ecos

ECOS **SecureBootStick®**

ECOS SecureBootStick® V7

User Manual

Version: Pre-release

Date: 05/2025

IT Security Solutions

Made in Germany

ECOS Technology GmbH | Sant' Ambrogio-Ring 13 a-b | D-55276 Oppenheim | Phone: +49 6133 939-0 | Fax: +49 6133 939-333
Managing Directors: Paul Marx, Gerald Richter | Company headquarters: Oppenheim
Local court Mainz HRB 6889 | USt.-ID: DE 203394263

Content

Introduction

You are looking at a fully functional version of the ECOS **SecureBootStick®**, which provides you with a high-security access to a terminal server/virtual desktop infrastructure or web applications from any private computer.

The Secure Boot Stick (SBS) guarantees the separation of your private operating system from your business working environment. This means that your personal data cannot be accessed and your operating system cannot be modified.

Other USB devices such as storage devices, printers, and more can be used with the Secure Boot Stick if configured by your IT administration or user support.

How to use the manual

This manual is aimed at end users of the Secure Boot Stick and contains information on commissioning and using the Secure Boot Stick. Please read this manual carefully before commissioning and keep it for future reference.

Abbreviations

The following abbreviations are used in this manual:

SBS	Secure Boot Stick
SMA	System Management Appliance

Symbols and references

The following symbols are used in this manual:

References

References show further information in other chapters.

Info

The 'Info' tag refers to additional information about a given function.

Note

Notes indicate important operational aspects and provide explanations on the probable causes of malfunctions. Read these notes carefully.

Minimum SBS requirements for host computers

The Secure Boot Stick is designed for use with all common desktop and laptop computers as a so-called host computer in order to ensure the widest possible support for devices used in the business and private environment.

When configuring the host computer's hardware, keep in mind that, depending on the market situation, manufacturers may replace chipsets in current device series or rework the way they are installed. This may result in incompatibilities which need to be checked and, if necessary, fixed by an update.

Please note that SX and ZX versions released for VS-NfD, EU and NATO RESTRICTED do not support Master Boot Record (MBR) and can only be booted using UEFI Secure Boot. Therefore, the host computer must have support for UEFI Secure Boot.

Minimum requirements for hardware configuration:

- x86 64-bit CPU
  Intel Core i3
  AMD Ryzen 3
- 4 GB RAM
- USB 3.0 connection for SBS

The following Apple hardware is supported:

- The basic requirement for all devices is an Intel x86 processor
- MacBook Pro until 2020
- MacBook Air until 2018
- Mac mini
- iMac

Unsupported hardware:

- Bluetooth input devices
- Microsoft Surface Pen
- Integrated webcam on Microsoft Surface (depending on certain hardware revisions)
- Integrated microphone on Apple MacBook (depending on certain hardware revisions)

Note on Apple hardware with M1 chip:

With the M1 chip, Apple has introduced a new generation of chips that combine not only many components of a standard PC, but are also based on a different processor architecture: Arm.

The Secure Boot Stick does not currently support the Arm architecture. This affects the entire Apple lineup from the end of 2020 (MacBook Pro, MacBook Air, Mac mini).

Safety note

For security reasons, please observe the following guidelines after activating the Secure Boot Stick:

- Protect the SBS from unauthorized access by third parties at all times.
- Always keep SBS and password/PIN separate.
- Report the loss of the SBS or password/PIN immediately to your IT administration or user support.
- Report any irregularities or anomalies during operation of the SBS to your IT administration or user support immediately.

Changed version numbering

With version V7.58, the version numbering scheme was changed to semantic versioning. The previous meaning of the second digit of the version number is thus returned to the actual purpose of the minor version number. Versions approved for VS-NfD, EU and NATO RESTRICTED are marked with the build identifier '+vsnfd'.

The exact version number can be found in the title bar of the destination selection window or in the system status overview: *7.4.3.7 System status*.

For pilot customers, an RC number (Release Candidate) may still be displayed.

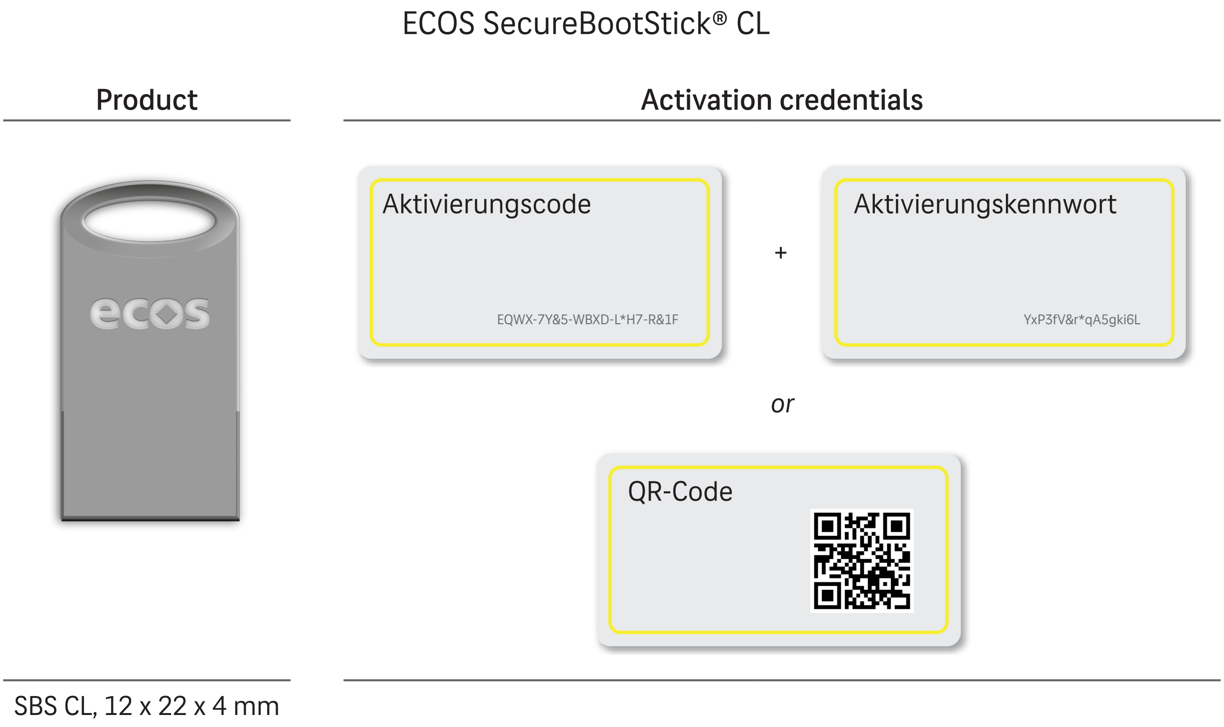
Software version	Old versioning	New versioning
Standard	V7.0.57	V7.60.9
VS-NfD	V7.1.57	V7.60.9+vsnfd

Part 1: First steps

1 Product overview

1.1 Scope

Please check all product and activation components for completeness, intactness and integrity upon receipt.



To scan a QR code, you need a webcam or a QR scanner capable of emulating a keyboard.

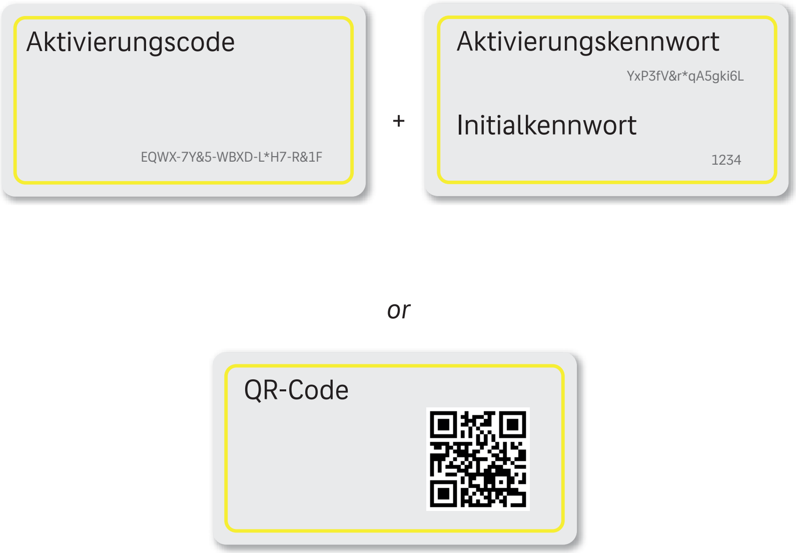
If your SBS CL has already been activated by your IT administration, you will only receive a start password for the SBS. Change this start password as described in section *7.4.3.6 Change start password*.

ECOS SecureBootStick® HE

Product

SBS HE, 12 x 41 x 4 mm

Activation credentials



Aktivierungscode

EQWX-7Y&5-WBXD-L*H7-R&1F

+

Aktivierungskennwort

YxP3fV&r*qA5gki6L

Initialkennwort

1234

or

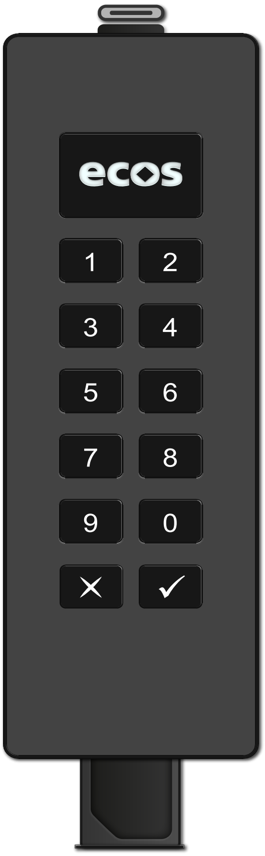
QR-Code

To scan a QR code, you need a webcam or a QR scanner capable of emulating a keyboard.

If your SBS HE has already been activated by your IT administration, you will only receive a start password for the SBS. Change the start password as described in section *7.4.3.6 Change start password*.

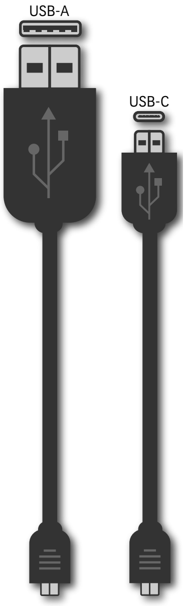
ECOS SecureBootStick® FX/SX

Product



SBS FX/SX, 28 x 85 x 13 mm

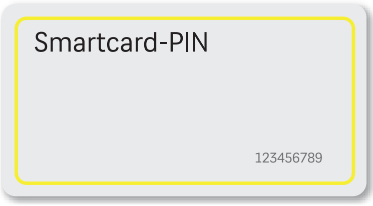
Accessories



USB adapter cable (2x)

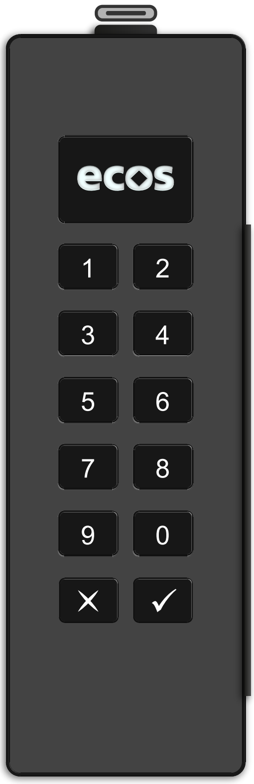
Smartcard

Activation credentials



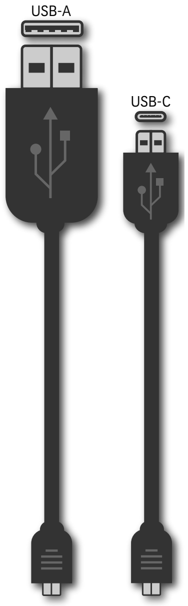
ECOS SecureBootStick® GX/ZX

Product



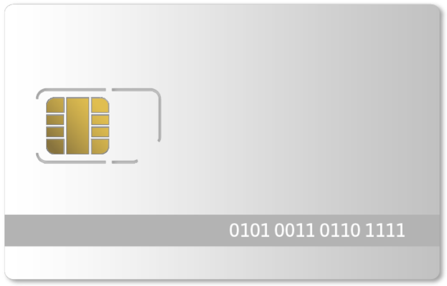
SBS GX/ZX, 28 x 85 x 13 mm

Accessories



USB adapter cable (2x)

Activation credentials



PKI card in ID-1 format

1.2 Description

There are various Secure Boot Stick versions, which differ in size and handling.

1.2.1 ECOS SecureBootStick® CL

The Secure Boot Stick CL is the smallest of the SBS product family. It is directly connected to the computer's USB port. The serial number of the SBS is located on the right side of the unit. Keep it to hand when communicating with the ECOS Helpdesk.

1.2.2 ECOS SecureBootStick® HE

The Secure Boot Stick HE is directly connected to the computer's USB port. The serial number of the SBS is located on the back of the unit. Keep it to hand when communicating with the ECOS Helpdesk.

1.2.3 ECOS SecureBootStick® FX/SX

Alongside the GX/ZX, the Secure Boot Stick FX/SX is one of the largest members of the SBS product family. The SBS SX differs from the SBS FX in that it is BSI-approved for VS-NfD, EU, and NATO RESTRICTED

A smartcard is required for the use of the SBS.

The serial number of the SBS is located on the back of the unit. Keep it to hand when communicating with the ECOS Helpdesk.

❶ Connector for USB adapter cable
❷ ECOS key
❸ PIN pad
❹ OK
❺ Cancel
❻ Smartcard compartment

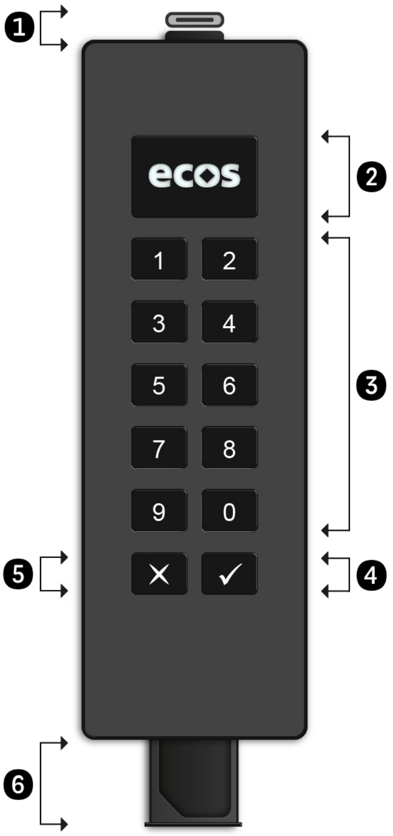


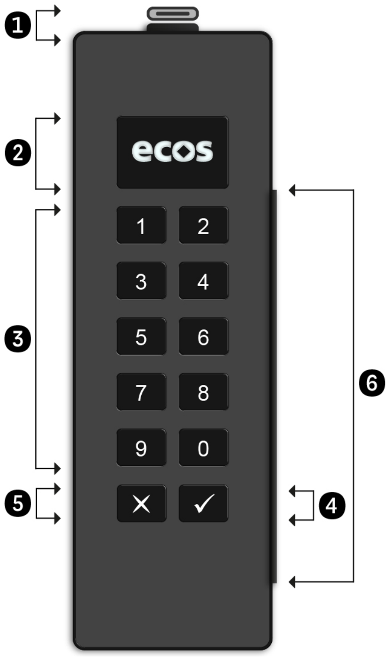
Abb. 1.01: *SBS FX/SX components*

1.2.4 ECOS SecureBootStick® GX/ZX

Alongside the FX/SX, the Secure Boot Stick GX/ZX is one of the largest members of the SBS product family. The SBS ZX differs from the SBS GX in that it is BSI-approved for VS-NfD, EU, and NATO RESTRICTED.

An ID card, PKI card or ID card in ID-1 format is required for the use of the SBS.

The serial number of the SBS is located on the back of the unit. Keep it to hand when communicating with the ECOS Helpdesk.



❶ Connector for USB adapter cable
❷ ECOS key
❸ PIN pad
❹ OK
❺ Cancel
❻ Smartcard compartment

Abb. 1.02: *SBS GX/ZX components*

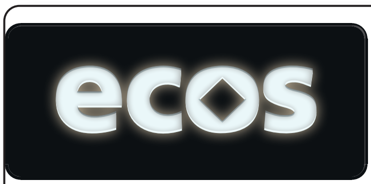
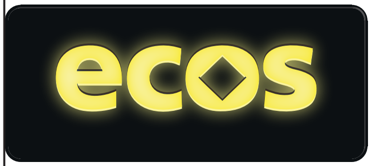
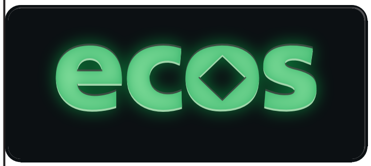
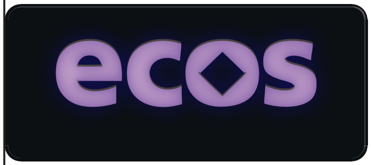
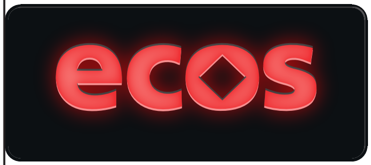
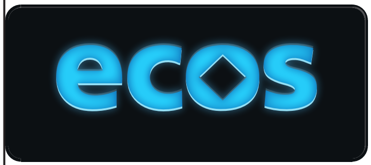
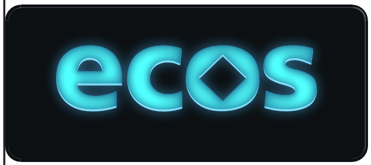
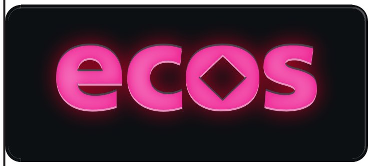
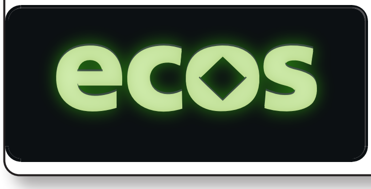
1.2.5 ECOS key

The ECOS key calls up the different Secure Boot Stick functions. The status of a selected function or operation is indicated by the different colors of the ECOS key. The ECOS key be lit continuously or flashing.

Some functions are only available to administrators. They are not explained in this manual.

The following functions are available to end users:

- 1: *9.5.1 Unlock data safe*
- 2: *9.5.2 Enable/disable write access for the data safe*
- 3: *6.6.2.1 Change smartcard PIN*
- 4: *6.6.2.2 Reset smartcard PIN*

	SBS inactive, but power-supplied
	*Solid:* SBS is active, data safe is disabled. *Flashing:* SBS is waiting for smartcard PIN entry
	◆ SBS is active, data safe is enabled with write access ◆ Smartcard detected ◆ Correct entry
	SBS is active, data safe is enabled with read access.
	Wrong entry
	ECOS key has been pressed, SBS awaits numerical input
	SBS awaits PUK entry
	SBS is inactive, data safe is enabled with read access
	SBS is inactive, data safe is enabled with write access.

2 Preparations

2.1 Secure Boot Stick

Have your Secure Boot Stick, computer and, if necessary, the activation data at hands.

Secure Boot Stick CL and HE require no preparation and can be connected directly to your computer's USB port.

For the Secure Boot Stick FX/SX, carefully take the smartcard out of the credit card-sized SIM frame. Gently open the smartcard tray and insert the smartcard as shown in figure 2.01. Close the card tray. Connect the SBS to your computer's USB port using the appropriate cable. The ECOS key briefly lights up green when the smartcard is detected and then lights up white.

On the Secure Boot Stick GX/ZX, the ID card slot is located on the right side of the SBS. Carefully insert your ID card with the chip facing upwards. Connect the SBS to your computer. The ECOS key briefly lights up green when the smartcard is detected and then lights up white.

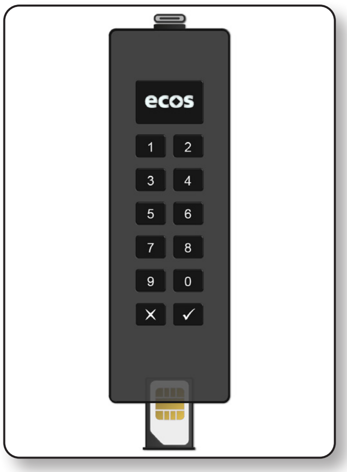


Fig. 2.01: *SBS FX/SX card slot*

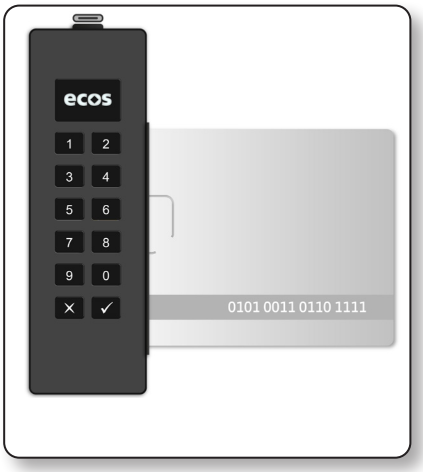


Fig. 2.02: *SBS GX/ZX card slot*

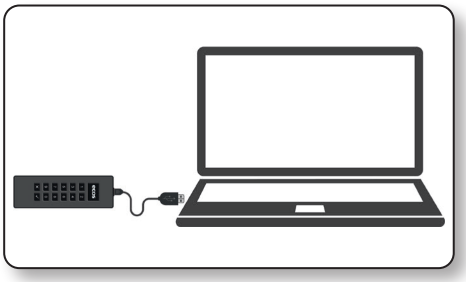


Fig. 2.03: *Connecting the SBS*

2.2 Setting up the boot order

In order for the Secure Boot Stick to start on your computer, you may need to adjust the boot order of your computer's BIOS. It determines the order in which the boot drives are initialized and thus the order in which the operating systems are started.

Connect the SBS to your computer's USB port and start it. If the SBS starts automatically, no further action is required on your part. If your private Windows operating system starts, you will need to adjust the boot sequence.

There are two ways to boot the Secure Boot Stick:

- one-time USB boot via the computer's boot menu
- permanent change of boot order in the BIOS settings

Since your computer will automatically boot from its internal hard drive if the SBS is not connected, we recommend that you change the boot order permanently.

If you use a BSI-approved SBS variant, your computer must support UEFI Boot. The so-called legacy boot via BIOS is prohibiteds for security reasons.
EFI and UEFI are further developments of the classic BIOS, which take over and extend the functions of the BIOS. In common language the term BIOS is still used. This manual is based on this linguistic understanding and uses the term BIOS as a synonym for EFI or UEFI.

2.2.1 One-time USB boot

Cancel the startup process of your computer by pressing the boot menu hotkey. The hotkeys calling up the boot menu differ depending on the vendor and model of your device. A list of hotkeys of the most common vendors can be found in section *8.2 Boot menu/BIOS hotkeys*.

If your device is not listed, look up the vendor and model number of your computer in combination with BOOT MENU HOTKEY on the Internet.

If you are having trouble accessing the boot or BIOS menu, your computer may have Fast Startup enabled. Please refer to section *9.1 Disable Windows Fast Startup* on how to disable the fast startup function.

What is BIOS?

The acronym BIOS stands for Basic Input Output System.

BIOS is a firmware located in a battery-buffered memory chip on the mainboard (also called motherboard) of your computer or notebook.

In this context, the BIOS is often described as 'non-volatile', which means that the memory chip containing the BIOS is powered by the mainboard battery. It is not deleted when the computer is switched off. This means that all BIOS settings will be available the next time the system is started.

The BIOS offers a configuration menu, also known as BIOS setup or boot menu, which can be accessed with a hotkey for a short time after the computer is powered on.

1. Switch off your computer.

2. Connect the SBS to your computer's USB port.

3. Start your computer.

4. Immediately after powering up, press the boot menu hotkey repeatedly.
   The time window in which to press the hotkey is relatively short. If you have missed the time window and your computer starts Windows, repeat the process from point 1.

5. If you have successfully aborted the boot process, the boot menu opens. Use the ↑ and ↓ keys to select the USB device and confirm with ENTER.
   The SBS is usually displayed as REMOVABLE DEVICE, USB HDD, JETFLASH TRANSCEND or with ECOS in the name. If the SBS is not displayed in the boot menu, try another USB port.

6. Your computer boots the selected USB device.

2.2.2 Permanent USB boot

To ensure that the Secure Boot Stick boots reliably when you start your computer, we recommend that you permanently change the boot order in your computer's BIOS settings.

To access your computer's BIOS, interrupt the boot process by pressing the BIOS hotkey. The keys for accessing the BIOS vary depending on the vendor and model of your computer. A list of hotkeys for the most common vendors can be found at *8.2 Boot menu/BIOS hotkeys*.

If your device is not listed, look up the vendor and model number of your computer in combination with BIOS HOTKEY on the Internet.

What is UEFI?

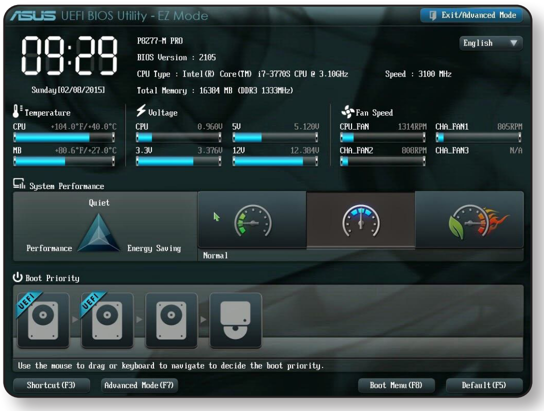
The acronym UEFI stands for Unified Extensible Firmware Interface. It is sometimes just called EFI.

UEFI is a successor to BIOS and has been replacing BIOS as a standard since 2010 with the launch of Windows 8. UEFI offers a modern graphical user interface, additional security features and supports faster boot times and larger hard disks.

What is the purpose of the BIOS?

The BIOS prepares your computer to start an operating system.

The BIOS is the first software that is executed at startup. It first checks the functionality of the central hardware components in a so-called Power On Self Test (POST), initializes these components, loads the required drivers, provides the runtime services for the operating systems and finally transfers control of the computer to the operating system.



Sunday[02/08/2015]

P8Z77-M PRO
BIOS Version : 2105
CPU Type : Intel(R) Core(TM) i7-3770S CPU @ 3.10GHz   Speed : 3100 MHz
Total Memory : 16384 MB (DDR3 1333MHz)

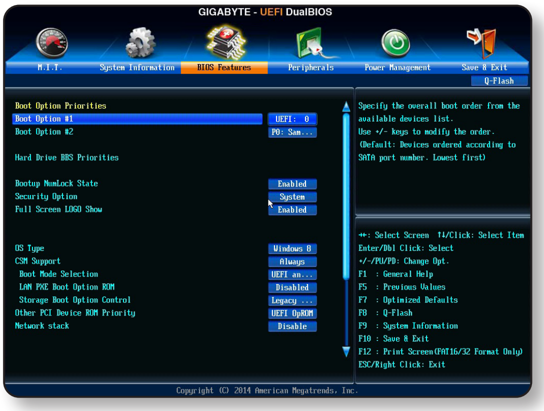
CPU +104.0°F/+40.0°C
MB +80.6°F/+27.0°C

CPU 0.960V 5V 5.120V
3.3V 3.376V 12V 12.384V

CPU_FAN 1314RPM CHA_FAN1 805RPM
CHA_FAN2 808RPM CHA_FAN3 N/A

Use the mouse to drag or keyboard to navigate to decide the boot priority.

Fig. 2.04: *ASUS UEFI*



Boot Option Priorities
Boot Option #1 UEFI: 0
Boot Option #2 P0: Sam...

Hard Drive BBS Priorities

Bootup NumLock State Enabled
Security Option System
Full Screen LOGO Show Enabled

OS Type Windows 8
CSM Support Always
Boot Mode Selection UEFI an...
LAN PXE Boot Option ROM Disabled
Storage Boot Option Control Legacy ...
Other PCI Device ROM Priority UEFI OpROM
Network stack Disable

Specify the overall boot order from the available devices list.
Use +/- keys to modify the order.
(Default: Devices ordered according to SATA port number. Lowest first)

→←: Select Screen ↑↓/Click: Select Item
Enter/Dbl Click: Select
+/-/PU/PD: Change Opt.
F1 : General Help
F5 : Previous Values
F7 : Optimized Defaults
F8 : Q-Flash
F9 : System Information
F10 : Save & Exit
F12 : Print Screen(FAT16/32 Format Only)
ESC/Right Click: Exit

Copyright (C) 2014 American Megatrends, Inc.

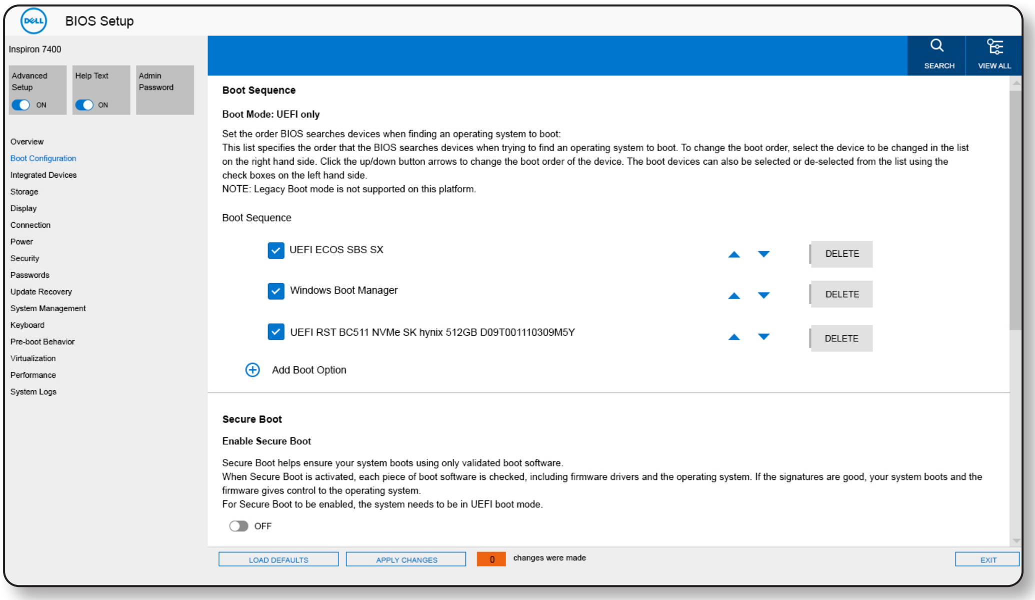
Fig. 2.05: *Gigabyte UEFI*

The design of the BIOS menu varies depending on the vendor. In legacy BIOS versions, there is usually no mouse support and you have to navigate using the arrow and ENTER keys. The mouse is supported by many modern UEFI versions. This manual describes the basic procedure.

1. Switch off your computer.
2. Connect the SBS to your computer's USB port.
3. Start your computer.
4. Immediately after powering up, press the BIOS hotkey repeatedly.
   The time window for pressing the BIOS setup button is relatively short. If you have missed the time window and your computer starts Windows, repeat the process from step 1.

5. If you have successfully interrupted the boot process, the BIOS menu appears. Navigate to the boot menu tab and confirm with ENTER.
   The boot menu is usually found under terms such as Boot, Boot Option, Boot Priority or similar.

6. Change the boot order.
   If the boot order appears in the form of a list, use the ↑ and ↓ keys to navigate to SBS and move it to the first position in the list.



Boot Sequence

Boot Mode: UEFI only

Set the order BIOS searches devices when finding an operating system to boot:
This list specifies the order that the BIOS searches devices when trying to find an operating system to boot. To change the boot order, select the device to be changed in the list on the right hand side. Click the up/down button arrows to change the boot order of the device. The boot devices can also be selected or de-selected from the list using the check boxes on the left hand side.
NOTE: Legacy Boot mode is not supported on this platform.

Boot Sequence

☑ UEFI ECOS SBS SX
☑ Windows Boot Manager
☑ UEFI RST BC511 NVMe SK hynix 512GB D09T001110309M5Y

Secure Boot

Enable Secure Boot

Secure Boot helps ensure your system boots using only validated boot software.
When Secure Boot is activated, each piece of boot software is checked, including firmware drivers and the operating system. If the signatures are good, your system boots and the firmware gives control to the operating system.
For Secure Boot to be enabled, the system needs to be in UEFI boot mode.

OFF

0 changes were made

Fig. 2.06: *Changing the boot order*

The keys you can use to make changes are usually shown at the bottom of the BIOS interface. If the SBS is not displayed in the BIOS, try another USB port.

7. Save your changes and exit the BIOS.
   You can often save your changes with Save and exit the BIOS with Exit. Some BIOS menus support a Save & Exit function that allows you to save changes and exit the BIOS menu at the same time.

8. Your computer restarts and boots the SBS.

If you have successfully changed the boot order, your computer will boot directly from the SBS.

2.2.3 Further BIOS and system settings

Depending on the model of your computer, you may need to adjust other BIOS and system settings.

2.2.3.1 Enabling USB boot

The BIOS can be set to allow booting from USB media. If this option is disabled, booting will be denied even though the SBS is detected as a boot device.

Enable USB BOOT in this case. Proceed as described in chapter *2.2.2 Permanent USB boot* and navigate to the boot settings in the BIOS menu.

Select USB BOOT and confirm with ENTER if necessary. Change the option to ACTIVATE or ENABLE and confirm again with ENTER.

Save your changes and exit the BIOS. Your computer restarts and boots the SBS.

> The USB boot option may be located in a different menu item. If you cannot find the option, look up the vendor and model number of your computer in combination with USB boot on the Internet.

2.2.3.2 Disabling UEFI Secure Boot

SECURE BOOT is a BIOS security feature. Signatures and valid keys ensure that critical firmware (such as the Windows boot manager) is only booted if it has not been tampered with or modified by a third party. SECURE BOOT is activated by default.

> If you use an Secure Boot Stick with BSI approval (SX or ZX), secure Boot must be activated.

Although the Secure Boot Stick has a valid signature, it is sometimes not immediately recognized by a computer. As a result, the SBS may not start.

Disable SECURE BOOT in this case. Proceed as described in chapter *2.2.2 Permanent USB boot* and navigate to the boot settings in the BIOS menu.

Select SECURE BOOT and confirm with ENTER if necessary. Change the option to DEACTIVATE or DISABLE and confirm again with ENTER.

Save your changes and exit the BIOS. Your computer restarts and boots the Secure Boot Stick.

> The Secure Boot option may be located in a different menu item. If you cannot find the option, look up the vendor and model number of your computer in combination with Secure Boot on the Internet.

2.2.3.3 Microsoft Pluton Security Chip

In 2020, Microsoft introduced a new security chip, the Microsoft Pluton, which has also been increasingly used by other vendors since 2022. This chip is part of the CPU and replaces the previous TPM chip, which was a separate hardware component. Pluton eliminates the need for external and therefore vulnerable communication between the CPU and the TPM chip. Sensitive data is shielded on the CPU.

However, Pluton also prevents any operating system other than Windows from booting. To use the SBS on a computer with Pluton, you must allow third-party certificates in the BIOS.

Start your computer as described in section *2.2.2 Permanent USB boot* and boot into the BIOS. Navigate to the security settings in the BIOS menu.

Enable the Microsoft & 3rd party CA option in the Secure Boot section. Depending on the vendor, this option can also be found under Secure Boot certificate keyset.

Save your changes and exit the BIOS. Your computer restarts and boots the Secure Boot Stick.

2.3 Setting the start volume on a Mac

A Mac boots from the internal hard disk by default, but can also boot from any connected USB device with a Mac-compatible operating system. On your Mac, this is called the start volume.

2.3.1 One-time USB boot

If you select the start volume via the Startup Manager, the Mac boots once from this device (e.g. volume or USB device). The next time you switch on your Mac, it will automatically start from the volume that was set as the default in the start volume settings. If the SBS is not displayed in the Startup Manager, a T2 security chip may be installed in your Mac. Please refer to section *9.2 Mac with T2 security chip* to find out how to adjust the settings.

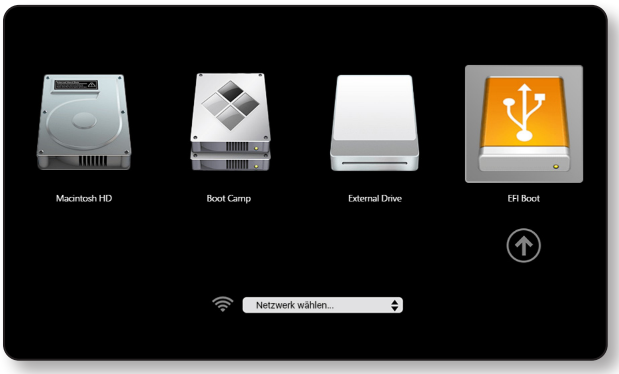


Fig. 2.07: *Select the start volume*

1. Turn off your Mac.
2. Connect the SBS to your Mac's USB port.
3. Start your Mac.
4. Press OPTIONS (⌥) on your keyboard immediately after powering up.
5. Press and hold OPTIONS (⌥) until the Startup Manager opens.
6. If your Mac is protected by a firmware password, you will be prompted to enter the password.
7. Select the desired start volume. The SBS is usually displayed as EFI BOOT. If the SBS is not displayed in the Startup Manager, try another USB port.
8. Confirm your selection with ENTER or by clicking on the arrow under the selected volume.
9. Your Mac boots the SBS.

Connect an external keyboard to your Mac to log in to the SBS and start activation if necessary. The keyboard drivers for Apple devices are only initialized after logging on to the SBS.

3 How to activate the SBS

Before using your Secure Boot Stick for the first time, you must activate it. Your IT administration or user support department has provided you with the required activation credentials to get started.

The activation process (called Easy Enrollment) usually starts automatically the first time you use the SBS and requires an active Internet connection.

The SBS sends the activation data to the System Management Appliance (SMA) for verification. If the data matches, the SMA returns the default configuration that has been defined by your IT administration. This configuration includes access to destination systems, language settings, keyboard layouts and other resources to which you have access rights.

The activation process varies depending on your SBS variant.

> ⚠ Your SBS may have already been activated by your IT administration. In this case, you already have a start password or a smartcard PIN and do not need to activate the SBS. Change start password or smartcard PIN as soon as possible. For further information, please refer to *6.6 SBS login*.

3.1 How to activate the Secure Boot Stick CL or HE

If you have received a Secure Boot Stick CL or HE from your IT administration or user support, you will need either an activation code and an activation password or a QR code for activation.

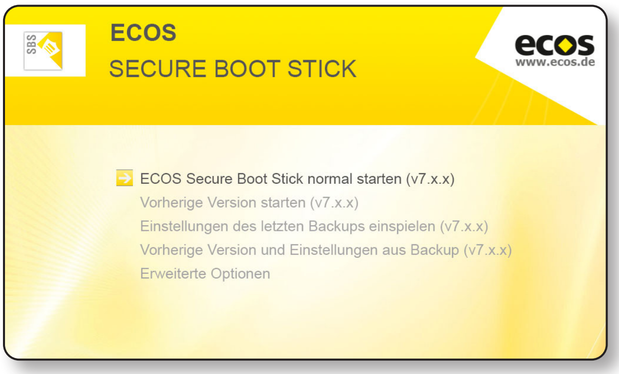
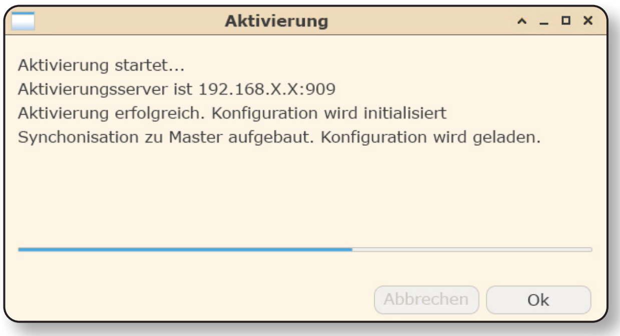

SBS
ECOS
SECURE BOOT STICK
ecos
www.ecos.de
ECOS Secure Boot Stick normal starten (v7.x.x)
Vorherige Version starten (v7.x.x)
Einstellungen des letzten Backups einspielen (v7.x.x)
Vorherige Version und Einstellungen aus Backup (v7.x.x)
Erweiterte Optionen

Fig. 3.01: *SBS boot menu*

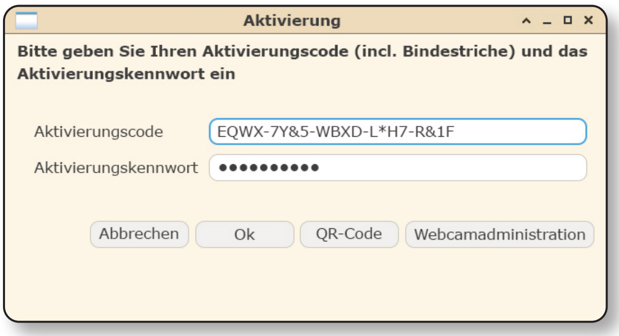
1. Connect your SBS to your computer's USB port.
2. Start your computer.
3. In the SBS boot menu, select the option Start ECOS Secure Boot Stick or wait 5 seconds until the SBS starts automatically.
4. If you use a SBS HE you will be asked for the start password.
5. The SBS desktop appears and Easy Enrollment starts automatically.
6. Make sure you have a working Internet connection.
7. Enter activation code (incl. hyphens) and activation password. If you have received a QR code, select this option. When your computer's webcam opens, scan the QR code. Alternatively, you can use a connected QR code scanner.
8. You may be asked to set a start password for future logins.

9. The activation process takes a few minutes. Restart the SBS after Easy Enrollment is complete. If you have set a start password during activation, you will now be prompted for it.



Aktivierung startet…
Aktivierungsserver ist 192.168.X.X:909
Aktivierung erfolgreich. Konfiguration wird initialisiert
Synchonisation zu Master aufgebaut. Konfiguration wird geladen.

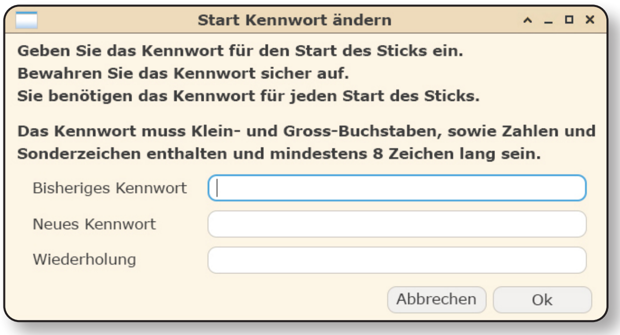
Fig. 3.02: *The activation process starts*



Bitte geben Sie Ihren Aktivierungscode (incl. Bindestriche) und das Aktivierungskennwort ein

Aktivierungscode: EQWX-7Y&5-WBXD-L*H7-R&1F
Aktivierungskennwort: ●●●●●●●●●●

Fig. 3.03: *Enter your credentials*

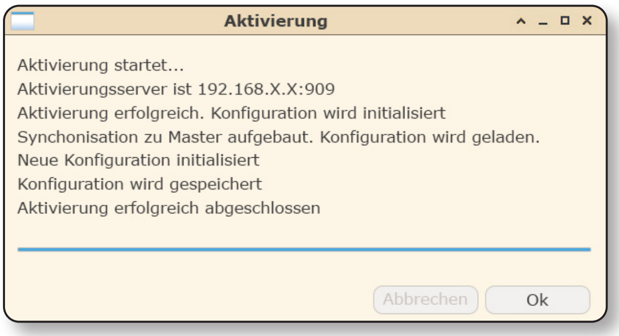


Geben Sie das Kennwort für den Start des Sticks ein.
Bewahren Sie das Kennwort sicher auf.
Sie benötigen das Kennwort für jeden Start des Sticks.

Das Kennwort muss Klein- und Gross-Buchstaben, sowie Zahlen und Sonderzeichen enthalten und mindestens 8 Zeichen lang sein.

Bisheriges Kennwort
Neues Kennwort
Wiederholung

Fig. 3.04: *Change your start password*



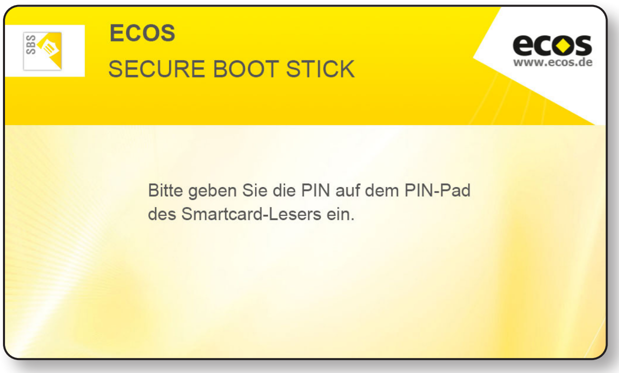
Aktivierung startet…
Aktivierungsserver ist 192.168.X.X:909
Aktivierung erfolgreich. Konfiguration wird initialisiert
Synchonisation zu Master aufgebaut. Konfiguration wird geladen.
Neue Konfiguration initialisiert
Konfiguration wird gespeichert
Aktivierung erfolgreich abgeschlossen

Fig. 3.05: *Activation is complete*

3.2 How to activate the Secure Boot Stick FX/SX or GX/ZX

If you have received a Secure Boot Stick FX/SX or GX/ZX from your IT administration or user support, you need the smartcard PIN for activation. The PIN has been set by the administrator during smartcard configuration.

1. Check that the smartcard is properly seated in your SBS.
2. Connect the SBS to your computer's USB port.
3. Start your computer.
4. In the SBS boot menu, select the option Start ECOS Secure Boot Stick or wait 5 seconds until the SBS starts automatically.
5. When prompted, enter the smartcard PIN on the PIN pad and press the ✓ key. The ECOS key flashes yellow.



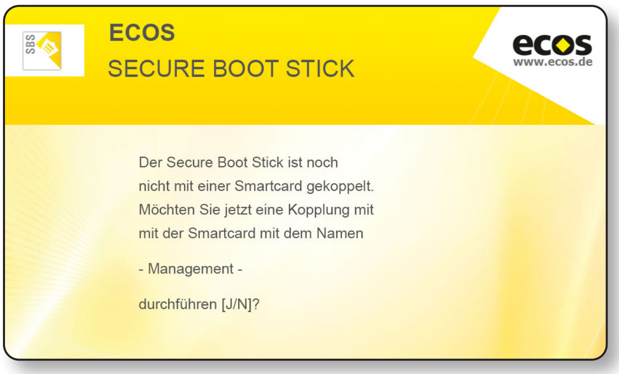
Bitte geben Sie die PIN auf dem PIN-Pad des Smartcard-Lesers ein.

Fig. 3.06: *Smartcard PIN prompt*

6. When you are prompted to pair the SBS with the smartcard, press J to confirm, then press ENTER. The ECOS key flashes green during pairing and then lights yellow.

7. The SBS desktop opens and Easy Enrollment starts automatically.

8. Make sure you have a working Internet connection.



Der Secure Boot Stick ist noch
nicht mit einer Smartcard gekoppelt.
Möchten Sie jetzt eine Kopplung mit
mit der Smartcard mit dem Namen

- Management -

durchführen [J/N]?

Fig. 3.07: *SBS smartcard pairing*

9. The activation process takes a few minutes. Restart the SBS after Easy Enrollment is complete.

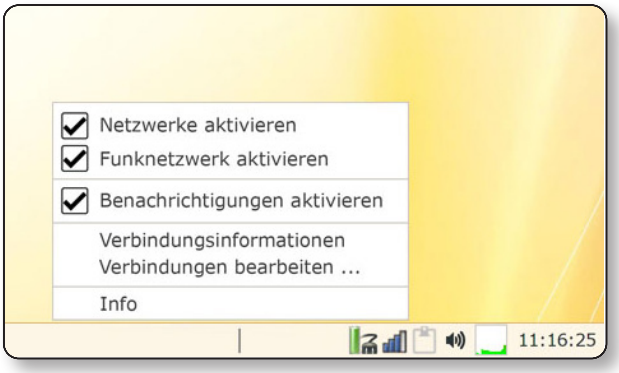
4 Internet connection

You can set up and edit an Internet connection in the SBS network manager, which can be accessed from the system tray of the SBS desktop.

If your computer is connected to the Internet via LAN, you usually do not need to set up any connection. If you want to use a wireless connection, you will need to set it up in the network manager.

The network icon shows whether and how your computer is connected to the Internet. If you are connected via a built-in LTE modem, the system bar displays an additional icon.

Move the mouse over the network icon to display the currently active connection.



☑ Netzwerke aktivieren
☑ Funknetzwerk aktivieren
☑ Benachrichtigungen aktivieren

Fig. 4.01: *Context menu of the network manager*

Icon overview:

No network connection. You are not connected to the Internet.

Ethernet network connection is active. You are connected to the Internet via LAN.

No wireless network connection. You are not connected to the Internet.

Wireless networks are available for connection. You are not connected to the Internet.

Wireless network connection is active. You are connected to the Internet via WLAN.

4G Mobile broadband connection. You are connected to the Internet via LTE.

To be able to use an Internet connection on the SBS, activate the checkbox Enable networks in the context menu of the network manager.

If you want to use the SBS with a wireless network connection, activate the checkbox Enable wireless network in the context menu. Click the network icon to display the available networks. Select your wireless network and enter your network key if necessary. You can display the password.

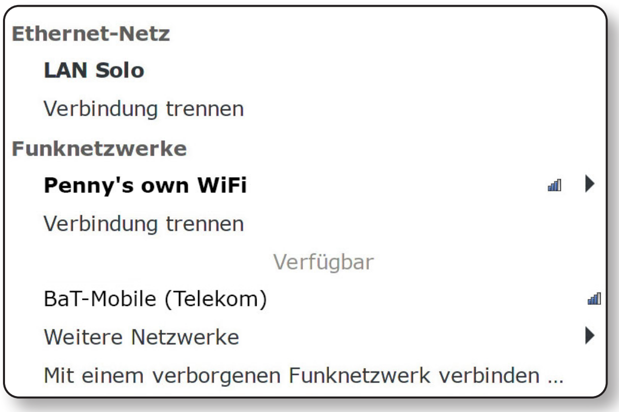
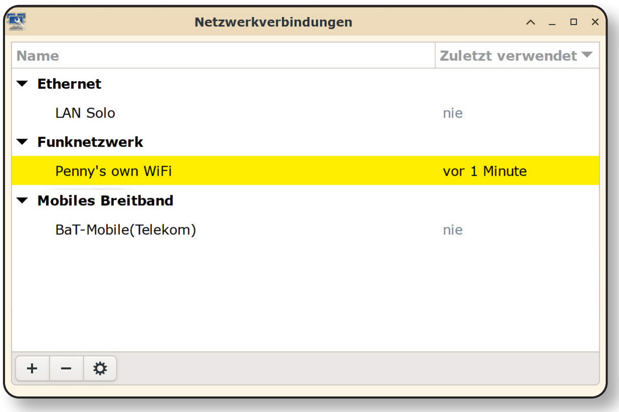


Fig. 4.02: *Available connections*

The option Edit connections of the context menu opens a window with previously used network connections. You can add new connections (+), delete (−) or edit (⚙) them.

For more information about editing options, please refer to section *7.3.1 Network manager*.

Information on setting up a mobile phone connection can be found at *9.4 Setting up a cellular network*.



Netzwerkverbindungen

Name	Zuletzt verwendet
Ethernet	
LAN Solo	nie
Funknetzwerk	
Penny's own WiFi	vor 1 Minute
Mobiles Breitband	
BaT-Mobile(Telekom)	nie

Fig. 4.03: *Editing network connections*

If you cannot connect to your wireless network after restarting the Secure Boot Stick, disable the quick start function of your Windows operating system. Windows quick start accelerates the system start of your computer by loading the last system status from a previously written system file. There is no real boot process. This can lead to hardware components and drivers not being loaded correctly. For information on how to disable Windows quick start, please refer to section *9.1 Disable Windows Fast Startup* .

5 Destination selection

The destination selection dialog shows an overview of all destination systems that your IT administration has released for your user account. Alternatively, destinations can also be displayed as icons on the SBS desktop.

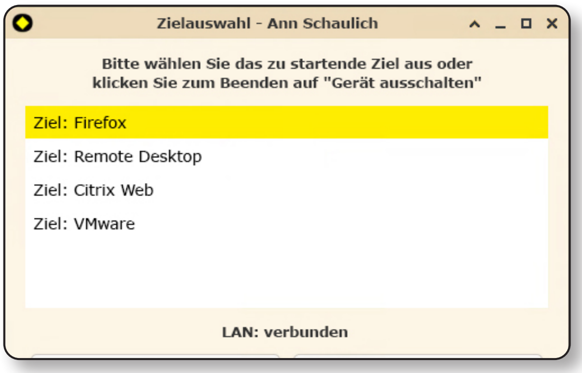
Select the desired destination so that it is highlighted in color. Press OK to confirm or double-click the selection to connect to the destination. Depending on the destination selection, you may need additional user credentials to get access to the relevant destination server.

If the destinations you have access to are displayed as icons on the SBS desktop, you can open a web browser destination in addition to another destination that is already open.

If you close your destination, the destination selection dialog reappears and you can select a new destination or shut down your computer via the SHUTDOWN button.

Possible destinations are:

- Web browsers
- Access to Remote Desktop (RDP) connections
- Access to Citrix connections
- Access to VMware connections
- Genua remote maintenance
- Access to SSH connections
- Access to VNC connections



Zielauswahl - Ann Schaulich

Bitte wählen Sie das zu startende Ziel aus oder klicken Sie zum Beenden auf "Gerät ausschalten"

Ziel: Firefox
Ziel: Remote Desktop
Ziel: Citrix Web
Ziel: VMware

LAN: verbunden

Fig. 5.01: *Destination selection dialog*

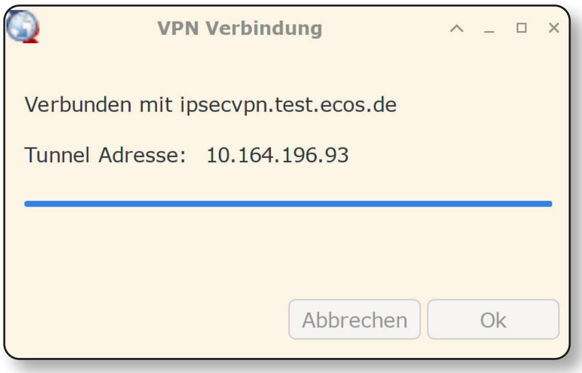
5.1 VPN

Your IT administration can configure the system to open a VPN connection when you select a destination. A Virtual Private Network (VPN) first creates a secure, uninterceptable tunnel across the Internet.

The address of the selected server and the IP address of the active VPN tunnel are displayed upon connection. Depending on the selected destination, the login screen of the destination server appears. Log in with your access credentials.

Please note that when you close the VPN connection window, the application using that VPN connection will also close automatically.

If a VPN connection cannot be opened, you will be shown an error message. In this case, please contact your IT administration, user support, or the ECOS Helpdesk. For further information about error messages, please refer to *8.1 Troubleshooting*.



VPN Verbindung

Verbunden mit ipsecvpn.test.ecos.de

Tunnel Adresse: 10.164.196.93

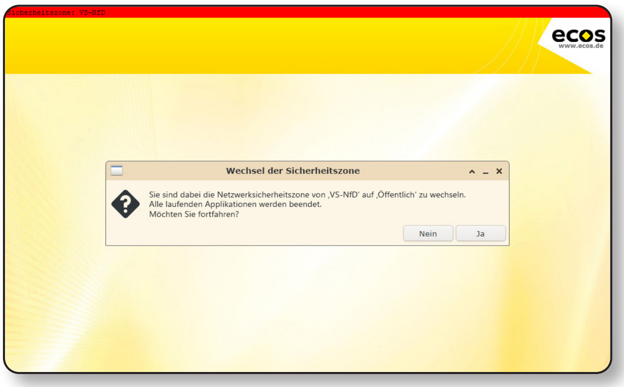
Fig. 5.02: *VPN connection with tunnel address*

5.2 Security zones in SBS version 8

Version 8 introduces security zones to prevent data leakage.

Setting up security zones allows your IT administration to classify access to destinations based on their connection.

When multiple security zones have been configured, SBS users cannot simultaneously open destinations that belong to different security zones. An active security zone is highlighted with a color and the name of the security zone at the top of the SBS desktop. Different security zones are highlighted with distinct colors.



Sie sind dabei die Netzwerksicherheitszone von ‚VS-NfD' auf ‚Öffentlich' zu wechseln.
Alle laufenden Applikationen werden beendet.
Möchten Sie fortfahren?

Fig. 5.03: *Change of security zone*

If you open a destination that belongs to a different security zone than the one you are currently working in, the active destinations are terminated and the memory is cleared.

A message box notifies you that the active destination is being terminated. Press Yes to confirm and open the new destination. Press No to cancel.

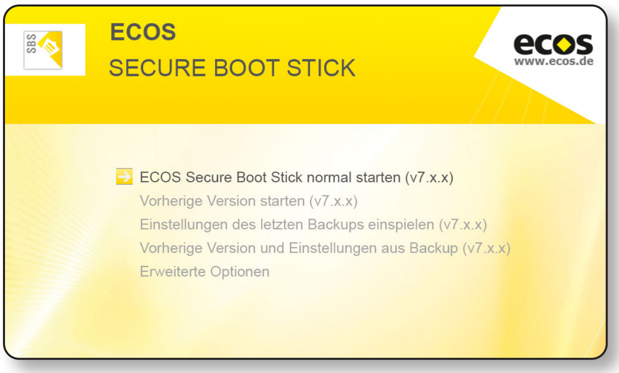
Part 2: Settings

6 SBS boot menu

Depending on your computer model and its hardware, you may need to adjust some settings in order for the SBS to boot properly. The SBS boot menu offers diverse options for this purpose.

The SBS desktop launches 5 seconds after the boot menu is displayed.

To interrupt this autostart and open the SBS boot menu, press the ↑ and ↓ keys. Select a menu item and press ENTER to confirm.



ECOS Secure Boot Stick normal starten (v7.x.x)
Vorherige Version starten (v7.x.x)
Einstellungen des letzten Backups einspielen (v7.x.x)
Vorherige Version und Einstellungen aus Backup (v7.x.x)
Erweiterte Optionen

Fig. 6.01: *SBS boot menu*

Please note: Since v7.x.30, the version number behind the menu items indicates which software version you can start.

6.1 Start ECOS Secure Boot Stick (v7.x.x)

This option allows you to start the SBS with the latest installed software and without additional settings. Depending on your SBS variant and the configuration made by your IT administration, you will be prompted to enter either a boot password or a smartcard PIN. For further information, please refer to section *6.6 SBS login*.

6.2 Start previous version (v7.x.x)

This option allows you to start the SBS with the previously installed software version without additional settings. It is useful if you have trouble starting the SBS after an update.

6.3 Restore settings from last backup (v7.x.x)

Select this option to start the SBS with the latest installed software version and the last saved configuration. This option is useful if you have trouble using the SBS after changing configuration settings. A backup of the configuration is made available by your IT administration on the SMA.

6.4 Previous version and settings from backup (v7.x.x)

Use this option to start the SBS with the previously installed software version and the last saved configuration. This option is useful if you have trouble using the SBS after an update. A backup of the configuration is made available by your IT administration.

6.5 Advanced options

The advanced options allow you to set additional boot options or run a hardware test.

6.5.1 Set boot options

The boot options allow you to change settings affecting the boot behavior of the SBS. This option is useful if particular hardware or hardware drivers are not supported.

The menu page shows the boot options you can change and their current setting.

- Use the ↑ and ↓ keys to navigate
- Press ENTER to confirm a selection
- Press Esc to return to a previous menu page

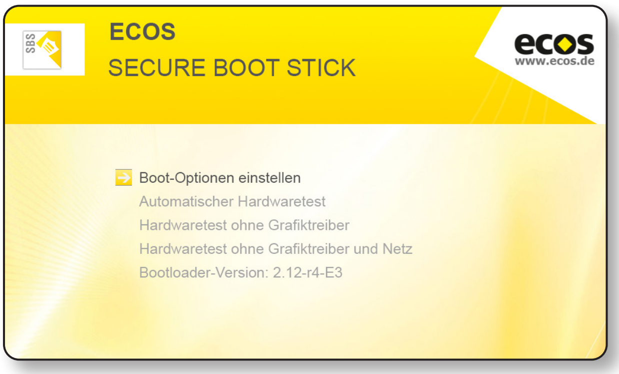
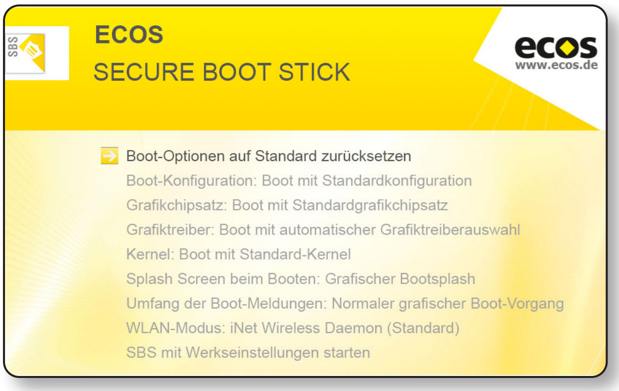

SBS
ECOS
SECURE BOOT STICK
ecos
www.ecos.de
Boot-Optionen einstellen
Automatischer Hardwaretest
Hardwaretest ohne Grafiktreiber
Hardwaretest ohne Grafiktreiber und Netz
Bootloader-Version: 2.12-r4-E3

Fig. 6.02: *Boot options*

6.5.1.1 Reset boot options to default

This will reset the boot options back to their default settings.



Boot-Konfiguration: Boot mit Standardkonfiguration
Grafikchipsatz: Boot mit Standardgrafikchipsatz
Grafiktreiber: Boot mit automatischer Grafiktreiberauswahl
Kernel: Boot mit Standard-Kernel
Splash Screen beim Booten: Grafischer Bootsplash
Umfang der Boot-Meldungen: Normaler grafischer Boot-Vorgang
WLAN-Modus: iNet Wireless Daemon (Standard)
SBS mit Werkseinstellungen starten

Fig. 6.03: *Reset boot options*

6.5.1.2 Boot configuration

Your IT administration may provide various configurations. If you have no information on alternative configurations, select the default configuration.

➡ Boot with default configuration
The SBS boots with the default configuration. This is the SBS default setting.

➡ Boot with alternative configuration 1-4
The SBS boots with the selected alternative configuration. Alternative configurations are defined by your IT administration and cannot be edited by SBS users.

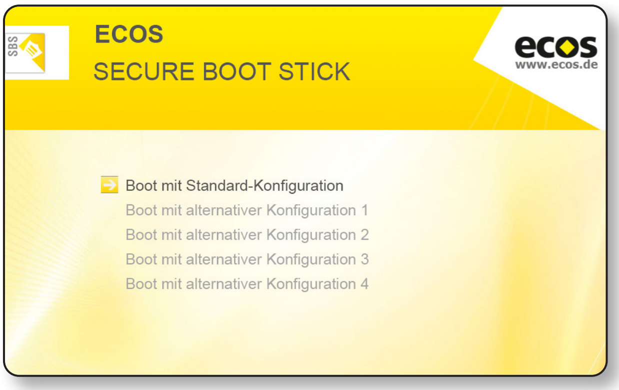

SBS
ECOS
SECURE BOOT STICK
ecos
www.ecos.de
Boot mit Standard-Konfiguration
Boot mit alternativer Konfiguration 1
Boot mit alternativer Konfiguration 2
Boot mit alternativer Konfiguration 3
Boot mit alternativer Konfiguration 4

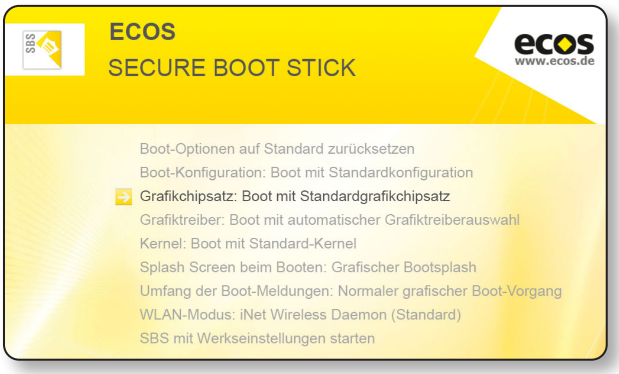
Fig. 6.04: *Boot configuration options*

6.5.1.3 Graphics chipset

Many modern computers contain more than one graphics card and therefore more than one graphics chipset.

The SBS selects the optimal chipset for graphics output automatically. However, if you are experiencing output problems, this option allows you to manually select a graphics chipset.

Frequently, a small sticker on your laptop indicates which graphics card is installed. Alternatively, you can find it in the system settings of your usual operating system.



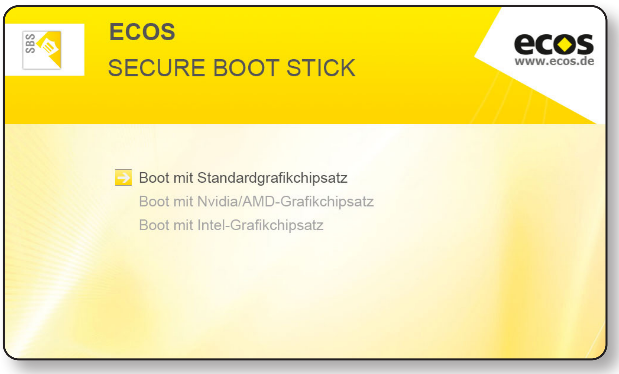
ECOS
SECURE BOOT STICK

ecos www.ecos.de

Boot-Optionen auf Standard zurücksetzen
Boot-Konfiguration: Boot mit Standardkonfiguration
➡ Grafikchipsatz: Boot mit Standardgrafikchipsatz
Grafiktreiber: Boot mit automatischer Grafiktreiberauswahl
Kernel: Boot mit Standard-Kernel
Splash Screen beim Booten: Grafischer Bootsplash
Umfang der Boot-Meldungen: Normaler grafischer Boot-Vorgang
WLAN-Modus: iNet Wireless Daemon (Standard)
SBS mit Werkseinstellungen starten

Fig. 6.05: *Options for graphics chipset*

Boot with default graphics chipset
The SBS boots with an automatically selected graphics chipset. This is the SBS default setting.



ECOS
SECURE BOOT STICK

ecos www.ecos.de

➡ Boot mit Standardgrafikchipsatz
Boot mit Nvidia/AMD-Grafikchipsatz
Boot mit Intel-Grafikchipsatz

Fig. 6.06: *Boot with default graphics chipset*

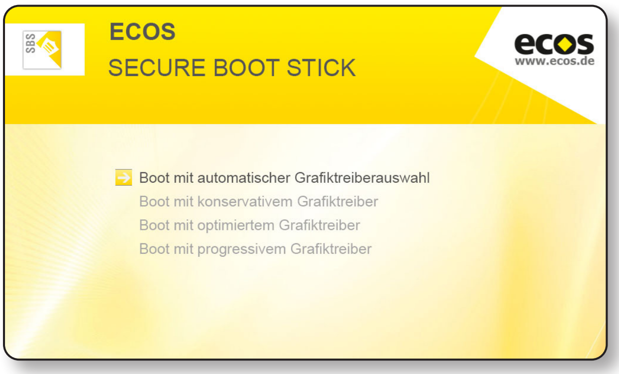
Boot with Nvidia/AMD graphics chipset
The SBS boots with a graphics chipset from Nvidia and AMD. Select this option if your device is equipped with a graphics card from one of these vendors.

Boot with Intel graphics chipset
The SBS boots with a graphics chipset from Intel. Select this option if your device is equipped with a graphics card from this vendor.

6.5.1.4 Graphics driver

Launching the correct graphics driver during the boot process is essential for a flawless graphics output because the operating system uses this driver to control the graphics card.

The Secure Boot Stick selects the optimal graphics driver automatically. However, if you are experiencing output problems, this subpage of the SBS boot menu allows you to manually select a graphics driver.



ECOS
SECURE BOOT STICK

ecos www.ecos.de

➡ Boot mit automatischer Grafiktreiberauswahl
Boot mit konservativem Grafiktreiber
Boot mit optimiertem Grafiktreiber
Boot mit progressivem Grafiktreiber

Fig. 6.07: *Boot with automatic graphics driver selection*

Boot with automatic graphics driver selection
The SBS boots with an automatically selected graphics driver. This is the SBS default setting.

➔ Boot with conservative graphics driver

The SBS boots with a reliable, older open source graphics driver that supports graphics cards from multiple vendors. Be aware that recent graphics cards may not be supported by older drivers.

➔ Boot with enhanced graphics driver

The SBS boots with an optimized/proprietary graphics driver from the graphics card vendor.

➔ Boot with progressive graphics driver

The SBS boots with the latest graphics driver from the respective graphics card vendor. Select this option if you are using a docking station with your computer.

6.5.1.5 Kernel

The kernel is the core of an operating system, on which all other components rely. The Secure Boot Stick supports various older kernel versions, which can be selected manually.

SBS kernel versions can change with an update, which is why the version numbers are indicated in the SBS boot menu.

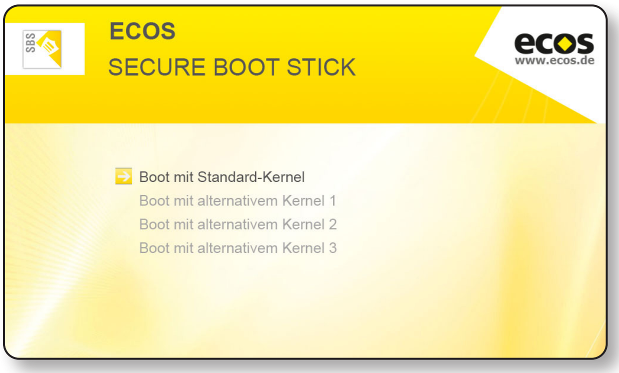
For older computers, changing the kernel can solve booting problems that may occur after an update of the SBS.

➔ Boot with default kernel

The SBS boots with the currently installed default kernel. This is the SBS default setting.

➔ Boot with alternative kernel 1-3

The SBS boots with an alternative, older kernel version.



ECOS
SECURE BOOT STICK

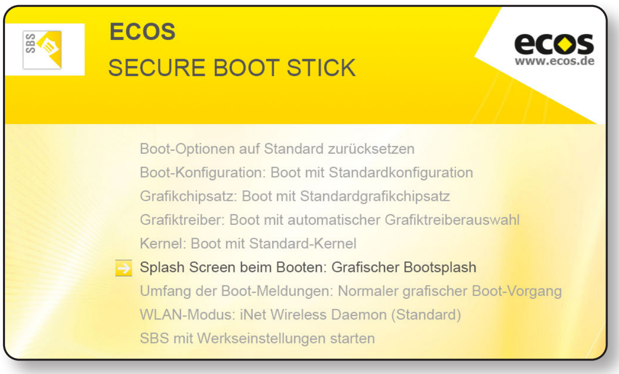
➔ Boot mit Standard-Kernel
Boot mit alternativem Kernel 1
Boot mit alternativem Kernel 2
Boot mit alternativem Kernel 3

Fig. 6.08: *Boot with default kernel*

6.5.1.6 Splashscreen during boot

A splashscreen or bootsplash is the graphical display during the boot process or when starting a program. It is also called the start screen.

Some graphics chipsets do not fully support graphical display during the boot process. The screen freezes or goes black and the boot process crashes. Change the boot splash manually to resolve this problem.



ECOS
SECURE BOOT STICK

Boot-Optionen auf Standard zurücksetzen
Boot-Konfiguration: Boot mit Standardkonfiguration
Grafikchipsatz: Boot mit Standardgrafikchipsatz
Grafiktreiber: Boot mit automatischer Grafiktreiberauswahl
Kernel: Boot mit Standard-Kernel
➔ Splash Screen beim Booten: Grafischer Bootsplash
Umfang der Boot-Meldungen: Normaler grafischer Boot-Vorgang
WLAN-Modus: iNet Wireless Daemon (Standard)
SBS mit Werkseinstellungen starten

Fig. 6.09: *Splashscreen options*

➔ Graphical bootsplash

The SBS boots with a graphical output of the boot process. This is the SBS default setting.

Textmode bootsplash
The SBS boots with a text output of the boot process.

No bootsplash
The SBS boots without displaying any graphical output of the boot process.

6.5.1.7 Boot message extent

System messages are useful for quick troubleshooting when problems arise during the boot process.

You can manually adjust the scope of the system messages.

Default graphical boot
The SBS boots without displaying any system messages. This is the SBS default.

Show detailed boot messages
The SBS displays relevant system messages.

Show very detailed boot messages
The SBS displays all system messages.

6.5.1.8 WLAN mode

Updating the SBS may affect wireless LAN support on older network interface controllers, leaving you unable to connect to the Internet.

While many recent network interface controllers and access points support WPA3 encryption to secure the wireless network, older network interface controllers often do not support this encryption.

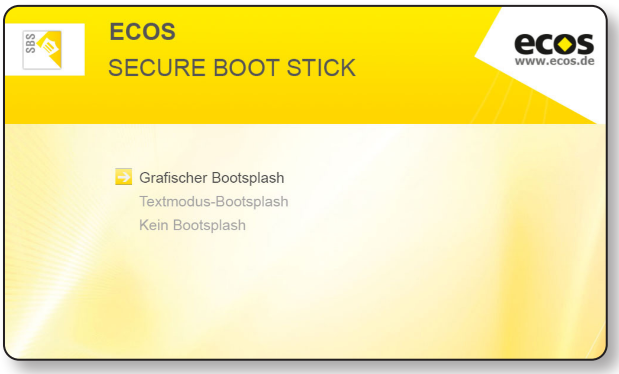


Fig. 6.10: *Select graphical bootsplash*

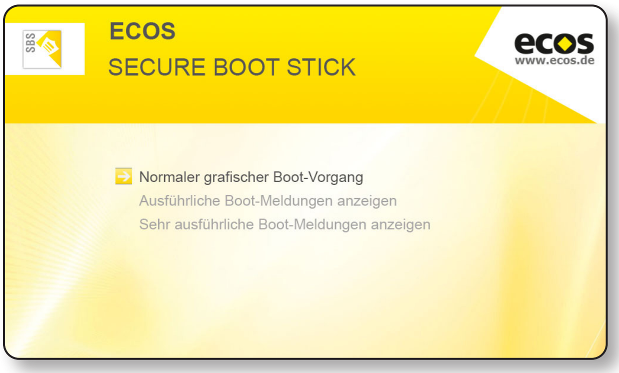
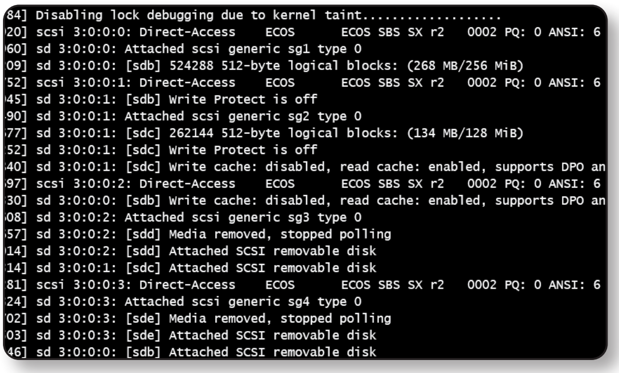

SBS
ECOS
SECURE BOOT STICK
ecos
www.ecos.de
Normaler grafischer Boot-Vorgang
Ausführliche Boot-Meldungen anzeigen
Sehr ausführliche Boot-Meldungen anzeigen

Fig. 6.11: *Boot message options*



```
84] Disabling lock debugging due to kernel taint...................
20] scsi 3:0:0:0: Direct-Access     ECOS      ECOS SBS SX r2   0002 PQ: 0 ANSI: 6
60] sd 3:0:0:0: Attached scsi generic sg1 type 0
09] sd 3:0:0:0: [sdb] 524288 512-byte logical blocks: (268 MB/256 MiB)
52] scsi 3:0:0:1: Direct-Access     ECOS      ECOS SBS SX r2   0002 PQ: 0 ANSI: 6
45] sd 3:0:0:1: [sdb] Write Protect is off
90] sd 3:0:0:1: Attached scsi generic sg2 type 0
77] sd 3:0:0:1: [sdc] 262144 512-byte logical blocks: (134 MB/128 MiB)
52] sd 3:0:0:1: [sdc] Write Protect is off
40] sd 3:0:0:1: [sdc] Write cache: disabled, read cache: enabled, supports DPO an
97] scsi 3:0:0:2: Direct-Access     ECOS      ECOS SBS SX r2   0002 PQ: 0 ANSI: 6
30] sd 3:0:0:0: [sdb] Write cache: disabled, read cache: enabled, supports DPO an
08] sd 3:0:0:2: Attached scsi generic sg3 type 0
57] sd 3:0:0:2: [sdd] Media removed, stopped polling
14] sd 3:0:0:2: [sdd] Attached SCSI removable disk
14] sd 3:0:0:1: [sdc] Attached SCSI removable disk
81] scsi 3:0:0:3: Direct-Access     ECOS      ECOS SBS SX r2   0002 PQ: 0 ANSI: 6
24] sd 3:0:0:3: Attached scsi generic sg4 type 0
02] sd 3:0:0:3: [sde] Media removed, stopped polling
03] sd 3:0:0:3: [sde] Attached SCSI removable disk
46] sd 3:0:0:0: [sdb] Attached SCSI removable disk
```

Fig. 6.12: *Very detailed output*

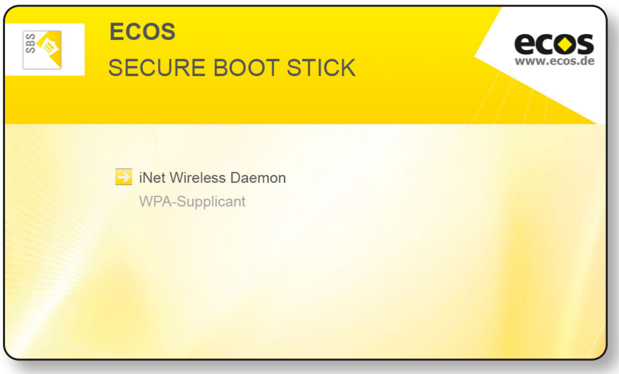


Fig. 6.13: *Select wireless LAN mode*

Since SBS v7.x.36, you can manually enable support for older network interface controllers and WPA3 encryption. Please note that your built-in network interface controller must also support WPA3 encryption.

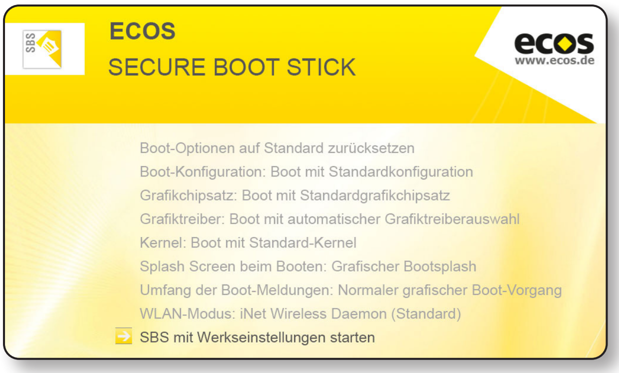
➡ iNet Wireless Daemon
The SBS boots with support for newer network cards as well as WPA2 and WPA3 encryption. This is the SBS default setting.

➡ WPA supplicant
The SBS boots with support for older network cards and WPA2 encryption.

6.5.1.9 Start SBS with factory settings

This option resets the SBS to the factory settings. It deletes all settings made by you and your IT administration.

For further use, the SBS must be reactivated. In this case, please contact your IT administration or user support.



ECOS
SECURE BOOT STICK

Boot-Optionen auf Standard zurücksetzen
Boot-Konfiguration: Boot mit Standardkonfiguration
Grafikchipsatz: Boot mit Standardgrafikchipsatz
Grafiktreiber: Boot mit automatischer Grafiktreiberauswahl
Kernel: Boot mit Standard-Kernel
Splash Screen beim Booten: Grafischer Bootsplash
Umfang der Boot-Meldungen: Normaler grafischer Boot-Vorgang
WLAN-Modus: iNet Wireless Daemon (Standard)
➡ SBS mit Werkseinstellungen starten

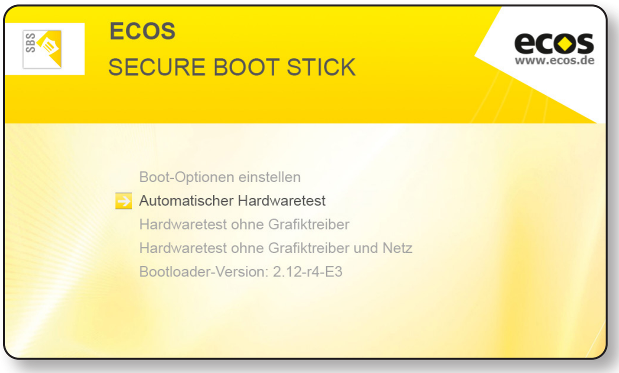
Fig. 6.14: *Start SBS with factory settings*

6.5.2 Automatic hardware test

Hardware tests are used to analyze a computer's hardware and a valuable tool for keeping the SBS software compatible with the latest computer models.

In addition to information such as vendor, model, serial number, hardware components, and drivers, the hardware test also contains information about your SBS, such as current version and variant.

The hardware test does not gather any personal data or files.



ECOS
SECURE BOOT STICK

Boot-Optionen einstellen
➡ Automatischer Hardwaretest
Hardwaretest ohne Grafiktreiber
Hardwaretest ohne Grafiktreiber und Netz
Bootloader-Version: 2.12-r4-E3

Fig. 6.15: *Automatic hardware test*

You will need an additional USB flash drive to store the results file that is generated during the hardware test. This additional USB flash drive must have been formatted with the FAT32 file system. To format the USB flash drive, please refer to *9.3 How to format a USB flash drive*.

The automatic hardware test runs a full scan of hardware components installed on your computer.

1. Connect your SBS and the additional USB flash drive to your computer's USB ports.

2. Start your computer.

3. When the SBS boot menu appears, cancel the autostart of the SBS desktop by pressing the ↑ and ↓ keys.

4. Use the ↓ key to select the menu item ADVANCED OPTIONS and press ENTER to confirm.

5. Use the ↓ key to select the menu item AUTOMATIC HARDWARE TEST and press ENTER to confirm.

6. The SBS starts the hardware test. The test takes about three minutes.
   Enter your smartcard PIN or start password when you are prompted to do so.

7. Once the hardware test is complete, your computer shuts down automatically.
   If your computer does not shut down, switch it off manually after about three minutes by pressing and holding the power button.

8. Unplug the SBS from the USB port, but keep the other USB flash drive plugged in. Boot your computer with your regular operating system.

9. Open your file manager and the additionally USB flash drive. The hardware test file is named **hwtest.txt**.

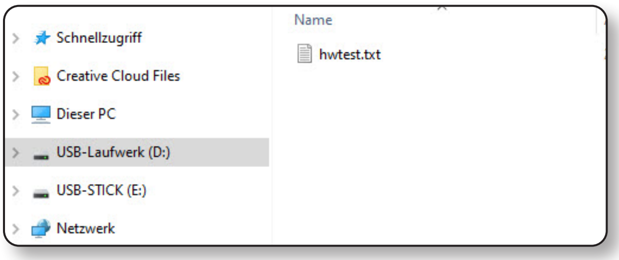


Fig. 6.17: *Output file on USB flash drive*

10. Send the file with a brief error description by e-mail to **hwtest@ecos.de**.

6.5.3 Hardware test without graphics drivers

Select this option if the automatic hardware test does not return a results file.

6.5.4 Hardware test without graphics drivers and network

Select this option if the automatic hardware test does not return a results file.

6.5.5 Bootloader version

Shows the current bootloader version. This options has no function.

6.6 SBS login

Depending on the variant and the settings made by your IT administration, the Secure Boot Stick will prompt you to enter either a start password or a smartcard PIN during the boot process to protect the SBS from unauthorized access. Without this entry, the SBS aborts the boot process and displays a corresponding message on the screen.

If your SBS has already been activated by your IT administration, you received either the smartcard PIN or the start password along with your SBS. Change start password or smartcard PIN immediately the first time you use the SBS. If you use an Apple device, connect an external keyboard to your Mac to be able to log in to the SBS.

If you activate your SBS yourself, set the smartcard PIN or the start password during Easy Enrollment. Please note that your IT administration may have defined password guidelines such as the minimum number of digits, characters or character classes your password must contain.

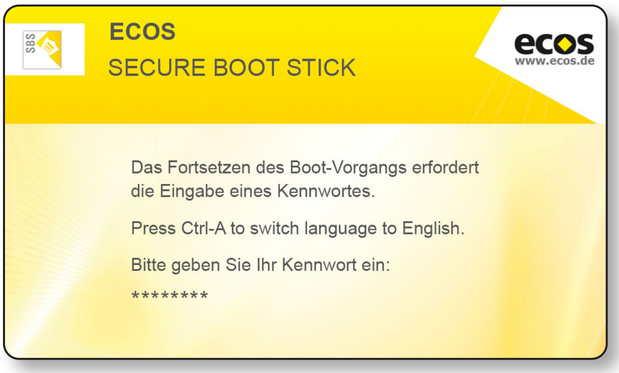
6.6.1 Start password

The SBS variants CL and HE require a start password.

Enter the password on your computer keyboard and press ENTER to confirm.

For further information on how to change the start password, please refer to *7.4.3.6 Change start password*.

If you have lost your password, please contact your IT administration or user support immediately.



Das Fortsetzen des Boot-Vorgangs erfordert die Eingabe eines Kennwortes.

Press Ctrl-A to switch language to English.

Bitte geben Sie Ihr Kennwort ein:

```
********
```

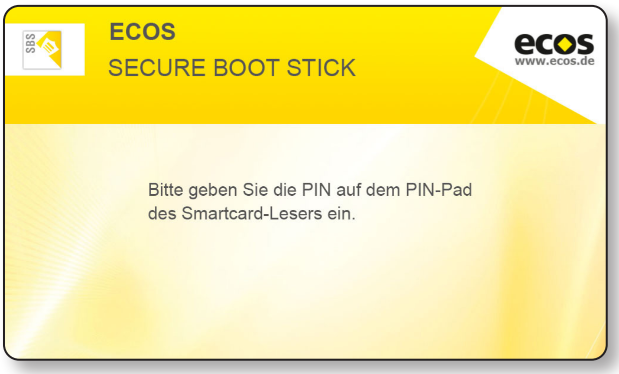
Fig. 6.18: *Password entry prompt on SBS CL or HE*

6.6.2 Smartcard PIN

The SBS variants FX/SX and GX/ZX require a smartcard PIN.

The ECOS key on the PIN pad flashes yellow when the SBS expects a PIN entry. Enter the smartcard PIN on the PIN pad and press the ✓ key to confirm.

If the PIN is correct the ECOS key lights yellow. If the entry is incorrect, the ECOS key lights red, then flashes red. After a few seconds, the ECOS key flashes yellow and you can enter the smartcard PIN again.



Bitte geben Sie die PIN auf dem PIN-Pad des Smartcard-Lesers ein.

Fig. 6.19: *PIN entry prompt on SBS FX/SX and GX/ZX*

You have approximately 60 seconds to enter the PIN before the PIN entry is cancelled.

You have three attempts to enter your smartcard PIN. After the third unsuccessful attempt, the SBS is locked and can only be unlocked with the PUK. Please contact your IT administration or user support for the PUK.

6.6.2.1 Change smartcard PIN

You can change the smartcard PIN manually on the SBS PIN pad.

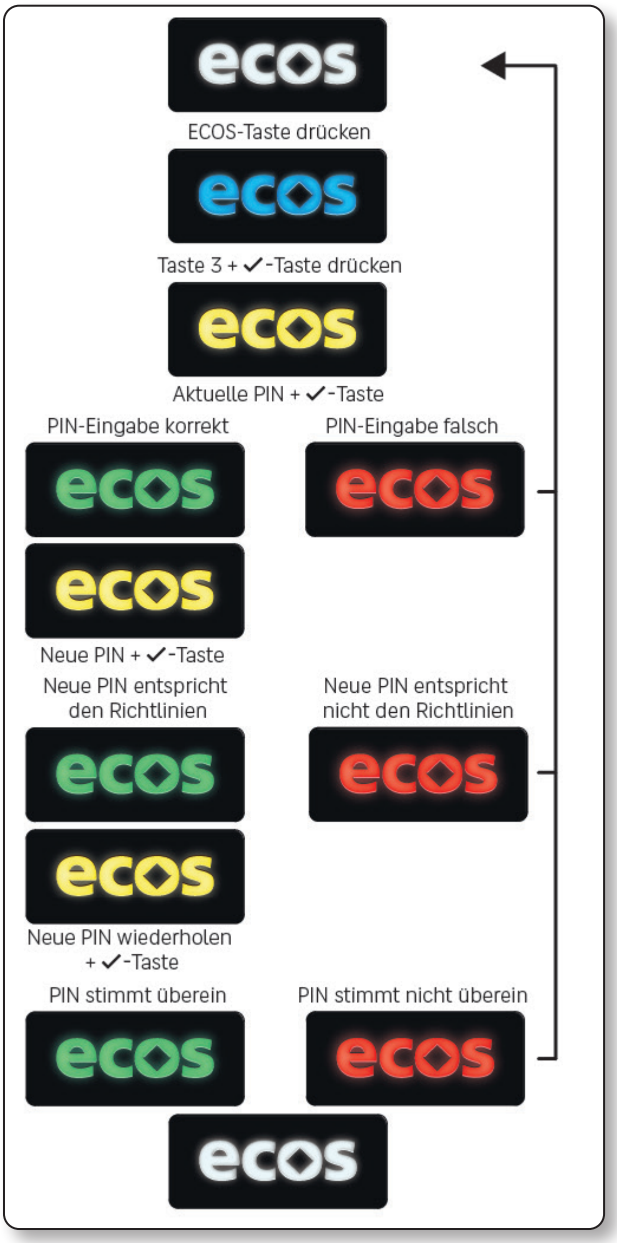


Fig. 6.20: *Change smartcard PIN*

1. Connect your SBS to your computer's USB port. Make sure the SBS has power.
   The ECOS key lights white.

2. Press the ECOS key.
   It lights dark blue, the digit keys are white.

3. Press 3 to change the smartcard PIN.
   The ECOS key lights yellow.

4. Press the ✓ key to confirm.
   The ECOS key flashes yellow.

5. Enter the current smartcard PIN.
   The ECOS key flashes yellow during entry.

6. Press the ✓ key to confirm.
   If the PIN is correct, the ECOS key briefly lights green, then flashes yellow.
   If the PIN is incorrect, the ECOS key briefly lights red, then white. The process is cancelled. Repeat the procedure beginning with step 2.

7. Enter a new smartcard PIN.
   The ECOS key flashes yellow during entry.

8. Press the ✓ key to confirm.
   If the new smartcard PIN complies with the password guidelines, the ECOS key briefly lights green, then flashes yellow.
   If the new smartcard PIN does not comply with the guidelines, the ECOS key briefly lights red, then white again. The process is canceled. Repeat the procedure beginning with step 2.

9. Re-enter the new smartcard PIN. The ECOS key flashes yellow during entry.

11. Press the ✓ key to confirm.

If the PIN is correct, the ECOS key briefly lights green, then white. The smartcard PIN was changed successfully.
If the PIN is incorrect, the ECOS key briefly lights red, then white. The process is canceled. Repeat the procedure beginning with step 2.

6.6.2.2 Reset smartcard PIN

If you lose your smartcard PIN or enter it incorrectly three times, your smartcard PIN must be reset. Please contact your IT administration or user support to obtain the PUK.

1. Connect your SBS to your computer's USB port. Make sure the SBS has power.
   The ECOS key lights white.

1. Press the ECOS key.
   It lights dark blue and the digit keys are white.

2. Press 4 to reset the smartcard PIN.
   The ECOS key lights light blue.

3. Press the ✓ key to confirm.
   The ECOS key flashes light blue.

4. Enter the PUK.
   The ECOS key flashes light blue during entry.

5. Press the ✓ key to confirm.
   If the PIN is correct, the ECOS key briefly lights green, then flashes yellow.
   If the PIN is incorrect, the ECOS key briefly lights red, then white.
   The process is canceled. Repeat the procedure beginning with step 2.

6. Enter a new smartcard PIN.
   The ECOS key flashes yellow during entry.

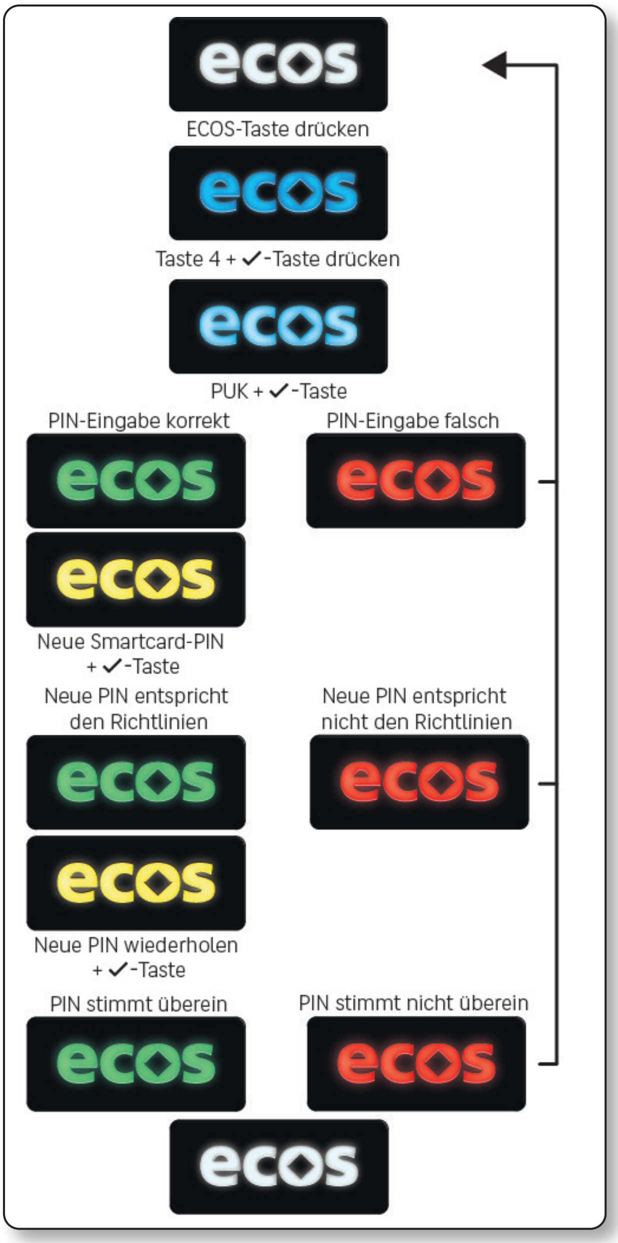

ecos
ECOS-Taste drücken
ecos
Taste 4 + ✓-Taste drücken
ecos
PUK + ✓-Taste
PIN-Eingabe korrekt
PIN-Eingabe falsch
ecos
ecos
ecos
Neue Smartcard-PIN + ✓-Taste
Neue PIN entspricht den Richtlinien
Neue PIN entspricht nicht den Richtlinien
ecos
ecos
ecos
Neue PIN wiederholen + ✓-Taste
PIN stimmt überein
PIN stimmt nicht überein
ecos
ecos
ecos

Fig. 6.21: *Smartcard PIN reset*

7. Press the ✓ key to confirm.
   If the new smartcard PIN complies with the password guidelines, the ECOS key briefly lights green, then flashes yellow.
   If the new smartcard PIN does not comply with the guidelines, the ECOS key briefly lights red, then white. The process is canceled. Repeat the procedure beginning with step 2.

8. Re-enter the new smartcard PIN.
   The ECOS key flashes yellow during entry.

9. Press the ✓ key to confirm.
   If the PIN is correct, the ECOS key briefly lights green, then white. The smartcard PIN has been successfully reset.
   If the PIN is incorrect, the ECOS key briefly lights red, then white. The process is canceled. Repeat the procedure beginning with step 2.

7 SBS Desktop

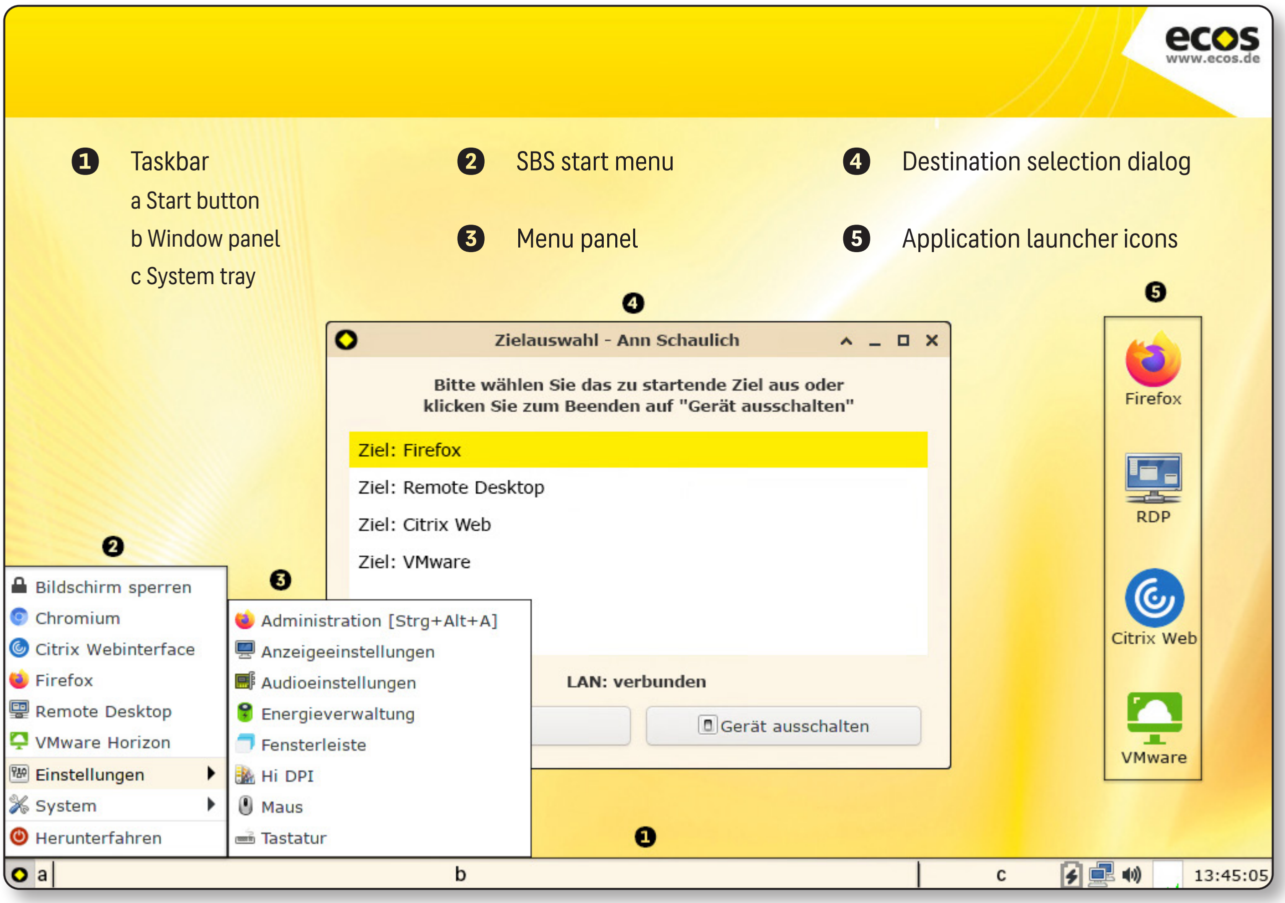
The SBS desktop is the main graphical interface of the Secure Boot Stick and includes a taskbar and a desktop background. The taskbar is organized into three sections:

- **Start button**
  The start button opens the SBS start menu and the two menu panels **Settings** and **System**.

- **Window panel**
  The window panel displays the tabs of all open application windows.

- **System tray**
  The system tray contains various indicators that provide information about the system, power, Internet connection, system time, and more.

Depending on your IT administration's configuration, the destinations enabled for your user account may be displayed in the start menu panel and as application launchers icons on the desktop.



1 Taskbar
a Start button
b Window panel
c System tray

2 SBS start menu

3 Menu panel

4 Destination selection dialog

5 Application launcher icons

Zielauswahl - Ann Schaulich

Bitte wählen Sie das zu startende Ziel aus oder klicken Sie zum Beenden auf "Gerät ausschalten"

Ziel: Firefox
Ziel: Remote Desktop
Ziel: Citrix Web
Ziel: VMware

LAN: verbunden

Fig. 7.01: *SBS desktop*

7.1 Start button

Click on the start button to open the SBS start menu. For further information on the SBS start menu and its functions, please refer to section *7.4 SBS Start menu*.

7.2 Taskbar

The window panel of the taskbar displays the tabs of all open windows and applications. Right-click on a tab in the window panel (alternatively on the window title bar) to open the context menu of the window with the following options:

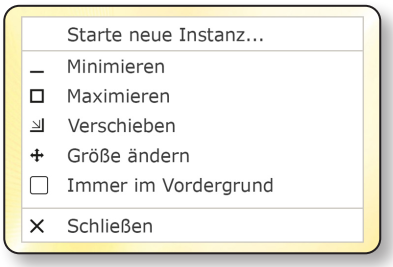


Fig. 7.02: *Window context menu*

LAUNCH NEW INSTANCE: This option launches a new instance of the running application.

MINIMIZE: Minimizes an open window to a tab on the window panel of the taskbar. Click on the tab to maximize the window.

MAXIMIZE: Enlarges a window to full-screen view. Click the menu item again to unmaximize.

MOVE: The mouse pointer grabs the title bar of the window. Move the mouse pointer around to move the window. Click to save its new position. Alternatively, move the window by dragging the window title bar.

RESIZE: The mouse pointer grabs the right bottom edge of the window. Move the mouse pointer around to enlarge or reduce the window. Click to save the new window size.

ALWAYS ON TOP: Enable this checkbox to keep the window on top of other active windows or applications.

CLOSE: Closes the window. Alternatively, close the window using the ✕ icon in the window title bar.

7.3 System tray

7.3.1 Network manager

Use the network manager applet in the system tray to set up and edit Internet connections. To learn how to add a new connection, please refer to section *6.5.2 Automatic hardware test*.

Right-click on the network manager icon to open a context menu with following options:

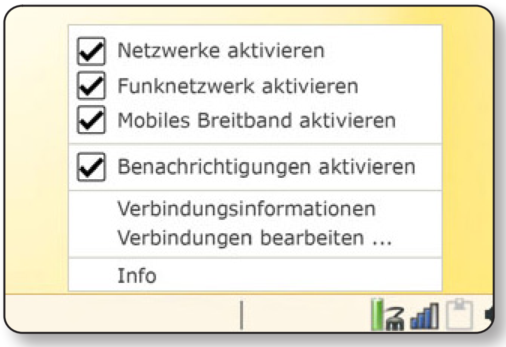

☑ Netzwerke aktivieren
☑ Funknetzwerk aktivieren
☑ Mobiles Breitband aktivieren
☑ Benachrichtigungen aktivieren
Verbindungsinformationen
Verbindungen bearbeiten ...
Info

Fig. 7.03: *Context menu of network manager*

ENABLE NETWORKING: Enables the general use of the Internet.

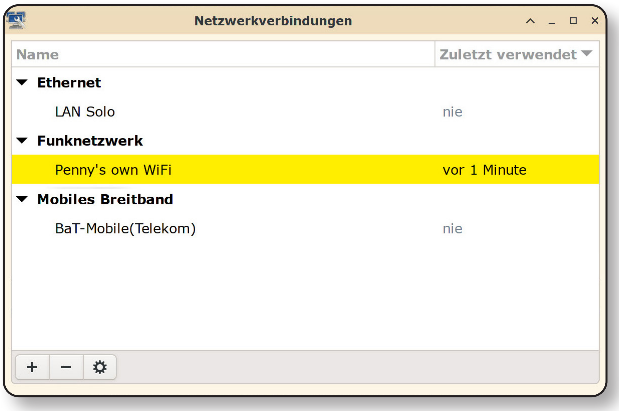
Enable Wi-Fi: This checkbox activates the use of wireless LAN and networks. This option is only displayed if the **Enable networking** checkbox is enabled.

Enable mobile broadband: Enables the use of mobile networks. This option is displayed if your computer is equipped with a mobile or LTE modem .

Enable notifications: Enables notifications from the network manager.

Connection information: Opens the connection information window, which displays information on the active connection, e.g. current IP address.

Edit connections: Opens the network connections dialog, in which you can add (+), delete (−) and edit (⚙) connections. Save your changes and, if necessary, reconnect to apply your changes.



Netzwerkverbindungen

Name	Zuletzt verwendet
Ethernet	
LAN Solo	nie
Funknetzwerk	
Penny's own WiFi	vor 1 Minute
Mobiles Breitband	
BaT-Mobile(Telekom)	nie

Fig. 7.04: *Edit network connections*

About: Opens the software information window of the Network Manager applet.

Edit connections

Delete the selected connection (−): Select the connection you wish to delete. Click the (−) button. In the next window, confirm that you wish to delete the selected connection by pressing 'Delete' or cancel the operation. The connection is deleted from the network connections list.

Edit the selected connection (⚙): Opens the editing dialog for the selected connection. This dialog also appears when you set up a new ethernet or wireless network connection. You can change the name of the connection in the 'Connection name' field located above the editing menu.

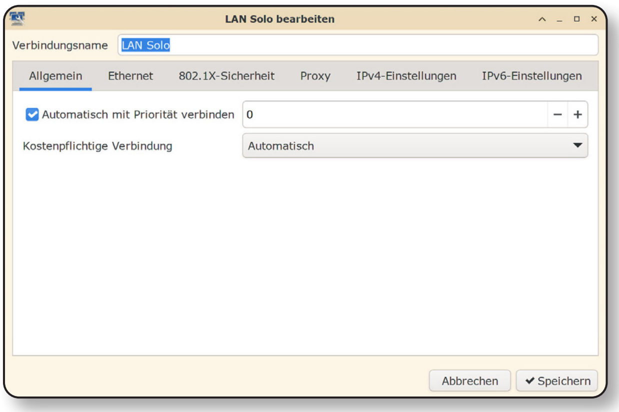
Depending on whether the network connection is LAN, wireless or mobile, the editing menu displays different tabs and functions.

Tab	Ethernet	Wireless network	Mobile broadband
General	✓	✓	✓
Ethernet (LAN)	✓	-	-
802.1x Security	✓	-	-
Wireless network (WLAN)	-	✓	-
Security of the wireless network	-	✓	-
Mobile broadband	-	-	✓
PPP settings	-	-	✓
Proxy	✓	✓	✓
IPv4 settings	✓	✓	✓
IPv6 settings	✓	✓	✓

General

Connect automatically with priority: Enable and determine the priority with which the SBS connects to this network. The lower the number, the higher the priority. For example, if you assign priority 1 to a LAN connection and priority 2 to a wireless LAN connection, the SBS connects via LAN first and only uses the WLAN connection if the wired connection is not available.

Metered connection: Select whether the network is metered or not.



LAN Solo bearbeiten

Verbindungsname: LAN Solo

Allgemein | Ethernet | 802.1X-Sicherheit | Proxy | IPv4-Einstellungen | IPv6-Einstellungen

☑ Automatisch mit Priorität verbinden: 0 − +

Kostenpflichtige Verbindung: Automatisch

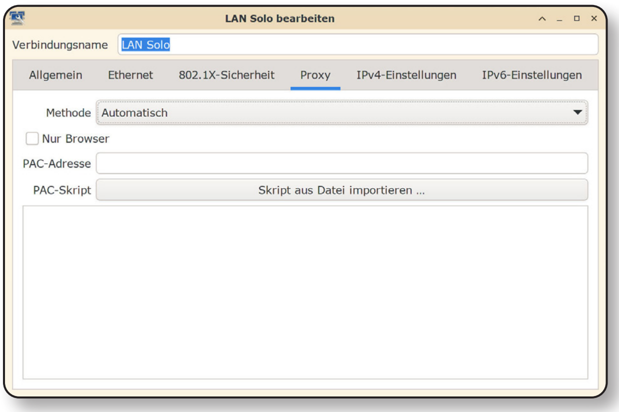
Fig. 7.05: *General settings*

Proxy

Method: Enable the use of a proxy for the network connection. You can choose between None and Automatic.

For browser only: Allows only the browser to use a proxy.

PAC URL: Enter the URL under which the PAC file (proxy auto-config file) is made accessible to the browser. It enables a browser to use the appropriate proxy for each URL.



LAN Solo bearbeiten

Verbindungsname: LAN Solo

Allgemein | Ethernet | 802.1X-Sicherheit | Proxy | IPv4-Einstellungen | IPv6-Einstellungen

Methode: Automatisch

□ Nur Browser

PAC-Adresse:

PAC-Skript: Skript aus Datei importieren ...

Fig. 7.06: *Proxy settings*

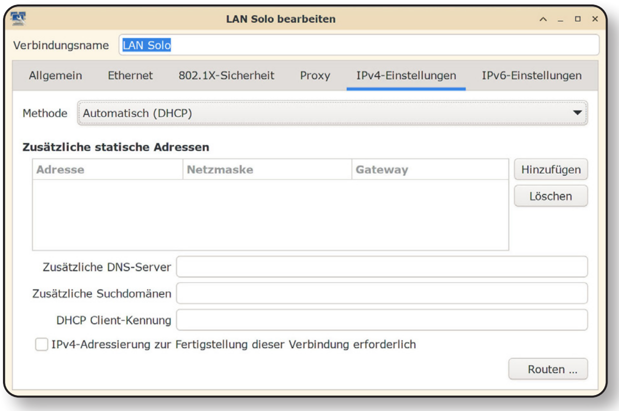
PAC script: Import a PAC script from a local file or enter it manually in the text field.

IPv4 settings

Method: Determines the method for determining the IPv4 settings.

Automatic (DHCP): The IPv4 settings are determined automatically. You can specify additional static addresses, DNS servers or search domains.

Automatic (DHCP), addresses only: The IPv4 address, the netmask and the gateway address are determined automatically via DHCP. Enter DNS server and search domains manually.



LAN Solo bearbeiten

Verbindungsname: LAN Solo

Allgemein | Ethernet | 802.1X-Sicherheit | Proxy | IPv4-Einstellungen | IPv6-Einstellungen

Methode: Automatisch (DHCP)

Zusätzliche statische Adressen

Adresse	Netzmaske	Gateway

Zusätzliche DNS-Server:

Zusätzliche Suchdomänen:

DHCP Client-Kennung:

□ IPv4-Adressierung zur Fertigstellung dieser Verbindung erforderlich

Fig. 7.07: *IPv4 settings*

Manual: The IPv4 settings are defined manually. The settings include the IPv4 address, the netmask, the gateway address as well as the DNS server and the search domains.

Link-local only: The SBS is assigned an IPv4 address in the range of 169.254.0.0 to 169.254.255.255 for this connection. Connecting to the Internet is therefore not possible.

Shared to other computers: When enabling this option, you share the network connection with a device that cannot open a direct network connection.

Disabled: This option disables IPv4 for this network connection.

Addresses: Allows you to enter (additional) static IPv4 addresses with netmask and gateway. You can add new or delete existing addresses.

DNS servers: Allows you to enter (additional) DNS servers. Multiple entries will be listed comma separated.

Search domains: Allows you to enter (additional) search domains. Multiple entries will be listed comma separated.

DHCP client ID: Allows you to enter a client ID. This ID is used instead of the MAC address, therefore, the name must be unique on the network.

Require IPv4 addressing for this connection to complete: When this option is enabled, this connection always uses IPv4 addressing. IPv6 addressing is ignored.

Routes: Allows you to add, edit and delete static routes manually.

Ignore automatically obtained routes: If you enabled this checkbox, this connection will only use the specified routes.

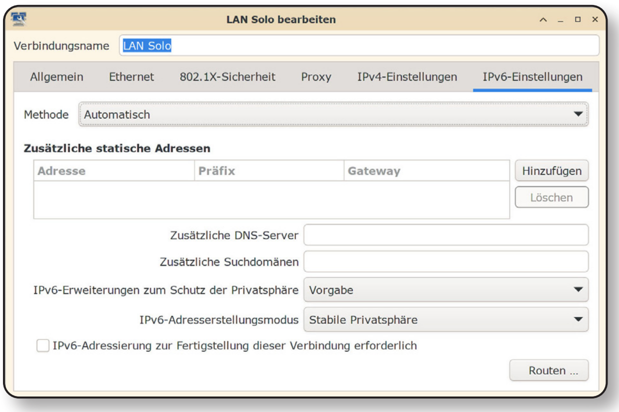
Use this connection only for resources on its network: If you enable this checkbox, connections are restricted to the local network.

IPv6 settings

These settings correspond to those that in the **IPv4 settings** tab.

The Method field offers an additional Ignore option to skip the use of IPv6 for this connection.

IPv6 privacy extensions: IPv6 addresses include the MAC address of the selected network interface controller, which is used to uniquely identify devices. Privacy extensions can be used to further protect privacy.



Verbindungsname: LAN Solo

Methode: Automatisch

Zusätzliche DNS-Server:

Zusätzliche Suchdomänen:

IPv6-Erweiterungen zum Schutz der Privatsphäre: Vorgabe

IPv6-Adresserstellungsmodus: Stabile Privatsphäre

□ IPv6-Adressierung zur Fertigstellung dieser Verbindung erforderlich

Fig. 7.08: *IPv6 settings*

Default: Uses the global settings of the network.

Disabled: The privacy extensions are disabled.

Enabled (prefer public address): The privacy extension is enabled and the public IPv6 address is preferred.

Enabled (prefer temporary address): The privacy extension is enabled and the temporarily generated IPv6 address is preferred.

IPv6 address generation mode: Allows you to define how the IPv6 address is created.

EUI64: The MAC address of the network interface controller is used to determine the address. The device can be identified with the IPv6 address.

Stable privacy: With this option, a secure cryptographic hash of a secret host-specific key is used to determine the address. The device cannot be uniquely identified with the IPv6 address.

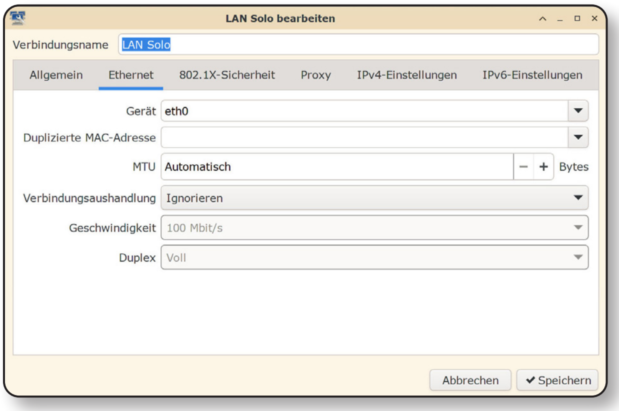
Ethernet

Device: Select the network interface for the built-in network card.

Cloned MAC address : Select how the MAC address of your network interface should be handled. The MAC address or hardware address uniquely identifies a device in a network.

Preserve: The MAC address is not changed.

Permanent: The actual MAC address of the network interface is used.



Verbindungsname: LAN Solo

Gerät: eth0

Duplizierte MAC-Adresse:

MTU: Automatisch − + Bytes

Verbindungsaushandlung: Ignorieren

Geschwindigkeit: 100 Mbit/s

Duplex: Voll

Fig. 7.09: *LAN settings*

Random: A new MAC address is generated for each connection.

Stable: The same incorrect MAC address is used for the same connection.

MTU: Allows you to set the maximum size of the data packets to be transmitted (maximum transmission unit). By default, the MTU is set to Automatic and can be adjusted manually. A value between 700-1000 bytes is recommended.

Link negotiation: Specify how a connection is to be negotiated.

Ignore: The speed and duplex mode of the connection are ignored during negotiation.

Automatic: The speed and duplex mode of the connection are negotiated automatically.

Manual: You can set speed and duplex mode of the connection manually. Please note that all devices in the network must support these settings.

Speed: Set the data transmission speed. It depends on the speed of your Internet access.

Duplex: Set the duplex mode. It determines the direction of the data transmission over a line.

Full: Data is transmitted simultaneously in both directions.

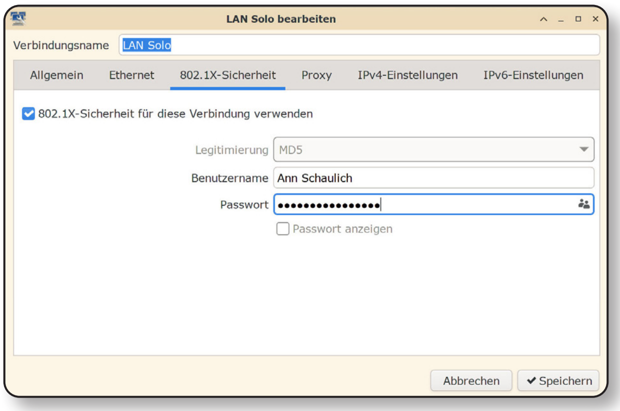
Half: Data is transmitted in both directions, but not simultaneously.

802.1X security

802.1X security for this connection: Enables 802.1X security for the network connection. This is a standard for authentication and authorization in networks.

Legitimization: Set the legitimation with which you authenticate yourself in the network. Currently, only the MD5 (Message-Digest Algorithm 5) authentication method is available.

Username: Enter the username for authentication.



LAN Solo bearbeiten

Verbindungsname: LAN Solo

☑ 802.1X-Sicherheit für diese Verbindung verwenden

Legitimierung: MD5

Benutzername: Ann Schaulich

Passwort: ••••••••••••••••

□ Passwort anzeigen

Fig. 7.10: *802.1X security settings*

Password: Enter the password for authentication. You can make the password visible using the **Show password** checkbox.

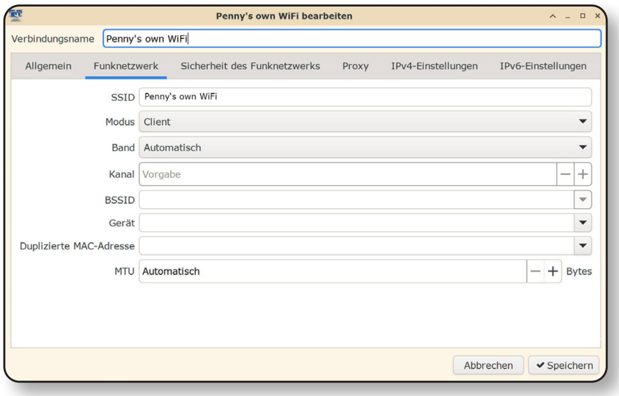
Wireless network

SSID: Enter the SSID of the WLAN network.

Mode: Select the WLAN mode of your network.

Client: In client mode, the SBS logs on to the access point (AP) as a client and connects to the WLAN.

Hotspot: Hotspot mode is a public wireless network that usually requires an additional login to the network.



Penny's own WiFi bearbeiten

Verbindungsname: Penny's own WiFi

SSID: Penny's own WiFi

Modus: Client

Band: Automatisch

Kanal: Vorgabe

BSSID:

Gerät:

Duplizierte MAC-Adresse:

MTU: Automatisch Bytes

Fig. 7.11: *Wi-Fi settings*

Ad-hoc: In ad-hoc mode, client devices connect directly to each other within the network without using an AP.

Band: Set the frequency band of the WLAN connection. The frequency determines, among other things, the range and speed of the wireless LAN. The lower the frequency, the greater the range, but the higher the frequency, the higher the supported speeds.

Automatic: The frequency band is determined automatically. Select this option if you do not know the frequency band of your wireless LAN.

A (5 GHz): The range is usually limited to one floor or an apartment. However, higher speeds are supported. These frequencies are not widely used at present.

B/G (2.4 GHz): The range is greater, often covering entire buildings. Speeds are generally lower as the frequency band is used by a large number of subscribers.

Channel: Set the channel of the frequency band. The frequency bands are split into different channels to ensure a better distribution of participants. Modern routers often have the ability to analyze surrounding wireless networks and the channels they use to find the best channel for your wireless network. If you know the channel of the wireless network you are using, set it accordingly, otherwise select the option default.

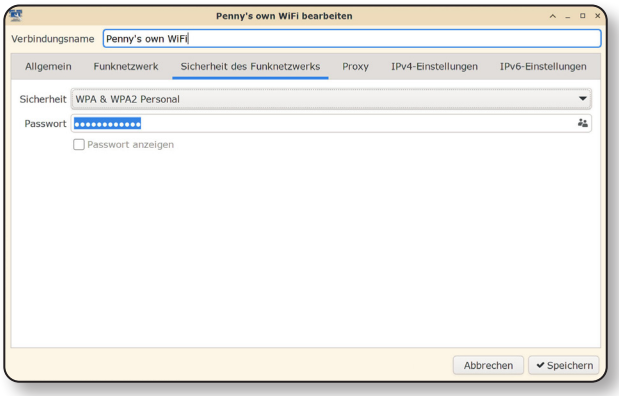
BSSID: Select the basic service set identifier. It usually corresponds to the MAC address of the access point or router and is used for unique identification and assignment to an access point.

Wi-Fi security

Security: Allows you to select the security protocol or encryption method of the wireless network that will be used für client authenticate in the wireless network .

LEAP: This is an outdated standard that should no longer be used.

Dynamic WEP (802.1X): This is an outdated standard that should no longer be used.



Verbindungsname: Penny's own WiFi

Sicherheit: WPA & WPA2 Personal

Passwort: ••••••••••••

□ Passwort anzeigen

Fig. 7.12: *Security settings for Wi-Fi*

WPA/WPA2/WPA3 Personal: This is the current (but expiring) default for WLAN encryption. It is used for private networks and requires a password.

WPA/WPA2 Enterprise: This is the current (but expiring) standard for WLAN encryption. It is used for organizational or company networks.

WPA3 Personal: This is the latest and most secure standard for WLAN encryption. It is not supported by older devices and requires a password.

Enhanced Open: This is a new security standard for open-access wireless hotspots.

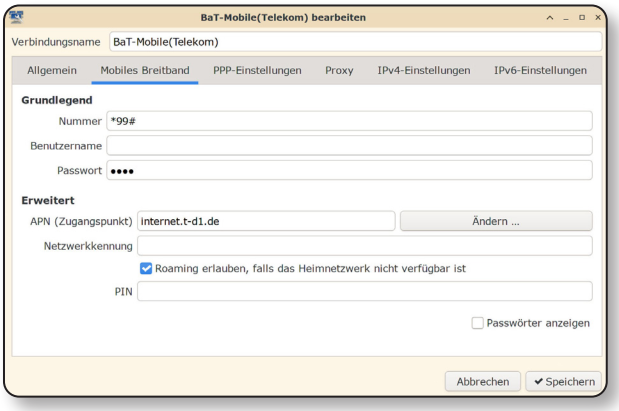
Mobile broadband

Number: Enter your cell phone provider's dial-in number. By default, German providers use the number *99#.

Username: Enter the username.

Password: Enter the password.

APN (access point): Enter the access point name of your cell phone provider.



Verbindungsname: BaT-Mobile(Telekom)

Grundlegend

Nummer: *99#

Benutzername:

Passwort: ••••

Erweitert

APN (Zugangspunkt): internet.t-d1.de

Netzwerkkennung:

☑ Roaming erlauben, falls das Heimnetzwerk nicht verfügbar ist

PIN:

□ Passwörter anzeigen

Fig. 7.13: *Mobile broadband settings*

NETWORK IDENTIFIER: Enter the mobile network code.

ALLOW ROAMING IF HOME NETWORK IS NOT AVAILABLE: Enable the checkbox to allow roaming when your home network is not available. Please note that there may be an additional charge for this service depending on your cell phone plan.

PIN: Enter your SIM card PIN.

Access data, APN and network ID can be obtained from your cell phone provider or on the Internet. Search for your cell provider in connection with APN and/or mobile broadband.

PPP settings

The point-to-point protocol is a network protocol that connects via dial-up lines. The Internet or cell phone provider uses this protocol to communicate the dial-in data (e.g. IP address or DNS server) to the end device.

ALLOWED METHODS: Allows you to enable an authentication method for your mobile broadband connection.

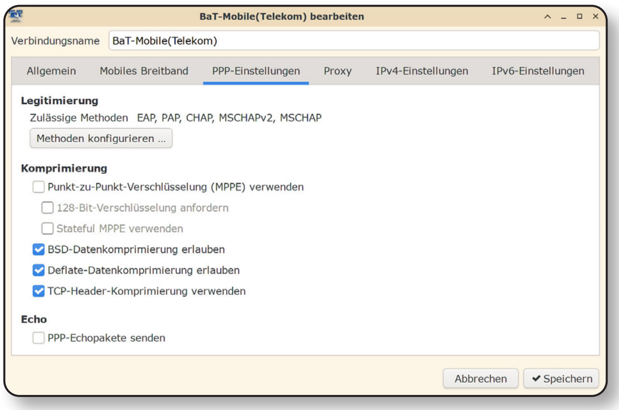
EAP: The extensible authentication protocol is an authentication protocol that is often used in wireless networks.

PAP: The password authentication protocol is an insecure and outdated authentication protocol used for PPP connections.

CHAP: The challenge handshake authentication protocol is the successor to PAP and is more secure than its predecessor thanks to the use of hash functions and random numbers.

MSCHAP: MSCHAP is a CHAP variant from Microsoft (MS).

MSCHAP v2: MSCHAP v2 is a later version of MSCHAP legitimization.



Verbindungsname: BaT-Mobile(Telekom)

Legitimierung

Zulässige Methoden EAP, PAP, CHAP, MSCHAPv2, MSCHAP

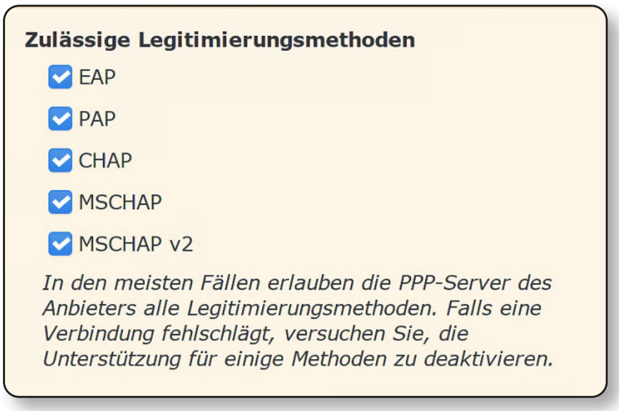
Komprimierung

- ☐ Punkt-zu-Punkt-Verschlüsselung (MPPE) verwenden
  - ☐ 128-Bit-Verschlüsselung anfordern
  - ☐ Stateful MPPE verwenden
- ☑ BSD-Datenkomprimierung erlauben
- ☑ Deflate-Datenkomprimierung erlauben
- ☑ TCP-Header-Komprimierung verwenden

Echo

- ☐ PPP-Echopakete senden

Fig. 7.14: *PPP settings*



Zulässige Legitimierungsmethoden

- ☑ EAP
- ☑ PAP
- ☑ CHAP
- ☑ MSCHAP
- ☑ MSCHAP v2

In den meisten Fällen erlauben die PPP-Server des Anbieters alle Legitimierungsmethoden. Falls eine Verbindung fehlschlägt, versuchen Sie, die Unterstützung für einige Methoden zu deaktivieren.

Fig. 7.15: *PPP legitimization*

USE POINT-TO-POINT ENCRYPTION (MPPE): This option activates Microsoft point-to-point encryption, an encryption protocol for data in PPP connections.

REQUIRE 128-BIT ENCRYPTION: A key with a length of 128 bits is required to use MPPE.

Use stateful MPPE: This checkbox enables the stateful mode for MPPE. Encryption mechanisms are only synchronized at the start of the session. If a packet is lost, the transmission is cancelled and a new synchronization is requested. This mode should only be used for connections where there is little or no packet loss.

Allow BSD data compression: The data to be transmitted will be compressed with PPP-BSD lossless compression.

Allow deflate data compression: The data to be transmitted will be compressed without loss using the deflate algorithm.

Allow TCP header compression: The TCP header of a data packet is compressed in order to increase the speed of slow connections.

Send PPP echo packets: Echo packets (echo request & echo reply) are used for line checking.

7.3.2 Battery

The battery icon shows the battery status of your device. Alternatively, use the context menu to set screen brightness, presentation mode and access power management.

For further information on power management, please refer to section *7.4.2.3 Power manager.*

7.3.3 Clipboard

This function is available since SBS version V7.x.42. Click on the clipboard icon to open the menu with the most recent entries.

Select the desired entry with a click and copy it with right-click + paste or a set key combination.

Clear history: Clears the clipboard of all entries.

Clipman settings: Opens the clipboard settings.

Use the context menu to call up the properties, deactivate the clipman or display information on the applet. Click Quit to terminate the function and hide the clipboard icon from the system tray.

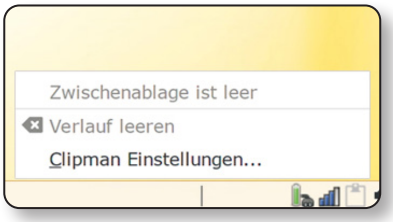


Fig. 7.16: *Clipman*

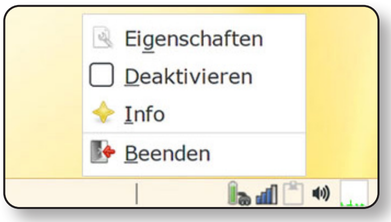


Fig. 7.17: *Clipman context menu*

7.3.3.1 Clipman settings

Behavior

Sync mouse selection: Enable this checkbox to synchronize the Clipman content with the default clipboard.

Paste instantly: Set the hotkey to automatically insert a selected entry from the history. You can choose Ctrl+V or Shift+Insert.

Position menu at mouse pointer: Enable this checkbox to open the menu at the position of the mouse pointer.

Maximum elements: Set the maximum number of items to be displayed in the menu. Enter a number directly or increase/decrease the quantity with + and −.

History

Remember history: Enable this option to store the history make it available for a new session.

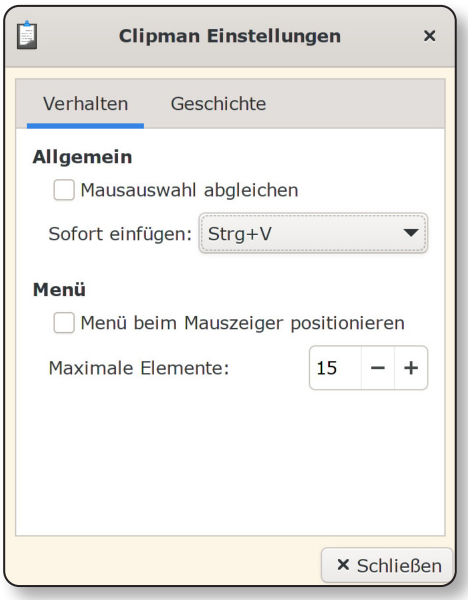
Remember last copied image: If you activate this checkbox, the last copied image is saved temporarily in the history.

Reorder history items: Enable this checkbox to display the most recently cached item at the top of the history.

Reverse history order: Enable this checkbox to display the history in reverse order.

Ignore mouse selections: If you enable this checkbox, the selection from the default clipboard will not be added to the history.

Size of the history: Set the number of entries in the history. Enter a number directly or increase/decrease the quantity with + and −.



Allgemein

☐ Mausauswahl abgleichen

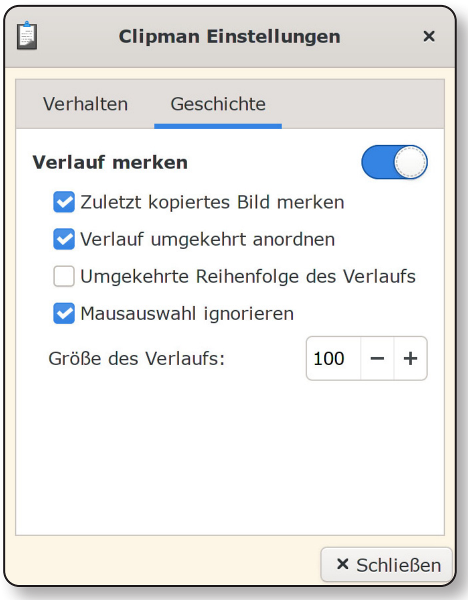
Sofort einfügen: Strg+V

Menü

☐ Menü beim Mauszeiger positionieren

Maximale Elemente: 15 − +

Fig. 7.18: *Clipman behavior*



Verlauf merken ●

☑ Zuletzt kopiertes Bild merken

☑ Verlauf umgekehrt anordnen

☐ Umgekehrte Reihenfolge des Verlaufs

☑ Mausauswahl ignorieren

Größe des Verlaufs: 100 − +

Fig. 7.19: *Clipman history*

7.3.4 Volume

Adjust the volume of your connected audio devices and microphones by clicking the speaker icon in the system tray.

7.3.4.1 Volume control/audio mixer

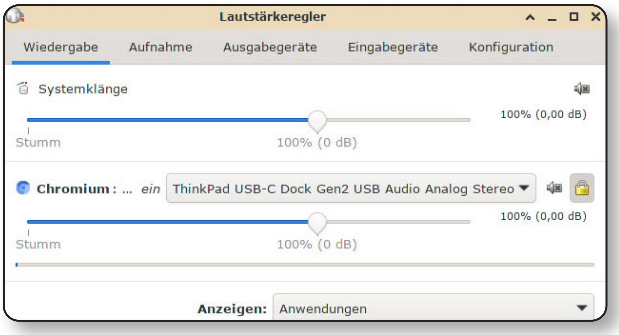
Playback

Lists the streams or applications that are currently playing audio content.

System sounds: Allows you to adjust the volume of the system sounds in percent (decibels).

Mute audio: Allows you to mute a stream/application.

Show: Select the streams you want to play.



Systemklänge 100% (0,00 dB)

Chromium : ... ein ThinkPad USB-C Dock Gen2 USB Audio Analog Stereo 100% (0,00 dB)

Anzeigen: Anwendungen

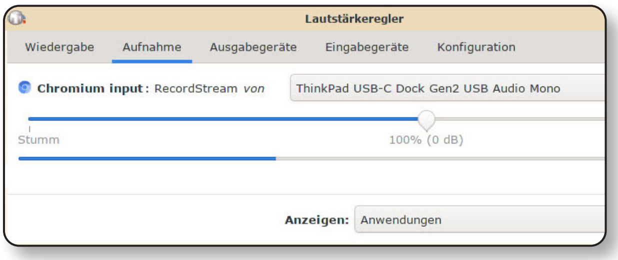
Fig. 7.20: *Audio mixer playback*

Recording

Lists the streams or applications that are currently recording audio content. Adjust the volume.

Mute: Allows you to mute a stream/application.

Lock channels together: Allows you to set whether the channels of the stream/application should be locked together or adjusted separately. To adjust them separately, use the channels Front left and Front right.



Chromium input : RecordStream von ThinkPad USB-C Dock Gen2 USB Audio Mono

Anzeigen: Anwendungen

Fig. 7.21: *Audio mixer recording*

Show: Allows you to select what you want to configure the recording for.

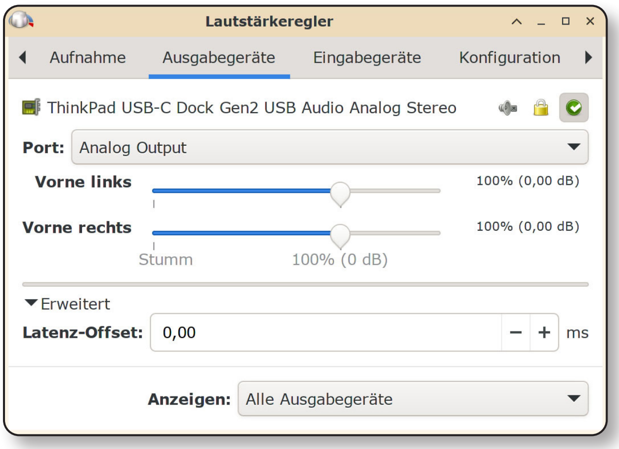
Output devices

Lists the built-in and connected audio output devices.

Port: Select the port for the respective device.

Mute: Allows you to mute output devices.

Lock channels together: Allows you to set whether the channels of the stream/application should be locked together or adjusted separately. To adjust them separately, use the channels Front left and Front right.



ThinkPad USB-C Dock Gen2 USB Audio Analog Stereo

Port: Analog Output

Vorne links 100% (0,00 dB)

Vorne rechts 100% (0,00 dB)

Latenz-Offset: 0,00 ms

Anzeigen: Alle Ausgabegeräte

Fig. 7.22: *Audio mixer output devices*

Set as fallback: Allows you to set an output device as fallback. This option is only useful if more than one output device is available.

Latency offset (Advanced): Set the latency manually in milliseconds (ms).

Show: Select the output device you want to configure.

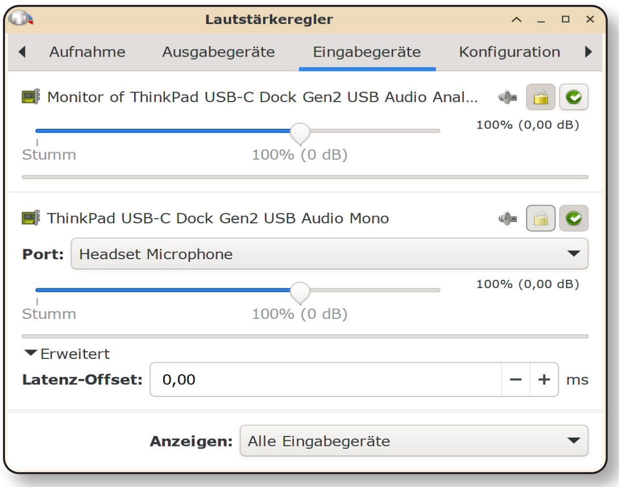
Input devices

Lists the built-in and connected audio input devices.

PORT: Select the port for the respective device.

MUTE: Allows you to mute input devices.

LOCK CHANNELS TOGETHER: Allows you to set whether the channels of the stream/application should be locked together or adjusted separately. To adjust them separately, set the channels FRONT LEFT and FRONT RIGHT.


Lautstärkeregler

Aufnahme | Ausgabegeräte | Eingabegeräte | Konfiguration

Monitor of ThinkPad USB-C Dock Gen2 USB Audio Anal...
Stumm 100% (0 dB) 100% (0,00 dB)

ThinkPad USB-C Dock Gen2 USB Audio Mono
Port: Headset Microphone
Stumm 100% (0 dB) 100% (0,00 dB)
Erweitert
Latenz-Offset: 0,00 ms

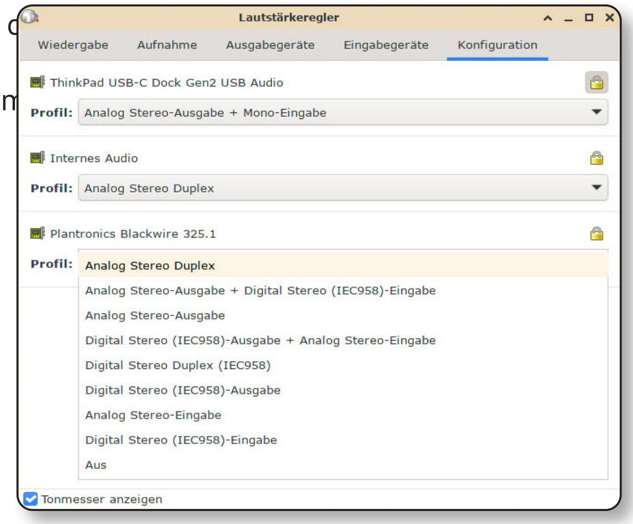
Anzeigen: Alle Eingabegeräte

Fig. 7.23: *Audio mixer input devices*

SET AS FALLBACK: Allows you to set an input device as fallback. This option is only useful if more than one c

LATENCY OFFSET (ADVANCED): Set the latency manually in m

SHOW: Select the input device you want to configure.


Lautstärkeregler

Wiedergabe | Aufnahme | Ausgabegeräte | Eingabegeräte | Konfiguration

ThinkPad USB-C Dock Gen2 USB Audio
Profil: Analog Stereo-Ausgabe + Mono-Eingabe

Internes Audio
Profil: Analog Stereo Duplex

Plantronics Blackwire 325.1
Profil: Analog Stereo Duplex
Analog Stereo-Ausgabe + Digital Stereo (IEC958)-Eingabe
Analog Stereo-Ausgabe
Digital Stereo (IEC958)-Ausgabe + Analog Stereo-Eingabe
Digital Stereo Duplex (IEC958)
Digital Stereo (IEC958)-Ausgabe
Analog Stereo-Eingabe
Digital Stereo (IEC958)-Eingabe
Aus

☑ Tonmesser anzeigen

Fig. 7.24: *Audio mixer configuration*

Configuration

Lists the built-in and connected audio devices.

PROFILE: Select a profile for the audio device. The options vary depending on the device. The option OFF disables the device and it is no longer listed in the other tabs.

SHOW VOLUME METERS: Enable/disable volume meter. Disabling this option hides the volume control below the respective devices on the Playback and Recording tabs and reduces CPU load.

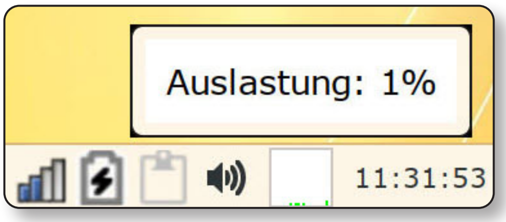


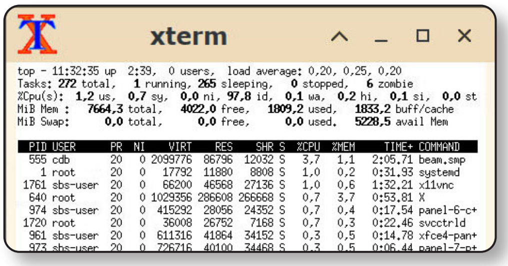
Fig. 7.25: *CPU usage*

7.3.5 CPU usage

CPU usage is a graphical representation of the current CPU load. The percentage is displayed on mouseover.

Click the system tray icon to open a detailed list of the current usage.

Contact your IT administration or user support if CPU usage is persistently in the red zone.


xterm

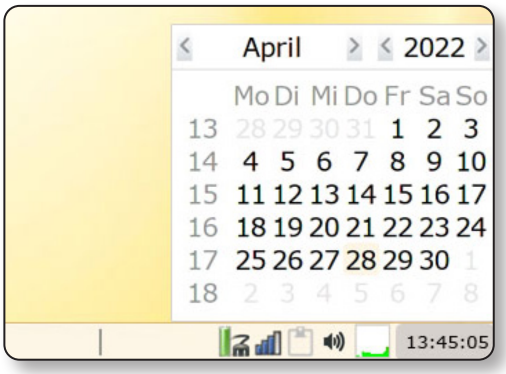
```
top - 11:32:35 up  2:39,  0 users,  load average: 0,20, 0,25, 0,20
Tasks: 272 total,   1 running, 265 sleeping,   0 stopped,   6 zombie
%Cpu(s):  1,2 us,  0,7 sy,  0,0 ni, 97,8 id,  0,1 wa,  0,2 hi,  0,1 si,  0,0 st
MiB Mem :   7664,3 total,   4022,0 free,   1809,2 used,   1833,2 buff/cache
MiB Swap:      0,0 total,      0,0 free,      0,0 used.   5228,5 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
  555 cdb       20   0 2099776  86796  12032 S   3,7   1,1   2:05.71 beam.smp
    1 root      20   0   17792  11880   8808 S   1,0   0,2   0:31.93 systemd
 1761 sbs-user  20   0   66200  46568  27136 S   1,0   0,6   1:32.21 x11vnc
  640 root      20   0 1029356 286608 266668 S   0,7   3,7   0:53.81 X
  974 sbs-user  20   0  415292  28056  24352 S   0,7   0,4   0:17.54 panel-6-c+
 1720 root      20   0   36008  26752   7168 S   0,7   0,3   0:22.46 svcctrld
  961 sbs-user  20   0  611316  41864  34152 S   0,3   0,5   0:14.78 xfce4-pan+
  973 sbs-user  20   0  726716  40100  34468 S   0,3   0,5   0:06.44 panel-7-p+
```

Fig. 7.26: *CPU usage details*

7.3.6 Date and time

The system time display is located at the right side of the taskbar. The current date and day of the week are displayed on mouseover. Click the indicator to open the calendar.



	April			2022			
	Mo	Di	Mi	Do	Fr	Sa	So
13	28	29	30	31	1	2	3
14	4	5	6	7	8	9	10
15	11	12	13	14	15	16	17
16	18	19	20	21	22	23	24
17	25	26	27	28	29	30	1
18	2	3	4	5	6	7	8

Fig. 7.27: *Time and calendar indicator*

7.4 SBS Start menu

You can open the SBS start menu using the start button in the taskbar or by right-clicking on the desktop background.

> Please note that some options in the SBS start menu can be hidden by your IT administration and are therefore not displayed.

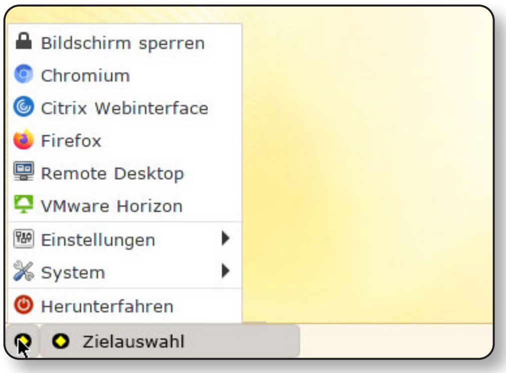


Fig. 7.28: *SBS start menu*

7.4.1 Lock screen

The Secure Boot Stick has a built-in screen lock that automatically locks the screen after a set period of inactivity, depending on your IT administration's configuration. It protects the SBS and your working environment from unauthorized access.

You can lock the screen immediately with Lock screen.

Unlock the Secure Boot Stick CL and HE the screen with your start password, if one has been assigned. If no start password has been assigned, unlock the screen by pressing a random key or moving the mouse. Unlock the Secure Boot Stick FX/SX and the GX/ZX by entering your smartcard PIN on the PIN pad.

.

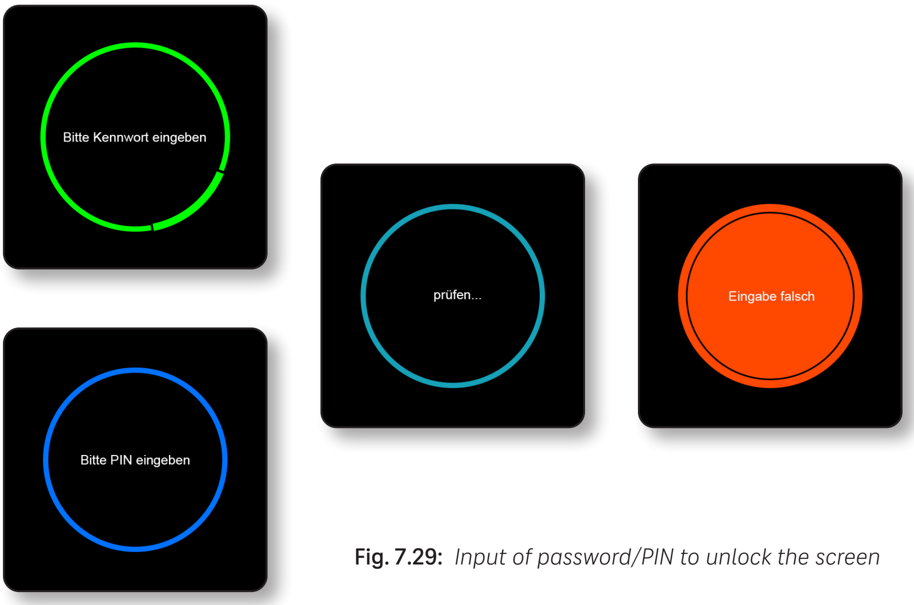


Fig. 7.29: *Input of password/PIN to unlock the screen*

Make sure to activate the password prompt with the mouse instead of the keyboard. Pressing a key, e.g. the space bar, is counted as an entry for the start password.

7.4.2 Preferences

This extended menu panel allows you to customize the SBS to your preferences and the needs of your workspace.

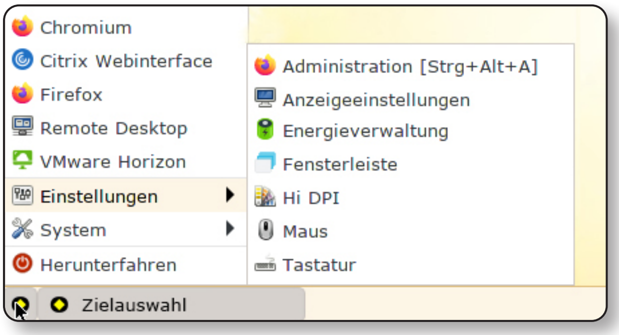


Fig. 7.30: *SBS Start menu with preferences panel*

7.4.2.1 Administration

This function for administration and error analysis of the SBS. This function is password-protected and reserved for your IT administration.

7.4.2.2 Display properties

Allows you to adjust the display and screen settings to your needs and requirements.

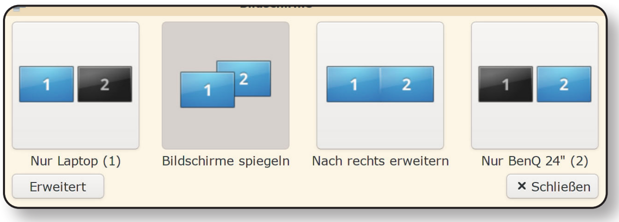
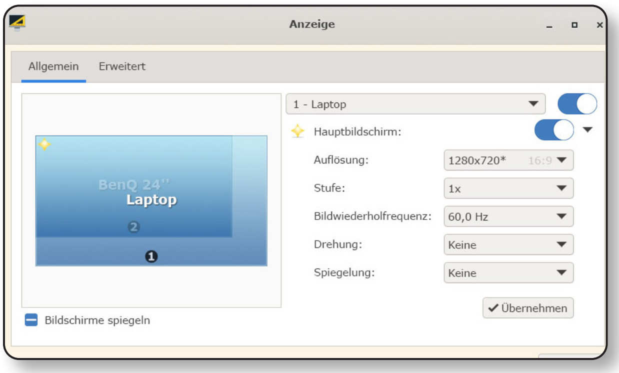


Fig. 7.31: *Multi-monitor settings*

General

Select the display for which you want to edit the settings. Only connected displays are shown.



1 - Laptop

Hauptbildschirm:

Auflösung: 1280x720* 16:9

Stufe: 1x

Bildwiederholfrequenz: 60,0 Hz

Drehung: Keine

Spiegelung: Keine

Bildschirme spiegeln

Fig. 7.32: *General display properties*

Select which display to set as the primary display when multiple displays are connected. A small asterisk marks the primary screen. Taskbar and destination profile selection are always displayed on the primary screen.

Press Apply to save your settings.

Resolution: Select the desktop display resolution. The resolution is displayed in pixels and as a ratio.

Scale: Set the scaling level. The higher the factor, the smaller the display.

Refresh rate: Allows you to set the frequency of the refresh rate. It indicates how many frames per second are processed and how smoothly the content is displayed. The display must support the selected refresh rate.

Rotation: Allows you to set the rotation of the screen display. You can rotate the display 90° to the left, to the right or 180° (vice versa).

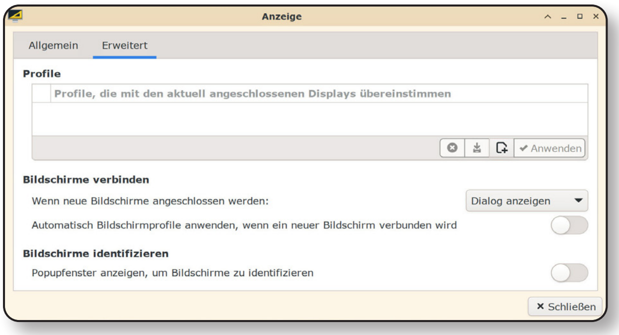
Reflection: Allows you to mirror the display. You can mirror horizontally, vertically or horizontally and vertically.

Advanced

Profiles: Allows you to create display profiles which, depending on the setting, are automatically applied when you connect a new display . Only the profiles that match the currently selected display are shown. To create a new profile, make the desired settings at General . Then add the profile with ⊞. You can edit or delete existing profiles.

Connecting displays

When new displays are connected: Select in the drop-down menu how to proceed when a display is connected.


Anzeige

Allgemein Erweitert

Profile

Profile, die mit den aktuell angeschlossenen Displays übereinstimmen

✔ Anwenden

Bildschirme verbinden

Wenn neue Bildschirme angeschlossen werden: Dialog anzeigen

Automatisch Bildschirmprofile anwenden, wenn ein neuer Bildschirm verbunden wird

Bildschirme identifizieren

Popupfenster anzeigen, um Bildschirme zu identifizieren

✕ Schließen

Fig. 7.33: *Advanced settings*

Do nothing: Nothing happens, the display is shown in the General tab so that settings can be made.

Show dialog: The multi-monitor dialog open so you can set how the connected monitor should display the image.

Mirror: The display is automatically mirrored on the connected monitor.

Extend: The display is automatically extended to the connected monitor.

Automatically enable profile when new display is connected: When enabled, a given screen profile is automatically applied to new displays.

Identifying displays

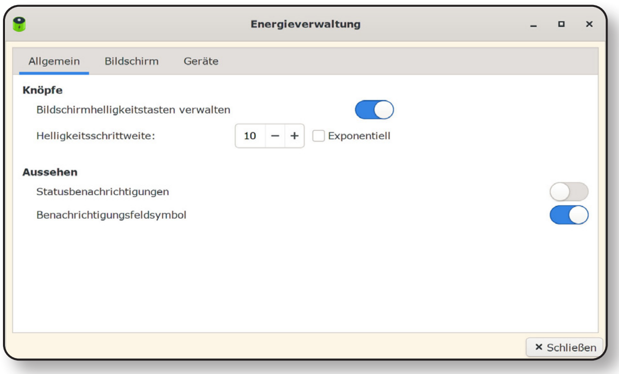
Show pop-up window to identify displays: When enabled, a small pop-up window opens and shows information about the new display, e.g. name or resolution.

7.4.2.3 Power manager

Allows you to adjust power options. Please note that changes to the energy settings may affect the battery life of your computer.

General

Buttons: Allow you to control the display brightness.


Energieverwaltung

Allgemein Bildschirm Geräte

Knöpfe

Bildschirmhelligkeitstasten verwalten

Helligkeitsschrittweite: 10 − + □ Exponentiell

Aussehen

Statusbenachrichtigungen

Benachrichtigungsfeldsymbol

✕ Schließen

Fig. 7.34: *General power management settings*

Brightness step count : Set the threshold value for the brightness adjustment, e.g. in steps of 10.

Appearance

Status notifications: Enables status notifications, e.g. for the battery status of your device.

System tray icon: Enables the battery indicator in the system tray of the taskbar.

Display

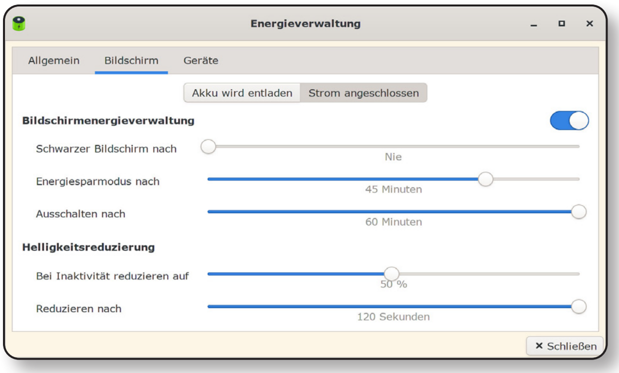
Allows you to manage energy options controlling battery and mains supply.

Display power management

Blank after: Set the period of inactivity in minutes, after which the displays go blank.

Put to sleep after: Set the period of inactivity in minutes, after which the energy-saving mode is activated.

Switch off after: Set the period of inactivity in minutes, after which the displays are switched off.



Energieverwaltung

Allgemein | Bildschirm | Geräte

Akku wird entladen | Strom angeschlossen

Bildschirmenergieverwaltung

Schwarzer Bildschirm nach: Nie

Energiesparmodus nach: 45 Minuten

Ausschalten nach: 60 Minuten

Helligkeitsreduzierung

Bei Inaktivität reduzieren auf: 50 %

Reduzieren nach: 120 Sekunden

Fig. 7.35: *Power manager display settings*

If some options in the power management are grayed out, reboot your SBS with an alternative kernel. For further information, please refer to section *6.5.1.5 Kernel*

Brightness reduction

On inactivity, reduce to: Set the brightness reduction in percent.

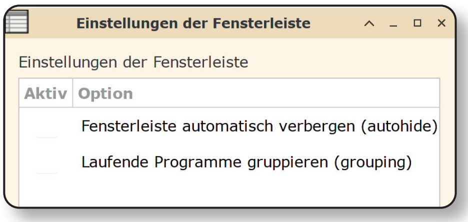
Reduce after: Set the period of inactivity in seconds, after which the display brightness is reduced.

Devices

Shows a list of all connected and installed power sources and their status.

7.4.2.4 Taskbar

Allows you to adjust the behavior of the taskbar. Choose whether to hide the taskbar and whether to group active applications on the taskbar.



Einstellungen der Fensterleiste

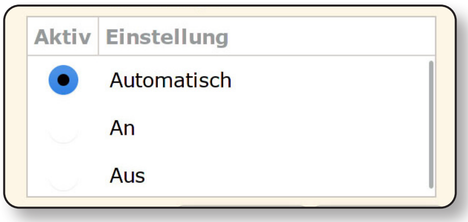
Einstellungen der Fensterleiste

Aktiv	Option
	Fensterleiste automatisch verbergen (autohide)
	Laufende Programme gruppieren (grouping)

Fig. 7.36: *Taskbar settings*

Hi DPI

Allows you to set the Hi DPI mode for high-resolution screens. These screens have a pixel density of at least 100 dpi and usually a width of at least 1920 pixels.



Aktiv	Einstellung
●	Automatisch
○	An
○	Aus

Fig. 7.37: *Hi DPI settings*

7.4.2.5 Mouse

Allows you to adjust mouse and touchpad settings.

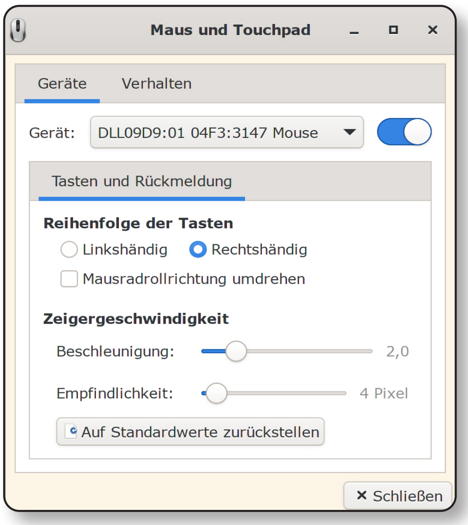
Devices

Device: Select the mouse or touchpad you wish to configure.

Buttons and feedback

Buttons: Set the mouse button assignment.. For left-handers, the option Left-handed is recommended. Right-handed is enabled by default.

Reverse scroll direction: Enable the checkbox to reverse the scrolling direction of the mouse wheel. This option is disabled by default.



Maus und Touchpad

Geräte | Verhalten

Gerät: DLL09D9:01 04F3:3147 Mouse

Tasten und Rückmeldung

Reihenfolge der Tasten

○ Linkshändig ● Rechtshändig

□ Mausradrollrichtung umdrehen

Zeigergeschwindigkeit

Beschleunigung: 2,0

Empfindlichkeit: 4 Pixel

Auf Standardwerte zurückstellen

✕ Schließen

Fig. 7.38: *Mouse button assignment*

Acceleration: Set the acceleration of the pointer. An acceleration of 2.0 is set by default.

Sensitivity: Set the sensitivity of the pointer. Default sensitivity is set to 4 pixels.

Reset to default s : Allows you to reset the values to the defaults.

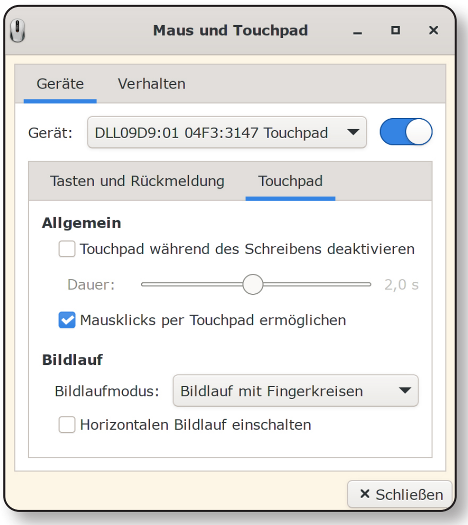
Touchpad

Disable touchpad while typing: Enable this checkbox to disable the touchpad during typing. It prevents accidental clicks when moving the cursor unintentionally.

Duration: Set the duration of the deactivation in seconds.

Tap touchpad to click: When this option is enabled, you can also use the touchpad for mouse clicks.

Scrolling: Set the scroll mode. Please note that the built-in touchpad must support the selected mode.



Maus und Touchpad

Geräte | Verhalten

Gerät: DLL09D9:01 04F3:3147 Touchpad

Tasten und Rückmeldung | Touchpad

Allgemein

□ Touchpad während des Schreibens deaktivieren

Dauer: 2,0 s

☑ Mausklicks per Touchpad ermöglichen

Bildlauf

Bildlaufmodus: Bildlauf mit Fingerkreisen

□ Horizontalen Bildlauf einschalten

✕ Schließen

Fig. 7.39: *Touchpad settings*

Disabled: Scroll mode is off.

Edge scrolling: Drag your finger along the edge of the touchpad to scroll.

Two-finger scrolling: Drag two fingers across the touchpad to scroll.

Circular scrolling: Drag one finger in circle ways across the touchpad. Start at the edge of the touchpad.

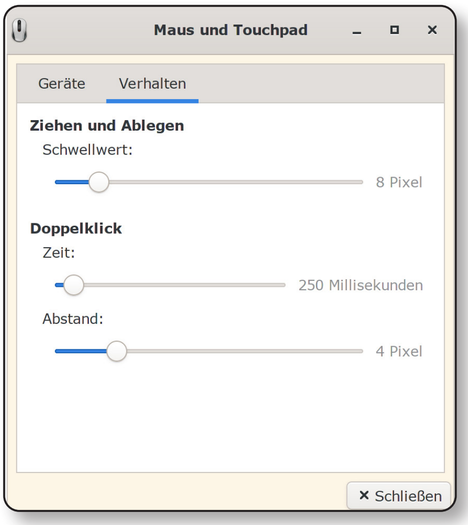
Enable horizontal scrolling: Enable this checkbox to turn horizontal scrolling on.

Behavior

Drag and drop: Set the threshold value for moving an object.

Time: Set the time interval in milliseconds for a double-click.

Distance: Set the distance in pixels for a double-click.



Maus und Touchpad

Geräte | Verhalten

Ziehen und Ablegen
Schwellwert: 8 Pixel

Doppelklick
Zeit: 250 Millisekunden
Abstand: 4 Pixel

✕ Schließen

Fig. 7.40: *Mouse and touchpad behavior*

7.4.2.6 Keyboard

Allows you to manage keyboard settings.

Behavior

Restore num lock state on startup: Enable the Num key automatically when you start the SBS.

Typing settings

Enable key repeat: Enable this checkbox to turn on key repeat when you press a key on your keyboard for a longer period of time.

Repeat delay: Set the repeat delay in milliseconds.

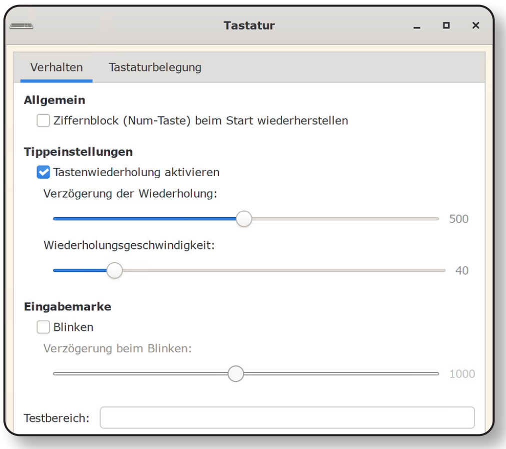
Repeat speed: Set the speed of the key repeat.

Cursor

Show blinking: When this checkbox is enabled, the cursor flashes when typing.

Blink delay: Set the delay for cursor blinking.

Test area: Use this field to test and check your keyboard settings.



Tastatur

Verhalten | Tastaturbelegung

Allgemein
□ Ziffernblock (Num-Taste) beim Start wiederherstellen

Tippeinstellungen
☑ Tastenwiederholung aktivieren
Verzögerung der Wiederholung: 500
Wiederholungsgeschwindigkeit: 40

Eingabemarke
□ Blinken
Verzögerung beim Blinken: 1000

Testbereich:

Fig. 7.41: *Typing settings*

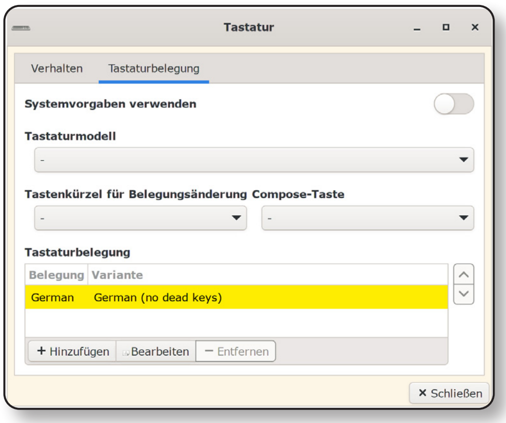
Layout

Use system defaults: Enable the system settings for your device. When enabled, the following options are not available.

Keyboard model: Select the keyboard model.

Change layout option and compose key: Select a hotkey to switch between different keyboard layouts.

Keyboard layout: Add, edit or delete keyboard layouts.



Tastatur

Verhalten | Tastaturbelegung

Systemvorgaben verwenden ○

Tastaturmodell
-

Tastenkürzel für Belegungsänderung Compose-Taste
- | -

Tastaturbelegung

Belegung	Variante
German	German (no dead keys)

+ Hinzufügen | Bearbeiten | − Entfernen

✕ Schließen

Fig. 7.42: *Tastaturbelegung*

7.4.3 System

The system panel allows you to configure system settings.

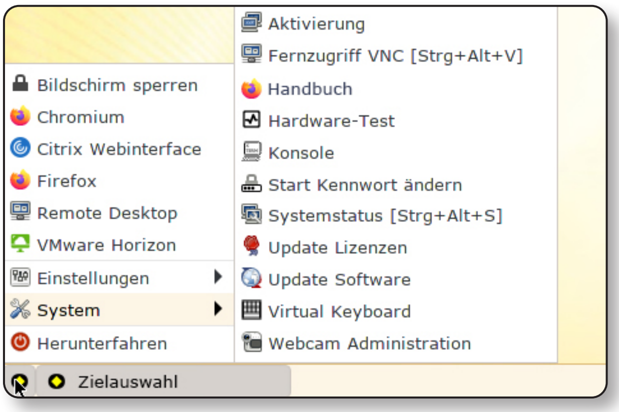


Fig. 7.43: *SBS Start menu and system panel*

7.4.3.1 Activation

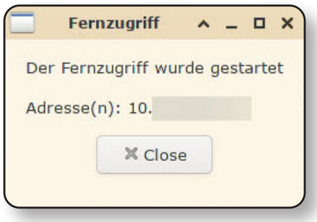
The SBS starts the activation automatically the first time it is used. Reactivation is usually only necessary if there are problems with the SBS that cannot be resolved.

Perform this action only if your IT administrator instructs you to do so and if you have new activation data..

For further information on how to activate the SBS, please refer to section *6.5.2 Automatic hardware test*.

7.4.3.2 Remote access VNC

Allows your IT administration or user support to access your SBS remotely and assist you with problems and errors. Access by VNC is only possible within the same network or with a VPN connection.



Der Fernzugriff wurde gestartet

Adresse(n): 10.[redacted]

Fig. 7.44: *Remote access*

To prevent system damage and unauthorized access to sensitive data, only allow remote access to your IT administration or user support.

7.4.3.3 Manual

Opens the SBS user manual as a PDF.

7.4.3.4 Hardware test

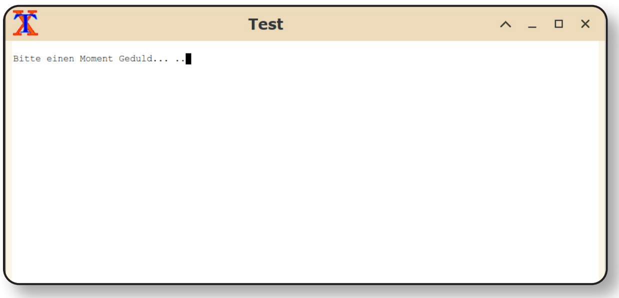
Hardware tests are used to analyze hardware problems and are a valuable tool for keeping the SBS software up to date and compatible with the latest computer models.

You can start a hardware test in the boot menu or in the start menu of the SBS desktop if, for example, a connected device is not working.

In addition to information about your device, e.g., vendor, model, serial number, installed hardware components and associated drivers, the hardware test also records information about your SBS, such as the currently installed version and model. The hardware test does not record personal data or files.

You will need an additional USB flash drive to store the TXT file that is generated during the hardware test. This additional USB flash drive must have been formatted with the FAT32 file system. To format the USB flash drive, please refer to *9.3 How to format a USB flash drive*.

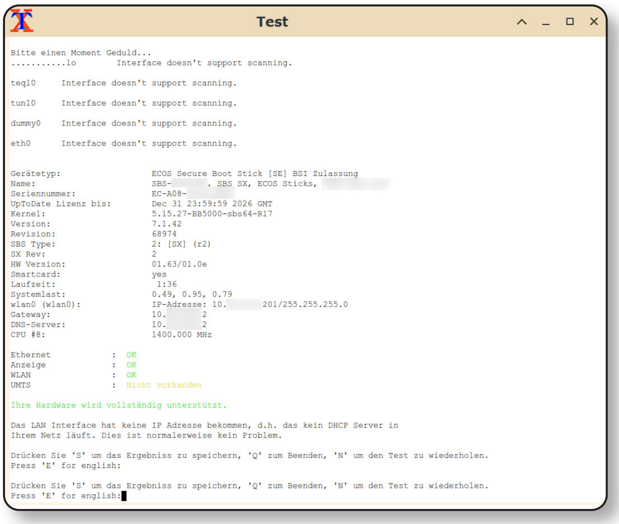
1. Switch off your computer.
2. Connect your SBS to a USB port on your computer.
3. Connect all devices (keyboard, mouse, monitors, docking stations, etc.) that you want to test.
4. Switch on your computer and boot the SBS.



```
Bitte einen Moment Geduld... ..
```

Fig. 7.45: *Hardware test*

5. Open the SBS start menu and select the menu item **System → Hardware test**.
6. The SBS starts the hardware test. The test takes about three minutes. Information about the installed and connected hardware is gathered. A summary of the results is displayed when the hardware test is complete. You can now save the results (S), end the test (Q), repeat the test (N) or get the results in German (D).
7. You can send the results file to ECOS Support by e-mail (M) or save them on the additional USB stick (U).
   Please note: Due to the security settings, you cannot save the results file on the SBS.



```
Bitte einen Moment Geduld...
...........lo        Interface doesn't support scanning.

teql0     Interface doesn't support scanning.

tunl0     Interface doesn't support scanning.

dummy0    Interface doesn't support scanning.

eth0      Interface doesn't support scanning.


Gerätetyp:                   ECOS Secure Boot Stick [SE] BSI Zulassung
Name:                        SBS-[redacted]. SBS SX, ECOS Sticks, [redacted]
Seriennummer:                EC-A08-[redacted]
UpToDate Lizenz bis:         Dec 31 23:59:59 2026 GMT
Kernel:                      5.15.27-BB5000-sbs64-R17
Version:                     7.1.42
Revision:                    68974
SBS Type:                    2: [SX] (r2)
SX Rev:                      2
HW Version:                  01.63/01.0e
Smartcard:                   yes
Laufzeit:                     1:36
Systemlast:                  0.49, 0.95, 0.79
wlan0 (wlan0):               IP-Adresse: 10.[redacted]201/255.255.255.0
Gateway:                     10.[redacted]2
DNS-Server:                  10.[redacted]2
CPU #8:                      1400.000 MHz

Ethernet            :  OK
Anzeige             :  OK
WLAN                :  OK
UMTS                :  Nicht vorhanden

Ihre Hardware wird vollständig unterstützt.

Das LAN Interface hat keine IP Adresse bekommen, d.h. das kein DHCP Server in
Ihrem Netz läuft. Dies ist normalerweise kein Problem.

Drücken Sie 'S' um das Ergebniss zu speichern, 'Q' zum Beenden, 'N' um den Test zu wiederholen.
Press 'E' for english:

Drücken Sie 'S' um das Ergebniss zu speichern, 'Q' zum Beenden, 'N' um den Test zu wiederholen.
Press 'E' for english:
```

Fig. 7.46: *Results file*

To e-mail the results of the hardware test directly to ECOS Support, make sure you have an active Internet connection. Follow the instructions on the screen and confirm the entries with ENTER.

To save the results file as a TXT file on a USB stick, follow the instructions on the screen and confirm your entries with ENTER.

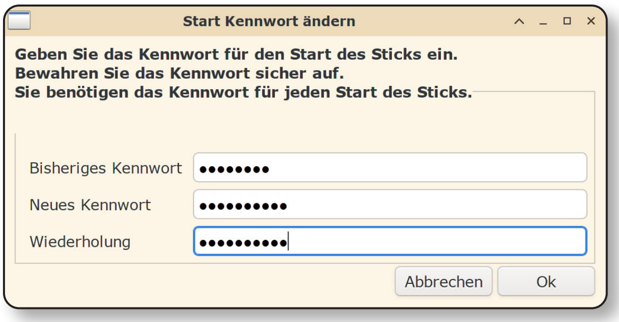
7.4.3.5 Shell

The shell allows in-depth settings to the operating system of the Secure Boot Stick. It is is therefore password-protected and reserved for your IT administration.

7.4.3.6 Change start password

Allows you change your start password. If you do not have a start password yet, leave the field for the previous password empty.

As of version V7.60.0, you can no longer assign a start password if you have an SBS variant with a PIN pad. These variants are protected with a PIN instead of a password.



Geben Sie das Kennwort für den Start des Sticks ein.
Bewahren Sie das Kennwort sicher auf.
Sie benötigen das Kennwort für jeden Start des Sticks.

Bisheriges Kennwort: ••••••••

Neues Kennwort: ••••••••••

Wiederholung: ••••••••••

Fig. 7.47: *Change start password*

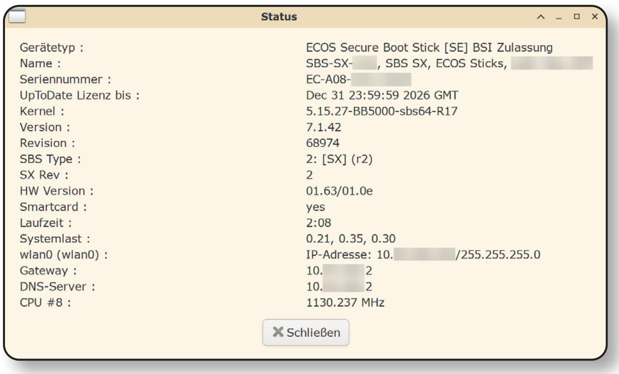
For further information on how to change the smartcard PIN, please refer to section *6.6.2.1 Change smartcard PIN.*

Your IT administration can define central guidelines for the complexity and length of your password. Please observe this password policy when changing your start password.

7.4.3.7 System status

The system status provides information about the Secure Boot Stick and the system, e.g. the SBS model, the SBS version, the serial number or the network connection.

This information is intended for troubleshooting to rule out hardware incompatibilities.



Gerätetyp :	ECOS Secure Boot Stick [SE] BSI Zulassung
Name :	SBS-SX-[redacted], SBS SX, ECOS Sticks, [redacted]
Seriennummer :	EC-A08-[redacted]
UpToDate Lizenz bis :	Dec 31 23:59:59 2026 GMT
Kernel :	5.15.27-BB5000-sbs64-R17
Version :	7.1.42
Revision :	68974
SBS Type :	2: [SX] (r2)
SX Rev :	2
HW Version :	01.63/01.0e
Smartcard :	yes
Laufzeit :	2:08
Systemlast :	0.21, 0.35, 0.30
wlan0 (wlan0) :	IP-Adresse: 10.[redacted]/255.255.255.0
Gateway :	10.[redacted]2
DNS-Server :	10.[redacted]2
CPU #8 :	1130.237 MHz

Fig. 7.48: *System status*

7.4.3.8 Update licenses

Licenses are an essential security factor and must be valid for the Secure Boot Stick to work properly. Besides, software updates are managed via licenses.

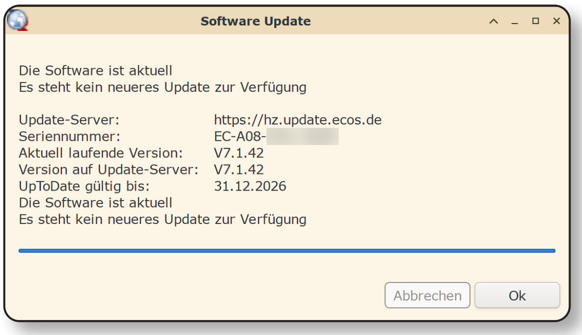
Licenses are usually made available by your IT administration on the System Management Appliance and your SBS is updated automatically. However, if the automatic license update fails, this function allows to update manually.

Make sure the SBS is connected to the Internet. The SBS connects to the update server, which checks for new licenses. If so, the SBS licenses are updated.

7.4.3.9 Update software

The Secure Boot Stick software from is continuously being developed to ensure security, implement new functions and support the latest computer models.

Software updates are usually delivered by your IT administration via the System Management Appliance and your SBS is updated automatically. However, if the automatic software update fails, this function allows to update manually.



Software Update

Die Software ist aktuell
Es steht kein neueres Update zur Verfügung

```
Update-Server:              https://hz.update.ecos.de
Seriennummer:               EC-A08-[redacted]
Aktuell laufende Version:   V7.1.42
Version auf Update-Server:  V7.1.42
UpToDate gültig bis:        31.12.2026
```

Die Software ist aktuell
Es steht kein neueres Update zur Verfügung

Fig. 7.49: *Software-Update-Dialog*

Make sure the SBS is connected to the Internet. The SBS connects to the update server, which checks for a new software version. If so, the SBS software is updated.

You can continue to work while the update is performed, but we recommend restarting SBS after the update is installed.

7.4.3.10 Virtual Keyboard

You can use the Virtual Keyboard to display an on-screen keyboard that you can use with your mouse.

Hide the keyboard using the keyboard icon in the system tray and close it using the context menu.

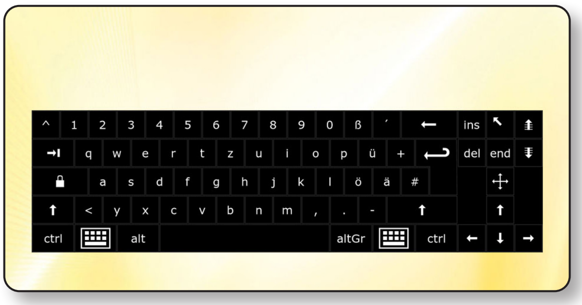

^ 1 2 3 4 5 6 7 8 9 0 ß ´ ← ins ↖ ⇞
⇥ q w e r t z u i o p ü + ↵ del end ⇟
a s d f g h j k l ö ä #
↑ < y x c v b n m , . - ↑ ↑
ctrl alt altGr ctrl ← ↓ →

Fig. 7.50: *Virtual keyboard*

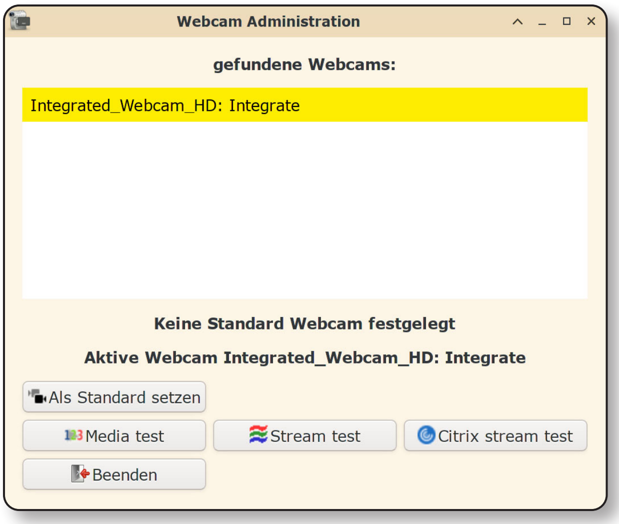
7.4.3.11 Webcam administration

The webcam administration allows you to manage built-in and connected cameras.

All detected webcams are listed. You can test these webcams for use in certain environments and set one as default camera.

Set as default: The selected camera is set as default input device.

Media test: Allows you to test the functionality of the selected camera. This function shows you a webcam preview and information about the functions. Return to the settings page via Webcam selection.



Webcam Administration

gefundene Webcams:

Integrated_Webcam_HD: Integrate

Keine Standard Webcam festgelegt

Aktive Webcam Integrated_Webcam_HD: Integrate

Fig. 7.51: *Webcam administration*

Stream test: Allows you to test the functionality of the selected camera in a VMware environment. This function shows you a webcam preview and information about the functions. Return to the settings page via Webcam selection.

Citrix stream test: Allows you to test the functionality of the selected camera in a Citrix environment. This function shows you a webcam preview and information about the functions. Return to the settings page via Webcam selection.

Quit: Exits the application.

7.4.4 Shutdown ⏻

This function shuts down Secure Boot Stick and computer.

Part 3: Troubleshooting and tutorials

8 Hints and troubleshooting

8.1 Troubleshooting

There are several reasons why you may have trouble connecting to an access destination.

Error description	Possible cause	Troubleshooting
It is not possible to connect to the selected destination server.	◆ The destination server is not connected to the Internet. ◆ The destination server is overloaded. ◆ The destination server has another, network-related error.	Contact your IT administration or user support.
VPN connection cannot be started.	◆ The MTU is too big.	Change the MTU for your Internet connection in the network manager. *7.3.1 Network manager*
VPN connection cannot be started.	◆ Your Internet connection uses the IPv6 network protocol. The IPv6 addresses used are not compatible with the protocol currently used by the SBS. The SBS cannot connect to the destination server. ◆ You are using a DSLite Internet connection that packages and transports IPv4 packets into IPv6 packets. This means that the transmission protocol of the SBS cannot establish a connection. ◆ The Internet connection you are using is too slow or unstable to maintain a continuous connection to the destination server. ◆ The SBS's certificates are no longer valid, making it impossible to open a VPN connection.	Contact your IT administration or user support.
VPN connection cannot be started.	◆ The firmware of the router you are using is not compatible with the requirements of the SBS.	Update your router's firmware if possible. Information on how to update your router can usually be found on the vendor's website.

If the steps listed above do not solve your problem, please contact your IT administration, user support or the ECOS Helpdesk.

8.2 Boot menu/BIOS hotkeys

To access your computer's BIOS or boot menu, you must press a special hotkey while your computer is booting. These hotkeys vary by vendor and model.

Should the vendor of your device not be listed below, or should the listed hotkey not open the boot menu or BIOS, please search the internet for the vendor, the model number and the term **BIOS** or **boot menu**.

Vendor	Opens BIOS	Opens boot menu
Acer	F2 or Del	F12
ASRock	F2 or Del	F11
Asus	F2 or Del	Esc
Dell	F2	F12
Fujitsu	F2	F12
Gigabyte	Del	
HP	F2 or F10	F9 or Esc
Intel	F2	F10
Lenovo	F1	F12
Medion	F2	F10
Microsoft	Louder + Power	
MSI	Del	F11
Samsung	F2	Esc
Sony	F2	
Terra	F2	F7
Toshiba	Press Esc at start, then F1	F12
Zotac	Del	F12

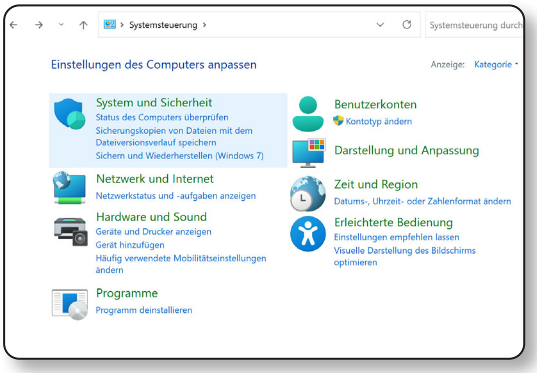
9 Tutorials

9.1 Disable Windows Fast Startup

The fast startup function introduced by Microsoft with Windows 10 speeds up the system start of your computer by skipping a couple of system checks and hiding graphical notifications during the boot process. The fast startup also skips USB port checks. It boots so quickly that no other or new boot media, such as the Secure Boot Stick, can be detected.

Disabling fast startup solves the problem.

1. Start your computer without connecting the SBS.
2. Open the Windows start menu ⊞.
3. Open the Control Panel.
4. Select the category System and Security.
5. Go to Power Options.
6. Select Change what the power buttons do.
7. Click on Change settings that are currently unavailable and confirm in the next window. Enter your administrator password when prompted to do so.
   The Shutdown settings are displayed.
8. Disable the checkbox Turn on fast startup (recommended).
9. Save your settings.
10. Switch off your computer.
11. Connect the SBS to your computer's USB port.
12. Start your computer. If the SBS starts automatically, no further action is required on your part. Otherwise, proceed as described in the sections *2.2.1 One-time USB boot* and *2.2.2 Permanent USB boot*.



Einstellungen des Computers anpassen

Anzeige: Kategorie

System und Sicherheit
Status des Computers überprüfen
Sicherungskopien von Dateien mit dem Dateiversionsverlauf speichern
Sichern und Wiederherstellen (Windows 7)

Netzwerk und Internet
Netzwerkstatus und -aufgaben anzeigen

Hardware und Sound
Geräte und Drucker anzeigen
Gerät hinzufügen
Häufig verwendete Mobilitätseinstellungen ändern

Programme
Programm deinstallieren

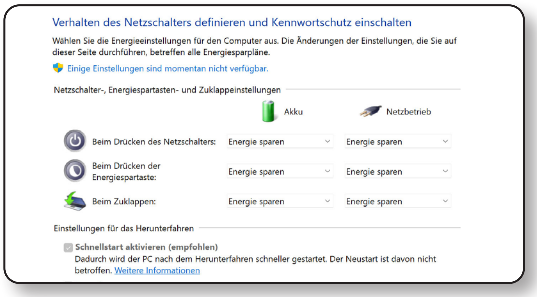
Benutzerkonten
Kontotyp ändern

Darstellung und Anpassung

Zeit und Region
Datums-, Uhrzeit- oder Zahlenformat ändern

Erleichterte Bedienung
Einstellungen empfehlen lassen
Visuelle Darstellung des Bildschirms optimieren

Fig. 9.01: *Control panel*



Verhalten des Netzschalters definieren und Kennwortschutz einschalten

Wählen Sie die Energieeinstellungen für den Computer aus. Die Änderungen der Einstellungen, die Sie auf dieser Seite durchführen, betreffen alle Energiesparpläne.

Einige Einstellungen sind momentan nicht verfügbar.

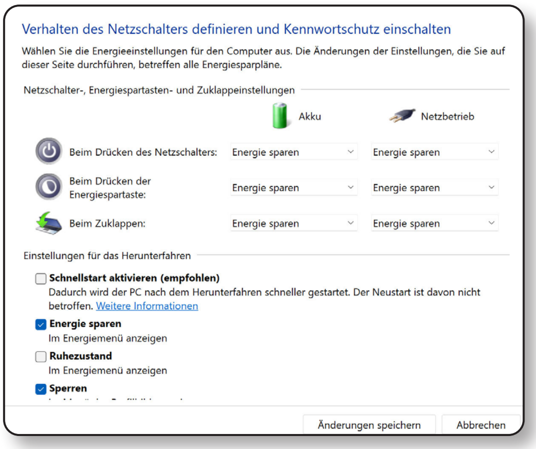
Netzschalter-, Energiespartasten- und Zuklappeinstellungen

	Akku	Netzbetrieb
Beim Drücken des Netzschalters:	Energie sparen	Energie sparen
Beim Drücken der Energiespartaste:	Energie sparen	Energie sparen
Beim Zuklappen:	Energie sparen	Energie sparen

Einstellungen für das Herunterfahren

☑ **Schnellstart aktivieren (empfohlen)**
Dadurch wird der PC nach dem Herunterfahren schneller gestartet. Der Neustart ist davon nicht betroffen. Weitere Informationen

Fig. 9.02: *Change power button action*



Verhalten des Netzschalters definieren und Kennwortschutz einschalten

Wählen Sie die Energieeinstellungen für den Computer aus. Die Änderungen der Einstellungen, die Sie auf dieser Seite durchführen, betreffen alle Energiesparpläne.

Netzschalter-, Energiespartasten- und Zuklappeinstellungen

	Akku	Netzbetrieb
Beim Drücken des Netzschalters:	Energie sparen	Energie sparen
Beim Drücken der Energiespartaste:	Energie sparen	Energie sparen
Beim Zuklappen:	Energie sparen	Energie sparen

Einstellungen für das Herunterfahren

☐ **Schnellstart aktivieren (empfohlen)**
Dadurch wird der PC nach dem Herunterfahren schneller gestartet. Der Neustart ist davon nicht betroffen. Weitere Informationen

☑ **Energie sparen**
Im Energiemenü anzeigen

☐ **Ruhezustand**
Im Energiemenü anzeigen

☑ **Sperren**

Fig. 9.03: *Disable fast startup*

If you need additional support, please contact your IT administration, user support or the ECOS Helpdesk.

9.2 Mac with T2 security chip

In 2018, Apple started including the T2 security chip in iMac Pro, Mac mini, MacBook Air, and MacBook Pro. The T2 security chip contributes to a secure boot process and prevents unauthorized access.

However, it can lead to errors when booting the Secure Boot Stick. Customizing the T2 security chip settings solves the problem.

Check system information to see if your device is equipped with a T2 security chip:

1. Start your Mac without connecting the SBS.
2. Log in with your user credentials.
3. Press and hold OPTIONS (⌥) while clicking the icon in the top menu bar.
   The Apple start menu opens.
4. Select System settings.
5. Go to Controller or Control in the left sidebar. Depending on the macOS version used, this item may also be named iBridge.
6. The controller information shows you the chip model and whether your device is equipped with a T2 security chip.

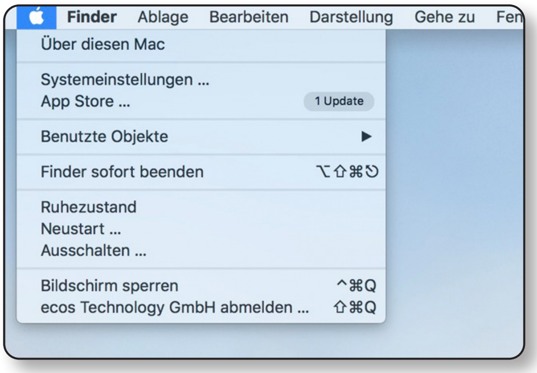
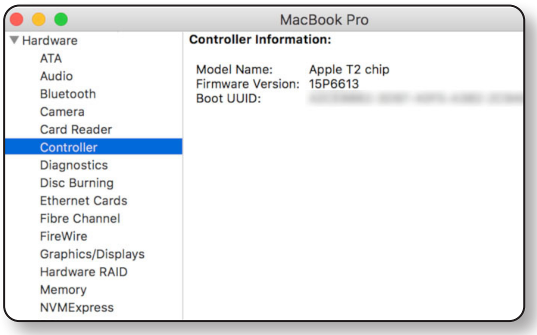


Fig. 9.04: *Apple start menu*



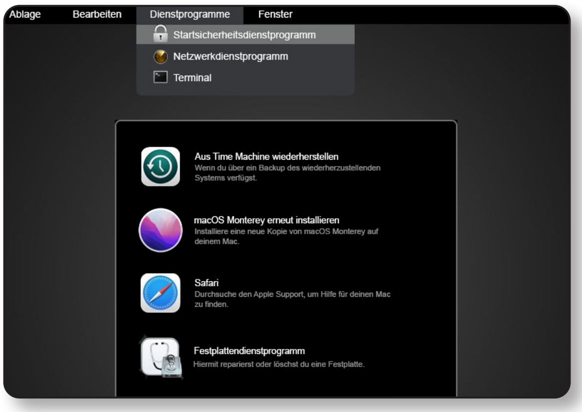
Controller Information:

Model Name: Apple T2 chip
Firmware Version: 15P6613
Boot UUID: [redacted]

Fig. 9.05: *Controller information*

To start your SBS on a Mac with T2 security chip, you need to allow booting from external media:

1. Start your Mac without connected the Secure Boot Stick and immediately press the hotkey COMMAND (⌘) + R until the Apple logo appears.
2. The macOS recovery starts.
3. The macOS Utilities window opens.
4. In the top menu panel, select **Utilities → Start-up Security Utility**.



Aus Time Machine wiederherstellen
Wenn du über ein Backup des wiederherzustellenden Systems verfügst.

macOS Monterey erneut installieren
Installiere eine neue Kopie von macOS Monterey auf deinem Mac.

Safari
Durchsuche den Apple Support, um Hilfe für deinen Mac zu finden.

Festplattendienstprogramm
Hiermit reparierst oder löschst du eine Festplatte.

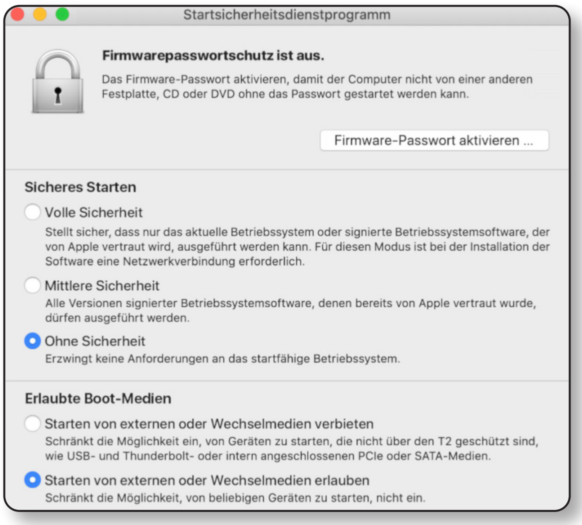
Fig. 9.06: *macOS-Wiederherstellung*

5. Enter the firmware or administrator password when prompted and press OK to confirm.

6. In the section Secure boot, select the option No Security.

7. In the section Allowed Boot Media, select Allow booting from external or removable media.

8. Restart your Mac.



Startsicherheitsdienstprogramm

Firmwarepasswortschutz ist aus.

Das Firmware-Passwort aktivieren, damit der Computer nicht von einer anderen Festplatte, CD oder DVD ohne das Passwort gestartet werden kann.

Firmware-Passwort aktivieren ...

Sicheres Starten

○ Volle Sicherheit
Stellt sicher, dass nur das aktuelle Betriebssystem oder signierte Betriebssystemsoftware, der von Apple vertraut wird, ausgeführt werden kann. Für diesen Modus ist bei der Installation der Software eine Netzwerkverbindung erforderlich.

○ Mittlere Sicherheit
Alle Versionen signierter Betriebssystemsoftware, denen bereits von Apple vertraut wurde, dürfen ausgeführt werden.

● Ohne Sicherheit
Erzwingt keine Anforderungen an das startfähige Betriebssystem.

Erlaubte Boot-Medien

○ Starten von externen oder Wechselmedien verbieten
Schränkt die Möglichkeit ein, von Geräten zu starten, die nicht über den T2 geschützt sind, wie USB- und Thunderbolt- oder intern angeschlossenen PCIe oder SATA-Medien.

● Starten von externen oder Wechselmedien erlauben
Schränkt die Möglichkeit, von beliebigen Geräten zu starten, nicht ein.

Fig. 9.07: *Startup Security Utility settings*

9.3 How to format a USB flash drive

A second, commercially available USB flash drive with a FAT32 file system is required to store the results file of the Secure Boot Stick hardware test. If the USB flash drive supports a different file system (such as FAT16 or NTFS), you must format it.

> Formatting the USB flash drive will irrevocably delete all data stored on it. Check your USB flash drive and back up any data and documents you want to keep.

1. Connect the USB flash drive to to your computer's USB port.

2. Start your Windows operating system.

3. Open the Windows Explorer.

4. Right-click on the USB drive to open the context menu.

5. Select Properties.

6. Select the tab General and check the information field File system.

7. If the file system is FAT32, the USB flash drive is already correctly formatted. Close the window and continue with the hardware test as described in sections *6.5.2 Automatic hardware test* and *7.4.3.4 Hardware test*. If the information field shows a different file system, proceed with step 8.

8. Close the Properties window and open the context menu of the USB drive again.

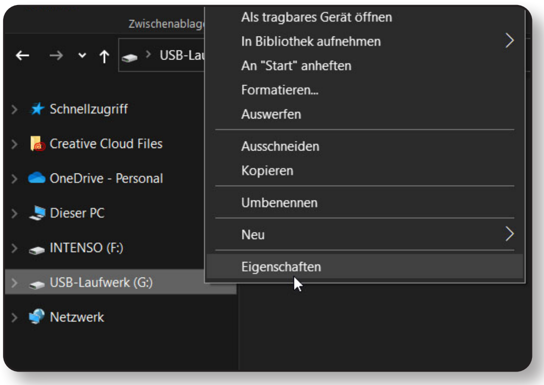
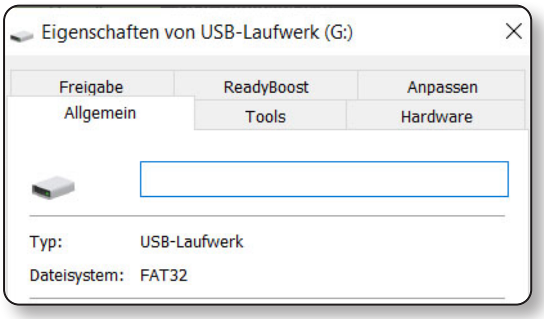


Fig. 9.08: *Context menu - properties*

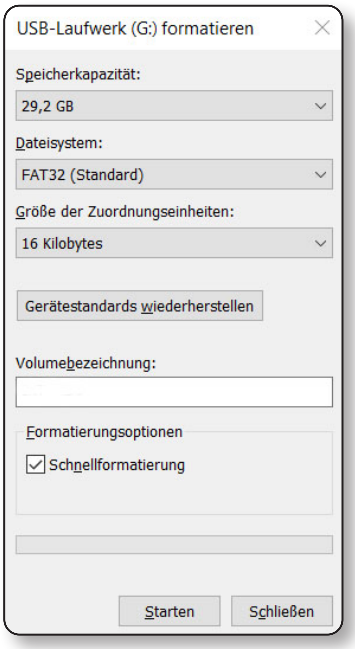


Eigenschaften von USB-Laufwerk (G:)

Typ: USB-Laufwerk

Dateisystem: FAT32

Fig. 9.09: *USB properties*



USB-Laufwerk (G:) formatieren

Speicherkapazität: 29,2 GB

Dateisystem: FAT32 (Standard)

Größe der Zuordnungseinheiten: 16 Kilobytes

Volumebezeichnung:

Formatierungsoptionen

☑ Schnellformatierung

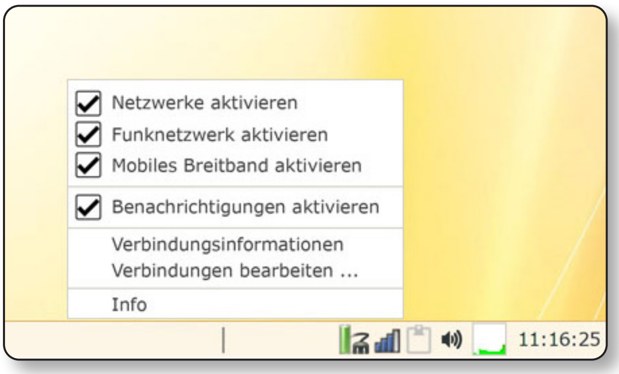
Fig. 9.10: *Format USB drive*

9. Select the option FORMAT....
   A new window opens.
10. In the FILE SYSTEM field, select the option FAT32.
11. If required, enter a random name for your USB flash drive in the VOLUME NAME field.
12. Start the formatting process.
13. Once formatting is complete, the USB flash drive is ready to be used as a storage medium for the hardware test.

9.4 Setting up a cellular network

If your computer is equipped with a cellular module and has a SIM card inserted, you can set up and use a connection to a cellular network. Make sure that ENABLE MOBILE BROADBAND is active.

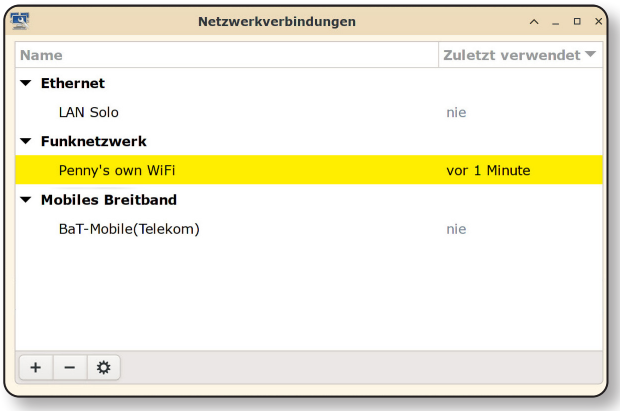
1. Connect your SBS to your computer's USB port.
2. Start your computer.
3. When the SBS desktop appears, right-click on the network manager icon in the system tray.
4. Select the option EDIT CONNECTIONS....
5. Click + (ADD A NEW CONNECTION).



☑ Netzwerke aktivieren
☑ Funknetzwerk aktivieren
☑ Mobiles Breitband aktivieren
☑ Benachrichtigungen aktivieren
Verbindungsinformationen
Verbindungen bearbeiten ...
Info
11:16:25

Fig. 9.11: *Open the network manager context menu*

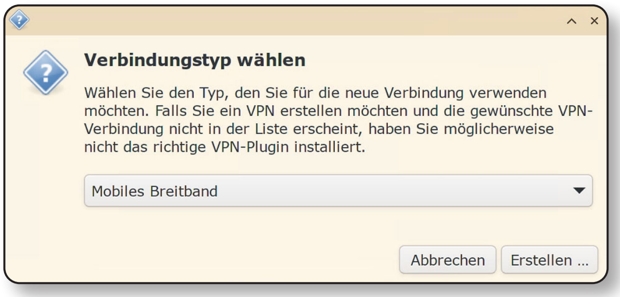
6. In the connection type dialog, select MOBILE BROADBAND and press CREATE... to confirm.



Netzwerkverbindungen

Name	Zuletzt verwendet
Ethernet	
LAN Solo	nie
Funknetzwerk	
Penny's own WiFi	vor 1 Minute
Mobiles Breitband	
BaT-Mobile(Telekom)	nie

Fig. 9.12: *Edit connections*



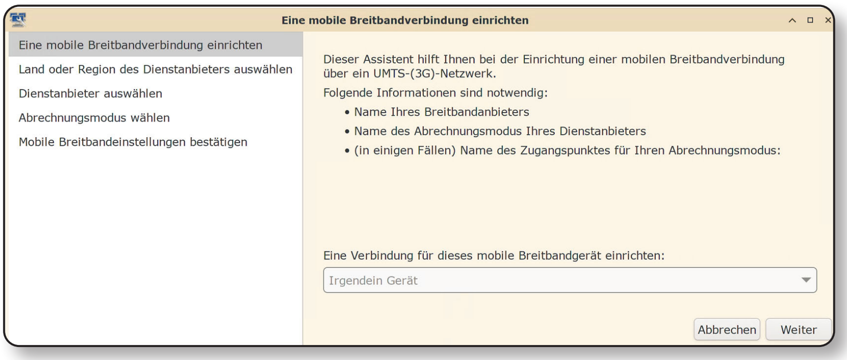
Verbindungstyp wählen

Wählen Sie den Typ, den Sie für die neue Verbindung verwenden möchten. Falls Sie ein VPN erstellen möchten und die gewünschte VPN-Verbindung nicht in der Liste erscheint, haben Sie möglicherweise nicht das richtige VPN-Plugin installiert.

Mobiles Breitband

Fig. 9.13: *Select connection types*

7. A wizard is launched to guide you through the setup process.



Eine mobile Breitbandverbindung einrichten

- Eine mobile Breitbandverbindung einrichten
- Land oder Region des Dienstanbieters auswählen
- Dienstanbieter auswählen
- Abrechnungsmodus wählen
- Mobile Breitbandeinstellungen bestätigen

Dieser Assistent hilft Ihnen bei der Einrichtung einer mobilen Breitbandverbindung über ein UMTS-(3G)-Netzwerk.

Folgende Informationen sind notwendig:

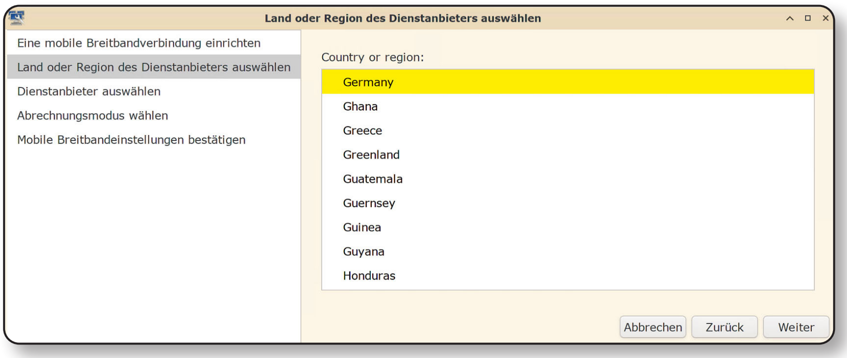
- Name Ihres Breitbandanbieters
- Name des Abrechnungsmodus Ihres Dienstanbieters
- (in einigen Fällen) Name des Zugangspunktes für Ihren Abrechnungsmodus:

Eine Verbindung für dieses mobile Breitbandgerät einrichten:

Irgendein Gerät

Fig. 9.14: *Wizard for mobile broadband connection*

8. Select the country of your cell phone provider and press Next to confirm.
   The countries are listed alphabetically.



Land oder Region des Dienstanbieters auswählen

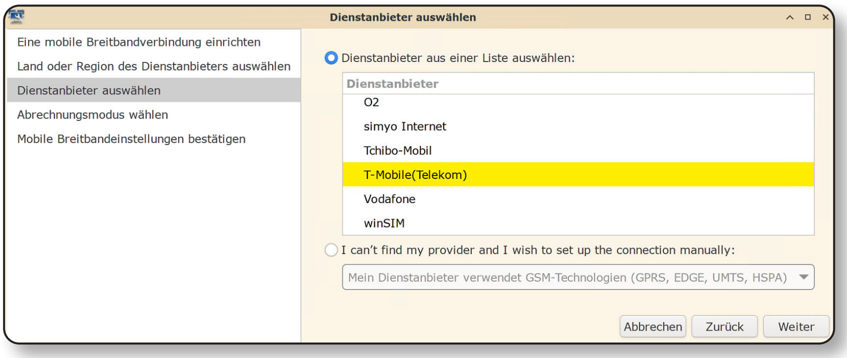
- Eine mobile Breitbandverbindung einrichten
- Land oder Region des Dienstanbieters auswählen
- Dienstanbieter auswählen
- Abrechnungsmodus wählen
- Mobile Breitbandeinstellungen bestätigen

Country or region:

- Germany
- Ghana
- Greece
- Greenland
- Guatemala
- Guernsey
- Guinea
- Guyana
- Honduras

Fig. 9.15: *Select country*

9. Select your service provider. If you do not know your provider or if your provider is not listed, you can also set up the connection manually.
   Press Next to confirm.



Dienstanbieter auswählen

- Eine mobile Breitbandverbindung einrichten
- Land oder Region des Dienstanbieters auswählen
- Dienstanbieter auswählen
- Abrechnungsmodus wählen
- Mobile Breitbandeinstellungen bestätigen

● Dienstanbieter aus einer Liste auswählen:

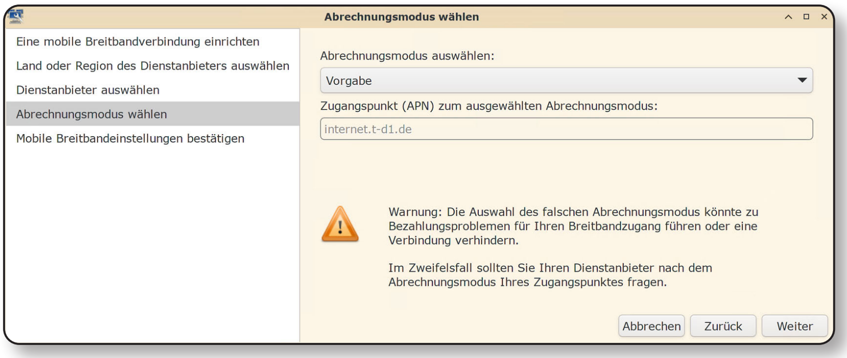
Dienstanbieter
O2
simyo Internet
Tchibo-Mobil
T-Mobile(Telekom)
Vodafone
winSIM

○ I can't find my provider and I wish to set up the connection manually:

Mein Dienstanbieter verwendet GSM-Technologien (GPRS, EDGE, UMTS, HSPA)

Fig. 9.16: *Select service provider*

10. Set the Billing mode and, if required, your your cell phone provider's Access point (APN). You will usually find this information in your cell phone contract.
    Press Next.



Abrechnungsmodus wählen

Eine mobile Breitbandverbindung einrichten
Land oder Region des Dienstanbieters auswählen
Dienstanbieter auswählen
Abrechnungsmodus wählen
Mobile Breitbandeinstellungen bestätigen

Abrechnungsmodus auswählen: Vorgabe

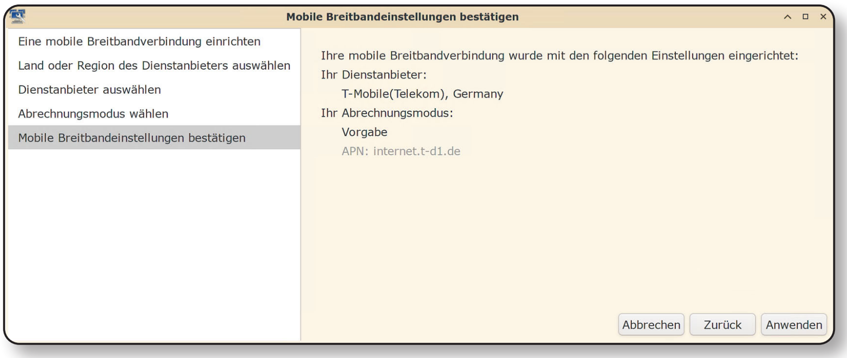
Zugangspunkt (APN) zum ausgewählten Abrechnungsmodus: internet.t-d1.de

Warnung: Die Auswahl des falschen Abrechnungsmodus könnte zu Bezahlungsproblemen für Ihren Breitbandzugang führen oder eine Verbindung verhindern.

Im Zweifelsfall sollten Sie Ihren Dienstanbieter nach dem Abrechnungsmodus Ihres Zugangspunktes fragen.

Fig. 9.17: *Billing mode and APN*

11. Check your settings and press Apply to confirm.



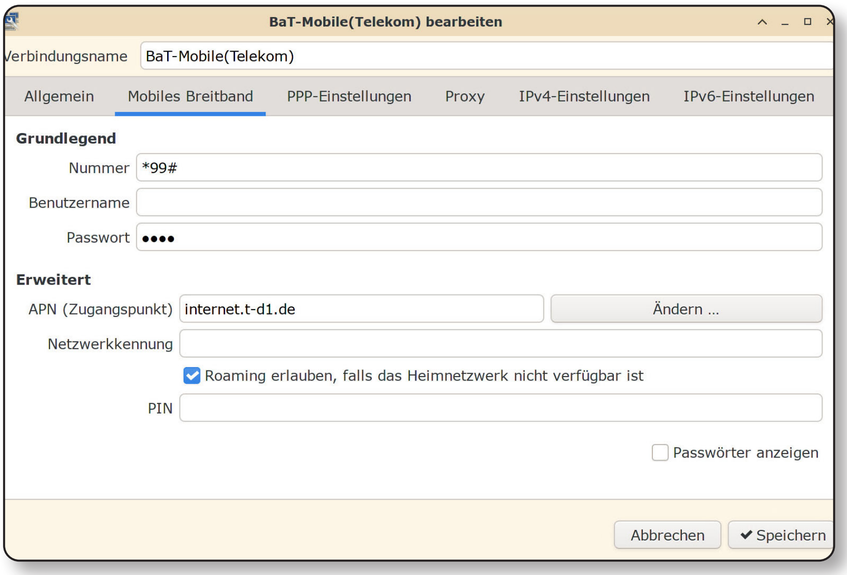
Mobile Breitbandeinstellungen bestätigen

Eine mobile Breitbandverbindung einrichten
Land oder Region des Dienstanbieters auswählen
Dienstanbieter auswählen
Abrechnungsmodus wählen
Mobile Breitbandeinstellungen bestätigen

Ihre mobile Breitbandverbindung wurde mit den folgenden Einstellungen eingerichtet:
Ihr Dienstanbieter:
T-Mobile(Telekom), Germany
Ihr Abrechnungsmodus:
Vorgabe
APN: internet.t-d1.de

Fig. 9.18: *Settings summary*

12. You can now make further settings, e.g. assign a new name. Please note that the connection will only be created after you have saved your settings



BaT-Mobile(Telekom) bearbeiten

Verbindungsname: BaT-Mobile(Telekom)

Grundlegend
Nummer: *99#
Benutzername:
Passwort: ••••

Erweitert
APN (Zugangspunkt): internet.t-d1.de
Netzwerkkennung:
☑ Roaming erlauben, falls das Heimnetzwerk nicht verfügbar ist
PIN:
□ Passwörter anzeigen

Fig. 9.19: *Connection editor*

9.5 FX/SX data safe

In addition to the Secure Boot Stick software, the SBS FX/SX also includes a hardware-encrypted data safe for the secure storage of data and documents. The data safe accessible from any operating system without the installation of software. A smartcard is required for the functionality.

You can use the data safe in two ways:

- During ongoing operation of SBS. The data safe is unlocked after booting.
  Please note that the data safe is only available if it has been configured on the SMA by your IT administration and if it has been released for the destinations of your user account.

- As USB drive under a different operating system (Windows, Mac OS, Linux).
  The data safe is unlocked after the SBS is connected to the started computer.

If you safely remove the SBS as removable media or shut down your computer, access to the data safe will be blocked and must be unlocked the next time you use it.

9.5.1 Unlock data safe

You can unlock the data safe on the PIN pad of the Secure Boot Stick .

1. Connect the SBS to your computer's USB port. Wait until the ECOS key lights white.

2. Press the ECOS key. It lights dark blue, the digit keys are white.

3. Press 1 to activate the data safe. The ECOS key lights green.

4. Press the ✓ key to confirm. The ECOS key flashes yellow.

5. Enter the smartcard PIN. The ECOS key flashes yellow during entry.

6. Press the ✓ key to confirm.
   If the PIN is correct, the ECOS key briefly flashes yellow, then lights green. The data safe is unlocked.
   If the PIN is incorrect, the ECOS key lights up red. The process is canceled. Repeat the procedure beginning with step 2.

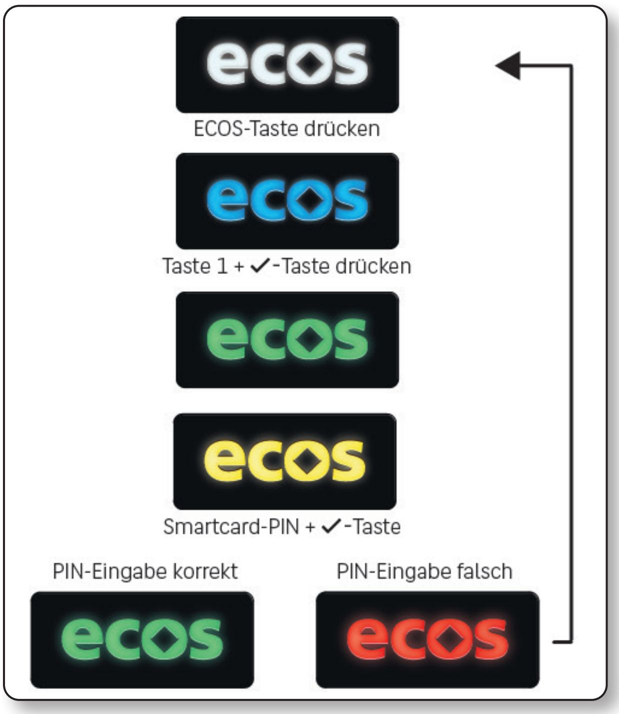


Fig. 9.20: *Unlock the data safe*

Please note that you cannot make any further entries (exception: PIN entry to unlock the screen) on the SBS PIN pad when the data safe is unlocked. To do this, you must reboot SBS.

9.5.2 Enable/disable write access for the data safe

The data safe can be used without write access, for example to read the documents without editing them.

Read-only access is recommended when using the data safe on an unknown device to prevent malware from altering the data safe contents.

Write access can be enabled and disabled while the SBS is running or on a regularly booted computer.

1. Connect the SBS to your computer's USB port.
   The ECOS key lights white. It lights yellow on a booted computer.

2. Press the ECOS key. The ECOS key lights dark blue.

3. Press 2 to enable/disable write access.
   The ECOS key lights green if write access is enabled
   The ECOS key lights magenta if write access is disabled.

4. Press the ✓ key to confirm. The ECOS key flashes yellow.

5. Enter your smartcard PIN. The ECOS key flashes yellow during entry.

6. Press the ✓ key to confirm.
   If the PIN is correct, the ECOS key flashes magenta to confirm that write access has been disabled. The ECOS key flashes green to confirm that write access is enabled. The ECOS key then lights white again.
   If the PIN is incorrect, the ECOS key briefly flashes red, then lights white. The process is canceled. Repeat the procedure beginning with step 3.
   If you have changed write access while the SBS was running, the ECOS key lights yellow instead of white.

7. Unlock the data safe as described above in section *9.5.1 Unlock data safe*.
   The ECOS key lights magenta when the data safe is unlocked in read-only mode.
   The ECOS key lights up green when the data safe is unlocked in write mode.

ECOS Technology GmbH
Sant' Ambrogio-Ring 13 a-b
D-55276 Oppenheim

E-Mail: info@ecos.de
Internet: www.ecos.de