

ETAS INCA V7.5



Installation Guide

Copyright

The data in this document may not be altered or amended without special notification from ETAS GmbH. ETAS GmbH undertakes no further obligation in relation to this document. The software described in it can only be used if the customer is in possession of a general license agreement or single license. Using and copying is only allowed in concurrence with the specifications stipulated in the contract.

Under no circumstances may any part of this document be copied, reproduced, transmitted, stored in a retrieval system or translated into another language without the express written permission of ETAS GmbH.

© Copyright 2024 ETAS GmbH, Stuttgart

The names and designations used in this document are trademarks or brands belonging to the respective owners.

MATLAB and Simulink are registered trademarks of The MathWorks, Inc. See [mathworks.com/trademarks](https://www.mathworks.com/trademarks) for a list of additional trademarks.

INCA V7.5 | Installation Guide R01 EN | 03.2024

Contents

1	Introduction	5
1.1	Intended Use	5
1.2	Target Group	5
1.3	Classification of Safety Messages	5
1.4	Safety Information	6
1.5	Data Protection	6
1.6	Data and Information Security	7
2	Preparing to Install	8
2.1	Package Contents	8
2.2	System Requirements	8
2.3	Privileges	9
2.4	Firewall Configuration	10
2.5	Configuring the Virus Scans	11
3	Installing the Software	12
3.1	Using the Service Pack Installer	12
3.2	Using the Single Installation	15
3.3	Installing Side by Side	16
3.4	Updating the Software	17
4	Licensing the Software	18
5	Addressing and Configuring the Network Adapter	19
6	Customizing the Installation	20
6.1	Customizing the Installation of the Service Pack Installer	20
6.1.1	Setting the Installation Behavior	20
6.1.2	Setting the Installation Behavior via Command Line Arguments	22
6.1.2.1	Command Line Arguments	23
6.1.2.2	Error Codes	25
6.2	Customizing the Single Installation	27
6.2.1	Setting the Installation Behavior	27
6.2.2	Setting the Licensing Behavior	29
7	Uninstalling the Software	32
8	Troubleshooting	33
8.1	Personal Firewall Blocks Communication	33

8.1.1	Cause: Permissions Given Through the Firewall Block ETAS Hardware	33
8.1.2	Cause: Permissions Given Through the Firewall Block XCP on Ethernet	34
8.1.3	Cause: Permissions Given Through the Firewall Block Diagnostics over IP (DoIP)	34
8.1.4	Change Personal Firewall Settings	34
8.2	Network Adapter Cannot Be Selected via Network Manager	36
8.3	Installation Failed	36
9	Contact Information	38
Index	39

1 Introduction

1.1 Intended Use

INCA and INCA add-ons are developed and approved for automotive applications and procedures as described in the user documentation for INCA and INCA add-ons.

ETAS GmbH cannot be made liable for damage that is caused by incorrect use and not adhering to the safety information.

1.2 Target Group

This software product and this user guide address qualified personnel working in the fields of automotive ECU development and calibration, as well as system administrators and users with administrator privileges who install, maintain, or uninstall software. Specialized knowledge in the areas of measurement and ECU technology is required.

1.3 Classification of Safety Messages

Safety messages warn of dangers that can lead to personal injury or damage to property:



DANGER

DANGER indicates a hazardous situation that, if not avoided, will result in death or serious injury.



WARNING

WARNING indicates a hazardous situation that, if not avoided, could result in death or serious injury.



CAUTION

CAUTION indicates a hazardous situation that, if not avoided, could result in minor or moderate injury.

NOTICE

NOTICE indicates a situation that, if not avoided, could result in damage to property.

1.4 Safety Information

Observe the following safety information when working with INCA and INCA add-ons:

**WARNING****Risk of unexpected vehicle behavior**

Calibration activities influence the behavior of the ECU and the systems that are connected to the ECU.

This can lead to unexpected vehicle behavior, such as engine shutdown as well as breaking, accelerating, or swerving of the vehicle.

Only perform calibration activities if you are trained in using the product and can assess the possible reactions of the connected systems.

**WARNING****Risk of unexpected vehicle behavior**

Sending messages via bus systems, such as CAN, LIN, FlexRay, or Ethernet, influences the behavior of the systems connected to it.

This can lead to unexpected vehicle behavior, such as engine shutdown as well as breaking, accelerating, or swerving of the vehicle.

Only perform the sending of messages via a bus system if you have sufficient knowledge in using the respective bus system and can assess the possible reactions of the connected systems.

Adhere to the instructions in the ETAS Safety Advice and the safety information given in the INCA help and user guides. Open the ETAS Safety Advice in the INCA help menu ? > **Safety Advice**.

1.5 Data Protection

If the product contains functions that process personal data, legal requirements of data protection and data privacy laws shall be complied with by the customer. As the data controller, the customer usually designs subsequent processing. Therefore, he must check, if the protective measures are sufficient.

1.6 Data and Information Security

To securely handle data in the context of this product, see the INCA Help section “Data and Information Security”.

2 Preparing to Install

This chapter contains information on the scope of delivery as well as hardware and software requirements to install the software.

2.1 Package Contents

The installation package or the installation DVD contains the following:

- INCA, MDA, and ETK Tools
- INCA add-ons
- Hardware Service Pack (HSP)
- Documentation:
 - INCA help
 - Manuals
 - Video tutorials



Note

For further information about downloading the installation package, see ["Installing the Software" on page 12](#).

2.2 System Requirements

The table below contains the minimum and the recommended requirements. The minimum requirements ensure that the software will run smoothly with smaller projects. The recommended requirements ensure that the software will operate very efficiently. Consider that large ECU projects and experiments require more memory.

For information on the causes influencing the INCA performance, see "Performance Tips and Tricks", which you will find in the **Manuals** folder of your INCA installation.



Note

For further information about the system requirements, see the release notes.

	Minimum system requirements	Recommended system requirements
General hardware	<ul style="list-style-type: none"> – Network adapter – DVD-ROM drive (in case of installation from DVD) 	<ul style="list-style-type: none"> – Network adapter – DVD-ROM drive (in case of installation from DVD)
Processor	<ul style="list-style-type: none"> – 2 GHz 	<ul style="list-style-type: none"> – 3 GHz quad core processor or equivalent
RAM	<ul style="list-style-type: none"> – 2 GB 	<ul style="list-style-type: none"> – 16 GB
Graphics card	<ul style="list-style-type: none"> – Resolution of at least 1024 x 768 – 256 MB RAM – 16-bit color and DirectX 9 	<ul style="list-style-type: none"> – Resolution of at least 1280 x 1024 – 1 GB RAM – 32-bit color and DirectX 9
Required free disk space	<ul style="list-style-type: none"> – 5 GB (not including the size for user data) 	<ul style="list-style-type: none"> – >10 GB
Operating system	<ul style="list-style-type: none"> – WINDOWS® 10, Version 1803 or higher (64-bit) – WINDOWS® 10 Enterprise, LTSC 2016 or higher (64-bit) – WINDOWS® 11 (64-bit) – WINDOWS® Server 2016/2019/2022 (64-bit) 	<ul style="list-style-type: none"> – WINDOWS® 10 (64-bit) – WINDOWS® 11 (64-bit)
English, French, Japanese, Chinese, and German operating systems are supported.		

2.3 Privileges

Administrator Privileges

You need administrator privileges for the following cases:

- Installing the software
- Accessing a specific version via COM API without re-registering the software

User Privileges

To work with the software, each user must have read and write access for the following folders and directories:

- Registry folder and all subfolders:
 - for INCA:
 - `HKEY_LOCAL_MACHINE\SOFTWARE\ETAS`
 - for some 32 bit components related to INCA operation:
 - `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\ETAS`
- TEMP directory used by INCA; the TEMP directory is determined during the INCA installation.
- Installation directory
- Shared components in ETASShared15 (e.g. `c:\Program Files\Common Files\ETAS\ETASShared15`)
- Directory for the program data (e.g. `c:\ETASData`) and all subdirectories
- Common files (`c:\Program Files\Common Files\ETAS`)
- Directory for the ETAS log files (e.g. `c:\ETAS\LogFiles, %AppData%\ETAS\Setup`) and all sub directories

In case of remote access, the same user privileges are required.

2.4 Firewall Configuration

The firewall used on the client PC must be configured in such a way that it does not block the communication to the measure and calibration hardware used by INCA. For further information on configuring the ports, refer to the user documentation of your firewall software.

Details on the ports that must be given permission by the firewall can be found in section ["Troubleshooting" on page 33](#).

2.5 Configuring the Virus Scans

Virus scans may reduce the system performance significantly, sometimes to such an extent that the system seems to freeze and recordings get unusable.

To avoid performance losses caused by virus scans

1. Exclude the following software paths¹⁾ from online virus scans:
 - <drive>:\Program Files\ETAS
 - <drive>:\ETAS
 - <drive>:\ETASData
 - **Temp** directory used by INCA
2. Set scheduled virus scans to times when INCA will not be used.

¹⁾ The exact paths may be different on your computer as they can be configured during installation.

3 Installing the Software

Before starting the installation, make sure that all requirements described in chapter "[Preparing to Install](#)" on page 8 are fulfilled. There are two different ways to install INCA on your computer. You can use the service pack installer or the single installation.

To download the INCA installation package

1. On the ETAS homepage, click **Download Center**.
2. Search for **INCA > INCA V7.5 > Software**.
3. Download the Installation Package (*.zip).
4. In the Windows File Explorer, select the downloaded ZIP file, right-click and select **Properties**.
5. On the **General** tab, at the Security option disable the **Unblock** button.
6. Extract the complete structure of the ZIP file.

Note

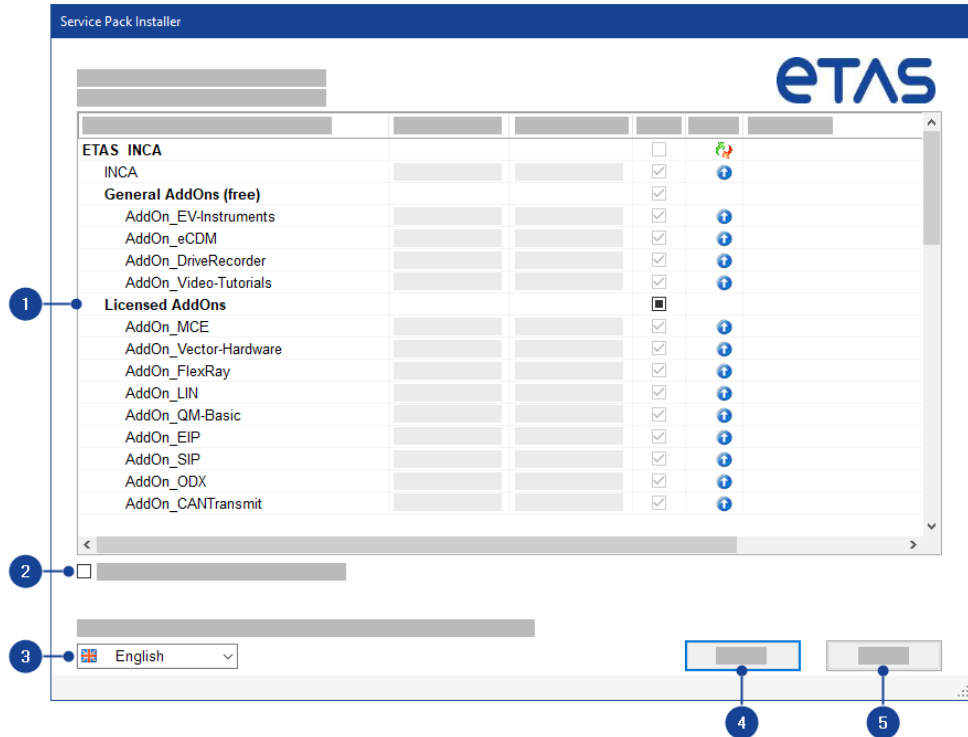
The fully qualified file name of all components of the setup and the directory name are subjects of a restriction and must fall below a certain character length. The character length is calculated individually.

The path length of the folder where you save the `Setup_ServicePack.exe` shall not exceed 80 characters.

Do not change the folder structure, the folder-names, or any name of installation executables of the installation package.

3.1 Using the Service Pack Installer

The Service Pack Installer combines installations of different programs and addons in one user dialog window. The Service Pack Installer uses default parameters for the installation. To customize the default installation, see "[Customizing the Installation](#)" on page 20.



1. The Service Pack Installer table lists all ETAS products that can be installed using the Service Pack Installer. The Installed Version column shows if and which version is already installed. The Package Version column shows the product version to be installed. In the Install column, the products to be installed can be selected.

If you are upgrading from INCA V7.4 to INCA V7.5, the Service Pack Installer automatically uses the product settings from your previous installation. Your INCA version information from these settings is displayed in the Comment column. To turn off this option, see ["Setting the Installation Behavior" on page 20](#).

The following status are displayed:

Status	Description
	Package will be processed during installation or repair.
	Package installation or repair is successful.
	Package will be downgraded to available version.
	Package will be upgraded to available version.
	No version is installed on the system.
	Package installation is interrupted to perform restart.
	Error occurred while installing or repairing the package.

2. Enables Repair mode to repair already installed versions in case the installation is corrupted.
3. Select the user interface language. The default setting is English. The language you select changes the user interface language for the Service Pack Installer and the language for newly and for all already installed INCA and INCA add-on products.
4. Starts the installation procedure.
5. Exits the Service Pack Installer when no installation process is running.

To install the software

1. Close all open ETAS software.

Note

Do not perform other software upgrades, such as an operating system upgrade, at the same time. Wait until all updates are installed and restart the computer before beginning the installation.

2. Execute the `Setup_ServicePack.exe` file from your installation directory.
The "Service Pack Installer" window opens.
3. In the **Install** column, enable your desired software products and add-ons.
To select all, enable the corresponding package on top level.
4. Select your preferred setup language.


Note

The language you select changes the user interface language for the Service Pack Installer and the language for newly installed and for all already installed INCA and INCA add-on products.

5. Click on **Install**.
The installation process is initiated.
6. Click on **Restart Options**.
The "Restart" dialog box opens.

Note

It is recommended to restart your system after the installation is finished.

Some installations require a restart in between the installation routine. In this case, a warning sign  is displayed in the Status column. After a restart, the installation will continue automatically.

7. Select the desired restart options.
8. Click **Ok**.

All your desired software products and add-ons will be installed in silent mode. This means no additional dialog windows are displayed during installation.

To install the software from a DVD

1. Close all open ETAS software.
2. Insert the DVD.
The installation routine starts automatically.
If this is not the case, execute the `Autostart.exe` file on the DVD manually.
3. Select your preferred setup language by clicking on the corresponding flag icon.
4. Click **Installation**.
5. Click **INCA V7.5/MDA V8.7/Add-ons** to install them sequentially.
The "Service Pack Installer" window opens.
6. Continue with step 3 in the [To install the software](#) instruction.

3.2 Using the Single Installation

If you use the Single INCA Installer, there is another installation routine than using the Service Pack Installer. With the single installation, you can install individual ETAS software products one by one.

To install INCA

1. Close all open ETAS software.
2. Depending on your company-specific regulations, the installation files are provided on DVD or on a network drive.
Execute the `setup.exe` file from your INCA installation directory. By default, `setup.exe` is located at `<root>\01_INCA_V7.5.<x>\00_Prod_INCA_75<x>_x64`.
If you install the software from a network drive, also execute the `setup.exe` file.
The "Installation Wizard" window opens.
3. Follow the steps of the installation wizard.

The *program files*, *program data*, *log files* and *temp files* are stored in different directories. If you uninstall or update the software later, only the program files will be deleted or overwritten. The program data will still be available. The program data includes the following:

- Databases
- User interfaces
- Demo files
- Measure files
- User profiles

 **Note**

Selecting the `Program Files` folder for INCA data files may lead to problems in INCA since the access to the `Program Files` folder depends on the Windows user rights.

Do not save INCA data files in the `Program Files` folder. Select a folder in a data area where all users have read and write access rights.

 **Note**

The language you select will change the global language settings for all already installed ETAS products.

 **Note**

You do not need to fill in the fields of the User Information form. INCA reuses the entered information for further use cases.



3.3 Installing Side by Side


You can install multiple versions of INCA side by side on your computer. That means, you can install INCA V7.5 on a computer that already has earlier INCA versions installed.

Before you install different INCA versions side by side, review the following:

- If you try to open a database from INCA V7.2 or previous version in INCA V7.3 or later, INCA will prompt you to convert this database to the new 64-bit format.
- If you use INCA V7.5 to open a database that was created in INCA V7.3 or INCA V7.4, you can later open and modify the database again in INCA V7.3 or INCA V7.4.
- If you use INCA V7.5 to open a database that was created in INCA V7.2, you can later open and modify the database again in the previous version as long as you convert your database manually into the format of the earlier version. In the Database Manager, you can convert your files manually via the import and export function, see [Exporting Database Object](#) and [Importing Database Object](#).
- If you use INCA V7.4 or earlier versions to open a database that was created in INCA V7.5, operations that were performed with implemented features that are specific to INCA V7.5 are lost.

3.4 Updating the Software

Use the Service Pack Installer to update the program. You are able to upgrade or downgrade your current INCA version. In the "Status" column, upgrades are displayed with the  icon and downgrades with the  icon.

Follow the instructions in chapter ["Using the Service Pack Installer" on page 12](#) to get a list of available updates. If there are updates available, in the Service Pack Installer table the new "Package Version" and the  icon are shown in the corresponding row.



Note

Manually update any INCA add-ons that are not included in the INCA Service Pack. Add-ons that are not updated may lead to unexpected behavior.

If you use INCA with hardware, it is also necessary to update all firmware. Use the recommended Hardware Service Pack (HSP). For corresponding versions see current release notes.

4 Licensing the Software

A valid license is required to use the software. You can obtain a license in one of the following ways:

- from your tool coordinator
- via the self-service portal on the ETAS website at www.etas.com/support/licensing
- via the ETAS License Manager

To activate the license, you must enter the Activation ID that you received from ETAS during the ordering process.

For more information about ETAS license management, see the [ETAS License Management FAQ](#) or the ETAS License Manager help.

To open the ETAS License Manager help

The ETAS License Manager is available on your computer after the installation of any ETAS software.

1. From the Windows Start menu, select **E > ETAS > ETAS License Manager**.
The ETAS License Manager opens.
2. Click in the ETAS License Manager window and press F1.
The ETAS License Manager help opens.

Remote usage of INCA

It is not allowed to use an INCA workstation license (MACHINE-BASED LICENSE) through internet or network applications, for example, Microsoft Remote Desktop, other terminal or device services. This does not apply for the operation of INCA over test bench protocols (ASAP 3, MCD-3 MC, iLinkRT).

The usage of a USER-NAMED or FLOATING license allows to access INCA via Microsoft Remote Desktop as long as it is ensured that only one user uses one license at the same time.

5 Addressing and Configuring the Network Adapter

The ETAS Network Manager is used for creating a configuration that will be used by the ETAS IP Manager. The IP Manager is responsible for dynamic IP addressing of the ETAS hardware used in your network (ETAS network).

In the Windows Start menu, select

E > ETAS INCA 7.5 > INCA V7.5 Tools > ETAS Network settings.

Follow the instructions given in the dialog. For further information about addressing and configuring the network adapter press **F1** in the ETAS Network Manager.

6 Customizing the Installation

To provide the users with the installation files, you can copy the data from the ETAS Download Center or the DVD to a network drive. A network installation has the advantage of allowing you to adjust the installation files even before actually installing the software on the computer. This allows you to set company-specific defaults.

You can configure the installation with the Service Pack Installer and also single installations of individual ETAS software products. When configuring individual ETAS software products, you can customize the installation behavior and the licensing behavior.

6.1 Customizing the Installation of the Service Pack Installer

You can change certain default settings before conducting the network installation of the Service Pack Installer.

This is done by adjusting the configuration file `Installation.xml`. This file is located in the installation directory of the Service Pack and can be opened with a text editor.

You can also use command line arguments to start and set up an installation routine for the Service Pack Installer.

6.1.1 Setting the Installation Behavior

In the configuration file `Installation.xml` of the service pack installer, you can define which programs and add-ons will be installed. This file is located in the installation directory of the service pack installer. There are three different types of XML tags within the file:

1. `<Product>` marks all software that will be installed.

This tag has two different attributes:

- `action: "install"` to install the software and `"default"` for no actions.
- `name:` The name of the software to be installed (INCA or MDA).

2. `<Category>` marks two different sections within a `<product>` tag (see table).

This tag has two different attributes:

- `action: "install"` to install the following add-ons and `"default"` for no actions.
- `name: "01_General AddOns (free)"` for free add-ons and `"02_Licensed AddOns"` for licensed add-ons.

3. `<Addon>` marks all available add-ons.

This tag has two different attributes:

- `action: "inherited"` takes the settings from the parent tag (`"install"` or `"default"`) and `"exclude"` won't install the add-on.
 - `name`: See the following table for all available add-ons.
4. `<VersionCheckFormerY>` specifies that the same product and add-on configuration that was specified during a previous installation will be used during the new installation with the Service Pack Installer.

EXAMPLE

If INCA V7.4 is already installed on the computer, the same product and add-on configuration will automatically be used when installing INCA V7.5.

The previous INCA V7.4 installation will not be changed, as the new INCA V7.5 version will be installed in parallel.

A former minor installation will be checked only as long as no current minor version is installed.

EXAMPLE

Once an INCA V7.5 Service Pack version has been installed, another INCA V7.5 Service Pack version will update or downgrade the INCA V7.5 SPz installation, but will no longer check for INCA V7.4 SPz versions.

You can turn on or off this option in the `Installation.xml` via the following settings:

true	<pre><VersionCheckFormerY>true</VersionCheckFormerY></pre> <p>Inherits the configuration from the previous minor version, for example, INCA V7.4 SPz, during the INCA V7.5 SPz installation.</p> <p>This is the default setting.</p>
false	<pre><VersionCheckFormerY>false</VersionCheckFormerY></pre> <p>The configuration has to be configured individually, only the other settings in the XML configuration file will be taken over ("Install").</p>

 **Note**

Make sure that the same products with the same name are available in the Service Pack.

Available values for the `action` parameter in the XML configuration file:

Value	Description
Default	A package installation will only be performed if this package is already installed and needs an up- or downgrade.
Install	Installation will be triggered if possible. Subsequent packages (add-ons) can only be installed when the related base product is already installed or has to be installed.
Exclude	Package will be excluded from the installation except it has a dependency to a parent package which will be upgraded or downgraded.
Inherited	The action of a subsequent package will be inherited from the parent category.

Following add-ons are available:

General Add-ons	Licensed Add-ons
AddOn_EV-Instruments	AddOn_MCE
AddOn_DriveRecorder	AddOn_Vector-Hardware
AddOn_eCDM	AddOn_FlexRay
AddOn_VN-Converter	AddOn_LIN
AddOn_Video-Tutorials	AddOn_QM-Basic
	AddOn_EIP
	AddOn_SIP
	AddOn_ODX
	AddOn_SOMEIP_MC
	AddOn_CANTransmit
	AddOn_CAN-Trace
	AddOn_INCA-VoiceRecorder
	AddOn_INCA-TOUCH
	AddOn_RDE

6.1.2 Setting the Installation Behavior via Command Line Arguments

You can use command line arguments to start and set up an installation routine for the Service Pack Installer. This means that no dialog windows are displayed and all commands are hidden during the installation routine. For example, you can

use this option to install INCA on a computer without interrupting the users' work.

Command Line Argument Example

```
Setup_ServicePack.exe [[/S |/VS | /I] | /T | /R | /Al-
lowRestart | /NoRestart | /CreateConfiguration | /NoAutoRe-
sume | /DefaultConfiguration=<filename> |
/RestartDelayTime=<mins> | /NoAutoResume | /?]
```

See below for a full description of the command line arguments. The error codes that can occur during installation are described in chapter ["Error Codes" on page 25](#).

6.1.2.1 Command Line Arguments

Argument	Description
/?;/help	Displays help window with supported command line arguments and package details that can be customized.
/S	Launches the Service Pack Installer in silent mode. This means that no dialog windows of the installation routine are displayed. All commands are hidden. For example, you can use this option to install INCA on a computer without interrupting the users' work. Note, that this argument only works in combination with the /NoRestart or /AllowRestart argument.
/VS	Launches the Service Pack Installer in very silent mode (no GUI and system tray notifications). Do not combine with /s argument.
/I	Package installations are started in interactive mode (GUI mode).
/T	Tests if there are packages to install and shows the results in the GUI.
/R	Forces repair/re-installation of all already installed packages.

Argument	Description
/NoRestart	Skips any restart request during installation if required. Use this parameter in combination with the silent parameter /s to omit a restart that might be necessary at the end of the installation. If the restart is omitted, this will be recorded in a log message. If the silent parameter is set, either the /AllowRestart or the /NoRestart Parameter must be set too. It is not recommended to use this command because the installation may not be completed.
/AllowRestart	Allows restart of the system between installations if required.
/RestartDelayTime=<mins>	Specifies the time to delay restart if required. Should be used in combination with /AllowRestart.
/NoAutoResume	<p>Recommended for usage with automated deployments such as SCCM to take control of system restarts and automatic resume.</p> <p>Specify this to omit an automatic system restart in between the installation and automatic resume after the system restart.</p> <p>If <code>setup.exe</code> returns exit code 26, then the deployment script must perform system restart and also run the setup again after performing the system restart.</p> <p>If <code>setup.exe</code> returns exit code 31, then the deployment script must perform system restart. /NoAutoResume cannot be combined with /NoRestart Or /AllowRestart.</p>

Argument	Description
/CreateConfiguration	Generate configuration file for a given Service Pack to generate a new <code>Installation.xml</code> file with default settings.
/DefaultConfiguration =<filename>	Set XML configuration file. If not set, the default <code>Installation.xml</code> is used in parallel with <code>SetupServicePack.exe</code> .
/Clean	Strictly for usage only when the Service Pack Installer fails with error code 27 after removing the partially installed product from the Add or Remove Programs Of Programs and Features from control panel. This will clean the registry from the path <code>SOFTWARE\ETAS\History\SPI</code> .

6.1.2.2 Error Codes

The `Setup_ServicePack.exe` returns code 0 if execution has been completed successfully.

The `Setup_ServicePack.exe` returns anything $\neq 0$ if an error occurred.

The following error codes are returned when you run the `Setup_ServicePack.exe` in silent mode.

Error Code	Description
0	Installation was successful.
1	Hotfix Installation package not found in the Service Pack folder structure.
2	Related version of INCA is not installed.
3	Path to the log files cannot be obtained.
4	User cancelled the Interactive installation.
5	Installation failed or aborted.
6	Error occurred while updating log file.
8	Error occurred while closing log file.
9	Error occurred while creating log file.
10	Error occurred while creating a copy of a package INI file.
11	Error occurred while copying a package INI file into the temp folder.

Error Code	Description
12	Exception thrown on comparing available package version vs. installed version.
13	Failed to de-serialize <code>Installation.xml</code> or file path of the <code>Installation.xml</code> is configured but file does not exist or invalid arguments provided.
14	The version of an already installed package could not be retrieved from the windows registry.
15	User does not have administrative rights, installation cannot start. Prerequisites not satisfied.
16	Starting installation failed.
17	Unable to get the Hotfix number from the installation package.
18	A package file version information could not be extracted correctly.
20	Another instance of this setup is running, please complete the other installation before continuing this setup.
25	Error occurred while creating standard configuration file <code>Installation.xml</code> .
26	A product has requested system restart to complete the installation. Service Pack Installer will resume the installation automatically after a system restart is performed.
27	Service Pack Installer cannot proceed because another version of the product is partially installed. Finish a previous installation to proceed further.
28	Could not find resume configuration path or file. Try to uninstall the product via "Apps&Features", "Programs and Features" in the Control Panel, or contact package vendor.
29	Invalid resume configuration. Try to uninstall the product via "Apps&Features", "Programs and Features" in the Control Panel, or contact package vendor.
30	A system restart is pending from a previous installation. Service Pack Installer will resume the installation after a system restart has been performed.
31	Installation was successful. System restart is triggered to complete the installation.

Error Code	Description
32	\Clean failed to clean the registry Software\ETAS\History\SPI of partial installed products. If you get this error message, contact the ETAS support team.
33	Invalid command line arguments, see "Setting the Installation Behavior via Command Line Arguments" on page 22 and "Command Line Arguments" on page 23 .
34	Installation aborted due to reboot/logoff/shutdown request by the user.

6.2 Customizing the Single Installation

You can change certain default settings before conducting the network installation of each individual ETAS software product.

This is done by adjusting the configuration file

`InstallationDefaultSettings.xml` and the license file `licencing.ini` of each individual product installation. These files are located in the installation directory of each product and can be opened with a text editor.

Even if you install the ETAS products via the Service Pack Installer, the installation can be configured using configuration files of each individual installation.

The settings made in the XML files can be used for both, automated and manual installation.

6.2.1 Setting the Installation Behavior

In the `InstallationDefaultSettings.xml` file, you can define different settings of each INCA and INCA add-on product installation.



Note

Every ETAS software uses its own configuration file. Existing information, for example TEMP folder, registry entry, defined from other software will be overwritten by the current installation or configuration file.

Ensure that you always specify the same settings for all installations.

You can define the following custom parameters or variables:

- `CONTINUE_ON_TRACE_OVERFLOW`
 - `true`

INCA skips the measure data if the trace buffer identifies a trap and the data might be outdated.

- `false`
Default setting: In case of a stack overflow, the ECU does not send any data during the reinitialization.
- `IPM_AUTO_IP_RANGE`
 - `true`
Activates the "Auto IP address range" checkbox in the Network Manager by default. The ETAS Network Manager will automatically assign default IP address ranges that will be used by the selected network adapter for addressing the ETAS hardware.
 - `false`
Deactivates the "Auto IP address range" checkbox in the Network Manager by default. The user will explicitly either have to set concrete IP address ranges or accept the defaults.
- `IPM_AUTO_CONFIG_NIC`
With this parameter, you can enable or disable several network adapters at once for auto-configuration through the Network Manager.
 - `true`
Activates the "Auto Configure ETAS Network" checkbox in the Network Manager by default. This makes it possible to activate multiple network adapters at once for auto-configuration. The Network Manager will use the first adapter that is enabled for auto-configuration and that has a valid IP configuration for ETAS¹⁾. It will then configure the IP address range automatically.
 - `false`
Deactivates the "Auto Configure ETAS Network" checkbox in the Network Manager by default. The user must explicitly to select the network adapter that shall be used for the ETAS network.
- `IPM_DEFAULT_OFFSET_START` and `IPM_DEFAULT_OFFSET_END`
The default IP address range used by the ETAS tools for the IP assignation of ETAS hardware can be defined using these settings. The default value can be either empty or a 32-bit decimal value. In case the default value is empty, these settings will not be considered by INCA. As the names of the settings indicate, they are offsets relative to the NIC subnet. This means that they are valid for every NIC configuration unless they fall outside the subnet host range. In case of undefined or invalid settings, the ETAS Network Manager will use fall-back values to define the IP range. Fall-back values are `-.2` for the start IP address offset and last valid host for the NIC subnet for the end IP address offset (e.g. 192.168.40.2 - 192.168.40.254)
- `PRODINSTDIR`

¹⁾ An IP configuration is valid if the network adapter either uses a fix IP address, or if DHCP and APIPA are enabled.

- Defines the installation path for INCA.

— LIMA_INIFILE

Defines the installation path for the `licensing.ini` file. The `licensing.ini` file contains your license information.
- DO_PRELOAD

On INCA startup, the .NET framework will be preloaded to improve the duration of the opening process of the Variable Selection Dialog.
- PRODDATAINSTDIRALL

Defines the path of the working files (e.g. configuration files, databases).
- ETAS_TEMPPATH

Defines the path of the temporary files.
- ETAS_LOGPATH

Defines the path of the log files.
- ETAS_LANGUAGE

Defines the desired language.
- CREATE_UNINSTALLATION_SHORTCUT

Automatically creates an uninstallation shortcut on your desktop.
- ENABLE_ERROR_REPORTING

Enables or disables the ZIP&SEND function in case of a software error.
- EMAIL_ERROR_REPORT_TO

Defines the recipient of the reporting e-mail (ZIP&SEND function). More than one address can be defined, separated by "," (comma).
- Following variables include personal and company information. Set any default values to automatically insert them into the form within the installation.

FirstName, LastName, Company, Department, AreaCode, Phone, Language, EMail, Street, ZIPCode, City, Country.

6.2.2 Setting the Licensing Behavior

Each license-protected software can be configured in such a way that a valid license and the company-specific license settings are automatically assigned to the respective software. This means that the installed ETAS product can be used immediately after installation.

To provide users with a fully licensed software version from a network drive, you need to adapt the `Licensing.ini` file. This file is located in the installation directory of the INCA installation package and can be opened with a text editor.



Note

Every licensed ETAS software uses its own license file. Existing settings defined from other software will be overwritten from the current installation or license file.

Ensure that you always specify the same settings for all installations.

You can define the following custom parameters or variables:

— `LicenseFileName`

Defines the absolute path to the location of the license file that will be added.

— `LicensesToBorrow`

Use this setting if licenses can be borrowed from a license server. To enable the borrow mechanism, enter the name of the product or feature license (e.g. INCA, MDA). If you enter more than one license name, the names must be separated by blanks.

— `BorrowExpiryMode`

Specifies whether the borrowed license expires on a certain date or after a certain amount of days:

- `Interval`

If the `BorrowExpiryMode` is set to `Interval`, the borrowed license will expire after a certain amount of days, that is defined in the parameter `BorrowExpiryInterval`.

- `Date`

If the `BorrowExpiryMode` is set to `Date`, the borrow period will expire at a certain date which is defined in the parameter `BorrowExpiryDate`.

— `BorrowExpiryDate`

If the `BorrowExpiryMode` is set to `Date`, this parameter specifies the date when the borrow period expires. The format is `yyyy-mm-dd`.

— `BorrowExpiryInterval`

If the `BorrowExpiryMode` is set to `Interval`, this parameter specifies the length of the borrow period in days.

— `BorrowAutomaticExtensionInterval`

This parameter specifies the borrow interval in days that is applied when an automatic extension of the borrow period is executed (as defined under `ExecuteBorrowAutomaticExtensionInterval`).

— `ExecuteBorrowAutomaticExtensionInterval`

Defines at what point in time the borrow period will be extended. The parameter defines the number of days till the expiration of the current borrow period. When the borrowed license expires, the borrow period will be

extended to the interval specified under `BorrowAutomaticExtensionInterval`. The borrow period will only be extended if `AutoborrowActive` is set `true`.

- `AutoborrowActive`

If this parameter is set `true`, the borrow period will be automatically extended to the interval specified under `BorrowAutomaticExtensionInterval`.

- `Ports`

In order for multiple users to work in parallel, different ports must be defined.

7 Uninstalling the Software

To uninstall INCA, choose **Add or remove programs**, **Apps & features**, or **Programs and Features** in the Windows Control Panel.

If you only like to remove individual components, start `INCA setup.exe` from the installation directory again. It will open the maintenance mode of INCA setup.

To uninstall components individually

1. Select **Modify** in the list and click on **Next**.
2. Select or unselect your desired add-ons and click on **Next**.
The installation wizard shows your changes.
3. Click on **Modify** to confirm your selection.



Note

Never delete files or folders manually.

8 Troubleshooting

8.1 Personal Firewall Blocks Communication

The Windows operating systems come with a built-in personal firewall. On many other systems it is very common to have personal firewall software from third party vendors, such as Symantec, McAfee, or Blacklce installed. The proceedings in configuring the ports might differ for each personal firewall software used. Therefore please refer to the user documentation of your personal firewall software for further details.

Personal firewalls may interfere communication with hardware or protocols, i.e., INCA does not get any response from the ECU or cannot send a request. The automatic search for hardware typically cannot find any Ethernet hardware at all, although the configuration parameters are correct. If a firewall is blocking communication to ETAS hardware or any protocol, you must either disable the firewall software while working with ETAS software, or the firewall must be configured to give the permissions for the following use cases.

8.1.1 Cause: Permissions Given Through the Firewall Block ETAS Hardware

- Outgoing limited IP broadcasts via UDP (destination address 255.255.255.255) for destination ports 17099 or 18001.
- Incoming limited IP broadcasts via UDP (destination IP 255.255.255.255, originating from source IP 0.0.0.0) for destination port 18001.
- Directed IP broadcasts via UDP to the network configured for the ETAS application, destination ports 17099 or 18001.
- Outgoing IP unicasts via UDP to any IP in network configured for the ETAS application, destination ports 17099 through 18020.
- Incoming IP unicasts via UDP originating from any IP in the network configured for the ETAS application, source ports 17099 through 18020, destination ports 17099 through 18020.
- Outgoing TCP/IP connections to the network configured for the ETAS application, destination ports 18001 through 18020.



Note

The ports that have to be used in concrete use cases depend on the hardware used. For more precise information on the port numbers that can be used refer to your hardware documentation.

8.1.2 Cause: Permissions Given Through the Firewall Block XCP on Ethernet

- Outgoing IP multicasts for XCP Slave Detection via UDP to any IP in network, destination IP 239.255.0.0, port 5556.
- Incoming IP multicasts for XCP Slave Detection via UDP from any IP in network, destination IP 239.255.37.45, port 3745.

8.1.3 Cause: Permissions Given Through the Firewall Block Diagnostics over IP (DoIP)

- Outgoing TCP/IP connections for DoIP to the DoIP network, destination port 13400.
- Outgoing IP unicasts via UDP for DoIP to the DoIP network, destination port 13400.
- Outgoing IPv4 limited broadcasts for DoIP via UDP (destination address 255.255.255.255) for destination port 13400.
- Outgoing IPv6 broadcasts for DoIP via UDP from any IP in the network, destination IP FF02:1, port 13400.
- Incoming IP unicasts via UDP for DoIP originating from the DoIP network, destination port 13400.

8.1.4 Change Personal Firewall Settings

As an example for a firewall configuration, you will find below a description on how to configure the Windows firewall.

If you have administrator privileges on your PC, a dialog window opens if the firewall blocks an ETAS product.



Note

Consult your IT responsible and/or check the IT security policies of your company before changing your firewall configuration and reconnecting the computer to the network!

To unblock a product

1. In the "Windows Security Alert" dialog window, click on **Unblock**.
The firewall no longer blocks the ETAS product in question. This decision survives a restart of the program, or even the PC.

Instead of waiting for the "Windows Security Alert" dialog window, you can unblock ETAS products in advance.

To unblock ETAS products in the firewall control

1. In the Windows search field, enter **Control Panel**.
2. Select **Control Panel**.
The "Control Panel" window opens.

3. In the "Control Panel" window, click **System and Security > Windows Defender Firewall** to open the "Windows Firewall" dialog window.
4. In the "Windows Firewall" dialog window, in the left column, click **Advanced Settings**.

The "Windows Firewall with Advanced Security" window opens.

In this window all inbound and outbound rules are listed. Make sure that the ETAS products and services you want to use are properly configured exceptions.

5. To add a new rule, in the left column, right-click **Inbound Rules** or **Outbound Rules** (depending on your requirement).
6. In the right column, click **New Rule**.
7. In the upcoming window, choose **Port** and follow the instructions to set the new rule. You find all required information in the beginning of this chapter.

Solution using the Example of the Windows Firewall, Users without Administrator Privileges

This section addresses users with restricted privileges, for example, no system changes, write restrictions, local log in.

Working with an ETAS software product requires "Write" and "Modify" privileges within the `ETAS`, `ETASData`, and ETAS temporary directories. Otherwise, an error message opens if the product is started, and a database is opened. In this case, no correct operation of the ETAS product is possible because the database file and some INI files are modified during operation.

The ETAS software has to be installed by an administrator anyway. It is recommended that the administrator assures that the ETAS program/processes are added to the list of the Windows firewall exceptions, and selected in that list after the installation. The "Window Security Alert" window opens when one of the actions conflicting with a restrictive firewall configuration is executed.

To unblock a program (no Admin privileges)

1. In the "Windows Security Alert" dialog window, activate the option **For this program, don't show this message again**.
2. Click **OK** to close the window.

An administrator has to select the respective ETAS software in the "Exceptions" tab of the "Windows Firewall" dialog window to avoid further problems regarding hardware access with that ETAS product.

8.2 Network Adapter Cannot Be Selected via Network Manager

Cause: APIPA is disabled

The alternative mechanism for IP addressing (APIPA) is usually enabled on all Windows systems. Network security policies, however, may request the APIPA mechanism to be disabled. In this case, you cannot use a network adapter which is configured for DHCP to access ETAS hardware. The ETAS Network Manager displays a warning message.

The APIPA mechanism can be enabled by editing the Windows registry. This is only permitted to users who have administrator privileges. It should only be done in coordination with your network administrator.

To enable the APIPA mechanism

1. Open the Windows "Registry Editor".
2. Open the folder `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\`
3. Click **Edit > Find** to search for the key `IPAutoconfigurationEnabled`.
If you cannot find any instances of this registry key, the APIPA mechanism has not been disabled on your system, i.e., there is no need to enable it. Otherwise proceed with the following steps.

4. Set the value of the key `IPAutoconfigurationEnabled` to 1 to enable the APIPA mechanism.

You may find several instances of this key in the Windows registry which either apply to the TCP/IP service in general or to a specific network adapter. You only need to change the value for the corresponding network adapter.

5. Close the registry editor.
6. Restart your workstation in order to make your changes take effect.

8.3 Installation Failed

Cause: One of the required INCA or INCA add-on installations failed

If one of the required INCA or INCA add-on installations fails, the installation of the complete service pack cannot be finished.

To solve the issue, do the following

1. Restart your computer.
2. Check if all ETAS programs are closed.
3. Repeat the installation and restart the computer.

4. Check, if the installation was successful.
If not, continue with step 5.
5. To install the whole service pack or selected add-ons again, enable the checkbox **Repair mode** in the Service Pack Installer.
6. Click **Repair**.
7. Check the log files for details about the issue. The following log files are stored under

`%PROGRAMDATA%\ETAS\SETUP_ServicePack\Logs\:`

- `<date_time>_SP_Setup.log`
- `<date_time>_SP_Setup_debug.log`

or

`%PROGRAMDATA%\ETAS\SETUP\Logs\`

- `<date_time>Setup.log`
- `<date_time>Setup_debug.log`

If there is no `DefaultLogPathName` key in the registry, the logs are stored in the `%temp%` or in the `%ALLUSERPROFILE%` folder.

Additional to the service pack installer logs, there are log files related to the last product/add-on installation at `%AppData%\ETAS\SETUP`. Check the end of the log for any indication for the failure reason.

8. If the installation still fails, contact your local support.

9 Contact Information

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:

www.etas.com/hotlines

ETAS offers trainings for its products:

www.etas.com/academy



ETAS Headquarters

ETAS GmbH

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

Index

A

Addressing and Configuring the Network Adapter	19
APIPA	36

C

Command Line Arguments	23
Contact Information	38
Customizing the Installation	20

D

Data	6-7
------------	-----

E

Error Codes	25
ETAS	
Contact Information	38
ETAS Network Manager	19,27,36

F

Firewall Configuration	10,33
------------------------------	-------

H

HSP	8
-----------	---

I

INCA Add-On	8
install.ini	27
Installation Failed	36
Installing the Software	14

N

Network Adapter	9,19,27,36
Network Adapter Cannot Be Selected	36

P

Personal Firewall Blocks Communication	33
----------------------------------------------	----

S

Safety Information	6
Service Pack Installer	12
Single Installation	15
System	8

T

Troubleshooting	33
-----------------------	----

U

Uninstalling the Program	32
Updating the Program	17