ETAS ES820 Drive Recorder Configurator and Service Pack V7.3

Installation and Administration

Copyright

Contents

1   Safety and Privacy Information

1.1   Intended Use

The ES820 Drive Recorder hardware together with the Drive Recorder Service Pack software and the Drive Recorder Configurator software is designed for the following purposes:

- Configuration via the Drive Recorder Configurator software for automatic execution of recording jobs on the basis of INCA export files
- Use in a vehicle for the purpose of test drives as well as use in the laboratory
- Integration into existing vehicle instrumentation, replacing the INCA PC
- Signal recording from ECUs, buses, networks, and measuring instruments
- Data transfer via USB and FTP

The Drive Recorder software consists of two components:

- Drive Recorder Configurator
- Drive Recorder Service Pack

To be able to operate the ES820 Drive Recorder, the Drive Recorder Configurator has to be installed on your local PC.

The Drive Recorder Service Pack is installed on the ES820 Drive Recorder already upon receipt of the device and can be updated regularly. The Drive Recorder Service Pack includes INCA installation files.

The Drive Recorder software also includes a Display App, which is designed to access the Drive Recorder by a touch screen monitor. For further information and the intended use of the Display App, read the ETAS Drive Recorder Display App - User Guide.

The ES820 Drive Recorder and the Drive Recorder Configurator software must only be used by qualified personnel as defined in "Target Group" below, under consideration of the "Safety Information" on page 7 , and for the purposes that are described in the corresponding user documentation. ETAS GmbH cannot be made liable for damage that is caused by improper use and not adhering to the safety instructions.

1.2   Target Group

The ES820 Drive Recorder together with the Drive Recorder Service Pack and the Drive Recorder Configurator is designed for engineers working in the field of measurement and calibration. Experience with the ETAS software INCA is necessary.

Test drivers may use the ES820 Drive Recorder after instruction and under supervision of a responsible calibration engineer.

This document addresses tool coordinators and also all those who manage their own device.

1.3   Classification of Safety Messages

The safety messages in this document warn of dangers that can lead to personal injury or damage to property:

> ⚠️ **DANGER**
>
> indicates a hazardous situation with a high risk of death or serious injury if not avoided.

> ⚠️ **WARNING**
>
> indicates a hazardous situation of medium risk which could result in death or serious injury if not avoided.

> ⚠️ **CAUTION**
>
> indicates a hazardous situation of low risk which may result in minor or moderate injury if not avoided.

> *NOTICE*
>
> indicates a situation which may result in damage to property if not avoided.

1.4   Safety Information

Hardware

> ⚠️ For safe connection and operation of the ES820 Drive Recorder, read the "ETAS ES800 Measurement, Calibration, and Prototyping System - User Guide" and the "ETAS ES800 System - Safety Advice".

Software

> ⚠️ Observe the ETAS Safety Advice, which is displayed when starting the Drive Recorder Configurator software.

Additionally, observe the following safety messages when configuring the device settings. You can access the **Device Settings** in the **Hardware Configuration** window of the Drive Recorder Configurator.

⚠️ **WARNING**

Risk of unexpected vehicle behavior

If the Drive Recorder is operated in combination with an ETK, an ECU reset is possible. An ECU reset can result in engine shutdown, which can cause unexpected vehicle behavior.

Even if **Allow ETK Reset** is turned **OFF**, the ETK and the ECU can be reset by executing the command **Run selected recording job with risk of ECU reset** or **Run selected experiment with risk of ECU reset**.

— Only modify the test setup when the vehicle is stationary.

— Only load experiments when the vehicle is stationary.

— Only update the software when the vehicle is stationary.

— Only start recording jobs when the vehicle is stationary.

— Before driving, always wait until the MEAS LED of the Drive Recorder is permanently lit.

If using the Display App, additionally pay attention to the following safety message:

> ⚠️ **WARNING**
>
> **Risk of unexpected vehicle behavior**
>
> If the Drive Recorder is operated in combination with an ETK, an ECU reset is possible. An ECU reset can result in engine shutdown, which can cause unexpected vehicle behavior.
>
> — Only modify the test setup when the vehicle is stationary.
>
> — Only start recording jobs when the vehicle is stationary.
>
> — Before driving, always wait until the **Recorder Status** window of the Display App shows green side bars.

1.5 Privacy Notice

Your privacy is important to ETAS. This Privacy Notice informs you about which personal data are processed when using this product, which data categories this product uses for personal data, and what technical measures you have to take to ensure the privacy of users. Additionally, information is provided on where this product stores personal data and how to delete them.

1.5.1 Data Processing

Note that personal data or data categories are processed when using this product. The purchaser of this product is responsible for the legal conformity of processing the data in accordance with Article 4 No. 7 of the General Data Protection Regulation (GDPR). As the manufacturer, ETAS GmbH is not liable for any mishandling of this data.

1.5.2 Data and Data Categories

When using the ETAS License Manager in combination with user-based licenses, particularly the following personal data and data categories can be recorded for the purpose of license management:

- Communication data: IP address
- User data: UserID, Windows User ID

Additionally, the ES820 Drive Recorder records the following personal data and data categories:

When configuring automated file transfer via FTP, the ES820 Drive Recorder stores the following personal data:

- User data: FTP file transfer User ID and password

When configuring automated file transfer to a Windows share, the ES820 Drive Recorder stores the following personal data:

- User data: Windows User ID and password

When using the ES820 Drive Recorder in combination with other software components, additional personal data or data categories may be collected for the purpose of measurement data analysis. Possible examples are the vehicle identification number (VIN), the number plate, GPS data, video data, audio data, or other measurement data. Your organization can determine which data or data categories are collected when configuring the measurement system. These data are stored in the measurement files and you can only delete them by deleting the respective measurement files.

Your organization is responsible for the compliant handling of the data in accordance with the applicable national law.

1.5.3   Technical and Organizational Measures

By default, the ES820 Drive Recorder does neither encrypt personal data nor any other data that is stored on the Drive Recorder hard disk. Data that is transferred by FTP is also not encrypted by default.

1.5.3.1   Encryption Features

To protect personal data as well as any other data that is stored on the ES820 Drive Recorder hard disk or transmitted via a network, the Drive Recorder Configurator software provides features for data encryption. The following features can be accessed and applied via the Drive Recorder Configurator **Hardware Configuration** window:

- Hard disk encryption

  You can access the **Hard Disk Encryption** feature via the **Hardware Configuration** window in the **Device Options**. If applied, all data on the ES820 Drive Recorder hard disk are encrypted.

- FTP security settings

  You can access this feature via the **Hardware Configuration** window in the **File transfer settings** and select either "none", "SFTP", or "FTPS". If SFTP or FTPS is enabled, the data is encrypted only during transmission.

- End-to-end encryption for file transfer

  You can access the **End-to-End Encryption** feature via the **Hardware Configuration** window in the **File transfer settings**. If applied, the transmitted data is encrypted during transmission as well as on intermediary and final locations, such as servers and computers.

You can find a detailed description about how to configure and apply the security settings in the section <u>"Managing Data Security" on page 29</u>.

1.5.3.2   Further Measures

In addition, we recommend your IT department to provide further suitable technical or organizational measures, such as classic theft protection and access protection to the hardware of the test set-up.

2   Finding out More

Apart from this document, you can find more information on the Drive Recorder in the following user documentation:

- ETAS ES800 Measurement, Calibration, and Prototyping System - User Guide
- ETAS ES800 System - Safety Advice
- ETAS Drive Recorder Display App - User Guide
- ETAS ES820 Drive Recorder - Tutorial
- Drive Recorder Configurator - Online Help
- INCA - Online Help

3   Installation

To install the Drive Recorder software components, take into account the over-
view of the Drive Recorder package contents, the system requirements, and
necessary preparations as described in this chapter.

You get information on how to download the installation files and how to
install the software components in the correct order.

3.1   Package Contents

The Drive Recorder software consists of three installation packages with the
listed components:

- Drive Recorder Configurator
  — Drive Recorder Configurator software
  — Documentation:
    Online Help
    Manuals in PDF format
    Release Notes
    What's New
- Drive Recorder Service Pack
  — Drive Recorder Control Software
  — Drive Recorder Configurator
  — INCA including basic add-on:
    INCA Drive Recorder Add-On
  — INCA licensed add-ons:
    INCA EIP Add-On
    INCA LIN Add-On
    INCA FlexRay Add-On
    INCA ODX-Link Add-On
    INCA Vector Hardware Add-On
- Drive Recorder Image
  — The Drive Recorder Image contains all necessary system software
    for resetting the Drive Recorder system to factory settings by use of
    the USB Rescue Stick. For more information, read "Resetting the
    Drive Recorder System to Factory Settings" on page 21.

3.2   System Requirements

The following system requirements are necessary to install and run the Drive Recorder Configurator software on your PC and to connect to the Drive Recorder:

	Minimum Requirements
Processor	Intel® Core™ i5 8 GB RAM
Operating System	Windows 10
Ethernet	Free Gigabit Ethernet RJ45 connector
USB	Free USB port (USB 3.0 recommended)

You may install INCA on the same PC. In this case, also take the system requirements for INCA into account. You can find the system requirements for INCA in the ETAS INCA - Installation Guide.

3.3   Version Compatibility

If you already have a Drive Recorder Configurator installation on your local PC, you must observe the following version compatibiliy requirements:

Drive Recorder Software

It is possible to have both installation versions Drive Recorder Configurator V7.3 and Drive Recorder Configurator V7.2 on your local PC at the same time. For operation, the versions of the Drive Recorder Configurator and the Drive Recorder Service Pack must match. In case of mismatch, a warning message is displayed.

To find out your current Drive Recorder Configurator version

- In the menu bar of the **Drive Recorder Configurator** window, click **Help** > **About**.

  The Drive Recorder Configurator version is displayed in the **About** window.

To find out the installed Drive Recorder Service Pack version

- In the menu bar of the Drive Recorder Configurator, click **Tools** > **Install** or click .

  The **Installation** dialog window opens. You can see the available EXE files in the **Available Installations** window area and the installes Service Pack version in the **Currently installed version** window area.

INCA

The Drive Recorder Service Pack version also indicates the INCA version that is included in the Drive Recorder Service Pack. Thus, best compatibility is given when you always use the same version of the INCA Service Pack, the Drive Recorder Service Pack, and the Drive Recorder Configurator. For more information on compatibility, read the Drive Recorder - Release Notes.

HSP

The Drive Recorder replaces the INCA PC in the measurement setup. If you use INCA or the Drive Recorder together with ETAS hardware, it is also necessary to update all firmware. For compatible versions, see the Drive Recorder - Release Notes.

To update the firmware via the Drive Recorder from your local PC

The Drive Recorder must be connected to your local PC via the HOST connector and via the Drive Recorder Configurator.

All hardware that is relevant for the HSP update must be connected to the Drive Recorder.

1. Switch the Drive Recorder into the passive mode.

   To switch between the active mode and the passive mode, press the Drive Recorder power button. In the passive mode, the ON LED is blinking with a 50% duty cycle. In the active mode, the ON LED is lit permanently.

2. Download the installation file for the appropriate HSP version from the ETAS Download Center.

3. To install the HSP Update Tool on your local PC, double-click the HSP installation file.

4. Open the HSP Update Tool.

5. To perform the firmware update for the connected ETAS hardware, refer to the information provided on the ETAS Download Center and in the HSP Update Tool – Online Help.

3.4   Installing the Drive Recorder Configurator

To be able to install the Drive Recorder Service Pack on the Drive Recorder, you must install the Drive Recorder Configurator on your local PC first.

To install the Drive Recorder Configurator on your local PC

1. Download the Drive Recorder Configurator ZIP file to your local PC from the ETAS Download Center.

2. Unzip the file on your local PC.

3. Double-click `DriveRecorder Configurator_<version>.exe`.

    A wizard leads you through the installation.

> **i   Note**
>
> Selecting the `Program Files` Windows standard folder for Drive Recorder data files may lead to problems in the Drive Recorder Configurator since the access to the program folder depends on the Windows user rights.
>
> Do not save Drive Recorder data files in the `Program Files` folder. Select a folder in a data area where all users have read and write access rights.

> **i   Note**
>
> The language that you select during installation changes the global language settings of all ETAS software that is already installed on your PC.

3.5   Files and Folders

After the installation of the Drive Recorder Configurator, installation files and data files are stored on your local PC.

The installation files, data files, log files, and temp files are stored in different directories. If you uninstall or upgrade the software later, only the installation files are deleted or overwritten, respectively. The data files are still available.

Folders that contain useful files and information are the data folders and the `Manuals` folder.

3.5.1   Data Folders and Files

The data files are stored in the following subfolders of
`..\ETASdata\DriveRecorder<Version>` by default:

Data Folder	Content
Archives	Drive Recorder Archive files (`*.dra`) with multiple content, e.g. INCA export files, recording job configuration files, hardware configuration files, Seed&Key files, etc.)
Configurations	Hardware configuration files (`*.xml`)
Export	INCA export files (`*.exp` and `*.exp.wsmd`)
ExternalTools	Software installation files (`*.exe`) for external applications
Installations	Drive Recorder Service Pack files (`*.exe`)
Licenses	ETAS license files (`*.lic`)
LogFiles	Log files (`*.log`) created by the Drive Recorder and INCA
Measure	Measurement files (`*.mf3` or `*.mf4`) Supported measurement file formats: MDF 3.0, MDF 3.3, MDF 4.0, MDF 4.1
RescueStickCreator	Installation files to create a USB Rescue Stick Subfolder for the Drive Recorder image file
Runtime	Firmware components for the Drive Recorder
Security	Customer-specific files for end-to-end encryption: .Net DLL files for the file encryption algorithms, subfolder `Certificates` for XML file for the public key Seed&Key files

On the Drive Recorder, the same folders exist. You can access them via the Drive Recorder Configurator for file transfer between your local PC and the Drive Recorder as described in the Drive Recorder Configurator - Online Help. This kind of file transfer is also used for "Installing the Drive Recorder Service Pack" on page 20.

3.5.2   Manuals Folder

The `Manuals` folder contains user documentation in PDF format. You can find it at the following default location:

`c:\ETAS\DriveRecorder<Version>\Manuals`

3.6   Preparing to Install Software on the Drive Recorder

To be able to install software on the Drive Recorder, you have carried out the instructions of "Installing the Drive Recorder Configurator" on page 15. When properly connected, you can install software on the Drive Recorder from your local PC via the Drive Recorder Configurator. Read how to connect the Drive Recorder to your local PC in the next sections.

3.6.1   Connecting the Drive Recorder Hardware to the Local PC

To install software on the Drive Recorder, the device must be connected to a suitable power supply and to your local PC. The permissible supply voltage range is 6 V to 32 V.

⚠️ For safe connection and operation of the ES820 Drive Recorder, read the "ETAS ES800 Measurement, Calibration, and Prototyping System - User Guide" and the "ETAS ES800 System - Safety Advice".

To connect the Drive Recorder hardware to your local PC

1. Establish the connection of the ES820 Drive Recorder hardware to a suitable power supply as well as the Ethernet connection between Drive Recorder and your PC. For this purpose, follow the instructions in the "ETAS ES800 Measurement, Calibration, and Prototyping System - User Guide" and use cables and a power supply as described therein.

2. Turn on the Drive Recorder and wait until the ON LED is lit permanently.

3. If you connect to the Drive Recorder from your local PC for the first time, see how "To configure the network settings on your local PC" on the next page.

3.6.2   Configuring the Network Settings on the Local PC

The default Drive Recorder IP address is 192.168.40.228. To be able to establish an Ethernet connection between your local PC and the Drive Recorder, you must adapt the network settings on your local PC.

<u>To configure the network settings on your local PC</u>

The Drive Recorder must be connected to your local PC and turned on as described in<u>"Connecting the Drive Recorder Hardware to the Local PC" on the previous page</u>. When the ON LED of the Drive Recorder is permanently lit, you can proceed with the following steps:

1. From the Windows 10 Start menu ⊞ , select ⚙ **Settings** > **Network & Internet** > **Network and Sharing Center**.

    The **Network and Sharing Center** window is displayed.

2. Click according to the sequence in the image below.

    After click 4, the **Internet Protocol Version 4** window opens.
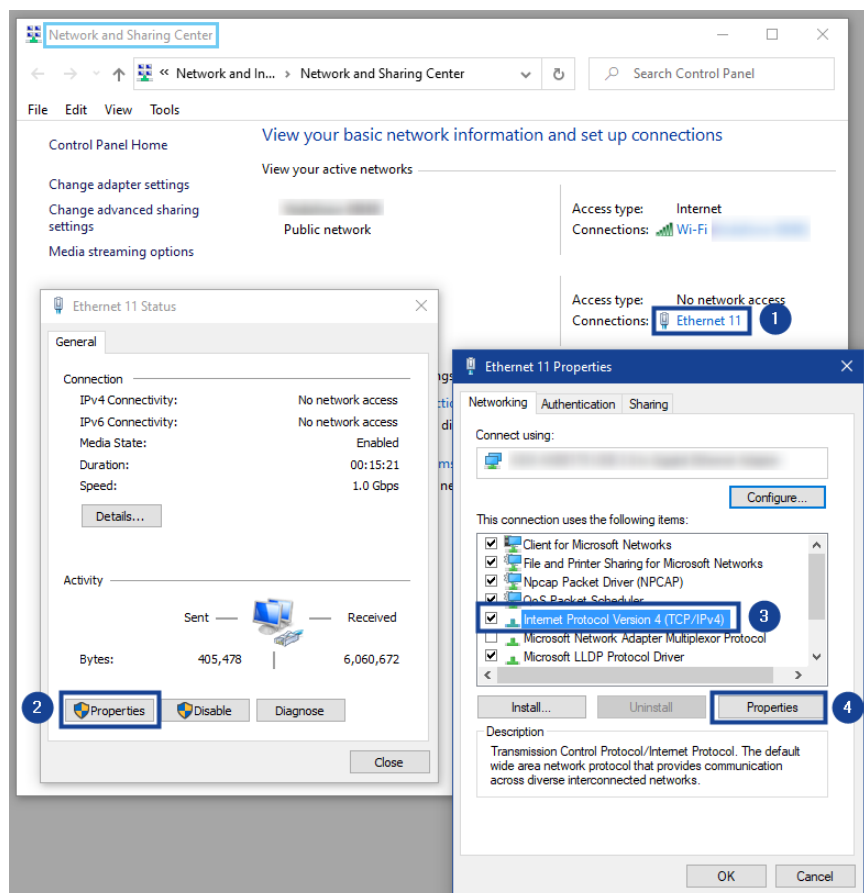
3. In the **Alternate Configuration** tab of the **Internet Protocol Version 4** window, make the following **User Configured** entries, according to the image below:

— IP adress: 192.168.40.99

— Subnet mask: 255.255.255.0
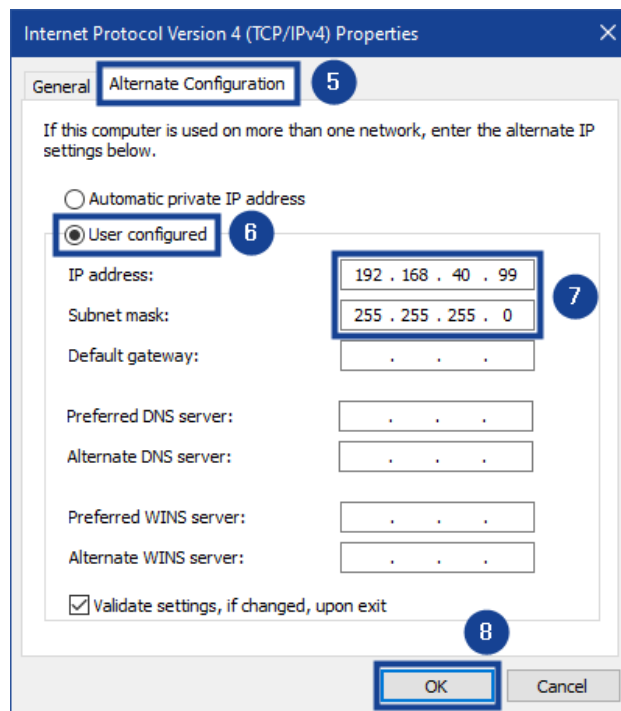
4. After you have confirmed the settings with **OK**, you can close the **Network and Sharing Center**.

3.6.3 Connecting to the Drive Recorder via the Drive Recorder Configurator

According to the previous sections, you have connected the Drive Recorder hardware to your local PC, turned on the Drive Recorder, and made the appropriate network settings on your local PC.

To connect to the Drive Recorder from your local PC via the Drive Recorder Configurator

Make sure that the ON LED of the Drive Recorder is lit permanently.

1. Start the Drive Recorder Configurator on your local PC.

2. In the menu bar, click **File** > **Connect Device** or click 🪁.

   The **Connect Device** dialog window opens.

3. Enter the following IP address in the **Device** field:

   192.168.40.228

4. Optionally, enable the **Automatically open configuration from device** option to open the current hardware configuration in the Drive Recorder Configurator.

5. Click **Connect**.

> The device connects to the Drive Recorder Configurator on your PC.

Now you can use the Drive Recorder Configurator for "Installing the Drive Recorder Service Pack" below or "Installing 3rd Party Software" on page 27.

3.7 Installing the Drive Recorder Service Pack

Before you begin to install the Drive Recorder Service Pack on the Drive Recorder, make sure that you have finished all steps described in "Preparing to Install Software on the Drive Recorder" on page 17.

ℹ Note

In order to transfer files and to install software, the Drive Recorder must be turned on and connected to your local PC.

To transfer the Service Pack EXE file to the Drive Recorder

Download the Service Pack EXE file from the ETAS Download Center and store the EXE file on your local PC at the following location:

`..\ETASdata\DriveRecorder<Version>\Installations`

Make sure that the ON LED of the Drive Recorder is lit permanently.

1. In the menu bar of the Drive Recorder Configurator, click **Tools** > **File Transfer from/to Drive Recorder** or click 🔼.

   The **File Transfer** window opens. You can see the folder structure on the local PC and on the Drive Recorder in the left and right part of the window, respectively.

2. To open the installation folders on both sides, click +. Select the EXE file that you want to transfer.
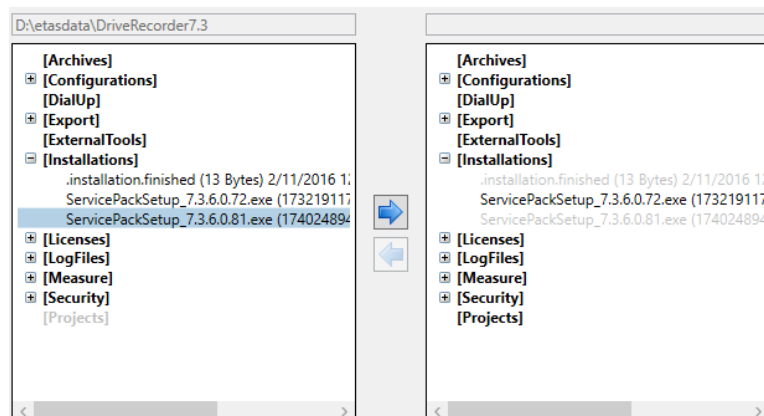
3. Click 🔜 to transfer the EXE file to the `installations` folder on the Drive Recorder.

To install the Service Pack on the Drive Recorder

Make sure that the ON LED of the Drive Recorder is lit permanently.

1. In the menu bar of the Drive Recorder Configurator, click **Tools** >
   Install or click ![icon].

   The **Installation** dialog window opens. You can see the available
   EXE files in the **Available Installations** window area and the
   installed Service Pack version in the **Currently installed version**
   window area.

2. In the **Available Installations** window area, select the cor-
   responding EXE file.

3. Click **Run installation**.

   The selected software is installed on the Drive Recorder. The
   installation and the rebooting of the Drive Recorder takes some
   time.

   When the ON LED is permanently lit again, the installation of the
   Service Pack is finished and your Drive Recorder is ready for oper-
   ation.

3.8   Resetting the Drive Recorder System to Factory Settings

> ### *NOTICE*
>
> Risk of Data Loss
>
> If you reset the Drive Recorder to the factory settings by the USB Rescue
> Stick, all your measurement data on the Drive Recorder hard disk are lost.
> From the `..\ETASdata\DriveRecorder<Version>` data folder, only
> data in the `Configurations`, `Runtime`, `LogFiles`, `Licenses`, and
> `Security` folders are preserved.
>
> For an encrypted Drive Recorder, the device-specific hardware configuration
> and the license file are lost as well.
>
> — Transfer your data to a different storage location regularly.
>
> — Make sure that you have a backup USB Security Key for your Drive
>   Recorder.
>
> — Save the license file at a secure location.

To upgrade or to downgrade your Drive Recorder, or to repair your Drive
Recorder installation, you have the option to create a USB stick for flashing.
This option is called *USB Rescue Stick*.

By default, the USB Rescue Stick solution is provided in the following folder,
together with your installation files:

```
..\ETASData\DriveRecorder<Version>\RescueStickCreator
```

3.8.1   Creating the USB Rescue Stick

To create the USB Rescue Stick with a system recovery image for your Drive Recorder on it, you need the following prerequisites:

- USB stick
- Recovery image for your Drive Recorder

  to be downloaded (see below)
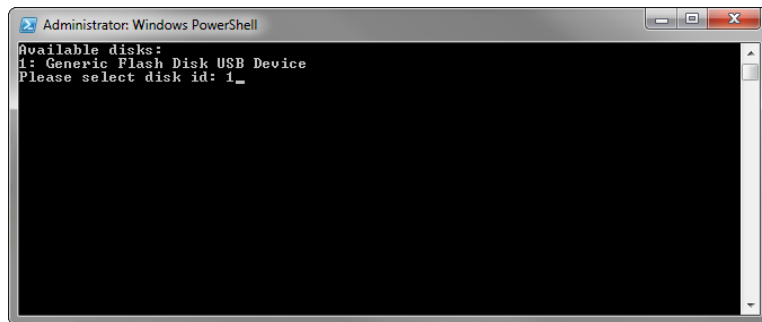
To create the USB Rescue Stick

1. Download the Drive Recorder image on your Drive Recorder from the ETAS Download Center.

2. To install the recovery image on your Drive Recorder, copy the image from the Download Center to the **images** folder.

   The default location for this folder is: `..\ETASData\DriveRe-corder<Version>\RescueStickCreator\images`

3. Connect the USB stick to your local PC.

4. In the **RescueStickCreator** folder, double click `start.bat`.

   ETASData > DriveRecorder7.3 > RescueStickCreator

   Name
   - externalDependencies
   - files
   - images
   - utils
   - .gitignore
   - createRescueStick.ps1
   - README_de.pdf
   - README_en.pdf
   - README_fr.pdf
   - README_jp.pdf
   - **start.bat**
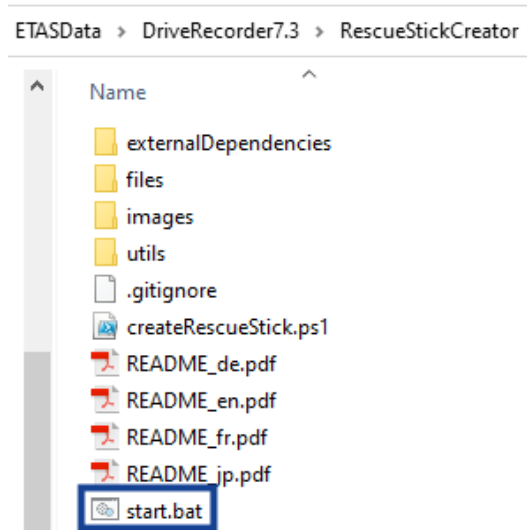
   The **Administrator: Windows Power Shell** window opens.

5. In the **Administrator: Windows Power Shell** window, select the USB device that you want to convert into the USB Rescue Stick and press <ENTER>.
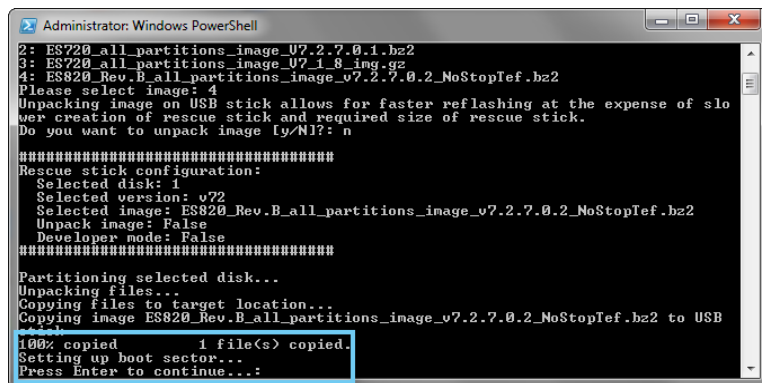
6. Select the image that you copied from the Download Center and press <ENTER>.

7. Wait until the **Administrator: Windows PowerShell** window displays the following message (framed in blue):

The creation of your USB Rescue Stick is finished. You can continue with "Flashing the Drive Recorder via the USB Rescue Stick" below.

3.8.2   Flashing the Drive Recorder via the USB Rescue Stick

As a prerequisite, you need a prepared USB Rescue Stick, see "Creating the USB Rescue Stick" on the previous page.

Before flashing your Drive Recorder, note the following:

- If the Drive Recorder hard disk is not encrypted, a backup of the license file is generated on the USB Rescue Stick and restored on the Drive Recorder during the flashing procedure. The same applies for hardware configuration files..

- If the ...\Configuration\ES720Settings.xml hardware settings file on the USB Rescue Stick is company-specific, the hardware settings file on the USB Rescue Stick overwrites the device-specific hardware settings file on your Drive Recorder.

  Otherwise, the device-dependent hardware settings file on your Drive Recorder remains unchanged.

1. Place the created USB Rescue Stick into a USB port of your Drive
   Recorder.

   The preferred port is 3.0.

2. Unplug all other stacked or connected devices and cables.

3. Restart the Drive Recorder.

   Flashing of the Drive Recorder starts. It takes about 15 minutes.

4. Wait until flashing is finished, which is the case when the Drive
   Recorder enters the low power standby mode.

5. Unplug the USB stick and activate the Drive Recorder.

   The restart scripts are launched.

6. Wait until the firmware update is finished.

   An ongoing firmware update is indicated by the ON LED and the
   MEM LED blinking synchronously. When the firmware update is
   finished, both LEDs stop blinking.

   The Drive Recorder reboots.

   When the ON LED is ON permanently, rebooting is finished.

NOTICE

Risk of system breakdown

If you interrupt the ongoing firmware update, it is possible that flashing fails
in such a mode that the Drive Recorder system cannot be recovered even by
restarting the flashing procedure.

In this case, use the "Contact Information" on page 36 and send your Drive
Recorder to ETAS for repair.

3.9   Upgrading and Downgrading

3.9.1   Drive Recorder Configurator

To upgrade the Drive Recorder Configurator, follow the same steps as
described in "Installing the Drive Recorder Configurator" on page 15. Down-
grading is possible in the same way.

In case of upgrading, the current Drive Recorder Configurator version is auto-
matically deleted first. An exception is upgrading from Drive Recorder Con-
figurator V7.2 to Drive Recorder Configurator V7.3. In this case, the older
version also remains on your PC.

The data files on your local PC remain unchanged upon upgrading or down-
grading.

3.9.2   Drive Recorder Service Pack

Upgrading from V7.3.x to V7.3.(x+n) is possible by following the instructions in "Installing the Drive Recorder Service Pack" on page 20. All files in the "Data Folder" on page 16 are preserved upon upgrading.

Upgrading from V7.2 to V7.3 as well as downgrading from any version is only possible by using the Drive Recorder image with the corresponding version. Follow the steps described in "Resetting the Drive Recorder System to Factory Settings" on page 21. In case the hard disk is encrypted, use the USB Security Key to unlock the hard disk first. Then the files in the `Configurations`, `Runtime`, `LogFiles`, and `Security` folders are preserved upon upgrading or downgrading. For more information about these folders, see "Data Folder" on page 16.

3.10   Licensing

The ES820 Drive Recorder is delivered with a MAC-based license including an INCA version on the Drive Recorder.

For INCA add-ons, you have to purchase an additional license for each add-on. You can obtain the license file required for licensing either from your tool coordinator or through a self-service portal on the ETAS Internet Site https://license.etas.com. To request the license file, you have to enter the activation number which you received from ETAS during the ordering process.

3.10.1   Installing the License on the Drive Recorder

The Drive Recorder must be turned on and connected to your local PC. The ON LED must be lit permanently.

To connect the Drive Recorder to your local PC, open the Drive Recorder Configurator and click **File** > **Connect to Drive Recorder**. Enter the IP 192.168.40.228 and click **OK**.

To install a license on the Drive Recorder

The installation of the license file requires the service mode (see step 3 below). For more information on the service mode, see "Using the Service Mode" on page 27.

1. Copy your license file (`*.lic`) into your Drive Recorder data folder. The default folder on your PC is:

   `..\ETASData\DriveRecorder<Version>\Licenses`

2. Open the Drive Recorder Configurator.

3. Click **Tools** > **Enter Service Mode**.

   The Drive Recorder is rebooting. Wait until the ON LED and the MEM LED are both blinking. Then, the device is in the service mode.

4. In the **Tools** menu, select **File Transfer from/to Drive Recorder**.

The **File Transfer from/to Drive Recorder** dialog window opens.

5. In the **Folders on the local PC** window area, select the desired license from the **Licenses** folder.

6. In the **Folders on the Device** window area, select the **Licenses** folder.

7. Enable **Overwrite existing**.

8. Click ➡.

The license file is now installed on the Drive Recorder.

9. Click **Close**.

10. Click **Tools** > **Quit Service Mode**.

The Drive Recorder reboots. When rebooting is finished, the ON LED is permanently lit and the license is updated.

3.11   Uninstalling

To uninstall the Drive Recorder Configurator

1. In the Windows Start menu ⊞, select ⚙**Settings** > **Apps**.

The **Apps and Features** window opens.

2. In the **Apps and Features**, select the Drive Recorder Configurator and click **Uninstall**.

The Drive Recorder Configurator is uninstalled from your local PC.

4   Administration

4.1   Installing 3rd Party Software

If you want to install 3rd party software on the Drive Recorder, the steps in "Preparing to Install Software on the Drive Recorder" on page 17 must be finished.

To install 3rd party software on the Drive Recorder, like drivers or 3rd party hardware configuration tools, follow the steps in "Using the Service Mode" below.

> **ℹ️ Note**
>
> In this document, only the general procedure for the installation of 3rd party software is described.
>
> You can find product-specific installation and configuration instructions in the Drive Recorder Configurator - Online Help, in the sections "Configuring 3rd Party Hardware" and "Drive Recorder Display App".

4.2   Using Remote Desktop Connection

For certain tasks, such as installing 3rd party software on the Drive Recorder, you must establish a remote connection.

To connect to the Drive Recorder from your local PC via Remote Desktop Connection

Make sure that the ON LED of your Drive Recorder is lit permanently and that you are connected to the Drive Recorder by the Drive Recorder Configurator.

1. On your local PC, open the **Remote Desktop Connection** Windows App.

2. Enter the following IP adress and User Name:

   Computer: 192.168.40.228

   User Name: DriveRecorder

3. Click **Connect**.

   The **Windows Security** window opens.

4. In the **Windows Security** window, enter the following login data:

   Password: etasdr

   Click **OK**.

   You are remotely connected to the Drive Recorder.

4.3   Using the Service Mode

The service mode allows carrying out installations and/or configurations on the Drive Recorder in such a way that they are preserved on the Drive Recorder even after a power cycle (ON/OFF), after wake-up, and after reconnecting the

Drive Recorder.

> **ℹ Note**
>
> The service mode replaces the "persist" option of Drive Recorder V7.2. For some features, like hard disk encryption, the service mode is automatically applied by the Drive Recorder. In these cases, a dialog window is displayed for information.

The following tasks are possible in the service mode:

- Installing drivers
- Connecting 3rd party hardware
- Creating hardware configuration files
- Creating recording job configuration files
- Encrypting and decrypting the hard disk

  In this case, the service mode is entered automatically.

- Transferring files from the Drive Recorder to the local PC and vice versa

The following tasks are *not* possible in the service mode:

- Applying a hardware configuration
- Applying a recording job
- Running a recording job or an experiment
- Installing a Service Pack
- Applying an archive
- Automatic file transfer

To use the service mode

1. To connect the Drive Recorder to your local PC, open theDrive Recorder Configurator and click **File** > **Connect to Drive Recorder**. Enter the IP 192.168.40.228 and click **OK**.

2. Make sure that the Drive Recorder is in the active idle state, which is the case when the ON LED is lit permanently.

3. In the menu bar, click **Tools** > **Enter Service Mode**.

   The Drive Recorder performs a restart. Wait until the ON LED and the MEM LED are both blinking. Then, the device is in the service mode.

4. If you want to install 3rd party software on the Drive Recorder and make configuration chages in 3rd party software, connect to the Drive Recorder from your local PC via Remote Desktop Connection.

   For other use cases, you can skip this step.

    i. On your local PC, open the **Remote Desktop Connection** Windows App.

    ii. In the **Computer** field, enter the following IP adress:

      192.168.40.228

    iii. Click **Connect**.

      The **Windows Security** window opens.

    iv. In the **Windows Security** window, enter the following login data:

      Password: etasdr

      Click **OK**.

      You are remotlely connected to the Drive Recorder.

5. On the Drive Recorder, make the installations or configuration changes that shall persist.

6. In the menu bar, click **Tools** > **Quit Service Mode**.

The Drive Recorder restarts and quits the service mode. The device reboots. Wait until the ON LED is lit permanently again. The installation of software is finished and the settings you have made remain on the Drive Recorder. You can now continue to use the device as usual.

4.4   Managing Data Security

To protect data that are stored on the hard disk of the Drive Recorder, the following measures are available from Drive Recorder V7.3:

You can access the security options via the Drive Recorder **Hardware Configuration** window and save the security settings in the Drive Recorder hardware configuration.

If you lose the USB Security Key for your device, a way to reaccess the hard disk is to reset the Drive Recorder to the factory settings by using the USB Rescue Stick.

NOTICE

Risk of Data Loss

If you reset the Drive Recorder to the factory settings by the USB Rescue Stick, all your measurement data on the Drive Recorder hard disk are lost. From the `..\ETASdata\DriveRecorder<Version>` data folder, only data in the `Configurations`, `Runtime`, `LogFiles`, `Licenses`, and `Security` folders are preserved.

For an encrypted Drive Recorder, the device-specific hardware configuration and the license file are lost as well.

— Transfer your data to a different storage location regularly.

— Make sure that you have a backup USB Security Key for your Drive Recorder.

— Save the license file at a secure location.

4.4.1 Encrypting the Hard Disk and Creating the USB Security Key

When the Drive Recorder Configurator and the Drive Recorder Service Pack are installed, you can encrypt the Drive Recorder hard disk. During this process, a device-specific USB Security Key is created. ETAS recommends creating a backup USB Security Key for each encrypted Drive Recorder as well.

To encrypt the hard disk of your Drive Recorder

To create the device-specific USB Security Key and a backup USB Security Key, you need two USB sticks.

1. Connect one of the USB sticks to an appropriate USB port of your Drive Recorder.

2. To connect the Drive Recorder to your local PC, open the Drive Recorder Configurator and click **File** > **Connect to Drive Recorder**. Enter the IP 192.168.40.228 and click **OK**.

3. Open an existing hardware configuration on the connected Drive Recorder. To do this, proceed as follows:

   — In the menu bar, select **File** > **Open From Device** > **Open Hardware Configuration From Device**.

   The **Hardware Configuration** dialog window opens with the stored properties.

4. Click **Device Options** > **Hard Disk Encryption** > **Encrypt Disk**.

   A wizard leads you through the hard disk encryption process. It takes about 30 minutes.

   Additionally, the USB stick now serves as a device-specific USB Security Key for your Drive Recorder.

5. To create a backup USB Security Key, insert the other USB stick into an appropriate USB port of your Drive Recorder.

6. Click **Create USB Security Key**.

   A backup USB Security Key is created for your device.

NOTICE

Risk of data loss

— Do not interrupt the hard disk encryption. Interruption leads to data corruption.

— The encryption process assigns the USB Security Key the name `ETAS-SECURE-KEY`. You must not change this name, otherwise the security key does no longer work.

4.4.2 Using the USB Security Key

To access the data of an encrypted Drive Recorder hard disk, you need the device-specific USB Security Key.

- Connect the USB Security Key to an appropriate USB port of the Drive Recorder.

  You can insert the USB Security Key either before you connect or after you have connected to the Drive Recorder from your local PC. Now you can access the data on the encrypted Drive Recorder hard disk.

Note

The USB Security Key unlocks the Drive Recorder hard disk for one power-up period after wake-up. After wake-up, you can disconnect the USB Security Key. If the Drive Recorder is switched off or falls into the standby mode, you must insert the USB Security Key again to make the Drive Recorder hard disk accessible after the next wake-up.

4.4.3 Replicating a USB Security Key

To create a backup USB Security Key for a specific device, you need the already encrypted Drive Recorder, the device-specific USB Security Key and another USB stick.

1. Connect the USB Security Key to an appropriate USB port of your Drive Recorder.

2. To connect the Drive Recorder to your local PC, open theDrive Recorder Configurator and click **File** > **Connect to Drive Recorder**. Enter the IP 192.168.40.228 and click **OK**.

3. Wait until the ON LED is permanently lit. The hard disk of the Drive Recorder is then accessible. Now you can remove the USB Security Key.

4. Connect the USB stick that is considered as backup.

5. Open an existing hardware configuration on the connected Drive Recorder. To do this, proceed as follows:

   — In the menu bar, click **File** > **Open From Device** > **Open Hardware Configuration From Device**.

     The **Hardware Configuration** dialog window opens with the stored properties.

6. Click **Device Options** > **Hard Disk Encryption** > **Create USB Security Key**.

   The USB stick now serves as an additional device-specific USB Security Key for your Drive Recorder.

NOTICE

Risk of data loss
— Do not interrupt the replication process. Interruption leads to data corruption.

— The encryption process assigns the USB Security Key the name `ETAS-SECURE-KEY`. You must not change this name, otherwise the key does no longer work.

4.4.4   Decrypting the Hard Disk

To decrypt the hard disk of your Drive Recorder, you need the device-specific USB Security Key.

1. Connect the USB Security Key to an appropriate USB port of your Drive Recorder.

2. To connect the Drive Recorder to your local PC, open theDrive Recorder Configurator and click **File** > **Connect to Drive Recorder**. Enter the IP 192.168.40.228 and click **OK**.

3. In the menu bar, select **File** > **Open From Device** > **Open Hardware Configuration From Device**.

   The **Hardware Configuration** dialog window opens with the stored properties.

4. Click **Device Options** > **Hard Disk Encryption** > **Decrypt Disc**.

   A wizard leads you through the decryption process. It takes about 30 minutes.

NOTICE

Risk of data loss

Do not interrupt the hard disk decryption. Interruption leads to data corruption.

4.4.5   Using FTPS or SFTP

To encrypt data during transmission via FTP, you can select FTPS or SFTP.

<u>To select the security option for FTP</u>

1. Open the Drive Recorder Configurator.

2. In the menu bar, click **File** > **Open from Device** > **Open Hardware Configuration from Device**.

   The **Hardware Configuration** window opens.

3. In the **Hardware Configuration** window, click **File transfer settings**.

4. In the **Server settings** window area, select the **Security type None**, **FTPS**, or **SFTP**.

5. Click **Apply on Drive Recorder**.

---

i   **Note**

If you apply FTPS or SFTP, the data is only encrypted during transmission. To protect the data also at the receiving location or on intermediary servers, use the end-to-end encryption feature which is described in the next chapter

---

4.4.6   Using End-to-End Encryption

To transfer your data securely and to protect it on intermediary servers, you can select the option for end-to-end encryption in the **File transfer settings** of the **Hardware Configuration** window. You can save this option in your Drive Recorder hardware configuration and apply it to the Drive Recorder. For this purpose, see <u>"To apply end-to-end encryption for file transfer" on the next page</u>.

A hybrid encryption method is used, which combines symmetric encryption of the data and asymmetric encryption of the symmetric key. The asymmetric encryption uses the public key / private key method.

- At the sender's end, a random, unique key is generated for each file transfer session. This key is used as the symmetric key to encrypt the files. For secure transmission to the receiver, the symmetric key is encrypted by a public key. Then each encrypted file is transmitted along with the encrypted symmetric key. For this purpose, the encrypted

symmetric key is copied for each file and the file name is adapted as follows:

— Encrypted file: `<filename>.enc`

— Encrypted symmetric key: `<filename>.key`

- The receiver uses his private key to decrypt the symmetric keys. Then the receiver can decrypt each file by its respective symmetric key.

To provide the public key and algorithms for key encryption and file encryption

The public key has to be provided by your company. The Drive Recorder supports the XML file format. The PEM file format is not supported.

ETAS provides the **RSA** algorithm for key encryption and the **AES-256** algorithm for file encryption by default. You can use your own algorithms as well. A .Net DLL file is needed that references the following file:

`C:\ETAS\DriveRecorder<Version>\Etas.Cryp-`
`tography.Contracts.dll`

Implement the interface `ISymmetricCryptographyAlgorithm` for the file encryption algorithm and `IAsymmetricCryptograhpyAlgorithm` for the key encryption algorithm.

- To transfer the security files from your local PC to the Drive Recorder, in the Drive Recorder Configurator, click **Tools** > **File Transfer** and use the **File transfer** window to copy the files to the appropriate directories:

  — Store the XML file for the public key on your Drive Recorder at the following location:

    `..\ETASData\DriveRecorder<Version>\Se-`
    `curity\Certificates`

  — Store the .Net DLL file for the key encrypion algorithm at the follwing location:

    `..\ETASData\DriveRecorder<Version>\Security`

  — Store the .Net DLL file for the file encryption algorithm at the following location:

    `..\ETASData\DriveRecorder<Version>\Security`

> **i** **Note**
>
> If you have questions about the implementation of the public key and encryption algorithms, use the "Contact Information" on page 36 to ask ETAS for help.

To apply end-to-end encryption for file transfer

The Drive Recorder must be connected to your local PC.

1. In the Drive Recorder Configurator, open the **Hardware Configuration** window by one of the following options:

   — Click **File** > **New** > **New Hardware Configuration**

   — Click **File** > **Open from File** > **Open Hardware Configuration from File**

   — Click **File** > **Open from Device** > **Open Hardware Configuration from Device**

   The **Hardware Configuration** window opens.

2. On the left, click **File transfer settings** > **Encryption (E2E)** .

3. In the right part of the window, make the following selections:

   — Select **End-to-end encryption**.

   — Select the **Path to public key** from the drop-down menu. This is your public key.

   — Select the **Key Encryption Algorithm** from the drop-down menu.

   — Select the **File Encryption Algorithm** from the drop-down menu.

4. To select the file types that shall be encrypted, click **File transfer settings** > **Automatic transfer settings**. Select the file types and the option **To Share**.

5. To save your settings to the Drive Recorder hardware configuration, click **Safe to File and Close** or **Apply to Drive Recorder**, depending on whether you have opened the hardware configuration from a file or from the device.

   End-to-end encryption is now saved to the current hardware configuration. After clicking **Apply to Drive Recorder**, end-to-end encryption is applied to all file types that are selected in the **Automatic transfer settings**.

   At the receiving location, the file names for the encrypted files and the respective keys are as follows:

   — Encrypted file: `<filename>.enc`

   — Encrypted symmetric key: `<filename>.key`

   The receiver can use the private key to decrypt the symmetric keys. Each file can then be decrypted by its respective symmetric key.

5   Contact Information

ETAS Headquarters

ETAS GmbH

Borsigstraße 24	Phone:	+49 711 3423-0
70469 Stuttgart	Fax:	+49 711 3423-2106
Germany	Internet:	www.etas.com

ETAS Subsidiaries and Technical Support

For details of your local sales office as well as your local technical support team and product hotlines, take a look at the ETAS website:

ETAS subsidiaries	Internet:	www.etas.com/en/contact.php
ETAS technical support	Internet:	www.etas.com/en/hotlines.php

Index