Securaze Creator

SECURAZE

Table of Contents

1. Securaze Creator 5
1.1 Creating a bootable USB drive 8
1.2 Managing licenses for offline use 12
1.3 Customizing a drive 13
Index 0

© 2026 Securaze GmbH

Securaze Creator

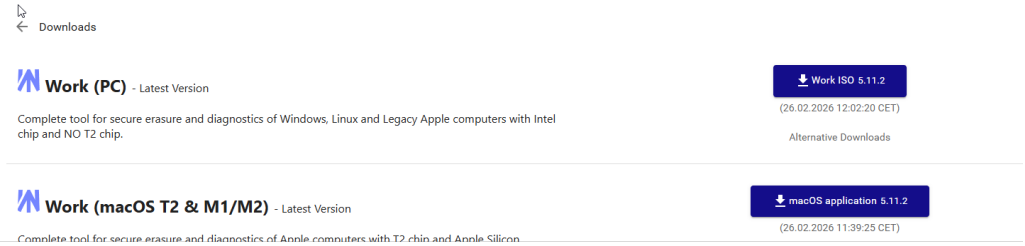
1 Securaze Creator

Securaze Creator is an application that turns USB flash drives / SD cards into bootable Securaze Work drives. With Securaze Creator you can burn the Securaze image, apply your settings and add licenses for offline use to several drives at once – **all in one run**. It is available for Windows and macOS (both Intel and Apple Silicon Macs are supported).

Step 1: Download the Securaze Work image

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: Download and install Securaze Creator

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



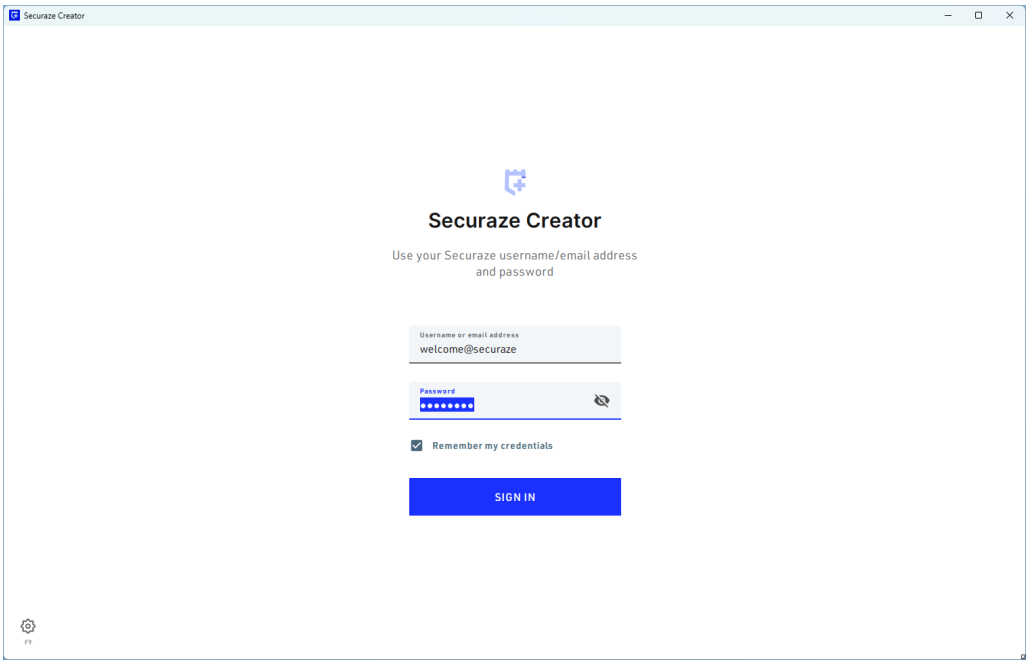
Start the download by clicking on the corresponding button. Securaze Creator will be downloaded to your system and installed.

Note for macOS: when you burn a drive for the first time, macOS will ask you to install the Securaze Creator helper. Confirm the prompt with your administrator credentials – this is required so that Securaze Creator is allowed to write images to USB drives.

Signing in

Open Securaze Creator and log in with your Securaze username / email address and password. Enable **Remember my credentials** if you want Securaze Creator to fill in your credentials the next time you start it.

© 2026 Securaze GmbH



The settings are already accessible on the login screen via the settings icon (F9) in the lower left corner. There you can change the language of the user interface and the URL of the backend server (we advise you not to change this setting unless you are told otherwise by your Administrator).

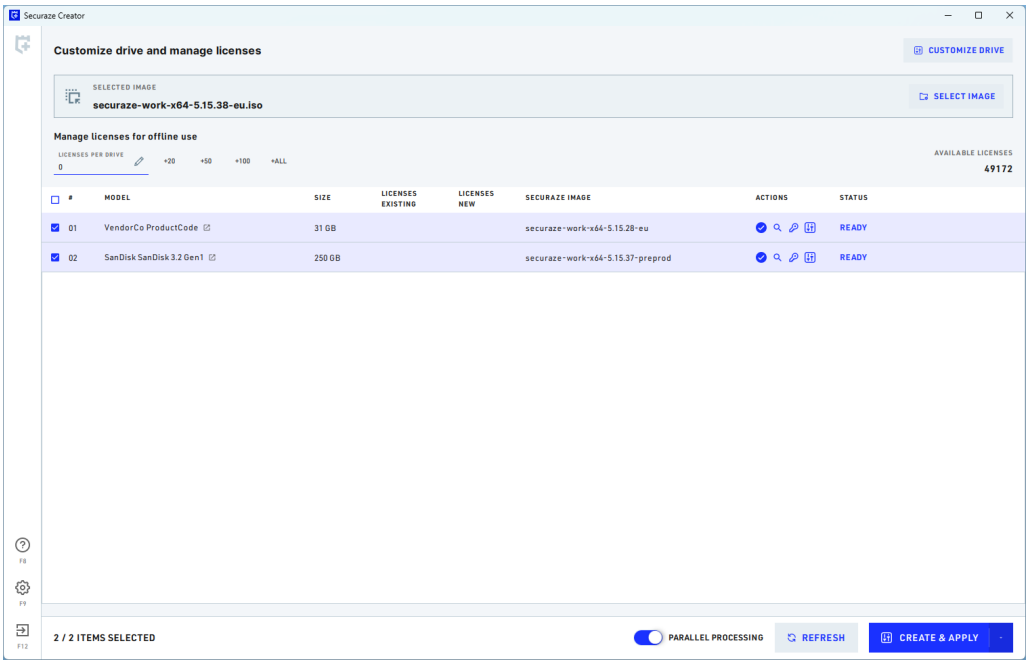
If you need assistance, you can also start a remote support session (**Start remote session**) from Securaze Creator, which allows the Securaze support team to view your screen.

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

The dashboard

Everything is done from a single dashboard: at the top you select the Securaze image and your drive settings, below it you define the licenses per drive, and the table shows all detected USB drives / SD cards. Drives are detected and refreshed automatically – there is no need to unplug and replug them.

© 2026 Securaze GmbH



• **SELECTED IMAGE** – the Securaze image that will be burned. Click **SELECT IMAGE** or simply drag & drop the ISO file onto the card.

• **CUSTOMIZE DRIVE** – opens the settings that will be applied to the drives (see Customizing drives 13).

• **SAVE AS ISO** - writes the settings into a copy of the selected image, an ISO file for virtual machines, servers or archiving, instead of onto a drive (see Creating bootable USB drives 8).

• **Manage licenses for offline use** – the number of licenses that will be added per drive (see Managing licenses for offline use 12).

• **Drive table** – all detected drives with size, existing/new licenses, the Securaze image currently on the drive and the status.

• **PARALLEL PROCESSING** – processes all selected drives at the same time.

The preferred way of working is one single run: choose the image, set your settings, optionally add offline licenses – and click **CREATE & APPLY**. How to do this is described in Creating bootable USB drives 8.

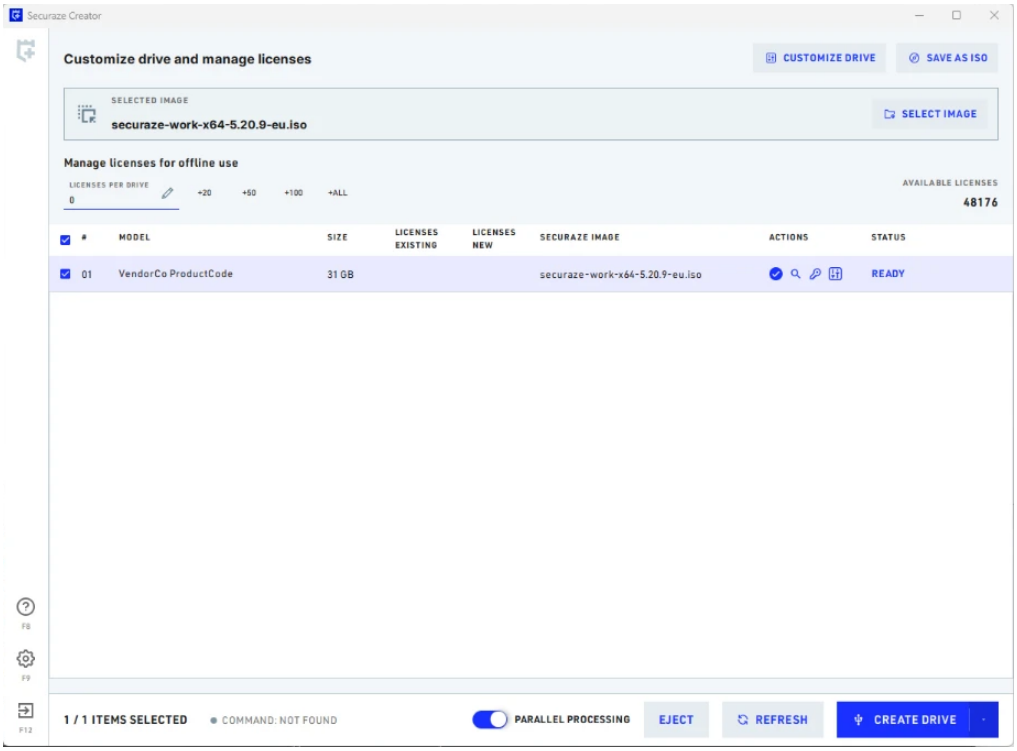
Securaze Creator remembers the settings you used: when you start it again, the last used image, settings and license selection are preloaded, so recurring runs only take a few clicks.

1.1 Creating a bootable USB drive

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

© 2026 Securaze GmbH

The preferred way: everything in one run



Plug in the USB drives / SD cards you want to use. They will appear in the drive table and are selected automatically. A drive you untick stays unticked.

Then:

1. Select the Securaze image you previously downloaded: click **SELECT IMAGE** or drag & drop the ISO file from the Windows Explorer / Finder onto the image card.

2. Optionally click **CUSTOMIZE DRIVE** and configure language, auto-login, Wi-Fi and workflows (see Customizing drives 13).

3. Optionally set the number of licenses per drive for offline use (see Managing licenses for offline use 12).

4. Click **CREATE & APPLY**. To write the settings into an ISO file instead of onto drives, see "Saving the image with your settings as an ISO" below.

Creating a drive erases it completely, so Securaze Creator asks first. The question - for example **Erase and create 2 drives?** - lists every drive that is about to be erased, with its name and size. **ERASE & CREATE ALL** starts (**ERASE & CREATE** for a single drive); **CANCEL** stops before anything is written. **CREATE DRIVE** asks the same question.

If you create drives all day, you can switch the question off: open **Options & Settings** with the settings icon (F9) at the bottom of the left sidebar, and on the **General** tab switch off **Ask before creating a drive**. Securaze Creator remembers this; **CREATE & APPLY** and **CREATE DRIVE** then start at once. **RESTORE STICK** still asks.

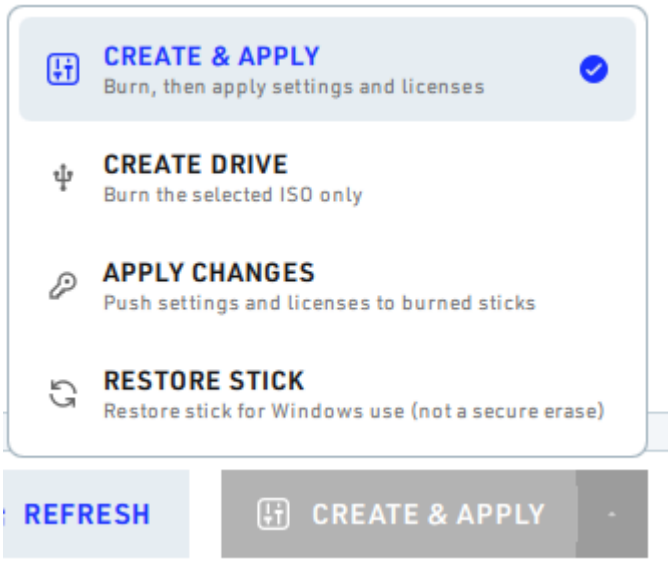
© 2026 Securaze GmbH

Securaze Creator will burn the image and then apply your settings and licenses to all selected drives in one pass. You can follow the progress per drive in the **STATUS** column. With **PARALLEL PROCESSING** enabled, all selected drives are processed simultaneously.

Please note that in case you already used a USB drive / SD card to burn a 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.

Working in separate steps

If you prefer, each step can also be done separately. Click on the arrow next to the **CREATE & APPLY** button to choose the action:



• **CREATE & APPLY** – burn, then apply settings and licenses (default).

• **CREATE DRIVE** – burn the selected ISO only.

• **APPLY CHANGES** – push settings and licenses to already burned drives, without burning again.

• **RESTORE STICK** – restore a drive for normal Windows use (this is a quick restore, not a secure erase).

When the work is finished, EJECT releases the selected drives so they can be unplugged safely; Securaze Creator confirms which drives are safe to unplug, or says if a drive could not be released.

The drives are rescanned automatically after each action, so you can apply further changes right away – there is no need to unplug and replug the drives.

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

© 2026 Securaze GmbH

Saving the image with your settings as an ISO

Instead of onto a USB drive, Securaze Creator can write your settings into a copy of the Securaze Work image: **SAVE AS ISO**, next to **CUSTOMIZE DRIVE** at the top of the dashboard. The result is an ISO file that starts Securaze Work with the settings a drive created with **CREATE & APPLY** would carry. The image you selected stays unchanged.

Use an ISO where a USB drive does not fit:

• virtual machines - start the virtual machine from the ISO;

• servers - mount the ISO as virtual media in the server's remote management, or start it from a boot server that boots ISO images over the network;

• a CD/DVD, or a USB drive written with another tool;

• archiving - keep a configured image for later, or for another site.

To save an ISO:

1. Select the Securaze Work image (**SELECT IMAGE**). **SAVE AS ISO** is grayed out until an image is selected.

2. Set the settings with **CUSTOMIZE DRIVE** and click **CONFIRM** (see Customizing drives 13).

3. Click **SAVE AS ISO**, choose a folder and a file name and save. The ending .iso is added if it is missing.

4. The button shows **SAVING ISO... n%** while Securaze Creator first reads the image and then copies it. A line below the button then says **Saved:** with the path of the new ISO - or, in red, why no ISO was made. If you close Securaze Creator during the copy, the copy stops and no unfinished file is left behind.

What goes into the ISO:

• The settings of **CUSTOMIZE DRIVE**, as on a drive - including Shopfloor mode, the time zone, the stored sign-in and Wi-Fi details, the erasure settings and the Windows reimaging mode. The ISO carries the stored credentials just as a drive does, so keep it as carefully as a configured drive.

• No offline licenses: an ISO cannot hold licenses. A machine started from it has to sign in - online, or to your local Securaze server - before it erases. For erasing without a connection, create a USB drive with licenses (see Managing licenses for offline use 12).

• No workflow files from the Workflows tab - Creator says so when you save an ISO with workflow files chosen. Stations started from the ISO use the workflows promoted in the Dashboard once they are signed in.

• No Windows setup from the Windows tab - only whether Windows may encrypt the drive by itself.

A saved ISO can be configured again: select it as the image, change the settings and save it under a new name. The new settings replace the ones in it.

© 2026 Securaze GmbH

When no ISO can be made, the line below the button says why:

• **The settings are switched off - switch them on in Customize drive first.** - switch on **Enable/disable all settings** on the General tab of **CUSTOMIZE DRIVE**.

• **An image cannot carry the Windows setup. Clear the Windows setup in Customize drive, or burn a stick instead.** - clear the fields of the Windows tab you filled in, or create a USB drive, which carries the Windows setup.

• **These settings are too long for the start line of the image (... of ... characters). Shorten the profile name, description or notes.** - the settings travel in the image's start line, which has a fixed length. Shorten the texts named; a custom standard with many settings takes room too.

• **These settings do not fit the image's place for them (... of ... bytes).** - shorten the settings as above.

• **This image has no place for settings: it was built before Save as ISO existed. Use a newer Work image.** - download the current Securaze Work image and select it.

• **Choose another name: the image cannot be written over itself.** - the file chosen is the selected image itself; save under another name or in another folder.

• **The image cannot be read: ... / The copy cannot be written: ... / The copy cannot be renamed to ...** - check that the image is still there, that the target folder is writable and has enough free space, and that no other program has a file of that name open.

Booting from the drive

To continue to the 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 the chapter "External BIOS Boot Up Keys" of this manual to find the key for your brand).

Select the USB drive you want to boot from.

Your computer will now boot and start Securaze Work.

1.2 Managing licenses for offline use

To erase devices offline (without a connection to the Securaze backend), you can add erasure licenses to your drives. This is done directly on the dashboard, in the section **Manage licenses for offline use**.

The number of **AVAILABLE LICENSES** of your account is displayed on the right, so that you are able to see the maximum number of licenses you can add.

© 2026 Securaze GmbH

In the field **LICENSES PER DRIVE** you can type in the number of licenses you wish to add to each selected drive, use the buttons "**+20**", "**+50**", "**+100**", or click "**+ALL**" to instantly add all available licenses.

The drive table shows the **LICENSES EXISTING** on each drive and the **LICENSES NEW** that will be added.

The licenses are written to the drives together with the image and settings when you click **CREATE & APPLY**, or on their own via the action **APPLY CHANGES** (see Creating bootable USB drives 8).

Existing license vaults on a drive are shown together with their **expiration date**. Licenses added for offline use are valid for a limited number of days; after the expiration date the licenses can no longer be used for offline erasure and have to be allocated again.

Please note: licenses that are still on a drive are transferred back to the account that was used for creating that drive as soon as the drive is burned or restored again.

1.3 Customizing a drive

Click **CUSTOMIZE DRIVE** to configure the settings that are written onto the drives - or into an ISO with **SAVE AS ISO** (see Creating bootable USB drives 8). The dialog has nine tabs: **General**, **Automation**, **Workflows**, **Erasure**, **Machine**, **Windows**, **Server & Storage**, **Login** and **Network**.

A setting left at its default leaves the station's own behavior in place. Settings marked **Use the preset** take what the preset in the Securaze Dashboard says.

Profiles

A set of settings can be saved under a name and reused. The name is entered in the **Profile name** field at the top of the dialog; if profiles are already saved, an arrow beside the field opens the list to load one.

• **SAVE AS NEW** stores the current settings under the name entered. It appears once the name does not belong to an existing profile.

• **RENAME** appears when a loaded profile is given a different name, and writes the settings and the new name onto it.

• **DELETE** removes the saved profile of that name. It happens immediately and without a confirmation; the settings on screen stay as they are.

A loaded profile keeps your changes: **CONFIRM** also saves them into that profile, as long as its name in **Profile name** has not been changed.

If you change a loaded profile and then load another one, the question **Keep the changes?** appears. **KEEP THEM** saves the changes into the profile you are leaving, **DROP THEM** discards them; then the other profile is loaded.

© 2026 Securaze GmbH

Exporting and importing a profile

With **EXPORT PROFILE** and **IMPORT PROFILE** at the bottom left of the dialog, a saved profile goes into a file (*.json) and back - for example to set up Securaze Creator on another computer with the same settings, or to keep a copy.

• **EXPORT PROFILE** is available when the name in **Profile name** is a saved profile. The file holds that profile as it was last saved.

• The passwords are left out of the file: the sign-in password (Login), the Wi-Fi password (Network), and the Wi-Fi password and the product key of the Windows setup (Windows). The message **Exported - without the sign-in and Wi-Fi passwords.** confirms the export.

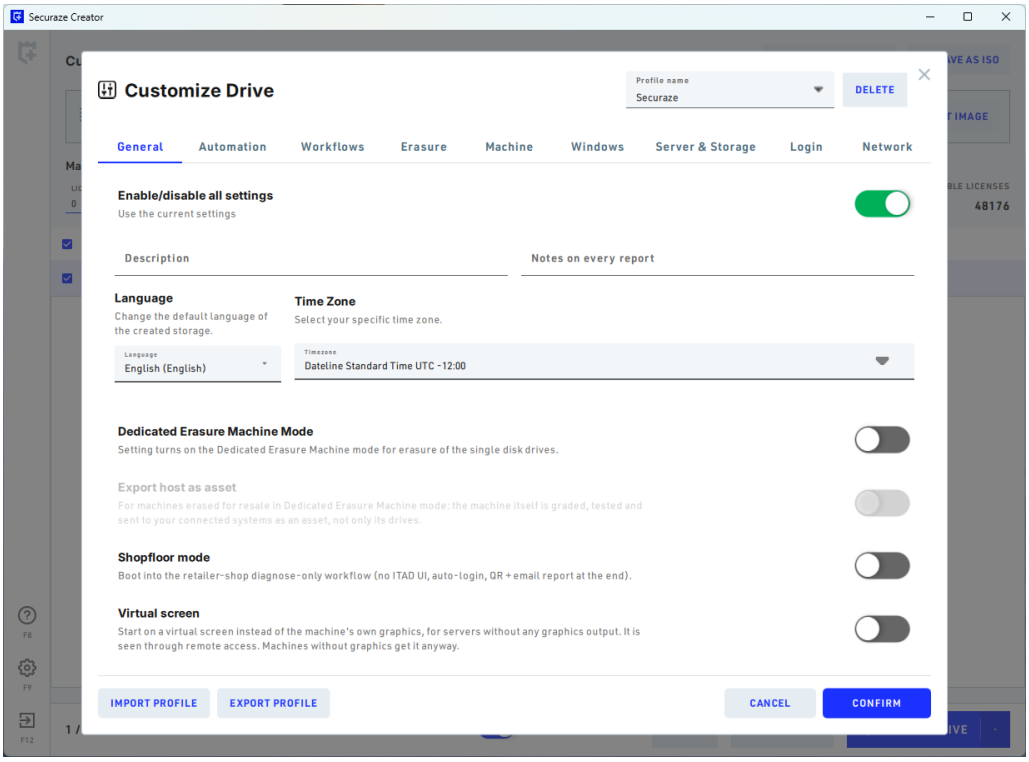
• **IMPORT PROFILE** adds the profile in the file to the saved profiles and says **Imported - pick it from the profile list to load it.** If a saved profile already has the same name (upper and lower case do not matter), the import replaces it. A file that is not a Securaze Creator profile is refused with **This file is not a Securaze profile.** - nothing is changed then.

• When an imported profile is loaded, the Login and Network tabs show **Password not in the imported profile - enter it.** below the password field. Enter the password before you create drives; an open network needs none.

• The workflow files themselves are not in the file. Workflows you added from files on the Workflows tab have to be added on the other computer too.

• Profile files of Securaze Creator and profiles of Securaze Command are different formats - a file exported from one cannot be imported into the other.

General



© 2026 Securaze GmbH

• **Enable/disable all settings** - the master switch. While it is off, every other tab is grayed out. **CONFIRM** switches it on automatically.

• **Description** - a short text that says what the profile is for. The PDF report that Securaze Work creates shows it in the **Configuration** row, after the profile name (profile name - description).

• **Notes on every report** - notes for every machine erased with the drive. They go on the report and are stored as the device's notes whenever the operator has not typed notes of their own.

Both fields are labeled by the gray text inside them.

• **Language** - the default language of the created storage.

• **Time Zone** - the time zone of the station, so that times on reports are correct. The list can be searched.

• **Dedicated Erasure Machine Mode** - the station is used for loose drives.

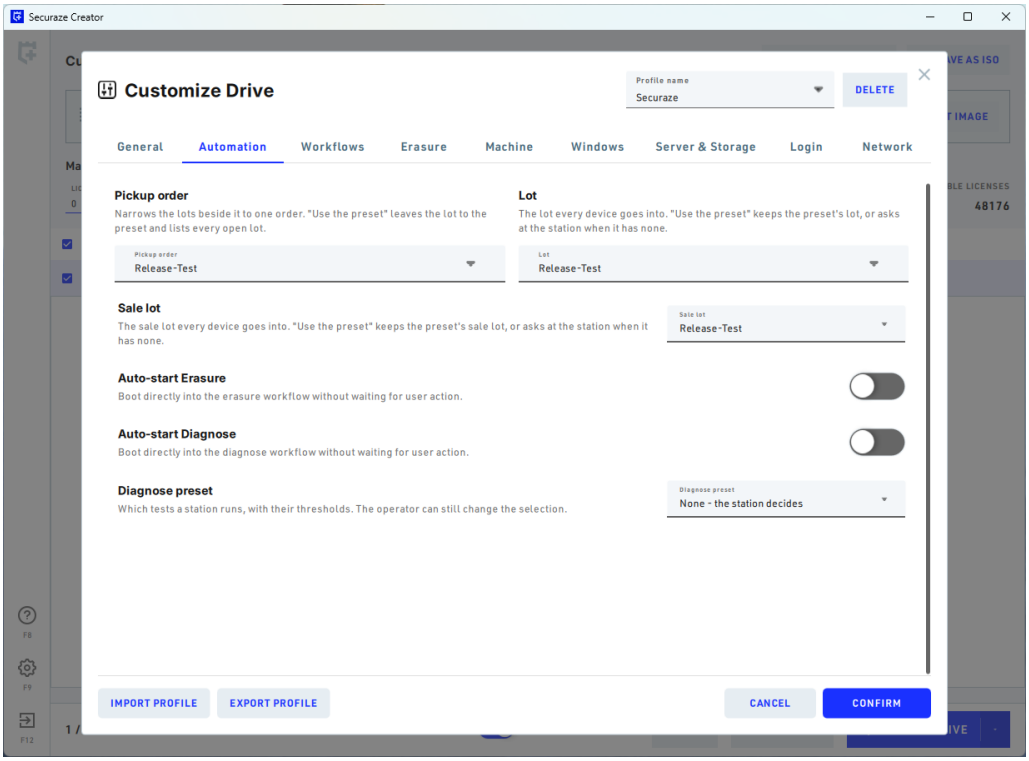
• **Export host as asset** - the machine itself is graded, tested and passed on as an asset, not only its drives. Can only be switched on together with Dedicated Erasure Machine Mode.

• **Shopfloor mode** - boots into the retail diagnose-only workflow: no ITAD interface, automatic login, QR code and email report at the end.

• **Virtual screen** - the station starts on a virtual screen instead of the machine's own graphics. This is for servers without any graphics output; you see the screen through remote access. Machines without any graphics get the virtual screen anyway.

© 2026 Securaze GmbH

Automation



• **Pickup order** - narrows the lots beside it to one order. **Use the preset** lists every open lot.

• **Lot** - the lot every device goes into. **Use the preset** keeps the lot of the preset, or asks at the station if it has none.

• **Sale lot** - the sale lot every device goes into, with the same **Use the preset** behavior.

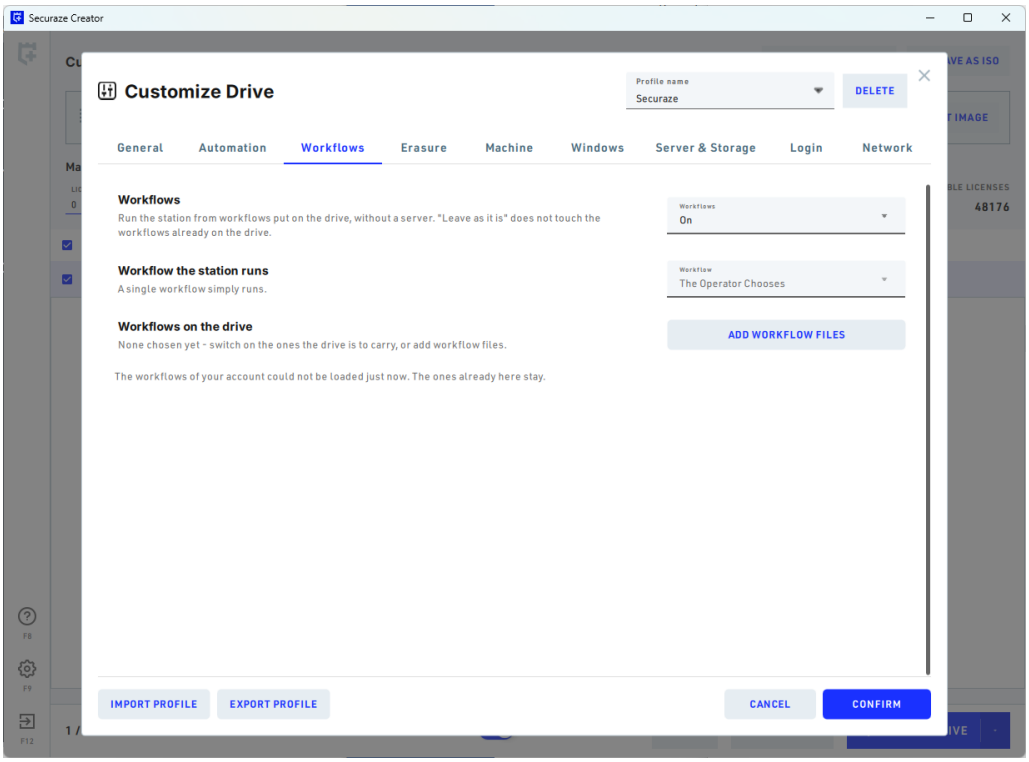
• **Auto-start Erasure** / **Auto-start Diagnose** - the station boots directly into that workflow without waiting for the operator.

• **Diagnose preset** - which tests the station runs, with their thresholds. **None - the station decides** leaves the choice open; the operator can change the selection in any case.

The automatic RAID teardown is on the **Server & Storage** tab, the automatic unfreeze on the **Erasure** tab.

© 2026 Securaze GmbH

Workflows



Here you put workflows on the drive, so that the station runs from them without a server.

The **Workflows** setting decides what applying the settings does to the workflows on the drive:

• **Leave as it is** (default) - the workflows already on the drive are not touched.

• **On** - the drive carries exactly the workflows switched on in the list below. Workflow files from an earlier apply are removed.

• **Off** - workflows are switched off on the drive. Workflow files already on it stay there, but are not run.

With **On**, two more settings appear:

• **Workflow the station runs** - with **The operator chooses** (default), the operator chooses one of the workflows on the drive after login. If you pick a workflow here, the station always runs that one. A single workflow on the drive simply runs.

• **Workflows on the drive** - the workflows of your account appear in the list by themselves, marked **From your account**; they are brought up to date each time the tab is opened. **ADD WORKFLOW FILES** opens a file dialog for further workflow files (*.json). Securaze Creator keeps its own copy of each file, so a saved profile still finds it after the original has moved. Each file appears in the list below, switched on.

Every workflow switched on in the list goes on the drive; nothing else does. **REMOVE** deletes Securaze Creator's copy of an added file at once.

© 2026 Securaze GmbH

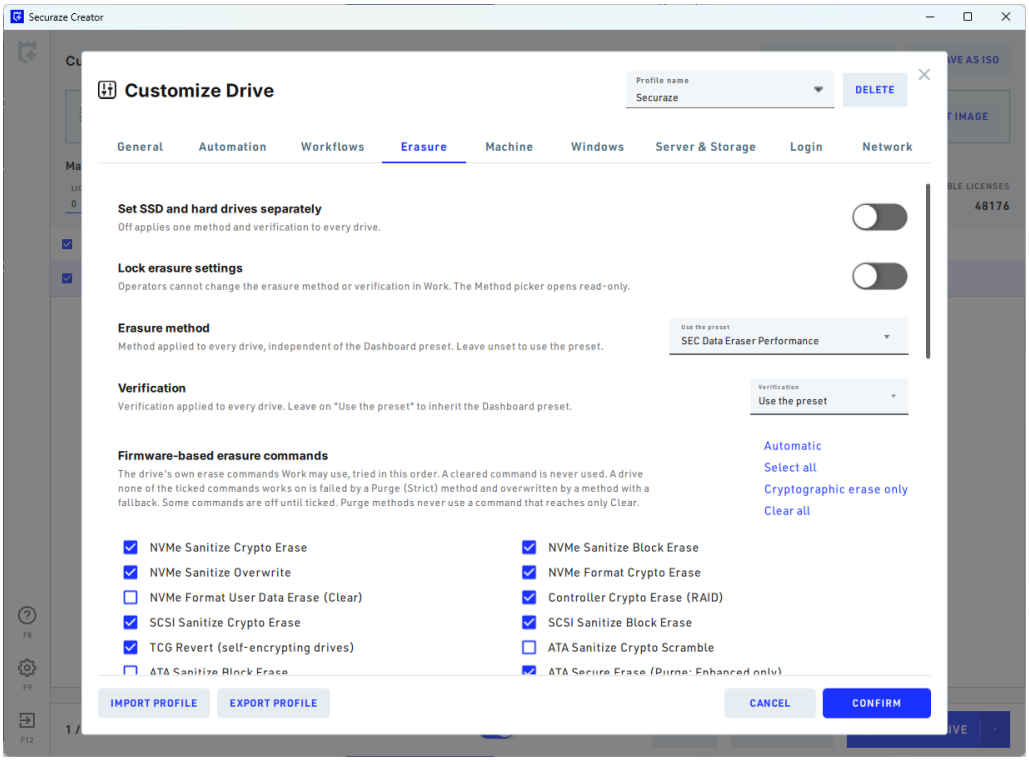
Only workflows made for Securaze Work can be added. A file that cannot be added is listed under **Not added:** together with the reason. A file with the same name as one already added replaces it.

A workflow that another workflow runs as one of its steps is marked **Part of "..." - goes on the drive with it**. It is switched on together with that workflow and cannot be switched off while that one is on, because the other workflow would stop at that step. It is not offered under **Workflow the station runs**. A workflow that is switched off in its own settings shows **switched off in the workflow itself, so it will not run** beside its file name.

If **Workflows** is **On** but no workflow is switched on, the other settings are still written, but the drive is marked as failed with a message that no workflow is chosen. Switch one on, or set **Workflows** to **Leave as it is**.

Workflow files do not go into an ISO made with **SAVE AS ISO**.

Erasure



How the drives are erased. Empty fields and **Use the preset** leave the decision to the preset of the Securaze Dashboard and to the station.

• **Set SSD and hard drives separately** - when off, one method and one verification apply to every drive; when on, SSD/NVMe and hard drives are set separately (**SSD / NVMe erasure method**, **Hard drive erasure method**, **SSD / NVMe verification**, **Hard drive verification**). Switching it off again copies the SSD settings to the hard drives.

• **Lock erasure settings** - the operator cannot change method or verification in Work; the method picker opens read-only.

© 2026 Securaze GmbH

• **Erasure method** - applied to every drive, independent of the Dashboard preset. Left unset, the preset applies. Each list offers only the methods meant for that kind of drive. A method set earlier that does not fit the list is shown with **- hard drives only** or **- SSDs only** behind its name.

• **Verification** - **Use the preset**, **Minimum**, **Last**, **All** or **Custom %**. Custom % reveals a field for a value between 1 and 100.

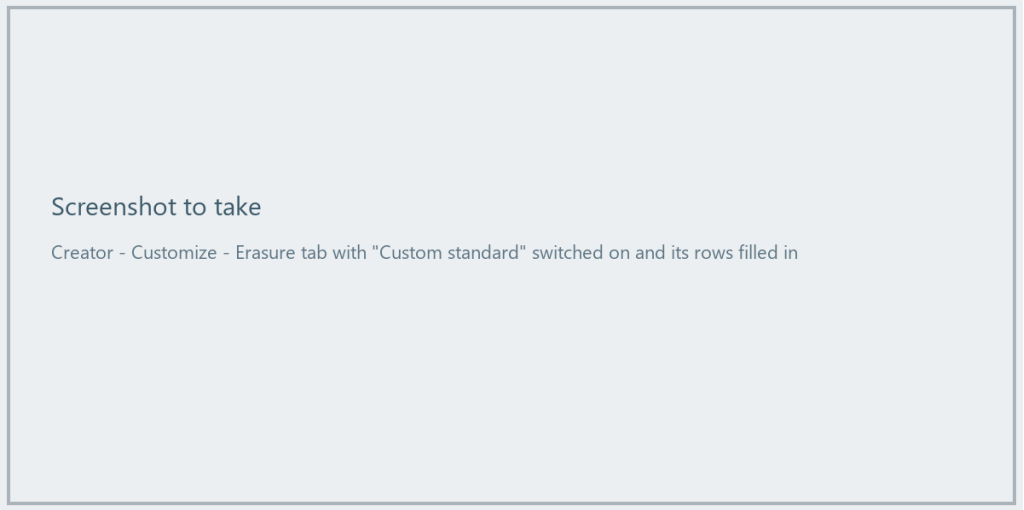
• **Firmware-based erasure commands** - the drive's own erase commands that Work may use, tried in the order of the list. A command that is cleared is never used. The links beside the list set it at once: **Automatic** (Work's own selection), **Select all**, **Cryptographic erase only** and **Clear all**.

The commands: NVMe Sanitize Crypto Erase, NVMe Sanitize Block Erase, NVMe Sanitize Overwrite, NVMe Format Crypto Erase, NVMe Format User Data Erase (Clear), Controller Crypto Erase (RAID), SCSI Sanitize Crypto Erase, SCSI Sanitize Block Erase, TCG Revert (self-encrypting drives), ATA Sanitize Crypto Scramble, ATA Sanitize Block Erase, ATA Secure Erase (Purge: Enhanced only), SCSI Sanitize Overwrite, ATA Sanitize Overwrite and Controller Overwrite (RAID, Clear). With **Automatic**, NVMe Format User Data Erase and the three ATA Sanitize commands stay off; they are used only when ticked.

A drive on which none of the ticked commands works is failed by a Purge (Strict) method and overwritten by a method with a fallback. Purge methods never use a command that reaches only Clear. Leave the selection on **Automatic** unless a customer requires certain commands (for example cryptographic erase only), or a drive model has trouble with one command.

• **Write pattern after erasure** - **Off** (default), **Zeros (0x00)** or **Ones (0xFF)**. After the drive's own erase has run and been proved, the whole drive is overwritten once with this pattern and verified, so it leaves in a defined state - for example when the next owner expects a drive that reads back as zeros. This takes as long as one full overwrite.

Custom standard



© 2026 Securaze GmbH

Your own erasure method, built from the parts the built-in methods are made of - for a customer or a contract that prescribes its own method.

• **Custom standard** - switch it on to set the method up; it starts with one pass of zeros. Switching it off deletes its setup. To use it, choose **Custom standard** as the erasure method above - for every drive, or for one kind of drive. The list of methods comes from your account; if it does not offer the custom standard yet, contact Securaze support.

On the report, the method has the name you give it in the Securaze Dashboard (**Settings** > **Securaze Standards**); without a name of your own it is called Custom standard. The custom standard uses the **Firmware-based erasure commands** and the **Write pattern after erasure** set above.

The rows below the switch:

• **Custom standard: level** - **Clear** (default) or **Purge**. With Purge, only firmware commands that reach Purge are used. If none of them ran, the method on the report is followed by "Purge not reached": the drive was cleared by the overwrite.

• **Custom standard: firmware erase** - **None** (default), **Before the overwrite** or **After the overwrite**: when the drive's own erase command runs. On NVMe, TCG and SAS drives it always runs first: when it works, the erasure is done, and the overwrite runs only when it fails.

• **Custom standard: firmware erase required** - shown when a firmware erase is chosen. On: the drive fails when its firmware erase fails. Off: the erasure carries on with the overwrite.

• **Custom standard: overwrite** - on by default: the drive is overwritten with the passes below. Off: only the firmware erase - then it has to be required.

• **Custom standard: passes** - the passes in order, separated by commas. Each pass is a byte in hex (00 to FF) or **random**, for example 00,FF,random. At most 35 passes.

• **Custom standard: encrypted pass data** - the pass data is encrypted, so no two drives get the same bytes.

• **Custom standard: passes in random order** - the passes run in a different order on every drive.

• **Custom standard: final pass with zeros** - after the last pass, one more pass with zeros.

• **Custom standard: rounds** - how often the passes run, 1 to 10. Empty: the station's setting.

• **Custom standard: read back every pass** - the verification reads back every pass, not only the last one.

• **Custom standard: least share read back (%)** - the verification reads back at least this share of the drive, 0 to 100. Empty or 0: the operator's verification setting.

© 2026 Securaze GmbH

• **Custom standard: fallback** - the method that runs instead when an erasure with the custom standard fails. **None - a failed erasure stays failed** (default), or one of the built-in methods.

The rows for passes, encrypted pass data, random order, final pass and rounds are shown only while **Custom standard: overwrite** is on.

A custom standard that cannot work is reported in red below the rows. Securaze Creator still writes the drive, but every erasure with such a method fails at the station - correct it first:

• **Custom standard is the erasure method but is not set up - every erasure with it fails. Set it up below.** - switch **Custom standard** on, or choose another erasure method.

• **Without an overwrite the firmware erase has to be required - else a drive whose firmware erase fails would pass unerased.** - switch on **Custom standard: firmware erase required**, or switch the overwrite on.

• **Purge needs a firmware erase - an overwrite alone reaches Clear.** - choose a firmware erase, or set the level to Clear.

• **The custom standard's overwrite has no passes - every erasure with it fails. Enter the passes here.** - enter at least one pass.

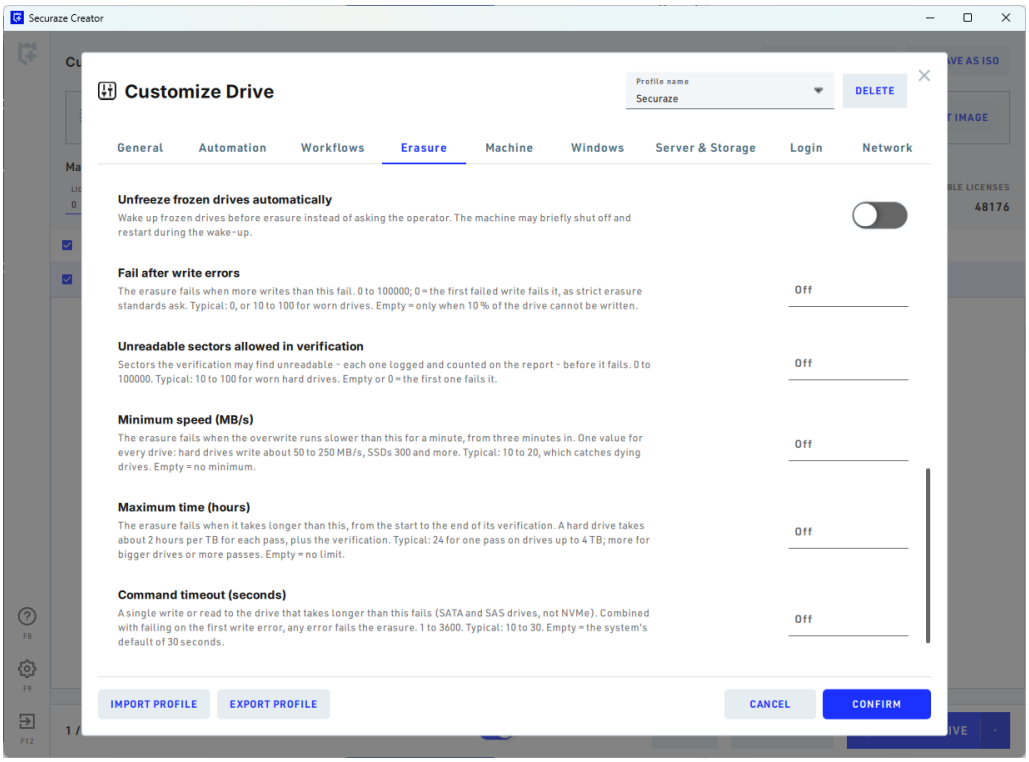
• **"..." is not a pass - a pass is a byte in hex (00 to FF) or random.** - correct the pass named.

• **At most 35 passes - this has ...** - remove passes, or use rounds instead of repeating the passes.

• **The custom standard is not readable.** / **The custom standard cannot fall back to itself.** - only seen with an imported profile: switch **Custom standard** off and on, and set it up again.

© 2026 Securaze GmbH

Format after erasure



• **Format after erasure** - **Off** (default), **NTFS**, **FAT32** or **ext4**. Once the erasure has succeeded and been verified, the drive gets a new partition table (GPT) with one partition over the whole drive and a quick format with this file system, so it leaves ready to use. There is no choice of partition size or volume label.

Good to know:

• Only where Securaze Work runs on Linux - as on every drive created from the Securaze Work image. Securaze Work on Windows does not format.

• Only after an erasure of this run that succeeded, verification included. A drive whose erasure failed is not formatted.

• The drive stays in progress until it is formatted (**Formatting as ...**), so it is not taken out too early. The drive details in Securaze Work then show a **Format** row: **Formatted as ...** or **Format as ... failed:** with the reason.

• A failed format does not make the erasure fail: the drive stays erased and certified.

• When Securaze Work cannot be certain which drive the device is (for example because the drive was unplugged or its connection changed), it does not format it and says why in the Format row.

• Not for a drive Windows is reimaged onto: it gets its own partitions. While **Windows reimaging** is set to **After the erasure, automatically**, no drive is formatted.

• The format is not part of the PDF report.

© 2026 Securaze GmbH

• **Unfreeze frozen drives automatically** - frozen drives are woken up before the erasure instead of asking the operator. The machine may briefly switch off and restart while doing so.

Erasure limits

Five limits stop an erasure that does not meet your requirements. They are empty by default, and an empty field shows **Off**. Empty does not switch the checks off - it means the erasure runs as it does without the setting: it fails when 10 % of the drive cannot be written, the first unreadable sector fails the verification, there is no speed or time limit, and the system's command timeout applies.

When a limit is reached, the erasure stops and the drive ends as **Failed** - not as canceled. Securaze Work shows the reason, for example in the drive's details. A fallback method (of a built-in method or of the custom standard) does not start after a limit has stopped the erasure.

• **Fail after write errors** - 0 to 100000. The erasure fails when more writes than this fail; 0 = on the first failed write. Empty: only the rule that always applies - the erasure fails when 10 % of the drive cannot be written.

• **Unreadable sectors allowed in verification** - 0 to 100000. How many sectors the verification may find unreadable before it fails; each one is noted in the erasure log. Empty or 0: the first unreadable sector fails the verification, as without a limit.

• **Minimum speed (MB/s)** - 1 to 100000. The erasure fails when the overwrite runs slower than this for a whole minute; it is judged from three minutes after the start, because every drive starts slowly. It applies to Work's overwrite only, not while a drive runs its own erase command. Empty: no minimum.

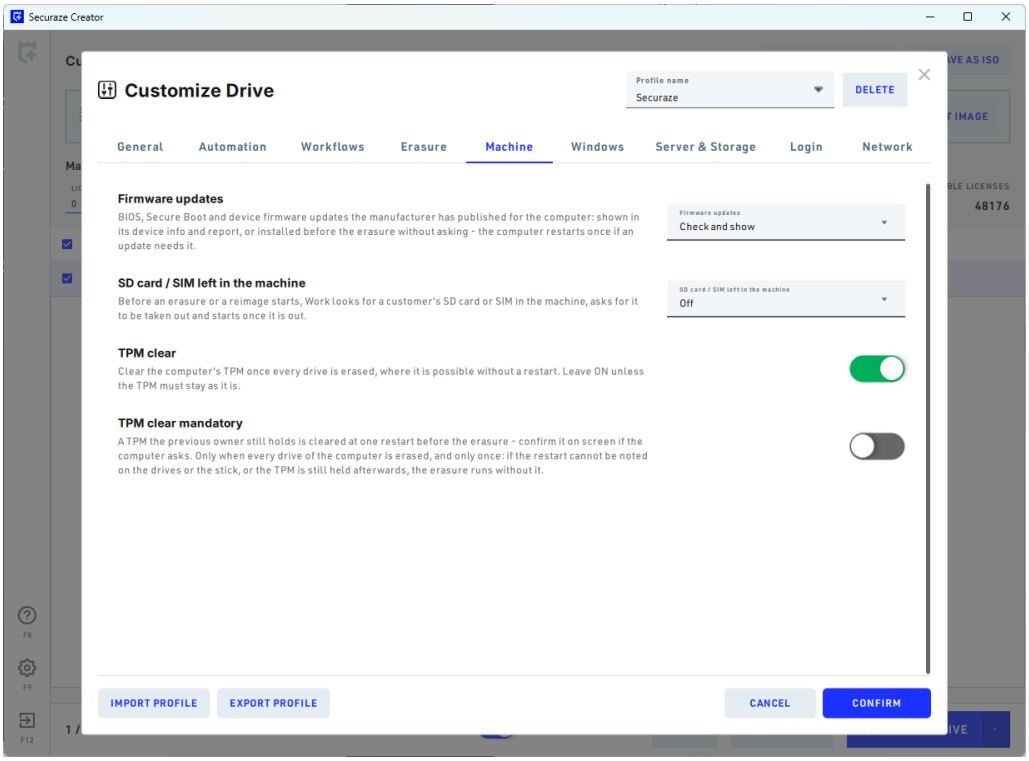
• **Maximum time (hours)** - 1 to 10000. The erasure fails when it takes longer than this, from its start to the end of its verification - the drive's own erase command included. Empty: no limit.

• **Command timeout (seconds)** - 1 to 3600. A single write or read that takes the drive longer than this fails. For SATA and SAS drives where Securaze Work runs on Linux; NVMe drives keep the system's value. The drive's previous timeout is put back after the erasure. Together with **Fail after write errors** set to 0, any error or hanging command fails the erasure. Empty: the system's default.

Set limits only when a customer or a contract requires them - for example that a drive with write errors or one that erases too slowly is rejected rather than certified after a long time.

© 2026 Securaze GmbH

Machine



The computer itself: its firmware, cards left in it, and its TPM.

• **Firmware updates** - BIOS, Secure Boot and device firmware updates the manufacturer has published for the computer. **Check and show** (default): they are shown in the device info and on the report. **Install without asking**: they are installed before the erasure - the computer restarts once if an update needs it; for machines that run without an operator. **Off**: not looked for.

• **SD card / SIM left in the machine** - before an erasure or a reimage starts, Work looks for a customer's SD card or SIM in the machine. **Off** (default), **Warn - the operator may go on** or **Wait until it is taken out** - then Work starts once the card is out.

• **Look for** - shown when the setting above is not Off: **SD card and SIM** (default), **SD card only** or **SIM only**.

• **TPM clear** - on by default: the computer's TPM is cleared once every drive is erased, where this is possible without a restart. Switch it off only if the TPM must stay as it is.

• **TPM clear mandatory** - off by default; available while TPM clear is on. A TPM the previous owner still holds is cleared at one restart before the erasure - confirm it on screen if the computer asks. This happens only when every drive of the computer is erased, and only once: if the restart cannot be noted on the drives or the stick, or the TPM is still held afterwards, the erasure runs without it.

© 2026 Securaze GmbH

Windows

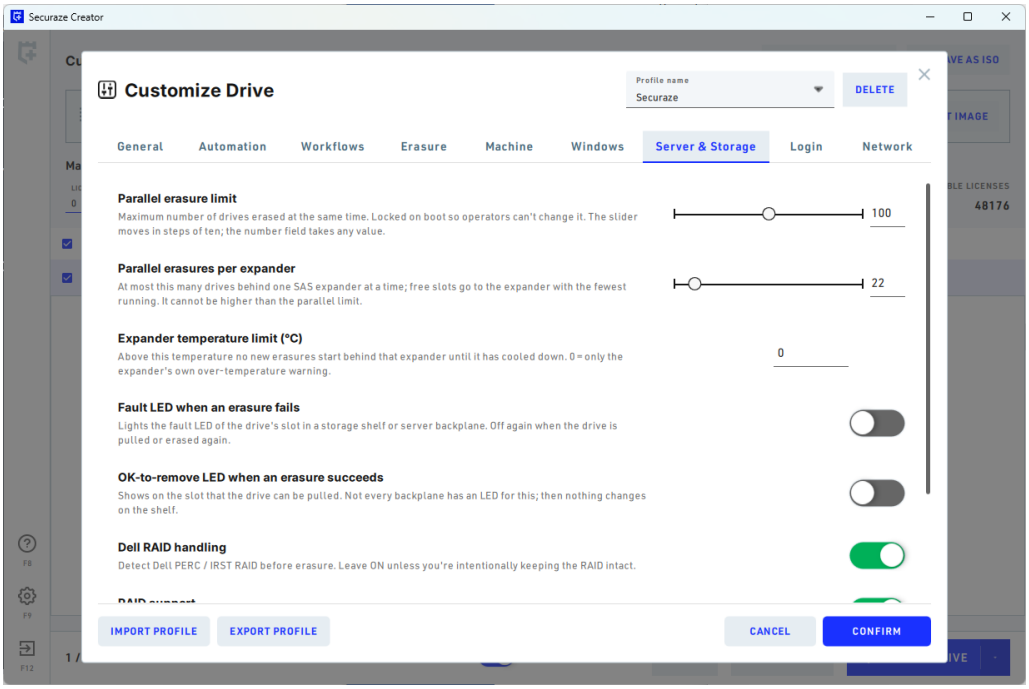
A fresh Windows on the machine's system disk, and how it is set up - the same settings as the Windows tab of a Securaze Command profile.

• **Windows reimaging** - **Off** (default), **Ask after the analysis**, **After the erasure, automatically** or **Reimage only - no erasure**.

When reimaging is on, the tab is divided into **Reimaging**, **Setup**, **Branding & clean-up** and **Drivers, BIOS & software**. All of these settings are described in the Securaze Windows Reimaging manual, chapter "The Windows tab of a Creator stick".

An ISO made with **SAVE AS ISO** cannot carry the Windows setup; only whether Windows may encrypt the drive by itself is carried. The reimaging mode, image, language, drivers and what happens after the reimage are carried.

Server & Storage



Settings for servers, storage shelves and RAID.

• **Parallel erasure limit** - the maximum number of drives erased at the same time, 1 to 200. It is locked at the station, so the operator cannot change it. The slider moves in steps of ten; the number field takes any value. Until you set it, the station keeps its own limit (the slider shows 10).

• **Parallel erasures per expander** - at most this many drives behind one SAS expander are erased at a time; free slots go to the expander with the fewest erasures running. It cannot be higher than the parallel limit. At the parallel limit (default) there is no limit per expander. Lower it when a shelf behind one expander gets too hot or too slow with all its drives running.

© 2026 Securaze GmbH

• **Expander temperature limit (°C)** - 0 to 120, with the value in °F beside it. Above this temperature no new erasures start behind that expander until it has cooled down. 0 (default) = only the expander's own over-temperature warning counts.

• **Fault LED when an erasure fails** - off by default. Lights the fault LED of the drive's slot in a storage shelf or server backplane; it goes off when the drive is pulled or erased again.

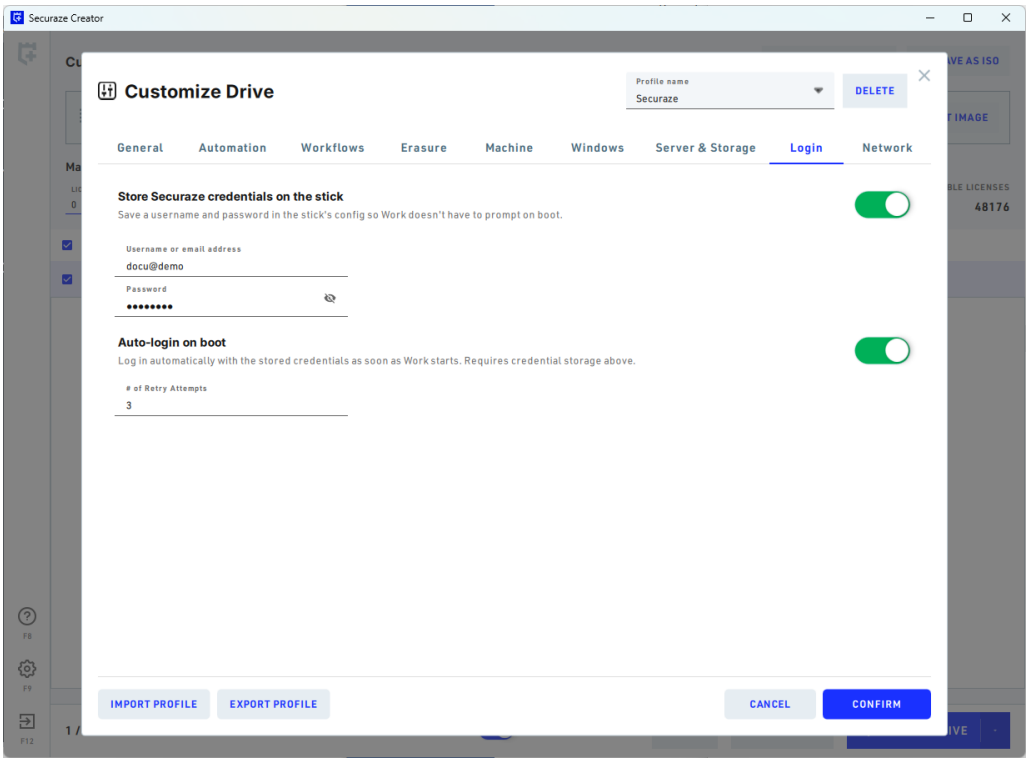
• **OK-to-remove LED when an erasure succeeds** - off by default. Shows on the slot that the drive can be pulled. Not every backplane has an LED for this; then nothing changes on the shelf.

• **Dell RAID handling** - detects Dell PERC / IRST RAID before the erasure. Switched on by default; leave it on unless the RAID is to be kept deliberately.

• **RAID support** - detects generic hardware RAID. Switched on by default and correct for most erasure targets.

• **Automatically tear down detected RAID** - off by default. A detected RAID is dismantled without the confirmation prompt so its drives can be erased. This only takes effect while RAID detection is switched on above.

Login

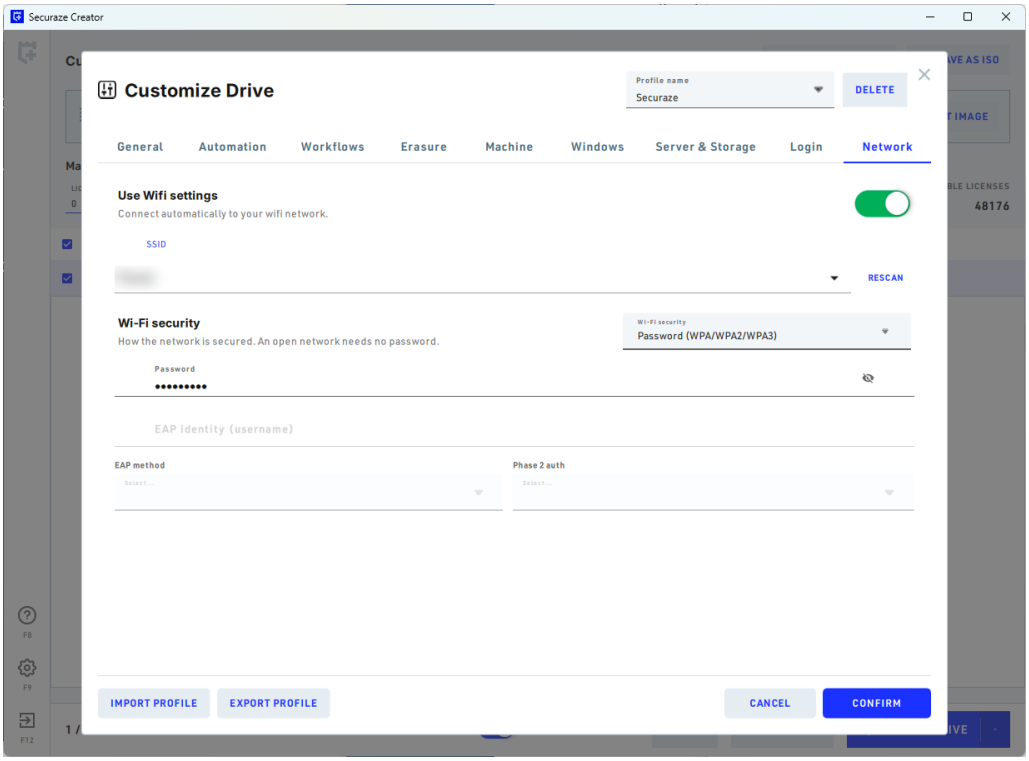


• **Store Securaze credentials on the stick** - a user name and password are stored in the configuration of the drive so that Work does not ask at boot.

• **Auto-login on boot** - Work signs in by itself with those credentials. The number of retry attempts can be set between 1 and 9 (3 by default).

© 2026 Securaze GmbH

Network



• **Use Wifi settings** - the station connects to the configured network by itself.

• **SSID** - a network found by the scan can be chosen, or a hidden network typed in. **RESCAN** repeats the search.

• **Wi-Fi security** - **Password (WPA/WPA2/WPA3)**, **Open network** (no password) or **Enterprise (802.1x)**.

• For an enterprise network the EAP identity, the EAP method (PEAP, TTLS, TLS, FAST, PWD, LEAP) and the Phase 2 authentication (MSCHAPV2, MSCHAP, PAP, CHAP, GTC, MD5, TLS) are entered as supplied by the network administrator.

CONFIRM keeps the settings in Securaze Creator; **CANCEL** and the X discard the changes. Saving, renaming, deleting, importing and exporting a profile and adding or removing workflow files take effect at once and are not undone by **CANCEL**. The settings are applied to the selected drives with **CREATE & APPLY**, or with the action **APPLY CHANGES**; **SAVE AS ISO** writes them into an ISO instead.

© 2026 Securaze GmbH



© 2026 Securaze GmbH