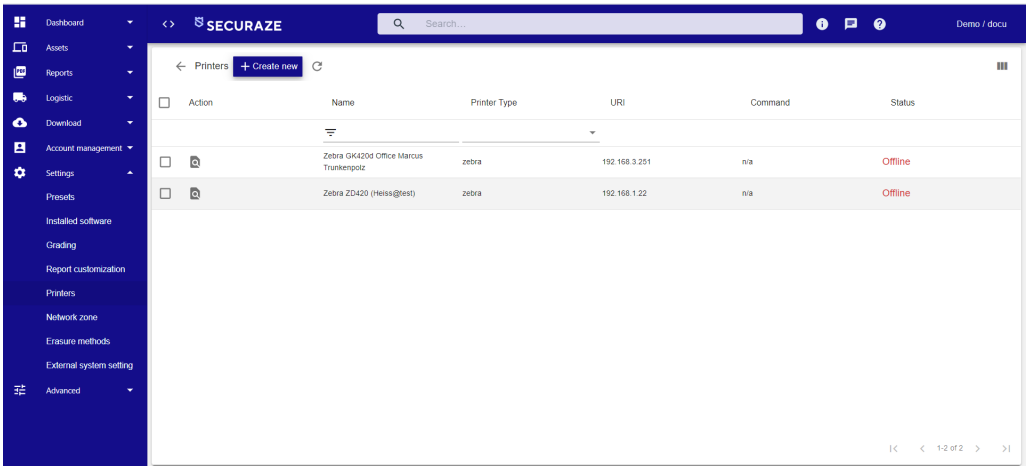
10.1.7.6.1 Creating a new printer

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**



10.1.7.6.1.1 Printer Type

Selected Godex printers are supported.

Zebra printers ZD420 and GK420 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

e.g.

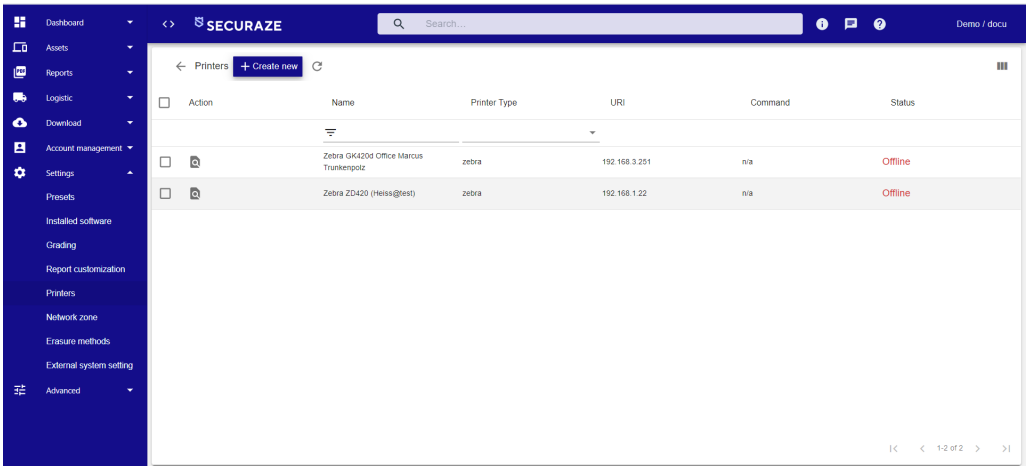
```
192.168.1.215
```

10.1.7.6.1.3 Direct connected USB printer

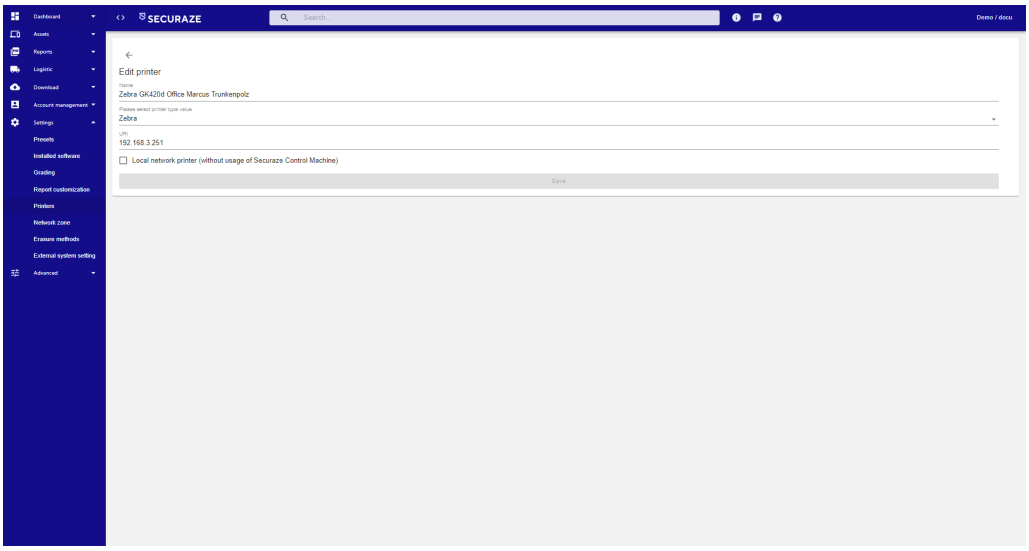
Directly connected printers.

10.1.7.6.2 Edit printer

To edit a printer, select the respective printer and click on **Printer details.**

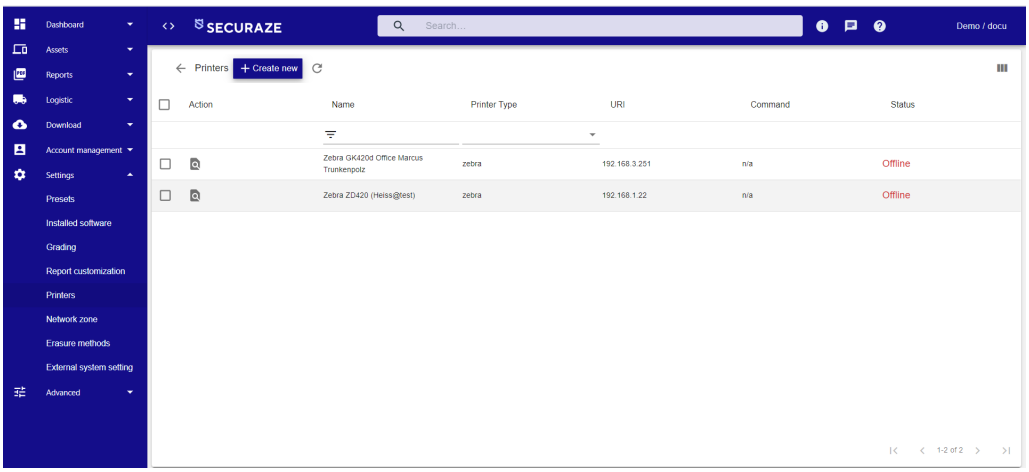


Make the desired changes and confirm them by clicking **SAVE**.

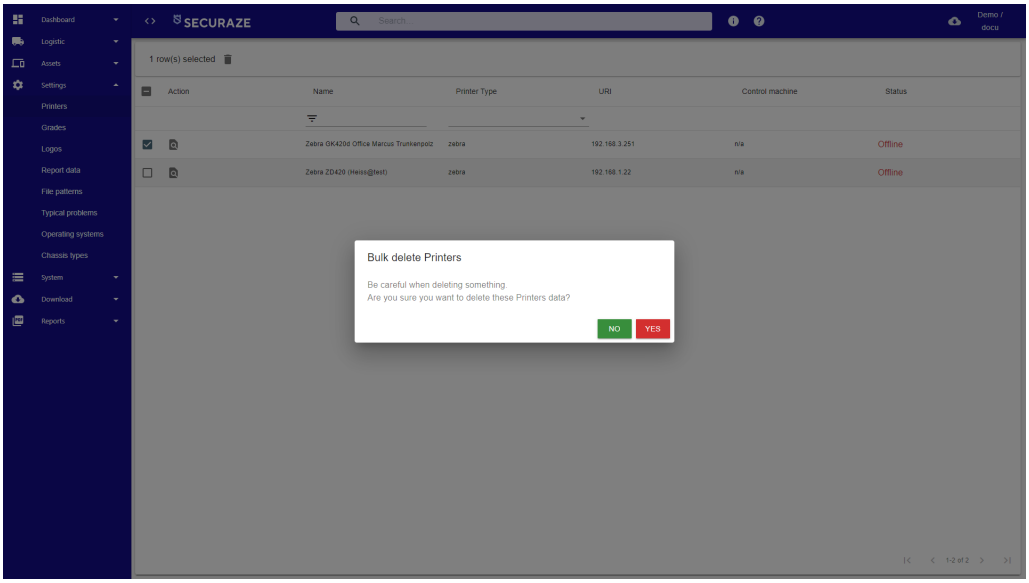


10.1.7.6.3 Delete printer

To delete a printer, select the printer and click **Remove all selected Printer**.



Confirm the erasure by clicking on **YES**.

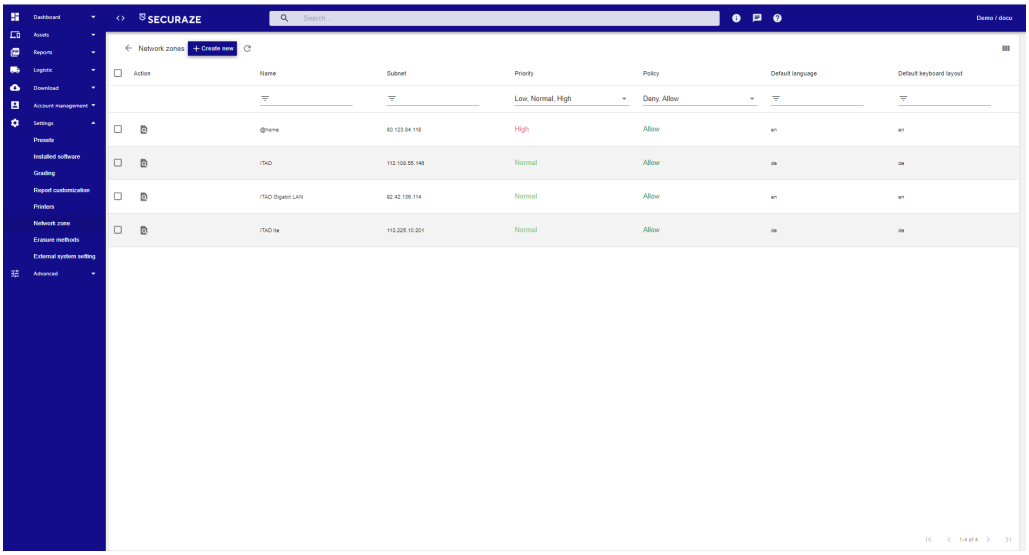


10.1.7.7 Network Zone

Creating a Network Zone has several advantages:

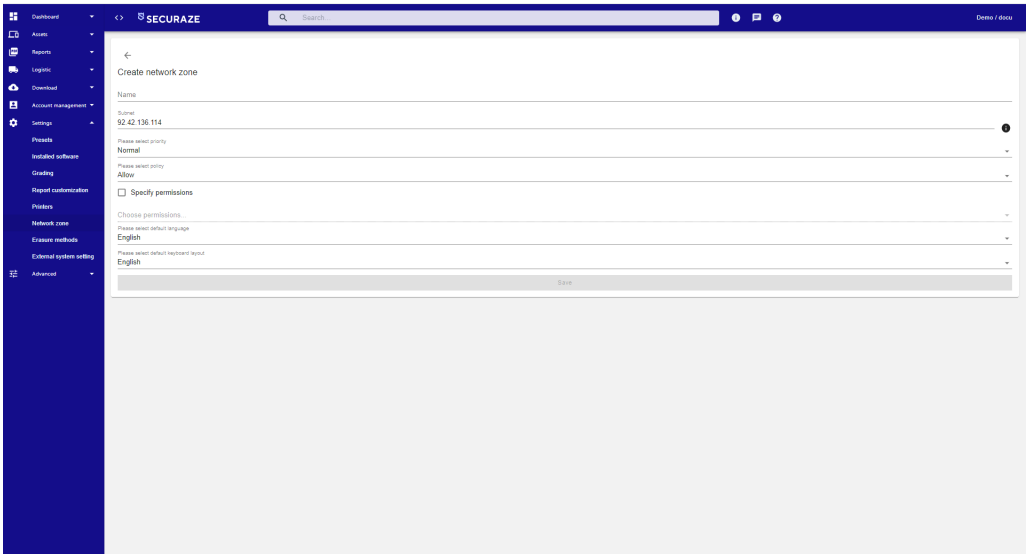
- Time saving for the operator during login process: reduce the length of the usernames. If the login happens within a network zone users can omit the namespace/domain - so instead of user@company.com / user@company-securaze-namepsace they just write "user"
- It is possible to allow or deny logins from 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.
- 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.



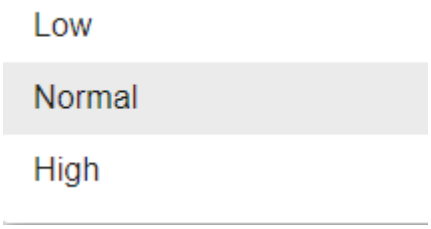
To create a new network zone, click in the Menu area on **Settings - Network Zone** and then on **Create New**.

First enter the name of the new network zone.



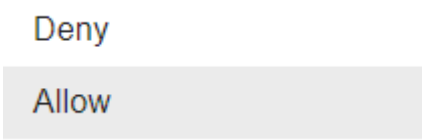
Then define the IP address or the network area including subnet of the network zone. The IP address of your external network connection is already stored here by default. Here you can see in the right area the **note**: The network zone only works properly if a static IP address or a subnet is assigned.

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:

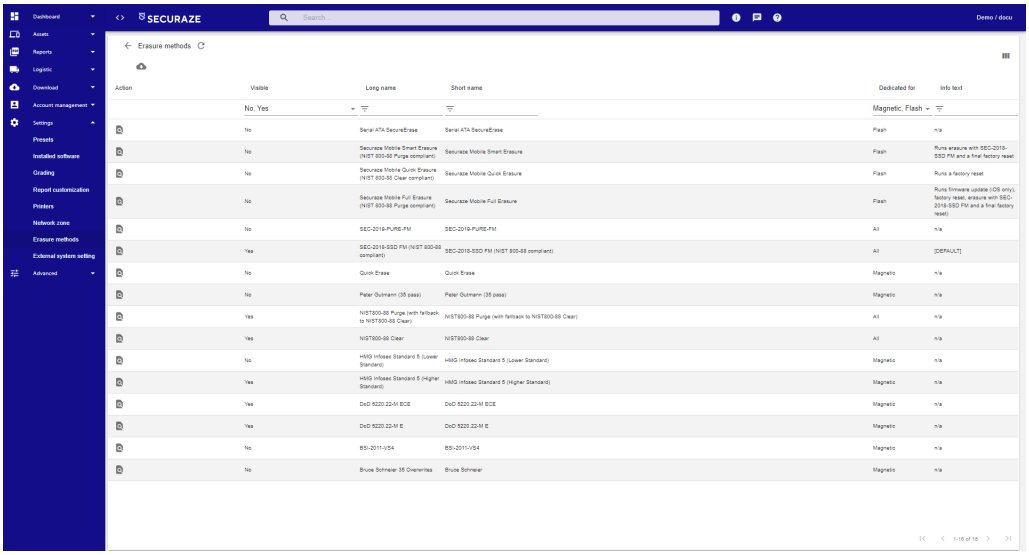


Finally, you can optionally specify permissions that should apply in this network zone. To do this, check the box **Specify permissions** and then select the desired permissions from the pull-down menu.

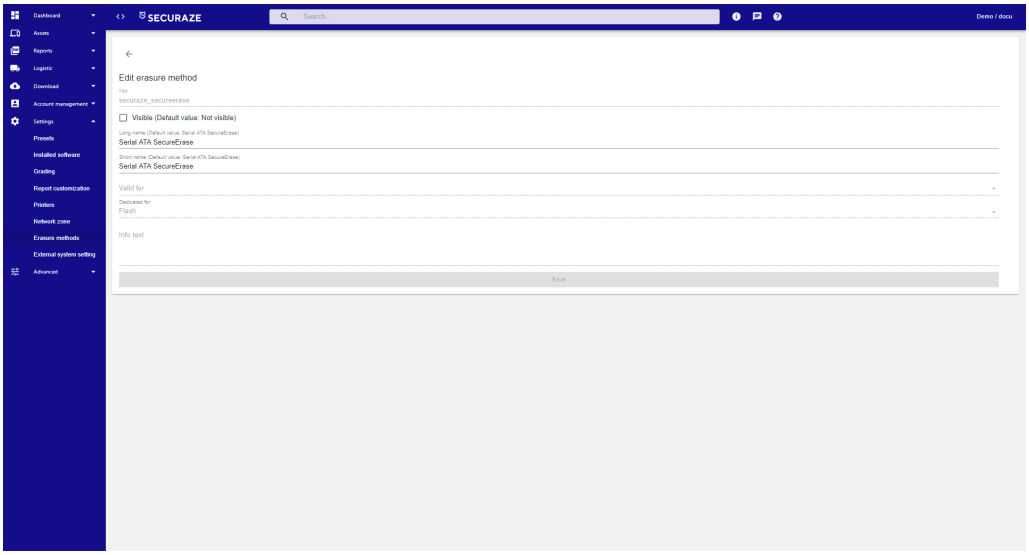
Click on **Save** in the bottom right area to confirm your entries.

10.1.7.8 Securaze Standards

Here you can see an overview of all Erasure Methods.



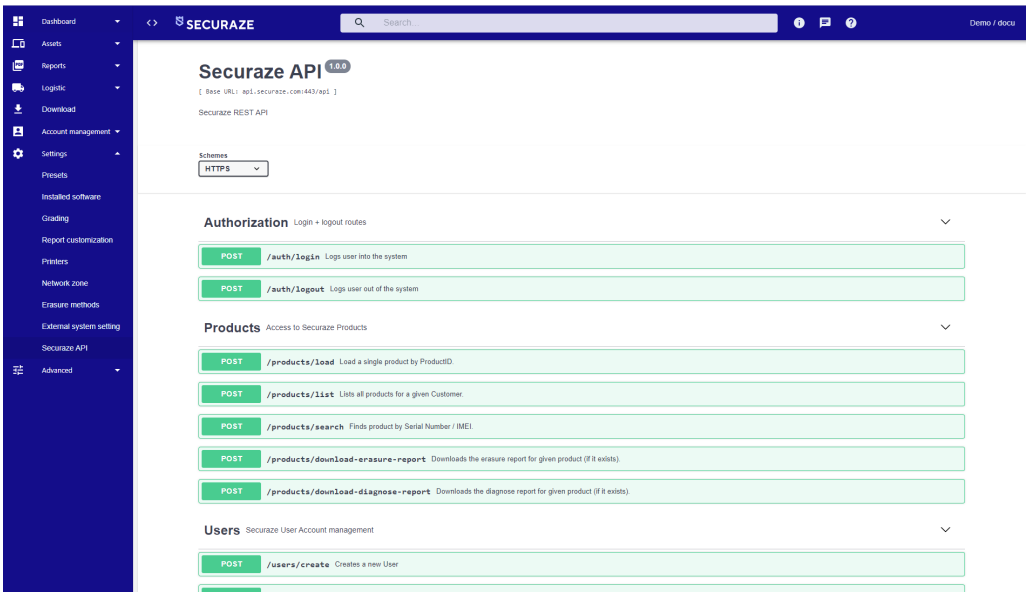
To edit an erasure method, select the respective erasure method and click **Erasure Method Details.**



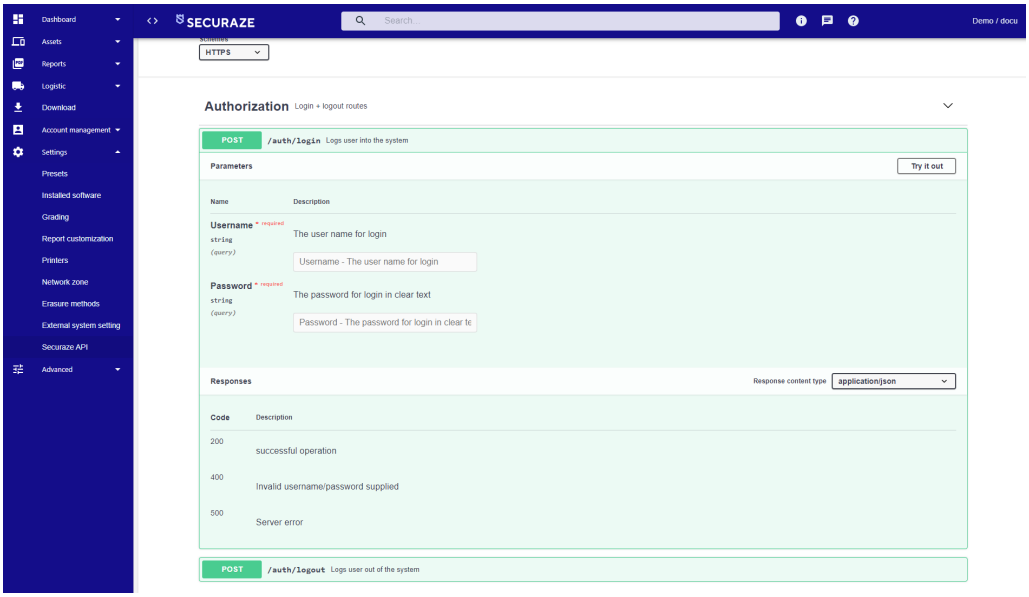
Make the desired changes and confirm them by clicking **SAVE**.

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.



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.

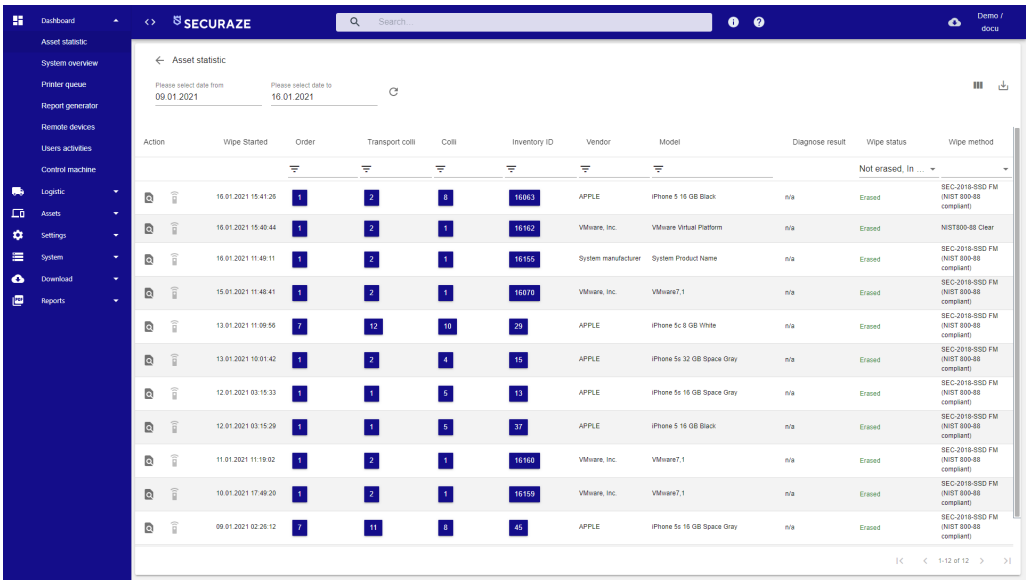
<u>There are APIs in the following categories:</u>
Authorization: Here you can login and logout.

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.

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.



Appendix

11 Appendix

11.1 Erasure Methods

The following erasure methods are currently supported.

#	Name	Main usage	Passes / Verification	Details
1	SEC-2024-SSD Performance (NIST 800-88 compliant)	ALL Default HDD+ SSD	1 pass min. 1% verification	Origin: Invented and published by Securaze Status: **Recommended, NIST 800-88 compliant** Usage: Should be used for fast and secure erasure of any SSD and HDD. Description: Invented and published by Securaze This erasure method is optimized for erasing solid-state drives (SSD) and all other flash-based storage, and can also handle traditional storage such as HDD in an optimized manner. This standard should be used for fast and secure erasure of SSDs and HDDs, as it is the best method for erasing SSDs and HDDs with minimal review. This method was invented as there was no standard for SSD erasure until then and it was highly needed. The 2021 SEC standard is a further development of the 2018 standard and has been optimized in various places to increase the speed of erasure.
2	SEC-2024-SSD Performance (3 Pass) (NIST 800-88 compliant)	ALL	3 pass min. 1% verification	Origin: Invented and published by Securaze Status: **Recommended, NIST 800-88 compliant** Usage: Should be used for secure 3 pass erasure of any SSD and HDD. Description: Invented and published by Securaze This erasure method is optimized for erasing solid-state drives (SSD) and all other flash-based storage, and can also handle traditional storage such as HDD in an optimized manner. This standard should be used for secure 3-pass SSD and HDD erasure as it is the best method for SSD and HDD erasure with minimal verification. This method was invented as there was no standard for SSD erasure until then and it was highly needed. The 2021 SEC standard is a further development of the 2018 standard and has been optimized in various places to increase the speed of erasure. . Passes:

Appendix

#	Name	Main usage	Passes / Verification	Details
				Pass 1: Format storage Pass 2: complete SEC-2018-SSD FM pass Pass 3: Format storage
3	SEC-2024-SSD 3rd Party Verifiable (NIST 800-88 Compliant)	ALL	2 pass	Origin: Invented and published by Securaze Status: **Recommended, NIST 800-88 compliant if 3rd party verification with an empty pattern is required** Usage: Should be used for fast and secure erasure of any SSD and HDD if 3rd party verification is required. Description: Uses SEC-2024-SSD Performance (NIST 800-88 compliant) for erasure and after successfull erasure overwrites the whole storage with an empty (NULL) pattern. This can be used for 3rd party verification of the erasure result. Passes: Pass 1: SEC-2024-SSD Performance (NIST 800-88 compliant) Pass 2: Write empty patterns (NULL) on the whole disk
4	SEC-2018-SSD FM (NIST 800-88 compliant)	SSD	1 pass min. 10% verification	Origin: Invented and published by Securaze Status: **Recommended, NIST 800-88 compliant** Usage: Should be used for secure erasure of any SSD. Description: Invented and published by Securaze. This solution should be used for secure SSD erasure as it is the best method for SSD erasure with balanced verification. SEC 2018-SSD FM is the proprietary SECURAZE erasure process which is optimized and suitable for the erasure of flash-based data media. This also includes the erasure of Solid State Drives (SSD). The following steps are performed: - Remove freeze lock for all disks - Reset and verify the Host Protected Area (HPA) - Reset and verify the Device Configuration Overlay (DCO) - Reset and verify the Remapped sectors - Write and verify verification patterns at specific locations before and after each run - Remove file system

Appendix

#	Name	Main usage	Passes / Verification	Details
				- Run Secure Erase (ES) and Secure Erase Advanced (ESA) firmware levels - Write and verify encrypted data stream on the entire disk All the above steps are performed in a single pass. Verification is performed after the run. 10% of the total addressable memory is read and compared with the data written in the last pass. A successful verification includes the following steps: - The written data must be readable from the data carrier without errors. - The amount of data read must match the amount of data written exactly. - The read data must be identical in content to the written data. To achieve an optimal erasure result, additional actions which go beyond SEC 2018-SSD FM have been implemented. - Final pass: To prevent erasure artifacts after successful erasure and verification, all addressable locations are finally overwritten with binary zeros. - Monitoring of reads and writes during passes: In order to detect faulty devices at an early stage and to keep the resulting delays as low as possible, all read and write processes are monitored. When a parameterizable threshold value is reached, the deletion is aborted with an error and a failed deletion is noted on the deletion report.
5	DoD 5220.22-M E	HDD	3 pass	Origin: Published by the U.S. Department of Defense (DoD) Status: **Avoid** Usage: Should be avoided and only used to fulfill specific customer needs. No secure erasure of SSDs possible. Passes: Pass 1: Overwrite with binary zeroes. Pass 2: Overwrite with binary ones (the compliment of the above). Pass 3: Overwrite with a random pattern, Verify the final overwrite pass.
6	DoD 5220.22-M ECE	HDD	7 pass	Origin: Published by the U.S. Department of Defense (DoD)

Appendix

#	Name	Main usage	Passes / Verification	Details
				Status: **Avoid** Usage: Should be avoided and only used to fulfill specific customer needs. No secure erasure of SSDs possible. Description: Extension of the DoD 5220.22-M standard. Passes: Pass 1-3: complete DoD 5220.22-M pass Pass 4: Overwrite with a random pattern. Pass 5-7: complete DoD 5220.22-M pass
7	BSI-2011-VS4	HDD	2 pass	Origin: Original standard of the BSI (Federal Office for Information Security) Status: **Avoid** Usage: Should only be used to fulfill specific customer needs. No secure erasure of SSDs possible. Passes: Pass 1: Overwrite with a random pattern. Pass 2: Overwrite with a random pattern.
8	Quick Erase / One Pass Zeros	HDD	1 pass	Origin: None Status: **Avoid** Usage: Should only be used to fulfill specific customer needs. No secure erasure of SSDs possible. Passes: Pass 1: Overwrite with a random pattern.
9	NIST 800-88 Clear	ALL	1 pass min. 10% verification	Origin: Published by the U.S. government. Status: **Recommended if suitable for usage** Usage: Should be used when protection against simple, non-invasive data recovery techniques and a moderate level of data protection is sufficient. Published by the U.S. Government. Description: NIST 800-88 is a U.S. government document that provides methodical guidance for erasing data from electronic storage media. Its aim is the effective sanitization of media to ensure that all data is irretrievably deleted once the data or storage medium has reached the end of its life.

Appendix

#	Name	Main usage	Passes / Verification	Details
				This erasure method was originally published for government use, but has gained acceptance in the private sector as the best way to ensure that data is removed from a disk when that data is transferred from a more secure to a less secure environment. This method uses standard read/write commands, techniques, and tools in order to overwrite all user-addressable storage locations with binary 1s and 0s, including logical file storage locations on an ATA hard disk or SSD. This method should be used when protection from simple, non-invasive data recovery techniques and a moderate level of data protection is sufficient. This standard can be used for floppy disks, disk drives, ATA hard drives, SCSI drives and flash media (USB sticks, memory cards, SSDs) The advantage of Clear is that storage media can be reused, reducing e-waste, and most devices support some level of Clear Sanitization. Compliance with NIST Guidelines 246 Passes: Pass 1: Apply logical erasure techniques, followed by 10% verification
10	NIST 800-88 Purge (with fallback to NIST800-88 Clear)	ALL	1 pass (+1 pass) min. 10% verification	Origin: Published by the U.S. government Status: **Recommended** Usage: Should be used when a more exhaustive level of erasure is required and for more confidential data. Published by the U.S. Government Description: NIST 800-88 is a U.S. government document that provides methodical guidance for erasing data from electronic storage media. Its aim is the effective sanitization of media to ensure that all data is irretrievably deleted once the data or storage medium has reached the end of its life. This erasure method was originally published for government use, but has gained acceptance in the private sector as the best way to ensure that data is removed from a disk when that data is transferred from a more secure to a less secure environment. This sanitization method includes overwrite, block erase, and cryptographic erase as logical techniques for cleaning up ATA hard disk drives and SSDs. This process should be used when a more comprehensive level of erasure is required and for more confidential data.

#	Name	Main usage	Passes / Verification	Details
				This method can be used for hard disk drives (ATA, SCSI), flash media (USB sticks, memory cards, SSDs). The advantage of this standard is also that the storage media can be reused, which reduces electronic waste. The Purge standard offers a higher level of media sanitization than Clear and is therefore used when handling more confidential data. Compliance with NIST Guidelines 246 Passes: Pass 1: Apply logical or physical erasure techniques, followed by 10% verification. (optional) Pass 2: If NIST 800-88 Purge fails it will fallback to NIST 800-88 Clear
11	NIST800-88r1 Purge (required Purge level, without fallback to Clear)	ALL	1 pass (+1 pass) min. 10% verification	Origin: Published by the U.S. government Status: **Recommended** Usage: Should be used when a more exhaustive level of erasure is required and Purge level must be reached. Passes: Pass 1: Apply logical or physical erasure techniques, followed by 10% verification.
12	NIST800-88r1 (3 pass)	ALL	3 pass	Origin: Invented and published by Securaze, uses NIST 800-88 compliant erasure Status: **Recommended if suitable for usage** Usage: Should be used when 3 pass time optimized NIST 800-88 compliant erasure is required Description: Invented and published by Securaze. NIST 800-88 is a U.S. government document that provides methodical guidance for erasing data from electronic storage media. Its aim is the effective sanitization of media to ensure that all data is irretrievably deleted once the data or storage medium has reached the end of its life. NIST 800-88 Rev. 1 is the most recent update to NIST 800-88 and is one of the most widely used standards for data sanitization required by the U.S. federal government. Its use has spread to numerous private companies and organizations. Uses NIST 800-88-compliant erasure and should be used when 3-turnaround time-optimized NIST 800-88-compliant erasure is required.

Appendix

#	Name	Main usage	Passes / Verification	Details
				Passes: Pass 1: Format storage Pass 2: complete SEC-2018-SSD FM pass Pass 3: Format storage
13	Peter Gutmann (35 Pass)	HDD	35 pass	Origin: Invented and published by Peter Gutmann Status: **Avoid** Usage: Should only be used to fulfill specific customer needs. No secure erasure of SSDs possible. Passes: 35 Passes with different random and fixed patterns
14	HMG Infosec Standard 5 (Lower Standard)	HDD	2 pass	Origin: Published by the British government Status: **Avoid** Usage: Should only be used to fulfill specific customer needs. No secure erasure of SSDs possible. Passes: Pass 1: Overwrite with binary zeroes. Pass 2: Overwrite with a random pattern, Verify the final overwrite pass.
15	HMG Infosec Standard 5 (Higher Standard)	HDD	3 pass	Origin: Published by the British government Status: **Avoid** Usage: Should only be used to fulfill specific customer needs. No secure erasure of SSDs possible. Passes: Pass 1: Overwrite with binary zeroes. Pass 2: Overwrite with binary ones (the compliment of the above). Pass 3: Overwrite with a random pattern, Verify the final overwrite pass.
16	Serial ATA SecureErase	ALL	1 pass	Origin: Provided by storage vendors Status: **Avoid** Usage: Erasure of SSDs possible, but fully relies on vendor algorithms.

Appendix

#	Name	Main usage	Passes / Verification	Details
				Passes: Pass 1: Run vendor firmware command Secure Erase
17	SEC-2019-PURE-FM	SSD	1 pass	Origin: Invented and published by Securaze Status: **Recommended if suitable for usage** Usage: Should be used for secure erasure of any SSD and HDD if no further vendor firmware functionality should be used.
18	Bruce Schneier	HDD	7pass	Origin: Invented and published by Bruce Schneier Status: **Avoid** Usage: Should only be used to fulfill specific customer needs. No secure erasure of SSDs possible. Passes: Pass 1: Overwrite with binary ones. Pass 2: Overwrite with binary zeroes. Pass 3-7: Overwrite with a random pattern.
19	NCSC-TG-025	HDD	3 pass	Origin: Invented and published by the US National Security Agency Status: **Avoid** Usage: Should be avoided and only used to fulfill specific customer needs. No secure erasure of SSDs possible. Passes: Pass 1: Overwrite with binary zeroes + verify. Pass 2: Overwrite with binary ones (the compliment of the above) + verify. Pass 3: Overwrite with a random pattern, Verify the final overwrite pass + verify.
20	IEEE 2883-2022 Clear	ALL	1 pass min. 5% verification	Origin: Published by Institute of Electrical and Electronics Engineers (IEEE) Status: **Recommended if suitable for usage** Usage: This sanitization method employs logical approaches to eliminate all accessible data from user-addressable storage locations, excluding hidden or non-addressable areas. It offers a moderate level of data protection by preventing straightforward, non-invasive data recovery attempts through software. Most devices are compatible with some form of Clear sanitization, maintaining their usability while safeguarding data. The standard is available for purchase through IEEE website as a downloadable PDF.

Appendix

#	Name	Main usage	Passes / Verification	Details
21	IEEE 2883-2022 Purge	ALL	1 pass (+1 pass) min. 10% verification	Origin: Published by Institute of Electrical and Electronics Engineers (IEEE) Status: **Recommended if suitable for usage** Usage: This technique involves either logical or physical methods to eradicate all data, rendering it inaccessible even to experts employing advanced laboratory data recovery techniques. Although it makes data recovery practically impossible, both the storage media and device can still be repurposed for future use. The standard is available for purchase through IEEE website as a downloadable PDF.
21	IEEE 2883-2022 Purge Strict	ALL	1 pass (+1 pass) min. 100% verification	Origin: Published by Institute of Electrical and Electronics Engineers (IEEE) Status: **Recommended if suitable for usage** Usage: Same as IEEE 2883-2022 Purge but enforces 100% verification of the erased data. The standard is available for purchase through IEEE website as a downloadable PDF.

11.2 NIST Guidelines

In December 2014, the US-based National Institute of Standards and Technology (NIST) updated their guidelines for sanitizing media to include requirements and released the NIST Special Publication 800-88 Revision 1.

When it comes to sanitization, NIST describe two processes to achieve different levels of security:

- Clear (an erasure process that protects against non-invasive data recovery methods)
  NIST 800-88 is a U.S. government document that provides methodical guidance for erasing data from electronic storage media. Its aim is the effective sanitization of media to ensure that all data is irretrievably deleted once the data or storage medium has reached the end of its life.
  This erasure method was originally published for government use, but has gained acceptance in the private sector as the best way to ensure that data is removed from a disk when that data is transferred from a more secure to a less secure environment.
  This method uses standard read/write commands, techniques, and tools in order to overwrite all user-addressable storage locations with binary 1s and 0s, including logical file storage locations on an ATA hard disk or SSD.
  This method should be used when protection from simple, non-invasive data recovery techniques and a moderate level of data protection is sufficient.
  This standard can be used for floppy disks, disk drives, ATA hard drives, SCSI drives and flash media (USB sticks, memory cards, SSDs)
  The advantage of Clear is that storage media can be reused, reducing e-waste, and most devices support some level of Clear Sanitization.

- Purge (for higher security, to protect against laboratory data recovery)
  NIST 800-88 is a U.S. government document that provides methodical guidance for erasing data from electronic storage media. Its aim is the effective sanitization of media to ensure that all data is irretrievably deleted once the data or storage medium has reached the end of its life.
  This erasure method was originally published for government use, but has gained acceptance in the private sector as the best way to ensure that data is removed from a disk when that data is transferred from a more secure to a less secure environment.
  This sanitization method includes overwrite, block erase, and cryptographic erase as logical techniques for cleaning up ATA hard disk drives and SSDs.
  This process should be used when a more comprehensive level of erasure is required and for more confidential data.
  This method can be used for hard disk drives (ATA, SCSI), flash media (USB sticks, memory cards, SSDs).
  The advantage of this standard is also that the storage media can be reused, which reduces electronic waste.
  The Purge standard offers a higher level of media sanitization than Clear and is therefore used when handling more confidential data.

The following tables show how the NIST requirements are supported by Securaze.Details regarding the individual NIST guideline are available here NIST Special Publication 800-88 Revision 1.

SSD

Type	Clear	Purge
ATA	Validated overwrite	Block Erase, Cryptographic Erase or Secure Erase
SCSI / SAS	Validated overwrite	Block Erase, Cryptographic Erase or Clear
NVMe	Validated overwrite	Format, Cryptographic Erase or Clear
eMMC	Validated overwrite	Block Erase, Cryptographic Erase or Clear
USB Removable Media	Validated overwrite	Not available
Memory cards	Validated overwrite	Not available

HDD

Type	Clear	Purge
ATA	Validated overwrite	Block Erase, Cryptographic Erase or Secure Erase
SCSI / SAS	Validated overwrite	Block Erase, Cryptographic Erase or Clear

Securaze erasure methods compliance with NIST Guidelines

SEC-2024-SSD Performance (1 Pass and 3 Pass)
In case of an successful erasure "SEC-2024 Performance" will exceed NIST Clear security level.

SEC-2018-SSD FM (NIST 800-88 compliant)
In case of an successful erasure "SEC-2018-SSD FM" will exceed NIST Clear security level.

NIST 800-88 Purge
In case of an successful erasure NIST Purge security level will be achieved.

NIST 800-88 Purge (with fallback to NIST800-88 Clear)
In case NIST Purge fails, automatically a fallback erasure to NIST Clear will be applied.

NIST 800-88 Clear
In case of an successful erasure NIST Clear security level will be achieved.

11.3 Erasure Duration

Some examples for average erasure durations.

SSD

Vendor	Device	Storage	Size	Method	Duration
Apple	MacBook Pro 13-Inch Early 2015	APPLE SSD SM0128G	128 GB	SEC-2024-SSD Performance	~ 6 minutes
Lenovo	T430S	INTEL SSDSC2BW18	128 GB	SEC-2024-SSD Performance	~ 9 minutes
Apple	MacBook Pro (13", 2019	APPLE SSD AP0128N	128 GB	SEC-2024-SSD Performance	~ 9 minutes
HP	Z4 G4 Workstation	OCZ-Vertex3	256 GB	SEC-2024-SSD Performance	~ 9 minutes
Lenovo	T470S	INTEL SSDSC2BW18	256 GB	SEC-2024-SSD Performance	~ 16 minutes
Dell	Latitude E7450	SAMSUNG SSD PM87	256 GB	SEC-2024-SSD Performance	~ 21 minutes
HP	EliteBook 840 G3	LITEON CV1-8B256	256 GB	SEC-2024-SSD Performance	~ 22 minutes
Apple	MacBook Pro (16", 2019)	APPLE SSD AP0512N	512 GB	SEC-2024-SSD Performance	~ 12 minutes
Lenovo	ThinkPad T460	SAMSUNG MZ7TY128	512 GB	SEC-2024-SSD Performance	~ 19 minutes
Apple	MacBook Pro (13", 2019	APPLE SSD AP1024M	1 TB	SEC-2024-SSD Performance	~ 17 minutes
Apple	MacBook Pro (13", 2020)	APPLE SSD AP1024N	1 TB	SEC-2024-SSD Performance	~ 25 minutes
Apple	MacBook Pro (15", 2016)	APPLE SSD SM2048L	2 TB	SEC-2024-SSD Performance	~ 42 minutes
Dell	Precision 7510	Samsung SSD 870 Evo	2 TB	SEC-2024-SSD Performance	~ 79 minutes
HP	ProLiant DL380 Gen10	KIOXIA NVMe SSD Controller Cx6	960 GB	IEEE 2883-2022 Purge	~ 38 minutes
HP	ProLiant DL380 Gen10	Intel NVMe Datacenter SSD P4500	3 TB	IEEE 2883-2022 Purge	~4 hours
HP	ProLiant DL380 Gen10	KIOXIA NVMe SSD Controller Cx6	4 TB	IEEE 2883-2022 Purge	~ 2:30 hours
HP	ProLiant DL380 Gen10	Samsung NVMe SSD SM961	4 TB	IEEE 2883-2022 Purge	~ 3:30 hours
HP	ProLiant DL380 Gen10	Micron Technology Disk SSD	8 TB	IEEE 2883-2022 Purge	~ 5 hours
Samsung	Galaxy TabPro S	LITEON -8B128	128 GB	SEC-2018-SSD FM	~ 10 minutes
Lenovo	ThinkPad T430s	INTEL SSDSC2BW18	180 GB	SEC-2018-SSD FM	~ 10 minutes
Dell	Precision 7510	SAMSUNG SSD SM87	256 GB	SEC-2018-SSD FM	~ 10 minutes
Dell	Latitude E6540	ADATA A SSD DP900	256 GB	SEC-2018-SSD FM	~ 13 minutes
Dell	Latitude 5480	Toshiba SSD	256 GB	SEC-2018-SSD FM	~ 15 minutes
HP	EliteBook 850 G6	Toshiba SSD	512 GB	SEC-2018-SSD FM	~ 35 minutes
Dell	Precision T1650	Samsung SSD 840	500 GB	SEC-2018-SSD FM	~ 45 minutes
HP	Elite x2 1012 G2	Toshiba SSD	1 TB	SEC-2018-SSD FM	~ 45 minutes

HDD

Vendor	Device	Storage	Size	Method	Duration
HP	EliteBook 8570p	TOSHIBA MQ01ACF0	320 GB	SEC-2024-SSD Performance	~ 55 minutes

Appendix

Vendor	Device	Storage	Size	Method	Duration
Apple	iMac (21,5", Mid 2014)	APPLE HDD HTS545	500 GB	SEC-2024-SSD Performance	~ 90 minutes
Apple	iMac (4K, 21,5", 2015)	APPLE HDD HTS541	1 TB	SEC-2024-SSD Performance	~ 3:30 hours
Acer	Aspire 5715Z	Hitachi HTS54251	160 GB	DoD 5220.22-M E	~ 2 hours
HP	ProBook 640 G1	WDC WD3200LPLX-6	320 GB	DoD 5220.22-M E	~ 3 hours
HP	ProBook 6470b	HGST HTS725032A7	320 GB	NIST800-88 Clear	~ 1 hours
HP	ProBook 640 G1	Seagate ST320LM010-1KJ15	320 GB	NIST 800-88r1 3 Pass	~ 45 minutes
HP	ProBook 6470b	HGST HTS725032A7	320 GB	NIST 800-88r1 3 Pass	~ 1 hours
HP	ProBook 440 G4	WDC WD5000LPLX-6	500 GB	NIST800-88 Clear	~ 2 hours
HP	ProDesk 400 G2	ST1000DM003-1E	1 TB	DoD 5220.22-M E	~ 5 hours
MSI	Server	HGST HMS5C4040BL	4 TB	NIST 800-88r1 3 Pass	~9 hours
MSI	Server	24 x HGST HMS5C4040BL	4 TB	NIST 800-88r1 3 Pass	~15 hours

Please find details on our Securaze erasure method SEC-2024-SSD Performance in the chapter Erasure Methods 237.

Appendix

Erasure Method duration comparison

SSD

Storage	Size	SEC-2024-SSD Performance	SEC-2018-SSD FM	NIST800-88 Clear
INTEL SSDSC2BW18	180 GB	9 minutes	10 minutes	11 minutes
INTEL SSDMCEAF18	180 GB	17 minutes	18 minutes	20 minutes
SAMSUNG SSD PM87	256 GB	20 minutes	22 minutes	22 minutes
LITEON CV1-8B256	256 GB	22 minutes	24 minutes	24 minutes
LITEON CV5-8Q256	256 GB	22 minutes	26 minutes	26 minutes

HDD

Storage	Size	SEC-2024-SSD Performance	SEC-2018-SSD FM	NIST800-88 Clear	DoD 5220.22-M E
TOSHIBA MQ01ACF0	320 GB HDD	55 minutes	1:14 hours	1:14 hours	2:30 hours
Seagate ST320LM010-1KJ15	320 GB HDD	45 minutes	1:00 hour	1:30 hours	3:04 hours

11.4 External BIOS Boot Up Keys

BIOS bootup settings:

Acer.
Once the power button on the device is pressed, either hold or continuously press the F2 key along with the Del (delete) key. If using an older model, either hold the F1 key or the combination of Ctrl (Control)+ Alt (alternate) + Esc (escape)

Dell
Once the power button on the device is pressed, either hold or continuously press the F2 key.

Chromebook
Once the power button on the device is pressed, either hold or continuously press the L+ Ctrl key. - (May Vary depending on the make/model)

HP
Once the power button on the device is pressed, either hold or continuously press the F10 key.

Lenovo

Once the power button on the device is pressed, continuously select the F1 key approximately 10-15 times.

Toshiba
Once the power button on the device is pressed, either hold or continuously press the F2 key.

Furthermore, you will find the Apple key shortcuts for DFU (Device Firmware Update) and recovery mode.

Apple

a. Hold the power button until an Apple logo appears on the screen. Once the logo is displayed, release the power and immediately hold the ‘Command’ and ‘R’ keys. This will direct one to the recovery mode.
b. For ‘DFU’ mode, ensure that the power supply is off. Press and hold the power for one second, while you're still holding the power press Ctrl+option+R-Shift as well. Hold all four keys while the Mac turns on, and off again. When it is turned off, release the Ctrl+Option+R-Shift while still holding the power. After around 10 seconds, you should be in DFU now, and can release the power button. If the display remains black, it is in ‘DFU’ mode.
c. (***Note***) The three keys that indicate direction are referring to either the left or right side of the keyboard.
d. To boot from an external drive (MAC erasure) Press and hold the power until the apple logo appears. Once the logo is present, release the power button and hold down the ‘Option’ key.

11.5 QR Codes Work Dongle Chromebook Erasure

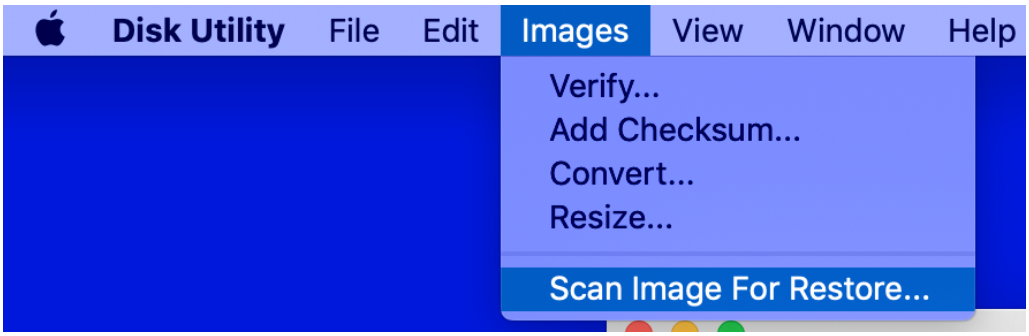
Start Erasure

Enter External Data

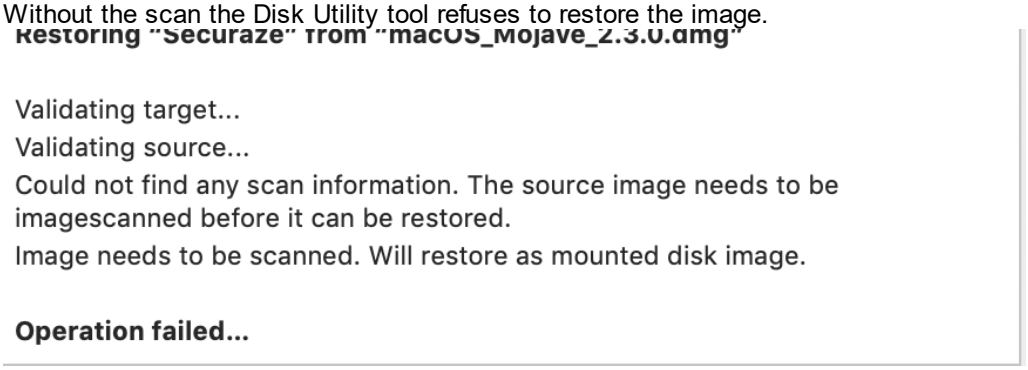
Enter Employee ID

11.6 DiskCreator (macOS)

Preparations: Pendrive
Generate a USB stick with the macOS image using the macOS Disk Utility. (Attention! The USB stick needs to be 32GB or larger.)
macOS BigSur currently can't generate macOS Images, any predecessor like Mojave is needed to generate the pendrive.
Copy the Securaze macOS Image to local storage and start the Disk Utility application. In the Images menu, run Scan Image for Restore, select the downloaded image, and scan it.

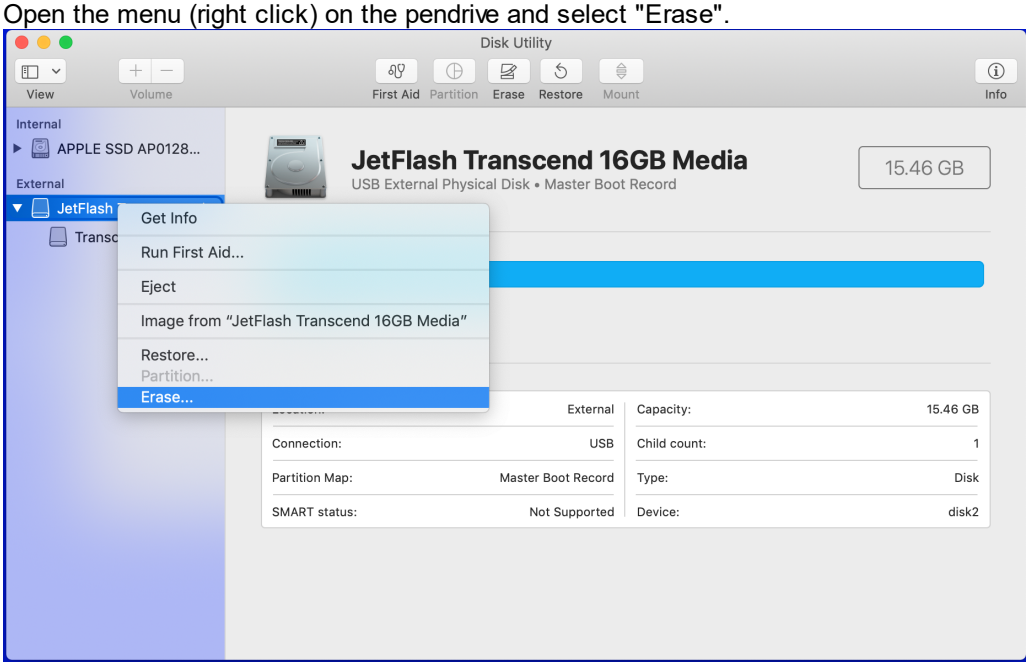


Without the scan the Disk Utility tool refuses to restore the image.

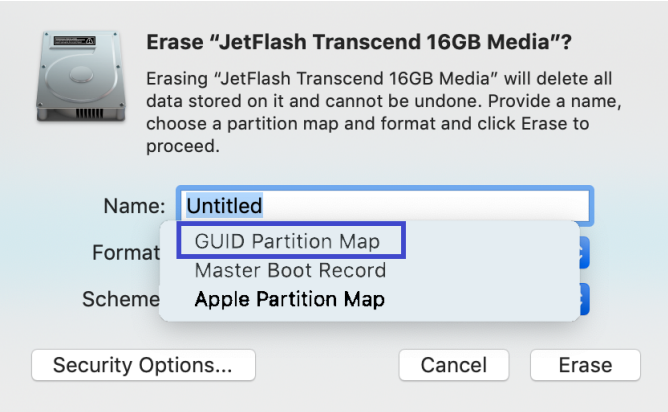


Plug-in the USB stick, which should hold macOS including Securaze Work.
Please make sure View -> Show All Devices" is checked. Otherwise the created scheme does not appear.

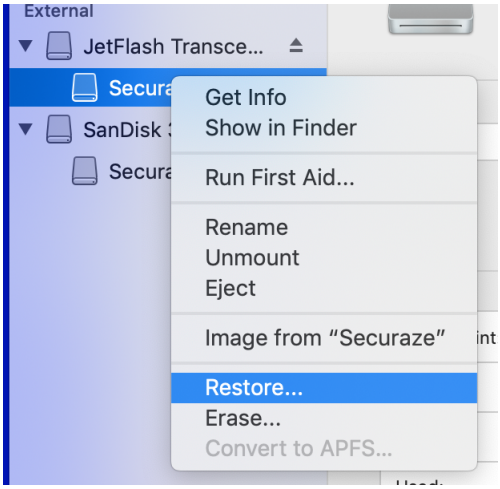
Open the menu (right click) on the pendrive and select "Erase".



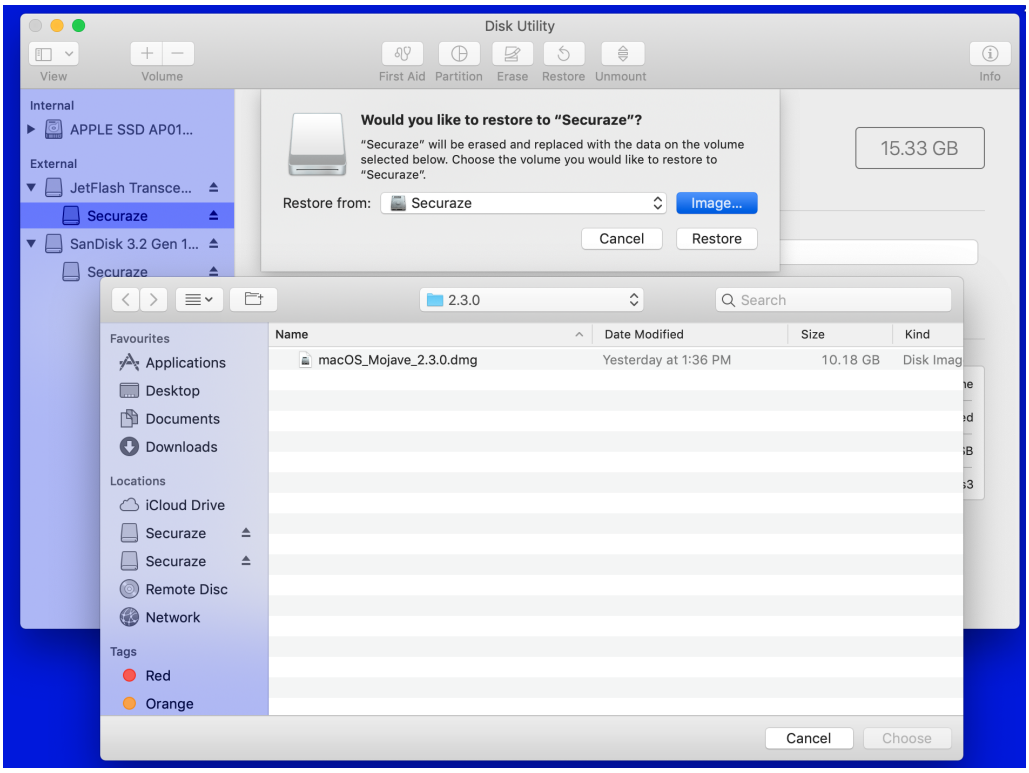
Choose a meaningful name such as "Securaze macOS Mojave" and select "GUID Partition Map" as the format.
Choose "macOS Extended (Journaled)" as the scheme.



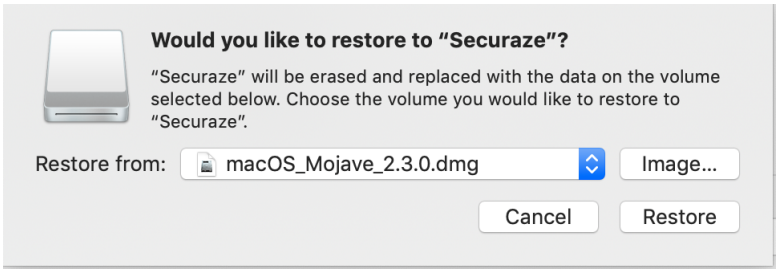
Start the deletion with "Erase" and close the confirmation dialog.
Open the menu on the newly created partition with your specified name and select "Restore".



Select the previously downloaded and scanned Securaze macOS image.



Press "Restore" to start the recovery process. This can take up to 15 minutes, depending on the speed of the used USB stick / SSD.



After the restore is finished it is ready for usage.